paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

MALWARE

2023

NETWORK THREAT TRENDS RESEARCH REPORT

VOLUME 2

Table of Contents

Executive Summary 3

Data Source and Methodology 4

Making Sense of Today's Malware 5

Malware Trend Analysis 10

Observation From the Malware Network Traffic 16

Malware Predictions in 2023 18

Conclusions and Takeaways 19

About Palo Alto Networks and Unit 42 23

Executive Summary

In this report, the Palo Alto Networks Unit 42 research team shares current trends in malware and the evolving threat landscape. This includes an analysis of the most common types of malware and their methods of distribution. With the growing volume and sophistication of today's threats, it's critical for network security professionals to understand the threat landscape and how to properly defend against it.

The insights provided in this report are intended to give you a better understanding of how the threat landscape is evolving and provide security recommendations for organizations to protect themselves.

Most findings are based on data and observations we gathered in 2022 and are a comparison to one year earlier. Data for AI was collected between November 2022 and April 2023. Here are some key highlights of the findings:

- We've seen a boom in traditional malware techniques taking advantage of interest in AI/ChatGPT.
- The ratio of malware impacting industries using Operational Technology (OT) has increased by 27.5%.
- Exploitation of vulnerabilities increased 55% compared to 2021.
- PDFs are the most popular file type for delivering malware as email attachments (66.6% of all attachments).
- While nearly 49% of network communication generated during sandbox analysis (including both malicious and benign files) uses encrypted SSL for its traffic, 12.91% of network traffic generated by malware (such as phoning home, getting time calibration) is encrypted with SSL.
- Cryptominer traffic has doubled in 2022.

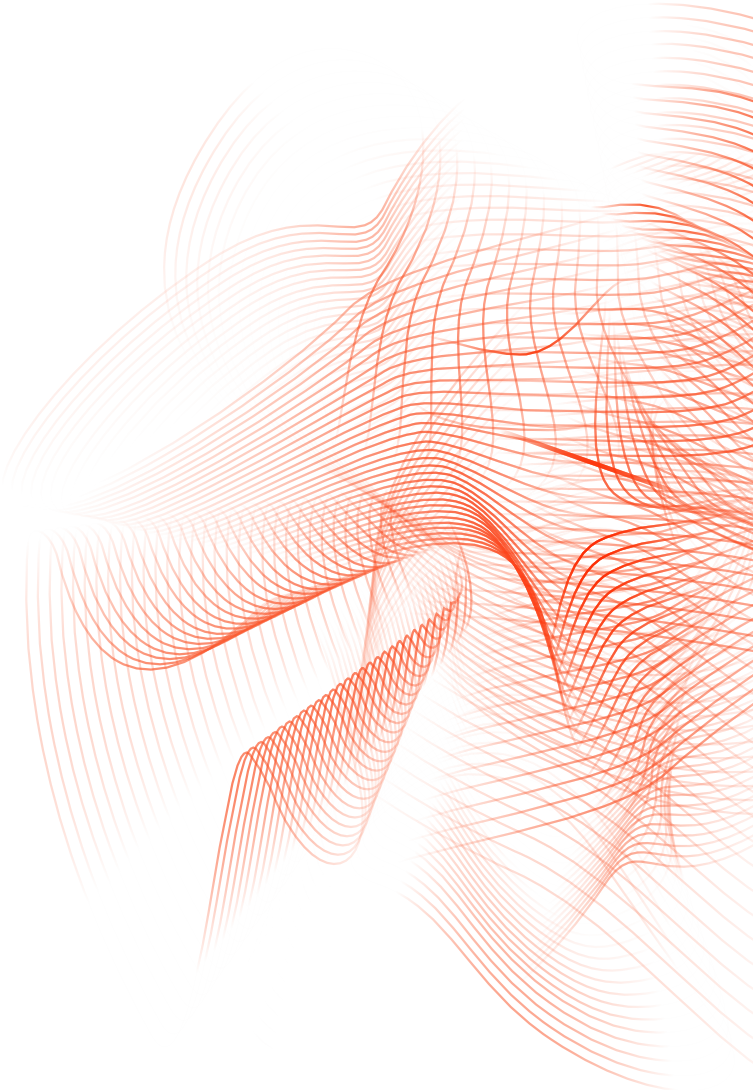
We will also discuss emerging advanced threats that organizations should be aware of. Sophisticated multivector attacks are designed to elude detection using an array of evasion tools and camouflage techniques. The result is a significant strain on IT and security teams charged with strengthening the organization's security posture. Armed with expert knowledge and recommendations, you can make your organization a less tempting target.

Data Source and Methodology

In this report, we cover data mostly from the 2022 calendar year. To elucidate threat trends, we also compare this with data from 2021 or earlier. Our data sources include Palo Alto Networks Next-Generation Firewall (NGFW), Cortex Data Lake, Advanced URL Filtering and Advanced WildFire. Data for AI/ChatGPT was collected between November 2022 and April 2023.

Real-world suspicious files are captured and submitted through Advanced WildFire, for analysis by Palo Alto Networks from telemetry collected from NGFW, Prisma SASE, Prisma Cloud and Cortex XDR. These files come from different regions, including the United States, Singapore, Japan, Australia and countries in the European Union. This data includes attacks targeting different environments like cloud containers and traditional network traffic. These attacks were on a variety of industries such as manufacturing, finance, education and tech companies.

Our data sources also include external feeds and sample exchanges among security vendors. Collected data contains more than 40 different file types, including Portable Executables (PE), dynamic-link library (DLL), scripts and compression files. By having such a large dataset, we hope to identify malware threat trends and provide analysis for the most significant and prevalent malware trends in the wild.



Making Sense of Today's Malware

Understanding threat actors' preferred methods and malware families can give you insights for how to set up your defenses to best protect your organization. You can prevent popular malware spreading mechanisms and learn what behaviors are common in the most prevalent malware types.

How Does Malware Spread?

