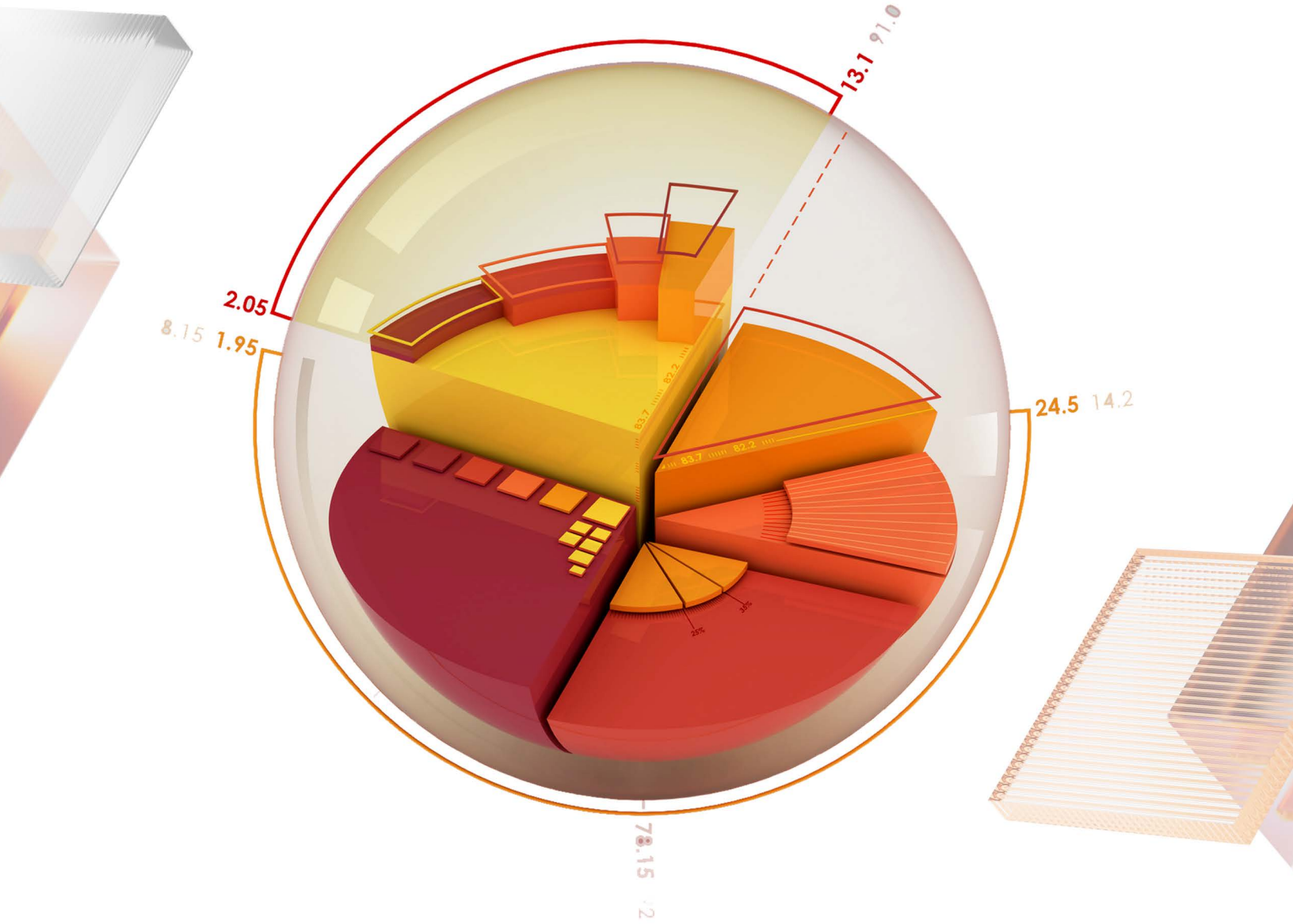
SONICWALL® | telecomservices SOLUTIONS INFORMATIQUES

2025 CYBER THREAT REPORT

THE NEED FOR SPEED AND STRONG ALLIES TO OVERCOME THE CYBERSECURITY BATTLEFIELD



Letter from CEO, Bob VanKirk

Together, we are facing a rapidly changing and increasingly complex threat landscape. The adversaries we face are both relentless and ever evolving, and our partners and customers turn to SonicWall for trusted protection. As we start a new year, I would like to take a quick moment to acknowledge the vital partnerships that are instrumental in our collective efforts to defend against cyber threats and ensure a secure future for all. By protecting systems and networks, we contribute to the safety of entire communities, ensuring that individuals and organizations can thrive without the fear of cyber threats. What an honor it is to do this together with all of you.

The stakes have never been higher, with threat actors employing more sophisticated and relentless tactics than ever before. SonicWall's data indicates that threat actors are moving at unprecedented speeds. We see the majority of hackers exploiting vulnerabilities within just two days after a working example of the exploit is made public. This urgency puts immense pressure on companies of all sizes, especially small and medium-sized businesses (SMBs), which may struggle to keep up.

In 2024, we witnessed alarming trends that underscore the urgent need for proactive defense strategies. Cyberattacks continue to advance and diversify, and critical network attacks could have led to a staggering minimum of 68 days of downtime, representing 19% of potential revenue at risk.

The United States (U.S.) healthcare sector faced unprecedented challenges, with over 198 million American patients impacted by ransomware. Exploitation often occurred alarmingly quickly, and our data identified 210,258 never-before-seen malware variants, averaging 637 new threats daily. This suggests that threat actors are continuously creating new variants, likely attributed to the rapid adoption and advancements of artificial intelligence (AI) tools, to enhance their success.

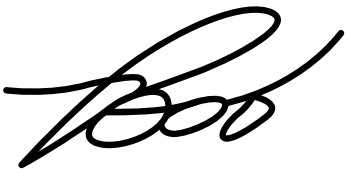
Given this landscape, it is essential for SMBs and businesses of all sizes to understand that they should not go it alone in the fight against cybercrime. Partnering with managed service providers (MSPs) and managed security service providers (MSSPs) is crucial for bolstering defenses. MSPs and MSSPs, in turn, should seek vendors that offer security operations center (SOC) services and 24/7/365 monitoring to ensure comprehensive protection.

Today, I am proud to introduce the 2025 SonicWall Annual Threat Report, a breakdown that captures the evolving nature of cyber threats over the past year. This report is not only a testament to our commitment to understanding the security landscape but also a vital resource to empower you, our partners, and customers, in protecting your organizations and start meaningful conversations about the critical nature of security in today's marketplace.

This year's report not only details these concerning statistics but more importantly, provides actionable insights designed to help develop and implement effective defensive strategies. We've also incorporated valuable perspectives from our 24/7 SOC analysts, and market insights from respected cybersecurity insurance providers.

I encourage all of our partners and customers to leverage this report as a strategic tool in your conversations with stakeholders and clients. The insights provided can help you articulate the importance of cybersecurity measures and the necessary steps to protect your organizations against the threats we face. Together, we can fortify our defenses and adapt to this dynamic threat landscape. Your feedback has been invaluable in shaping our efforts, and we remain committed to supporting you with the resources you need to secure your environments effectively.

On behalf of the entire SonicWall team, including our dedicated Capture Labs threat researchers, I am excited to share this vital look at the latest developments in cybersecurity and how we can navigate these challenges together.



Bob VanKirk
President & CEO
SonicWall

Executive Summary

THREAT LANDSCAPE

48 HOURS

61% of the time, hackers leverage new exploit code within 48 hours.

Organizations were saved from a potential 68 days of downtime in 2024.

68 DAYS

6B

Our sensors defended against over 6B critical network attacks, for the third consecutive year.

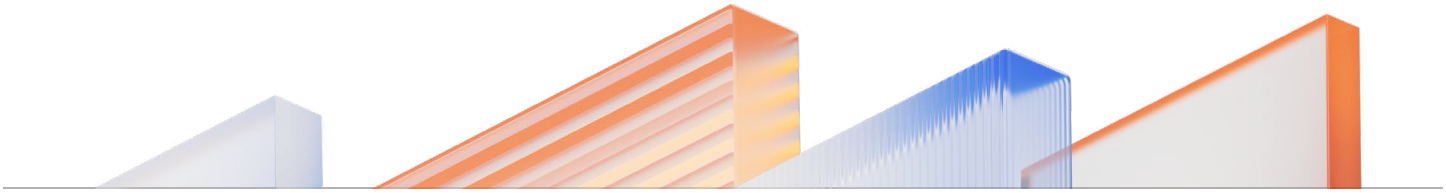
RANSOMWARE

Ransomware intensifies in North America (+8%) and explodes in LATAM (+259%).

▲259%

$850,700

Average Ransomware Cost: In 2024, the average ransomware payment reached $850,700, with total related losses often exceeding $4.91 million when factoring in downtime and recovery costs.



MALWARE

▲8%

Malware trended up 8% YoY, including a massive 92% spike in May alone.

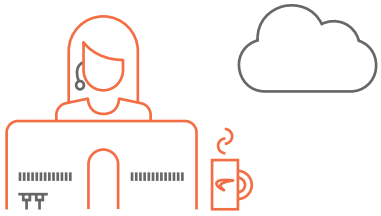
IoT AND ENCRYPTED

IoT attacks (+124%) and encrypted threats (+93%) continue to climb globally.

▲124%

SECURITY OPERATION CENTER (SOC)

85%



Identity, cloud, and credential compromise account for 85% of actionable alerts.

33% of reported cyber insurance events are BEC incidents - up from 9% YoY.

33%

RTDMI™

637

— NEW VARIANTS —

A DAY

SonicWall identified 210,258 'never-before-seen' malware variants – 637 a day.

