breathetechnology
support | cloud | security | infrastructure | comms

EMPOWERING BUSINESS THROUGH SECURE TECHNOLOGY

SONICWALL®

2024 SONICWALL CYBER THREAT REPORT

NAVIGATING THE RELENTLESS SURGE IN CYBERCRIME

CERTIFIED ISO 9001:2015 COMPANY

CERTIFIED ISO 27001:2013 COMPANY

bcs Chartered IT Professional

Chartered Institute of Information Security

CISP

National Cyber Security Centre

CYBER ESSENTIALS

CYBERCOMPANIES.COM TOP CYBERSECURITY CONSULTING COMPANIES in 2023

INTRODUCTION

A NOTE FROM OUR CEO

Almost 18 months ago, we kicked off our outside-in approach across all of SonicWall, with the focus on truly understanding the needs and pain points of our partners and customers and using that insight to drive the delivery of our products and services.

2023 was a significant year that started to show the results of that approach. We added Solutions Granted, a leading Managed Security Services Provider (MSSP), serving more than a thousand Managed Service Providers (MSPs) across North America. And we doubled down on our cloud-security platform for the modern, remote workforce with our acquisition of Banyan Security, which added SSE solutions, including Zero Trust Network Access (ZTNA), to SonicWall's growing portfolio.

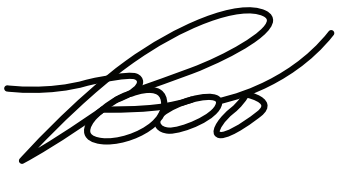
These strategic moves empower our MSP partners to offer their customers 24x7x365 protection with a team of threat analysts and experts, without the expense of assembling their own in-house SOC. We also extended SonicWall's portfolio to the cloud and provided partners and their customers with more flexibility, which will be key to the continued development of SonicWall's cybersecurity platform.

Customers should expect to see a growing number of managed security offerings from firewalls to cloud security as the SonicWall platform expands. But as the SonicWall 2024 Cyber Threat Report shows, threat actors are relentless, adding new tactics and spreading to every corner of today's growing attack surface.

With malicious intrusions up 6%, malware up 11% and cryptojacking up 659%, the odds that any given organization will be targeted are skyrocketing.

In this volatile environment, yesterday's safeguards are no longer enough: Businesses of all sizes need proven solutions and proactive strategies based on the most up-to-date threat intelligence.

That's why SonicWall continues to publish the SonicWall Cyber Threat Report: to provide threat intelligence to not only offer actionable insight, but to drive our roadmap and build solutions that help our partners. On behalf of our network of trusted partners and the entire SonicWall team, including our Capture Labs threat researchers, we're excited to share this exclusive look at the evolving cybersecurity landscape.



Bob VanKirk
President & CEO
SonicWall

A NOTE FROM BREATHE'S MD

"Our customers value their cyber security more than ever. Everyone has become aware of the high levels of Cyber-attacks against schools, public sector and businesses. Schools and small to medium businesses being the most affected.

The national Cyber Centre that advises all government departments including the department for education (DFE) and is constantly communicating and doing their best to educate us on the risks.

Their advice for small to medium business is second to none. Gone are the days of criminals running into banks with tommy guns. It's much easier to hold a school or business at ransom after a Cyber attack and data theft or to empty someone's bank account from the comfort of a desk. Less octane filled operations, but very effective. As the use of cloud services rose after the pandemic lock downs and our ways of working changed for ever, so did Cyber Crime.

It would be ignorant to think that we will not experience a data breach, account compromise, phishing attack or even a full network compromise at some point.

It's your duty to:

- Protect yourself. Have your systems and processes reviewed or audited. Understand what the risks are, the latest threats, and the best proactive and mitigation measures.
- Have the minimum security baseline in place in order to protect your staff, your students or customers, your data, and your systems.
- Someone with the right experience needs to assume the CISO (Chief Information Officer) and DPO roles. You cannot manage cyber security or IT unless you hold someone qualified responsible. Regardless of whether this is in-house managed or outsourced.
- This is a big one. If you have a managed IT service provider, do not assume that they are qualified for security. You must check their credentials and memberships and see what systems and processes are in place.
- It is also critical to have an IT security plan or policy in place. Without a plan, there can be no structure or defined functionality and responsibilities. It should cover the defences, the risks they mitigate, if you have a security framework in place, and who is responsible. There should also be regular management reporting and meetings to effectively govern cyber security. Don't simply rely on IT. This is a management decision, and the plan should be agreed upon by the management team. Even if you are non-technical.
- The same applies to the backup, disaster recovery, and business continuity plans. This definitely is not an IT decision! IT can guide, facilitate, import, and support the plan, but it is completely a management decision. Consider your risks! The risks of yesterday were staff errors, hardware failures, natural disasters, the server room overheating or flooding, theft, and power outages. The risks of today are all of those, and the biggest risk is cyberattack. Your plan should cover all scenarios with SLA's and an indication of how long disaster scenarios or even basic backup recovery will take and affect your ability to function.
- Both your IT cyber security plan and backup plan should include the latest government guidelines and best practices.
- Do you have an incident response plan? Or would a cyberattack cause pure chaos and your staff possibly cause more damage? Can you continue to operate? The NCSC has a response plan that can be adapted for your trust, business or school.
- In the event that the attack has a severe impact or the attacker is demanding ransom, Can you make your final stand? Often, this comes in the form of an offsite or offline backup, hosted outside of your network.
- The only way to know if your systems will provide the correct amount of protection is to test them. Examples include penetration tests to see the outside of your network as an attacker would, internal vulnerability scanning to check systems and applications for vulnerabilities, and backup and DR testing.
- Finally, if you are serious about your cyber security, consider certification. An external audit and certification does mean that you have done as much as you can to ensure you have the systems and processes in place to keep the organisation, people, and systems safe. A simple, cost-effective first step is the government's Cyber Essentials Certification. It's available for both schools and businesses. It also shows your stakeholders and customers that you are on the case. The next step is ISO 27001, which is a bit costlier and more involved. However, we truly believe in the benefits we get from the ISO certifications. The processes, global best practices, and independent checking of these.

