HP WOLF SECURITY

The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back

AN HP WOLF SECURITY REPORT

Contents

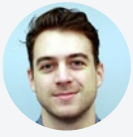
Report contributors

ALEX HOLLAND
Report author, Senior Malware Analyst at HP Inc.

JOANNA BURKEY
Chief Information Security Officer at HP Inc.

DR. IAN PRATT
Global Head of Security for Personal Systems at HP Inc.

BORIS BALACHEFF
Chief Technologist for Security Research and Innovation at HP Labs, HP Inc.



PATRICK SCHLÄPFER
Malware Analyst at HP Inc.

MICHAEL CALCE
Former black hat "MafiaBoy," HP Security Advisory Board Chairman, CEO of DecentraWeb, and President of Optimal Secure

DR. MIKE MCGUIRE
Senior Lecturer in Criminology at the University of Surrey, UK, and expert author on cybersecurity

ROBERT MASSE
HP Security Advisory Board member and Partner at Deloitte

JUSTINE BONE
HP Security Advisory Board member and CEO of MedSec

Executive Summary

The dark web has supercharged the cybercrime economy like nothing before it.

By providing an anonymous online environment in which cybercriminals can collaborate, organize, hone their skills and establish illicit shops, the dark web has allowed cybercrime to evolve into a multi-faceted, reputation-sensitive service industry.

This report, produced by HP Wolf Security in collaboration with Forensic Pathways[1] – and alongside security experts in both industry and academia – identifies how cybercriminals are now operating on a professional footing with easy-to-launch malware and ransomware attacks being offered on a "Software as a Service" basis. As a result, even people with rudimentary IT skills are now able to launch cyberattacks at targets of their choosing.

"Digital transformation has supercharged both sides of the attack-defense divide – shown, for instance, by the increasing popularity of 'as a service' offerings. This has democratized malicious activity to the point where complex attacks requiring high levels of knowledge and resources – once the preserve of advanced persistent threat (APT) groups – are now far more accessible to a wider group of threat actors," says Alex Holland, Senior Malware Analyst at HP Wolf Security's Threat Research team – and author of this report.

These complex attacks are also being fueled by the data breaches that have left billions of personal credentials available on dark-web markets for minimal sums. Many of the malware variants and exploits that are used in ransomware and data extortion attacks sell for less than $10. It's perhaps little surprise that the FBI estimates cybercrime losses in the US alone were running at an astonishing $6.9 billion in 2021.[2]

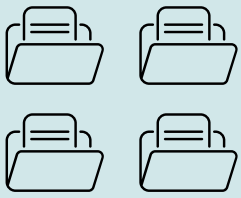
> "Digital transformation has supercharged both sides of the attack-defense divide."
>
> Alex Holland, Senior Malware Analyst at HP Inc.

Yet, while it can feel as though the odds are stacked against cyber defenders, there are huge opportunities to improve our defenses. In many ways, it is simply a case of mastering the basics. While the impact of cyberattacks has increased, and tools and techniques have evolved, the key attack vectors have remained relatively unchanged. This presents defenders with the chance to challenge whole classes of threat and enhance resilience.

5 key cybercrime facts

11 billion

Today, one data breach notification website holds over 11 billion records[3]



Over

3/4

of malware adverts listed are under $10

Custom exploits cost

$1,000-$4,000

92%

of cybercriminal marketplaces have dispute resolution services, while all allow buyers and sellers to leave reviews

91%

of marketplace adverts for exploits are under $10

Section 01

From Cyber Hobbyists to Cyber Syndicates – How Financially Motivated Cybercrime Evolved

Setting the Blueprint for Cybercrime Communities

By the mid-1990s, a thriving hacker subculture was communicating globally over Internet Relay Chat (IRC).[4] Initially, hackers sought to score bragging rights for their technical skills. But with the dotcom boom, many realized there might be serious money to be made.

"Back in the day you had to figure stuff out yourself and show off what you could do technically to be noticed. Today, only a small minority of cybercriminals really code, most are just in it for the money – and the barrier to entry is so low that almost anyone can be a threat actor. That's bad news for businesses."

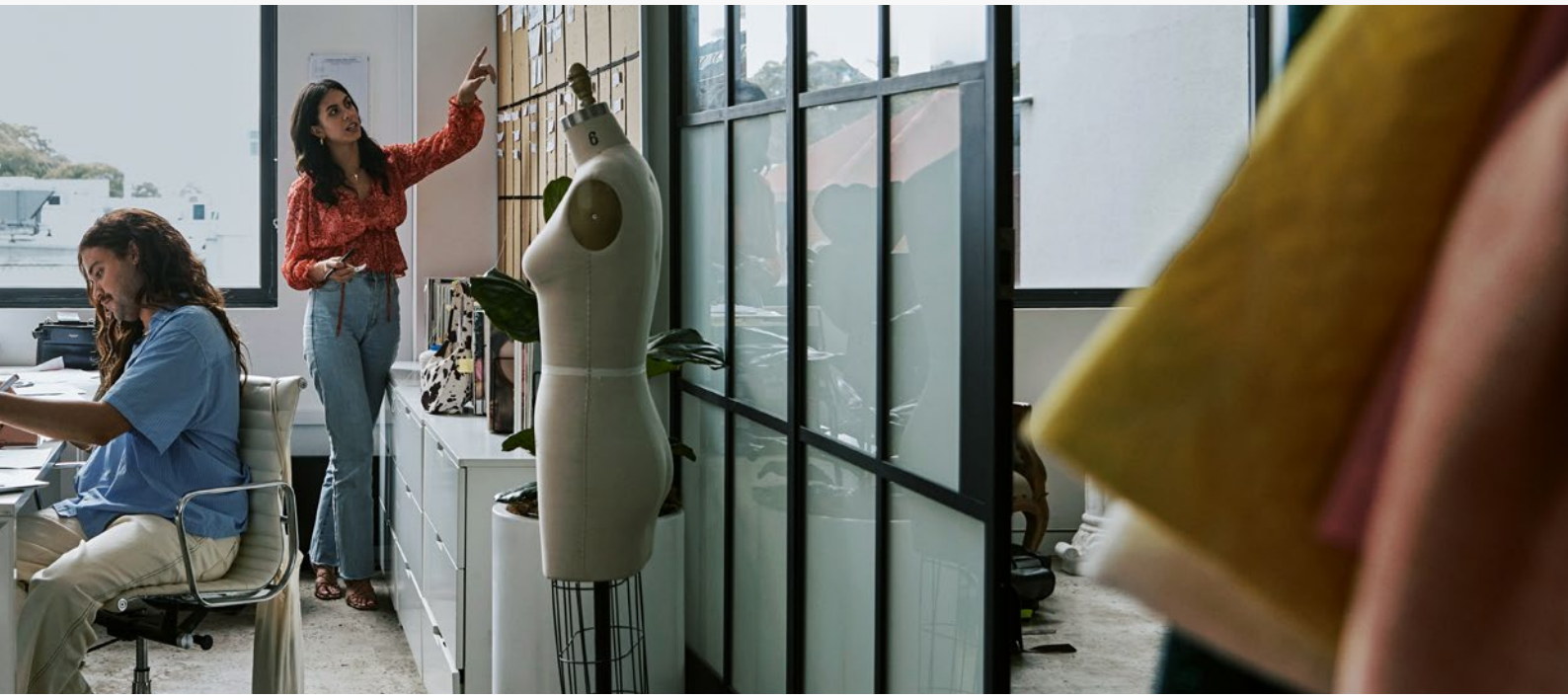
Michael Calce, HP Security Advisory Board Chairman and former hacker "MafiaBoy."