The Escalation of Ransomware Attacks in 2024

In 2024, ransomware attacks continued to plague organizations across the globe, solidifying their place as one of the costliest threats in cybersecurity. Last year saw significant advancements in ransomware attacks with threat actors frequently utilizing double extortion as a tactic. There was a dramatic increase in attack volume in the Americas, with LATAM and NOAM increasing 259% and 8% respectively. And while ransomware certainly affected industries across the board, healthcare was hit particularly hard with major impacts and catastrophic consequences.

Double and Triple Extortion Is the New Normal

Double extortion was prolific throughout the year with triple extortion also rising, especially in the healthcare industry. This specific tactic involves encrypting an organization's most critical data while simultaneously threatening to release sensitive information unless demands are met. This tactic is used to place even more pressure on ransomware victims to pay the threat actors as the cybercriminals are essentially holding the data hostage in multiple different ways. And in the case of triple extortion in the healthcare industry, threat actors will even go to the patients themselves and threaten to release their data unless ransom is paid. The growing sophistication of ransomware tools, including AI and Ransomware-as-a-Service (RaaS), has made these multi-front attacks much more accessible for even small-time threat actors.

Healthcare and Ransomware: An Unhealthy Relationship

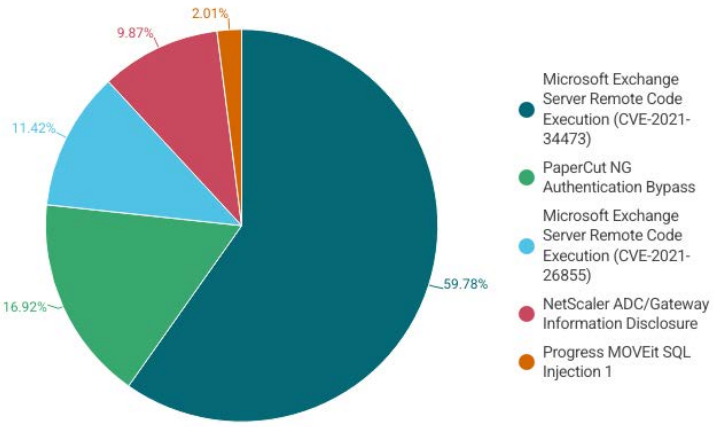
The healthcare sector was hit with an unparalleled surge in ransomware attacks in 2024 with more than **198 million** Americans impacted by breaches, including the Change Healthcare breach, which was one of the largest breaches in history affecting more than 100 million people.

Ransomware was far and away the biggest threat to the healthcare industry, utilized in **95%** of all breaches in this sector. Highly visible ransomware groups like LockBit and BlackCat (formerly ALPHV) leveraged Ransomware-as-a-Service (RaaS) models to carry out widespread attacks and take advantage of critical vulnerabilities to infiltrate systems. RaaS models have made more reliable ransomware software accessible to smaller, less advanced threat groups. Some of the most exploited vulnerabilities include:

- Microsoft Exchange Server flaws like ProxyShell and ProxyLogon, which accounted for 60% of exploited healthcare vulnerabilities
- The MOVEit SQL injection vulnerability (CVE-2023-34362) was responsible for many breaches, such as the attack on CareSource which affected over 3 million patients.

Most Exploited Healthcare CVEs

Top 5 vulnerabilities leveraged by ransomware groups in the healthcare sector



Operational Challenges

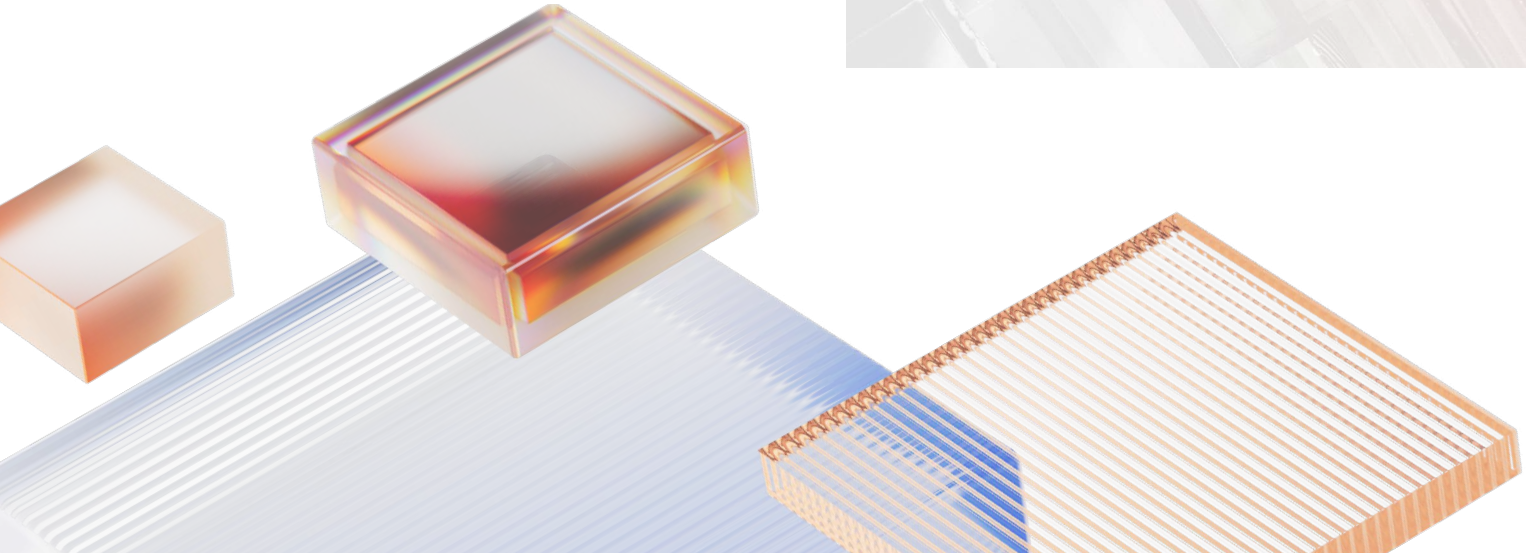
Not only were healthcare organizations heavily targeted by ransomware attackers - they were also among the least prepared to handle the fallout. The amount of time it takes to recover is reflective of the growing complexity of ransomware incidents across the board. In healthcare in particular, many organizations still function using legacy systems and many delay patching for far too long leaving themselves wide open to critical vulnerabilities. This perfect storm combines to make healthcare providers ill-equipped to counter sophisticated threats and ill-equipped to recover from them. which brings the total cost of an average attack to more than five times the average payment number, or $4.91 million.

SOC POV

Our Managed Security Services (MSS) team saw a 25% increase in ransomware over a 30-day period around the end of 2024 going into 2025 citing Fog ransomware, Akira and SafePay as the most active groups.

CYBER INSURANCE POV

In 2024, the average ransomware payment made to threat actors was $850,700, but that number doesn't begin to tell the entire story. Recovery costs have also skyrocketed, which brings the total cost of an average attack to more than five times the average payment number, or $4.91 million.



Staggering Spike in Business Email Compromise (BEC) Attacks

This year saw a significant increase in Business Email Compromise (BEC) attacks, furthering their position as one of the most widespread cyber threats. BEC attacks typically rely on deception and impersonation – two things that, when done correctly, can be very hard to identify. Nearly one-third of all reported cyber events were BEC attacks, up dramatically from only 9% in 2023.

Man-in-the-Middle and Credential Theft: Key Ingredients

Man-in-the-middle (MitM) attacks played a key part in BEC attacks, with threat actors leveraging compromised emails (typically obtained by credential theft) or other compromised communication channels to intercept messages or even manipulate internal communications. That's what makes these attacks so conniving and dangerous – they alter the perception of reality. An employee may believe they're communicating with somebody they work closely with – in reality, they could be dispersing pertinent information to a cybercriminal.

Vendor Email Compromise (VEC) Soars

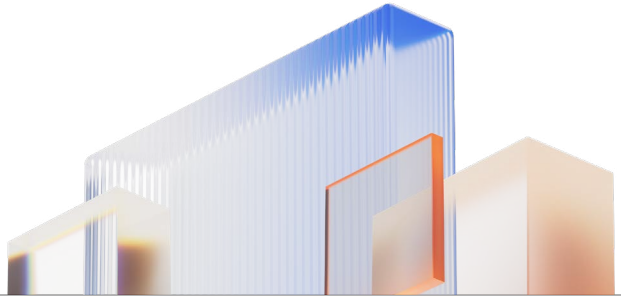
According to Abnormal Security, in the first half of 2024 VEC attacks spiked by 68% in the construction and engineering industry and 70% in the retail and consumer goods manufacturing industries. A VEC attack is very similar to a BEC attack. In a VEC attack, the threat actors impersonate or steal the credentials of a vendor and exploit the trusted relationship between the vendor and its many clients to steal from not just one, but multiple companies. Once an attacker worms their way into a vendor's systems, they can gain key information such as payment schedules, identities of decision makers, financial processes and much more. When the attackers have gained enough information, they strike, either impersonating invoices, fabricating a story to request urgent payment from large clients or using the information gained in some other malicious way.

CYBER INSURANCE POV

BEC Losses Bigger than CISA's Budget - In 2024, global losses from BEC attacks exceeded $2.95 billion. To put this into perspective, that's $150 million more than the entire budget for the Cybersecurity and Infrastructure Security Agency (CISA), which had a budget of $2.8 billion in 2024.

SOC POV

An industry-leading consulting firm recently observed a BEC attack targeting one of their high-ranking executives. The victim received an email from a trusted, but compromised account, containing a OneDrive link which redirected the employee to a fraudulent Microsoft login page designed to steal their credentials. Once compromised, the attacker gained access to the executive's email and propagated the scam by sharing their contact list via an external file share.