Breathe is ideally placed to help you with the tasks above. Often, the best starting point is an IT or cyber security audit. We look forward to helping you and sharing our experience."

Craig van Aswegen
MD & Snr IT Management Consultant
Breathe Technology LTD

Small Cracks Lead to Big Payouts

Cyberattacks are big news. Reports of attacks at large, well-known companies or local government offices make headlines on a seemingly constant basis. For those following cybersecurity a bit more closely, the view isn't too different, with cybersecurity news outlets' coverage of top breaches dominated by household names like Mailchimp, MGM, Activision and 23andMe.

Based on what gets reported, it wouldn't be unreasonable to assume that cybercrime is a far bigger problem for Wall Street than for Main Street. Unfortunately, nothing could be further from the truth. In a 2023 blog, CISA reported that **small businesses are three times more likely to be targeted by threat actors** than larger organizations. And these SMB attacks represent billions of dollars in losses each year.

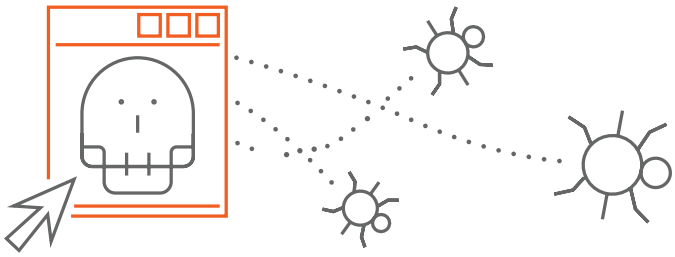
That's a key reason why SonicWall is so committed to researching and publishing the latest threat intelligence. With SMBs making up 80% of our end users, our data presents a view of the threat landscape unlike what you'll find anywhere else — one centered less around large multinational conglomerates, and more on businesses just like yours.

2023's Top Trends

Perhaps the biggest trend we observed in the 2023 landscape was acceleration. SonicWall Capture Labs threat researchers noted increased attack volumes nearly across the board. **Malware jumped 11% year-over-year, with encrypted threats up 117% and cryptojacking up 659%**. This trend bore out on a regional basis as well, with attack volume increases outpacing decreases nearly 3 to 1.

Rather than the relentless push and pull of outside forces we've seen at work over the past several years, we saw threat actors in 2023 sticking with tried-and-true methods. While one would expect increasing malware attack volumes and persistently high phishing levels to be accompanied by high rates of new malware, we found the opposite to be true: Never-before-seen malware detections actually *fell* 38% year over year.

But this doesn't mean threat actors weren't refining their craft. SonicWall researchers observed the emergence of Microsoft OneNote files as an initial threat vector, as well as massive campaigns targeting vulnerabilities in WinRAR and MOVEit.



Our data continued to reflect vulnerabilities as the most common ransomware vector — and this will likely remain the case as the number of vulnerabilities continues to climb. **A record 28,834 CVEs were published in 2023**, a 15% increase over 2022's numbers. In December, SonicWall's threat researchers **discovered and responsibly disclosed CVE-2023-51467**, a vulnerability affecting ApacheOFBiz. Large numbers of exploitation attempts have since been observed.

Other campaigns displayed a similar level of innovation. Novel phishing campaigns driving targets to highly convincing Microsoft Outlook and American Express login pages were observed, along with phishing campaigns utilizing QR codes to bypass file scanning technology. Cybercriminals took advantage of inflation and uncertain economic conditions to launch fraudulent loan apps packed with spyware functionalities and credential-theft capabilities. And Google scripts embedded in PDFs were weaponized to commit cryptocurrency theft, demonstrating the need for heightened vigilance even in seemingly trusted environments.

From SMB to the Enterprise, Today and Tomorrow

We're already looking toward a future threat landscape much different from today's, as threat actors continue adopting ChatGPT and other generative AI technology to refine phishing attempts, carry out highly convincing Business Email Compromise (BEC) attacks, and quickly write malicious code.

But AI also holds great promise for the world's defenders. SonicWall was an early adopter of AI and machine learning, with Capture ATP and RTDMI already capable of detecting many of these types of attacks. But in coming years, we'll begin to see the true potential of AI as a defensive tool.

Highest Since 2019

In 2023, SonicWall Capture Labs threat researchers recorded 6.06 billion malware attacks — a year-over-year increase of 11%. This marks the highest global attack volume for any year since 2019, indicating that malware levels have risen back to their pre-pandemic levels as threat actors continue to become more plentiful, resourceful and active.

But while global malware was up, this was the combination of two opposing trends. Malware in Asia and Europe actually *dropped* by 2%, but this was easily offset by larger increases in North America (+15%) and LATAM (+30%).