It's vital to understand how threat actors gain access to systems and what they do when they have it. From there, we need to know what sorts of commands they issue once they're inside targeted networks.

Vulnerability Exploitation

55% increase in vulnerability exploits in the wild compared to 2021.

Vulnerabilities Continue to be a Popular Method for Threat Actors to Infect Victims

By the time security researchers and software vendors close the door on one vulnerability, threat actors have already found the next open door to leverage.

This constant churn creates pressure on enterprise security teams attempting to protect their networks from bad actors exploiting those vulnerabilities.

As shown in Figure 1, we've seen increases in threat actors' exploit attempts of vulnerabilities for the last four years. The data in the figure shows increases starting in 2019. Between 2021-2022, we saw a 55% increase in vulnerability exploitation attempts, per customer, on average.

Much of this increase can be attributed to the increase in exploitation attempts using the Log4j and Realtek supply chain vulnerabilities. A top malware sample on the Linux platform, a Mirai variant, spreads by exploiting newly discovered vulnerabilities within firewalls, switches, wireless routers and internet of things (IoT) devices.

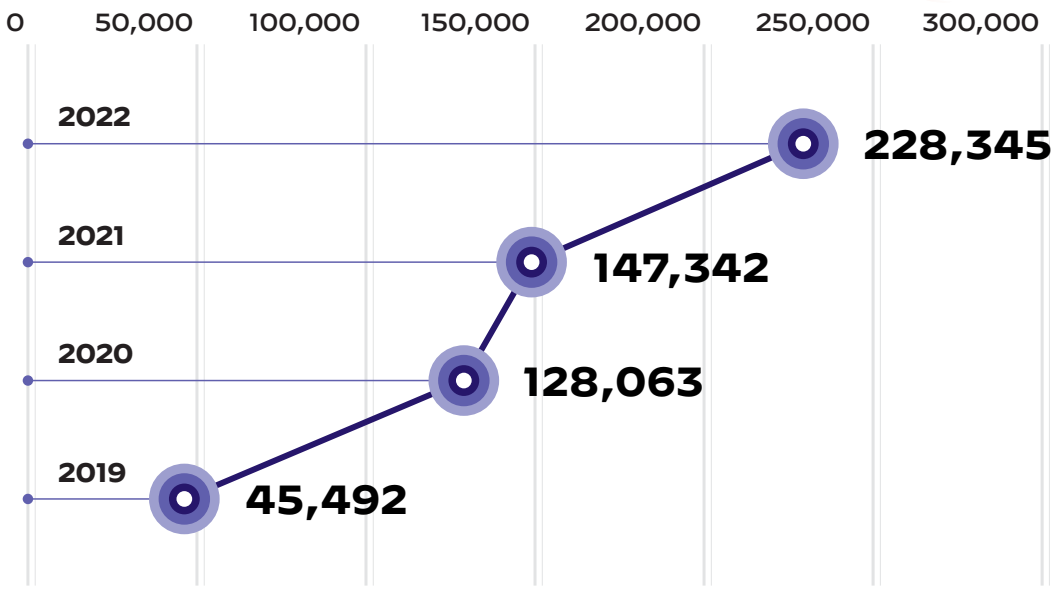


Figure 1. Vulnerability exploitation attempts

Attackers are using both vulnerabilities that are already disclosed and ones that are not yet disclosed. (aka exploiting zero-day vulnerabilities). We continue to find that vulnerabilities using remote code execution (RCE) techniques are being widely exploited, even ones that are several years old.

While using old vulnerabilities might seem counterproductive, they still have significant value to attackers. In some cases, vulnerabilities discovered years ago have not been patched. This could be either because the company failed to fix the issue, or they didn't provide the patch in a way that customers could easily find. In other cases, the product could lack a patch because the product is at the end of its supported lifespan.

But the full weight of responsibility is not just on the vendor supplying the product with a vulnerability. Organizations must also have appropriate processes in place for updating in a safe and timely fashion. For example, companies must have a policy in place for acquiring, testing and applying patches, as well as the bandwidth to apply them. Many companies could also lack awareness of available fixes, which effectively turns an old, known vulnerability into something as risky as a zero-day threat.

Threat actors know these problems exist, and they continue to try these old vulnerabilities because they're counting on organizations to fail at some point in the process of applying patches.

Email as Infection Vector

Email continues to be a popular infection vector for threat actors, but they have to pair it with social engineering tactics for it to be successful. Figure 2 shows that even though executables are the file type of choice for malware once on a victim's system, attackers are more likely to deliver malicious PDF files in email attachments.

PDFs are the primary malicious email attachment type being used 66% of the time to deliver malware via email. PDF files are commonly used in a business environment, and victims are less likely to be wary of an expected file type, versus unexpected file types like EXEs. They could also simply be unaware that this type of file could be used for nefarious purposes.