The Speed of Threat Actors

An analysis of major vulnerabilities exploited in the wild shows that most attacks begin within 48 hours of proof-of-concept (PoC) disclosure. This trend is supported by Google's Threat Analysis Group, which reports that many vulnerabilities are exploited just days after being made public.

These attacks regularly target flaws in Microsoft Exchange, IoT devices and third-party software like MOVEit. Advanced Ransomware-as-a-Service (RaaS) operations have streamlined the exploitation of these vulnerabilities. Groups like LockBit and BlackCat are known for their rapid response to new security weaknesses.

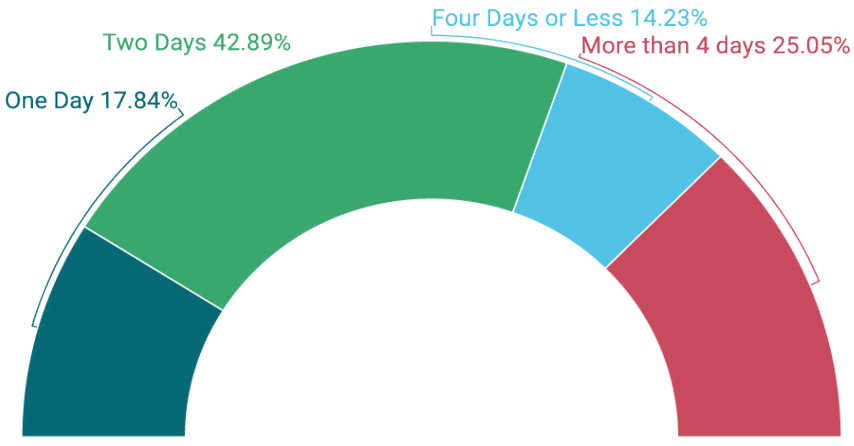
LockBit, for example, quickly exploited CVE-2024-27198 (JetBrains TeamCity Authentication Bypass), launching ransomware attacks within 24 hours of the vulnerability's disclosure. Similarly, the Cl0p ransomware gang leveraged a critical flaw in another file transfer product to breach 66 companies and issue ransom demands within a mere 48 hours of the PoC disclosure.

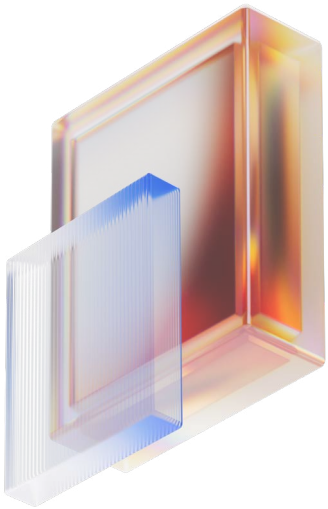
"As an MSP, we see firsthand how quickly cyber threats evolve. The speed at which threat actors utilize publicly available weaponized code — often within one to four days — reinforces the critical need for proactive security measures. The days of waiting weeks to patch vulnerabilities are over. Attackers have reduced their response time to hours, pointing to the need that businesses need an MSP that can proactively monitor, detect, and respond to emerging threats before they lead to costly breaches."

-PARTNER POV
FARZAD VAHID, FORNIDA

Time of Threat Actor Exploitation

How fast hackers leverage exploit code





Living Off the Land Binaries (LOLBins): No Laughing Matter

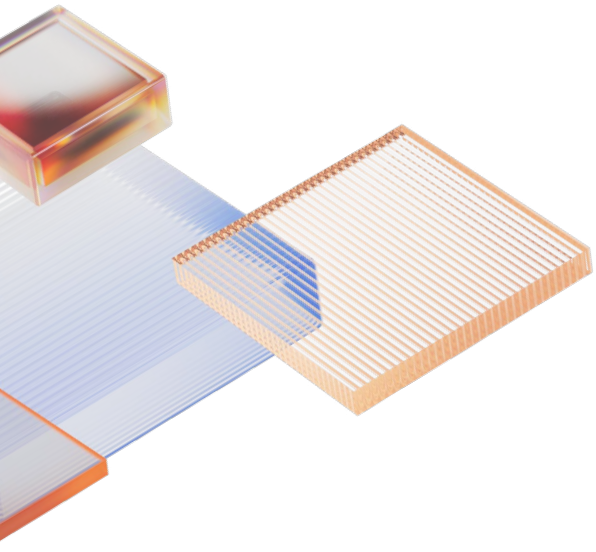
Living Off the Land Binaries (LOLBins) refers to programs included in your operating system that have legitimate, helpful uses that keep your computer running. Imagine you're at home and want to fix something using tools you already have lying around instead of buying new ones. Cybercriminals sometimes do something similar when they attack computers—they use tools and programs already built into your computer instead of bringing their own hacking software. When an attacker uses one of these "clean" tools (binaries) for wrongdoing, it can trick security software because these are tools that are supposed to be running on your computer on any given day. Blocking or disabling these tools will most likely impair the functionality of your operating system.

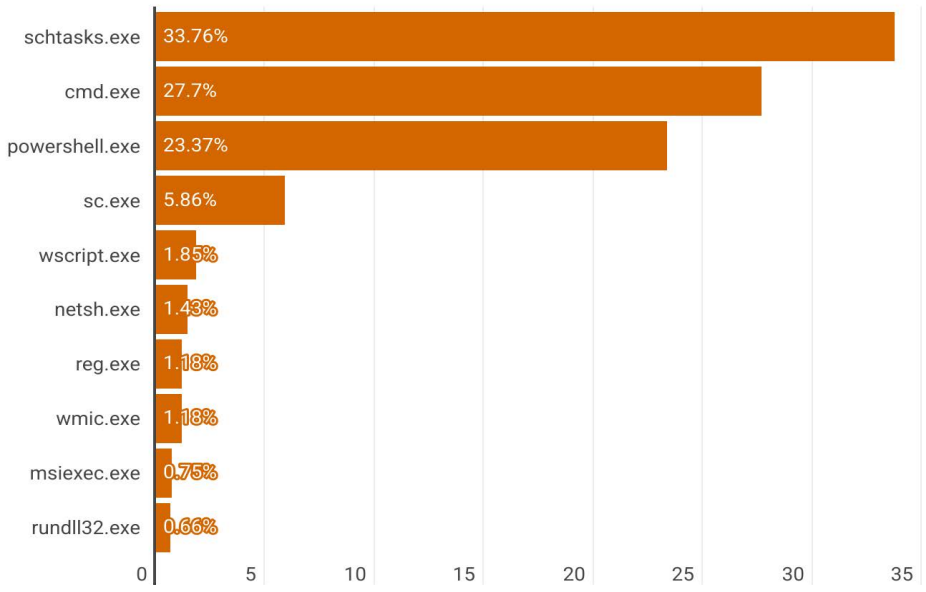
Threat actors leverage these tools for lateral movement and privilege escalation within compromised networks. For example, CISA reports that LockBit and their affiliates frequently use tools, including PowerShell and batch scripts, for reconnaissance, credential hunting and privilege escalation. Similarly, Sygniav reports that BlackCat (ALPHV) has been observed using PowerShell techniques and tools like schtasks to move laterally and disable Windows Defender.

The adoption of LOLBins aligns with the broader trend of exploiting trusted infrastructure for malicious purposes, as seen in the rise of fileless malware. SonicWall's threat researchers identified schtasks.exe, cmd.exe, and powershell.exe as the most abused LOLBins, accounting for more than 80% of all identified cases.

Prevalence of Abused LOLBins

The graph highlights significant usage rates for certain binaries. Schtasks.exe was used in 34% of identified LOLBin abuse cases, allowing attackers to schedule tasks for persistence or malicious script execution. Cmd.exe accounted for 28% of cases, often exploited for command execution as part of broader fileless attacks. Powershell.exe, with a 23% prevalence, proved highly versatile, enabling sophisticated techniques like process injection and data exfiltration. Notably, the 2024 SonicWall Mid-Year Threat Report found that 90% of prevalent malware families leverage PowerShell in some way. Other binaries, including sc.exe, wscript.exe, and netsh.exe, showed lower but still concerning usage rates, indicating their exploitation in niche or targeted attack scenarios.





Common Use Cases in Cyberattacks

LOLBins are integral to fileless malware campaigns, where attackers utilize native system tools to avoid leaving traditional artifacts, thus evading detection by conventional signature-based solutions. For example:

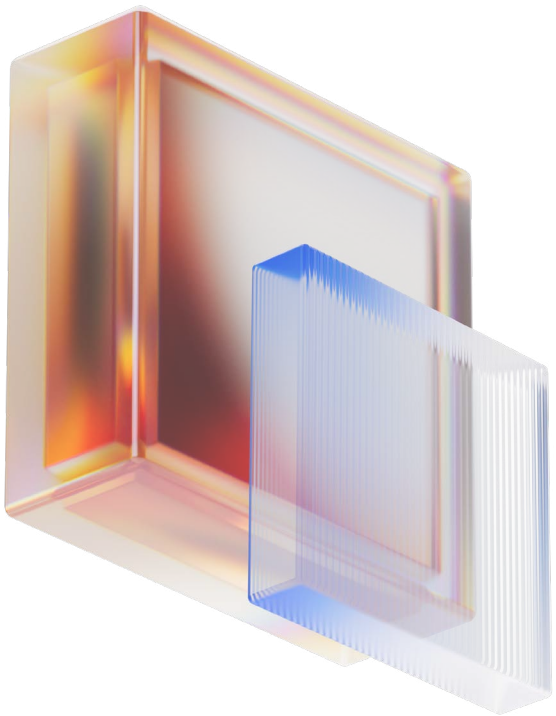
- **wscript.exe**: Commonly abused for running malicious scripts in phishing campaigns, allowing attackers to execute VBScript payloads covertly.
- **cmd.exe**: Extensively utilized by threat actors for executing commands directly on compromised systems, often serving as a gateway for broader command-and-control operations.
- **rundll32.exe**: This tool used to be one of the most widely utilized LOLBin by threat actors, and although it has fallen to a mere 0.66% prevalence as more effective methods for fileless malware have risen, it's still effective for loading malicious DLLs and evading sandbox detections.