KEY POINTS

Global hacker communities started to form, sharing exploits and attack techniques.

Groups and individuals traded off kudos, demonstrating their technical prowess.

Attacks were not usually financially motivated.



DIY Cybercrime Kits Open the Cybercrime Marketplace

The launch of malware kits began to lower the skills levels needed. But these "sole trader" fraudsters had little power to scale their operations until they started collaborating and pooling skills. This led to hackers specializing in perfecting different parts of the attack chain – whether penetrating systems, developing malware or laundering stolen money and cryptocurrency.

KEY POINTS

Commoditized malware kits lowered the barriers to entry.

Cybercriminals started to pool their strengths in new networks, specializing in specific areas.

Monetization was focused on fraud and targeted online banking users instead of businesses.

IN FOCUS

ZeuS and SpyEye

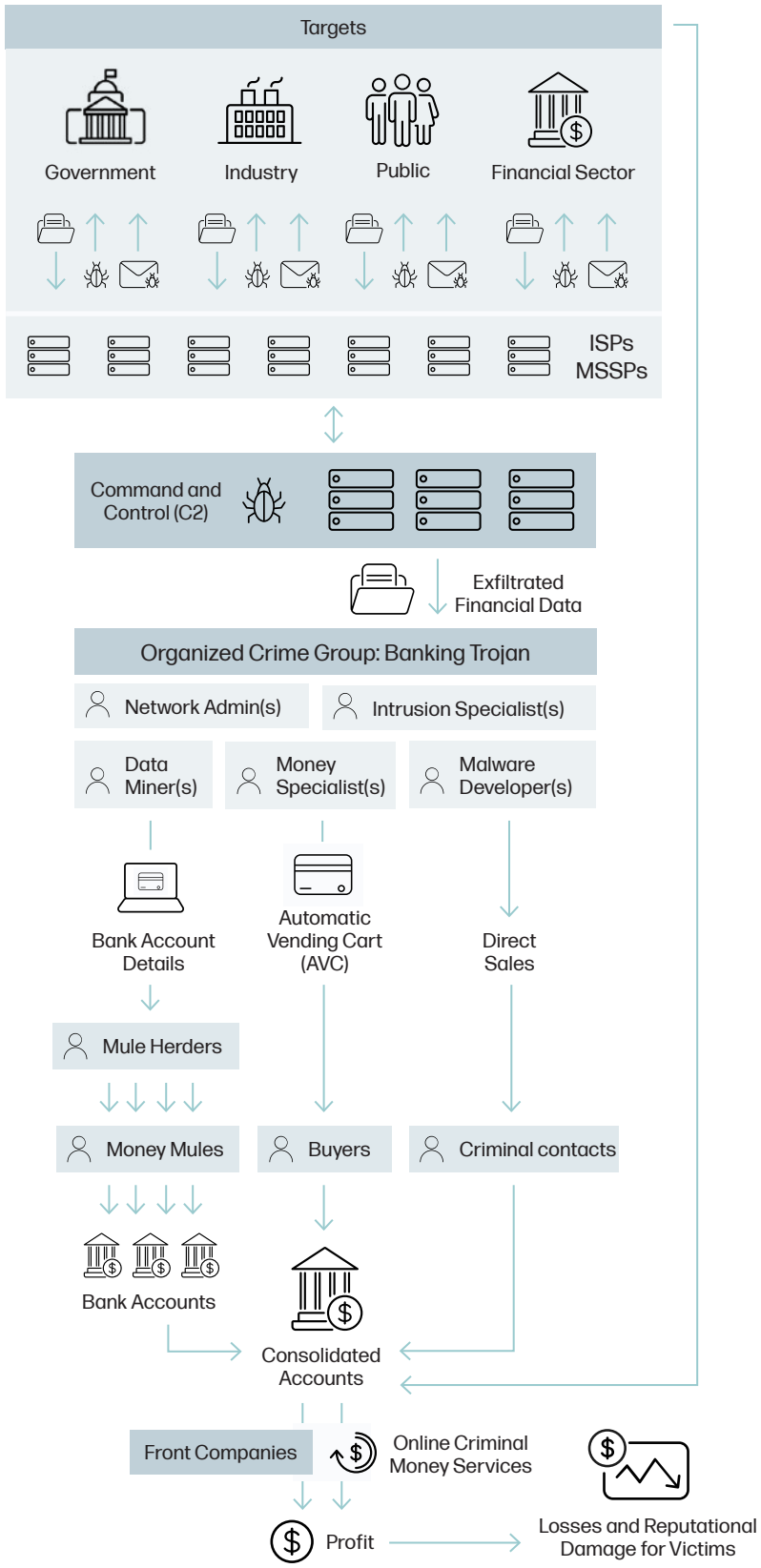
The ZeuS DIY banking trojan kit enabled people to establish, host and command a network of compromised computers – a botnet – that could fraudulently withdraw cash, or acquire credit card numbers, from many online bank accounts.[5]