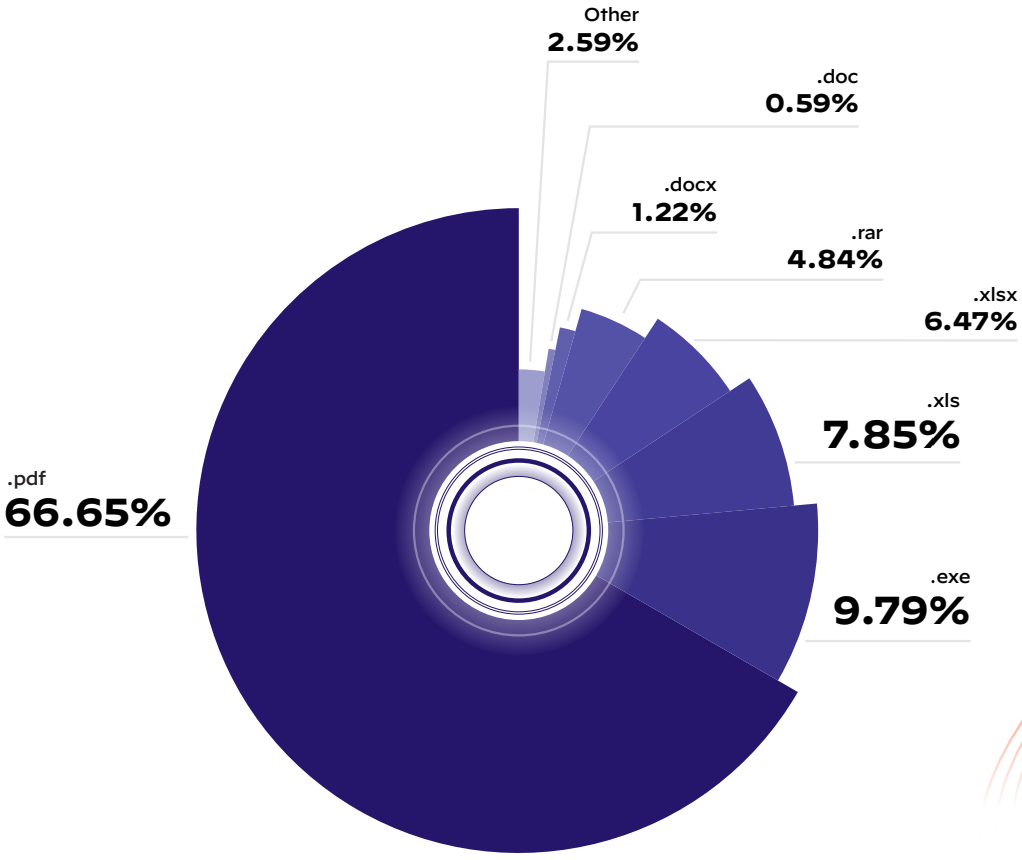


Figure 2. Malicious email attachment file types

Most people are aware of warnings against clicking strange links in emails, so PDF phishing schemes could fly under their radar better than a text-based email with just a plain link. Naming conventions expected in a business context like `invoice_AUG_4601582.pdf` or `Updated Salary Evaluation` could lure unsuspecting targets into opening these attachments.

The attachments themselves might contain a URL link to click, or a button that sends victims to a website with a malicious purpose.

Compromised Websites

Threat actors exploit secure environments to catch victims off-guard and breach their digital defenses. One such technique is to find ways to inject their malicious code onto legitimate websites. They search for vulnerabilities in websites, or in third-party plugins or libraries. Once found, threat actors often exploit those vulnerabilities using techniques such as injection attacks.

A malicious script injection campaign we recently tracked used malicious code that dynamically loaded JavaScript on a website from an attacker-controlled URL. The code then redirected victims to different sites where it deployed malicious content.

Since attackers controlled the redirection chain, they could continuously change the malicious content to distribute phishing pages, malware or adware. Many of the malicious scripts were injected into legitimate corporate homepages, putting more people at risk.

Websites created using WordPress have become a favorite target. This could be an indicator that one or more vulnerable third-party plugins could have allowed threat actors to perform malicious script injections.

Fresh Domains for Mayhem

It's not just already established websites that have value to threat actors. To stay under the radar of detection mechanisms, malware authors have found newly registered domains (NRDs) to be helpful for phishing, social engineering or spreading malware.

Threat actors using NRDs can snare people using either authorized or unauthorized drive-by-download attacks. In authorized drive-by-download attacks, a victim downloads malware after taking an action (such as clicking a button) without being fully aware of the implications. In an unauthorized drive-by-download, the malware download happens without the knowledge of the victim. Attackers can use a variety of techniques such as social engineering or disguised icons to trick users into executing the malware.

Figure 3 shows that threat actors are more likely to target people visiting adult websites (20.2%) and financial services (13.9%) sites when creating NRDs.

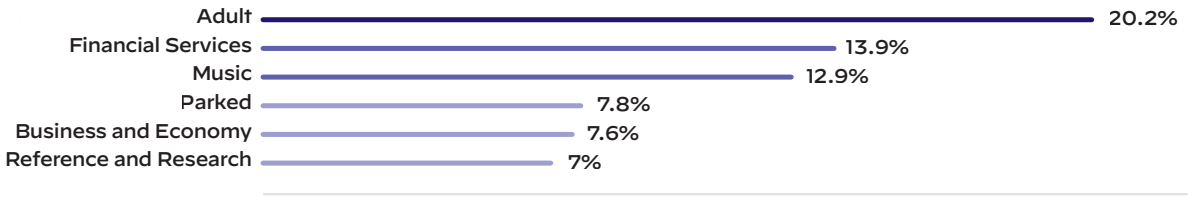


Figure 3. Newly registered domain category distribution

Threat actors prefer adult websites for spreading malware because these sites draw a high volume of traffic. People visiting these sites are also likely to be expecting to download files to view.

Financial and music services websites are also high in NRDs, which indicate they are lucrative targets for threat actors to spoof when launching phishing campaigns. People should be careful when accessing unfamiliar sites.

Malware Families and Variants

To better understand the current threat landscape, it helps to step back and look at which families of malware are most commonly used. Grouping malware by families and studying their variants help us pinpoint and understand common techniques used by attackers.

It is also valuable for tracking the evolution of threats and gaining insight into the goals of those who seek to exploit.

Figure 4 looks at common malware families with respect to the number of the variants within that family. While reviewing tens of thousands of malware samples from our telemetry, we found that the Ramnit malware family had the most variants in our detection results.

Ramnit and its family of variants are used to steal credentials from browsers or other applications on compromised systems. The attackers' goals were typically monetization by stealing credentials or cryptocurrency and creating a backdoor on the victim's system for further access.

