LOGPOINT

Zero to '22:
A look back and a look ahead

2022 Year in review - an emerging threats report

www.logpoint.com

FOREWORD

The only certainty regarding information security is that nothing is certain. Even with the evidence we have, we will never know for sure what's coming next. Instead of throwing up our hands and whining that it's difficult to make assessments in a data-poor environment (or worse, simply making stuff up), we got to work. The result is our annual review of the security analytics and security research landscape.

For front-line security personnel and those of us in the business of preventing cyberattacks and breaches, 2022 offered no rest. Faced with the tremendous disruption caused by COVID-driven social, economic, and technical developments in 2020, opponents honed their tradecraft to become even more adept and aggressive. As a result, a succession of high-profile attacks devastated numerous companies and were breakthrough moments in cybersecurity on their own.

The last year has been unusual in many ways, but it has also been especially notable in the dark realm of cybercrime. From highly publicized **critical infrastructure attacks** to large supply chain breaches, financially motivated criminals and malevolent state actors have rarely, if ever, come out swinging as they have in the previous year. We attempted to investigate what our data had to say about these and other frequent action types employed against organizations.

Understanding the year's past attacks provides insight into the altering dynamics of adversary tactics, which is crucial for keeping up with today's challenges. This year's report provides critical insights into what security teams need to know about an increasingly ominous threat landscape, based on first-hand observations, customer-given telemetry, as well as insights drawn from the peer reports.

Nilaa Maharjan

Logpoint Global Services and Security Research

Nilaa Maharjan is a First-Class graduate with Bachelors in Networking and Cybersecurity with a passion for offensive and defensive security in a research capacity. He has been working as cyber security analyst and researcher for 3+ years and with the Logpoint Security Research Team, is leading the Emerging Threat Protection research to bring out the investigation, analytics, detection, and response techniques.

TABLE OF CONTENT

ABOUT LOGPOINT EMERGING THREATS PROTECTION

The cybersecurity threat landscape continuously changes while new risks and threats are discovered all the time. Not every organization has enough resources or the know-how to deal with evolving threats.

Emerging Threats Protection is a managed service provided by a Logpoint team of highly skilled security researchers that are experts in the field of threat intelligence and incident response. Our team keeps you informed on the latest threats and provides custom detection rules and tailor-made playbooks designed to help you investigate and mitigate emerging incidents.

EXECUTIVE SUMMARY AND KEY FINDINGS

Increasing tensions in Eastern Europe and the Middle East, a steady stream of critical vulnerabilities forcing organizations to scramble to patch their systems, and public leaks exposing the inner workings of organized cybercriminal ransomware gangs have all had a significant impact on cybersecurity events over the past year.

Our Security Analytics and Research team maintain a knowledge base of cyber threats, and we use our expertise to inform and protect organizations around the world. Our analysts identified the following high-level patterns throughout the threat environment between November 2021 and November 2022, based on insights from customer telemetry, incident response, underground monitoring, proactive threat research, and intelligence relationships:

1. Changes in advanced persistent threats (APTs) from nation-state actors and other highly skilled attackers amidst the **Russia-Ukraine war** and major players like **Ryuk** and Conti going underground.
2. The immense rise in ransomware attacks involved critical infrastructure emanating primarily from Russian and North-Korean groups.
3. Development in phishing attacks, as threat actors are integrating social threats and AI into their existing arsenals.
4. The comeback of Infostealers and Loaders with the return of **Emotet** and **IcedID** and new players like **Bumblebee**.
5. The most common exploits are from years old, essentially confirming that most organizations still do not patch **CVEs** (also known as Common Vulnerabilities and Exposures) for more than two years.
6. Data breaches alongside ransomware attacks as part of double and triple extortion methods saw a huge rise as over 42 million records have been exposed in the last 12 months (Source: **Statista**) which is lower than in previous years but caused more financial and reputational damage with hacks such as Crypto(.)com, Microsoft, NVIDIA and Red Cross Data Breach.
7. IoT (Internet of Things) attacks increased as more devices are connected to the internet, including cars and home security devices.
8. **Insider threats** increased rampantly following the mass layoffs that took post-pandemic and the tech layoffs that started mid-2022. The increase in remote work has led to a lack of physical security controls, making it easier for malicious insiders to access sensitive information. The rise of digital transformation has created more opportunities for insiders to access and exploit valuable data for personal gain.

LETTER FROM OUR REPRESENTATIVE

Cybercrime has become one of the biggest challenges of recent times. According to the statistics, the cost of cybercrime in 2022 was $8.4 trillion, which is expected to reach $10.5 trillion by 2025. This indicates that security is getting harder and we are falling behind. To add to the problem, the attackers have begun to work together and collaborate on developing more deceptive and targeted cyber exploits. Besides, this year's Ukraine-Russia conflict has further transformed the cyberattack into global political, economic, and technical warfare.

Cyber threats are constantly evolving and can be difficult to predict. So, it is vital for security professionals to accurately assess and understand cyber risks and implement effective security controls to prevent or quickly respond to common attacks. However, the truth is, we cannot prevent every attack. What we can do is, build the necessary capabilities to enable proper detection and timely response. This is where Logpoint can offer a helping hand. With SIEM, SOAR, UEBA, and EDR functionalities, we can help organizations of all sizes improve their cybersecurity posture and better prepare themselves against cyber threats.

When I look back on 2022, I'm amazed at what Logpoint's security research team has accomplished in terms of building detection and response capabilities. The dedicated team of researchers continuously tracks and analyzes recent cyber scenarios and produces the technical details and analytics packages easily consumable by our customers. These contents are carefully crafted based on the TTPs involved in such attacks and are also mapped to the Mitre ATT&CK matrix. This MITRE mapping enhances the SIEM capabilities by allowing analysts to understand the specifics and progression of an attack. Additionally, each blogpost includes SOAR playbook details required to timely respond to such attacks. All of these contents in the form of alerts, dashboards, and playbooks are available to our customers. The report further outlines the security best practices to tackle such attacks. Overall, the report comes as a complete package to help our customers significantly reduce the time to detect and respond to cyber-attacks.

Finally, this is the year-end report where we summarize the excellent work the team has done during 2022, with a view into 2023. We cover three aspects here. First, we take a look back at the most prominent threats we faced in 2022. Second, how Logpoint helped customers and security researchers build the capabilities to detect and respond to such attacks. And, third, what the future of cyberattacks would look like in 2023.

Cheers!

Roshan Pokhrel

Logpoint, CISO

SECURITY LANDSCAPE: A MAZE OF RISKS

“If we wish to see where our future is headed, all we need to do is have a look at our past and that will tell us all the answers.” — Anthony T. Hincks

As organizations continue to strengthen their defenses and cybersecurity programs, threat actors are finding it increasingly necessary to use **zero-day exploits** to achieve their operational and strategic goals. Strengthened defenses have led to a rise in the development and purchase of zero-day exploits, as defense-in-depth strategies make it more difficult for adversaries to find exploitable vulnerabilities.

A common theme we saw this year was a massive rise in Advance Persistent Threats (APTs). To avoid law enforcement and sanctions, ransomware groups are engaging in continuous "retirements" and rebranding. The Hacker-as-a-Service (HaaS) business model, where an ill-intended individual can hire APTs or as a group at any step of the Kill-Chain, has also gained traction and grown since 2021. Furthermore, threat groups are showing a greater interest in and capability for conducting supply chain attacks and attacks against **Managed Security Services Providers (MSSPs).**

Geopolitical Tug-of-War: Pulling Cybersecurity in Every Direction

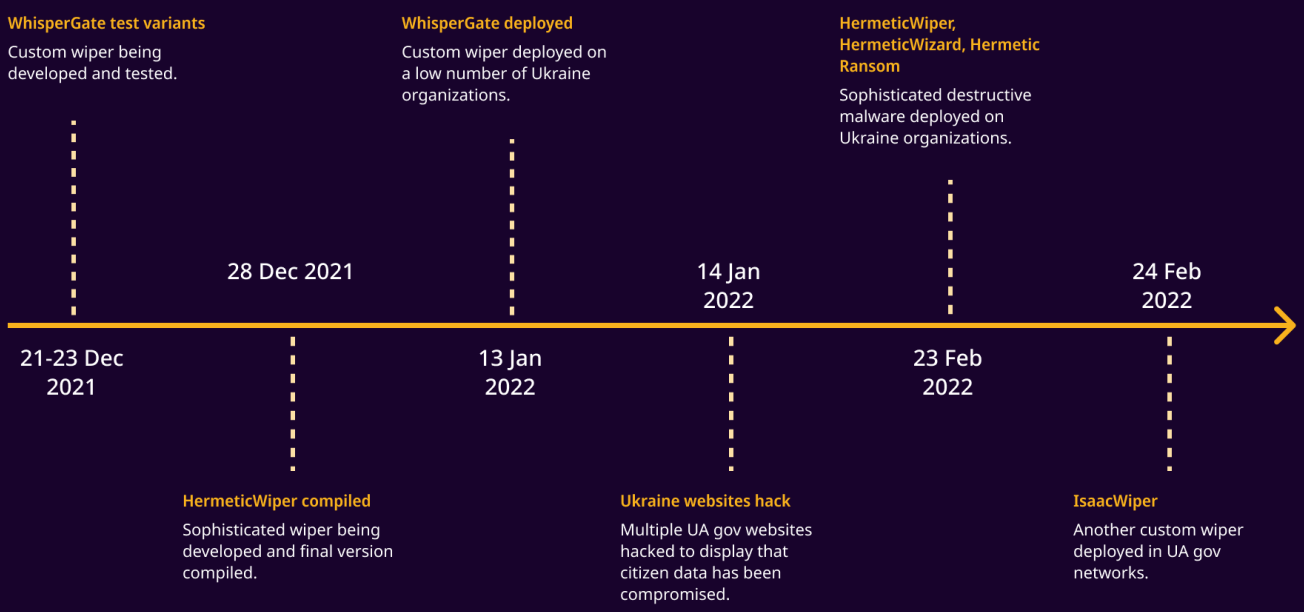
During the reporting period, the conflict between Russia and Ukraine changed the threat landscape as we have never seen before. Significant increases in hacktivist activity, cyber actors executing operations in tandem with kinetic military action, hacktivist mobilization, cybercrime, and aid from nation-state groups were only scenes we were used to in movies.