It cost $8,000,[6] but in 2009 it found itself up against the $1,000 SpyEye banking trojan.[7] Besides undercutting ZeuS on price, SpyEye had a "kill ZeuS" feature to uninstall its rival if it was present on an infected PC.[8]

The ZeuS and SpyEye projects later merged,[9] but the leaking of the ZeuS source code soon afterwards led to a proliferation of cybercrime competition and a blizzard of ZeuS variants being deployed in attacks, including the ICE IX, Citadel and KINS banking trojans.[10] [11] [12]

ZeuS	$8,000
SpyEye incl. "kill ZeuS" feature	$1,000

A closed group banking trojan operation. Building on research from the UK's National Cyber Security Centre (NCSC) into organized crime groups and the cybercrime ecosystem, the chart shows the relationships between the roles, infrastructure, goods and services involved in a malware enterprise.[13]



New Monetization Methods Spur Ransomware's Rise

As law enforcement and banking security experts began gaining the upper hand – sometimes by wrestling control of botnets from cybercriminals – cryptocurrencies like Bitcoin and Monero were in ascendence. These gave cybercriminals a new, hard-to-trace way of monetizing attacks that would destroy people's data if they didn't stump up a ransom.

This growth period for destructive attacks also saw cybercriminals increase collaboration, establishing a support ecosystem in which those with different illicit skill sets sold specialized products and services. In other words, cybercriminals were beginning to offer Malware as a Service (MaaS) .

KEY POINTS

Threat actors shifted from fraud to data denial and destructive attacks.

The cybercriminal world started to mirror digital "as a service" models making attacks easier to launch.

Ransomware started to emerge as the monetization method of choice.

IN FOCUS

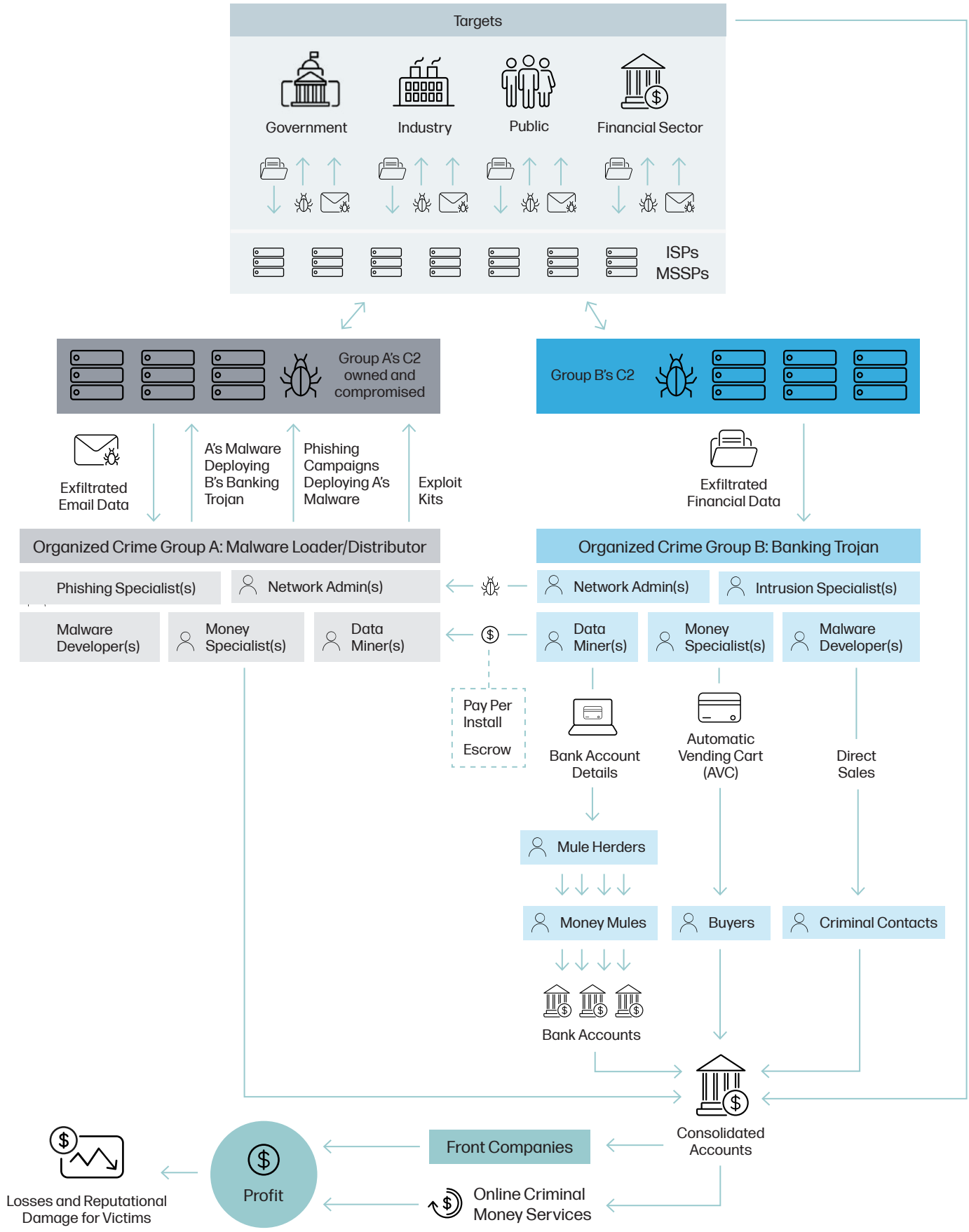
The growth of ransomware

Initially, ransomware variants like CryptoLocker relied on opportunistic attacks by targeting systems already infected by the ZeuS variant Gameover ZeuS, demanding a $700 ransom or the equivalent in Bitcoin to decrypt an infected machine's data.[14]

Attacks like WannaCry and NotPetya took this to the next level by using destructive methods to cripple critical infrastructure.[15] [16]

CryptoLocker, a ransomware variant spread via the Gameover ZeuS botnet

A chart mapping out the entities, goods and services involved in a malware distribution operation, where malware family A distributes B through an "access as a service" arrangement.[13]



Targeting Businesses To Maximize Payouts

Since 2018 cybercrime has continued its move towards service and platform business models, with threat actors tapping into complex supply chains to launch attacks using specialist "plug and play" components.