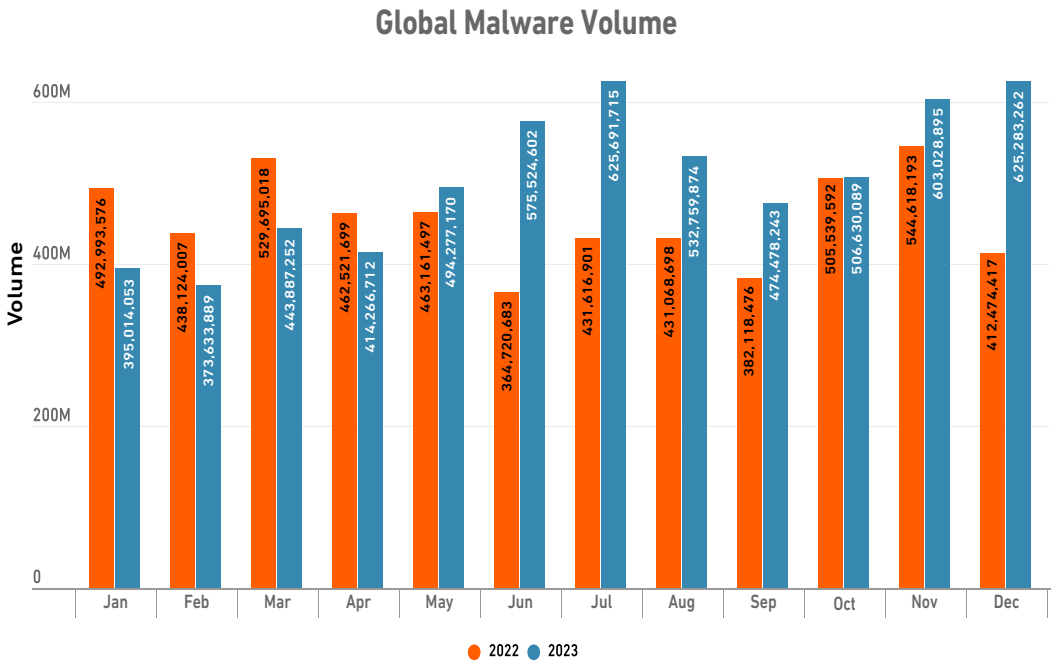
This divergence also appeared in our industry-specific data. Education, which saw by far the most malware in 2022, experienced 3% less in 2023. Malware targeting healthcare and retail, on the other hand, rose 20%, and attacks targeting government spiked 38%. But the hardest-hit were customers in finance—malware attacks on these businesses *doubled*. This increase was enough to make finance the hardest-hit industry we studied in 2023, up from the bottom of the list in 2021 and the middle of the pack in 2022.

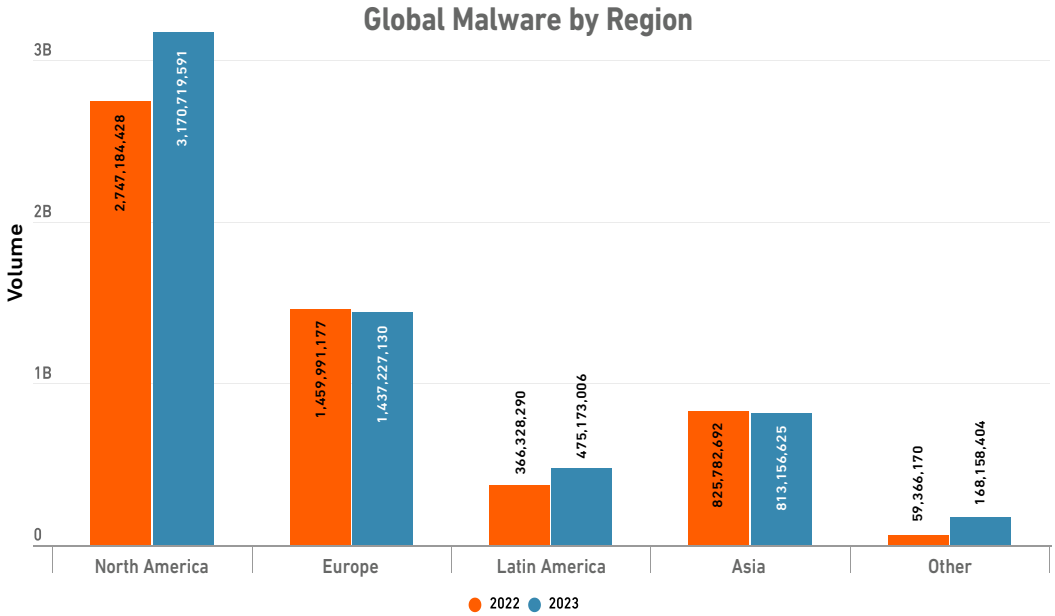
One and Done: Malicious OneNote Files

In early 2023, SonicWall researchers observed threat actors leveraging a new initial vector to infect systems: the use of Microsoft OneNote files. These weaponized attachments were being sent via email, accompanied by a variety of social engineering techniques designed to maximize the odds the attachments would be opened and the target would click on the hidden malicious files tucked inside, triggering the payload execution.

But as security vendors quickly wised up, they began triggering detections based on those attached payload files. Then threat actors pivoted to using a URL that, when clicked, would point to the payload. At the same time, attackers began bloating their code with repeated null bytes at the end of the OneNote files, pushing the file size above 500 MB in an attempt to bypass many AV scanning solutions.

By March, however, the use of these files had already begun to fall dramatically, likely due to Microsoft releasing an Office update that blocked embedded files with dangerous extensions from opening in OneNote. But even though this trend was short-lived, it was widespread enough to make malicious OneNote files the most popular type of malicious Office file for all of 2023, with Qakbot, AsyncRat, AgentTesla and others all using OneNote attachments as an initial entry point.





Malicious PDFs Are Prevalent

Using malicious PDFs has long been a preferred tactic of threat actors. But their use increased dramatically in 2023, growing from roughly a fifth of all new malicious filetype detections to nearly a third—a clear sign that this tactic continues to succeed.

As these attacks grew, so did the innovation, leading to the creation of many notable variants. SonicWall observed several instances of PDFs containing QR codes in 2023, with one example threatening the user with the expiration of a Microsoft password if the target failed to scan the code.

Another PDF featured a malicious URL created by using Google Script in an attempt to evade detection. This complex scam came complete with a fabricated Bitcoin transaction record and a fake "mining progress" bar, enticing targets to enter financial information in order to receive their fictitious funds.