Needless to say, geopolitics is having an increasing impact on cyber activities. Destructive attacks were and are still a common operational feature of state actors. During the Russia-Ukraine conflict, cyber operators were seen carrying out activities alongside kinetic military activity.

A new wave of hacktivism has emerged, particularly since the beginning of the Russia-Ukraine crisis with soldiers on both sides. The consequences of war were ugly and damage was not lopsided. Supporters beyond the war territories were massively impacted as disinformation was used as a prominent cyber warfare tool. It was used even before the 'physical' war began as a warm-up for Russia's invasion of Ukraine.

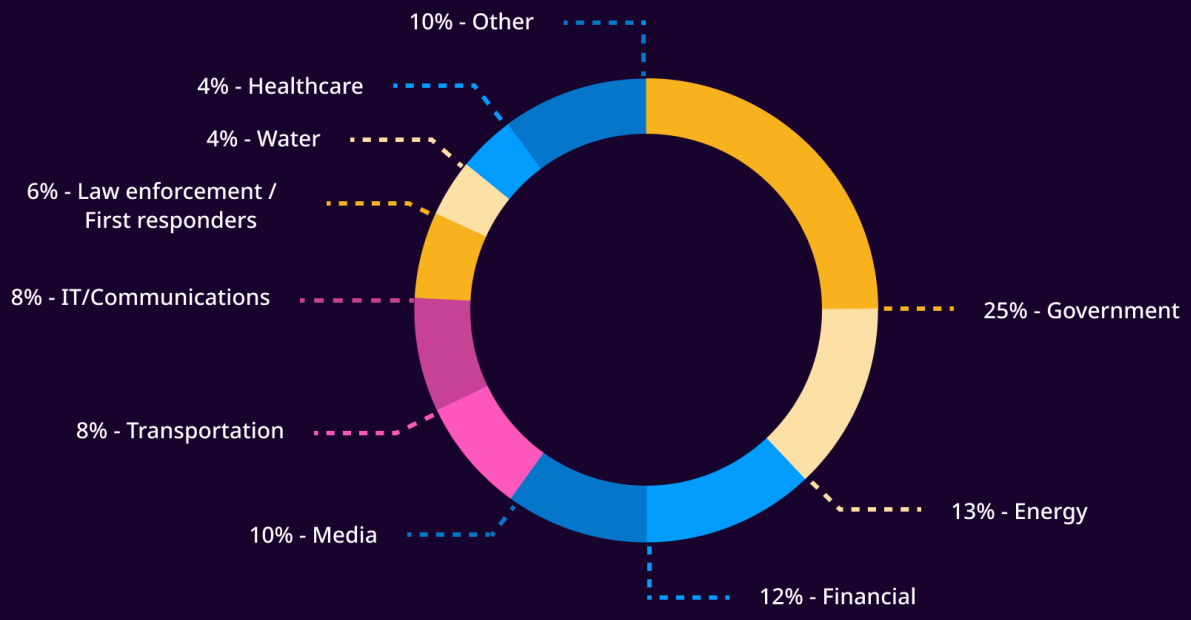
We did cover the war on the cyber front. However, a lot has happened since then.

Timeline of recent cyberattacks in Ukraine



Destruction targets in Ukraine by sector

February-October



Source: Data compiled by EPRS

Of course, there are no easy answers as to whether Russian Cyber Warfare operations were simply inept, or whether Ukrainian cyber defenses were robust; perhaps it was a combination of the two.

More information is needed to determine how effective Ukrainian cyber defenses are today against Russian cyberattacks. There are numerous cybersecurity metrics for assessing the resilience and security of computer networks without revealing critical information during a conflict. Nevertheless, assessing the success and flaws of cyber operations is never straightforward. What's obvious is that Russia's "cyber army," has yet to undertake any decisively successful operations in its conflict with Ukraine.

Phishing: Still Hooking the Most Victims in 2022

Phishing attacks, as expected, continued to increase, with more sophisticated techniques being used to target businesses, government organizations, and individuals. Notably, using threats to entice victims as we saw with IcedID, among other social engineering tactics such as impersonation, leveraging personal data from social media to craft convincing lures, and using increasingly sophisticated methods to evade security countermeasures. One major factor driving the increase in phishing attacks is the widespread adoption of remote work and online collaboration tools. As more employees work from home, hackers are finding new opportunities to target individuals and organizations.

Another factor is the growing sophistication of phishing techniques. Hackers are becoming increasingly adept at creating convincing fake emails and websites, making it difficult for even savvy users to spot a phishing attempt.

Phishing by numbers

- 55% of phishing websites use targeted brand names to deceive individuals into giving away sensitive information. (Source: F5)
- In June 2022, the Marriott hotel chain was hacked, resulting in the theft of 20 GB of guest information. (Source: BleepingComputer)
- 84% of U.S.-based organizations have reported that regular security awareness training has helped reduce the number of employees who fall victim to phishing attacks. (ProofPoint)
- 92% of Australian organizations have experienced a successful phishing attack, representing a 53% increase from the previous year. (Source: Comparitech)
- One of the most costly phishing attacks involved compromised emails, with 19,369 complaints and a total loss of $1.8 billion. (Source: HoxHunt)
- According to Verizon's 2022 report, 36% of all data breaches involved phishing.
- Amazon and Google are the most commonly impersonated brands for phishing attacks (13%), followed by Facebook and Whatsapp (9%), and Netflix and Apple (2%). (Source: Cisomag)
- It is estimated that nearly 1.2% of all emails sent are malicious, which translates to approximately 3.4 billion phishing emails per day. (Source: ZDNet)

THE YEAR OF RANSOMWARE

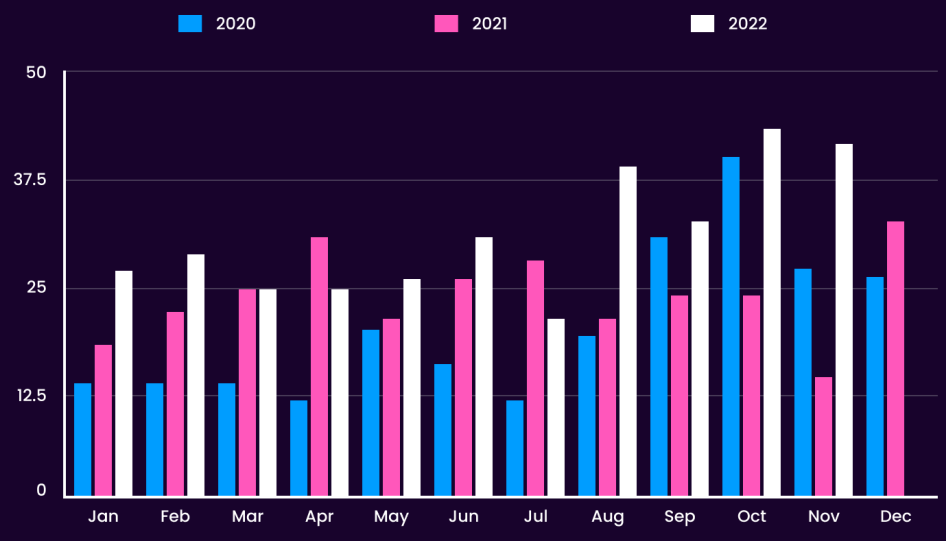
Ransomware attacks have continued to trend upward in 2022, with a significant increase in the number and their sophistication. Ransomware attacks have targeted a wide range of industries, including **healthcare, education**, and **government agencies**, resulting in significant disruptions and financial losses.

One of the major drivers of this trend has been the use of Ransomware-as-a-Service (RaaS) platforms, which have made it easier for even relatively unskilled attackers to launch ransomware attacks. Additionally, the rise of cryptocurrencies has provided attackers with a convenient way to receive payment for their ransom demands, making ransomware attacks even more lucrative.

We identified a potential new trend in cyber attacks, where smaller organizations are targeted in more significant numbers rather than just focusing on large corporations. Cybercriminals likely employ this strategy to avoid attracting the attention of law enforcement.

In terms of network defense, the window of opportunity for managing a successful defense against ransomware has been reduced. The ransomware window encompasses the time from the initial compromise to the deployment of ransomware and the encryption of data. In 2022, the median length of this window is 4.5 days, compared to 5 days in 2021. The mean dwell time for ransomware in 2021 was 22 days, whereas in 2022 it decreased to 11 days. Ransomware operators are more efficient in their tactics and are spending less time idling on compromised systems.