It has also become more organized and targeted. Criminals are taking much more time to understand a target's infrastructure to maximize their impact, whether that's achieving a bigger ransom or disabling a more critical piece of infrastructure.

"In the last century, the economy shifted from sole traders to mass production, to service models, to platforms like Amazon," says Dr. Mike McGuire, Senior Lecturer in Criminology, University of Surrey, UK. "The cybercrime economy did this in less than 25 years."

KEY POINTS

Cybercriminals provide specialized services in complex supply chains.

Campaigns can be launched quickly using "plug and play" services and solutions.

Businesses are targeted to maximize the impact and increase the payout.

IN FOCUS

Ransomware role profiles

Ransomware is now the cybercrime monetization method of choice, with criminals operating professionally with high levels of direct and indirect collaboration. They generally fall into the following specialized roles:

DISTRIBUTORS

Those responsible for distributing malware, for example via email or exploit kits.

ACCESS BROKERS

People that sell the unauthorized access they have obtained to other criminals.

INTRUSION SPECIALISTS

Those skilled in penetration testing, also known as red teaming. They are responsible for identifying and stealing valuable data in a network, extending the intrusion to points where ransomware can be deployed to cause maximum damage.

MONETIZERS

Threat actors specializing in handling and cashing out payments.

Section 02

Cybercrime Collaboration – Entering Today's Cybercrime Factory

In tracing the history of cybercrime, it's evident that attacks become more sophisticated and damaging when threat actors pool their knowledge and resources. A key enabler is the maturing marketplace, where forums and chatrooms encourage trustworthy interactions and penalize dishonesty.

We have taken a deep dive into the dark web and hacking forums to help us understand how these venues operate and how cybercriminals use them to buy, sell and discuss attacks. To do this, Forensic Pathways collected dark-web marketplace listings using automated crawlers that monitor content on the Tor network. With over 35 million URLs indexed, they found around 33,000 active websites, including 5,502 forums and 6,529 marketplaces.

KEY POINTS

Access and Control are the Name of the Game.

Commodification Lowers Barriers to Entry.

The Irony of Honor Among Thieves – Why Reputation Counts on the Dark Web.

Cyber Watering Holes for Recruitment and Collaboration.

Here are four key findings that businesses should take notice of:

1. ACCESS AND CONTROL ARE THE NAME OF THE GAME

Every intrusion requires a point of entry into a victim's network, making access and control the Holy Grail of cybercrime. Social engineering is among the most favored ways into a system. In the first quarter of 2022, 69% of malware isolated by HP Wolf Security had been sent via email – in messages disguised as innocent-looking business documents.[17]

Another way in is via stolen usernames and passwords from the dark web itself: our research found the average cost of Remote Desktop Protocol credentials sold on the dark web is $5. One site that collects information lost in corporate data breaches has no less than 11 billion credentials.[2]

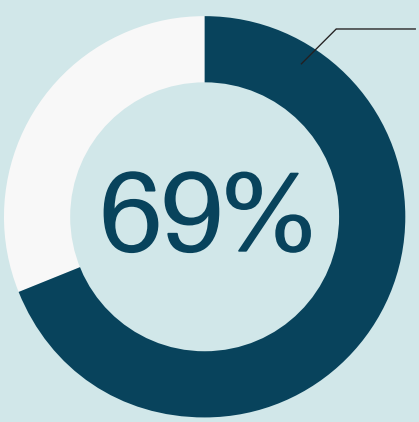
Exploiting security flaws and weaknesses within software is another method. Our research found 130 such vulnerabilities under discussion on the dark web, with the focus on the most severe but easiest-to-execute ones.

Publicly disclosed flaws are assigned a Common Vulnerabilities and Exposures (CVE) identifier, meaning they are being tracked in the industry-wide Common Vulnerabilities and Exposures Database.[18] In what's known as the Common Vulnerability Scoring System, the CVEs are scored out of 10 for severity. We found the average level under discussion on the dark web was 7.4.

The most popular targets were versions of the Windows operating system, Microsoft Office, web content management systems, web and mail servers. Threat actors are focusing on vulnerabilities that allow them to gain initial access to networks and control over systems.

Even the patches issued by vendors to fix security flaws can help the criminals. "Rather than investing resources in finding new vulnerabilities, some cybercriminals will keep a close eye out for new vendor patches to reverse engineer them to understand the vulnerability, and create an exploit, knowing that many organizations will be slow to deploy the patch," says Dr. Ian Pratt, Global Head of Security for Personal Systems at HP.

In Q1 of 2022:



of malware isolated by HP Wolf Security had been sent via email.[17]

One site that collects information lost in corporate data breaches has no less than

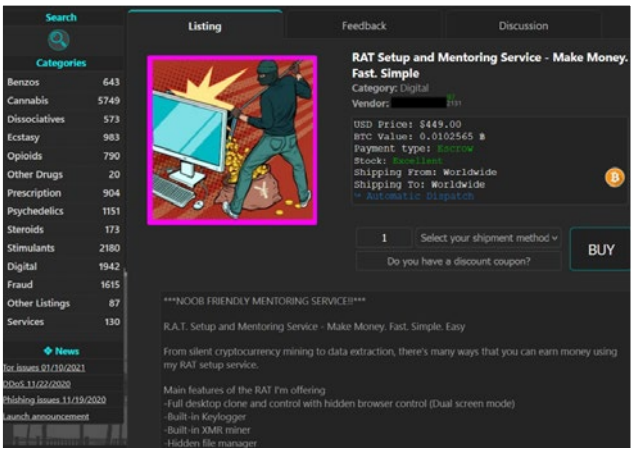
11 billion

credentials.[2]

2. COMMODIFICATION LOWERS BARRIERS TO ENTRY

With exploits and malware now such cheap commodities, new ways to make money are emerging: cybercriminals can now rent the attack software they need and share the ransomware spoils with the malware vendor by paying them a commission. Malware authors are even differentiating their product offerings by giving users access to mentoring services and detailed "playbooks" explaining all they need to know.