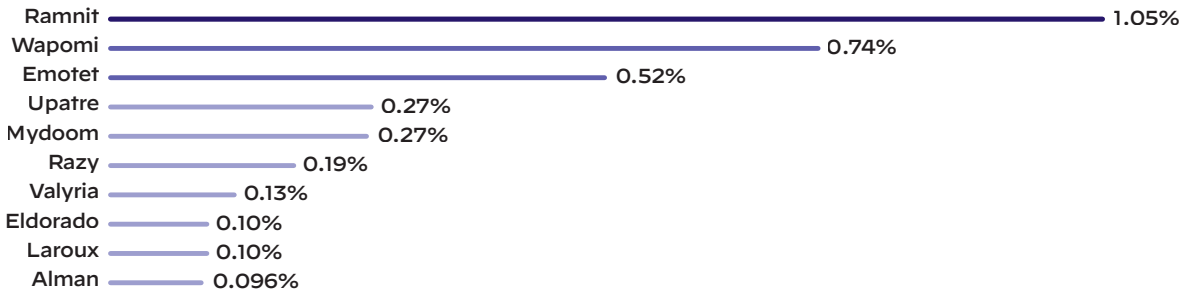


Figure 4. The most diverse malware families

Malware Trend Analysis

Another important aspect of malware trends to explore is how attackers are using evasive techniques. If malware can run without detection, the threat actors have more opportunity to exploit a system for financial gain, espionage or information theft.

Threat actors are using tactics such as evading sandboxes, or laying in wait and relying on human interaction to trigger attacks. These activities reveal a deep understanding of common security tools and services.

Attackers are also exploring attacks on different operating systems, including Linux systems and IoT devices. This evasion and diversification, combined with the continued prevalence of attacks, means threat actors will continue to keep security teams on their toes.

AI Is Getting Popular, So Are Related Scams

ChatGPT has gained significant attention and popularity due to its AI capabilities that can assist people in various tasks including drafting, translating and summarizing the meaning of articles. The current cultural focus on AI has extended to questions about its potential impact on cybersecurity. While there are proofs of concept (PoC) demonstrating how AI could create malicious activity, we have not yet seen a noticeable rise in attributable real-world attacks of this type. However, we see many more traditional techniques attempting to take advantage of AI trends, resulting in a boom in AI/GPT-related scams.

Between November 2022-April 2023, we noticed a 910% increase in monthly registrations for domains, both benign and malicious, related to ChatGPT. We also saw tremendous growth (17,818%) in attempts to mimic ChatGPT through squatting domains – website names that are deliberately registered to appear similar to a popular brand or product. Squatting domains can cause security risks and consumer confusion, while creating opportunities for malicious actors to profit, such as through advertising revenue or scam attacks.

The popularity of ChatGPT has also led to the appearance of related grayware, which is software that falls somewhere between malicious and benign. This category includes adware, spyware and potentially unwanted programs. Grayware might not be explicitly harmful, but it can still cause issues or invade peoples' privacy. Figure 5 shows this trend, in the weeks surrounding the public release of the ChatGPT API. It suggests that cybercriminals are looking to exploit the popularity of ChatGPT to spread potentially unwanted or harmful software. Therefore, it is important for users to remain vigilant and take steps to protect their systems and data.

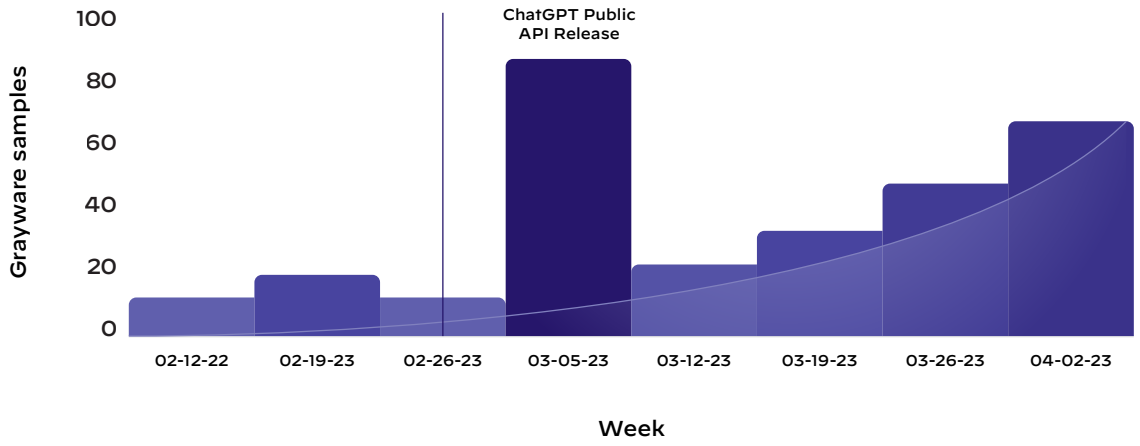


Figure 5. Grayware related to ChatGPT

The speed with which scammers used traditional techniques to profit off the AI trend underscores that organizations need to exercise caution around internet activity and software that are getting attention in popular culture. At the same time, it remains possible that threat actors could find ways to take advantage of the unique technological capabilities of AI.

For the time being, the main way that organizations can prepare for this possibility is to continue to employ defense-in-depth best practices. Security controls that defend against traditional attacks will be an important first line of defense against any developing AI-related attacks going forward.

Malware Aimed at Industries Using Operational Technology (OT) is Increasing

Industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and other operational technology (OT) systems can be high-value targets for cyberthreats. These systems are used in critical infrastructure industries such as energy, transportation, manufacturing and healthcare. Any disruption to these systems can have severe consequences for public safety, the environment and the economy.

These industries face a wide range of security threats, including malware, ransomware, physical attacks, supply chain attacks and vulnerability exploits. When attackers are successful, this can lead to production loss, equipment damage, environmental damage and even endangering human life.

We have conducted in-depth research with the aim of providing a comprehensive overview of the current threat landscape facing particular industries.

In these industries, between 2021 and 2022, we saw the average number of attacks experienced per customer in the manufacturing, utilities and energy industry increased by 238%. This finding is visualized in Figure 6.

In the last year, we saw seasonal fluctuations and an increase of 27.5% in the ratio of malware targeting industries above, over all network sessions.