Ransomware Trend by Month



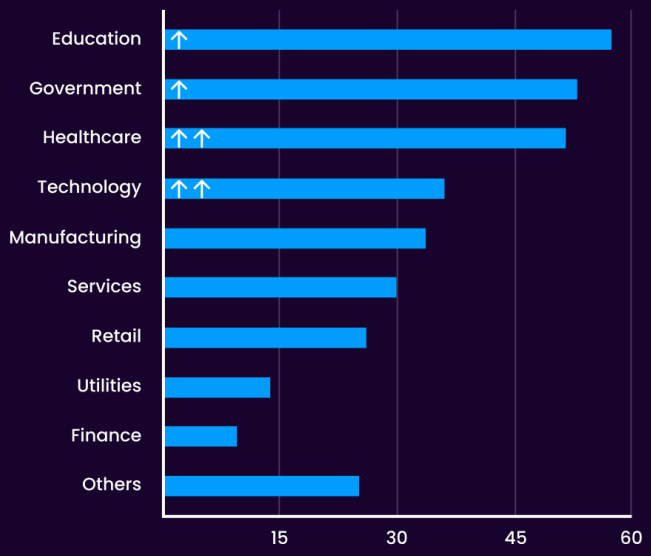
Key Trends

86% of all attacks use PowerShell

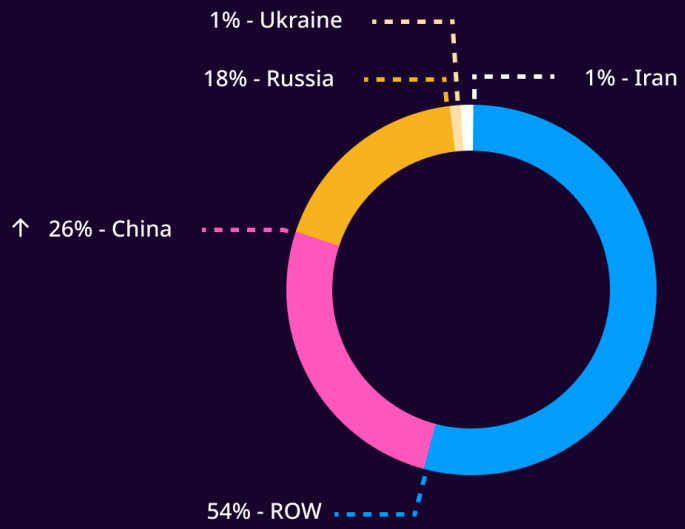
89% of all attacks exfiltrate data

Average payout US $258, 143k
+13.2% from Q2/22

Ransomware by Industry

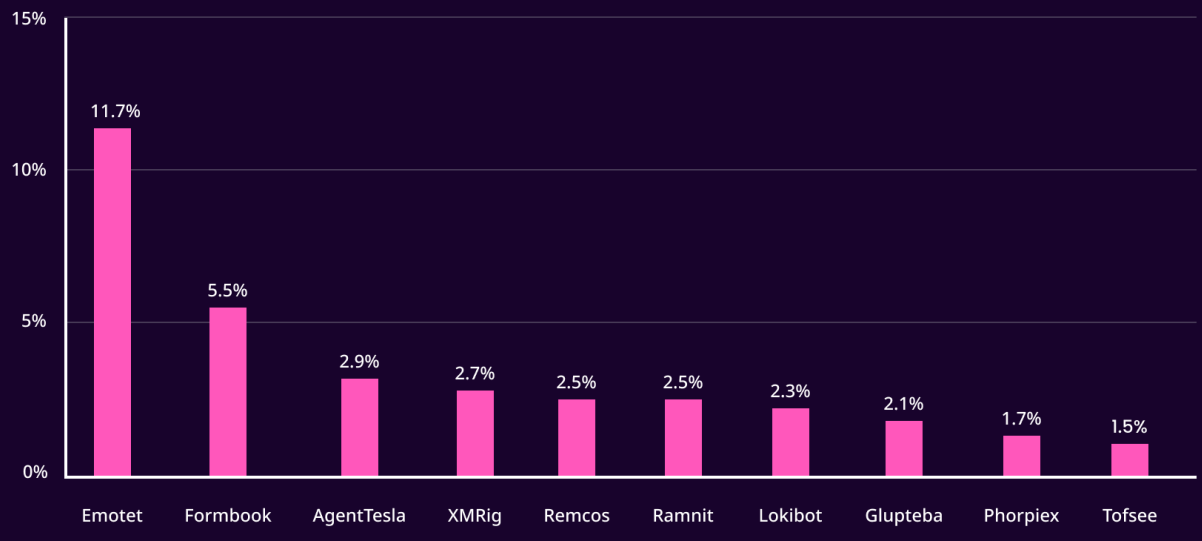


Ransomware Exfiltration Country



Top Malware Families

Most prevalent malware globally. Percentage of corporate networks attacked by each malware family.



Source: **Checkpoint**

Load the Loaders

The use of loaders in the ransomware ecosystem has changed, with the emergence of **new loaders and the disappearance of some old ones.** Loaders are a type of malware that load second-stage payloads, such as ransomware. There are signs that the groups operating these loaders are collaborating closely and may be moving away from using complex botnets to give them capabilities.

Infostealers are a significant enabler of ransomware operations because they allow attackers to quickly and easily obtain credentials that can be used to initially access victims' systems. On a single day in June 2022, over two million stolen credentials obtained by infostealers were observed being offered for sale on just one underground marketplace. Infostealers have been distributed using innovative methods, such as cloned websites and trojanized installers for secure messaging apps like Signal.

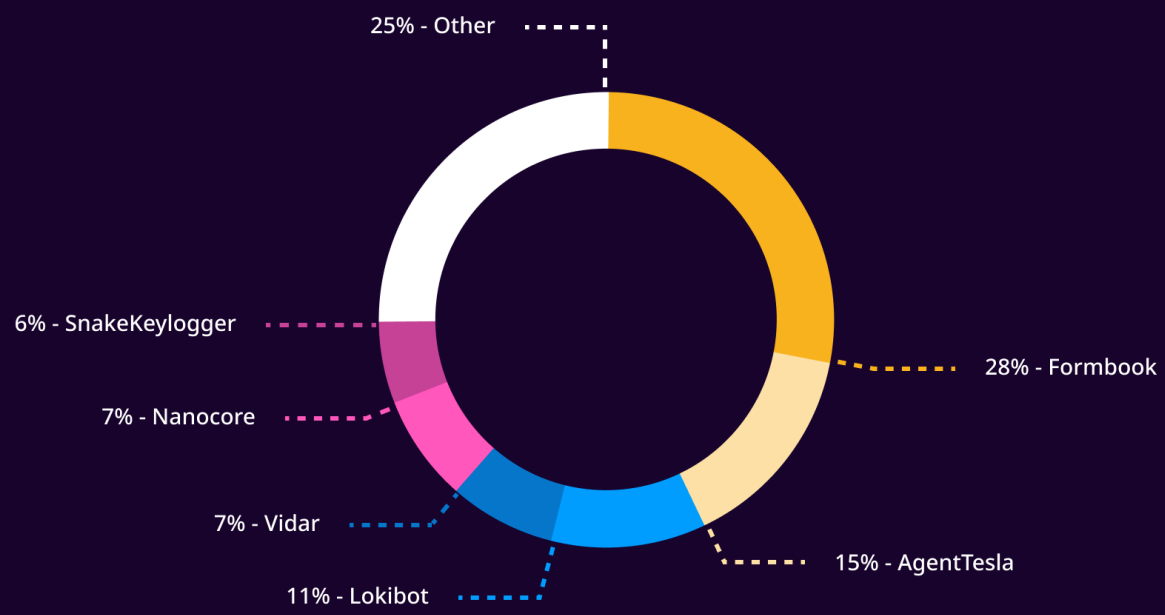
LNK to ISO

Operators were observed increasingly using ISO, ZIP, and LNK file types to deliver **Qakbot**, **Emotet**, and **IcedID** in an attempt to bypass Microsoft's measures to block macro-enabled documents. Additionally, Qakbot, Emotet, and IcedID operators were observed leveraging living-off-the-land binaries (LoLBins) present on victim environments to download and launch malicious payloads. In some instances, Qakbot and Emotet affiliates used various LoLBins in their attack sequence in an effort to enhance the probability of remaining undetected within an organization.

Infostealer Malware: Global Analysis

Formbook remains the most popular info-stealing malware, which has been sold as a service on underground forums since 2016. It is designed to collect information through keylogging. In March, a campaign involving Formbook was found to be targeting Ukrainians with spam, using fake government funding approval letters to lure victims. This was followed by a peak in Formbook's activity in April. The Snake Keylogger is a new entry on the chart. It is a modular .NET keylogger and info stealer that first appeared in late 2020 and quickly gained popularity among cybercriminals. It has a range of capabilities, including recording keystrokes, taking screenshots, harvesting credentials and clipboard content, and supporting the exfiltration of stolen data using HTTP and SMTP protocols. Snake is usually spread through emails containing DOCX or XLSX attachments with malicious macros, but in May, researchers reported that it had started spreading through PDF files as well. This could be because Microsoft has started blocking internet macros in Office by default, forcing cybercriminals to explore other file types such as PDFs. Finally, the popular Raccoon stealer has dropped out of the ranks. A report in March suggested that a key member of the Malware-as-a-Service operation may have been impacted by the conflict in Eastern Europe and temporarily suspended all activities. However, Raccoon reappeared in June with the newly developed Raccoon Stealer V2, which included improvements and new features.

Top infostealer malware globally



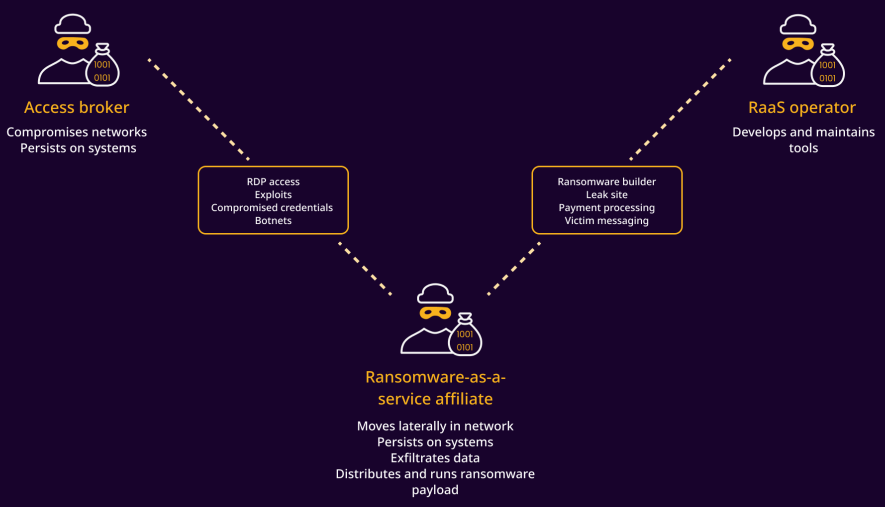
RaaS Model: Understanding the new standard

The cybercriminal economy is evolving to act as a connected ecosystem of numerous participants with varying strategies, goals, and skill sets. Attacks have moved from attackers using off-the-shelf tools like Cobalt Strike to attackers being able to buy access to networks and the payloads they dump on them. Regardless of the attacker's skill level, the impact of a successful ransomware and extortion attack stays the same.