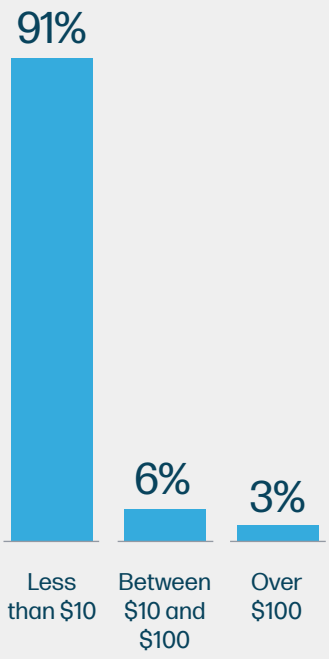
This development shows how many cybercriminals are no longer selling malware tools but have shifted to selling their expertise and skills within a new service-driven economy.



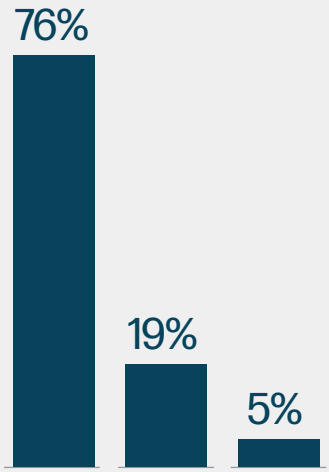
Malware mentoring service for sale

The Low Cost of Cybercrime

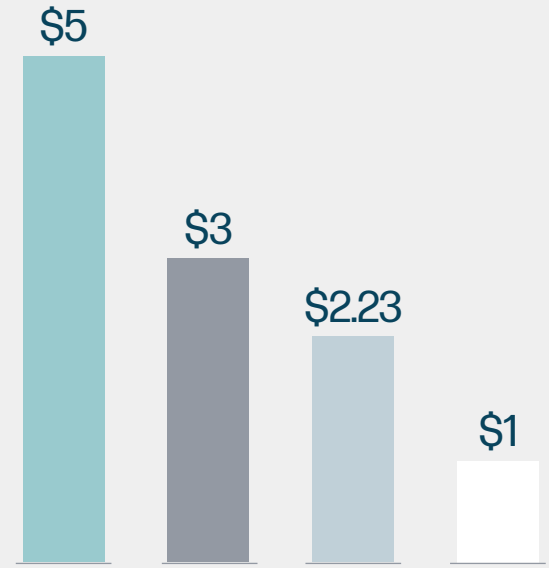
Out of 174 exploits advertised on the dark web:



Out of 1,653 malware ads:



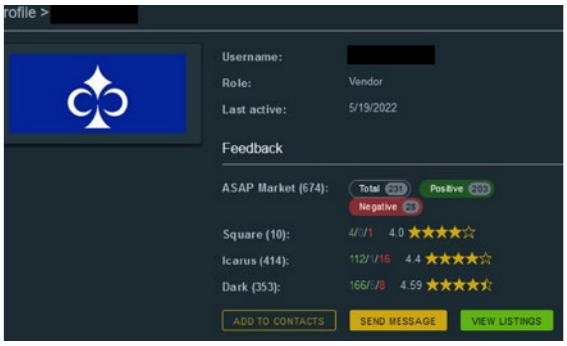
Average price of malware on cybercriminal marketplaces



3. THE IRONY OF HONOR AMONG THIEVES – WHY REPUTATION COUNTS ON THE DARK WEB

Trust is essential for cybercriminal marketplaces, so they have developed sophisticated mechanisms to encourage fair dealing – such as vendor and buyer reputation scores and customer reviews.

And since the average lifespan of a website on the anonymous Tor network is only 55 days, marketplaces have developed ways to track seller feedback so it isn't lost when a market closes or is taken down by law enforcement.



A marketplace listing showing vendor reputation scores from other markets

4. CYBER WATERING HOLES FOR RECRUITMENT AND COLLABORATION

Being able to connect with potential customers, partners and employees easily is a vital part of the cybercrime ecosystem, and forums, specialist chat groups and closed encrypted networks provide hubs where cybercriminals can make connections and recruit partners.

"The dark web is a cybercriminal front of house with cutting-edge customer service, where features such as escrow payments differentiate sellers in a crowded market," says McGuire.

"But behind this is a covert 'invisible net,' where a handful of powerful groups pull the strings from the top, running multinational cyber syndicates that share intel, recruit, and work together to maximize yield or disrupt carefully selected targets."

Dark Web Study Findings on Vendor Reputation Management

100%

of cybercriminal marketplaces have vendor feedback scores.

77% of cybercriminal marketplaces require a "vendor bond" – a license to sell – which can cost up to $3,000.

92% of cybercriminal marketplaces offer third-party dispute resolution services.

85%

use escrow payments – a seller will only receive funds once the buyer has received the agreed product or service.

Section 03

Horizon Scanning – How Might Cybercrime Change in the Next 5 to 10 Years?

Against this backdrop of growing collaboration, specialization and professionalization, the big question now is: how might the threat environment evolve in the future? In a horizon-scanning exercise, we identified four key expectations IT security professionals should be aware of.