As we've seen in past years, threat actors have gone to extremes in 2023 to replicate well-known and trusted brands — and they're getting better at it all the time. Some examples include malicious PDFs masquerading as iTunes receipts, warnings about multiple login attempts to a Wells Fargo account, and even the login page for collaboration platform RingCentral.

Top Tactics by Threat Actors

Portable Executable (PE) Files Reign Supreme

PE files continue to be the most-used final payload due to delivery simplicity, use of general tools, and ease of execution. But in 2023, we noted an increase in PE malware written in .NET. Likely due to its accessibility and rich functionality, we observed the majority of PE malware is now being written in .NET, including prominent malware families such as RedLine, AgentTesla and AsyncRAT.

Fortunately, PE malware are red-flagged file types, which are examined thoroughly for malicious intent. And while some malware authors use script files as initial vectors for other malware, or write complete malicious code using JavaScript, VBScript, PowerShell or others, SonicWall customers are protected: RTDMI's exceptional script emulation capability provides excellent detection of malicious scripts.

WinRAR Offers Easy Win for Attackers

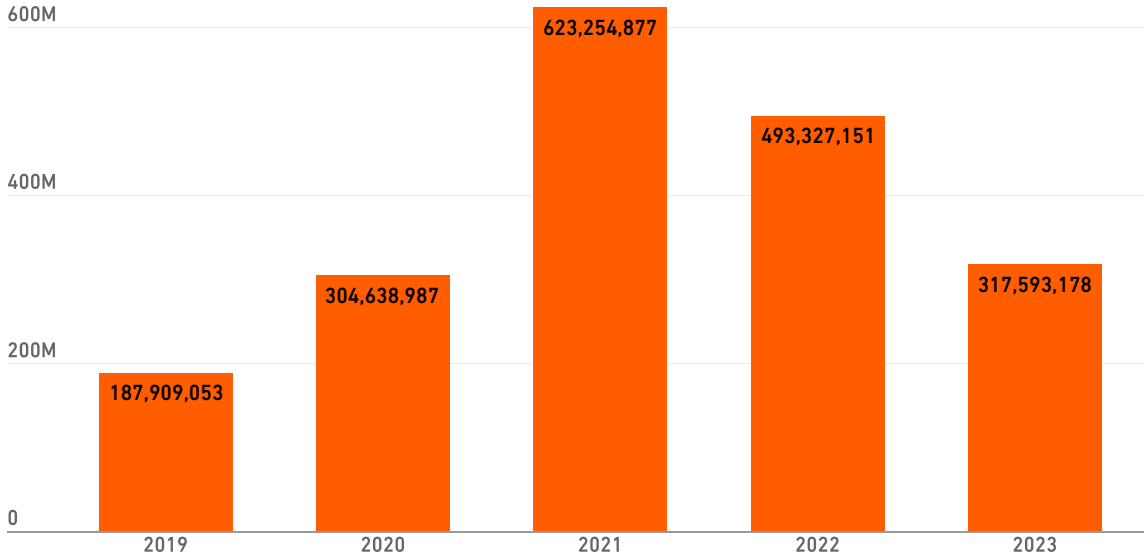
Threat actors began exploiting a new vulnerability in popular Windows file archiver tool WinRAR in early 2023. By the second half of the year, multiple stealer malware families — including AgentTesla, Remcos, Rhadamanthys and Guloader — were implicated in a variety of campaigns exploiting CVE-2023-38831, which allows attackers to execute arbitrary code within zip archives. Due to the widespread use of WinRAR in enterprises, these campaigns quickly proliferated globally, targeting the U.S., the Middle East and Asia. They've now been linked to state-sponsored hackers from Russia and China, including Sandworm, APT28, APT 30 and others.

Still a Force to be Reckoned With

The ransomware attack landscape continued to evolve in 2023. SonicWall Capture Labs threat researchers recorded 317.6 million ransomware attacks, a decrease of 36% year-over-year — but the third-highest total on record. This trend was reflected across several regions: North America and Europe each saw ransomware fall by a third, and in LATAM, attacks fell by 52%.

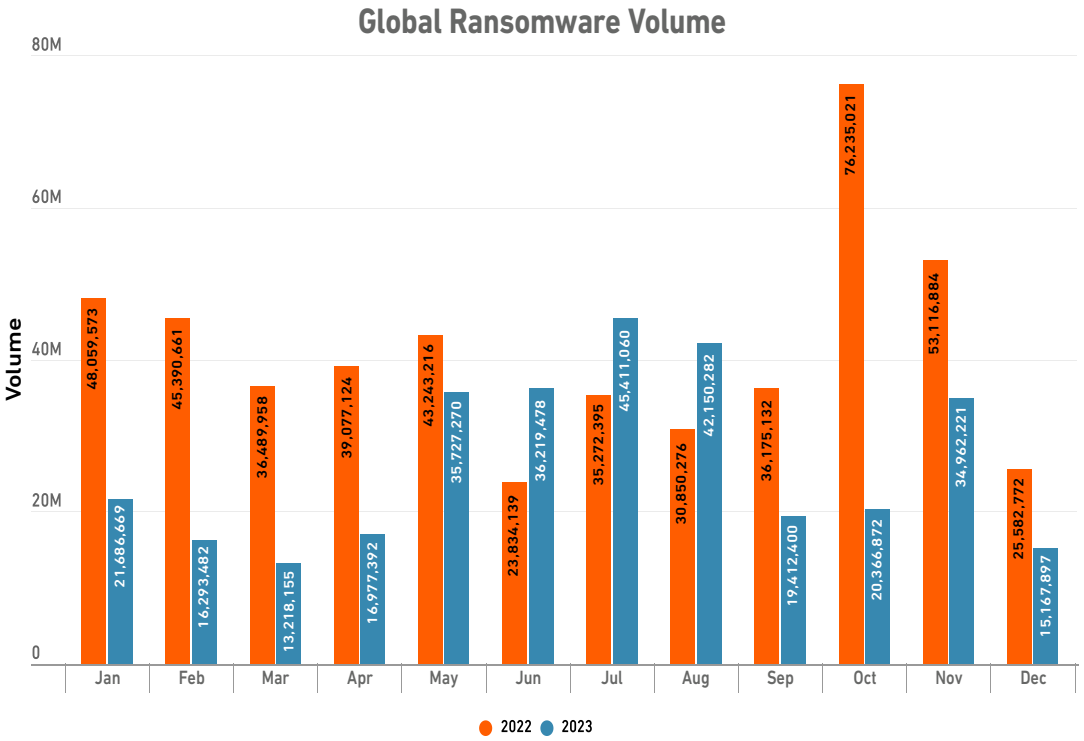
A notable exception was Asia. Ransomware volumes hit a record high in 2023, rising to 17.5 million — a 1,627% increase since 2019. This increase was spearheaded by attacks on the financial sector. In May, the LockBit ransomware group stole 15 million customer records and 1.5 terabytes of internal data from Bank Syariah Indonesia. In November, the Industrial and Commercial Bank of China (ICBC), the world's largest bank by assets, was also attacked by Lockbit. And according to an IDC report released in September 2023, roughly three-quarters of enterprises in India were hit by ransomware in 2022 — a number that has likely continued to climb since.