RaaS is a contract between an operator and an “affiliate“. The RaaS operator creates and maintains the tools that power ransomware activities, such as ransomware payload builders and payment sites for connecting with victims. The RaaS program may additionally include a leak site for sharing bits of data exfiltrated from victims, allowing attackers to demonstrate the authenticity of the exfiltration and attempt to extort payment.

Many RaaS programs also include extortion support services, such as hosting leak sites and integrating them into ransom notes, as well as decryption negotiation, payment pressure, and bitcoin transaction services.

RaaS provides the payload or campaign impression of being a single ransomware family or set of attackers. However, the RaaS operator sells access to the ransom payload and decryptor to an associate, who performs the intrusion and privilege escalation and is in charge of the actual ransomware payload deployment. The profit was subsequently divided among the parties. Furthermore, RaaS developers and hosts may profit from the payload by selling it and running campaigns with additional ransomware payloads, thus complicating matters when it comes to tracing the criminals behind these operations.



Major Breaches

6/1	Flexbooker data breach (3.7 million accounts leak)
17/1	$35 million worth of crypto currency was stolen from **crypto.com**
24/1	Canadian foreign ministry breach
27/1	French justice ministry victim of Lockbit
7/2	Cyber attack on Vodafone Portugal
15/2	Ukrainian Defense Ministry and two of the country's largest banks offline
26/2	1TB of data from Nvidia 1TB of data from Nvidia leak
28/2	Total of 6.5 TB of data of Turkish based airline's data leaked
31/3	65 terabytes of data wiped from Russian federal Air Transport Agency
8/4	Attack on India power grid by Chinese threat actor
11/4	Deutsche Windtechnik, a leading wind turbine provider hit by blackbasta ransomware
13/4	Enemybot: a new Mirai, Gafgyt hybrid botnet joins the scene
21/4	American Dental Association hit by Black Basta ransomware
28/4	Largest library services in Germany hit by lockout
7/5	Database containing the personal details and login credentials of 21 million users of VPNs like SuperVPN, GeckoVPN, and ChatVPN was leaked in a Telegram group
31/5	Costa Rica's public health agency hit by Hive ransomware
1/6	Arguably the largest distributed denial of service (DDoS) attack on record, which had a peak of 46 million requests per second (rps)
1/6	The Argentinian multimedia giant hit by hive ransomware
15/6	Plainedge Public Schools hit by Blackcat
18/6	Cybersecurity vendor Entrust hit by Lockout
19/7	Huge Database of 69 milliom records stolen from Neopets
20/7	5.4 million Twitter account Information leaked
10/8	Cisco hit by Yanluowang ransomware
3/9	Vodafone Italia's 310 GB data for sale
15/9	Suffolk County Government 4TB data leaked by blackcat ransomware group
15/9	Uber officially confirmed an attack resulting in an organization-wide cybersecurity breach
18/9	GTA 6 source code and videos leaked after Rockstar Games hack
20/9	**Crypto Trading Firm Wintermute Loses $160 Million in Hacking Incident**
23/9	6 million user records from Swachhata Platform leaked
24/9	Microsoft misconfigured public bucket leads to the leak of sensitive data of 65,000+ entities in 111 countries
3/10	Ferrari hit by RansomEXX
7/10	Barcelona Health Centers hit by RansomExx and leaks 52 GB data
13/10	Medibank confirms hacker had access to data of all 3.9 million customers
14/10	Dropbox suffers data breach following phishing attack
19/10	Kingfisher hit by lockout and 1.4TB of data exfiltrated
2/11	$28 million stolen from cryptocurrency platform Deribit
12/11	AirAsia hit by Daixin ransomware group(5 million unique passengers and all employees data exfiltrated)
2/12	Rackspace a cloud service provider hit by ransomware

OLD BUGS - OLD TRICKS: A REFRESHER

To a lesser extent, cyber attackers continued to exploit publicly known, outdated software vulnerabilities - some of which were also routinely exploited in 2021 or earlier. On average, it takes an organization 60 days to patch a critical vulnerability, and less dangerous vulnerabilities take even longer to patch if they are addressed at all. For many of the most exploited vulnerabilities, researchers or other actors released proof of concept (POC) code within two weeks of the vulnerability's disclosure, likely facilitating exploitation by a broader range of malicious actors. The exploitation of older vulnerabilities highlights the continued risk to organizations that fail to patch software promptly or are using software that is no longer supported by a vendor.

In addition to these long-standing vulnerabilities, several new ones have been discovered in 2022. In fact, the number discovered so far in 2022 is on track to surpass the record set in 2021, with over 17,700 discovered to date, compared to just over 20,000 in all of 2021. However, only a small percentage of vulnerabilities are actually targeted and exploited by cyber threat actors. So far, CISA has identified 70 released in 2022 that are being actively exploited by cyber threat actors. Some of the vulnerabilities discovered in 2022 are minor or have been mitigated by automatic patches, reducing their impact. However, others pose a significant threat. We ran background monitoring to notify us of any CVEs being used starting in 2022 till mid-December of the same year. The top CVEs being actively exploited and released in 2022 in order of their occurrence in the wild are listed below.

CVE-2022-1096: Google Chrome Type Confusion

Seen: 12539

Certain versions of **Chrome** from **Google** contain the following vulnerability:

Type confusion in V8 in Google Chrome before 99.0.4844.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-30190: MSDT Remote Code Execution: Follina

Seen: 9848

Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.

CVE-2022-30190, also known as Follina, is a Microsoft vulnerability that has seen active exploitation in 2022. Follina is a remote code execution (RCE) vulnerability affecting the Microsoft Support Diagnostic Tool (MSDT). On the CVSS scale, this vulnerability is rated as 7.8. Threat actors can exploit the Follina vulnerability by using a malicious Microsoft Word document that uses Microsoft's URL handlers to launch the MSDT executable. This executable has the ability to run PowerShell commands, allowing the attacker to execute code on the target system.Certain versions of Chrome from Google contain the following vulnerability:

Type confusion in V8 in Google Chrome before 99.0.4844.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-1388: F5 BigIP iControl REST Authentication Bypass

Seen: 8946

Certain versions of **Big-ip Access Policy Manager** from **F5** contain the following vulnerability:

On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions that have reached End of Technical Support (EoTS) are not evaluated

CVE-2022-26134: Atlassian Confluence (CVE-2022-26134 and CVE-2022-26138)

Seen: 7413

CVE-2022-26134 and CVE-2022-26138 are vulnerabilities in Atlassian Confluence. Both vulnerabilities are ranked as 9.8 on the CVSS.

CVE-2022-26134 is an OGNL injection vulnerability that allowed unauthenticated users to achieve RCE. This vulnerability was frequently exploited to install web shells, crypto miners, and other types of malware on vulnerable systems.

CVE-2022-26138 involves the use of hardcoded credentials for the disabledsystemuser account within the confluence-users group. The details of this vulnerability were leaked on Twitter, allowing many attackers to access the account on vulnerable systems and see any data visible to users of the confluence-users group.

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.

CVE-2022-40684: FortiOS Authentication Bypass

Seen: 6452

Certain versions of **FortiOS** from **Fortinet** contain the following vulnerability:

An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

CVE-2022-0847: Fedora Privilege Escalation

Seen: 6220

Certain versions of **Fedora** from Fedora project contain the following vulnerability:

A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read-only files and as such escalate their privileges on the system.

CVE-2022-22965/63: SpringShell

Seen: 5694

Spring4Shell is an RCE vulnerability in the Spring Framework, which is commonly used in Java applications. This vulnerability is also known as CVE-2022-22965 and has a CVSS score of 9.8. It can be exploited if a Spring-based Java application is run on Tomcat and packaged as a WAR using data binding. This vulnerability is actually a workaround to a patch for CVE-2010-1622.

CVE-2022-22963 is another vulnerability related to Spring that has a CVSS score of 9.8. This vulnerability impacts the Spring Cloud Function (SCF) library. An attacker can achieve RCE by using specially crafted SpELs as a routing expression.

An alarming number of attacks were being reused from years before and remain a dark patch in every organization's cyber defense. This year a common trend was to use proven old vulnerabilities with a poor track of patching.

Attackers will often search for and target these vulnerabilities because they know that many organizations may not have patched them yet. This is particularly concerning because these vulnerabilities have already been identified and solutions or patches have been developed to address them.

However, if an organization has not applied the patch, they are still at risk of being exploited.

Surprisingly, even the biggest newsmakers have been attacked quite frequently. This highlights the importance of regularly patching and updating systems to protect against known vulnerabilities.