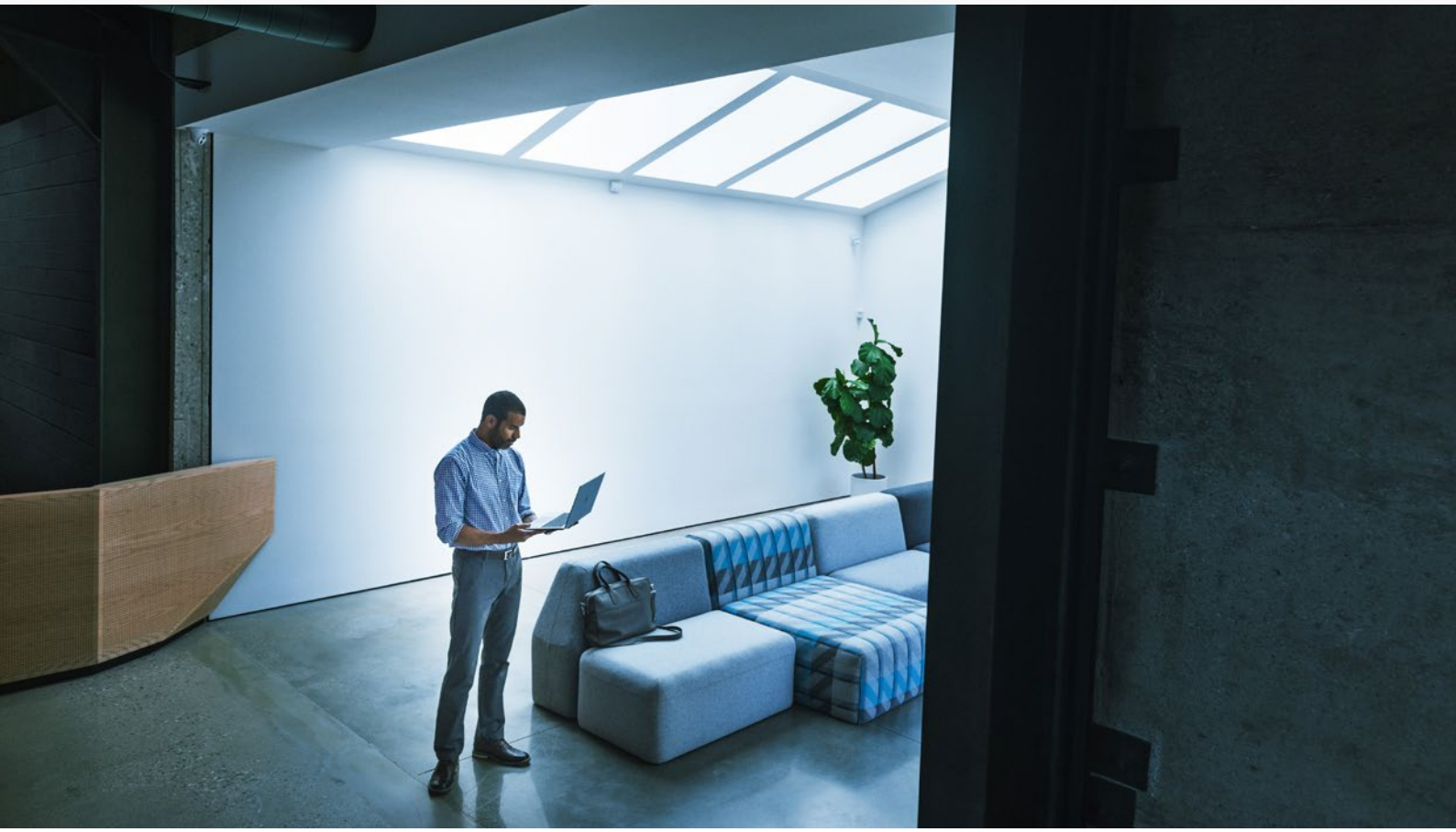
KEY POINTS

Destructive Data Denial Attacks to Become Even More Damaging.

Increasing Professionalization to Drive More Targeted Attacks.

Emerging Technologies to be both Weapon and Shield.

Attackers to Focus on Driving Efficiencies to Increase Return on Investment.



1. DESTRUCTIVE DATA DENIAL ATTACKS TO BECOME EVEN MORE DAMAGING

As organizations increasingly embrace both hybrid working and digital transformation, attackers will likely take advantage of the ever-widening attack surface. We can expect to see extortion attacks using the threat of data destruction against sectors that depend on IoT devices and data in time-sensitive and critical ways.

We are also seeing a resurgence in destructive attacks on critical infrastructure, such as the wiper attacks in late 2021 and 2022, following in the footsteps of Shamoon (2012) and Michelangelo (1991), with malware that wipes data and disables systems without demanding a ransom.[19] [20]

2. INCREASING PROFESSIONALIZATION TO DRIVE MORE TARGETED ATTACKS

Cybercrime techniques have, over the past decade, been converging with those of the nation-state-based Advanced Persistent Threat (APT) hacking groups, such as those operating out of North Korea.[21] These are characterized by human-operated attacks harnessing a deep understanding of victims' networks, and our research suggests this blurring of the lines will continue.

According to McGuire, North Korea is leading the way in using cybercrime to circumvent financial sanctions by investing in cybercrime through its Lazarus hacking group. "North Korea has undoubtedly shown a way forward for impoverished nations to not only boost their economies, but to also potentially get around sanctions. The horse has bolted, this is happening and that has been a definitive change over the past four years," says McGuire.

3. EMERGING TECHNOLOGIES TO BE BOTH WEAPON AND SHIELD

Cybercriminals are also expected to develop attacks that take advantage of new and developing technologies. That could include a shift towards data integrity attacks driven by artificial intelligence (AI), such as where attackers damage organizations by seeding fake news using deepfakes or tampering with AI training data. This emphasizes the need for organizations to maintain robust audit trails that can't be changed.

New platforms such as Web3 could provide new levels of control over personal data for their users. For cybercriminals, this could mean new opportunities to create reputation systems that support cybercrime and allow them to increase collaboration by easily transferring their reputations across multiple marketplaces and forums.

A further risk to be wary of is a possible extension of "cloud cracking" – where hackers use distributed computing in the cloud to speed up brute-force attacks. If this were ever extended to quantum computers, the consequences for cybersecurity could be catastrophic, as those ultrafast computers might be used to break the classical cryptographic algorithms that protect ecommerce, banking and communications today.[22]

4. ATTACKERS TO FOCUS ON DRIVING EFFICIENCIES TO INCREASE RETURN ON INVESTMENT

Many of the vulnerabilities we saw attackers discussing on the dark web were several years old – and the top three exploits isolated by HP Wolf Security, in early 2022, were at least four years old.[17] When the window of opportunity to exploit old vulnerabilities is so large, the return on investment to weaponize new vulnerabilities is poor. Instead, cybercriminals are more likely to focus on increasing the speed and efficiency of their intrusions.