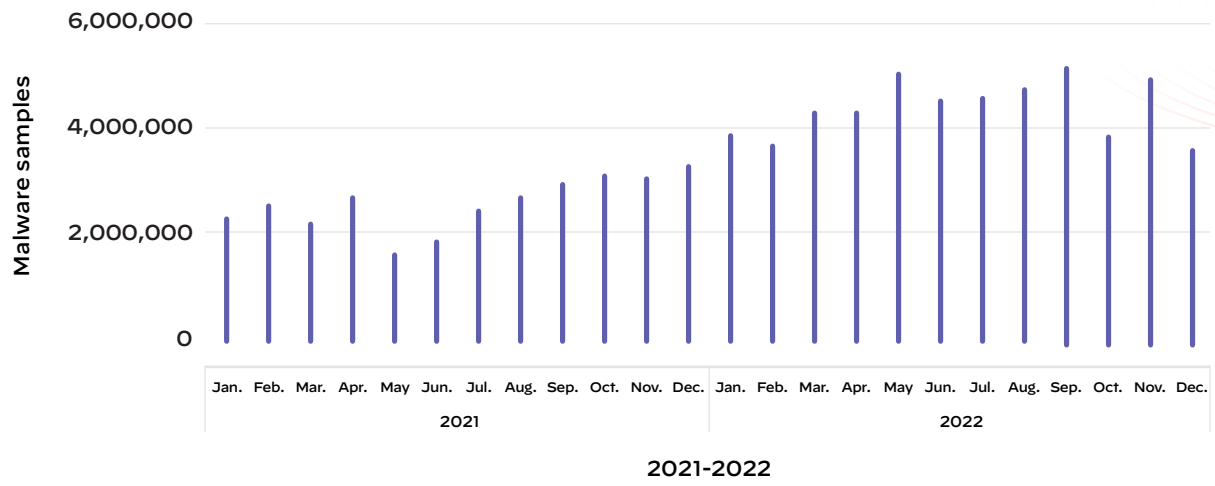


Figure 6. Unique malware samples in manufacturing, utilities and energy industries

To mitigate these risks, it is essential for organizations to implement comprehensive security measures that cover all aspects of their OT systems. This requires regular risk assessments, vulnerability testing and security awareness training for all stakeholders involved.

By taking a proactive approach to OT security and adopting a holistic approach, organizations can effectively protect their critical infrastructure and ensure their systems continue to operate safely and efficiently.

Zero-Day Attacks

Zero-day attacks are much more difficult to defend than known threats, hence they pose a higher risk than other exploits. During the time after a zero-day vulnerability becomes widely known, but before organizations can apply a patch, the risk of an exploit is particularly high. Once the vulnerability is public, attackers can weaponize it for profit, especially when a Proof of Concept (PoC) is available.

There are times when this interval can be especially risky, such as when an issue is complex and patches can't be quickly made available. This risk can be compounded if security vendors don't yet have protections in place and mitigations are not yet available.

Table 1 includes notable CVEs that are considered High or Critical severity as well as attempted attacks we observed earlier this year. As you can see, it often doesn't take long for threat actors to take advantage of a vulnerability.

CVE	Date Publicly Disclosed[1]	NVD Record Date[2]	Date Exploit-in-the-Wild First Discovered
CVE-2020-35131	01/07/2021	01/08/2021	01/28/2021
CVE-2020-29557	12/11/2021	01/29/2021	02/17/2021
CVE-2021-32172	04/26/2021	10/07/2021	06/15/2021
CVE-2021-33544	07/08/2021	09/13/2021	07/19/2021
CVE-2022-31446	05/23/2022	06/13/2022	06/19/2022
CVE-2022-2488	07/19/2022	07/20/2022	08/11/2022

Table 1. Vulnerability disclosure vs. exploit-in-the-wild time

Highly Evasive Threats

Over the past several years we've observed how malware authors have continued the trend of statically and dynamically armoring their payloads from traditional detection methods.

Our industry has standardized types of static and dynamic detection methods such as the following:

- Static signatures like YARA, imphash, ssdeep and many others
- Antivirus instruction emulation to scan for patterns unique to malicious executables
- Sandboxes used to find suspicious events during execution
- Supervised machine learning models that incorporate data or features from all of these sources

Malware is considered highly evasive when it has effectively countered the set of traditional detection techniques in order to make detection problematic.

Trends in Evasive Threats

A significant minority of malware now falls into the category of being highly evasive. Malware authors continue to move in this clandestine direction.

A growing number of samples are using red team tools such as Cobalt Strike and Metasploit. These frameworks were created for the specific purpose of avoiding the previously mentioned categories of detection techniques. Several malware families are now using Cobalt Strike as well as Brute Ratel to avoid detection.

Each year our operations team also encounters new variations of an old idea – sandbox evasions. In early September 2022, we discovered a GuLoader variant that successfully evaded most security vendors. This variant contained a shellcode payload protected by anti-analysis techniques, which are meant to slow human analysts and sandboxes processing the sample. We see a continually increasing diversity of methods being used to avoid behavioral detection.

Raising the Bar for Detection

Given that highly evasive malware demonstrates awareness of the industry standard practice, we must go above and beyond to improve detection capabilities. One approach that has been shown to be effective against this threat is analyzing process memory during execution.

The key idea of this approach is that parsing artifacts and other useful information from changes in process memory can provide insights that cannot be easily hidden. This solves the problem of sandbox evasions by removing the need for behavioral analysis from a full detonation within a sandbox. In order for malware performing a sandbox evasion to determine that it will not fully execute its payload, it must load its code into memory, which renders it detectable.

Ransomware Increases and Diversifies

Ransomware is getting easier for threat operators as ransomware-as-a-service (RaaS) operations gain popularity. This offers criminals an array of easy-to-use tools and services that make launching ransomware attacks incredibly simple.

We also saw an increase in multi-extortion ransomware activity, where cybercriminals add further pressure on victims to pay. Attackers do this by threatening to publish data stolen from their victim, harass their victims or launch denial of service attacks against them.