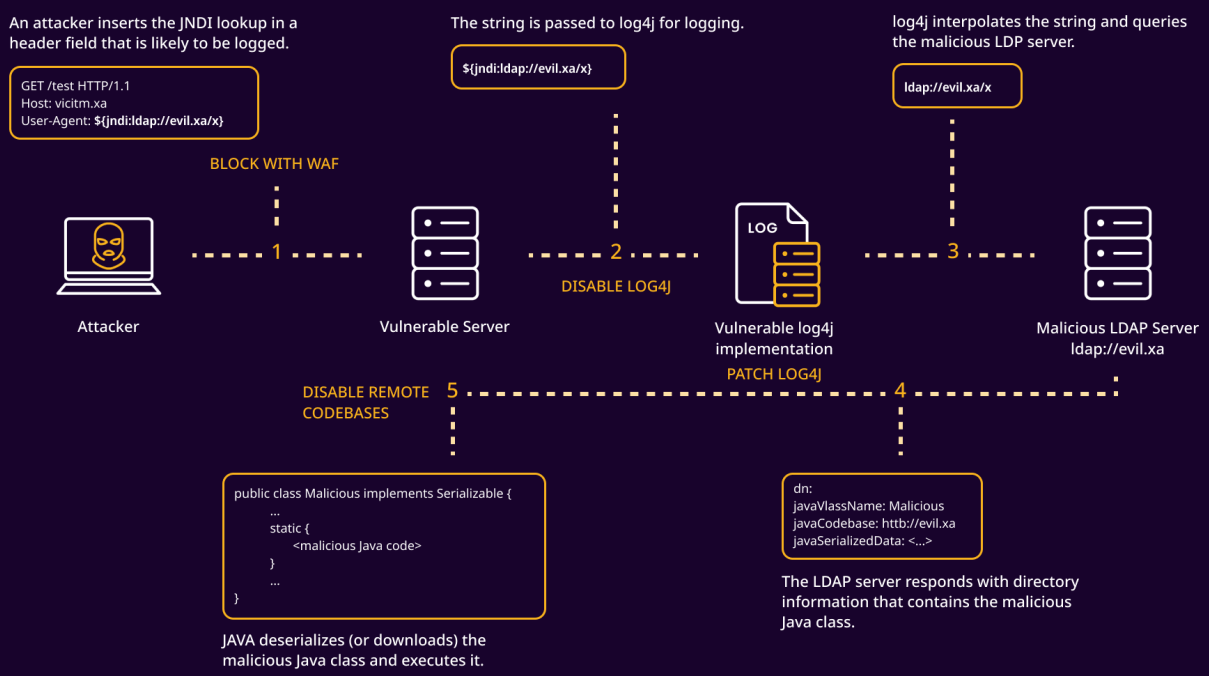
It is also important for organizations to have robust security measures in place and to regularly monitor their systems for any signs of compromise. By staying vigilant and proactive in their cybersecurity efforts, organizations can better defend against these types of attacks.

Log4Shell (CVE-2021-44228)

Log4Shell is another vulnerability that has garnered attention in 2022. This flaw affects the widely-used Apache Java logging library, Log4j, and was released in December 2021. This logging library is used by many web applications around the world, making it a target for threat actors.

Successful exploitation of Log4Shell can result in a remote code execution condition, allowing threat actors to download and execute malicious payloads on the server side.

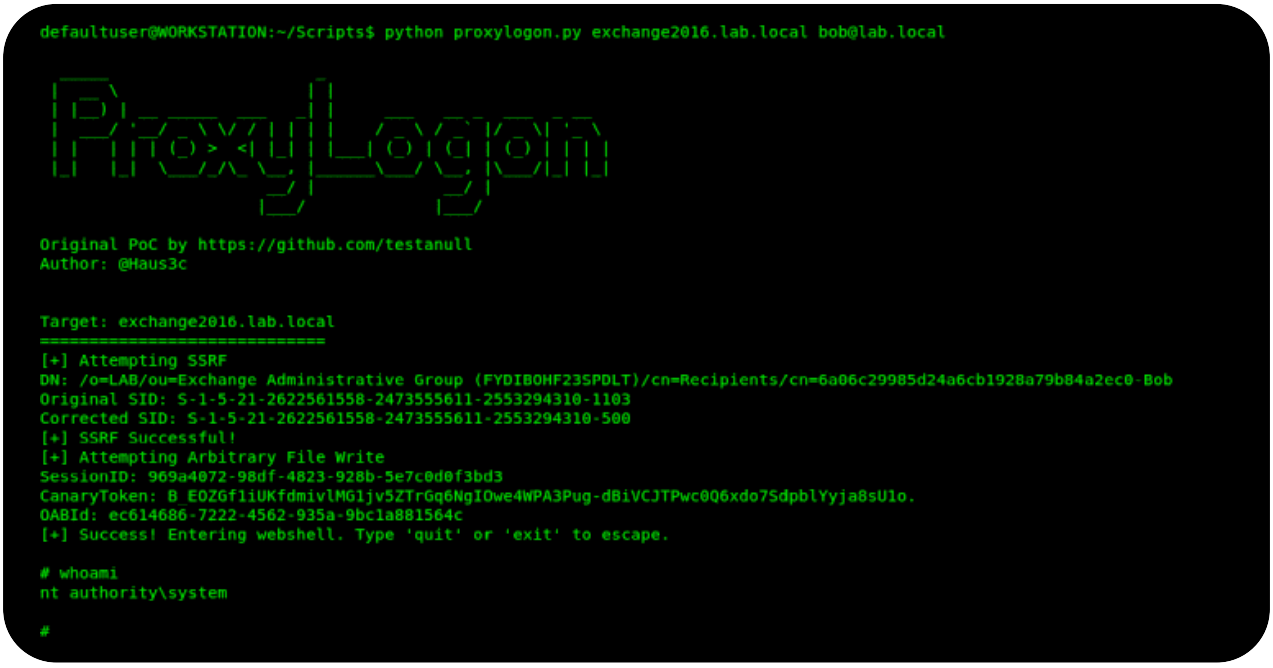
We covered Log4Shell as soon as it materialized with detailed detection methods using Logpoint solutions. We also delve into updates further in the report below.



ProxyLogon (CVE-2021-26855)

ProxyLogon is a critical vulnerability impacting Microsoft Exchange 2013, 2016, and 2019. It enables an attacker to bypass authentication and impersonate an administrator. Due to the absence of patches for internal networks, this flaw remains one of the most widely exploited vulnerabilities in 2022.

The **DEVCORE** team publicly disclosed this vulnerability in August 2021, and it has since been included in various exploit kits and used by various threat actors to inject malicious payloads if the vulnerability is present. This flaw can be easily exploited on port 433 without user interaction, providing access to lateral movement, persistence, and remote manipulation.



ZeroLogon (CVE-2020-1472)

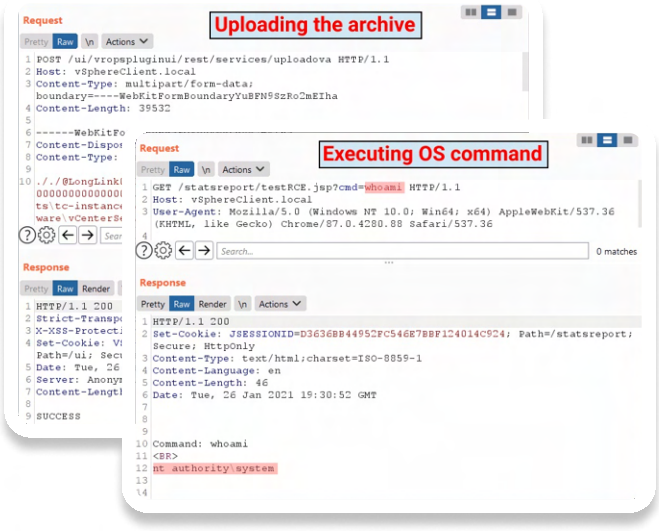
Similarly, the CVE-2020-1472, also known as ZeroLogon, continues to be exploited by threat actors in the wild. This flaw, which was discovered in August 2020, is a cryptographic flaw in the login process. Specifically, the initialization vector (IV) is always set to all zeros, while an IV should always be a random number.

Taking advantage of this vulnerability, an attacker can connect to the Active Directory netlogon remote protocol (MS-NRPC) and log on using NTLM.

VMware vSphere Client (CVE-2021-21972)

A remote code execution vulnerability is classified with a severity rate of 9.8 and was discovered in February 2021 in the VMware vSphere client (HTML5). vSphere is a popular virtualizer used in corporate infrastructures and internal networks.

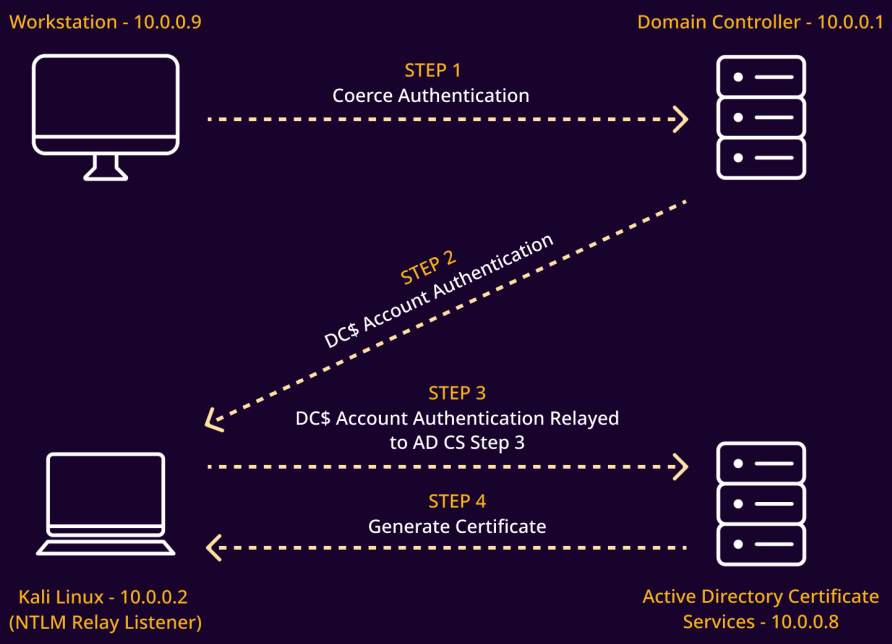
An insider threat can escalate privileges and execute remote commands on the 443 port through this vulnerability. After that, the machine can be used as a springboard to access the entire infrastructure.