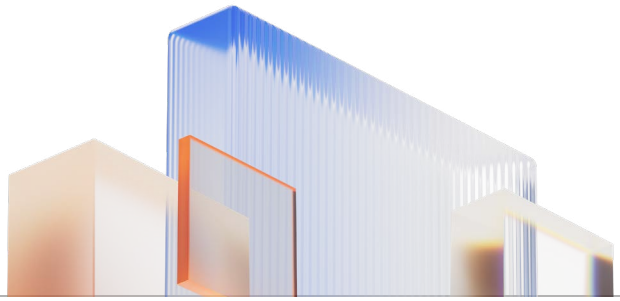
SOC POV

At a childcare facility, our Managed Security Services (MSS) team observed attackers exploiting a check-in kiosk as their initial entry point. The kiosk, an unpatched Windows machine with direct internet access, enabled them to execute lateral movement using pre-existing binaries. They then established persistence by embedding a hidden object within the Group Policy Editor.

AI POV

LOLBin abuse will likely persist as attackers evade detection by leveraging trusted system tools like PowerShell, cmd.exe, and schtasks.exe. As fileless malware and Zero Trust adoption grow, adversaries will refine these tactics to bypass security measures. Advanced threat hunting and behavioral monitoring are crucial to countering this trend. - Open AI, 2/5/25, v4.0

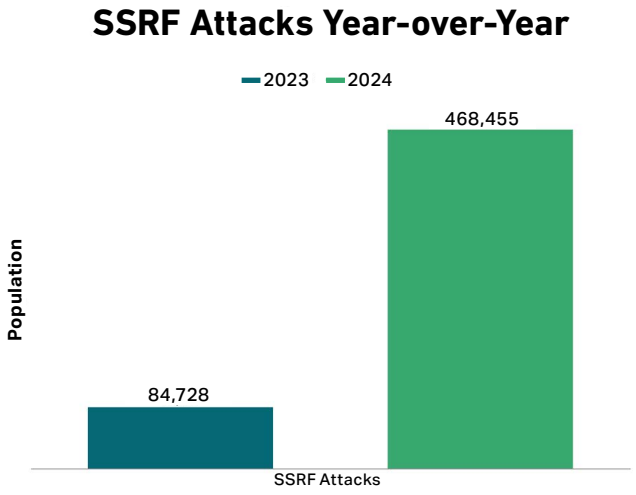




AI Automation Tools Lower Barrier for Entry While Increasing Attack Complexity

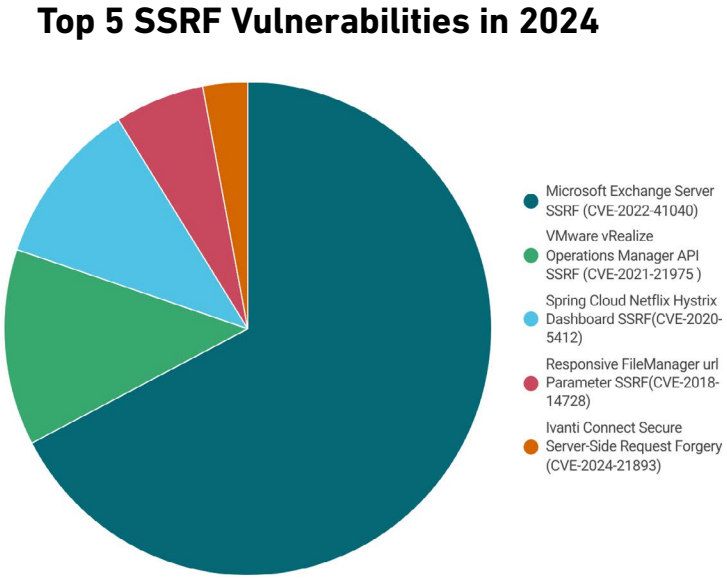
Server-Side Request Forgery (SSRF) attacks have long been a favored tool in cybercriminals' arsenals. In this type of attack, a threat actor essentially tricks the server into making a request to potentially sensitive internal services within an organization. In some attacks, they may also be able to force the server to access arbitrary external services, which could result in leaked sensitive data such as authorization credentials. Traditionally an SSRF attack would require substantial expertise in identifying vulnerabilities, crafting payloads and navigating the complexities of various server configurations. The introduction of AI-powered tools, particularly those leveraging natural language processing (NLP) and generative models, has reduced the technical barrier to entry. Some of the ways AI tools have lowered the barrier for entry with these attacks include:

- **Locating Unpatched Systems**: AI-powered scanners identify legacy systems with unpatched SSRF vulnerabilities, even in large, complex infrastructures.
- **Automating Exploit Chaining**: AI streamlines the process of chaining SSRF with other vulnerabilities, creating automated workflows for privilege escalation and lateral movement.
- **Evading Detection**: AI enhances obfuscation techniques, making SSRF payloads harder for security solutions to detect.



SSRFs became a critical cybersecurity concern in 2024, marked by a dramatic 452% increase compared to 2023. The increasing use of SSRF attacks in conjunction with other vulnerabilities such as privilege escalation and command injection has magnified the impact of SSRF attacks, allowing threat actors to gain broader access and more deeply penetrate targets.

Older Threats Revitalized by AI



Some of the most widely used SSRF vulnerabilities weren't actually new. Attackers have utilized AI tools to breathe new life into exploiting older vulnerabilities that remain unpatched in many systems. Some examples include:

- **VMware vRealize Operations Manager API SSRF (CVE-2021-21975)**: This vulnerability allows attackers to access internal services through the vRealize Operations Manager API, leading to sensitive data exposure.
- **Microsoft Exchange Server SSRF (CVE-2022-41040)**: A significant flaw that enables attackers to exploit Microsoft Exchange servers, bypassing authentication and potentially leading to remote code execution.

- **Spring Cloud Netflix Hystrix Dashboard SSRF (CVE-2020-5412)**: A vulnerability in the Hystrix Dashboard was exploited to target internal services, exposing sensitive information.

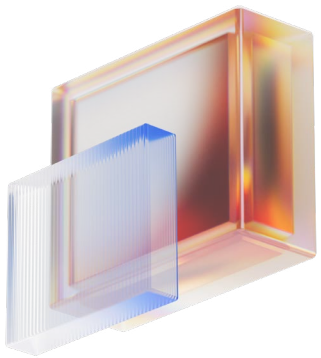
The continued use of these older SSRF vulnerabilities illustrates the persistent risks of delayed patch management, and the resurgence of older vulnerabilities on the backs of AI means that organizations need to continue worrying about these older vulnerabilities while simultaneously preparing for newer threats.

Business Email Compromise

Before the rise of generative AI, threat actors needed to have a specialized skillset including mimicking company writing styles, crafting highly contextualized phishing emails, and knowing how to avoid tripping the wires on traditional security systems while carrying out their attacks. AI tools can now do all of this for the threat actors at a high level, meaning that any threat actor who knows how to craft an AI prompt can now conceivably carry out one of these attacks.

The Role of Generative AI in Open-Source Software (OSS) Security

Generative AI provides the benefit of accelerating coding and increasing accessibility and simultaneously may introduce vulnerabilities when not properly validated. Attackers can also utilize the same AI tools being used to accelerate coding for nefarious purposes, such as identifying and exploiting weaknesses in an organization's systems, which creates an even greater need for stricter code validation and review processes.

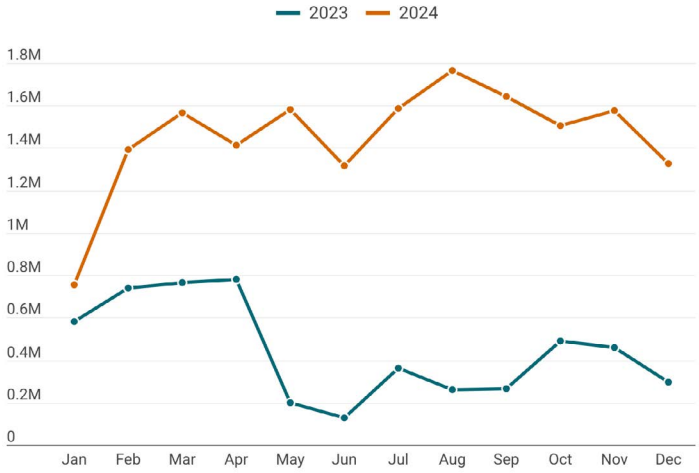


"We consistently see how AI is reshaping the cyber threat landscape, making it easier for attackers to exploit pre-existing vulnerabilities, automate sophisticated attacks, and bypass traditional defenses. The rapid rise of AI-powered SSRF attacks and BEC shows that businesses can no longer afford a reactive approach to security. Organizations need a proactive security partner who can detect and mitigate threats in real-time, strengthen defenses against AI-powered attacks, and ensure compliance with evolving security regulations to stay ahead of emerging risks."

-PARTNER POV
LUIS ALVAREZ, PRESIDENT & CEO, ALVAREZ TECHNOLOGIES

The Internet of Things (IoT) Continues to Expand – And So Do IoT Threats

IoT attacks targeting IP cameras became a major target for threat actors. In 2024 alone, SonicWall prevented more than 17 million attacks on IP cameras, ranging from 750,000 to 1.8 million attacks each month. Attackers are beginning to take note of the often-weak defenses of connected devices – specifically those used in government and critical infrastructure. These devices are left vulnerable to disruptive activities such as surveillance manipulation and Distributed Denial of Service (DDoS) attacks. IP cameras are often found in sensitive locations like government facilities and even polling locations, meaning the increase seen could have been at least partially attributed to the global 2024 elections. One of the most alarming IoT threat leveraged is the Hikvision IP Camera Command Injection (CVE-2021-36260) vulnerability, which allows threat actors to enter commands directly into the camera's systems, allowing them to take full control of the device.