In the future, for example, we are likely to see attackers using AI and machine learning techniques to enable targeted spear-phishing attacks at scale. Attackers could deploy offensive tools that utilize AI capabilities to tailor phishing emails to key individuals at an organization and speed up their post-exploitation activities after gaining an initial foothold into a network.

Section 04

Master the Basics, Plan for Resilience and Collaborate to Reduce Risk and to Increase Your Chances of Winning the Game

So how should organizations, enterprises and governments attempt to reduce the levels of opportunity to commit cybercrime? Our panel of experts found that cyber resilience can be improved in three important ways.

KEY POINTS

Master the Basics to Reduce Cybercriminals' Chances

Focus on Winning the Game

Cybercrime is a Team Sport: Cybersecurity Must be too

1. Master the Basics to Reduce Cybercriminals' Chances

FOLLOW BEST PRACTICE

Every organization should ensure that multifactor authentication is rolled out; closely control what software employees can install, and ensure patches are tested, approved, deployed and verified quickly.

REDUCE YOUR ATTACK SURFACE

Focus on reducing risk from top attack vectors like email, web browsing and file downloads. Invest in security controls, such as isolation technologies, that eliminate risk from entire vectors but don't get in the way of employee workflows.

PRIORITIZE SELF-HEALING HARDWARE TO BOOST RESILIENCE

Given that breaches happen, it makes sense to use resilient self-healing hardware too – so that recovering from an attack is as swift as possible.

"CISOs have a huge list of worries – the more you can take off that list by having security built in the better. And, ultimately, humans are the biggest exploit.

"This is why organizations must view security as a stack, streamlining tech and building resilience in from the hardware up to reduce the attack surface and remove the onus from the individual."

Michael Calce, HP Security Advisory Board Chairman and former hacker"MafiaBoy"

2. Focus on Winning the Game

PLAN FOR THE WORST-CASE SCENARIO

As well as your defenses, focus on business continuity in the event of an attack. By preparing in advance and anticipating what tactics attackers might use, organizations can recover more quickly.

LIMIT RISK POSED BY YOUR PEOPLE AND PARTNERS

Your game is only as strong as your team. Organizations should have processes in place to vet supplier security and educate their workforce about social engineering.

BE PROCESS-ORIENTED AND PRACTICE REACTIONS

Rehearse responses to attacks so you can identify problems, make improvements and be better prepared. "We need to shift away from monitoring statistics and focus more on winning the game. You can have a team with exceptional stats and solid players, but what matters is: can they win when it counts," said Robert Masse, HP Security Advisory Board member and Partner at Deloitte.

"For CISOs, this means: can your team detect, prevent, and recover from an attack before it gets serious? Having regular practice games, monitoring performance, strategizing tactics and potential adversarial maneuvers – these are things that can help you beat the odds."

"If the worst happens and a threat actor breaches your defenses, then you don't want this to be the first time you have initiated an incident response plan.

"Ensuring that everyone knows their roles, and that people are familiar with the processes they need to follow, will go a long way to containing the worst of the impact."

Joanna Burkey, Chief Information Security Officer at HP Inc.

3. Cybercrime is a Team Sport: Cybersecurity Must be Too

TALK TO YOUR PEERS

Attackers are collaborating more than ever – so should defenders. It is increasingly important to share threat information in real time with industry peers. "Security essentials can stop garden variety malware, but the most dangerous stuff only shows up when scouring the underground," says Justine Bone, HP Security Advisory Board member. "On their own, most organizations don't have the time or resources for this. As an industry we need to invest more in understanding this murky world and share that information with our peers, so we can defend against it and disrupt it more effectively."

WORK WITH THIRD-PARTY SECURITY SERVICES

The defensive team should involve third parties such as security assessors and penetration testing companies. These can highlight weak spots and critical risks that need addressing.

USE THREAT INTELLIGENCE AND BE PROACTIVE IN HORIZON SCANNING

Monitoring open discussions on underground forums is an opportunity for network defenders to understand the threats facing their organizations and inform their defenses. "It's vital to be proactive in understanding your threat environment. If you are too inward-looking you won't be able to see what is coming round the corner," says Boris Balacheff, Chief Technologist for Security Research at HP Labs.

"One of the biggest reasons for hope is seeing how the cybersecurity community has grown in its size and willingness to share. Much like adversaries, collaborating and sharing knowledge is essential for fighting back against the tide of attacks.

"By proactively scanning the landscape for threats and sharing insights with our peers, we can together build a more secure and resilient digital world."

Alex Holland, Senior Malware Analyst at HP Inc.

Methodology

HP commissioned an independent study carried out by dark-web investigation firm Forensic Pathways.

The firm collected dark-web marketplace listings using automated crawlers that monitor content on the Tor network. Its Dark Search Engine tool has an index consisting of >35 million URLs of scraped data.

The collected data was examined and validated by Forensic Pathway's analysts. This report analyzed approximately 33,000 active websites across the dark web, including 5,502 forums and 6,529 marketplaces. Between February and March 2022, Forensic Pathways identified 17 recently active cybercrime marketplaces across the Tor network and 16 hacking forums across the Tor network and the web containing relevant listings that comprise the data set.

About HP Wolf Security

HP Wolf Security is a new breed[a] of HP's portfolio of hardware-enforced security and endpoint-focused security services, designed to help organizations safeguard PCs, printers, and people from circling cyber predators.

HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services. Visit hpwolf.com.

[a] HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

About Forensic Pathways

Forensic Pathways Ltd. specializes in threat intelligence, cyber security services, dark web monitoring, and social media investigations.

In 2016 Forensic Pathways began scraping data from the Tor network and hidden services (dark web). Its "Dark Search Engine" can be used to safely search the dark web and monitor for content of interest.

Glossary of Key Cybercrime Terms

ADVANCED PERSISTENT THREAT (APT) – a highly capable threat actor that gains unauthorized access to a target network and remains undetected over a long period of time.