For more details about this vulnerability, see this VMware report.

PetitPotam (CVE-2021-36942)

The PetitPotam flaw affects Windows servers where the AD Certificate Services (CS) have not been configured to protect against NTLM relay attacks. This allows a threat actor to gain control of a domain controller by forcing it to authenticate with an NTLM relay server controlled by the attacker, allowing the attacker to intercept traffic and impersonate clients. PetitPotam can be fixed by installing KB5005413 or enabling protections such as EPA or SMB signing for services that allow NTLM authentication. More details about the PetitPotam vulnerability can be found here.



CVE: FINAL THOUGHTS

It is concerning that attackers are still able to exploit old CVEs in 2022, despite updates and notices from security vendors, product owners, and security professionals addressing those vulnerabilities. This might point to a larger underlying issue of the need for regular patching and maintenance of systems to prevent vulnerabilities from being exploited.

In some cases, critical servers may not be able to be upgraded, leaving them vulnerable to attacks. In these situations, companies should implement proper protocols including network hardening and the use of DMZ zones alongside multiple security products that can help to mitigate the risk of these systems being compromised. However, it is important to note that even with these measures in place, attackers may still be able to find and exploit vulnerabilities in systems.

To prevent these types of attacks, it is essential for organizations to prioritize the security of their systems. Regular patching and updates, as well as ongoing monitoring and maintenance, are crucial to ensuring the security of systems and preventing attacks.

LOGPOINT COVERAGE

Over the year, we released 24 thoroughly researched security-specific emerging threats reports, including ransomware, zero-days, and trending attack patterns. The goal was to not just produce noise around the threats but to make sure security teams can understand the threat in detail, and how to detect and prevent them. Here, we look back at some of the biggest hitters of 2022 and their current operations until the end of the year.

Updates on the biggest hitters of 2022

Log4shell

Organizations remain vulnerable, **72%** are at risk of the Log4Shell vulnerability as of October 1, 2022, as revealed by **Tenable's** latest telemetry study, which is based on data collected from more than **500 million tests**.

An organization may have removed Log4Shell from their system at some point, but as they continue to add new assets to their environments, they may encounter the flaw again. To prevent this, it is important for organizations to regularly check their systems for Log4Shell and other vulnerabilities, which is an ongoing process that requires constant monitoring.

- **28% of organizations** across the globe have fully remediated Log4Shell as of October 1, 2022, a 14-point improvement from May 2022
- **53% of organizations** were vulnerable to Log4j during the time period of the study, which underscores the pervasive nature of Log4j and the necessary ongoing efforts to remediate even if full remediation was previously achieved
- As of October 2022, **29% of vulnerable assets** saw the reintroduction of Log4Shell after full remediation was achieved
- Some industries are in better shape than others, with engineering (**45%**), legal services (**38%**), financial services (**35%**), non-profit (**33%**), and government (**30%**) leading the pack with the most organizations fully remediated. Approximately **28%** of CISA-defined critical infrastructure organizations have fully remediated
- Nearly one-third of North American organizations have fully remediated Log4j (**28%**), followed by Europe, Middle East and Africa (**27%**), Asia-Pacific (**25%**), and Latin America (**21%**)
- Similarly, North America is the top region with the percentage of organizations that have partially remediated (**90%**), Europe, the Middle East, and Africa (**85%**), Asia-Pacific (**85%**), and Latin America (**81%**).

Netwalker

The NetWalker ransomware is not currently active since the arrest of one of its associates in 2021. Additionally, a joint operation by U.S. and Bulgarian authorities took down the Circus Spider website, which removed the threat of data disclosure. However, the team behind NetWalker is still active, so there is a chance that the ransomware could come back. To protect against NetWalker and other ransomware, it is important to educate users not to click on links or download attachments from emails, and organizations must invest in security software.

SpringShell

Since the coverage of **SpringShell** back in May, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) **issued an alert** warning of both the Spring4Shell and Spring Cloud Function vulnerabilities.

Alongside VMware, the agency urges administrators to apply fixes to resolve these issues urgently.

Though not as impactful as once thought, Microsoft and CISA still have an active warning of limited, in-the-wild exploitation.

The CERT Coordination Center has provided a **vendor impact list.** It appears that software using Spring offered by organizations including **Blueriq**, **Cisco**, **Jamf**, **PTC**, Atlassian's **ACSB**, and **Red Hat** are affected.

Companies including **F5** and **Fortinet** are investigating the issue and any potential customer impact.

Advisories have **also been released** for VMWare products using the Spring framework and, therefore, vulnerable to CVE-2022-22965: VMware Tanzu Application Service for VMs, Tanzu Operations Manager, and Tanzu Kubernetes Grid Integrated Edition (TKGI).

Patches have been developed **and released** in Spring Framework versions 5.3.18 and 5.2.20. In addition, the project has also pushed fixes in **Spring Boot 2.6.6** and **Spring Boot 2.5.12.**

Spring has released an **'Am I affected?'** guide alongside **workarounds** if immediate patching is not possible.

Bumblebee

Similar to the TTPs we tracked with the ETP report, new campaigns were active for the third quarter of 2022, which have subsided for now. The hackers used Bumblebee to gain access to the system through a contact form campaign. This is not the first time Bumblebee has been used in an intrusion, as we have previously reported on two similar instances. The attack began with the delivery of an ISO file containing an LNK and DLL, which were used to load a Meterpreter agent and Cobalt Strike Beacons.

The hackers then conducted reconnaissance, bypassed user access controls, stole credentials, exploited a ZeroLogon vulnerability to gain higher privileges, and spread throughout the network.

Follina

Follina is a vulnerability that affects a wide range of Microsoft products, including Office suite versions from 2013 to 2021, as well as some Microsoft 365-licensed versions of Office, installed on Windows desktop computers and servers since 2007. The vulnerability is highly impactful, as Office is a widely used business productivity software, and it can be exploited even when Office VBA macros are turned off. Follina has been observed being used by state-backed APT actors in phishing campaigns to install Qbot malware on victim systems and in phishing attacks against government agencies in the US and EU. It is easy to exploit and publicly available proofs-of-concept make it simple to access or create Follina malware, meaning that even novice attackers can potentially take control of systems. Not a high number of exploits have been detected since the official release of the patch which is a good sign. However, if the systems have not been patched, organizations still are at a high risk of being compromised.

QBot

QBot, unlike the rest on the list, has been constantly one-upping its tactics each month. Since our coverage, QBot was found using phishing campaigns that started with stolen reply-chain emails, prompting the users to open an attached HTML file. The attached file includes a method for concealing harmful code within an HTML document by using a base64-encoded SVG image. The image is embedded in the HTML in order to mask the malicious code.

SVG (scalable vector graphics) is an XML-based file format for vector images, which means that it is made up of lines and shapes rather than pixels like raster image types (such as JPG or PNG). One feature of SVG is that it can contain HTML <script> tags, which allows it to execute JavaScript code when the SVG is displayed in an HTML document using an <embed> or <iframe> tag. This means that an SVG file can be used to display an image while also running JavaScript code, potentially allowing malicious code to be hidden within the file.

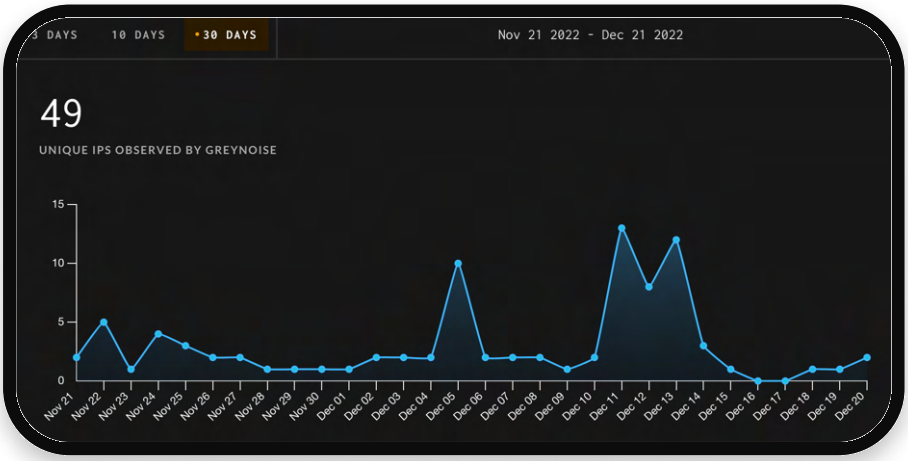
In the technique described, the malicious code is included in a zip archive and smuggled into the SVG image using JavaScript. When the SVG is displayed in an HTML document, the JavaScript inside the SVG is executed, which assembles the zip archive and installs the malware on the end user's device. Essentially, the SVG image acts as a container for the malicious code, which is hidden within the image and executed when the image is loaded.

In the technique described, the malicious code is included in a zip archive and smuggled into the SVG image using JavaScript. When the SVG is displayed in an HTML document, the JavaScript inside the SVG is executed, which assembles the zip archive and installs the malware on the end user's device. Essentially, the SVG image acts as a container for the malicious code, which is hidden within the image and executed when the image is loaded.

However, after the initial infection, the techniques still remain the same. Our detection rules and playbooks still work to prevent the threat in its track, however, responders are suggested to keep their techniques updated.