IoT Botnet

The Reaper IoT Botnet takes advantage of flaws in IoT devices to take full control, and the threat actors then use the botnet to carry out large-scale attacks. Where other botnets rely on weaknesses such as bad passwords, Reaper focuses on vulnerabilities, increasing the threat level for IoT hardware.

These trends signal a shift from opportunistic attacks to more targeted operations designed to undermine surveillance, disrupt critical services or enable espionage.

Open-source Software (OSS)

Open-source software (OSS) has transformed software development enabling both innovation and cost-efficiency, especially for IoT devices. At the same time, when thousands of IoT devices all use the same OSS, it can leave the door open to catastrophic consequences when a vulnerability arises. SonicWall data shows that there are three OSS projects exploited more frequently than others which are all also leveraged in IoT devices.

- **PHP**: Vulnerabilities like CVE-2017-9841, CVE-2018-20062, and CVE-2024-4577 enable arbitrary code execution, presenting substantial risks.
- **Apache**: Known vulnerabilities such as Log4j CVE-2021-44228 facilitate remote code execution and data leakage.
- **OpenSSL**: Issues like Heartbleed (CVE-2014-0160) remain exploited due to their ability to expose sensitive data

AI POV

IoT attacks will continue to rise as more connected devices with weak security are deployed in critical sectors. Threat actors are shifting from opportunistic exploits to targeted attacks using botnets like Reaper and vulnerabilities in IP cameras and OSS components. Without stronger security frameworks, patch management, and threat monitoring, IoT devices will remain prime targets for cybercriminals. - OpenAI, 2/5/24, v4

Increasing Diversity in Attack Types: Cybercriminals Are Getting Creative

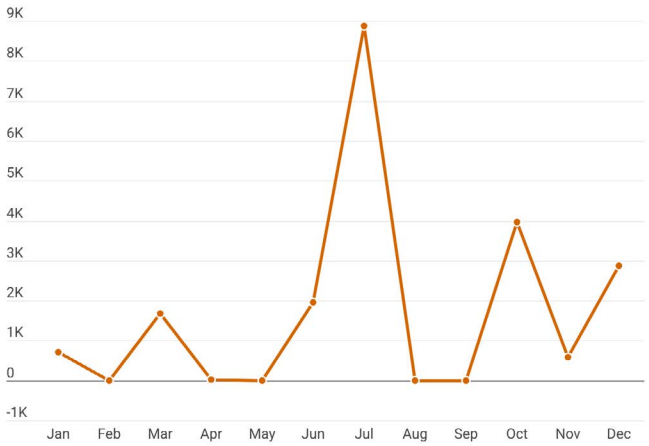
Cyberattacks are becoming more diverse as cybercriminals create new strategies and refine proven strategies to exploit vulnerabilities. The cost of a cyberattack is rising – and the cost isn't just financial. A cyberattack can cause long-term damage to reputations and have long-term consequences.

Strela Stealer Strategies Grow Alongside Malware

Strela Stealer was first detected in November 2022, and since then it has become one of the most persistent and dangerous threats in Europe. SonicWall Capture Labs saw consistent activity through 2024, with the biggest months being:

- **July and December**: Possibly linked to holiday and vacation periods, during which employees might be less available and resources stretched thin.
- **October**: This month signals the start of fiscal reporting for many companies, which means more sensitive information is being passed around, making it an ideal time for threat actors to strike.

StrelaStealer Unique Variants



Originally, threat actors were delivering Strela Stealer through JavaScript files in email attachments with a goal of obtaining email credentials from platforms like Microsoft Outlook and Mozilla Thunderbird. In 2024, the malware became more advanced by using better hiding techniques and targeting specific regions. It avoids attacking Russia while focusing on countries like Germany, Spain, Poland, and Italy, likely for geopolitical reasons. One way Strela Stealer evades detection is by checking the system's language settings and keyboard layout to determine if it's in a targeted country. This malware highlights how cybercriminals are not only improving their tools but also becoming more strategic in their attacks.

"Cybercriminals are becoming more strategic, combining new attack methods with proven tactics to exploit vulnerabilities. The cost of a cyberattack isn't just financial — it can permanently damage a company's reputation and disrupt operations. Businesses need a security partner that stays ahead of evolving threats, providing proactive protection, real-time monitoring, and strategic defenses to defend their most critical assets."

-PARTNER POV
JOSH SKEENS, CEO, LOGICALLY

AI POV

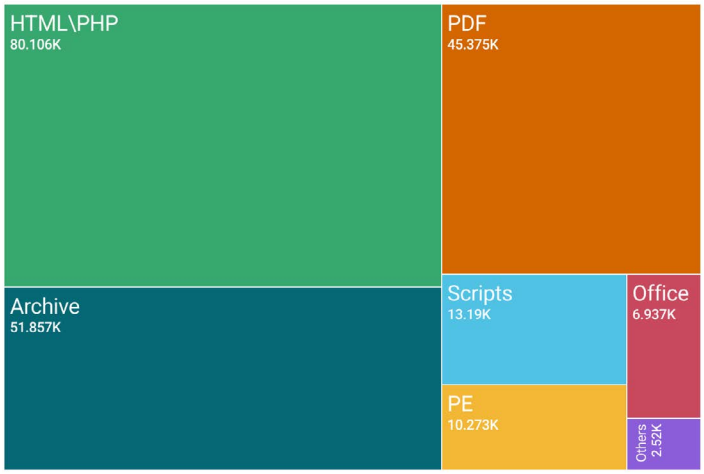
In 2024, the global average cost of a data breach reached $4.88 million, marking a 10% increase from the previous year—the largest annual rise since the pandemic." - OpenAI, 1/29/25, v4.0

The Hidden Risks in Everyday Life: PDFs, HTML Phishing, and Fake Mobile Apps

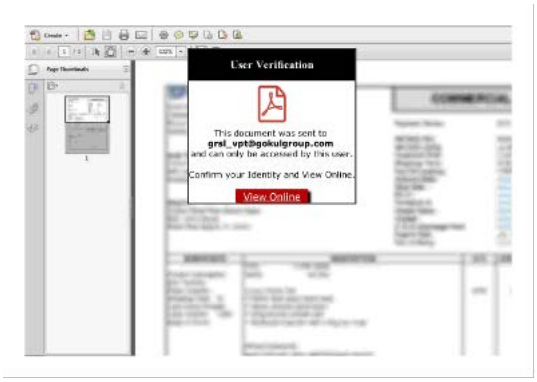
File-based attacks, specifically malicious PDFs and HTML phishing files, saw a major uptick. SonicWall data showed that 38% of malicious files detected were HTML-based with PDFs coming in closely behind at 22%.

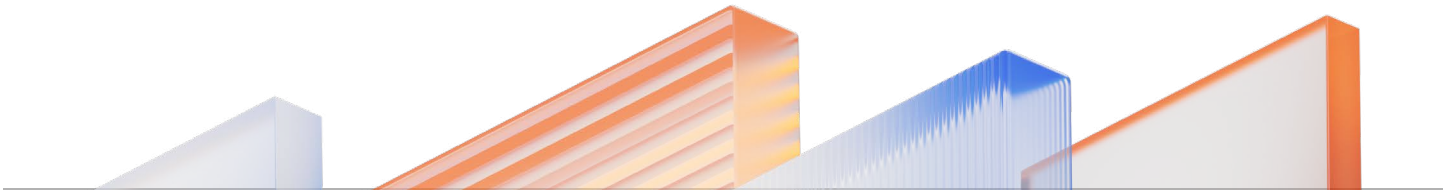
Files Used in Malicious Attacks

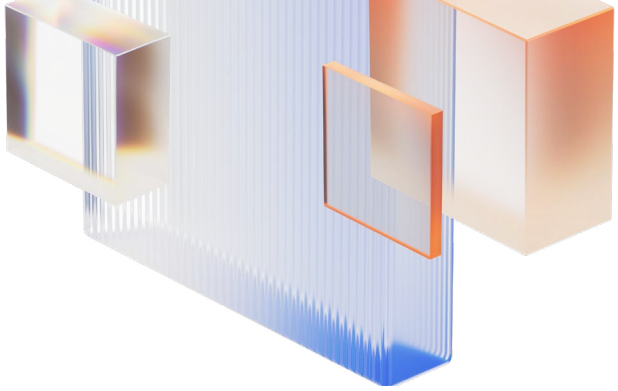
Breakdown of everyday files used by threat actors



Attackers use these types of files because it's easy for them to evade security systems enabling them to easily exploit the human element to steal sensitive information, such as credentials. Threat actors have been directing victims to phishing sites through embedded QR codes inside malicious PDFs. Once the victim scans the QR code, the victim is taken to what appears to be a legitimate login page. In reality, the information they enter will be sent back to the threat actors and used maliciously. This type of attack is often just the first. Once the attackers have a set of stolen credentials, they typically continue the attack by utilizing tactics like BEC, corporate espionage, and data theft.