BULLETPROOF HOSTING (BPH) – a web hosting provider that allows almost any kind of content to be hosted, such as malware, and takes steps to ensure the privacy of its customers.

DARK WEB – part of the internet that isn't indexed by search engines.

DDOS (Distributed Denial of Service) – an attack that makes a system or service unavailable by flooding it with requests from many systems.

ESCROW SERVICES – an arrangement where a third party will receive and disburse funds once a transaction – and any conditions agreed upon as a part of this transaction – are met.

EXPLOIT – code, data, or commands that take advantage of a vulnerability in an application or a system to cause unintended or unanticipated behavior to occur.

EXPLOIT BUILDERS – tools that let users create an exploit without the use of coding, lowering the barrier to entry for cybercriminals to gain access to vulnerable systems.

FULLY UNDETECTABLE (FUD) – refers to malware's ability to evade detection.

INTERNET OF THINGS (IoT) – computers embedded in everyday objects that can send and receive data through the internet.

MALWARE – software designed to adversely affect a computer or network, for example, damaging, destroying or stealing data from it.

MALWARE AS A SERVICE – the ecosystem of specialized malware goods and services bought and sold by cybercriminals.

PACKERS – tools that compress executables to reduce their size. They are often used to obfuscate malware.

PHISHING – a social engineering technique where an attacker tries to trick a victim into revealing sensitive information or infecting their computer with malware over email.

PURPLE TEAMING – a methodology where a red team and a blue team (defensive cybersecurity specialists) work closely together to maximize the security of an organization.

RANSOMWARE – malware that denies access to a computer system until a sum of money is paid.

REMOTE ACCESS TROJAN (RAT) – malware that enables an attacker to control a computer remotely.

RED TEAM – a group of offensive cybersecurity specialists that challenge an organization's systems, processes and people to identify security risks.

REMOTE DESKTOP PROTOCOL (RDP) – a protocol that allows a user to connect to another computer remotely, see the display, and input commands to the device over a network connection.

SPEAR PHISHING – a form of phishing targeting specific individuals or groups within an organization.

INFORMATION STEALER – malware that gathers sensitive information from a system, such as usernames and passwords.

TOR – Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication.

TROJAN – malware that is disguised as legitimate software.

ZERO DAY – a software vulnerability that has not been previously discovered, which can be exploited by attackers to achieve a malicious goal, for example gaining unauthorized access to a system.

References

[1] Clarifyi. (2022). *The forensic approach to Threat Intelligence* [Online]. Available: https://clarifyi.com/

[2] Federal Bureau of Investigation. (2022). *Federal Bureau of Investigation Internet Crime Report 2021* [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[3] T. Hunt. (2022). *Have I Been Pwned* [Online]. Available: https://haveibeenpwned.com/

[4] Radware. (2022). *IRC (Internet Relay Chat)* [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/irc-internet-relay-chat/

[5] Trend Micro. (2015, Aug. 31). *A Brief History of Notable Online Banking Trojans* [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

[6] B. Acohido. (2014, Feb. 5). *Lessons from the capture of SpyEye's mastermind* [Online]. Available: https://eu.usatoday.com/story/cybertruth/2014/02/05/lessons-capture-spyeye-mastermind/5182697/

[7] Federal Bureau of Investigation. (2014, Jan. 28). *Botnet Bust: SpyEye Malware Mastermind Pleads Guilty* [Online]. Available: https://www.fbi.gov/news/stories/spyeye-malware-mastermind-pleads-guilty

[8] B. Krebs. (2010, Apr. 1). *SpyEye vs. ZeuS Rivalry* [Online]. Available: https://krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/

[9] B. Krebs. (2010, Oct. 24). *SpyEye v. ZeuS Rivalry Ends in Quiet Merger* [Online]. Available: https://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/

[10] D. Fisher. (2011, May 10). *Zeus Source Code Leaked* [Online]. Available: https://threatpost.com/zeus-source-code-leaked-051011/75217/

[11] A. K. Sood, R. J. Enbody, R. Bansal. (2012, Aug. 1). *Inside the ICE IX bot, descendent of Zeus* [Online]. Available: https://www.virusbulletin.com/virusbulletin/2012/08/inside-ice-ix-bot-descendent-zeus

[12] B. Krebs. (2013, Jul. 25). *Haunted by the Ghosts of ZeuS & DNSChanger* [Online]. Available: https://krebsonsecurity.com/2013/07/haunted-by-the-ghosts-of-zeus-dnschanger/

[13] National Cyber Security Centre. (2017, Apr. 9). Cyber crime – understanding the online business model [Online]. Available: https://www.ncsc.gov.uk/pdfs/news/ncsc-publishes-new-report-criminal-online-activity.pdf

[14] United States Department of Justice. (2014, Jun. 2). *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator* [Online]. Available: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[15] BBC News. (2017, May 13). *Massive ransomware infection hits computers in 99 countries* [Online]. Available: https://www.bbc.co.uk/news/technology-39901382

[16] MITRE Corporation. (2022, Apr. 25). *NotPetya* [Online]. Available: https://attack.mitre.org/versions/v11/software/S0368/

[17] HP Wolf Security. (2022, May 12). *HP Wolf Security Threat Insights Report Q1 2022* [Online]. Available: https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf

[18] MITRE Corporation. (2022). *CVE* [Online]. Available: https://cve.mitre.org/

[19] MITRE Corporation. (2021, Feb. 9). *Shamoon* [Online]. Available: https://attack.mitre.org/versions/v11/software/S0140/

[20] Trend Micro. (2017, Mar. 6). *The Michelangelo Virus, 25 Years Later* [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-michelangelo-virus-25-years-later

[21] L. Constantin. (2019, Apr. 10). *Cybercrime groups raise the bar for security by borrowing APT techniques* [Online]. Available: https://www.csoonline.com/article/3387943/cybercrime-groups-raise-the-bar-for-security-teams-by-borrowing-apt-techniques.html

[22] J. Chu. (2016, Mar. 3). *The beginning of the end for encryption schemes?* [Online]. Available: https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303