ProxyNotShell

When we covered ProxyNotShell, it was still a zero-day. Since then, a patch has rolled out. A security researcher, Janggggg, released a proof-of-concept (PoC) exploit for the ProxyNotShell vulnerability a week after Microsoft released security updates for it. The exploit has been successfully used by attackers to backdoor Exchange servers. ANALYGENCE's senior vulnerability analyst, Will Dormann, confirmed that the exploit works on Exchange Server 2016 and 2019, and may be able to be modified to work on Exchange Server 2013. GreyNoise, a threat intelligence company, has been monitoring ProxyNotShell exploitation since late September and has compiled information on the scanning activity and a list of IP addresses associated with these attacks.



Source: GreyNoise

Attacks involving the combination of **CVE-2022-41082** and **CVE-2022-41040** security flaws have been taking place since September 2022, with the goal of deploying Chinese Chopper web shells on compromised servers for purposes such as data theft and maintaining a persistent presence on the server. Microsoft confirmed on September 30 that these vulnerabilities were being actively exploited in the wild. The Exchange Team has recommended that users install the relevant updates as soon as possible in order to protect against these attacks.

LockBit

LockBit seems to have gotten a boost in activity since we last saw it. It was already a leader in its class. However, since then we saw some massive attacks courtesy of Lockbit.

In October 2022, a LockBit affiliate carried out a ransomware attack on Japanese tech company Oomiya, which produces microelectronics and facility system equipment. The attackers stole data using the LockBit ransomware and threatened to leak it unless Oomiya paid an undisclosed ransom by October 20, 2022. Oomiya's supply chain includes major organizations in various industries, such as healthcare, communications, manufacturing, automotive, and semiconductors, meaning that the security incident could have a significant impact on these third-party organizations. The company operates in four main areas: manufacturing and design of chemical and industrial products, pharmaceutical development, design of electronic materials, and factory manufacturing. There have been no reports on the status of negotiations between Oomiya and LockBit 3.0 or the affiliate that used the ransomware.

In addition to attacking Oomiya, LockBit 3.0 also targeted Kingfisher insurance, a UK insurance company that offers specialized insurance, including home and car insurance, under eight different brands. The group claimed to have stolen 1.4 TB of personal data belonging to employees and customers of Kingfisher and demanded that the company pay an undisclosed ransom by November 28, 2022. The ransomware gang was able to infiltrate Kingfisher's servers and retrieve the data before making their demands.

In early November 2022, LockBit 3.0 also targeted Thales, a defense and technology company based in France. The group stole some of Thales' data and threatened to publish it on their data leak site by November 7, 2022. Thales acknowledged the extortion attempt and stated that they had not received a direct ransom notification from LockBit. The company launched an internal investigation and informed the ANSSI national cyber security agency about the incident. By November 10, 2022, LockBit had published Thales' data on their leak site, which Thales confirmed.

ANALYTICS LANDSCAPE

Throughout this report, we find that ransomware and security misconfiguration is the most common pains to enterprise-level organizations. These threats impact organizations that have difficulty protecting themselves, which benefits the attackers. Starting in 2022, we had taken a more proactive approach to deal with these situations. Using telemetry data to improve features and provide additional security context through publications, we hope to have a leg up on threat actors.

As an introductory test, we reached out to our customers to sample data. The data used throughout this report contains anonymized data from our ever-growing and highly expansive network of customers to analyze their data anonymously and share what we learn with the broader security industry.

We used information about the threats we saw and responded to using Logpoint features and alerts. We aim to equip security teams and show how our unique perspective can help security technology developers achieve positive outcomes for their users and the broader community.

For the report, Logpoint performed two main techniques.

Firstly, Logpoint collected alert fire rates from managed customers which were then used to generate an anonymized report.

Additionally, by imitating threat actors' behavior, their malware, techniques, and recorded actions, Logpoint mimicked adversarial TTPs in networks and endpoints without negatively affecting any networks or systems. With the aid of internal tools, open-source, and paid sandboxes, Logpoint analyzed hundreds of attacks. The data came from a variety of places, including forums, malware sandboxes, blogs, white papers from security firms and researchers, commercial and open-source threat intelligence services, and social media.

ALERTS BY NUMBERS

Over the last 365 days, we have released multiple alerts as part of our attack series. This year the most notable ones were:

- LOLBAS
- OSQuery
- Emerging Threats Protection

LOLBAS

LOLBAS (Living Off The Land Binaries and Scripts), refers to legitimate Windows tools and scripts that can be used for malicious purposes. These tools are often present on a target system and can be used by an attacker to perform actions such as executing code, creating new processes, or accessing system resources without being detected. For this exact reason, LOLBAS are becoming increasingly popular among attackers as a way to carry out malicious activities, much more than traditional malicious files such as macros or VBA scripts.

Over a few weeks, we covered the entire LOLBINS, released alongside our regular alert packages as our small effort against the rising LOLBAS situation. Security professionals should be aware of the potential for these tools to be abused and should monitor for unusual activity that may indicate their use in an attack. It is important to have proper security measures in place to protect against the abuse of these tools and to be able to detect and respond to any malicious activity that may occur.

OSQuery

OSQuery is a powerful open-source tool that allows users to perform real-time analysis of an operating system's state. It can be used to detect potential security threats and anomalies on a system by allowing users to run SQL-like queries to search for specific information about the system and its processes. For example, OSQuery can be used to search for specific files, network connections, or system log entries that may indicate the presence of malicious activity. It can also be used to monitor for changes to system configurations or settings that may be indicative of an attempted attack.

One of the key benefits of OSQuery is its ability to quickly and accurately identify potentially malicious activity on a system. By running regular queries, security professionals can identify any unusual or suspicious activity and take appropriate action to prevent or mitigate an attack. In addition, OSQuery's real-time analysis capabilities allow it to detect potential threats as they happen, rather than after the fact.

We have diverted our efforts to make use of OSQuery, where applicable, to assist in easier detection. The alerts are few and between for now, but we will continue to push them out with updates.

EMERGING THREATS PROTECTION

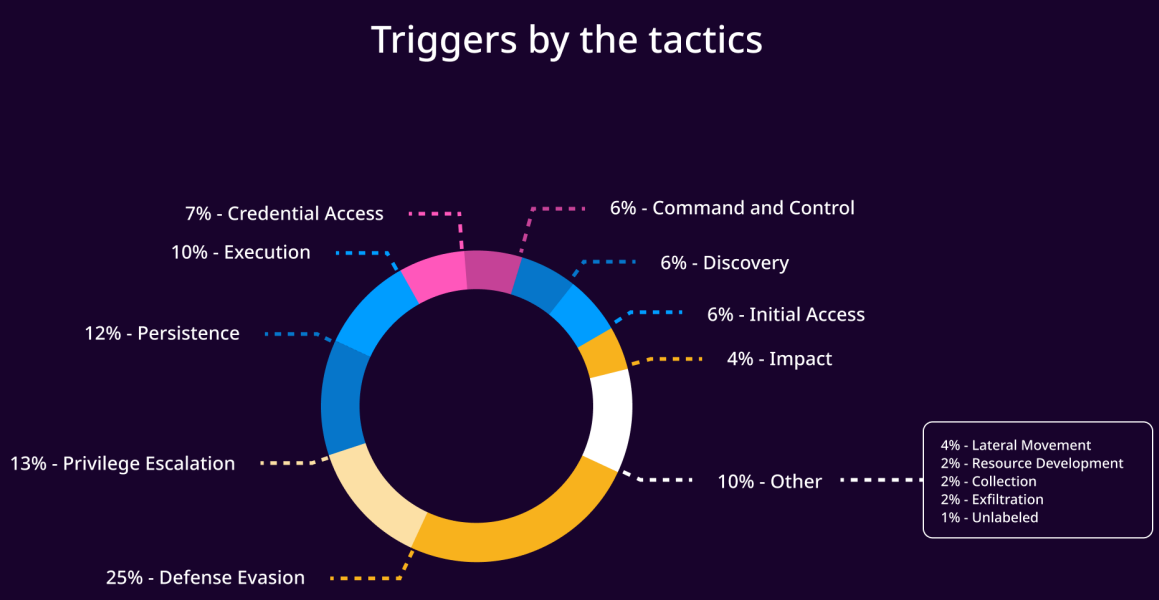
Every other week a new vulnerability is discovered and becomes public. Some customers know how to deal with them, while others don't. The Logpoint Security Research team researches and investigates new major vulnerabilities discovered, and builds SIEM rules and SOAR playbooks for investigation and response. With each new edition of Emerging Threats Protection, we released alert and investigation queries that provide base-level security to detect any particular threat in question.

We also regularly add vendor-specific analytics. In the last year, we added 22% of new alerts to our arsenal and removed 3% of alerts we deemed as legacy content.

One of the major improvements we made was thanks to real-world testing by simulating hundreds of attacks over periods of months and on different sets of variables. This helped us with the transparency of how the customers might be using Logpoint and how we can fix those issues on our side. We strive to constantly improve our queries and capabilities and this year we saw a 24% increment in our coverage after simulation attacks with Picus and Atomic Red Team.