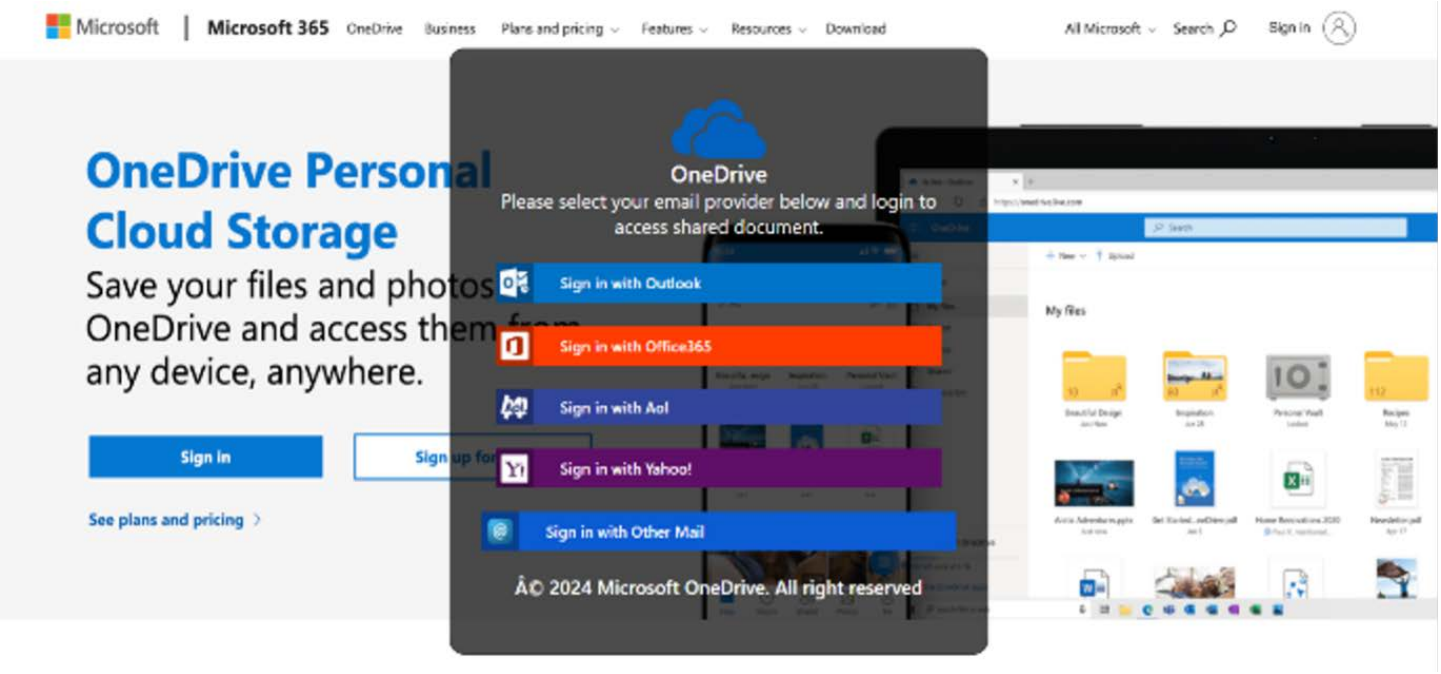




HTML phishing attacks grew by 10%, becoming a primary method for compromising user credentials. Some of the techniques threat actors use in HTML phishing include:

- **Form-Based Phishing**: HTML phishing pages often prefill the victim's email address to lend authenticity and prompt the user to enter their password.
- **Archive Delivery**: HTML files are commonly distributed within ZIP or RAR archives to bypass security measures and trigger user curiosity.

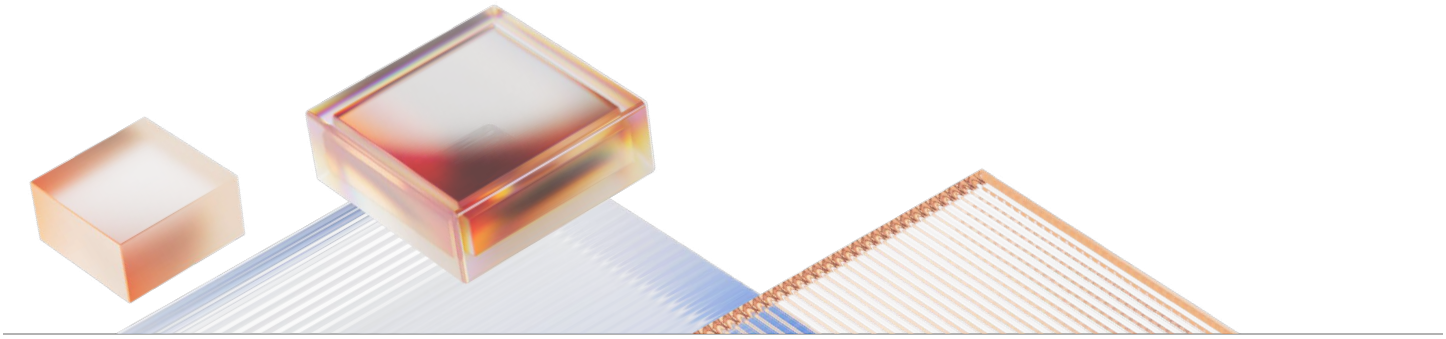
These are real-life examples:



Common Files, Uncommon Threats

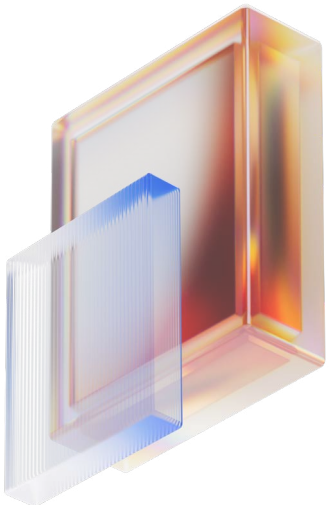
ZIP and RAR files containing malicious payloads have also become a common method for bypassing email filters. These threats work by distributing ransomware, trojans or remote access tools (RATs) to their unsuspecting targets. These methods have been used in recent high-profile attacks such as the Bumblebee Malware Loader which sent phishing emails with ZIP archives containing malicious LNK files to evade detection.

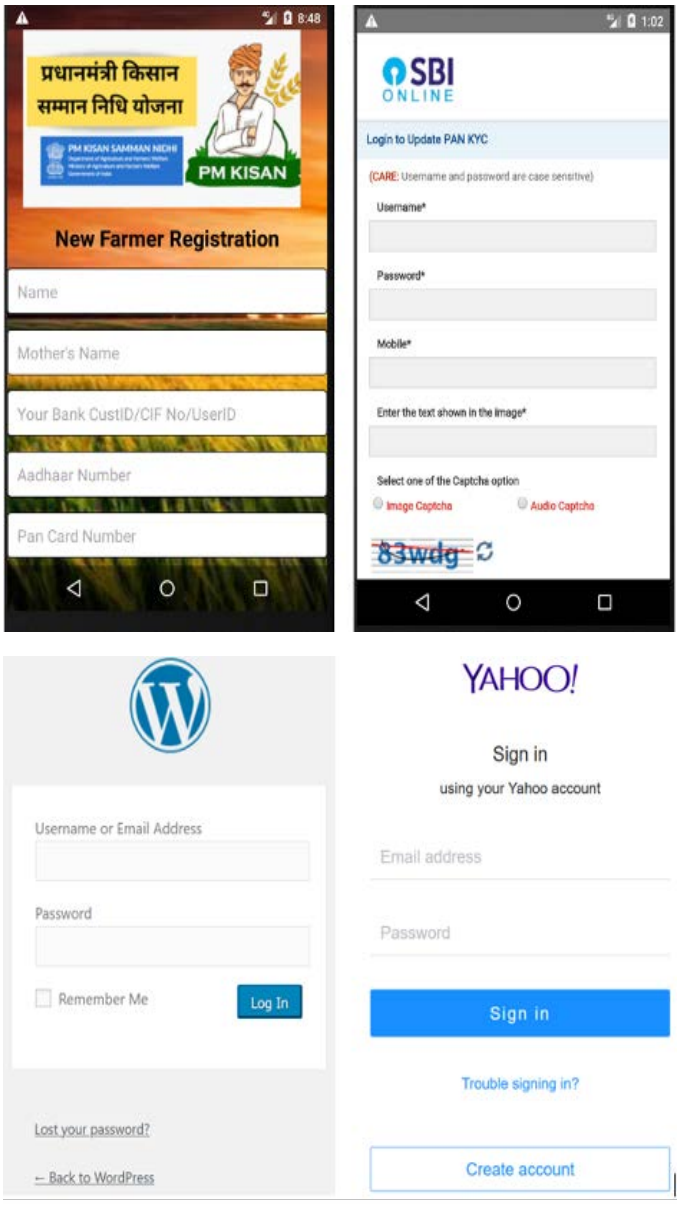
The increasing use of HTML, PDF and other file-based attacks is a first-rate example of the growing diversity and outright creativity threat actors are showing when creating these new attack methods. These attacks span multiple industries and businesses of all sizes. Packaging malicious payloads in seemingly ordinary or common files makes it much harder for traditional security methods to catch these attacks before damage is done.



Deceptive Android Apps: Exploiting Trust and Permissions for Mobile Fraud

Fake Android apps have become yet another serious cyber threat, particularly in the Asia-Pacific (APAC) region, where mobile fraud as a whole has surged. Threat actors in this region take advantage of the high density of Android smartphones and the general cultural trust in authority figures. The way these apps work is by requesting permissions from a user's device that aren't really necessary for the app to function, such as the ability to receive and read the device's text messages. Attackers utilize this to intercept one-time passwords (OTPs) and hijack user accounts. These apps will often pose as legitimate financial or government services. Combine this with the fact that they target victims with a lower digital literacy and it's easy to see how they're able to deceive victims into providing sensitive information.