Ransomware is among the types of malware that uses a wide variety of vulnerabilities to exploit their victim and deploy their payload. These attacks are also commonly spread via social engineering techniques such as malvertising campaigns, as well as by abuse of Microsoft Remote Desktop Protocol.

Linux Threats Target Cloud Workloads and IoT Devices

While representing a relatively small number of attacks, Linux malware is on the rise. Attackers are looking for new opportunities in cloud workloads and IoT devices that run on Unix-like operating systems. The growing prevalence of this family of operating systems among mobile and "smart" devices could explain why some attackers are turning their eyes toward Linux systems.

Figure 7 shows that the most common type of threat against Linux systems is botnets. The malware families of choice for this type of operating system are Mirai (14.3%) and Gafgyt (4.7%).

The release of the Mirai source code in 2016 enabled attackers to create new variants with new exploits and new functionality. These variants usually spread by continuously updating their arsenal of exploits, looking for victims by actively scanning and then exploiting any vulnerable IoT device they can find on the internet.

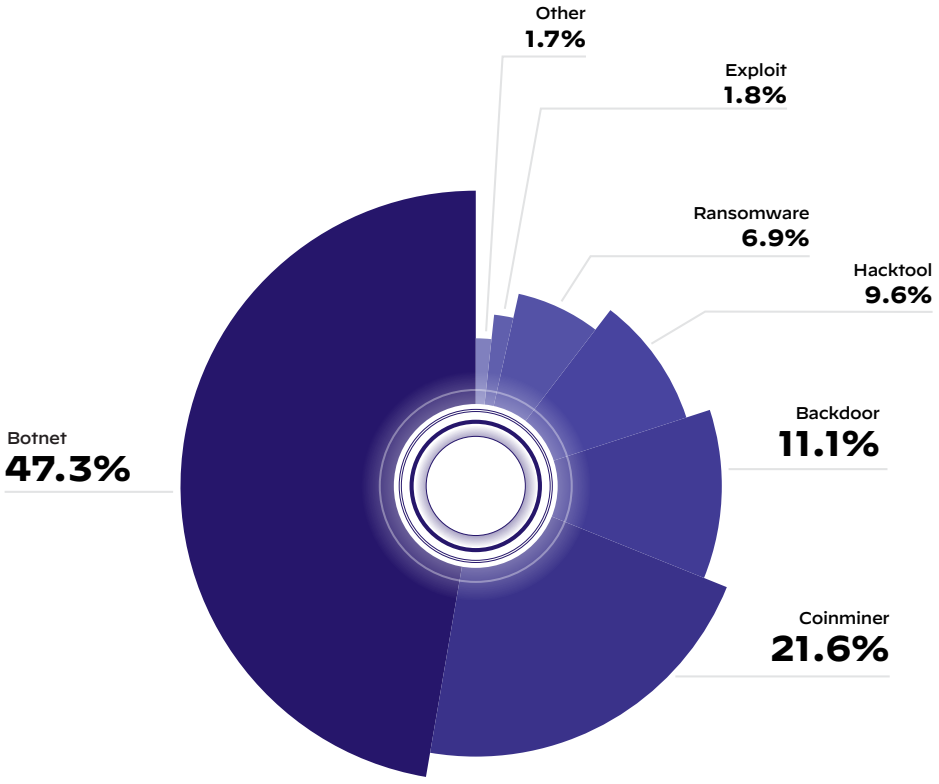


Figure 7. Malware type distribution in Linux systems

Observation From the Malware Network Traffic

More than 647 million command and control (C2) traffic sessions were detected during 2022.

We reviewed C2 traffic captured by Palo Alto Networks services to gain more insight into active malware activities. Here's what we found.

Decrypting Traffic Becomes Increasingly Important

We collected over 134 million network traffic sessions generated by samples during sandbox analysis and found SSL was the most common protocol for both benign and malicious samples, constituting 48.94% of traffic.

In the portion of this traffic generated by malware, 12.91% of sessions were SSL encrypted. To better understand the nature of the encrypted traffic, we also checked the reputation of the Server Name Indication (SNI) and IP addresses of each session. 3.6% of this SSL encrypted traffic was being received by endpoints with a bad reputation, meaning they could be C2 servers or other attacker-controlled devices.

SSL traffic is of particular concern because it's the same kind of encryption that legitimate web and email traffic uses to keep data secure. To determine whether this traffic is benign or malicious, enterprises should decrypt SSL traffic for security inspection.

The FormBook malware family uses SSL to pull down its second stage. Our sandbox can extract session keys from memory to decrypt SSL traffic so there's no need to use a meddler in the middle (MitM) to get this information.

In addition to monitoring SSL communications on the network, it's a good idea to check for malicious network activity in SSL tunnels. This technique is also useful for detection within malware sandboxing environments.

Growth in Cryptominer Traffic

Sifting through network traffic can help us identify trends in malware activity. Figure 8 shows how, by reviewing 647 million signature triggers, we were able to identify the distribution trend of different malware categories during each month in 2022.

There is one particularly notable point from the trend graph, which shows that cryptominer traffic has increased dramatically since April 2022. Within the subset of customers who have both a Cortex Data Lake (CDL) license and Threat Prevention license, 45% of sampled organizations had a signature trigger history that contains cryptominer-related traffic.

95.5% of the cryptominer traffic came from XMRig miners attempting to log in to its mining pool. This traffic includes both XMRig variants and malware incorporating XMRig.

Because XMRig is open-source software, its source code is publicly available. This makes it easy for malware authors to modify and integrate into their own code. XMRig is available on a variety of platforms including Windows, Linux and macOS. It can be customized to mine a variety of different cryptocurrencies and can be configured to use different mining algorithms and pools.