BY THE TACTICS

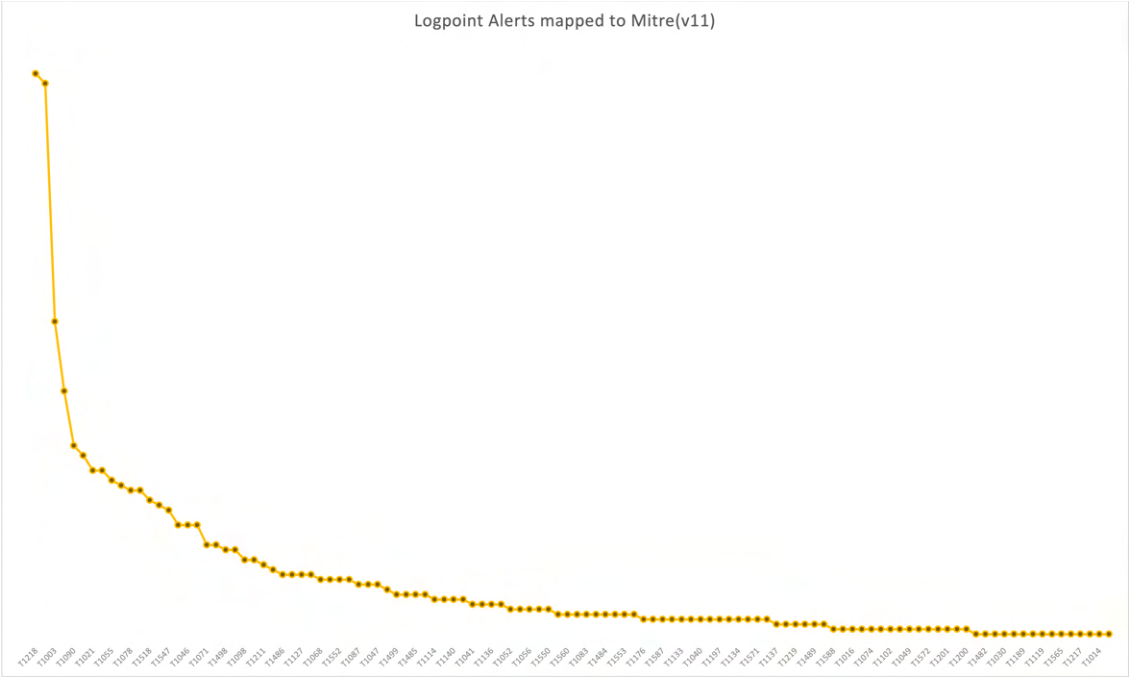
Starting with MITRE ATT&CK® mappings to our endpoint behavior rules, we found that ~34% of alerts fell within the defense evasion bucket, followed by execution at ~22% and credential access at ~10% as shown below.



From our findings, defense evasion is a key component of all types of attacks, not just targeted ones. In addition to bypassing security measures, these techniques also allow threats to avoid being detected. By evading detection, threats can remain on a system for a longer period and increase the chances of success. It also indicates that defense evasion has become a necessity for threats that expect to encounter security measures in place.

Triggers by the tactics	Percentage
Defense Evasion	25%
Privilege Escalation	13%
Persistence	12%
Execution	10%
Credential Access	7%
Command and Control	6%
Discovery	6%
Initial Access	6%
Impact	4%
Lateral Movement	4%
Resource Development	2%
Collection	2%
Exfiltration	2%
Unlabeled	1%

Individually, "System Binary Proxy Execution" at (12.72%) was the most detected technique with “Command and Scripting Interpreter" at a close second with (12.5%) and "OS Credential Dumping": (7.1%), "Event-Triggered Execution": (5.5%) and "Proxy": 39 following suit.



CONCLUSION

The improvements made to Logpoint’s analytics over the past year have been significant compared to what we had planned and have greatly benefited both the company and its customers. Sharing this data with customers has provided valuable visibility into the company, the product, and the team, and has helped to build trust and transparency. The goal of these efforts has been to ensure that customers have the information they need to make informed decisions and to feel confident in the company's ability to protect against cyber threats. We can harness the data we have collected to further develop and improve the solutions we provide to our customers. Without going into many details, we found that more generic attack patterns trigger the most as expected. However, from a deeper dive, we noticed that most customers did not have a proper setup to make the best out of the features provided by Logpoint out of the box. For this, we also have updated our configuration guide regarding the alerts and other features.

It is important to note that the team is fully committed to helping customers with their cyber defense efforts. By providing access to data and insights, the team is working alongside customers to identify potential vulnerabilities and implement effective solutions. With the team's support, customers can feel confident that they have the tools and resources they need to keep their systems and data secure. Overall, the efforts made by the company to improve analytics and share data with customers have helped to build a strong foundation for cybersecurity and have contributed to the overall success of the company.

With so many variables and uncertainties that can affect the course of many events, it is tough to make concrete forecasts, but we can hedge our bets. There are some general trends and issues that are likely to shape the year ahead. Some of the key factors that may influence the global economy, politics, and society in 2023 include the ongoing impacts of the war in Ukraine, the tail end of the COVID-19 pandemic, the potential for further political and social tensions, ongoing technological advances, and their potential impacts, and the potential for natural disasters and other global challenges. As the year progresses, it will be important to stay informed about these and other developments and to be prepared for potential changes and challenges that may arise.

Based on these issues we have come up with a few forecasts of our own and how a company should go about dealing with them.

Forecast 1:

Names will change, Tools will change, Attacker remains the same

Since we covered a few “Decommissioned“ APT groups and their tactics, we have been seeing similar TTPs being used by 'new' groups, which leads us to wonder if it is just a rehash of the same group, some members breaking off and sticking to what that works or a definite copy cats.

Recommendation 1:

Thoroughly looking at trending APT gangs and putting necessary defense mechanisms against their TTPs might give peace of mind regarding their security posture and potential breaches. However, a proactive approach is always a must.

This should include implementing and regularly updating security controls such as firewalls, intrusion prevention systems, and endpoint protection, as well as regularly training employees on how to identify and prevent potential attacks. Additionally, consider implementing a threat intelligence program to stay up-to-date on the latest tactics and techniques being used by attackers, and ensure that your organization is prepared to respond quickly and effectively to any potential threats.

Forecast 2:

No one is safe. We’re all in it together

The war is far from over and more psychological attacks will keep coming as everyone including the willing and unwilling participants are caught in the crosshairs. Critical infrastructures like healthcare, power grids, and water suppliers are going to see a rise in attacks.

Recommendation 2:

Everything has become fair in cyber warfare. To crumble an entire nation, critical infrastructure will continue to be targeted and companies need to prioritize cybersecurity measures to protect themselves and their customers. This can include implementing strong password policies, regularly updating software and systems, and training employees on how to identify and prevent potential attacks. It may also be beneficial for companies to consider investing in cybersecurity insurance to provide additional protection in the event of an attack.

Forecast 3:

The “Art“ificial “in“telligence Phishing

The future of phishing is looking artificial, as AI-powered attacks become the hook du jour. With machine learning algorithms constantly improving, these cybercriminals are casting a wider net and reeling in unsuspecting victims at an alarming rate. It's no longer a question of if you'll fall for a phish, but when. So beware, and make sure to keep your wits about you, or you may find yourself in deep water with these clever computerized con artists. Trust us, you don't want to be left out to dry by a phishing AI.

Recommendation 3:

As the use of artificial intelligence (AI) in phishing attacks becomes more prevalent, companies need to take steps to protect themselves and their employees. Phishing attacks can have serious consequences, including the loss of sensitive data and financial losses. To mitigate these risks, companies should implement several measures.

First and foremost, strong email security measures should be put in place. This can include using spam filters and implementing two-factor authentication for email accounts. It is also important to educate employees about the various tactics that phishers use and how to spot and report suspicious emails. Anti-phishing software can also be a useful tool in detecting and blocking phishing emails before they reach employee inboxes.

In addition to these measures, it is important for companies to regularly update their security systems and software. Keeping these systems and software up to date ensures that they can protect against the latest threats, including those that use AI. By staying vigilant and following these recommendations, companies can help to reduce their risk of falling victim to a phishing attack and protect their sensitive data and systems.

Forecast 4:

Comebacks and Duplicates

Many in the cyber community know of the success that existing and olden malware has had. Even though the actors have disbanded, or are in the low, one can never rest assured. If the comeback of Emotet and IcedID and new players like Bumblebee have taught us anything, the attack will come with a new flavor, not if but when. This will include file-less malware like with the use of LOLBINS.

Recommendation 4:

There are of course no one-step resolutions to deal with ATPs. However, one can start by implementing application whitelisting, regularly updating software and systems, training employees to recognize and report suspicious activity, use of endpoint protection, staying up-to-date on the latest tactics and techniques being used by APTs with a threat intelligence program, and considering investing in cybersecurity insurance. It is important to be proactive in protecting against APTs and to have a comprehensive security strategy in place to defend against these types of threats.

Forecast 5:

More of IoT hacks

It is likely that in the future, we will see an increase in the use of IoT devices as a means of launching cyber attacks. These attacks may target individuals, businesses, or even entire infrastructure systems. IoT devices are often poorly secured and can be easily hacked, making them an attractive target for cybercriminals. As a result, we will likely see more news stories about IoT-based things like cars, smart homes, AI assistants, and other connected devices being hacked.

Recommendation 5:

As more and more devices will be added as a way of convenience or for "security", each new device should be considered as a new vector for attacks. Add to the fact that many IoT companies do not provide security updates or measures in the first place, a line of defense must be implemented in-house by default. This may include implementing strong passwords and regularly updating software and firmware, as well as regularly scanning for and identifying vulnerabilities in these devices. It may also be advisable to implement network segmentation and access controls to limit the potential impact of any successful IoT-based attacks. Companies should also consider implementing security measures such as firewalls and intrusion detection systems to protect against IoT-based threats. Additionally, companies should educate their employees on the importance of cybersecurity and the potential risks associated with IoT devices.

CONCLUSION

The past year has been marked by numerous high-profile cyber attacks and a constantly changing threat landscape. Threat actors, including financially motivated criminals and state-sponsored groups, have demonstrated increased aggression and sophistication. In order to stay ahead of these challenges, it is crucial for security teams to understand the changing dynamics of adversary tactics, as outlined in this year's report.

Based on data from customer telemetry, incident response, underground monitoring, proactive threat research, and intelligence relationships, the report highlights key findings such as the continued prevalence of phishing attacks, the impact of the rise in ransomware, and the importance of addressing critical vulnerabilities in order to prevent successful breaches.

The report also offers insights and forecasts for the year ahead, including the potential emergence of new types of malware and the ongoing threat of APT activity. Overall, the report serves as a valuable resource for security professionals looking to stay informed and prepared in the face of an increasingly ominous threat landscape.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**