Global Ransomware Volume by Year



2023's Top Ransomware: LockBit

The arrest of two affiliates barely made a dent in LockBit's numbers: It remained the leading ransomware group in 2023. This is likely due to consistent innovations, such as bug bounty programs to enhance "product" quality, marketing efforts, and the regular release of updated toolkit versions with improved capabilities. After the leak of LockBit 3.0/ "Black," SonicWall engaged the threat actors, who then made a staggering ransom demand (You can see the details here.)



Still Top of Mind: Why it Matters Today

Assuming you don't live in one of the rising ransomware hotspots, how concerned should you be about ransomware?

In our 2023 SonicWall Threat Mindset Survey, we asked customers which types of cyberattack they're most concerned about. Once again, ransomware topped the list at 83%, beating out phishing, encrypted threats, fileless malware, IoT attacks and more.

Despite a decrease in ransomware attack volume amongst our SMB customers, we believe these respondents are on the right track.

Some historical context may be useful here. A 36% decrease sounds like a lot — until you consider ransomware's growth between 2020 and 2022. Even after this drop, 2023 still had enough ransomware to be the third-highest year on record. **And with 27% more ransomware in the second half of 2023 than the first half, ransomware is trending in the wrong direction to meaningfully undo 2021 and 2022's meteoric spikes**.

When cybersecurity vendors like SonicWall measure ransomware and other threats, they can only see what's happening across their own ecosystem. While SonicWall (with its large partner and MSP customer base) noted a decline in ransomware over 2023, some other vendors recorded increases over the same period. With increased law enforcement efforts making each attack riskier, and SMBs no longer being "easy pickings" for threat actors deploying spray-and-pray-style attacks, there seems to be a shift toward focusing on fewer, more highly targeted attacks with a bigger potential payday.

But this doesn't mean there aren't easy pickings to be had. Organizations are increasingly moving data and workflows to the cloud, but often aren't ensuring these instances have the same protection as on-prem. As threat actors continue refining ransomware attacks on SaaS, failing to ensure sufficient security in the cloud could have disastrous results.

There are also still plenty of huge ransomware campaigns being run. In late May, SonicWall observed the exploitation of a critical-rated, zero-day SQL injection vulnerability within MOVEit Transfer. The popularity of this file transfer tool — and its widespread adoption by enterprises — made it a target of the Cl0p ransomware gang. It leveraged CVE-2023-34362 to conduct a supply chain attack that affected about 2,000 organizations across financial, insurance, healthcare, education and government, with data theft impacting more than 62 million people.

It's important to note that vulnerabilities such as this one were the most common vector SonicWall observed for ransomware in 2023 — and those campaigns contributed to ransomware payments surpassing $1 billion for the first time in 2023.

INTRUSIONS

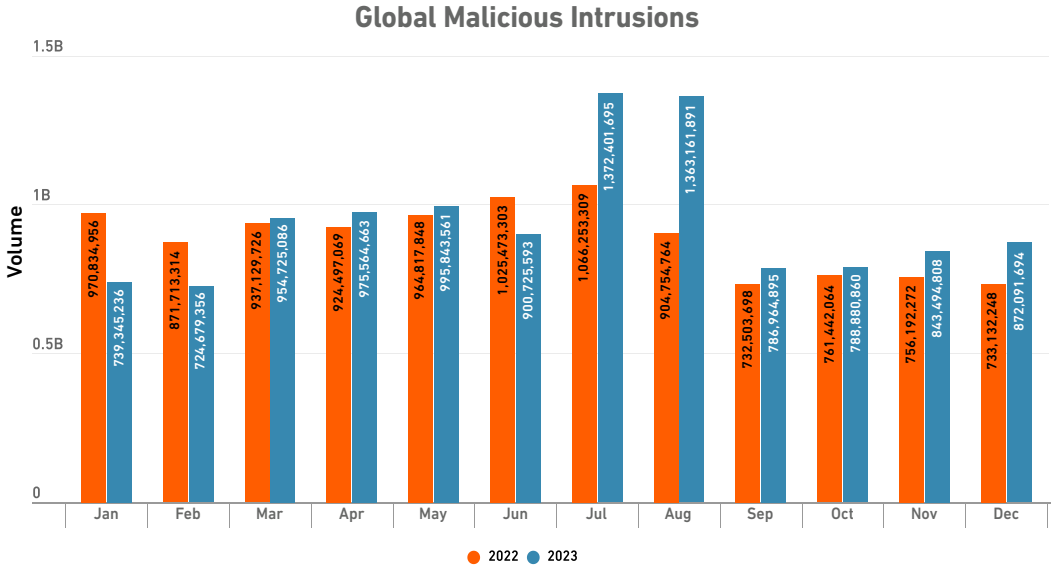
Attempts Up 20%

Overall intrusion attempts continued to climb in 2023, rising to 7.6 trillion, a 20% increase over 2022's total. Since SonicWall began reporting this metric in 2013, the number of intrusion attempts has increased each year — and over the past decade, the number of intrusions has risen 613%.