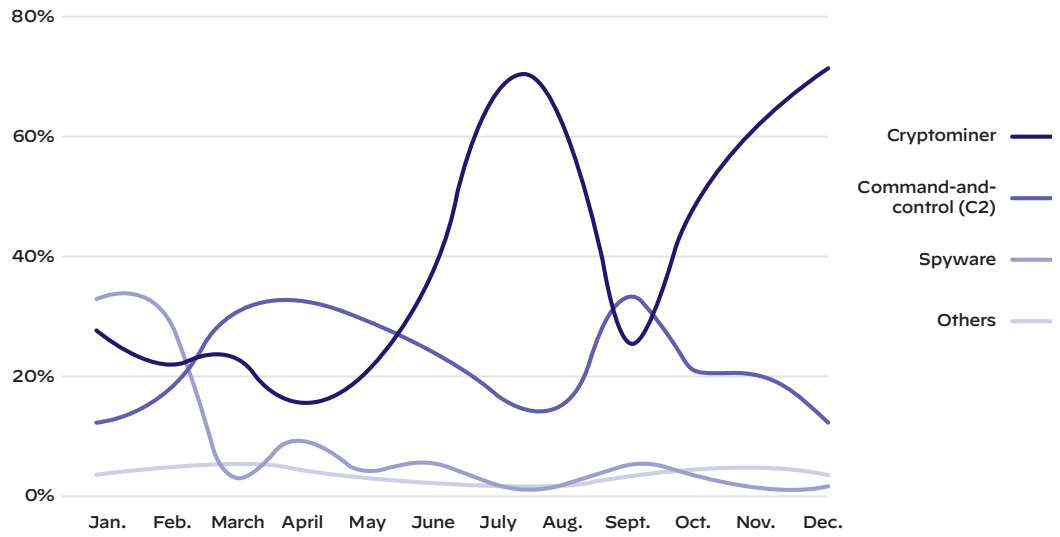


Figure 8. C2 traffic category distribution

Malware Predictions in 2023

Our goal for analyzing data gathered in 2022 is to thwart not just today's attacks, but to gain insights that could help us be better prepared to fight attacks in the future. We've identified some predictions and trends that organizations should consider as they re-evaluate their security approach in 2023 and beyond.

Evasive Threats will Continue to Become Increasingly Complex

While attackers' continued use of old vulnerabilities shows that they will reuse code as long as it proves lucrative, there comes a point where creating newer, more complex attack techniques is necessary. When basic evasions became popular and security vendors started detecting them, attackers responded by moving toward more advanced techniques. Of course, security vendors will continue to respond with improved protections, and thus the cycle repeats.

Encrypted Malware in Traffic will Keep Increasing

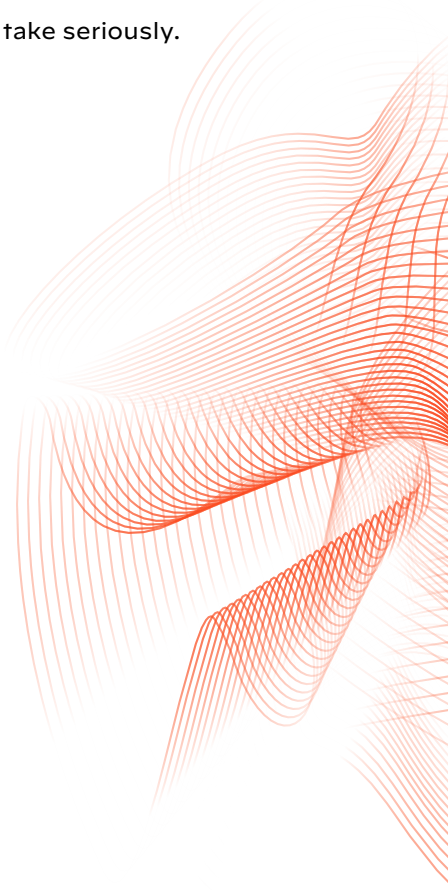
As threat actors adopt more tactics that mimic those of legitimate businesses, we expect that more malware families will use SSL encrypted traffic to blend in with benign network traffic. At this point, 12.91% of malware traffic is already SSL encrypted, and we anticipate more threat actors will see the benefit of using this popular protocol.

Spreading Malware through Vulnerabilities will Continue to Increase

The number of new vulnerabilities being discovered increases every year, giving attackers more motivation to pursue these opportunities to exploit potentially unpatched systems. It gets progressively harder to mitigate all of these new vulnerabilities in time, for a variety of reasons. This only makes the target of vulnerable systems more tempting to attackers.

Cryptominers/Coinminers

Cryptominer traffic is on the rise. This leads us to believe that cryptomining continues to be an area of interest to threat actors. Whether or not you use cryptocurrency, backdoor-like malware is something we all need to take seriously.



Conclusions and Takeaways

Malware is always becoming more complex and more evasive. Threat actors are always looking for new ways to make their spreading mechanisms more effective and impactful.

To this end, threat actors have been using traditional malware techniques to create a flood of new threats that take advantage of the public's growing interest in AI and ChatGPT. While we've not seen AI itself being used to create new threats, this flood illustrates that attackers don't yet find it necessary to go to such great lengths to trick potential victims when simple social engineering techniques will do just fine.

Similarly, malware hitting industries using operational technologies (OT) have largely been traditional, non-targeted malware rather than threats attacking OT specifically. While the ratio of targeted attacks on OT has grown, it is still a very small percentage of overall traffic.

Organizations must simultaneously guard against new, sophisticated attacks as well as the malware built to exploit old vulnerabilities. In this constant race between attackers and defenders, security practitioners need to find new ways to stay ahead.

Security defenders who can keep up with these trends have an advantage in making their environment a less tempting target. It's imperative organizations reassess their security strategy, deploy the right tools and ensure they are following best practices.

Here are some key considerations as you assess your security posture:

Take a Holistic View of Your Environment

Taking a holistic view of the security of your environment gives you comprehensive oversight of your network, endpoints and cloud (whether public, hybrid or on-premises). This means ensuring you're properly using the security capabilities architected into all levels of your hybrid cloud environment (e.g., hardware, firmware, operating system or software), and securing the data itself at rest, in flight and in use.