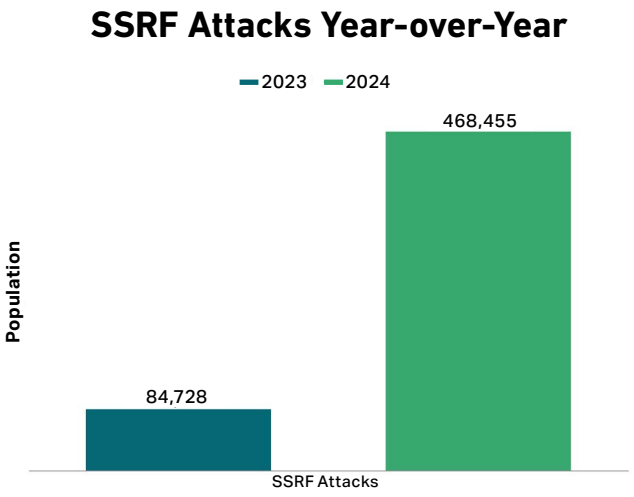
Threat Report Battle Cards

Problem

Without a zero-trust network, attackers can infiltrate one part of your system and use it to access sensitive internal information, even if it's stored elsewhere.

Context

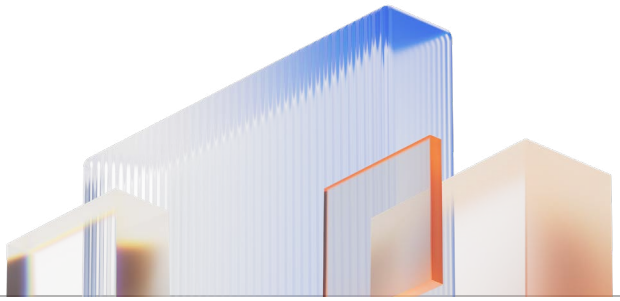
AI-driven automation tools have made SSRF attacks easier, allowing attackers to trick your server into requesting sensitive data. SSRF attacks increased by 452% in 2024.



How SonicWall Helps

SonicWall's Cloud Secure Edge (CSE) enforces zero-trust security by blocking unauthorized requests. It ensures servers cannot be tricked into trusting malicious requests, preventing attackers from accessing other parts of your network.

For more context, see page 11 of the 2025 SonicWall Cyber Threat Report.



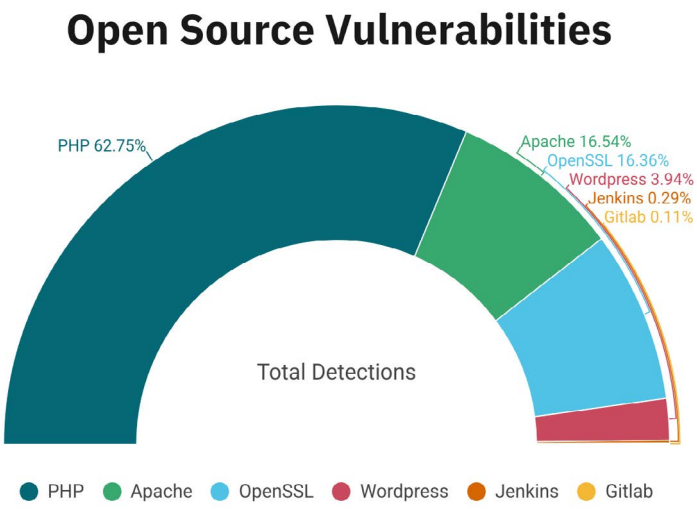
Open-source software has become an integral part of modern software. Our sensors have identified some of the most widely used open-source projects constantly under attack through older vulnerabilities. Ensuring to partner with an MSSP which can help monitor and perform regular patching is critical to securing your network.

Problem

Open-Source Software (OSS) such as PHP, OpenSSL and Log4j are deeply embedded in many development pipelines and often have a large number of vulnerabilities that go unnoticed and unpatched.

Context

Resource strain and the cybersecurity skills gap means many organizations don't have the people, processes and technology in place to patch in a timely manner.



How SonicWall Helps

SonicWall's SOC monitors your network 24/7, 365 days a year, making sure patching is done in a timely manner and monitoring your network for any and every threat.

For more context, see page 13 of the 2025 SonicWall Cyber Threat Report.

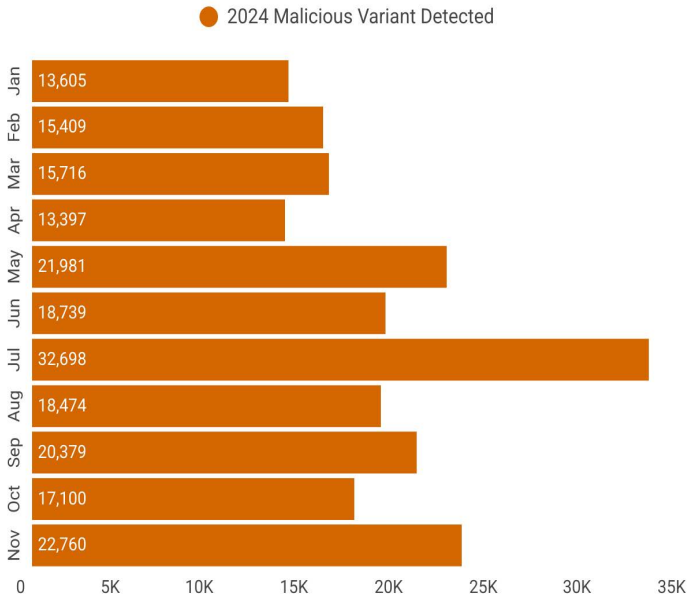
Problem

Threat actors are utilizing generative AI models to quickly produce never-before-seen file-based threats, which are harder to detect with traditional security methods, delivering malicious payloads through seemingly innocuous files.

Context

SonicWall's sandboxing solution detected 19,000 unique file-based threats per month in 2024, more than 200,000 unique variants in 2024 alone.

RTDMI Malicious Variants



How SonicWall Helps

SonicWall's Capture Advanced Threat Protection (ATP) is capable of seamlessly detecting never-before-seen threats, stopping them in their tracks before they do damage to your network, without interfering with your business.

Problem

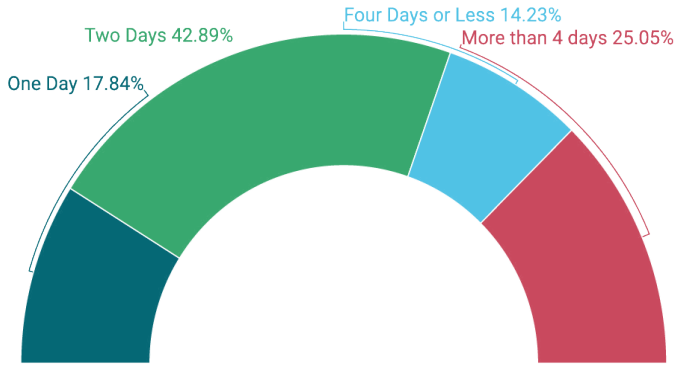
SonicWall's 2024 threat data shows that 75% of the time in-the-wild exploitation occurred within 96 hours of a proof of concept (PoC) being released.

Context

The speed of threat actors is increasing dramatically with the use of AI-automated tools and collaboration between threat actors.

Time of Threat Actor Exploitation

How fast hackers leverage new exploit code



How SonicWall Helps

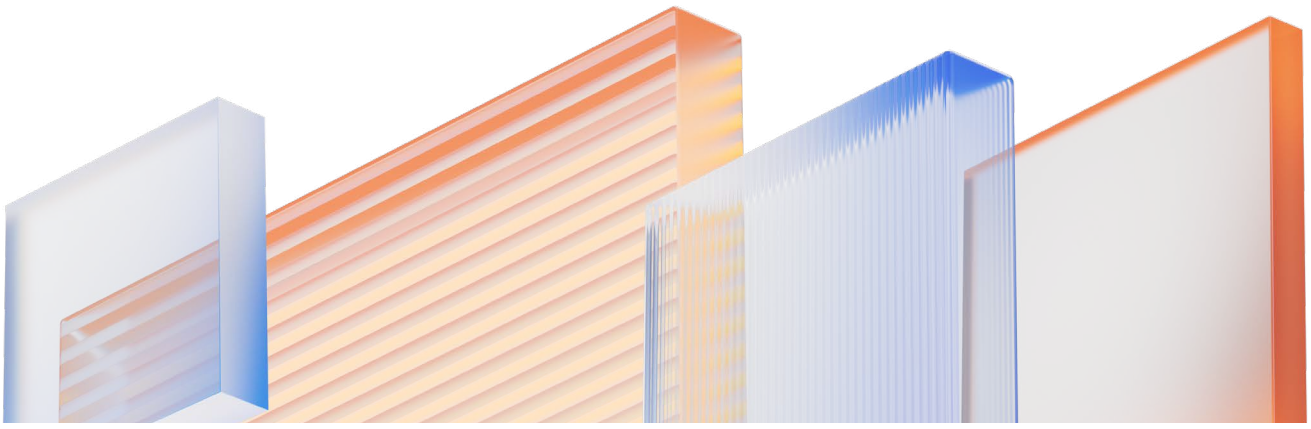
SonicWall's firewall is updated with the latest detections for publicly available exploit code within 24 hours on average, which has contributed to saving 68 days of downtime per organization in 2024.

For more context, see page 8 of the 2025 SonicWall Cyber Threat Report.

Challenges to Having an Effective Security Strategy

Understanding the challenges of maintaining good cybersecurity practices is essential for security partners, MSPs, and MSSPs. The evolving threat landscape requires organizations to adopt a proactive and layered approach to cybersecurity. Addressing these challenges involves real-time monitoring, rapid patch deployment, Zero Trust security models, and ongoing user education. By overcoming these challenges together, we can create a more secure environment for all.

1. **Rapid Exploitation of Vulnerabilities**: The speed at which threat actors are taking advantage of security gaps is faster than ever. 75% of the time, hackers started taking advantage of security weaknesses within four days or less after a demonstration of how to exploit them was made public. This puts immense pressure on security teams to identify and address vulnerabilities swiftly.
2. **Increasing Ransomware Threats and Recovery Costs**: Ransomware attacks remain one of the most damaging cyber threats. As an example, in the U.S. healthcare sector alone over 198 million individuals were impacted by breaches, with recovery costs exceeding $4.91 million per incident, highlighting the dangers of not having backup solutions and recovery plans.
3. **Human Error**: Mistakes made by individuals significantly impact cybersecurity posture. These missteps can unintentionally increase the risk of data breaches or unauthorized access.
4. **Surge in Business Email Compromise (BEC) Attacks**: BEC attacks have spiked, now accounting for one-third of all reported cyber insurance claims. Attackers are using sophisticated AI-driven techniques, making these scams harder to detect.
5. **Expanding Attack Surface from IoT Devices**: As the number of Internet-connected devices increases, it presents new security challenges. Attackers target these devices due to weak configurations.
6. **Rising Complexity of AI-Powered Cyberattacks**: The use of AI in cyberattacks has continued to climb. AI-driven attacks, including Server-Side Request Forgery (SSRF) attacks, saw a significant rise.
7. **File-Based Attack Methods and Malicious Automation**: Malicious phishing attacks, particularly through PDFs and HTML files, are on the rise. These often include deceptive links and QR codes, making them harder to detect.



Strategic Actions to Strengthen Your Cybersecurity Defense

The threat landscape continues to evolve at an unprecedented pace — leaving no organization immune. However, one constant remains: many of the attacks highlighted in this report can be prevented with strong cybersecurity hygiene. Taking proactive measures can greatly enhance your security posture, including:

Implement Real-Time Patch Management - Organizations with poor patch management hygiene are highly vulnerable to cyberattacks. By continuously scanning for and applying patches, businesses can prevent ransomware infections, data breaches, and system compromises before threat actors can take advantage of known weaknesses.

Adopt a Zero Trust Security Model - Threat actors leverage AI and automation to infiltrate networks. Security teams need to enforce strict access controls, assume no implicit trust, and validate every access request.

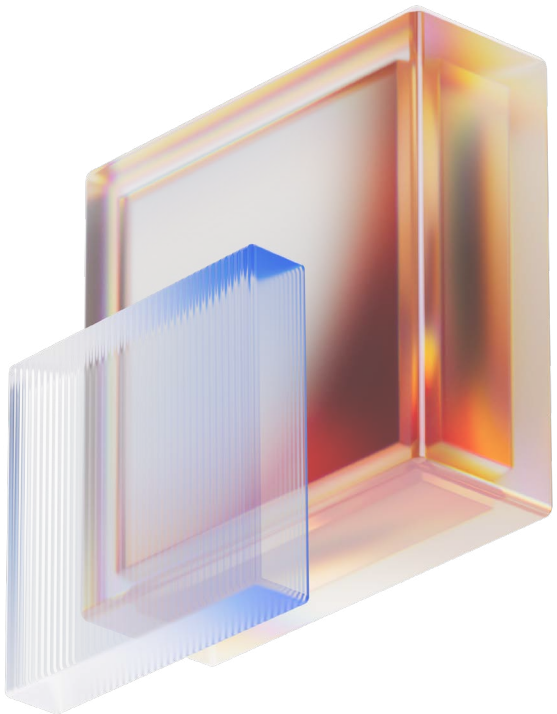
24/7 SOC Services for Real-Time Threat Protection – MSPs/MSSPs should partner with security vendors offering SOC services and 24/7/365 monitoring because cyber threats evolve rapidly, with attackers exploiting vulnerabilities within hours of discovery. Continuous monitoring ensures real-time threat detection, rapid incident response, minimized downtime, protecting clients from costly breaches and operational disruptions.

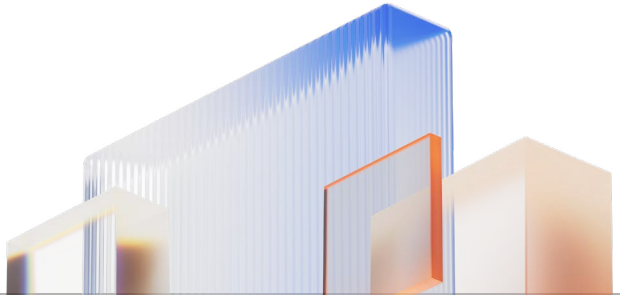
Enhance Ransomware Preparedness – Organizations are faced with the reality of preparing for catastrophic ransomware breaches. Implement regular backups, network segmentation, and endpoint detection & response (EDR) solutions.

Strengthen IoT Security - IoT attacks surged 124% in 2024. Secure IoT devices by changing default credentials, applying firmware updates, and restricting network access.

Monitor Cloud Environments and SaaS Applications - 78% of security alerts were tied to cloud-based threats. Enforce multi-factor authentication (MFA), CASB solutions, and least-privilege access policies.

Conduct Regular Cybersecurity Awareness Training - Human error remains a major attack vector. Regular training on phishing, social engineering, and credential hygiene can significantly reduce risk.





Key Takeaways

SOC PoV

- Ransomware attacks spiked 25% at the end of 2024, driven by aggressive activity from Fog Ransomware, Akira, and SafePay groups."
- A leading consulting firm faced a BEC attack where a compromised trusted account tricked a top executive into revealing credentials, allowing attackers to spread the scam through their contact list.
- Attackers exploited an unpatched, internet-facing check-in kiosk at a childcare facility, using it for lateral movement and establishing persistence via the Group Policy Editor.

AI PoV

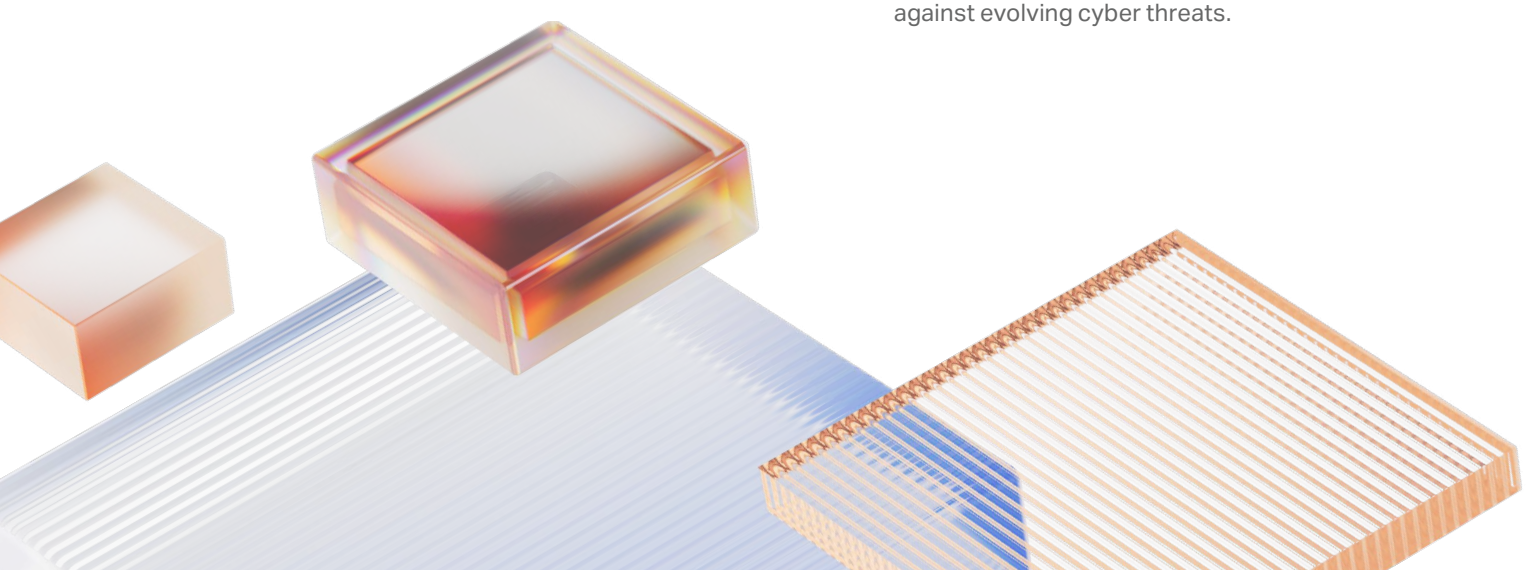
- Attackers are increasingly abusing trusted system tools like PowerShell and cmd.exe to evade detection, advanced threat hunting and behavioral monitoring are essential to counter LOLBin abuse.
- IoT devices with weak security flood critical sectors, targeted attacks using botnets like Reaper will surge, highlighting the urgent need for stronger security frameworks and proactive monitoring.
- The global average cost of a data breach surged to $4.88 million in 2024, marking the largest annual increase since the pandemic.

Cyber Insurance PoV

- The total cost of a ransomware attack averaged $4.91 million, over five times the average $850,700 ransom payment, due to soaring recovery expenses.
- Global BEC attack losses topped $2.95 billion — surpassing CISA's entire $2.8 billion annual budget by $150 million.

Partner PoV

- With threat actors exploiting vulnerabilities within days, businesses need an MSP that can proactively monitor, detect, and respond to threats before they escalate into costly breaches.
- AI-powered attacks like SSRF and BEC are accelerating, making proactive, real-time threat detection and defense essential for businesses to stay ahead of evolving risks.
- Businesses need a security partner that delivers proactive protection, real-time monitoring, and strategic defenses against evolving cyber threats.



SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

www.sonicwall.com

The SonicWall Threat Report could not be possible without the tireless efforts of the Capture Labs Team.

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and is recognized as a leading partner-first company. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real-time, SonicWall provides seamless protection against the most evasive cyberattacks across endless exposure points for increasingly remote, mobile and cloud-enabled users. With its own threat research center, SonicWall can quickly and economically provide purpose-built security solutions to enable any organization—enterprise, government agencies and SMBs—around the world. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035

As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.