While some of this increase can be attributed to low-severity hits associated with pings and other typically benign actions, there's also been an uptick in moderate- to high-severity hits — otherwise known as "malicious intrusions." These intrusion attempts increased to 11.3 billion in 2023, a 6% increase year over year.

Malicious intrusion volumes were also up across every industry we studied. Moderate and high-severity hits rose 19% for education customers, 34% for retail customers, 36% for healthcare, 46% for government, and 47% for finance customers.

These attempts set off alerts that must be reviewed by SOC analysts, or MSPs with SOC analysts, contributing to alert fatigue and taking valuable time away from other critical initiatives. And when an intrusion is successful, threat actors are free to exfiltrate data, execute malicious code, encrypt systems and more — potentially grinding operations to a halt and costing these organizations thousands or millions in remediation costs and compliance fines.



What is an Intrusion Attempt?

A malicious intrusion attempt is a security event in which a threat actor tries to gain unauthorized access to a system or resource by exploiting a vulnerability. While the exploit of unpublished "zero-day" vulnerabilities make the most headlines, the most commonly exploited vulnerabilities are generally public and published as CVEs. But because not everyone patches at the same rate, attackers have an opportunity to use unpatched software or appliances as an entry point into a network.

Once threat actors are inside the network, vulnerability exploitation continues as attackers attempt to gain network persistence and lateral movement using other vulnerabilities in unpatched systems within the network.

SonicWall tracks the detection and prevention of exploits coming from both external and internal sources. When a piece of code that constitutes a vulnerability passes a firewall with Intrusion Prevention enabled, and the firewall detects and neutralizes that code, an intrusion attempt is counted.

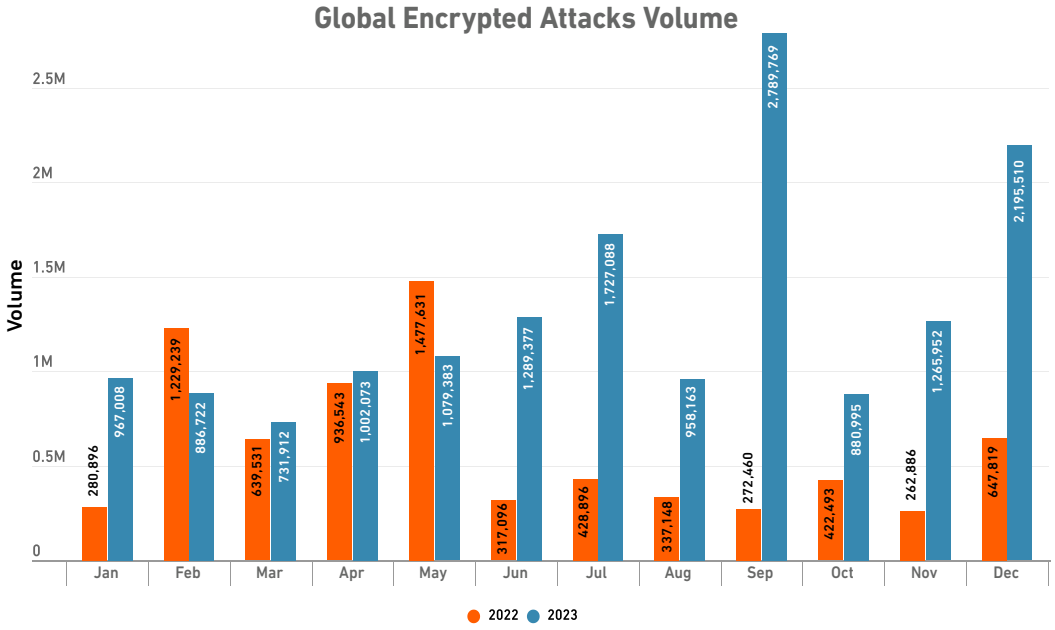
ENCRYPTED THREATS

Encrypted Attacks More Than Double

In 2023, SonicWall Capture Labs threat researchers observed 15.7 million encrypted attacks. This is the most it's been since we began reporting on this threat metric, and we've seen an increase of 117% year over year.

While North America saw a more modest increase of 30%, triple-digit jumps were recorded in Europe, Asia and LATAM, where encrypted attacks rose 182%, 462% and 527% respectively.

Even sharper increases were observed in some of the industries we studied — all of which experienced triple-digit spikes. Finance saw the smallest increase: attacks on these customers "only" doubled. But healthcare (252%), education (429%), government (629%) and retail (680%) all saw encrypted threats skyrocket in 2023.



What Are Encrypted Threats?

Most industry analyst firms conclude that between 80-90 percent of network traffic is encrypted today, requiring you to scan encrypted traffic. While TLS (Transport Layer Security) provides added security for web sessions and internet communications, attackers increasingly use this encryption protocol to hide malware, ransomware, zero-day attacks and more.

Legacy firewalls and other traditional security controls lack the capability or processing power to detect, inspect and mitigate threats sent over HTTPs traffic, making this a highly successful avenue for threat actors to deploy and execute attacks.