Have a Process for Patching

Minimizing the impact of vulnerabilities requires keeping up with patches. Having a comprehensive process for quickly patching these newly discovered vulnerabilities and maintaining regular updates helps reduce the time enterprises are at risk for attack. This process should include annual audits to ensure enterprises keep up with regular maintenance.

Security Best Practices Are Everyone's Responsibility

Compliance, security operations and human resources should work hand in hand to ensure security best practices are being followed at every level of your organization. Within the security team, this means continuously assessing risk, working to educate your staff about emerging risk, and adopting the right tools to deliver efficiency and speed.

Decrypt SSL to Expose Potential Threats

Threat actors can use the SSL protocol to evade detection. By enabling decryption on your next-generation firewalls, security teams can inspect and control SSL/TLS and SSH traffic to detect and prevent threats that would otherwise remain hidden in encrypted traffic.

Using virtual machine introspection (VMI) to capture the symmetric keys for each SSL connection allows detection to happen in a way that is invisible to the malware.

Detect Newly Registered Domains

Threat actors favor NRDs for launching malicious campaigns. Academic and industry research reports have shown that NRDs are risky, as they're useful for a variety of problematic activities including phishing, malware and scams. Blocking and closely monitoring NRDs in enterprise traffic allows you to prevent this type of activity.

For Palo Alto Networks customers, we recommend blocking access to NRDs with Advanced URL Filtering and DNS Security. If access to NRDs is allowed, then alerts should be set up for additional visibility.

We define NRDs as any domain that has been registered or had a change in ownership within the last 32 days. Our own analysis has indicated that the first 32 days is the optimal time frame for identifying NRDs to be detected as malicious.

Detect Phishing in PDF Files

It is important to detect both malicious and phishing PDF files. In addition to traditional detection approaches, like signature-based detection and malicious URL labeling, machine learning models can protect against rapidly changing PDF phishing campaigns.

Simplify and Consolidate Vendor Relationships

The complexity of managing vendors and point solutions can create security gaps. Security teams should work toward consolidating their vendor environments and pursuing platforms that are comprehensive and scalable.

Adopt a Zero Trust Mindset

At its core, Zero Trust seeks to eliminate implicit trust throughout the enterprise by continuously validating all digital transactions. This is inherently a much more secure approach and helps deal with some of the most sophisticated and dangerous types of threats. Organizations can evolve into a Zero Trust enterprise by applying Zero Trust best practices comprehensively across users, applications and infrastructure.

A Zero Trust deployment should focus on implementing controls across the entire organization – on-premises, in the data center and in cloud environments – to maximize security efficacy and keep your organization safe. Organizations should re-evaluate legacy virtual private server (VPS) solutions for ways to reduce the attack surface on today's cloud-first business operations.

Educate Your Staff

Despite the work security teams do to strengthen their security posture, human activity will continue to pose risk. Inform employees of the tactics attackers are using in phishing schemes and threats posed by email attachments, even if it appears at first glance to be from a trusted source.

Continually reinforce the need for using secure networks. Your organization can reduce its risk by improving security awareness for all employees through regular training and updates on emerging phishing tactics.

Palo Alto Networks Can Help

Throughout this report, we've discussed a variety of ways the malware landscape is changing. We deliver reports like this to better inform and equip you with information to protect your organization. The more you know about your adversaries, the better you can defend your organizations from attacks.

Palo Alto Networks has a range of solutions that do the heavy lifting of putting many of the techniques we've discussed into practice. Our complete solutions detect and prevent attacks from both known and unknown threats, inline or in the cloud and at scale, so your business is protected, but does not slow down.

The Palo Alto Networks Cloud-Delivered Security Services bring the network effect of thousands of customers across various security technologies to coordinate intelligence and provide consistent protection across all attack vectors. Deployed across our range of machine learning-powered Next-Generation Firewalls – hardware PA-Series, software VM-Series and CN-Series, and cloud-delivered Prisma Access along with Cloud-Delivered Security Services – our services help eliminate coverage gaps.

Advanced WildFire malware prevention service is natively integrated into all Palo Alto Networks products and blocks activity associated with known and unknown malware variants as well as other file-based threats. Advanced Threat Prevention leverages the firewall's visibility to inspect all traffic and automatically prevent known exploits, malware and spyware regardless of port, protocol or SSL encryption.

The Palo Alto Networks Cortex platform provides the visibility and tools to cohesively protect against threats coming from the network, from firewalls to an XDR endpoint solution. This eliminates the risks of siloing aspects of security operations and gaps between security tools to better guard against threats.

Cortex Xpanse helps you track known and unknown assets in your organization. Our attack surface management solution continuously builds and updates a record of all internet-connected assets, helping identify all exposure risks. Dive deeper and read the Cortex Xpanse Attack Surface Threat report.

The Palo Alto Network Prisma SASE platform secures your hybrid workforce with the superior security of Zero Trust Network Access 2.0 while providing exceptional user experiences from a unified, cloud-native security product. Protect all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach.

The Palo Alto Networks Prisma Cloud enables security and DevOps teams to effectively collaborate to accelerate secure cloud-native application delivery from Code to Cloud. The platform delivers continuous visibility and threat prevention throughout the application lifecycle across multicloud environments.

With code to cloud coverage that encompasses software, infrastructure, workloads, data, networks, web applications, identity and API security, Prisma Cloud addresses your security needs at every step in your cloud journey. With over 10 billion cloud assets secured and over 1 trillion cloud events processed daily, you can trust Prisma Cloud to protect your cloud at any scale.

We are here to help. Learn more about how we can help protect your business at **www.paloaltonetworks.com**

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably's Best Companies for Diversity (2021), and HRC's Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

About Unit 42

Palo Alto Networks Unit 42 brings together world-renowned threat researchers, elite incident responders and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster. Visit paloaltonetworks.com/unit42.

paloalto® NETWORKS | UNIT 42™ BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

www.paloaltonetworks.com