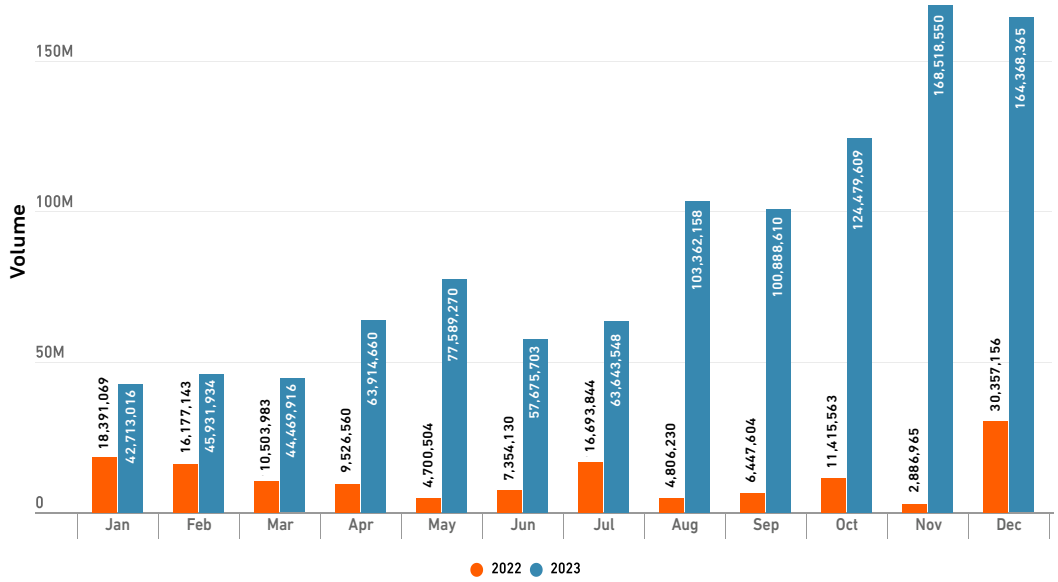
Why It's Dangerous (And Why It's Climbing)

In last year's threat report, we noted a concerning milestone: The number of cryptojacking hits, which had remained fairly low since we began tracking in 2018, surpassed 100,000 for the first time.

But as it turned out, cryptojacking's ascent was only beginning. In 2023, the number of cryptojacking hits had sailed past 2022's full-year total by early April, and continued to pick up steam from there. By the end of the year, SonicWall Capture Labs threat researchers had recorded *1.06 billion* cryptojacking hits—a 659% increase over 2022's totals. This total was fueled by unprecedented attack volumes in November and December—which each had more cryptojacking hits than were noted for the entire year in 2022.

Large increases were also observed across every region. In APAC and LATAM, cryptojacking hits rose 87% and 116% respectively. But truly massive increases were recorded in NOAM (+596%) and Europe (+1,046%).

Global Cryptojacking Volume



What Is Cryptojacking?

Cryptojacking is a type of cyberattack where threat actors hijack a victim's computing resources to mine cryptocurrencies without their consent or knowledge. It involves the installation of malware, often delivered via phishing emails or compromised websites, that secretly runs in the background on a victim's computer, smartphone or server. This malware uses the device's processing power and energy to solve complex mathematical problems ("proof of work"), generating cryptocurrency for the attacker.

Cryptojacking's Current Course

In 2023, the vast majority of cryptojacking attacks once again involved XMRig. This open-source software is a legitimate tool readily available on the internet—but because it's relatively easy to use and configure, it's often abused. It's accessible to even novice threat actors, but also provides an avenue through which more advanced users can modify code in an attempt to evade detection and increase profits.

XMRig is often trojanized, or snuck into other software or adware bundles. It's spread via phishing, malvertising, vulnerabilities, malicious droppers, cracked software applications and more. It's efficient and capable of mining the Monero cryptocurrency (also known as XMR, and often the crypto of choice for cybercriminals due to its privacy features) at a relatively high rate without consuming excessive amounts of system resources. But it still eats up a lot of CPU as it mines in the background — and it does so *constantly*.

This ultimately proves costly, both in terms of productivity, as cryptojacking can slow non-mining activities significantly, and also in terms of actual money: Not only is the victim paying for the increased energy consumption, they may also have to replace devices that overheat or have their lifespan shortened by these taxing processes.

It's also costly to the environment: From 2020-2021 alone, mining Bitcoin had the same carbon footprint as operating 190 gas power plants or burning 84 billion pounds of coal. The total power expenditure from these mining activities exceeds the power consumption of many developed nations.

Crypto mining has been ranked among the most harmful industries for the environment. A study in Scientific Reports found that from 2016 to 2021, each U.S. dollar worth of mined Bitcoin caused 35 cents worth of climate damage.

Despite the high cost of mining cryptocurrency, cryptomining is not illegal, and cryptojacking is rarely prosecuted—though this may be changing. 2024 has already seen one high-profile cryptojacking arrest, as a collaboration between Europol, Ukrainian law enforcement and a cloud provider resulted in the arrest of a suspect believed to have illegally mined more than $2 million in cryptocurrency.

According to SonicWall data, cryptojacking hits made up one-sixth of all malware hits in 2023. As illicit mining becomes more popular, we may start to see the same sort of concerted public and private sector responses that emerged from the early 2020s boom in ransomware.

RTDMI Detections Surpass 1.5 Million

Despite increases across most threat types, SonicWall Capture Advanced Threat Protection (ATP) with Real-Time Deep Memory Inspection (RTDMI) recorded significantly fewer never-before-seen malware variants in 2023: 387,000, a 38% decrease year over year.

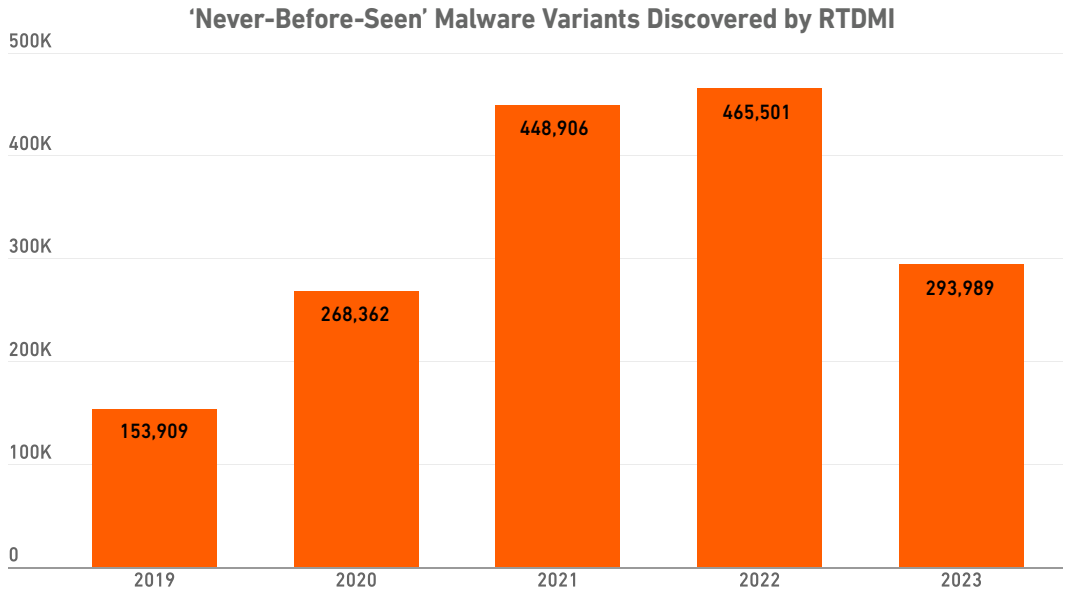
Taken alongside rising malware and persistently high phishing levels, this offers useful information about the 2023 threat landscape: Threat actors aren't slowing down, but for the time being, they're finding variants that work and using them repeatedly. December in particular saw significantly fewer new variants than usual, falling to the lowest level since August 2020.

To be clear, there are still plenty of new malware variants being created — the 800-plus never-before-seen variants per day that customers averaged in 2023 was enough to push all-time detections past the 1.5 million mark. But the pace of innovation does seem to have slowed, at least temporarily.

RTDMI Steps Up Credential Security

But while threat actors may have spent 2023 content to rely on the tried-and-true, SonicWall spent the same time period improving our tools and products. We added a new engine module to RTDMI, making it much better at detecting credential theft over HTML.

HTML phishing scams one of the most common methods of stealing credentials, with pages often highly obfuscated via iframe redirection, JavaScript, dynamic loading and other methods to avoid raising suspicion. The addition of this new module makes it possible to detect these highly obfuscated files. It renders HTML content securely in a sandbox environment and de-obfuscates the final state, where the malicious activity or intent can be clearly observed without endangering the network.



"Zero-Day" vs. "Never-Before-Seen" Attacks

The "zero-day attack" is one of the most well-known cybersecurity concepts due to its connection to high-profile breaches. These attacks are completely new and unknown threats that target a zero-day vulnerability without any existing protection (such as patches, updates, etc.) from the target vendor or company.

Conversely, SonicWall tracks detection and mitigation of "never-before-seen attacks," which is the first time that SonicWall Capture ATP identifies a signature as malicious. These discoveries often closely align with zero-day attack patterns due to the volume of attacks analyzed by SonicWall.

WHAT YOU CAN DO

As the rising tide of threats detailed in this report shows, you can't avoid being targeted. However, there are actions you can take to strengthen your overall cybersecurity approach:

1. **Enable Multifactor Authentication (MFA)**
   Enabling MFA significantly enhances authentication security—even if someone gains access to your passwords, they won't be able to access your accounts since a second authentication is required by you, the user.
2. **Patch Promptly**
   While zero-day vulnerabilities make headlines, most exploit attempts target vulnerabilities months or years old.
3. **Conduct Regular Security Assessments**
   This will help you identify vulnerabilities, assess risks, and proactively strengthen defenses, ensuring robust protection against evolving threats.
4. **Conduct Ongoing Security Trainings:** As technology advances, so does cybersecurity. By deploying basic trainings and routine practices — such encouraging employees to not click on malicious links and training employees to identify and report potential security risks — companies can create a more educated and vigilant workforce.
5. **Scan Encrypted Traffic**
   Experts estimate that 80-90 percent of all network traffic today is encrypted. But many legacy firewalls lack the capability or processing power to detect, inspect and mitigate cyberattacks sent via HTTPs traffic *at all*, let alone using TLS 1.3 — so threat actors routinely use encryption to deploy and execute malware. According to SonicWall data, from 2022 to 2023, malware sent over HTTPS rose a staggering 117%. All told, SonicWall recorded 15.8 million encrypted attacks in 2023 — almost as many as in 2021 and 2022 combined. The growth in encrypted traffic and encrypted threats highlights the necessity of ensuring all of this traffic is scanned.
6. **Extend Your Protection to the Cloud**
   As companies move data and workflows to the cloud, more comprehensive and flexible approaches that include Security Service Edge (SSE) and Zero-Trust Network Architecture (ZTNA) are a necessity for hybrid work environments.

For up-to-date threat intelligence and industry updates, follow the SonicWall blog.

Get in touch

www.breathetechnology.com
(live chat available)

London 020 3519 0124
Cambridge 01223 209920
Sheffield 0114 349 8054
Suffolk 0144 059 2163

lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms