2023

SONICWALL CYBER THREAT REPORT

CHARTING CYBERCRIME'S SHIFTING FRONTLINES

SONICWALL®

sonicwall.com | @sonicwall

Table of Contents

Introduction 3
A Note From Bob 3
2022 Global Attack Trends 4
Ransomware Down … But Not Out 5
Top Data Breaches of 2022 6
Ransomware Remains Top of Mind in 2022 8
CVEs 10
Published CVEs Break 25,000 for First Time 10
Log4j 13
Log4j Intrusion Attempts Surpass 1 Billion 13
Ukraine 16
Ukraine Sees Unprecedented Attack Volume in 2022 16
Breach and Attack Simulation 17
Cybercriminals Shifting from Cobalt Strike to Sliver 17
Key Findings from 2022 19
Malware 21
Malware Up for the First Time Since 2018 21
Ransomware 33
Ransomware Reverses Course 33
Capture ATP & RTDMI 42
RTDMI Detections Continue to Rise 42
Cryptojacking 44
Cryptojacking Continues Record-Breaking Run 44
Encrypted Attacks 50
Encrypted Attacks Fall 28% 50
Intrusion Attempts 52
Overall Intrusion Attempts Up 52
Malicious PDF/Office Files 56
Malicious PDFs Up by More than a Third 56
IoT Malware 59
IoT Malware Nearly Doubles 59
Non-Standard Ports 64
Non-Standard Port Attacks Defy Expectations 64
Phishing 66
Health and Finances Top Phishing Topics for 2022 66
Conclusion 67
The Next Step is Up to You 67
About the SonicWall Capture Labs Threat Network 68

INTRODUCTION

A NOTE FROM BOB

This marks our 11th year of publishing the annual SonicWall Cyber Threat Report. Over the last 30-plus years, we've deployed millions of firewalls and endpoints globally. To this day, SonicWall has more than 1.1 million active sensors that report threat information multiple times a day, providing us with rich sets of threat data. This threat intelligence contributes to our strong security efficacy, but also highlights key real-time trends in the market.

Over the past year, cybercriminals faced with increasing media attention, heightened awareness and intensifying law-enforcement pressure began shifting away from established hotspots to new areas. As a result, organizations already dealing with macroeconomic pressures, supply-chain challenges and continued geopolitical strife often found themselves confronted with a cyberattack.

2022 reinforced the need for cybersecurity in every industry, and every facet of business, as threat actors targeted anything and everything. For instance, while the retail and finance industries typically see lower cyberattack volume compared with other industries, in 2022 both verticals experienced double-digit increases in malware, including *triple*-digit increases in IoT malware attacks and cryptojacking.

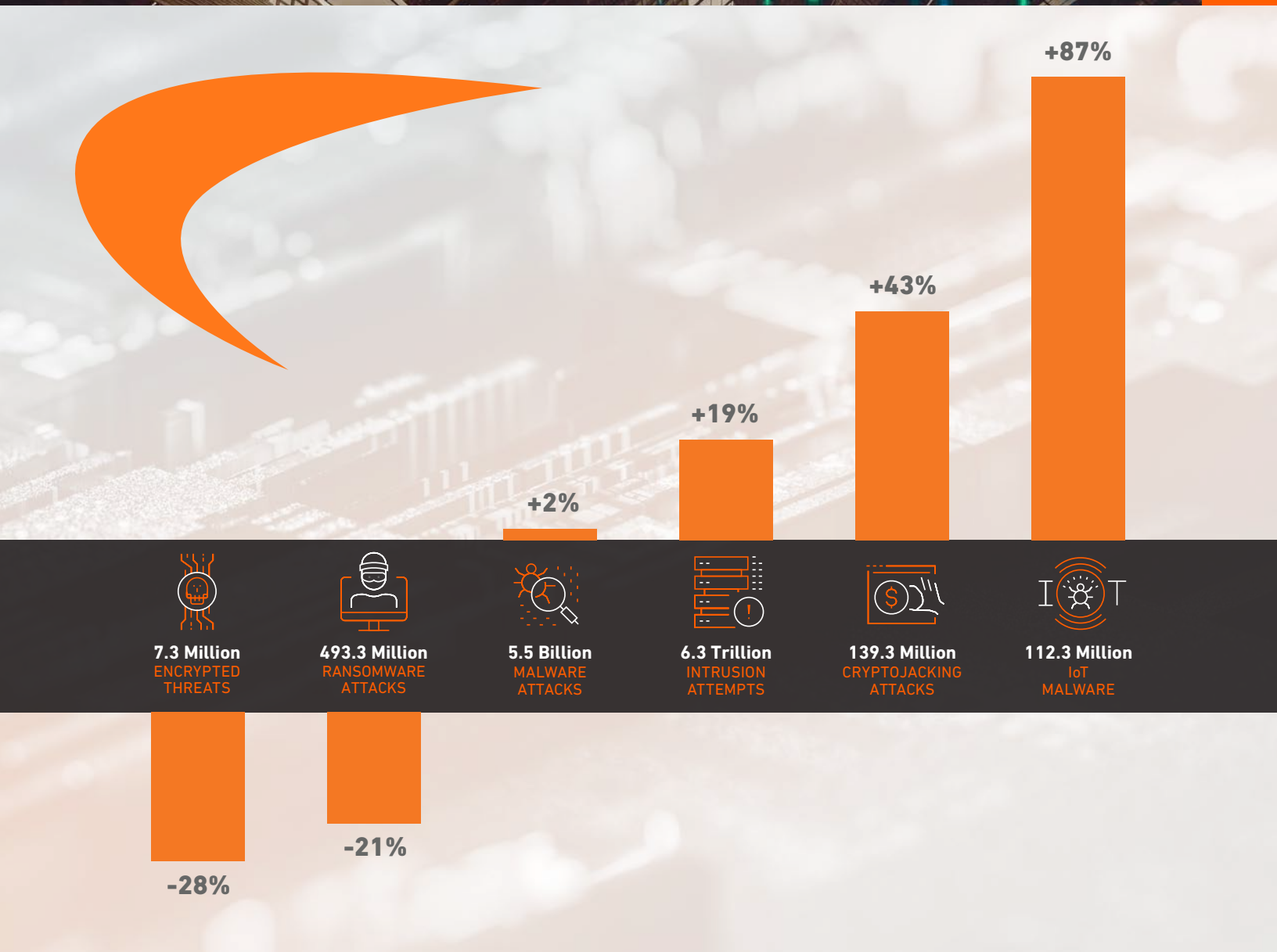
These trends were compounded by the fact that new tactics are being developed with breathtaking speed. 2022 brought growth in pure extortion attacks, the fall of 'Big Ransomware,' widespread expansion to Linux and cloud targets, the adoption of powerful new languages and platforms, and the growing specter of AI and quantum attacks.

In this volatile threat environment, preparation is more critical than ever before. And today, being prepared means more than just deploying the most advanced solutions. It means developing comprehensive cybersecurity strategies, based on the most current threat intelligence available.

The 2023 SonicWall Cyber Threat Report is your guide to attackers' rapidly evolving tactics. On behalf of our network of trusted partners and the entire SonicWall team, including our Capture Labs threat researchers, we're pleased to share these key insights on cybercrime's shifting frontlines, as well as the actionable threat intelligence you need to arm your organization against today's ever-changing threat environment.

Bob VanKirk
President & CEO
SonicWall

2022 GLOBAL ATTACK TRENDS



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.

While the past several years have given the cybersecurity world plenty to worry about, there have nonetheless been a few things we could count on. Malware was falling. Ransomware was rising. And attackers continued to prioritize targets in the U.S.

But from start to finish, 2022 was characterized by change. Ushered in by the announcement of the historic Log4j vulnerabilities just weeks before, the year brought a seismic shift in cybercriminal behavior that sent ripples across every region and every industry.

Ransomware Down … But Not Out

For the past two years, ransomware has been on a tear, increasing 62% year over year in 2020 and another 105% in 2021. During this time, Ransomware-as-a-Service (RaaS) took off, compromised credentials became cheaper and more plentiful than ever, and the number of vulnerabilities continued hitting record highs.

But despite there being fewer barriers of entry for new threat actors than ever before, in 2022, SonicWall Capture Labs threat researchers observed a *21% drop* in ransomware year over year. Other vendors have noted a similar decline, as have U.S. government agencies.

As Goes Russia, So Goes Ransomware

In May, U.S. National Security Agency (NSA) Cybersecurity Director Rob Joyce remarked on the decreasing ransomware levels. "There's probably a lot of different reasons why that is, but I think one impact is the fallout of Russia-Ukraine," Joyce said.

With roughly two-thirds of state-sponsored cyberattacks coming from Russia, and 75% of money generated by ransomware in 2021 going to groups "highly likely to be affiliated with Russia," anything affecting that country has an outsized effect on cybercriminals, and in turn, cybercrime. According to Joyce, sanctions have made it harder for cybercriminals to move money and buy infrastructure needed for attacks, making cybercriminals less effective.

But while becoming "less effective" should result in an even decrease across the board, what's actually being observed are huge decreases in places that generally see the most ransomware — particularly the United States, where ransomware fell by nearly half.

Ransomware or Bust

2021 was a banner year for ransomware busts. Cybercriminals associated with Netwalker, Egregor, Lockergoga, MegaCortex and the Trickbot malware were brought to heel amid a flurry of headlines, and when a 30-month investigation involving INTERPOL, South Korea, Ukraine and the U.S. resulted in the arrests of the Cl0p ransomware kingpins, it sent the message that the U.S. was no longer the safe profit center it once was.

But two bigger wake-up calls were yet to come. In January 2022, the Darkside members responsible for the Colonial Pipeline attack were arrested by Russian authorities. Then, in another rare (and no doubt politically motivated) show of cooperation with the U.S., Russian intelligence services arrested members of the infamous REvil gang the same week. Cybercriminals, who had been accustomed to acting with impunity, suddenly became aware that there were very few places left to hide.

In January 2022, a sampling of Dark Web cybercriminal chatter published by ZDNet revealed an undercurrent of fear running through the underworld. "This is a big change. I have no desire to go to jail," one said in response to the REvil arrests. Another seemed to take them as a warning, saying that anybody who expected Russia to protect them would be "greatly disappointed." Still others worried that Dark Web admins might reveal their identities to law enforcement.

But as the risk of attacking targets in the U.S. went up, the perceived payoff dropped. Mounting cyberinsurance requirements and the specter of mandatory reporting offered businesses even more motivation to harden defenses. And in 2022, the U.S. government created the Virtual Asset Exploitation Unit, increasing tracking and enforcement efforts against ransomware operators.

Faced with a risk/benefit analysis no longer working in their favor, some cybercriminals shifted targets, leading to double-digit ransomware *increases* in places like Europe and Asia. Still others are diversifying their tactics.

Jack of All Trades

Unlike ransomware, which announces its presence, thrives on branding and notoriety, and relies heavily on direct contact with victims, cryptojacking can succeed in complete silence. And for some cybercriminals feeling the heat from increased enforcement efforts and ongoing geopolitical conflict, a consistent, lower-risk income stream may be worth sacrificing a potentially higher payday.

"[Cryptojacking] has a lower potential of being detected by the victim; unsuspecting users across the world see their devices get unaccountably slower, but it's hard to tie it to criminal activity, much less point to the source," Terry Greer-King, SonicWall Vice President for EMEA, told Tech Monitor.

Top Data Breaches of 2022

NAME	INDUSTRY	DATE	IMPACT
Philippines COMELEC	Government	January	60 GB of data, including usernames and PINs for vote-counting machines
U.S. Department of Education	Government	January	820,000 student records
Texas Dept. of Insurance	Government	January	1.8 million records
Crypto.com	Finance	January	500+ cryptocurrency wallets (more than $30M)
ICRC (International Committee of the Red Cross)	Charity	January	515,000 records
Flexbooker	Software	January	3.7 million records
GiveSendGo	Fundraising	February	90,000 records
Harbour Plaza Hotel Management	Hospitality	February	1.2 million records
Credit Suisse	Finance	February	18,000 Credit Suisse accounts
Nvidia	Technology	February	71,000+ employee records
Microsoft	Software	March	Bing, Bing Maps & Cortana partial source code
Ronin Bridge Hack	Finance	March	$625 million in crypto
Pegasus Airlines	Travel	March	6.5 TB of data, including source code, flight crew PII and passwords/secret keys
Morgan Stanley Clients	Finance	March	Unknown number of client accounts
Cash App	Finance	April	8.2 million records
Elephant Insurance	Insurance	May	2.7 million records
SuperVPN, GeckoVPN & ChatVPN	Technology	May	21 million records
Cost Rican Government	Government	May	670GB data
National Registration Dept. of Malaysia	Government	May	22.5 million records
Alameda Health System	Healthcare	May	90,000 records
Verizon	Telecommunications	May	Hundreds of employee records
Flagstar Bank	Finance	June	1.5 million records
Shields Health Care Group	Healthcare	June	2 million records
Choice Health Insurance	Healthcare	June	600MB of data, including names, SSNs, and other PII
OpenSea	Finance	June	$1.7 million in NFTs
Neopets	Entertainment	July	69 million records
Twitter	Social Media	July	5.4 million accounts
Uber	Travel	July	57 million records
OneTouchPoint	Marketing	July	2.65 million records
Cisco	Technology	August	2.75 GB of data, including engineering files and NDAs
Plex	Software	August	20 million records
Okta	Technology	August	169 domains
Nelnet Servicing	Finance	August	2.5 million records
Optus	Telecommunications	September	9.8 million records
Samsung	Telecommunications	September	Unknown
North Face	Apparel	September	200,000 records
Revolut	Finance	September	50,150 records
Mydeal	Retail	October	2.2 million records
Vinomofo	Food & Beverage	October	500,000 records
Medibank	Healthcare	November	9.7 million records

In 2022, SonicWall researchers recorded a 43% increase in cryptojacking, on the heels of a 19% increase in 2021. This growth set a new record and pushed observed attack volumes past the 100-million mark for the first time ever.

At least one ransomware gang, Astralocker, publicly announced it's leaving ransomware entirely in favor of cryptojacking, and a comparison of our ransomware data with our cryptojacking findings suggests others could be using these attacks along with or in place of ransomware.

But while some criminals are slowing or abandoning ransomware in favor of cryptojacking and other attack types, others are abandoning the "ware" but keeping the "ransom."

The Rise of Extortion Groups

An increased awareness of ransomware motivated many organizations to create and maintain strong backups and incident response plans, making file encryption less effective than it once was.

In response, 2022 brought a growth in the number of ransomware groups no longer actually deploying ransomware. These attackers, referred to as "extortion groups," include both Lapsus$ and Karakurt — both of which became major threats without encrypting a single endpoint. By using social engineering, vulnerability exploits, stolen credentials or other tactics, these groups gain illegal access to a target network. Then, once they've stolen data, they threaten to leak the information if victims don't pay up.

But while these attacks involve reputational damage, data leaks, and the risk of compliance issues and lawsuits like traditional ransomware, they're much harder to trace. Since there's no actual ransomware involved, tracking is often conflated under "malware." However, this is a distinct form of extortion and needs to be tracked by vendors despite a lack of encrypting endpoints.

When Will Ransomware Rebound?

While several factors could be responsible for the drop in ransomware, there are also many signs it could soon make a turnaround.

First, it bears mentioning that we aren't actually seeing any sort of widespread abandonment of ransomware. While attacks are down 21%, 2022's ransomware volume is still much closer to the sky-high totals we saw in 2021 than to what we saw in 2018, 2019 and 2020. If we remove 2021 as an outlier, ransomware is still on the rise.

In fact, many criminals actually doubled down on ransomware in 2022. Several new ransomware groups formed, including Black Basta, Quantum, Lilith, Stormous and more, and in November, a new version of the highly popular LockBit ransomware was released.

And as 2022 wound down, larger campaigns were once again making headlines. In December, the U.K. news site The Guardian was attacked, and in early 2023, a new ESXiArgs campaign infected over 3,800 victims with ransomware.

Perhaps not coincidentally, SonicWall observed an uptick in ransomware in Q4, when attack volume rose to the highest level since Q3 2021. While we can't be sure yet whether this is a sign of sustained growth, we can be sure ransomware isn't going anywhere soon.

A Lapsus in Judgment

In early 2022, a new cybercriminal group began dominating the headlines. Calling themselves "Lapsus$," they quickly became known for their brazen tactics: Instead of lurking in the corners of the Dark Web, this group actively cultivated a social media presence, accumulating more than 50,000 followers on Telegram. Here, they solicited input on who should be targeted next, ultimately engaging in some of the biggest big-game hunting imaginable: Okta, Nvidia, Samsung, Microsoft and others were all breached. To facilitate these breaches, the group publicly recruited new accomplices, offering money for inside information or assistance.

By mid-September, less than a year after becoming active, the group was gone, its members nabbed in three high-profile arrests. None was older than 21.

In Latin, a "lapsus" refers to a "lapse, slip or error." And it quickly became clear that much of the group's trademark attention-seeking was exactly that.

Seemingly operating with a presumption of invincibility, they failed to recognize the main reason they'd been able to earn so much attention in the first place: Most of the world's other cybercriminals had suddenly become very, very quiet.

Ransomware Remains Top of Mind in 2022

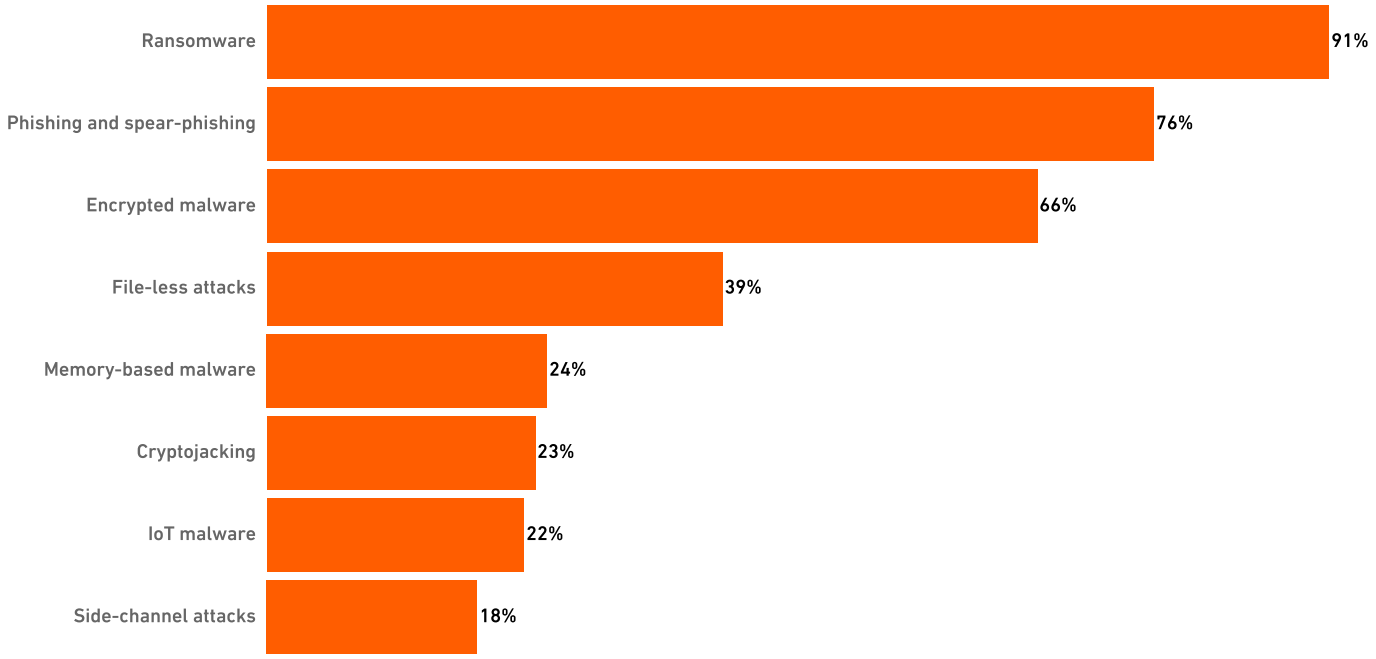
While ransomware was on the decline in 2022, it was still ranked as the top threat in SonicWall's inaugural Threat Mindset survey, released in August.

For this survey, SonicWall surveyed customers across a variety of industries located around the globe, asking a series of questions to evaluate the sentiments of those "on the ground" in the war on cybercrime.

When asked what types of cyberattack they're most concerned about, 91% of respondents answered ransomware. Phishing and spear-phishing, which are often used as vectors for ransomware, were ranked second, with roughly three-quarters of respondents rating them as a concern.

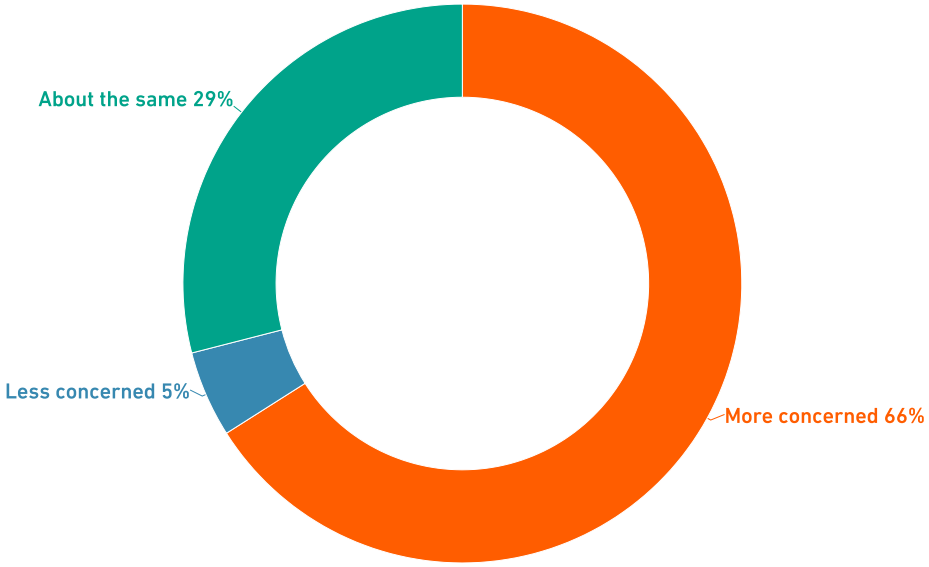
WHEN ASKED WHAT TYPES OF CYBERATTACK THEY'RE MOST CONCERNED ABOUT, 91% OF RESPONDENTS ANSWERED RANSOMWARE.

Which types of cyberattacks are you most concerned about?



Source: 2022 SonicWall Threat Mindset Survey.

Are you more or less concerned about cyberattacks in your organization in 2022 than in previous years?



Source: 2022 SonicWall Threat Mindset Survey.

What's more, 66% of respondents reported being more concerned about attacks this year than last year, with another 29% reporting that they have roughly the same amount of concern about attacks as they did in 2021. Only 5% reported being less concerned.

The survey's open-ended questions provided a more in-depth look at how respondents were perceiving their risk, along with what they planned to do about it.

"Frankly, I live in terror of a ransomware attack and state-sponsored intrusions. On my logs, I have seen massive increases in probes from Russia, China and a handful of other (what I would call) enemy nations," a business professional employed at a small business healthcare company said.

Another respondent, an IT director for a financial services business, said that they were doubling down on training in response to the recent increase in attacks.

"The evolving cyber landscape has made us train users a lot more," they said. "It's made us spend more on cybersecurity. It scares the hell out of me that an end user can click on something and bring our systems down — even though we're well protected."

For more on how SonicWall customers perceive the current state of cybersecurity — and their place in it — download the 2022 SonicWall Threat Mindset Survey.

CVEs

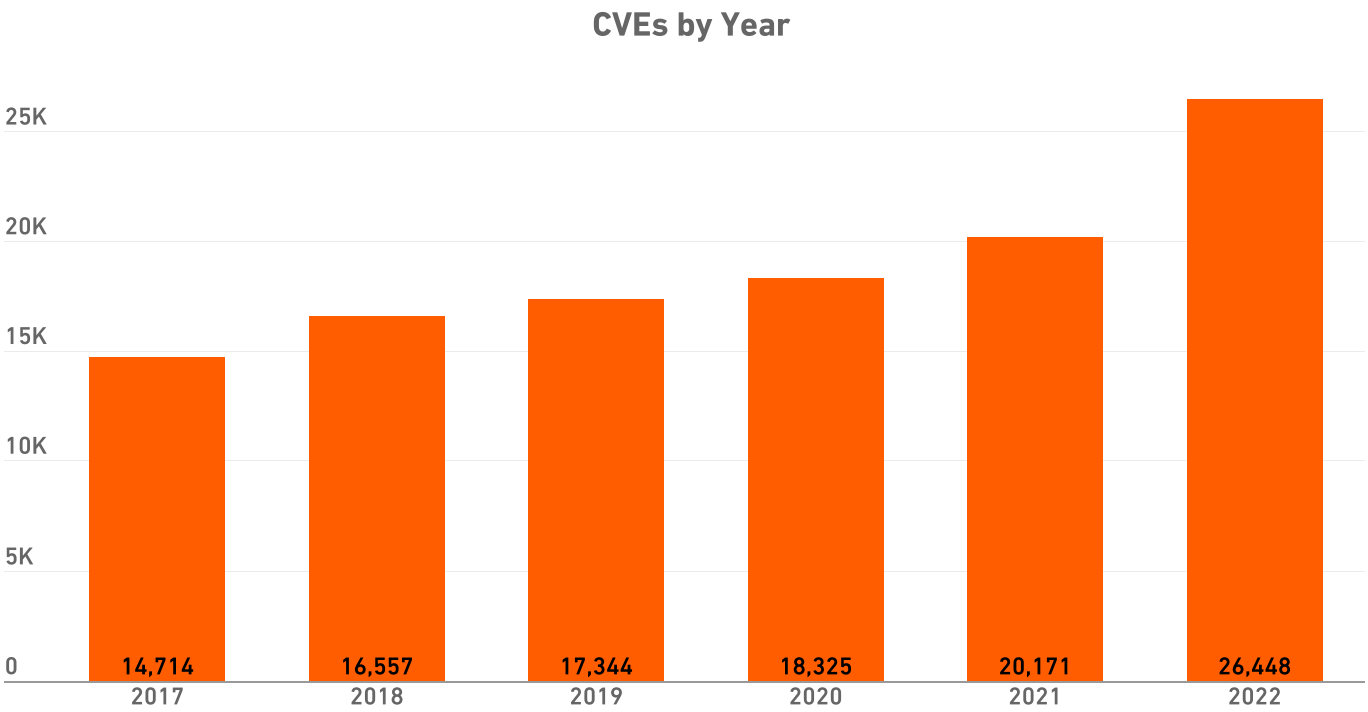
Published CVEs Break 25,000 for First Time

A total of 26,448 Common Vulnerabilities and Exposures (CVEs) were published in 2022, according to NIST. This marks the sixth year in a row that a record number of vulnerabilities has been discovered, and the first time in history that the number of CVEs has passed 25,000.

While this milestone represents the hard work those in the cybersecurity industry are doing to identify vulnerabilities more quickly and efficiently, it isn't necessarily cause for celebration. It also reflects the pernicious trends that make quicker and more efficient work necessary in the first place.

As organizations deploy more software and tools, the attack surface continues to grow. And the more products a company utilizes, the more likely it is that one will be vulnerable. (A good example of this is the Apache Log4j vulnerabilities; see page 13)

The most severe vulnerabilities, the ones rated a nine or above on the 10-point scale, become entry points for cybercriminals, and attackers are increasingly utilizing this means of entry to deploy ransomware and other malware and to exfiltrate data.



2022 Brought Progress in Patching

In July 2022, CISA released its list of top vulnerabilities exploited by criminals in 2021 (Alert AA22-117A), and within it was some encouraging news.

In 2020, each of the top 10 most exploited vulnerabilities had a patch or updated version available. Even so, only two of them were actually *discovered* in 2020, with some going back as far as 2017. In other words, most cybercriminals weren't exploiting zero-day vulnerabilities — instead, they were exploiting vulnerabilities that should have been patched months or *years* before.

The outlook was much better in 2021, however. In this list, *all* of the top 10 most exploited vulnerabilities were discovered the same year. (We actually had to make our list longer before any from previous years showed up — of these, only a single entry, CVE-2018-13379, appeared on last year's list.)

While some of these rankings are undoubtedly due to how much the newer vulnerabilities are being exploited (case in point: Log4Shell), the fact that a majority of the old vulnerabilities on the more recent list are not the *same* old vulnerabilities that were on the 2020 list suggest that we may finally be seeing some progress on the patching front.

Top 15 Most Exploited Vulnerabilities

CVE	VENDOR/PROJECT	PRODUCT	TYPE
CVE-2021-44228 (Log4Shell)	Apache	Log4j	Remote code execution (RCE)
CVE-2021-40539	Zoho	ManageEngine AD SelfService Plus	RCE
CVE-2021-34523 (ProxyShell)	Microsoft	Exchange Server	Elevation of privilege
CVE-2021-34473 (ProxyShell)	Microsoft	Exchange Server	RCE
CVE-2021-31207 (ProxyShell)	Microsoft	Exchange Server	Security feature bypass
CVE-2021-27065 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-26858 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-26857 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-26855 (ProxyLogon)	Microsoft	Exchange Server	RCE
CVE-2021-26084	Atlassian	Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972	VMware	vSphere Client	RCE
CVE-2020-1472 (ZeroLogon)	Microsoft	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688	Microsoft	Microsoft Exchange Server	RCE
CVE-2019-11510	Ivanti	Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379	Fortinet	FortiOS and FortiProxy	Path traversal

Source: CISA, Top Routinely Exploited Vulnerabilities, 2022 (Alert AA22-117A).

2022 Zero-Day Vulnerabilities

Of the more than 26,000 vulnerabilities published in 2022, SonicWall Capture Labs threat researchers tracked 35 zero-days being actively exploited in 2022. This is a 150% increase from 2021's total of 14.

2022 Zero-Day Vulnerabilities

MONTH	CVE	NAME
January	CVE-2022-22587	Apple Memory Corruption Vulnerability
February	CVE-2022-24086	Adobe Commerce and Magento Open Source Improper Input Validation Vulnerability
February	CVE-2022-22620	Apple Webkit Remote Code Execution Vulnerability
March	CVE-2022-1096	Google Chromium V8 Type Confusion Vulnerability
March	CVE-2022-22965	Spring Framework JDK 9+ Remote Code Execution Vulnerability [Spring4Shell]
March	CVE-2022-26485	Mozilla Firefox Use-After-Free Vulnerability
March	CVE-2022-26486	Mozilla Firefox Use-After-Free Vulnerability
June	CVE-2022-26134	Remote code execution in Atlassian Confluence Server
June	CVE-2022-30190	Microsoft Windows Support Diagnostic Tool MSDT Remote Code Execution Vulnerability [Follina]
August	CVE-2022-32893	Multiple vulnerabilities in Apple macOS Monterey
August	CVE-2022-32894	Multiple vulnerabilities in Apple macOS Monterey
August	CVE-2022-2856	Multiple vulnerabilities in Google Chrome
September	CVE-2022-3236	Remote code execution in Sophos Firewall
September	CVE-2022-37969	Privilege escalation in Microsoft Windows common log file system driver
September	CVE-2022-40139	Multiple vulnerabilities in Trend Micro Apex One
September	CVE-2022-32917	Multiple vulnerabilities in Apple macOS Monterey
September	CVE-2022-3180	Remote code execution in WPGateway plugin for WordPress
September	CVE-2022-31474	Arbitrary file read in BackupBuddy WordPress plugin
September	CVE-2022-41040	Microsoft Exchange Server Elevation of Privilege
September	CVE-2022-41082	Microsoft Exchange Server Remote Code Execution
September	CVE-2022-41352	Zimbra TAR Remote Code Execution
September	CVE-2022-3075	Remote code execution in Google Chrome
October	CVE-2022-3723	Remote code execution in Google Chrome
October	CVE-2022-42827	Multiple vulnerabilities in Apple iOS 16 and iPadOS 16
October	CVE-2022-41033	Privilege escalation in Microsoft Windows COM+ Event System Service
November	CVE-2022-4135	Remote code execution in Google Chrome
November	CVE-2022-41091	Multiple vulnerabilities in Microsoft Windows Mark of the Web
November	CVE-2022-41125	Privilege escalation in Microsoft Windows CNG Key Isolation Service
November	CVE-2022-41128	Remote code execution in Microsoft Windows Scripting Languages
November	CVE-2022-41073	Privilege escalation in Microsoft Windows Print Spooler service
December	CVE-2022-42856	Remote code execution in Apple iOS
December	CVE-2022-27518	Remote code execution in Citrix ADC and Citrix Gateway
December	CVE-2022-44698	SmartScreen MOTW bypass in Microsoft Windows
December	CVE-2022-42475	Remote code execution in FortiOS sslvpnd
December	CVE-2022-4262	Remote code execution in Google Chrome

Log4j Intrusion Attempts Surpass 1 Billion

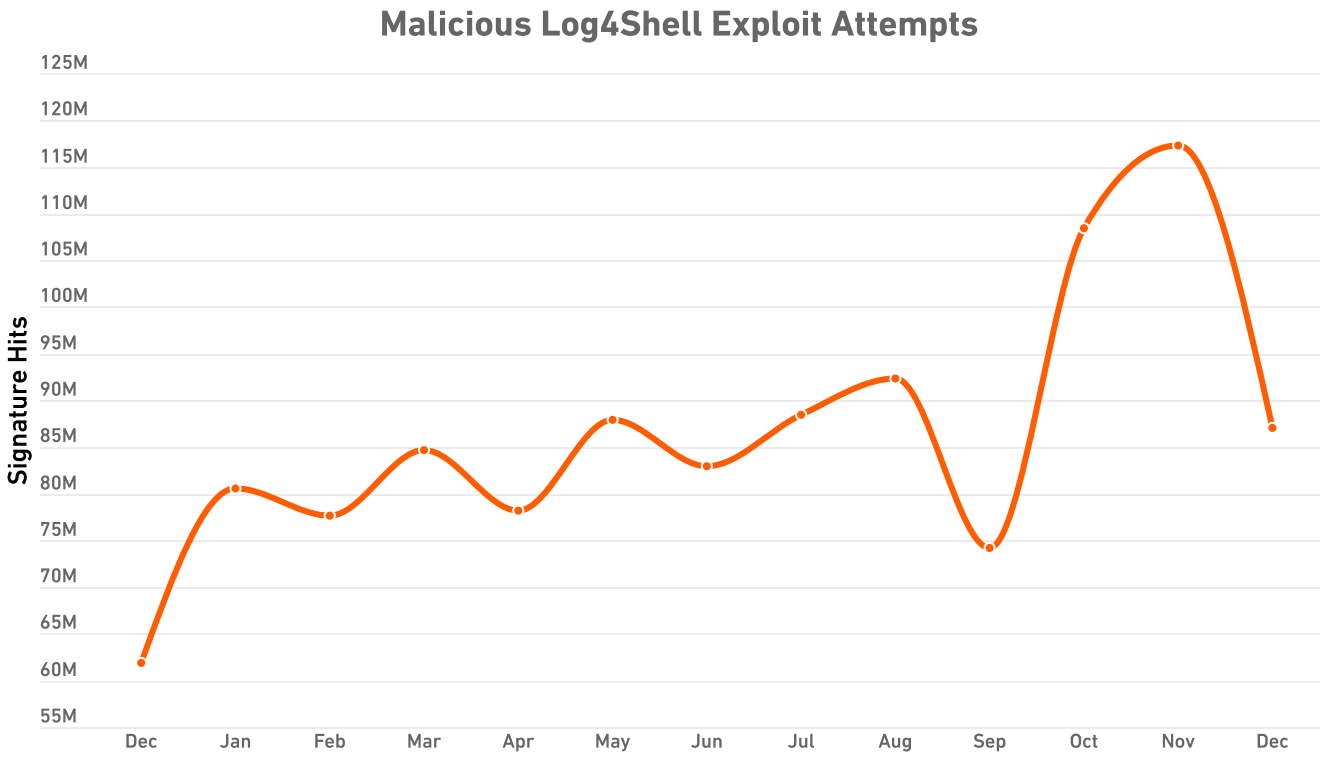
It's now been more than a year since the announcement of the Apache Log4j vulnerabilities sent shockwaves through the tech community. Since December 2021, SonicWall Capture Labs threat researchers have been tracking attempted exploits of this vulnerability, and so far, attack volumes show no signs of slowing.

SonicWall logged a total of 1.12 billion intrusion attempts against the Log4j vulnerabilities in 2022. While some had hoped for an initial frenzy of attacks followed by a gradual decrease, our researchers have observed the opposite: 61.9 million attempts were observed in December 2021, the month the attacks were announced — and every month in 2022 exceeded that total by at least 10 million.

Worse, these attempts seemed to pick up steam as 2022 went on: The second half of the year had 15% more intrusion attempts than the first half.

What Are the Log4j Vulnerabilities?

These vulnerabilities affect Log4j, a highly popular Full Open-Source Software (FOSS) logging library with two primary branches, 1.x and 2.x, the former of which is at end of life. This software is used to record, or log, security and performance information. Because the software was widely used, and the Log4j vulnerability existed *for eight years* before it was announced, the vulnerabilities affect millions of consumer and business products — everything from the Minecraft video game to the Mars 2020 helicopter mission Ingenuity.



How Attackers Targeted Log4j

Given how widespread and easily exploited these vulnerabilities were, it's no surprise that threat actors sprang into action almost immediately.

In late December 2021, just weeks after the vulnerabilities were announced, major Vietnamese crypto trading platform ONUS was attacked via a payment system running a vulnerable version of Log4j. Soon after, the attackers threatened to publish ONUS customer data unless they paid a $5 million ransom.

Then in November 2022, a CISA alert warned of attacks by an Iranian government-sponsored APT. This group had exploited the Log4Shell vulnerability to gain access to an unpatched VMware Horizon server in a federal civilian executive branch organization. Once inside, it installed the XMRig cryptominer, moved laterally to the domain controller, compromised credentials, and finally placed Ngrok reverse proxies to maintain persistence.

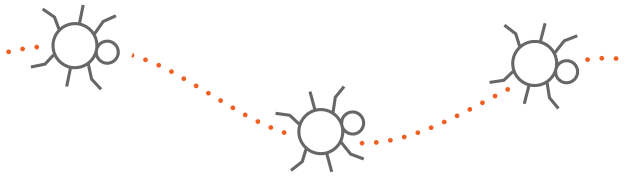
Campaigns such as these have involved a large variety of malware. A new ransomware family, known as Khonsari, was discovered after it successfully targeted a small group of Minecraft players running servers vulnerable to Log4j. There's also been a recent resurgence in Mirai botnet malware, this time using vulnerable Log4j deployments to gain initial access to publicly exposed routers, network cameras and other connected devices.

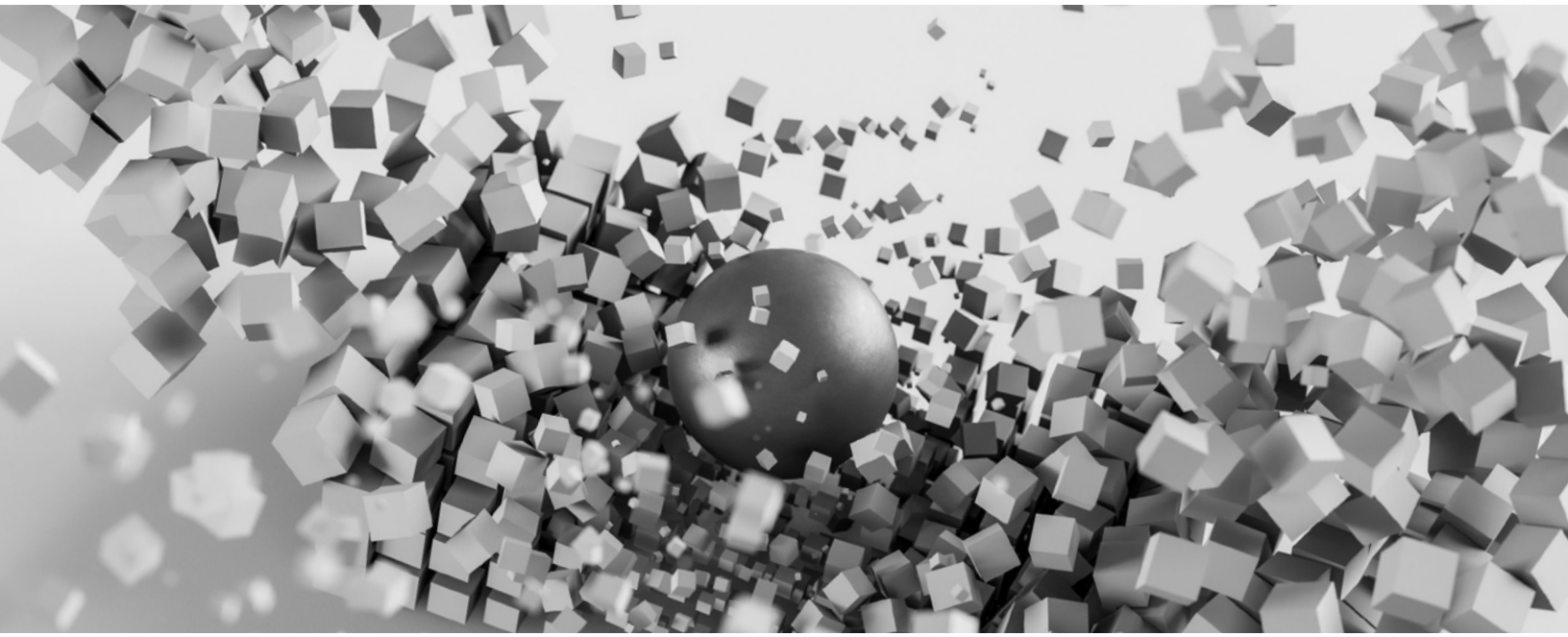
The Worst May Be Yet to Come

But despite the numerous attacks that occurred in 2022, it's unlikely we've seen the worst of it. First, we still have no idea how many threat actors leveraged the vulnerability shortly after it was disclosed to quickly install backdoors before silently moving on.

What's more, even though many organizations are committed to patching, a lack of visibility into where Log4j exists in ecosystems has limited the effectiveness of these efforts. An estimated 70,000 open-source projects have Log4j as a direct dependency, and another 174,000 projects have it as a transitive dependency. And as new assets are added to the environment, it's possible to become vulnerable again and again.

In another year, we'll likely have a better idea what the future of the Log4j vulnerabilities will look like. In the meantime, this is perhaps the best argument yet for creating a SBOM (software bill of materials). Knowing where Log4j exists on your system and making sure new instances are patched quickly will go a long way toward reducing your risk now and in the future.





Who's Exploiting Log4j?

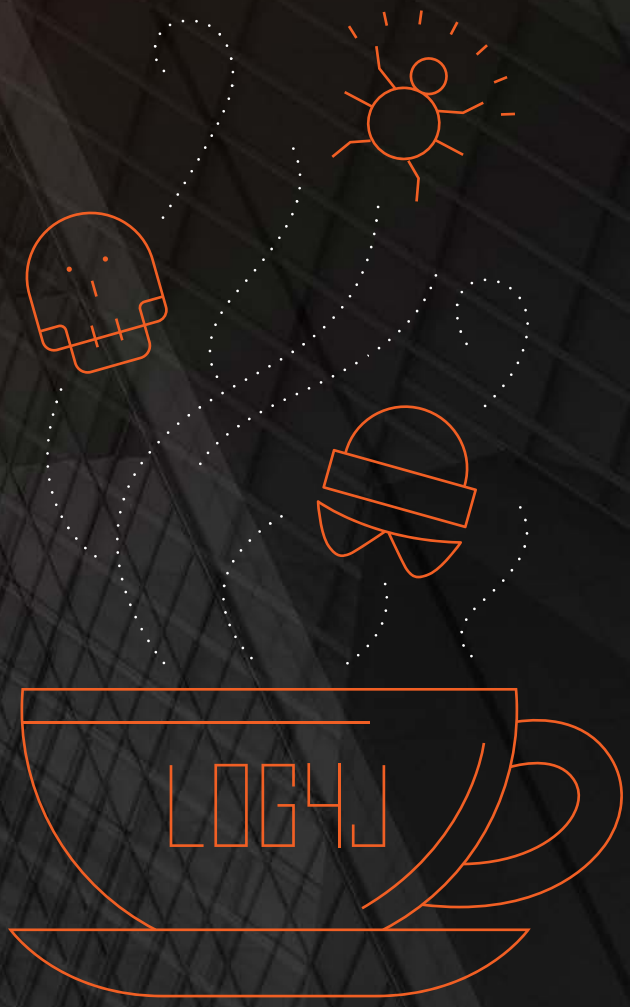
In addition to high-profile attacks, entire campaigns have been observed from a number of groups, including:

- Hafnium: Another China-linked group, Hafnium, was exploiting the Log4Shell vulnerability as early as mid-December 2021 to attack virtualization infrastructure.
- Conti: In December 2021, Conti was observed entering a network through an alternate initial access vector. The group then exploited the Log4Shell vulnerability to move laterally and gain access to internal VMware vCenter server instances, ultimately allowing it to encrypt virtual machines.
- Lazarus: This North Korean group used a Log4j vulnerability to gain access to the networks of energy companies in the U.S., Japan and Canada. Once inside, the group installed backdoors and stole credentials and sensitive information.
- Deep Panda: The China-based APT group Deep Panda was observed in April 2022 exploiting Log4Shell to deploy a new rootkit known as Fire Chili, along with the Milestone backdoor.
- Phosphorus/Charming Kitten: In mid-January, these Iranian state-sponsored attackers exploited Log4j vulnerabilities in publicly exposed Java applications to drop CharmPower, a novel PowerShell-based modular backdoor, in order to conduct follow-on attacks.
- Aquatic Panda: A China-based APT group known for intelligence collection and industrial espionage, Aquatic Panda exploited an unpatched Log4j vulnerability in an attempt to deploy malware within a "large academic institution." (Fortunately, the attack was disrupted before it could succeed.)
- Islamic Revolutionary Guard Corps: Since 2021, affiliates of the Islamic Revolutionary Guard Corps — actually a primary branch of the Iranian Armed Forces — have been observed exploiting VMware Horizon Log4j vulnerabilities to gain initial access to networks. Once inside, the group typically conducts ransomware operations, including encrypting disks and exfiltrating data for later extortion. Among those successfully attacked are a U.S. municipal government and a U.S. aerospace company.

Log4j vs. Log4Shell

As media coverage of the Log4j vulnerabilities grew, so did the growth of another term: "Log4Shell." But what's the difference?

Far from being its own distinct set of vulnerabilities, Log4Shell is a nickname given to the worst of the Log4j vulnerabilities. This vulnerability, also known as CVE-2021-44228, was a zero-day remote-code execution (RCE) vulnerability with a 10.0 rating on the Common Vulnerability Scoring System (CVSS). Over time, the name "Log4Shell" has also been used by some to describe the entire suite of vulnerabilities discovered in the Apache Log4j Java-based logging utility.



UKRAINE

Ukraine Sees Unprecedented Attack Volume in 2022

While the Russia-Ukraine conflict may have resulted in suppressed ransomware attack volume in the rest of the world, it had a dark side: It sent attack levels through the roof in Ukraine, as cyber warfare zeroed in on both military targets and critical civilian and communication infrastructure.

Because SonicWall requires a minimum of 1,000 active sensors in a region for public reporting, and our footprint in Ukraine falls far short of that threshold, we don't generally report on cybercrime in Ukraine. But amid the ongoing conflict, the sensors we do have there recorded an enormous amount of malicious activity.

Despite Ukraine's relatively small number of sensors, the country appears high in the rankings when compared with other nations. With 7.1 million attacks in 2022, Ukraine ranks No. 13 in total ransomware volume, and also had the third-highest ransomware spread percentage at 2.23%.

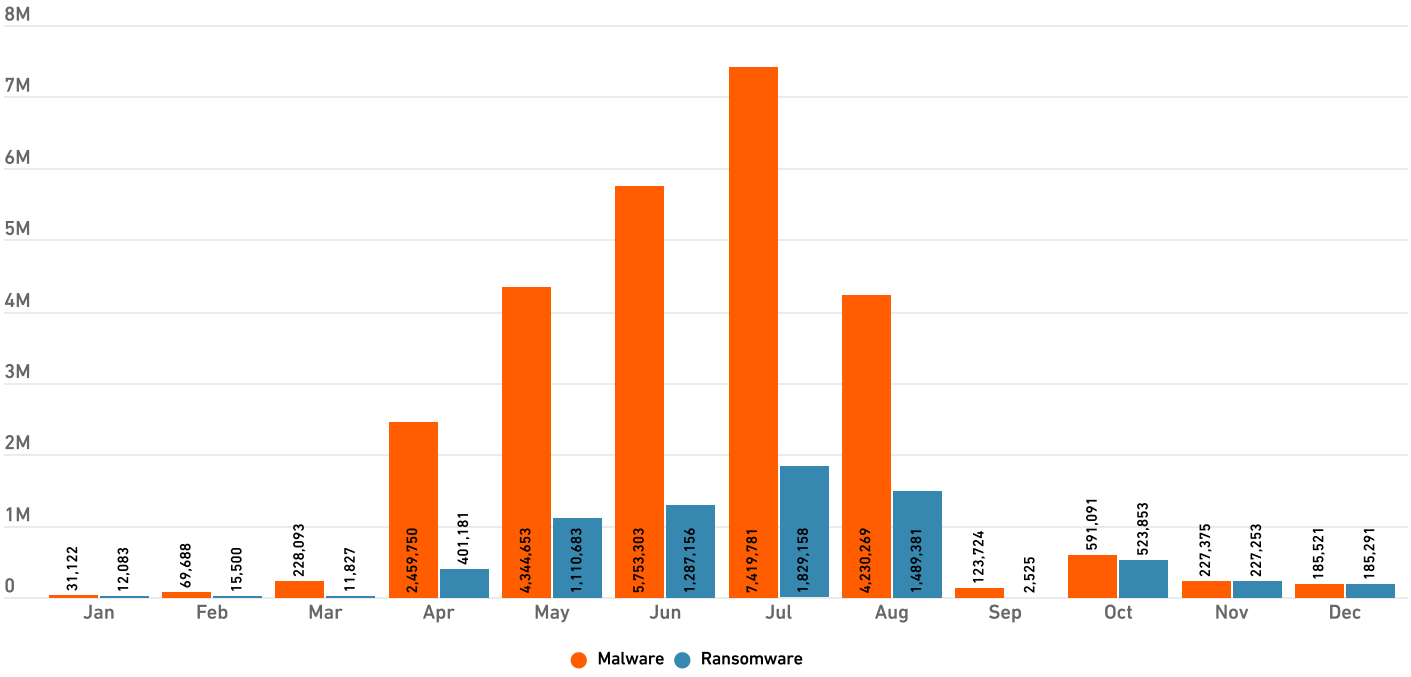
These numbers were fueled by a massive 8,105% increase in total malware and a 5,835% increase in ransomware.

Along with other Eastern European countries, Ukraine was once given preferential treatment among certain threat actors, with a number of examples specifically sparing those living in the region.

The opposite seemed to be true in 2022, however, as SonicWall observed several attacks targeting Ukraine directly:

- Caddywiper Hits Ukrainian Networks, Wipes Data and Renders Machines Unbootable
- A Look at PartyTicket Ransomware Targeting Ukrainian Systems
- HermeticWiper Data Wiping Malware Targeting Ukrainian Organizations

2022 Attack Volume | Ukraine



Note: Threshold for statistical relevancy not met. SonicWall typically requires minimum of 1,000 active sensors for public reporting.

BREACH AND ATTACK SIMULATION

Cybercriminals Shifting from Cobalt Strike to Sliver

The practice of using legitimate system administration, forensic or security tools to conduct cyberattacks has become so ubiquitous that it even has a name: "Living off the Land (LotL) attacks."

This method is attractive because the necessary tools are already deployed and available for threat actors, allowing them to operate without raising suspicion. And because they're legitimate tools/binaries/scripts, they're significantly less likely to be flagged as malicious by anti-malware solutions. For instance, legitimate NetCat — a tool used by system admins to transfer data, test and troubleshoot networks — also allows threat actors to surreptitiously enumerate internal networks with scanning, create a backdoor as a persistence mechanism, and even exfiltrate data.

In a similar fashion, threat actors have increasingly utilized legitimate offensive security tools such as Cobalt Strike, a commercial penetration testing tool that allows security teams to replicate the tactics and techniques of advanced adversaries in a network. Over the past several years, the abuse of Cobalt Strike has skyrocketed, increasing by 161% between 2019 and 2020 alone.

But Cobalt Strike has several *strikes* against it. Due to its widespread adoption and use in high-profile attacks such as SolarWinds, there's been an increased focus on detecting and mitigating attacks using the tool.

Cobalt Strike is also quite expensive. At $5,900 per user for a one-year license, cybercriminals typically use older versions that have been cracked and pirated. This tends to make detection even easier — because paying customers are generally running the latest version of Cobalt Strike, the use of older versions is often a breach indicator.

Ever on the lookout for better ways to evade cyber defenses, attackers have recently begun to supplement or replace Cobalt Strike with a similar (but more obscure) tool, known as Sliver, in their attacks.

What is Sliver?

Like Cobalt Strike, Sliver is a platform designed for adversary simulation, but with the added benefits of being more obscure and open source. Because the framework is written in Golang, it's cross-platform compatible and available for Microsoft Windows, MacOS and Linux operating systems. Sliver's implants supports broad command and control paths (C2) over Mutual TLS (mTLS), WireGuard, HTTP(S) and DNS to evade detection, and are dynamically compiled with per-binary asymmetric encryption keys.

As it provides all the necessary capabilities for comprehensive adversary simulation, it's a worthy alternative for security teams — but these qualities also make it attractive to attackers.

How Attackers Use Sliver

Sliver is generally regarded as more flexible and easier to use than Cobalt Strike. After compromising a victim's network, the attacker deploys implants (essentially Sliver payloads) inside the target's servers or endpoints, then uses Sliver for C2 interactions. Cross-platform implants can be generated in several formats, including executable file, shellcode, shared library/DLL file or service.

These implants can be obfuscated via the 'garble' or 'gobfuscate' libraries, making them harder to detect. But even when detected, this obfuscation can significantly increase analysis time — while researchers have created tools that can help de-obfuscate strings in payloads, according to Microsoft, it remains a fairly manual process.

Sliver also supports the use of stagers, which are the smaller payloads used by C2 frameworks to limit the amount of code used in an initial payload. Stagers retrieve and launch full-sized backdoors and are useful for things like phishing emails, but they also make file-based detection more difficult.

Sliver is also highly customizable — another quality attackers find attractive. According to Microsoft, operators aren't limited to Sliver's default DDL or executable payloads. "Motivated threat actors can generate a Sliver shellcode and embed it in custom loaders like Bumblebee that then run the Sliver implant on a compromised system," the company said.

Once Sliver is deployed, it offers attackers full access to the target system, allowing it to conduct subsequent steps in the attack chain.

Who's Using Sliver?

While Sliver was introduced in mid-2019, its use among cybercriminals didn't start picking up until 2021, when its adoption was spearheaded by powerful nation-state actors.

- **Cozy Bear/The Dukes/APT29:** This group is part of Russia's foreign intelligence service, the SVR, and has attacked organizations in the U.S., U.K., Europe and elsewhere. It was among the first high-profile groups to attack using Sliver: After a July 2020 joint government report on the attempted sabotage of COVID-19 vaccine development described the group's methods in detail, it reportedly adopted Sliver as part of a larger change in tactics, techniques and procedures (TTP).
- **DEV-0401/Bronze Starlight:** This China-based APT group began replacing Cobalt Strike with Sliver in June 2022. Unlike other Ransomware-as-a-Service (RaaS) operators, this group is involved in every stage of the attack cycle — however, researchers suspect that the ransomware is merely a decoy to hide its true objectives, such as intellectual property theft and espionage.
- **Exotic Lily:** What sets this group, likely based in central or eastern Europe, apart is that it isn't known to exploit vulnerabilities — instead, members pose as employees of legitimate companies, complete with social media profiles and AI-generated photographs. Spoofed email accounts are then used to deliver the attack payload within spearphishing emails.
- **DEV-0237/FIN12:** This RaaS affiliate group is known for deploying a wide variety of payloads, including Hive, Ryuk, Conti and others. The group has replaced Cobalt Strike with Sliver in its attacks, and has been observed using it in conjunction with the SystemBC RAT.
- **TA551/Shathak:** This group acts as an initial access broker. It uses malicious macros placed in Microsoft Office documents that, if enabled, are capable of directly loading the Sliver framework.

To be clear, Cobalt Strike is still king, and likely will be for some time. But as defenders and antimalware and EDR solutions continue to improve their abilities to detect it, we expect to continue seeing a shift to Sliver, as well as other C2 frameworks such as Brute Ratel and PoshC2.

Key Findings from 2022

▲2%

Malware

Malware rose for the first time since 2018, reaching 5.5 billion attacks — a 2% increase year over year. Skyrocketing cryptojacking and IoT malware rates fueled much of this jump.

READ MORE ON PAGE 21. »

▼21%

Ransomware

On the heels of 2021's meteoric highs, ransomware fell in 2022, with volumes dipping to 493.3 million. While this represents a 21% year-over-year decrease, it's still far above the levels seen in 2017, 2018, 2019 or 2020.

READ MORE ON PAGE 33. »

465K

RTDMI Discoveries

SonicWall's patented Real-Time Deep Memory Inspection™ discovered 465,501 never-before-seen malware variants in 2022. This new high-water mark pushed the all-time detection total past the 1 million mark.

READ MORE ON PAGE 42. »

139M

Cryptojacking

As cybercriminals shifted to lower-profile revenue sources in 2022, the number of cryptojacking attempts rose to a record high of 139.3 million.

READ MORE ON PAGE 44. »

Key Findings from 2022

△87%

IoT Malware

With the number of connected devices continuing to rise, IoT malware jumped 87% year over year to a new high of 112.3 million.

READ MORE ON PAGE 59. »

△19%

Intrusions

The number of overall intrusion attempts in 2022 hit 6.3 trillion, a 19% increase over 2021's total. Fortunately, however, the number of *malicious* intrusions fell 10%.

READ MORE ON PAGE 52. »

△35%

Malicious PDF and Office Files

SonicWall Capture Advanced Threat Protection (ATP) sandbox recorded a 35% increase in the number of new PDF-based attacks in 2022. These attacks now make up 19% of total malicious files identified by Capture ATP.

READ MORE ON PAGE 56. »

▽17%

Phishing

Phishing decreased 17% globally in 2022, with Financial/ Mortgage, Cryptocurrency, Healthcare and Pandemic the top themes for malicious emails.

READ MORE ON PAGE 66. »

▽28%

Encrypted Attacks

Encrypted attacks fell 28% year-over-year to 7.3 million, down from 10.1 million in 2021.

READ MORE ON PAGE 50. »

MALWARE

Malware Up for the First Time Since 2018

After three straight years of decline, malware reversed course in 2022, rising to 5.5 billion hits — a 2% increase year over year.

While the increase is small, it's being fueled by massive growth in two areas. In 2022, cryptojacking rose 43% and IoT malware jumped 87%. Together, these increases were more than enough to offset a 21% drop in global ransomware volume, pushing overall malware trends into positive territory for the first time since 2018.

But unlike the seismic shifts underpinning it, a quick look at the 2022 malware trend line reveals an unusual degree of stability. This is both good news and bad news: No massive jumps or upward trajectory means that, at least for the moment, malware growth isn't accelerating. But sustained levels of malware indicate that this uptick likely isn't just temporary — at least for the time being, elevated levels of malware are here to stay.

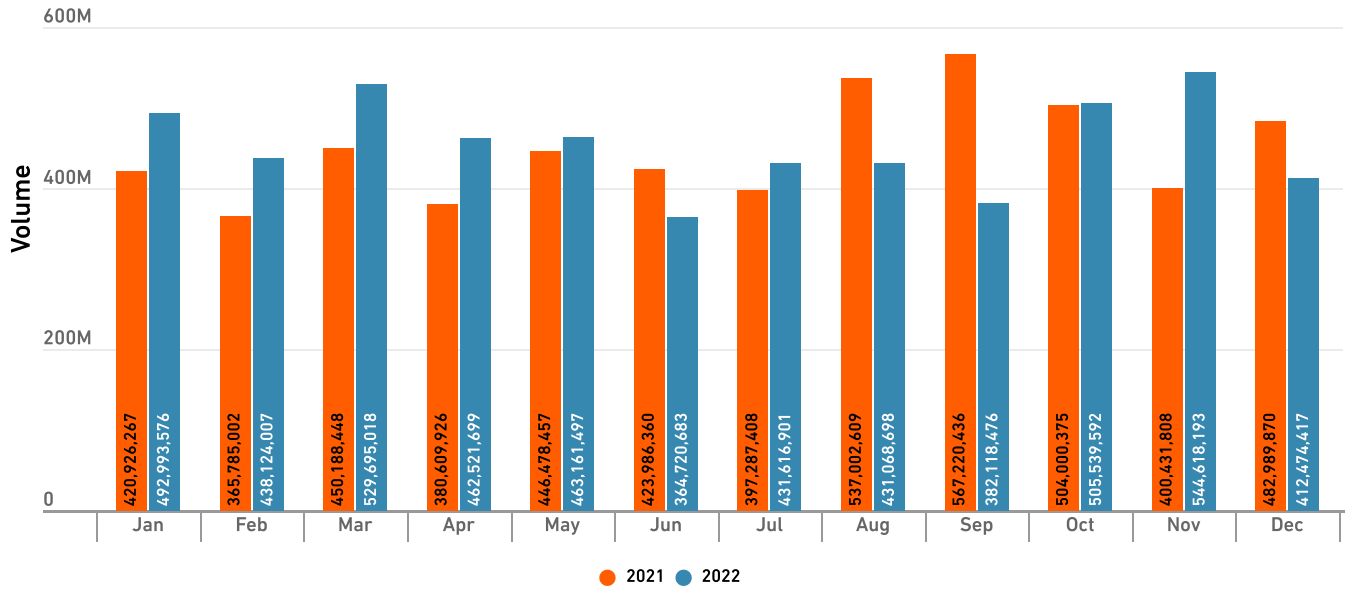
Malware by Region

In 2022, Europe, LATAM and Asia recorded double-digit increases of 10%, 17% and 38%, respectively.

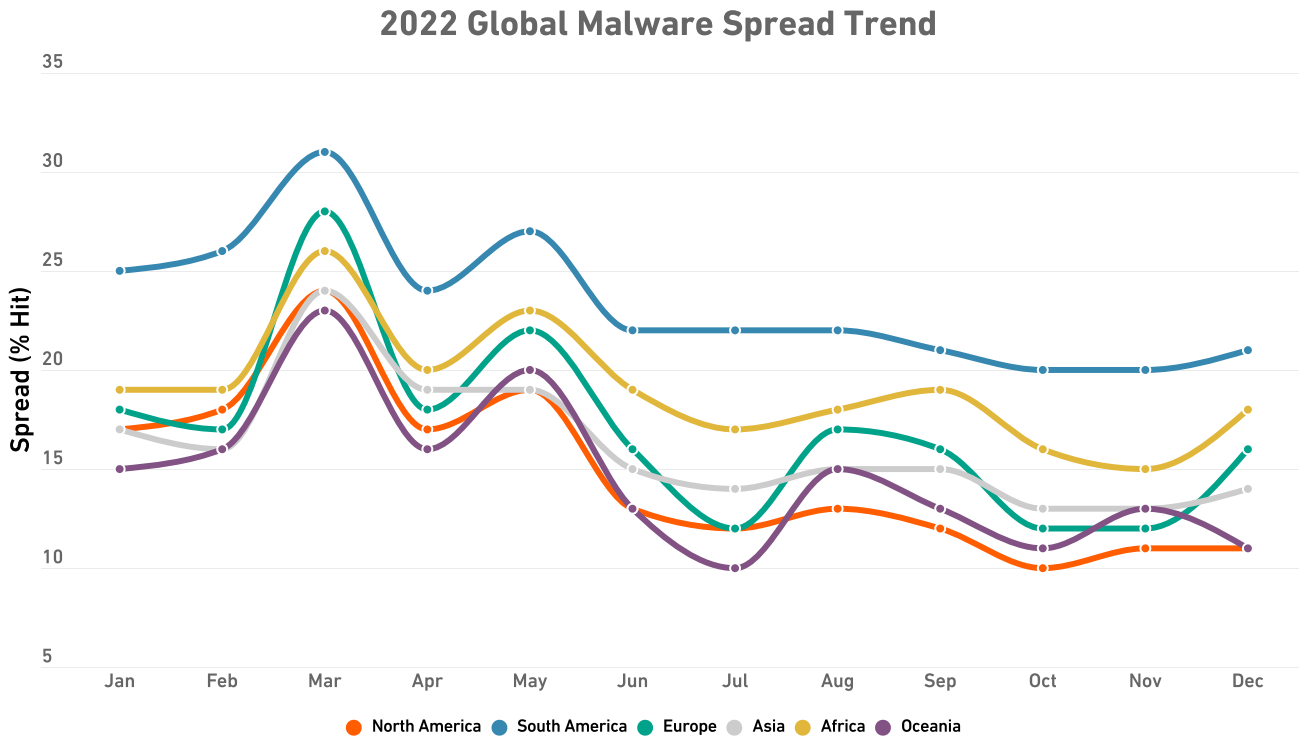
But North America, which has experienced the highest malware volume for four years running, showed a double-digit *decrease*, falling 10% year-over-year to 2.75 billion — its lowest volume since 2017.

And it's still trending downward: In December, malware attempts in North America fell to 158.9 million, the lowest monthly volume since 2018. Taken together, these trends suggest we're likely to see cybercriminals continue to shift from targets in North America and other cybercrime hotspots to elsewhere in the world.

Global Malware Volume



SONICWALL



What is Malware Spread?

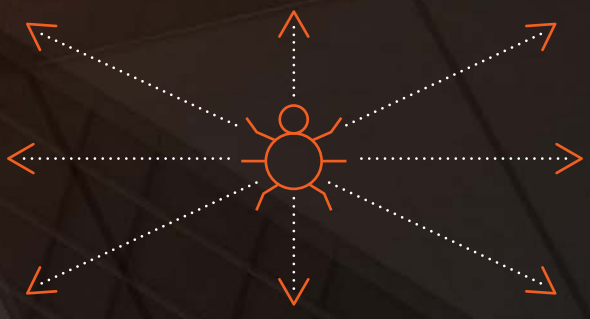
The data on the following pages offers a look at some of the countries with the highest malware volume. But just because a country sees a higher number of attacks doesn't mean that you're more likely to be targeted there.

Malware totals are useful in calculating trends, but they're of limited utility when determining relative risk: They ignore factors such as size, population, number of sensors and more.

To figure out the odds of a given organization in a particular area seeing an attack, we use the malware spread percentage — a calculation of what percentage of sensors recorded a malware attack.

If we think of malware volume as being similar to the total amount of rainfall in a region, then malware spread percentage could be compared to the probability or precipitation, or "chance of rain."

In other words, while annual precipitation numbers can be useful in determining whether your area saw more rainfall than it did last year, it says nothing about whether your umbrella will see heavier use than your sunglasses. As with "chance of rain," malware spread percentage considers a variety of additional factors to provide a more meaningful risk assessment.

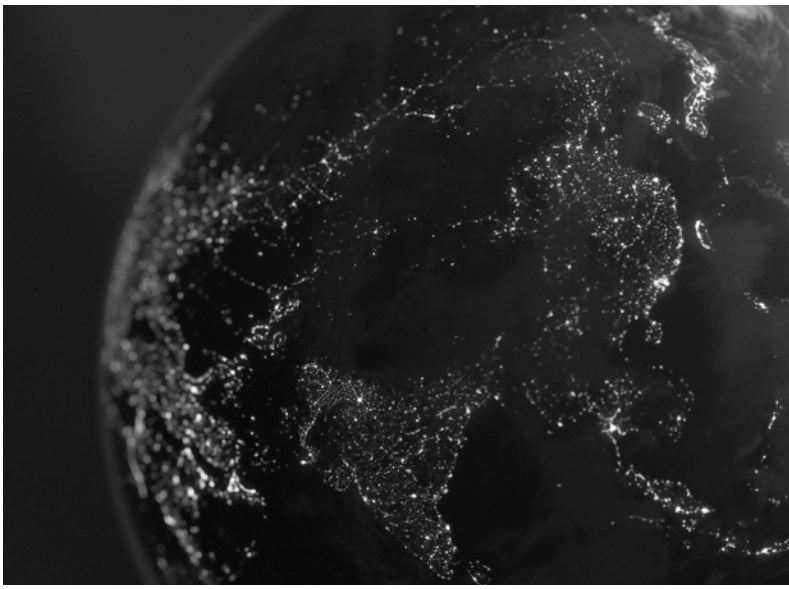


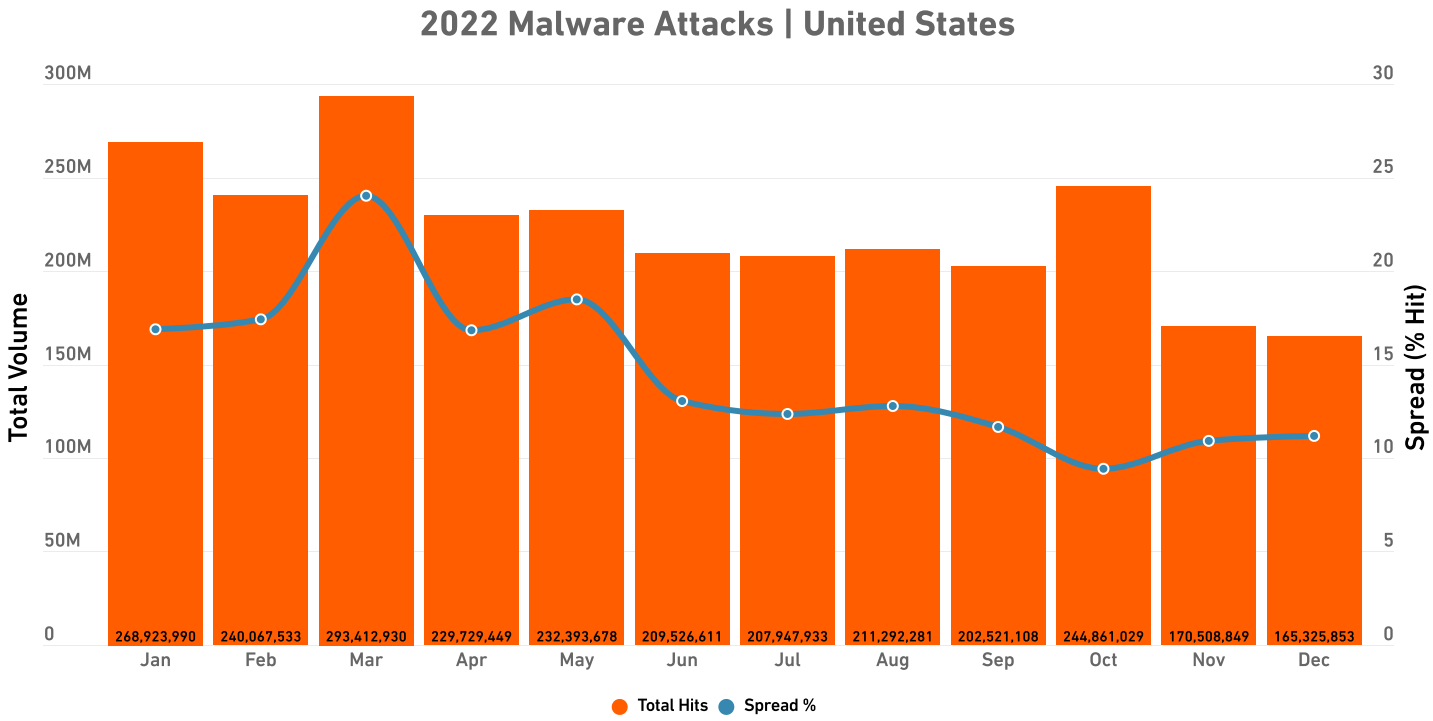
Malware Volume By Country

As in most years, 2022's country-level data showed a huge variety in outcomes, each of which contributes to the overall shifts we're seeing at the regional and global level.

To help illustrate the variety of ways that malware trends evolved over the past year, we looked at a sample of eight countries in a variety of regions, some near the top of the list in terms of malware volume, and some further down.

Despite their differences, these countries all happen to share two things in common. In each one, malware spread peaked in March, and each one had a lower average malware spread percentage in the second half than in the first half — which, considering there is no corresponding drop in volume, suggests that these attacks are becoming more targeted over time.



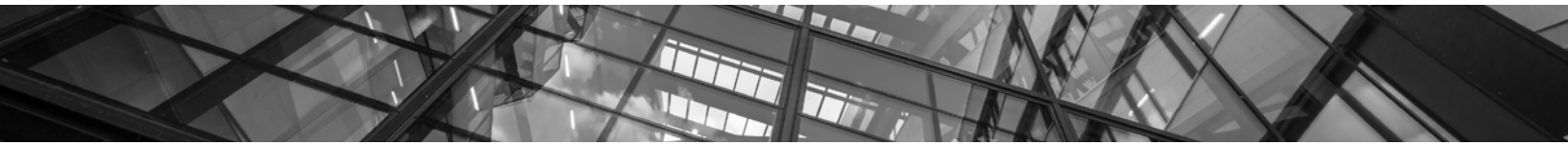


MALWARE RANK
1

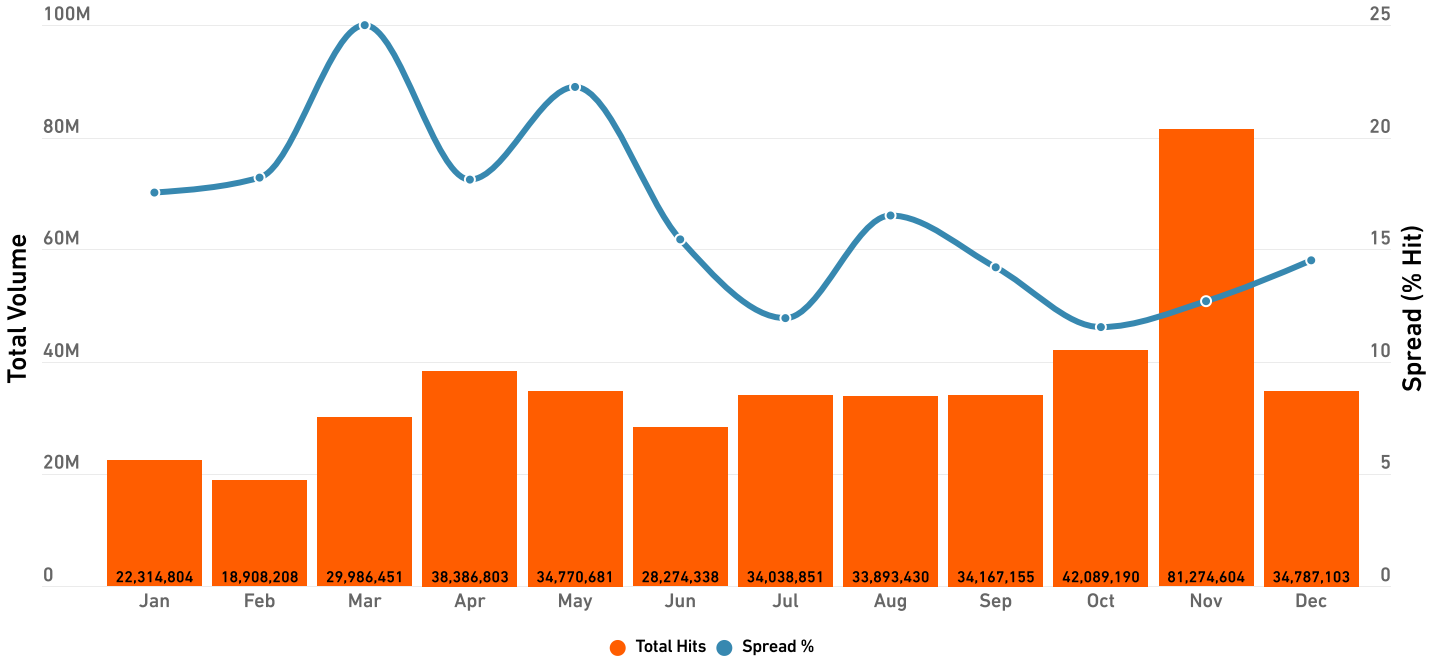
2022 ATTACK VOLUME
2.68 BILLION

YoY CHANGE
-9%

After averaging more than 250 million in the first quarter, malware in the U.S. trended downward as cybercriminals began targeting other areas.



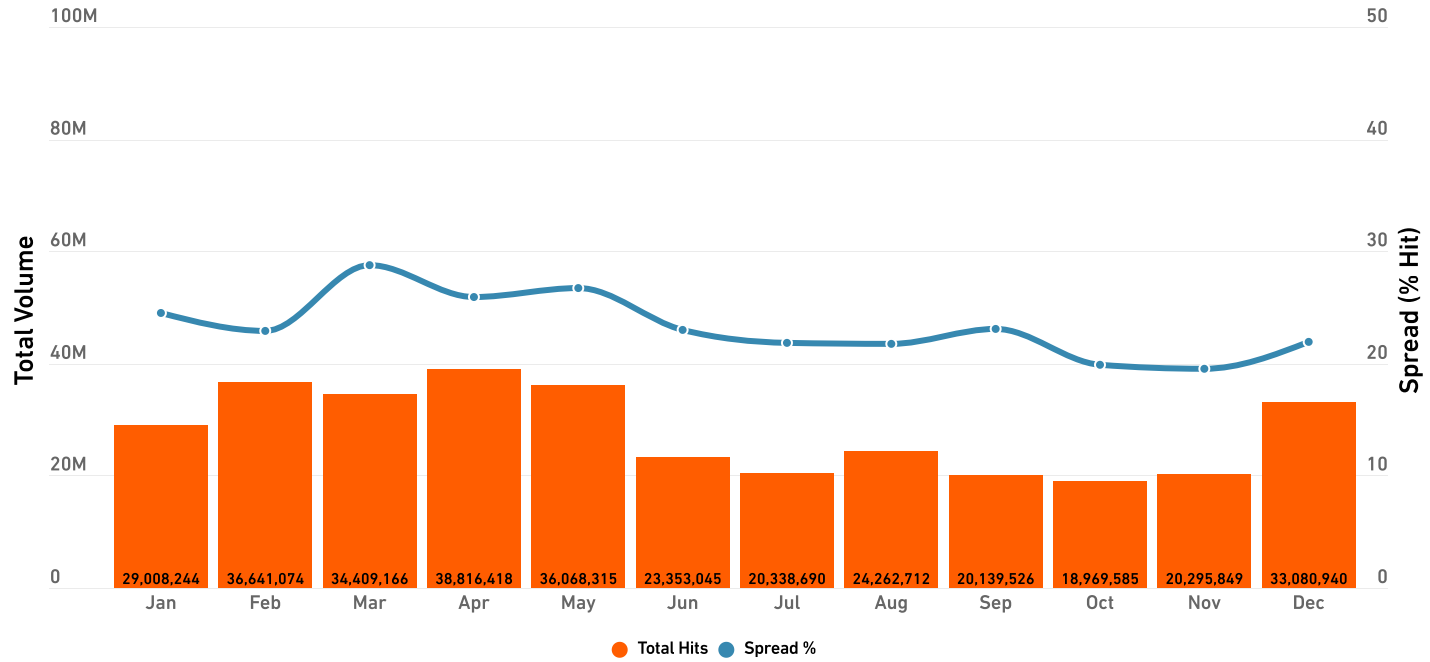
2022 Malware Attacks | United Kingdom



MALWARE RANK	2022 ATTACK VOLUME	YoY CHANGE
2	432.9 MILLION	-13%

Malware in U.K. trended upward as 2022 went on, with Q4's totals up 122% from Q1's. But low volume in the first half contributed to an overall year-over-year decrease.

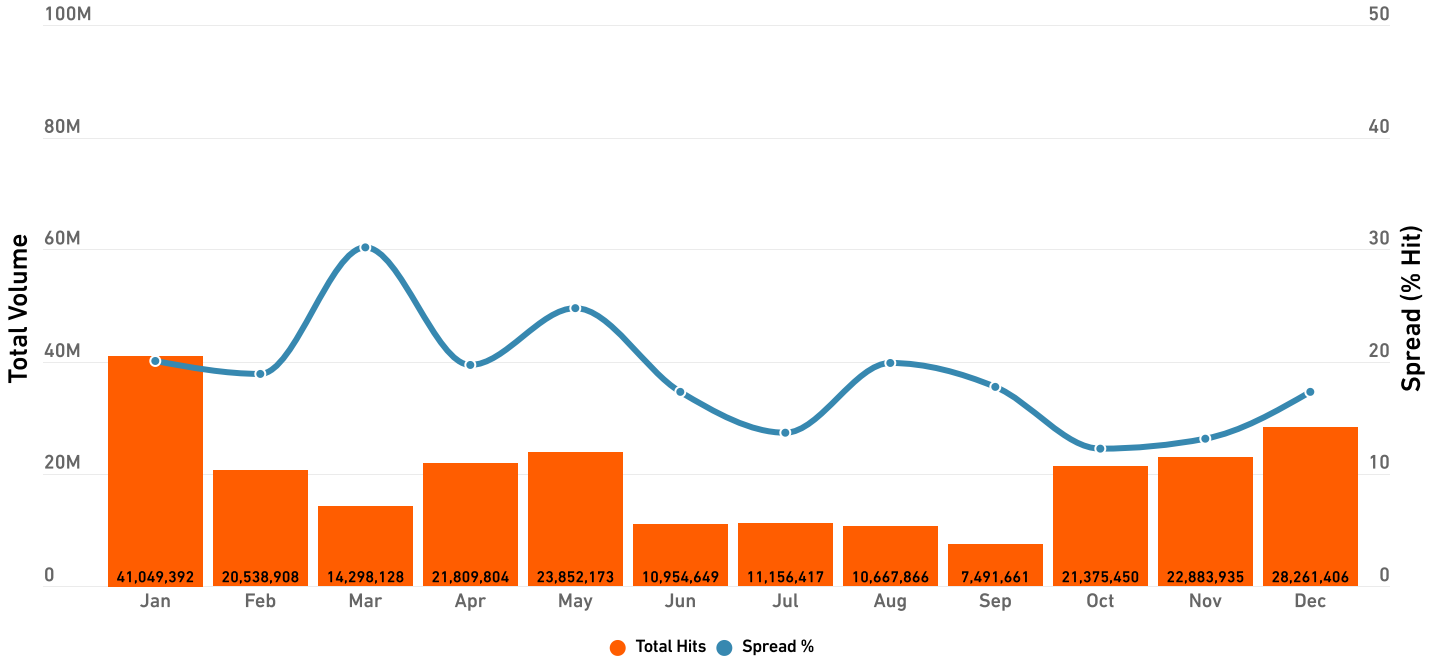
2022 Malware Attacks | India



MALWARE RANK	2022 ATTACK VOLUME	YoY CHANGE
3	335.4 MILLION	+31%

Despite attack volumes mostly trending downward in 2022, India experienced the largest attack volume increase of any country we studied.

2022 Malware Attacks | Germany



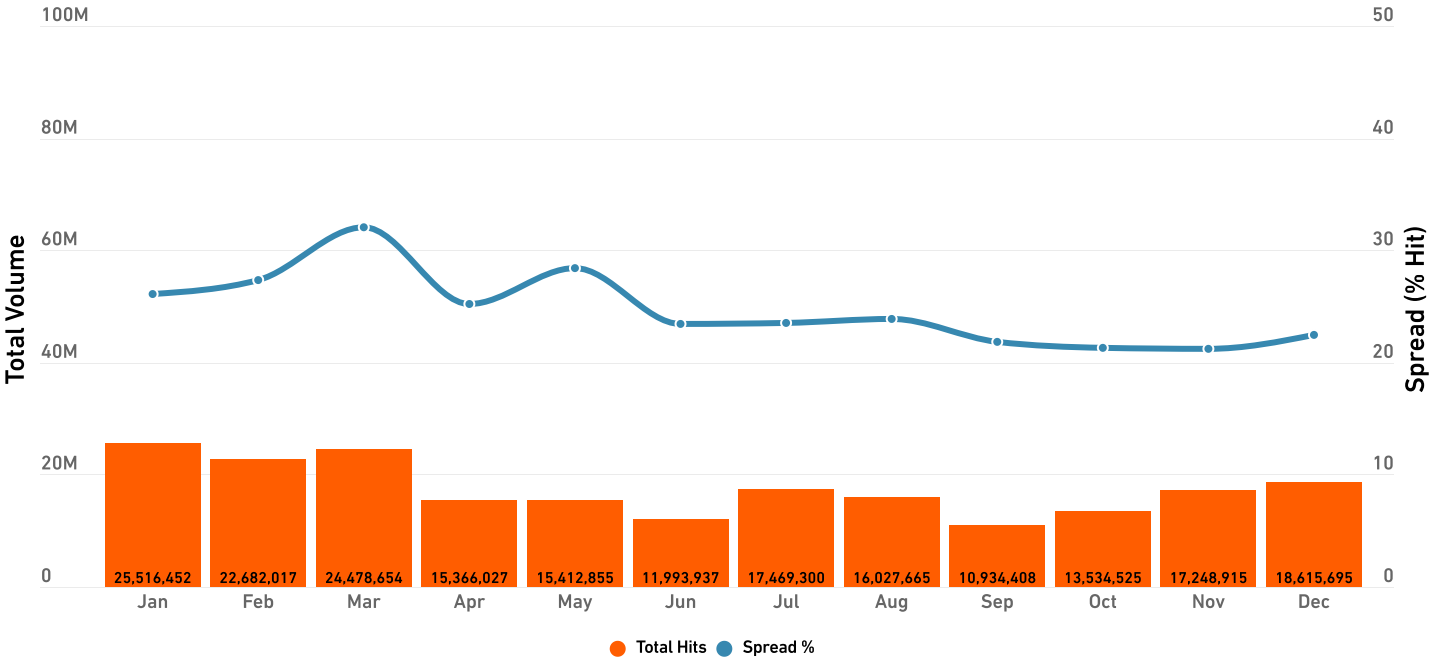
MALWARE RANK
4

2022 ATTACK VOLUME
234.3 MILLION

YoY CHANGE
-28%

While attacks rebounded in Q4, it wasn't enough to offset unusually low Q2 and Q3 volumes. The resulting 28% drop was the biggest decrease of any country we studied.

2022 Malware Attacks | Brazil



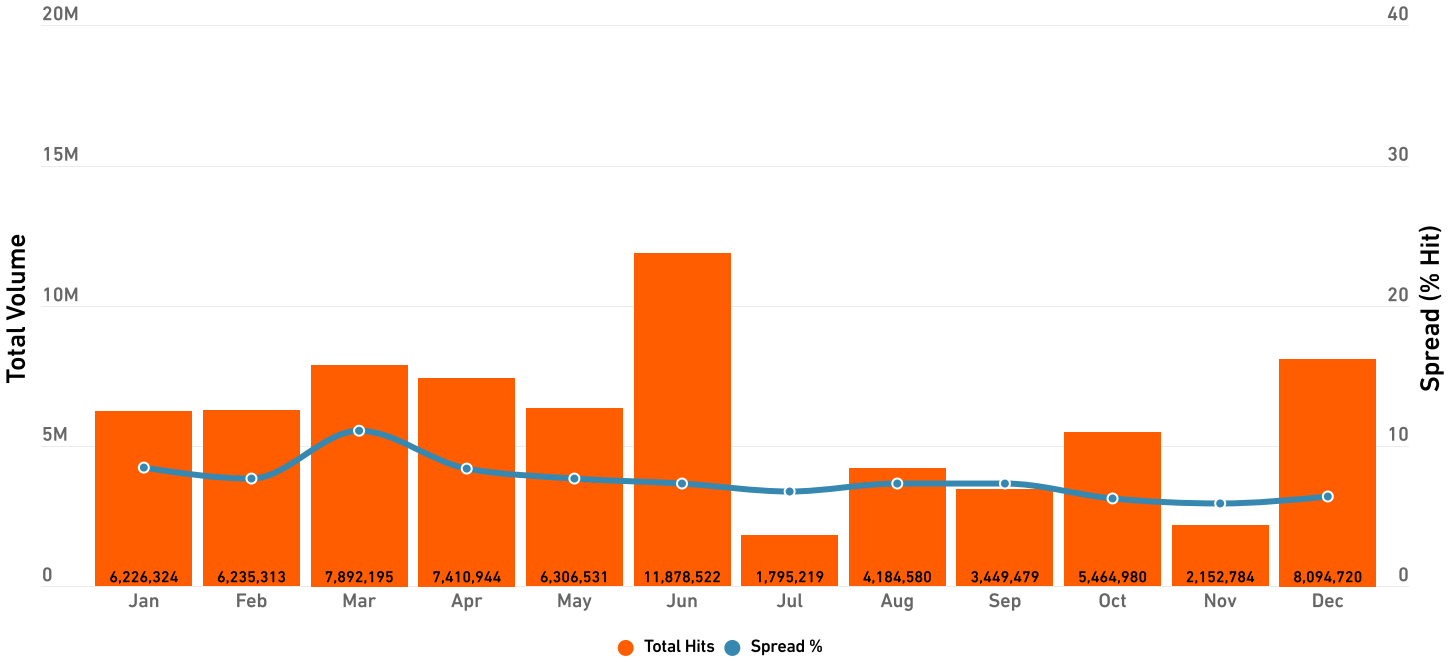
MALWARE RANK
6

2022 ATTACK VOLUME
209.3 MILLION

YoY CHANGE
-1%

With a difference of just 1.4 million between 2021's malware total and 2022's, yearly attack volume was essentially flat.

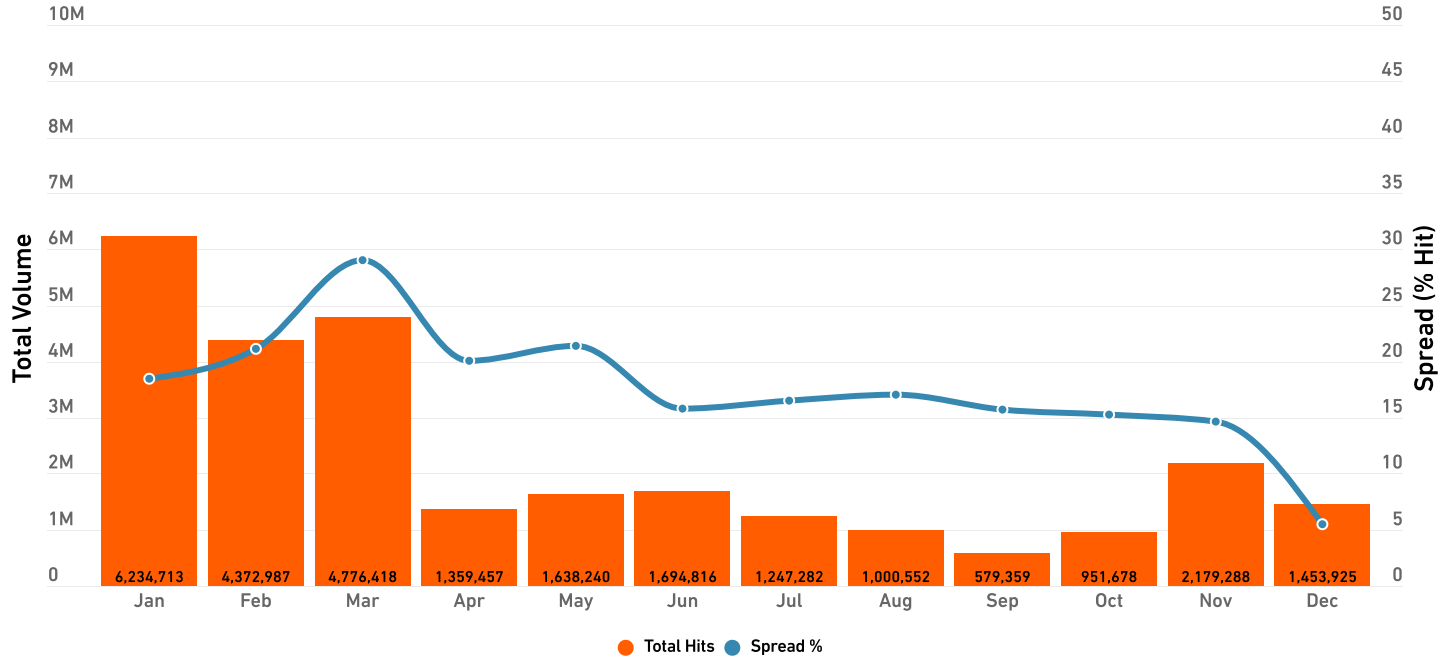
2022 Malware Attacks | United Arab Emirates



MALWARE RANK	2022 ATTACK VOLUME	YoY CHANGE
12	71.1 MILLION	-14%

While malware in UAE dropped in 2022, this comes on the heels of a 33% increase in 2021 — meaning the region is still seeing dramatically higher malware.

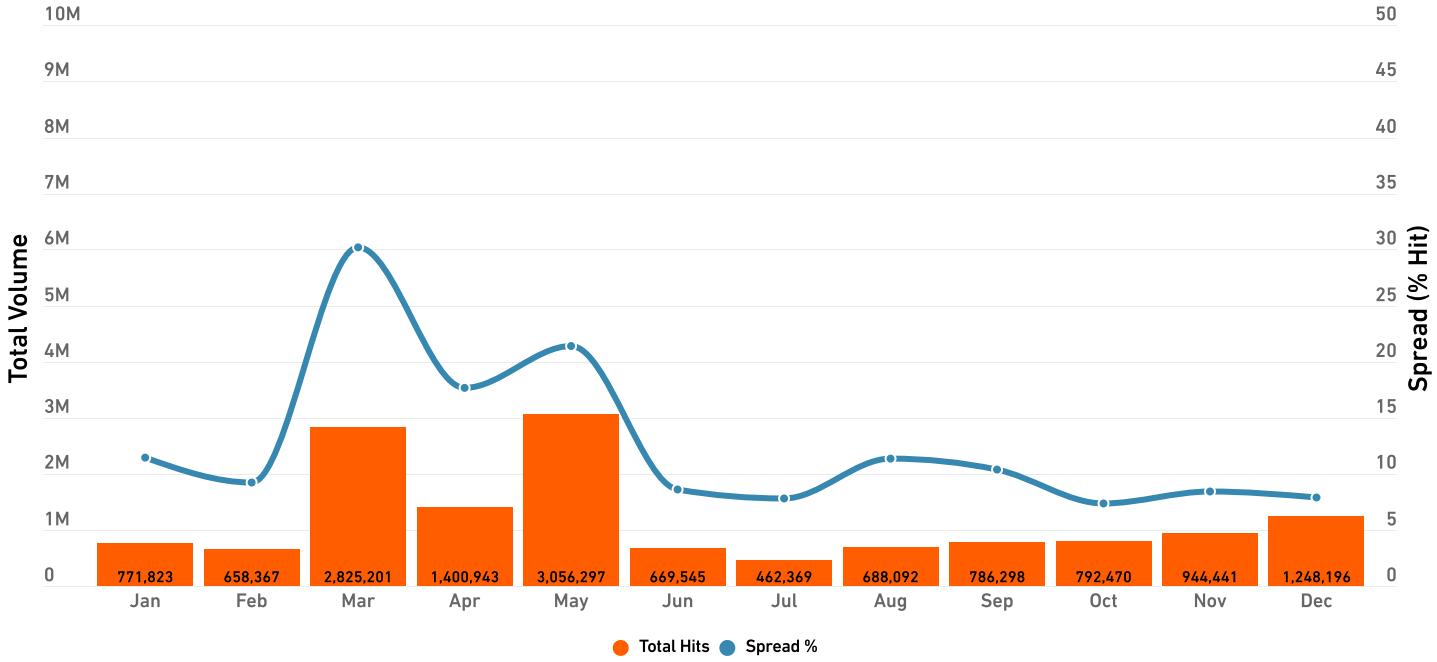
2022 Malware Attacks | Mexico



MALWARE RANK	2022 ATTACK VOLUME	YoY CHANGE
21	27.5 MILLION	-14%

Malware in Mexico has recently reversed course: After increasing 73% in 2020, it increased just 3% in 2021, then dropped in 2022.

2022 Malware Attacks | Japan

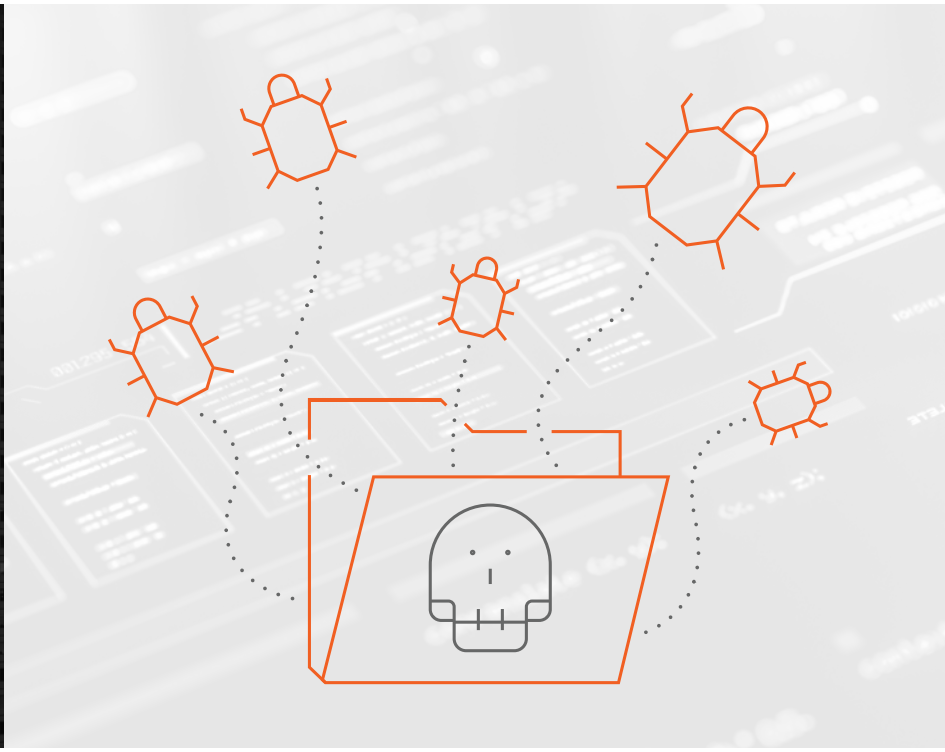


MALWARE RANK	2022 ATTACK VOLUME	YoY CHANGE
32	14.3 MILLION	+2%

In March, malware spread in Japan spiked to just over 30% — though the yearly average was just under 13%.

Top 10 Malware File Names

1. purchase order.exe
2. soa.exe
3. invoice.exe
4. swift copy.exe
5. quotation.exe
6. img-order-confirmation-pdf.exe
7. payment copy.exe
8. ziraat bankasi swift mesaji.exe
9. shipping documents.exe
10. new order.exe



Malware Spread by Country

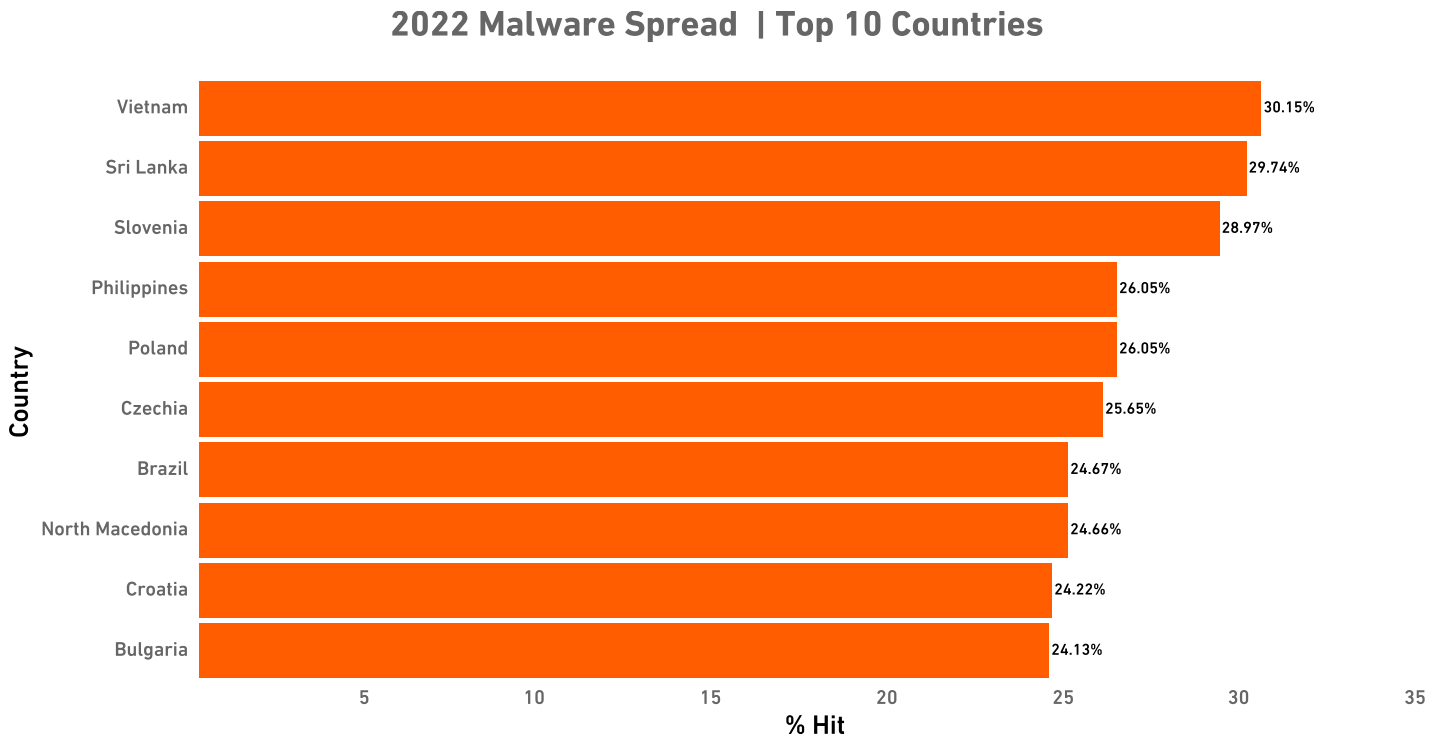
Despite seeing a decrease in malware volume in 2022, the U.S. and U.K. are still the countries with the highest malware volume. But based on our malware spread data, an organization is most likely to see a malware attempt in Vietnam: 30.2% of customers there were targeted in 2022.

But while the same three countries — Vietnam, Sri Lanka and Slovenia — topped the malware spread list in 2022 as they did in 2021, there's a lot of variation further down the rankings. Most notably, the rise of Europe as a new cybercrime hotspot is showing up in SonicWall's malware spread data as well. Between 2021 and 2022, the number of European countries on the list doubled, and European countries now make up a majority of the top 10.

We're also continuing to see malware spread drop overall: Last year, the highest-ranked country had a malware spread of 36.5%. This year, it's fallen to 30.2%.

One thing remained unchanged from 2021, however: The country where you're least likely to be targeted by malware is still Luxembourg, where just 6.3% of SonicWall sensors recorded malware hits (down from 6.6% in 2021.)

BETWEEN 2021 AND 2022, THE NUMBER OF EUROPEAN COUNTRIES ON THE LIST DOUBLED, AND EUROPEAN COUNTRIES NOW MAKE UP A MAJORITY OF THE TOP 10.



Not a Safe Bet

Over the years, SonicWall Capture Labs threat researchers have observed a number of malicious apps masquerading as legitimate, including a fake McAfee app, a fake Dr. Web app and a fake version of Google Update for Android over the course of 2022.

But since Google Play store banned sports betting apps in some areas, we've observed an increase in these imposters, too. One, highlighted in our June 22 update, purports to be an app known as "Dream11." The legitimate version boasts over 130 million downloads — but since it's nowhere to be found, many have inadvertently downloaded a version laden with malware.

This app displays convincing icons and, once executed, features the correct match schedule. However, past this page, the app does not respond. Instead, it performs several malicious activities, such as allowing the malware to receive commands via SMS, reading/sending SMS, reading/deleting contacts, location tracking, audio recording, keystroke logging and more.

While SonicWall protects against this threat, we urge our users to always be vigilant when installing apps.

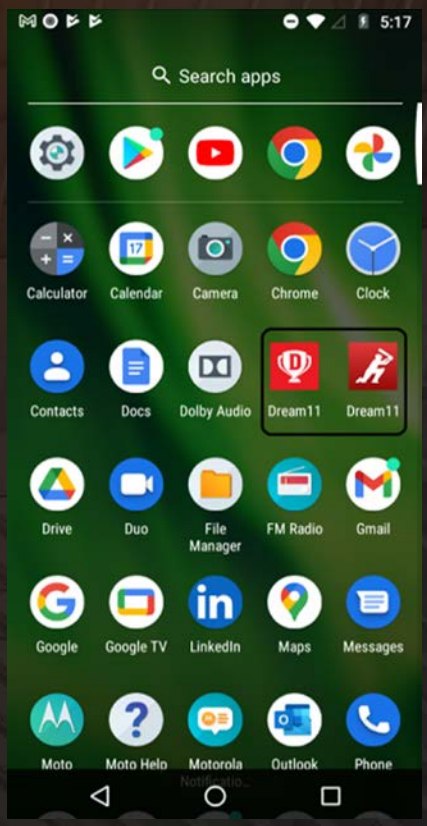


Fig. 1: Malicious app icons

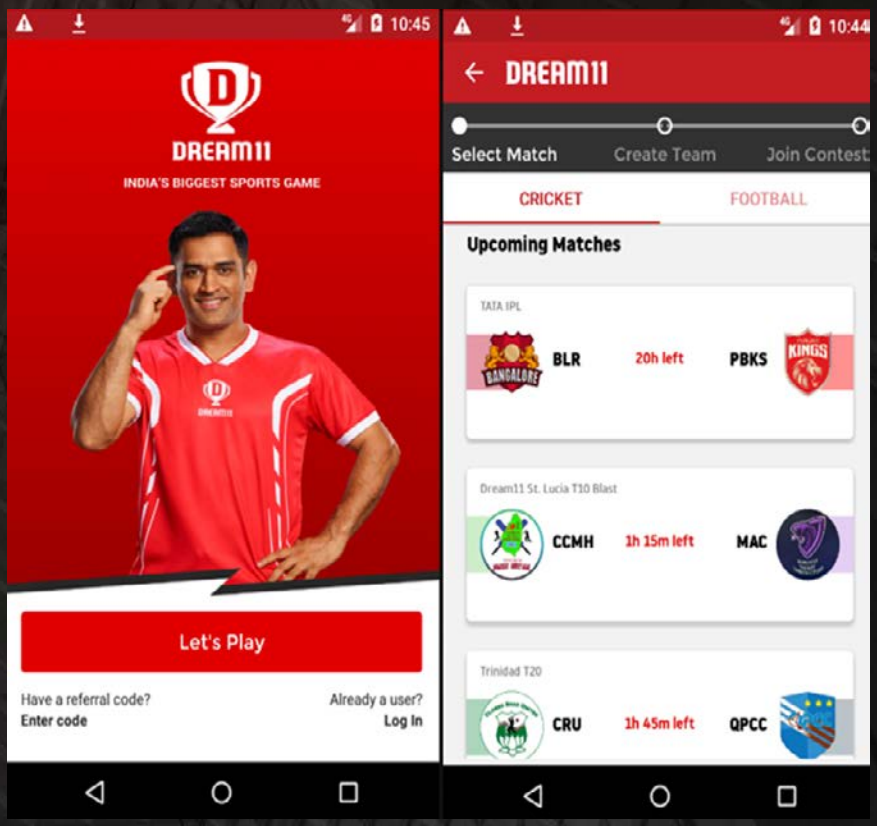
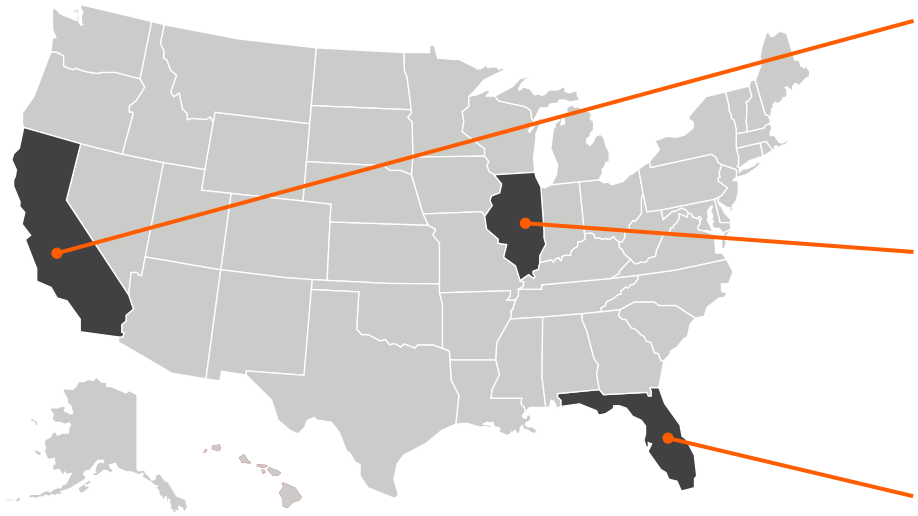


Fig. 2: Showing the correct match schedule



321M
Malware attacks in California

315M
Malware attacks in Illinois

191M
Malware attacks in Florida

Malware by State

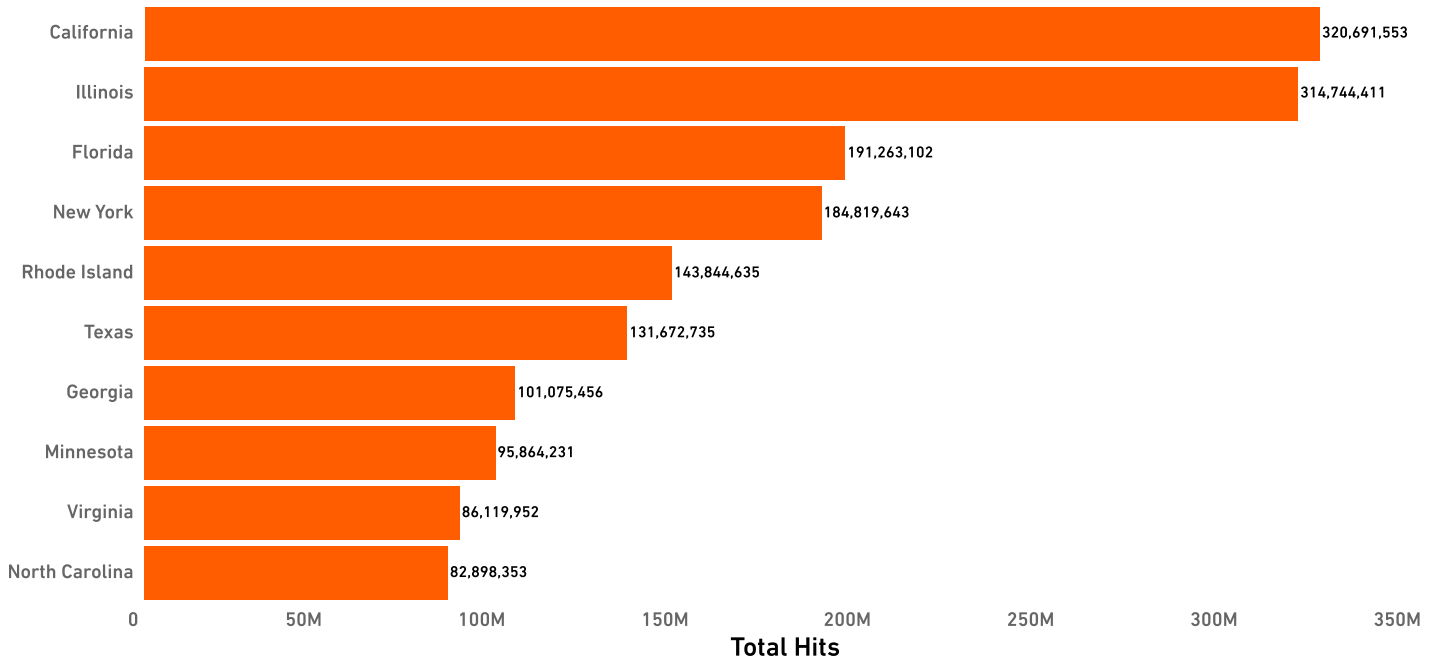
In 2021, Florida recorded 625.4 malware hits — compared with second-ranked New York, which had less than half that total. Louisiana, which rounded out the top 10, had roughly a tenth of that at 69.9 million.

In 2022, we've seen this range narrow considerably. This year, California had the worst malware attack volume, but with 320.7 million hits, it's less than half what Florida saw in 2021 — and Illinois was right behind it.

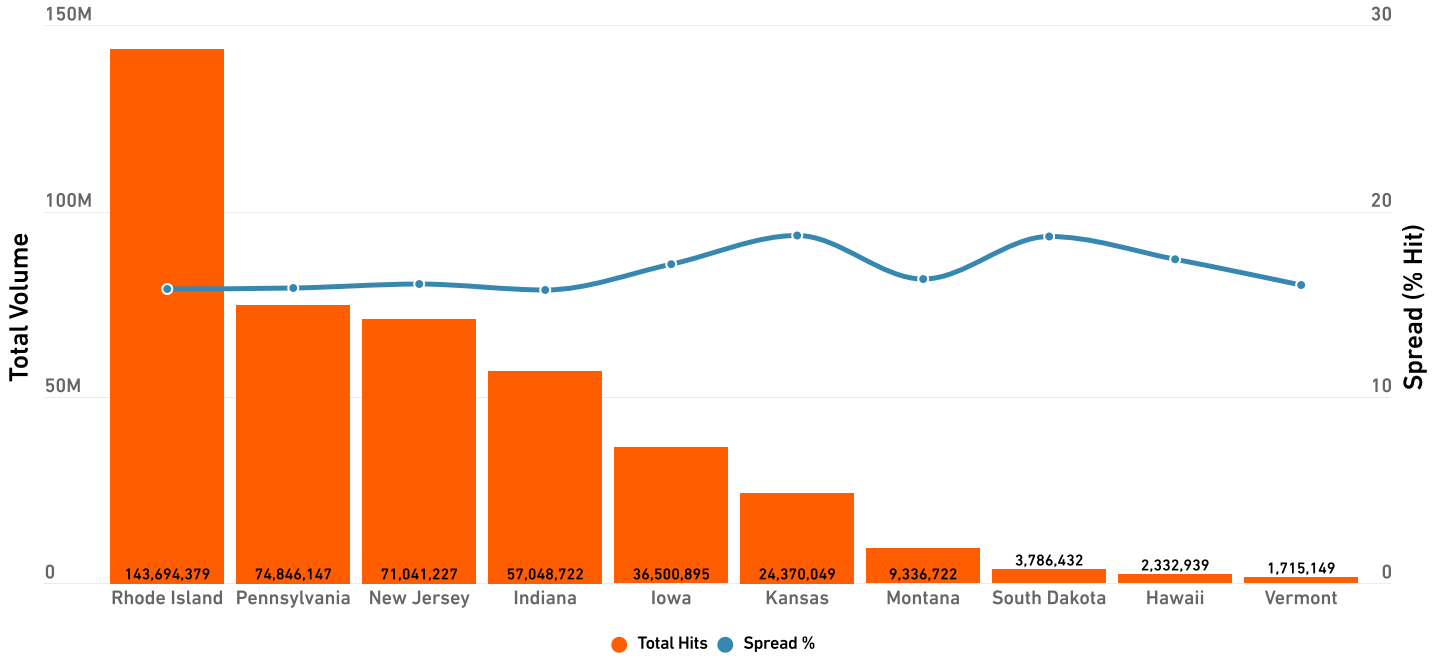
The attack volume for No. 10, however, grew: North Carolina had 82.9 million malware attacks.

This trend echoes what we're seeing at the regional and country level. States that typically experience more malware are seeing less, and states that may have once considered themselves "safe" are seeing an uptick.

2022 Malware Volume | Top 10 U.S. States



2022 Malware Spread | Top 10 Riskiest U.S. States



But once again, these states weren't actually the riskiest for malware. In fact, four of the top 10 states for malware volume appeared in the bottom 10 for malware spread, including California. (Only one state on the top-10 list for worst malware volume appears in the top-10 list for worst malware spread: Rhode Island.)

So which state is the riskiest? For the third year in a row, it's Kansas, where approximately 18.7% of SonicWall sensors logged a malware hit. Fortunately for those in the Sunflower State, however, this continues to fall: from 26.7% in 2020, to 21.4% in 2021, to 18.7% in 2022.

Conversely, Texas was the lowest: only 12.7% of sensors there logged a malware attempt.

2022 Brings Surge in Wiper Malware

SonicWall in 2022 observed an uptick in so-called wiper malware. In contrast with ransomware, intended to render files unusable until a ransom is paid, wiper malware is designed to "wipe" or render data unusable permanently.

In February, SonicWall Capture Labs threat research team analyzed a sample believed to be targeting Ukrainian organizations. Known as HermeticWiper, the malware prevents Windows from recording any information in the memory dump file and disables the VSS (Volume Shadow Copy Service, which is used to back up application data). Finally, it corrupts the first 512 bytes, the Master Boot Record (MBR) for every physical drive. It then initiates a reboot and, once completed, the missing OS prompt is displayed, leaving the system unusable.

Another wiper targeting Ukrainian networks, CaddyWiper, was analyzed by SonicWall in March. This malware iterates through files, including critical system files, and replaces their contents with null bytes. Once the data is overwritten, the physical drive is also overwritten with null bytes, rendering the machine unbootable.

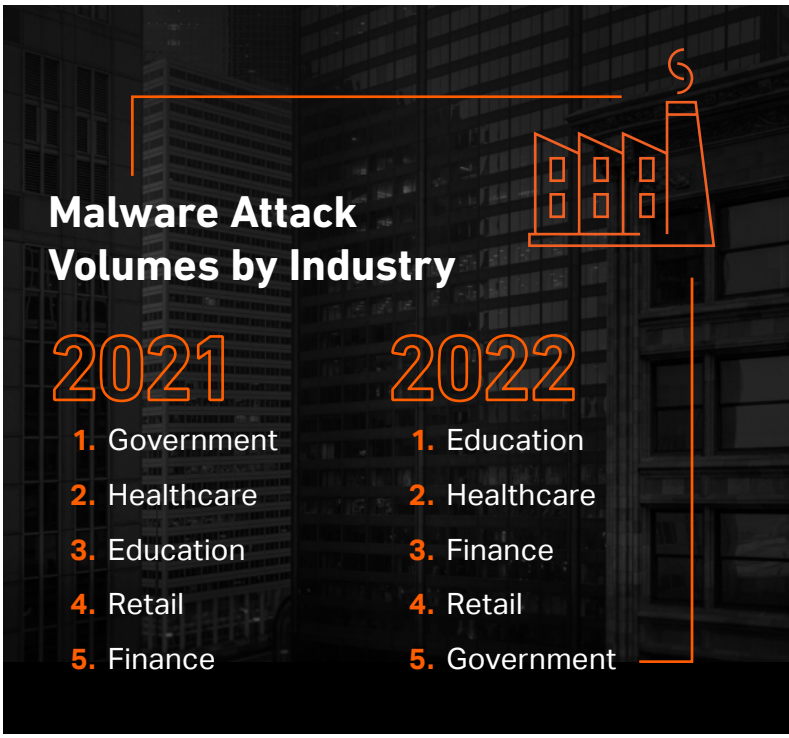
In October, SonicWall analyzed yet another wiper, this one a multicomponent infection purporting to be a picture. It arrives as a file titled "SexyPhotos.jpg," but is actually a self-extracting archive. While a ransom note is displayed, the malware only gives the appearance of encrypting files — instead, it's intended to delete all data on a given drive.

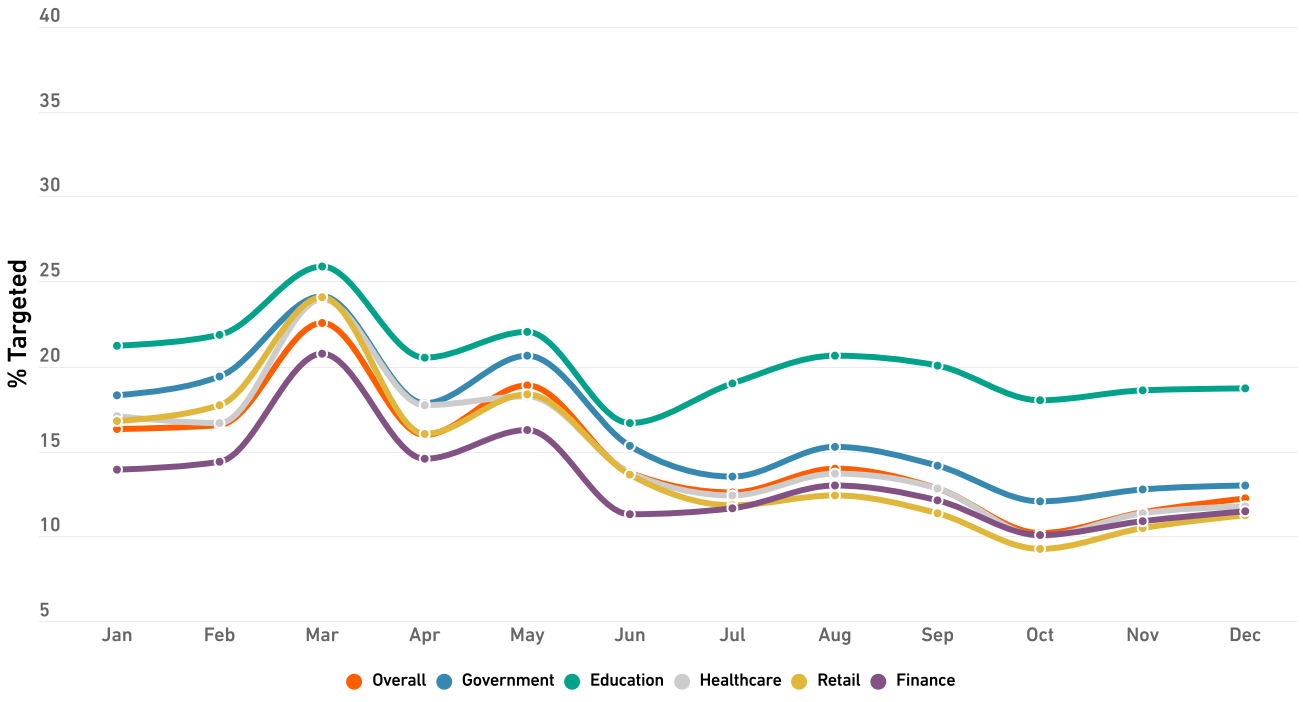
Malware by Industry

Malware targeting those in the healthcare industry fell 15% year over year, while government customers saw an even larger drop of 58%. Retail and finance, on the other hand, experienced double-digit increases, with overall malware attack volume rising 50% and 86%, respectively.

The largest increase, however, was in education, where malware volume jumped 157%. But this is actually the average of two outcomes: Attacks targeting higher education customers rose a (relatively) modest 26%, while attacks targeting K-12 institutions skyrocketed 323%.

When it comes to the average percentage of customers targeted by malware in 2022, every industry we studied showed a decrease from 2021's average. The percentage of healthcare customers targeted in 2022 slightly edged out the percentage of retail customers targeted, but the rankings remained otherwise unchanged.





RANSOMWARE

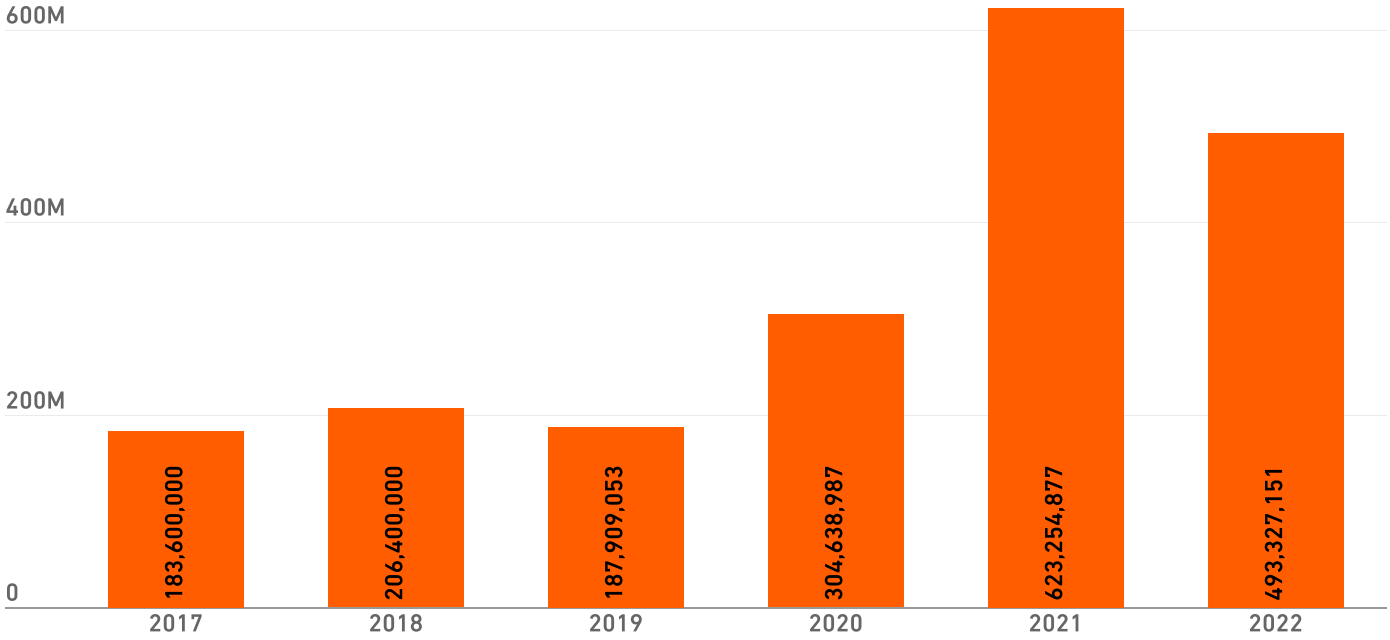
Ransomware Reverses Course

2022 brought a bit of a reprieve from 2021's sky-high ransomware volumes. In 2022, SonicWall Capture Labs threat researchers recorded 493.3 million ransomware attempts, down 21% year-over-year.

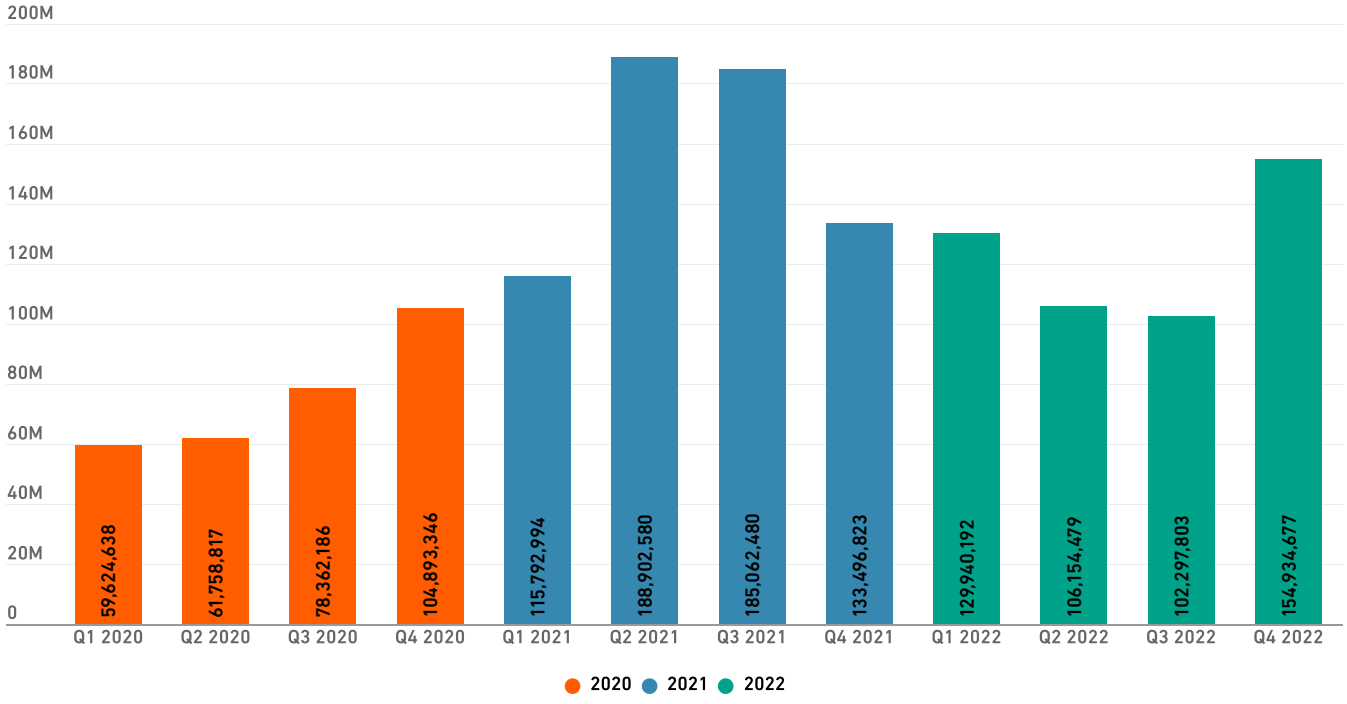
Unfortunately, however, we're already seeing signs of a potential reversal. After ransomware bottomed out in June, bringing the lowest attack volume we'd seen since July 2020, the trend line began reversing. When attacks doubled between September and October, it pushed Q4 ransomware totals to 154.9 million — the highest quarter we've seen since Q3 2021.

This is especially concerning because ransomware in 2022 wasn't that low to begin with. Despite dropping by a little more than a fifth, 2022 was still the second-highest year on record for ransomware attacks globally. And it's far closer to the stratospheric volumes we saw in 2021 than it is to prior years, outpacing 2017 (+155%), 2018 (+127%), 2019 (+150%), and 2020 (+54%) by significant margins.

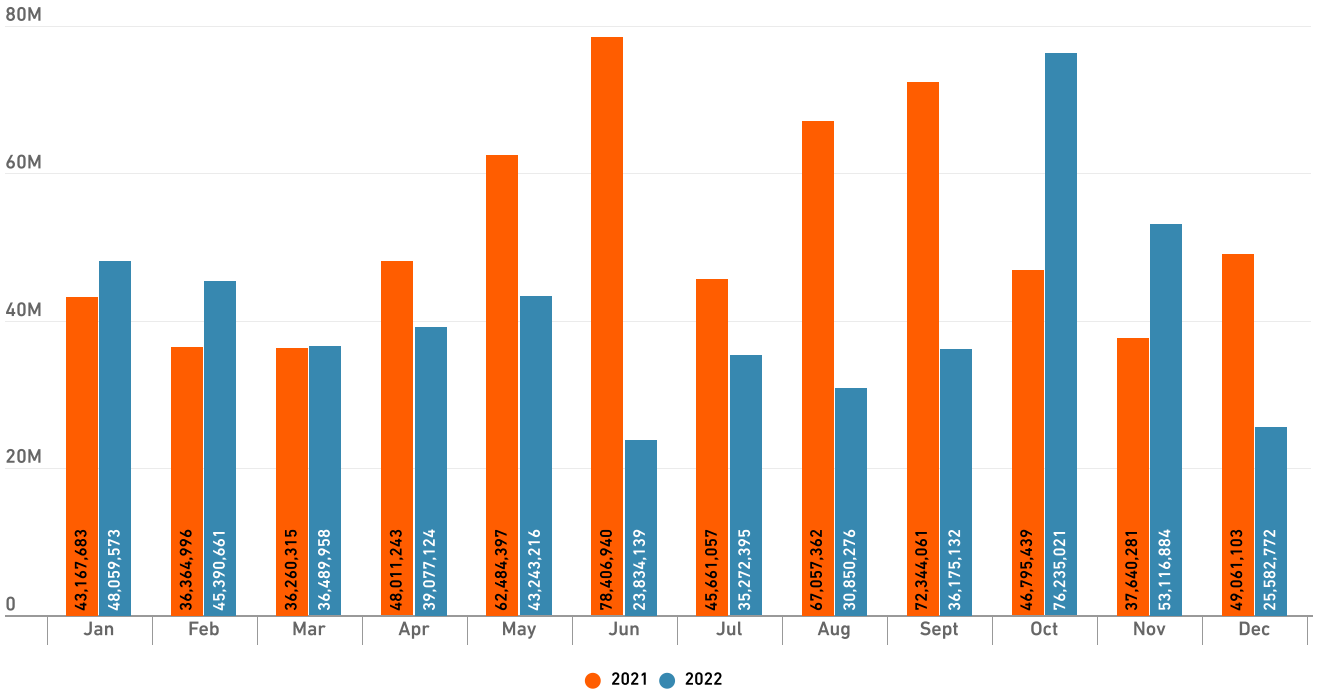
Global Ransomware Volume by Year



Global Ransomware by Quarter



Global Ransomware Volume



Ransomware by Region

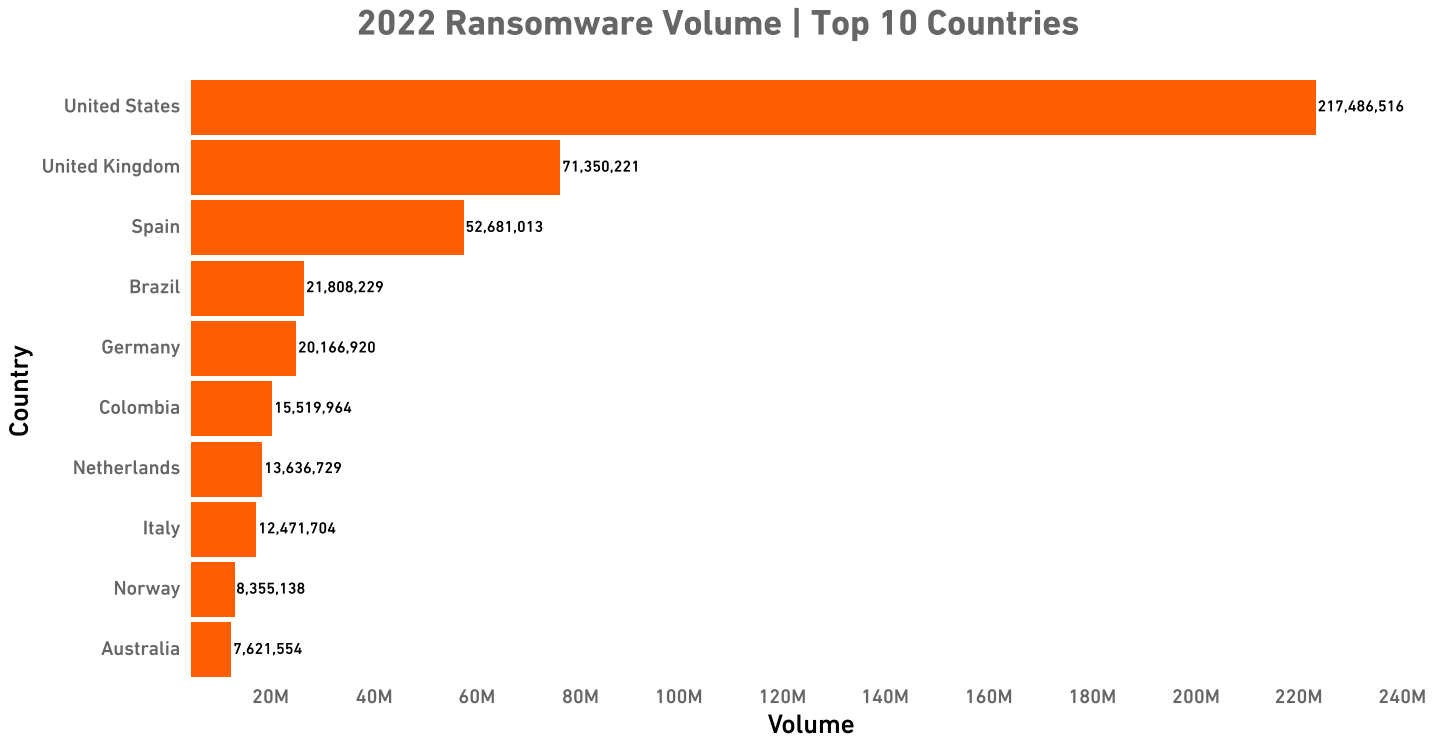
Earlier in this report, we mentioned that attackers were beginning to shift their crosshairs from the U.S. to targets in Europe and Asia. This turn in tactics brought double-digit change to both regions, with North America's attack volumes falling 48% year-over-year, and Europe's volumes rising 83%.

The inflection point for this change seems to have occurred in mid-year: In May, ransomware volume in North America fell below that of Europe for the first time since 2019. After rebounding slightly, North America's attack volumes dipped again in August, and remained below those of Europe for the rest of the year.

While a large number of attacks early in the year kept North America's full-year total above that of Europe, at 222.6 million versus 204.8 million, the two regions haven't been this close at any point in recent memory.

Summer was also a turning point for attack volumes in Asia, resulting in two very unbalanced halves. In the first six months of 2022, a total of 6.6 million ransomware attempts were recorded in Asia. In the second half this total jumped to 10.7 million, fueling a year-over-year increase of 39%.

In LATAM, where ransomware attacks fell 33% year-over-year, 2022 brought uncharacteristic volatility. From Q1 to Q2, ransomware dropped 77%, then fell another 83% from Q2 to Q3. But November brought ransomware totals 12 times those observed in October, setting a new high point for the year. But these gains were completely erased in December, when total attacks fell a staggering 99% to by far the lowest point seen all year. One possible explanation for these highly erratic trends is that, while attackers seem to be targeting LATAM less on average, there are still large campaigns being run.



Ransomware by Country

Despite a 48% year-over-year drop, the United States once again saw the highest ransomware attack volume of any country in 2022 — but with a 112% jump, the U.K. is beginning to catch up. In contrast, ransomware attacks in Germany fell 42%, moving it from the second-highest attack volume to fifth.

One newcomer to this list was Spain: Last year, the country wasn't even in the top 10 for ransomware volume, but 2022 brought a massive spike that propelled the country all the way up to No. 3 on the list. And while India's ransomware volumes still fall short of making the top 10, it also saw a large jump in 2022, with ransomware volumes up 51% year over year.

… But There's a Catch

While overall attack volume was down in 2022, the attacks that *did* occur were often worse, for several reasons.

Due to better prevention and response techniques, the percentage of people willing to pay a ransom continued to drop in 2022. While this is a positive change, it's put a squeeze on ransomware operators' profits. In an attempt to recoup some of these losses, attackers responded by increasing the amounts demanded, pushing the average ransomware payment ever higher.

Even for the victims that paid these princely sums, the nightmare often wasn't over: Double extortion tactics also increased in 2022, with one report showing a 120% year-over-year spike in the number of victims facing subsequent ransom demands.

More ruthless than *how* cybercriminals were attacking, however, was *who* they were attacking. Despite PR messages from some ransomware groups promising not to attack hospitals and healthcare facilities, SonicWall found that these ransomware attacks grew 8% year-over-year, often with catastrophic effects.

In April, a healthcare conglomerate consisting of 65 hospitals and 450 healthcare facilities across the U.S. experienced a ransomware attack, incurring a staggering $100 million in lost revenue and mitigation costs. That same month, a ransomware attack on a medical center in Yuma, Ariz., resulted in the theft of Social Security numbers, health insurance information, names and medical information for more than 700,000 patients.

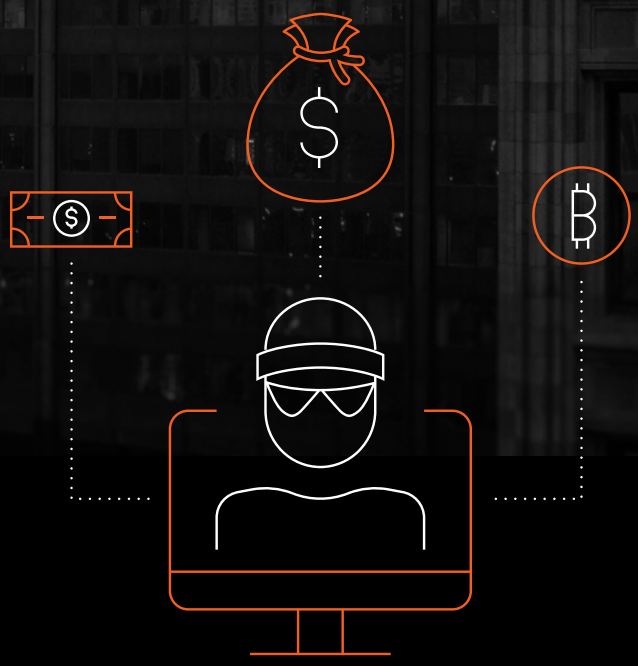
But while SonicWall observed an increase in attacks on healthcare in 2022, it observed a significantly larger 275% spike in attacks on education. While schools often don't have the money to pay the large ransoms demanded of them, their networks contain a great deal of student data, which cybercriminals can use to open credit cards or sell for a high price on the dark web.

In one particularly egregious example, attackers took advantage of the U.S.'s long Labor Day weekend to launch an attack on the Los Angeles Unified School District (LAUSD), the second-largest school system in the country. After LAUSD refused to pay the ransom demand, the threat actors published 500GB of stolen data including Social Security numbers, bank account info, W-9 forms and sensitive student health information.

Perhaps most frightening, however, were the attacks on governments. On Nov. 15, Miller County, Ark., was hit by a ransomware attack that spread through a mainframe, ultimately affecting a total of 55 counties. While no data was stolen, more than a week later many were still unable to turn on their computers and relying on pen and paper for daily operations. The disruption ultimately stretched well into December.

But 2022 also proved that, should attackers ever set their sights on disrupting governance at the national level, they could potentially succeed. When Costa Rica was hit by ransomware in April 2022, it marked the first time a country had ever declared a national emergency in response to a cyberattack. When the country refused to pay the outlandish ransom demand, the country's import and export logistics collapsed, endangering scores of perishable items stored in the tropical country's cold storage.

While this attack is now believed to have been little more than a diversionary tactic (see page 39), rather than a legitimate attempt to destabilize a nation, it provides a terrifying proof of concept for how successful such a ransomware attack *could* be.



Ransomware by Industry

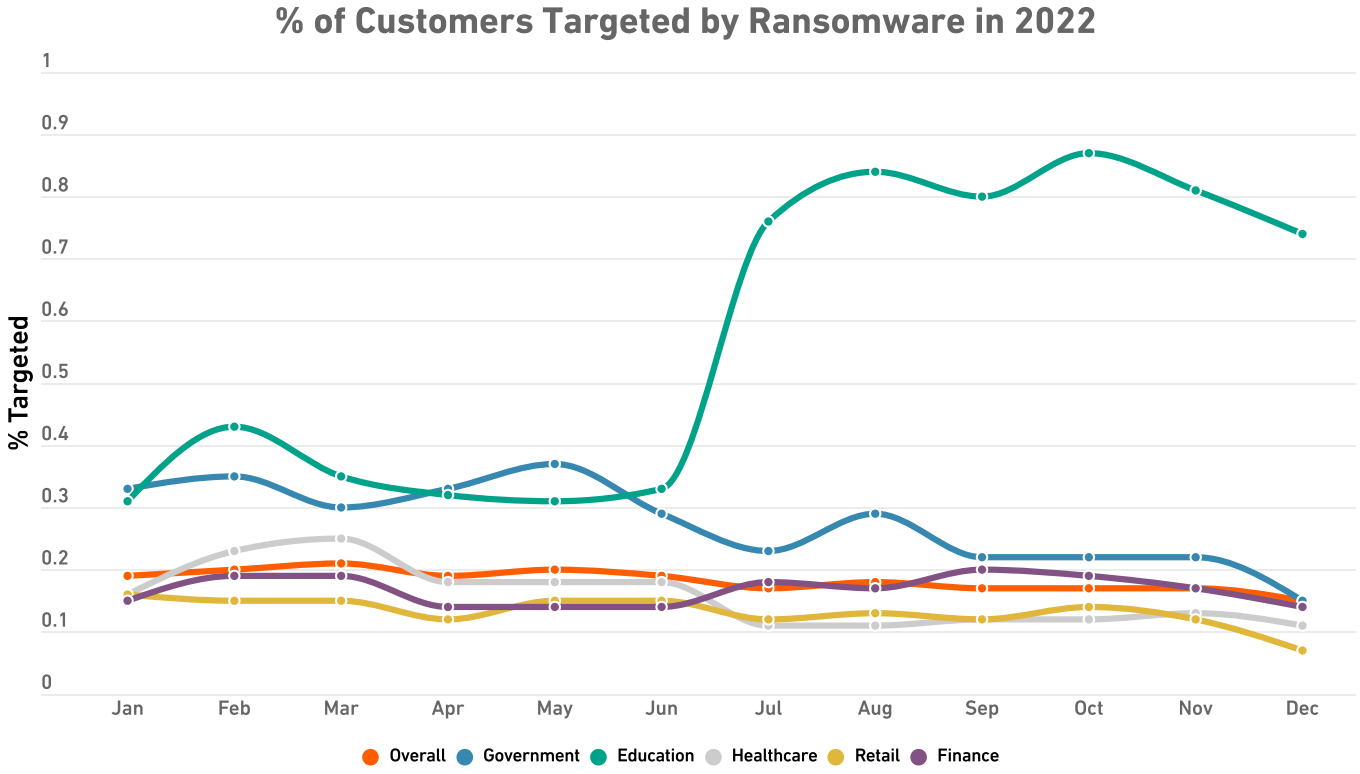
As with the regional and country data, the industry-specific data also showed a huge variety in outcomes. Customers in government and the retail industry saw double-digit decreases in ransomware, with attack volumes falling 82% and 50%, respectively.

But the other industries studied saw the opposite. With an 8% year-over-year increase, healthcare saw the smallest jump, but customers in finance (+41%) and education (+275%) weren't so lucky.

A 275% jump is bad enough on its own — but as we saw in the malware data (see page 32), this number is actually the confluence of disparate trends. Higher education customers experienced a 29% decrease in ransomware, putting it roughly in the middle on the list of industries we studied when taken on its own.

But this double-digit drop serves as a counterbalance to an absolutely massive increase in attacks on K-12 institutions and primary schools. *Attacks on these schools rose 827%*, disproportionately impacting the world's children and educators.

The per-customer data showed education customers once again inordinately affected by ransomware. In addition to being the only industry studied to have a higher average percentage of customers targeted this year than last year, ransomware attacks spiked in the second half — pushing education to a distant first in terms of how many education customers saw a ransomware attempt.



2022 Ransomware Trends

Is This the End for Big Ransomware?

While some ransomware groups were busy retraining their crosshairs on new targets in 2022, others were reorganizing, rebranding or simply going inactive. The DarkSide group kicked off this trend when it publicly announced it was disbanding amid an investigation into its attack on Colonial Pipeline. But over the past year, we've seen the fall of several other large ransomware groups, including PYSA, Conti and REvil.

Following a spate of attacks on education institutions in the U.K. and 12 U.S. states, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) released a warning about the PYSA group in March 2021, but it did little to slow the group's growth: One report found that attacks increased 50% between August and November 2021, at times surpassing even Conti. But despite being one of the top three ransomware groups in the final months of 2021, the group appears to have stopped operating entirely sometime in the first half of 2022.

Conti itself also disappeared in 2022 — but it chose to burn out rather than fade away. In 2021, IC3 reported that Conti was responsible for more ransomware attacks on critical infrastructure than any other variant. The group also conducted a number of attacks on high-profile targets, such as Ireland's health services and Japanese electronics company JVCKenwood, demanding ransoms in the millions of dollars.

But in 2022, amid the worsening Russia/Ukraine conflict, Conti — reportedly based out of Russia — published a blog vowing its "full support" for the Russian government. In retaliation, an unknown pro-Ukrainian hacker gained access to the group's internal messaging server, then began leaking nearly two years' worth of private chats, laying bare virtually every aspect of the group's operation.

About a month and a half later, the group carried out its highly publicized and disruptive ransomware attack on the Costa Rican government. But despite a $10 million dollar ransom demand, it's now believed that the attack wasn't financially motivated — instead, it was intended as a smokescreen, giving the group time to disband its operation and filter members into smaller, affiliated groups.

REvil also seems to have shut down in 2022, though its true fate is uncertain. Four months after the arrest of group leaders, the REvil's TOR servers began operating again — only this time, it sent visitors to a completely different-looking site, ostensibly belonging to a new operation with no discernible name. While it's still unclear whether original REvil members or hijackers are behind the new operation, signs point to a rebrand, likely in an attempt to escape the group's notoriety.

Attackers Continue Adopting Rust

While its use in malware isn't new, 2022 brought an increase in the number of ransomware strains pivoting to Rust. This program language touts fast and memory-efficient performance and a better user experience, as well as guaranteed memory-safety and thread-safety for greater stability.

ALPHV/BlackCat was the first major cybercrime group to adopt Rust for ransomware, and in July, the Hive ransomware gang followed. Other strains observed using Rust include Nevada, Agenda, Luna, Nokoyawa and RansomExx.

Intermittent Encryption Becoming a RaaS Selling Point

Ransomware attacks have a high profit potential, but it traditionally hasn't been a quick process: It isn't rare for an attack to be spotted and stopped during the encryption process.

However, a newer technique, known as intermittent encryption, promises to make encryption faster while making detection more difficult. Intermittent encryption works by encrypting some parts of a file while skipping others. This cuts the encryption time significantly, but still renders the file unusable. Because less of each file is being encrypted, the process also is less intensive, making it less likely to be flagged as malicious.

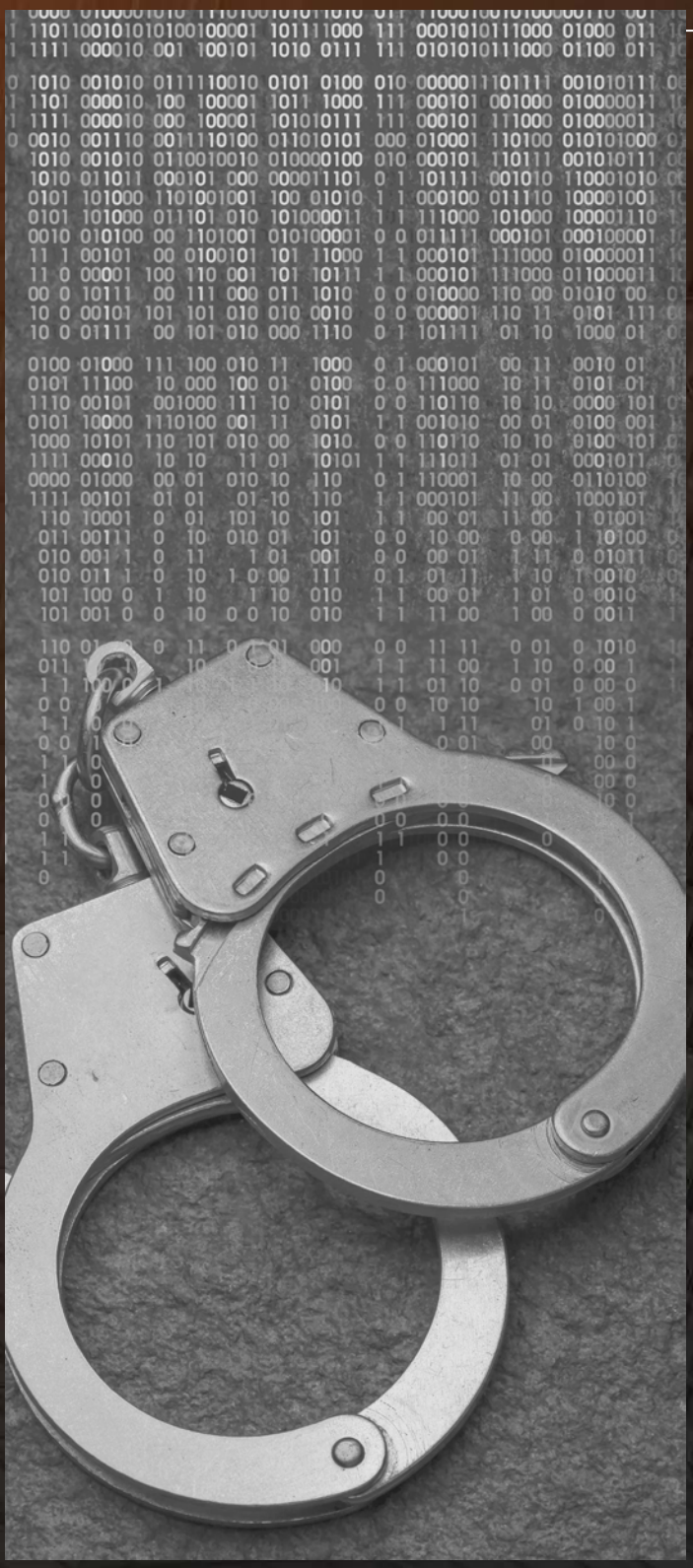
Speed advantages like this make strong selling points for RaaS offerings. After Lockbit 2.0, which incorporates intermittent encryption, was released, the LockBit group published data showing its encryption speeds beat those of its competitors. Not content to take cybercriminals at their word, Splunk conducted its own speed tests, confirming that LockBit was indeed fastest, and took only half as long as Ryuk.

Perhaps uncoincidentally, in 2022 SonicWall observed a 70.7% decrease in attacks using Ryuk, with total volume dropping from 180.4 million hits in 2021 to just 52 million a year later.

Notable Ransomware Developments in 2022

SonicWall researchers took a closer look at several new trends and development in 2022. Here are a few of the most noteworthy:

JANUARY	
Jan. 14	Linux-Based Ransomware Found Targeting VMWare ESXi Servers
FEBRUARY	
Feb. 4	Argos 2.0 Ransomware Threat Actor Gives Up Decryption Key
Feb. 11	Ransomware Asking Victims To Subscribe To A YouTube Channel
Feb. 25	Bitpylock Ransomware Leaves Decryption Key Visible In Decompiled Code
MARCH	
March 4	A Look At Partyticket Ransomware Targeting Ukrainian Systems
March 25	Ransomware Not Asking For Payment But Asks The Victim To Help The Needy
APRIL	
April 15	"Targetcompany" Ransomware
JULY	
July 13	Android Ransomware Purports To Be A Free Social Media Follower Application
July 22	New Lilith Ransomware In Early Development
SEPTEMBER	
Sept. 30	Clipboard Hijacker Dropped By Stop Ransomware
NOVEMBER	
Nov. 11	Tor Chat With Black Basta Ransomware Operator Runs Dry
DECEMBER	
Dec. 16	Cryptonite Ransomware Leaves Files Unrecoverable



2022's Biggest Busts

2022 was another banner year for ransomware busts, as law enforcement in the U.S., U.K., Canada, Brazil and even Russia brought some of ransomware's key players to justice:

January 14, 2022 – Based on intelligence provided by the U.S., Russia announced that it had "dismantled" the REvil ransomware gang. During the bust, Russian authorities seized more than 426 million rubles in cash and cryptocurrency, as well as luxury cars that had been purchased with ransomware proceeds.

March 24, 2022 – Seven members of the Lapsus$ extortion group were arrested in London, including one of its leaders who was only 16 years old.

September 23, 2022 – A 17-year-old hacker suspected of being involved in cyberattacks on Uber and Rockstar games was arrested in London. While these two attacks did not involve ransomware or extortion, both the suspect and the attacks were determined to be connected with Lapsus$.

October 19, 2022 – Following an investigation on the breach of Brazil's Ministry of Health, Brazilian authorities arrested another suspect allegedly connected with Lapsus$.

October 26, 2022 – After an investigation involving authorities from France, the U.S., Canada and Europol's European Cybercrime Centre, Mikhail Vasiliev was arrested at his Ontario, Canada, home. Known to Europol as "one of the world's most prolific ransomware operators," Vasiliev was allegedly linked to the Lockbit ransomware and several high-profile attacks.

January 26, 2023 – Months after it penetrated Hive's networks, the U.S. FBI announced in January that it had successfully disrupted the group's operations in 2022. While no arrests have been made as of publication, Hive's website has been seized and its decryption keys were captured and provided to victims.

CAPTURE ATP & RTDMI

RTDMI™ Detections Continue to Rise

SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) continued to raise the bar in 2022. The technology identified and mitigated 465,501 never-before-seen malware variants — more than in any other year since the technology was introduced and an average of 1,279 per day.

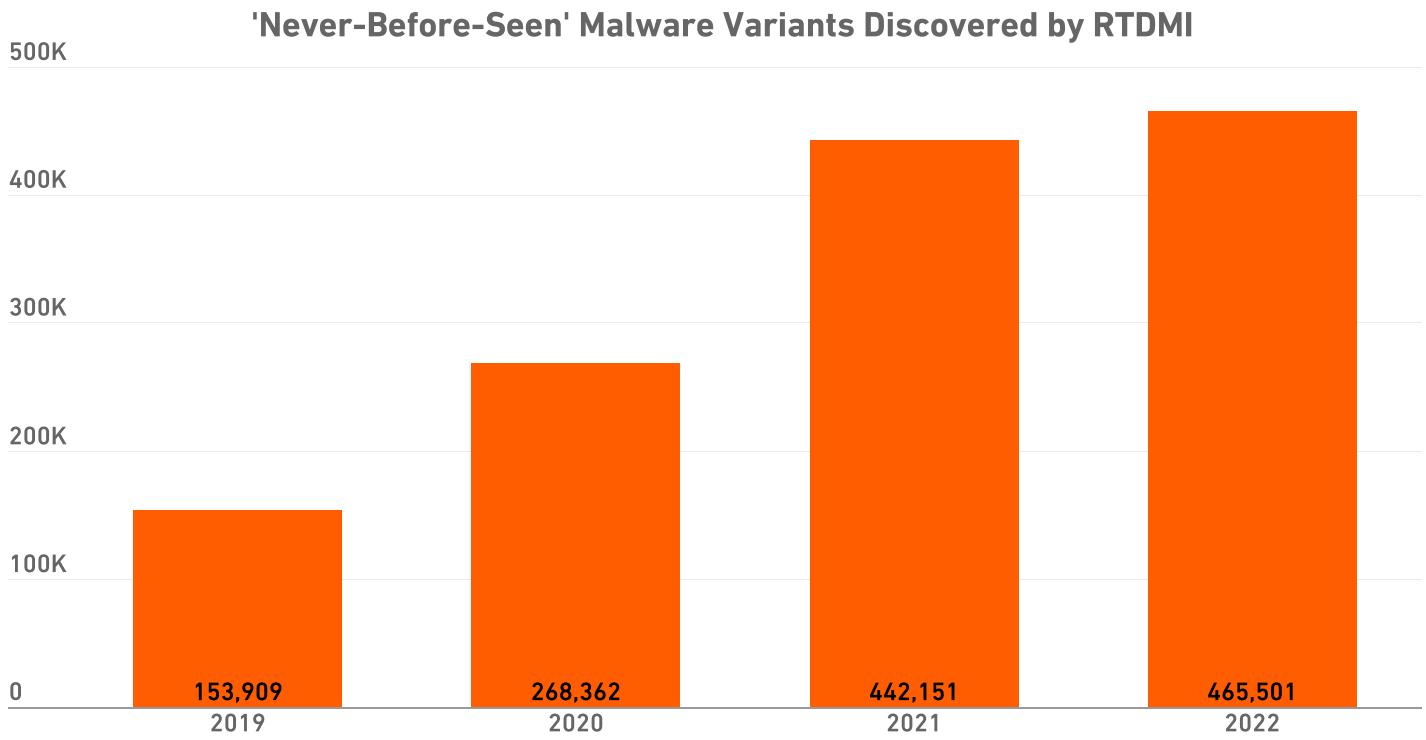
This increase was enough to push the all-time number of never-before-seen malware variants detected past the 1 million mark. The 2022 count also represented the first time a yearly detection total surpassed 450,000.

But that wasn't all that set 2022 apart. In March alone, the technology detected 59,259 new variants, more than in any other month. Combined with higher-than-average detections in January and February, this helped push Q1 to a total of 147,851 never-before-seen malware variants — the highest of any quarter on record.

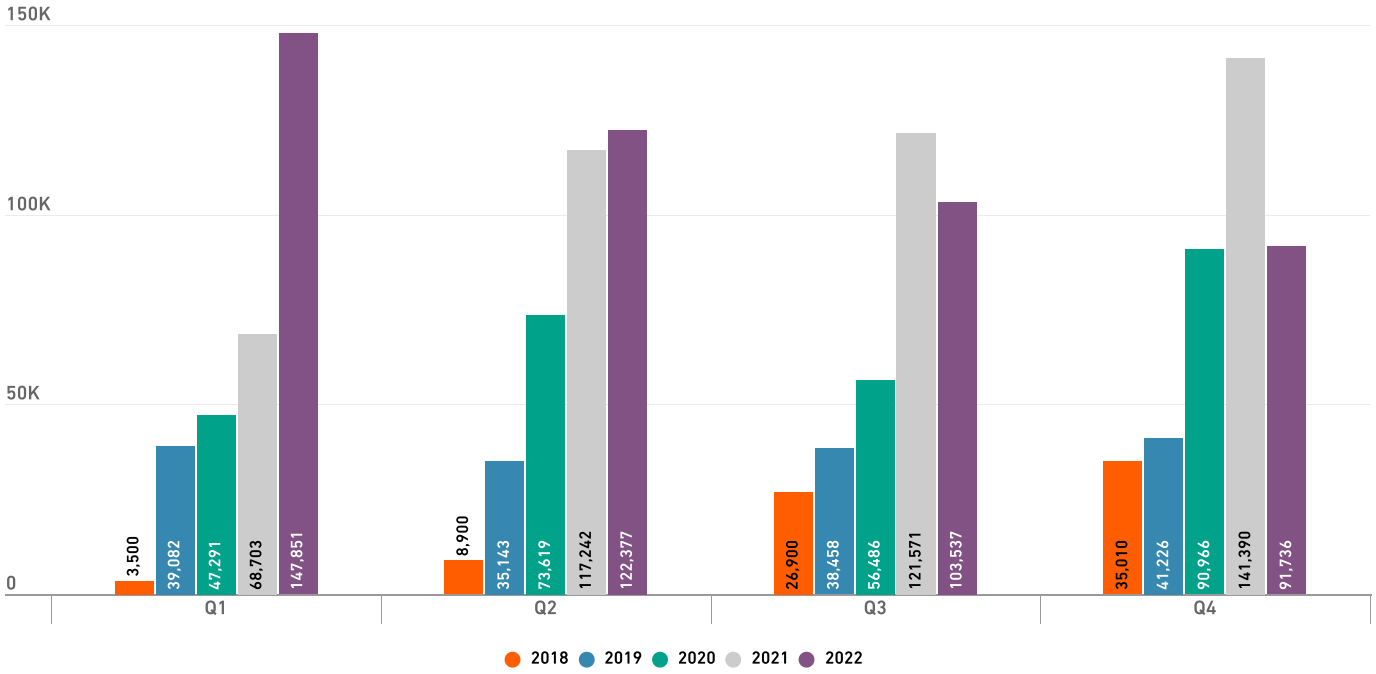
"Zero-Day" vs. "Never-Before-Seen" Attacks

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 protections (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 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.



'Never-Before-Seen' Malware Variants Found by RTDMI™



Since it was added to SonicWall's Capture Advanced Threat Protection — a multi-engine sandbox service designed to mitigate new and more evasive forms of malware — RTDMI has served as a force multiplier to SonicWall's already robust threat detection capabilities. RTDMI is capable of finding malware that relies on various anti-evasion techniques, such as repacking, recompiling or otherwise obfuscating itself in an effort to evade all existing industry detections. That includes malware that hides its weaponry via encryption and hasn't yet displayed any malicious behavior.

RTDMI is not only highly effective — it's getting even more effective over time. By leveraging machine learning capabilities, it continually improves its ability to recognize and mitigate cyberattacks never before seen by anyone in cybersecurity.

CRYPTOJACKING

Cryptojacking Continues Record-Breaking Run

As cybercriminals complemented ransomware with more low-profile revenue streams in 2022, cryptojacking rates began to accelerate significantly. By year's end, SonicWall Capture Labs threat researchers recorded 139.3 million cryptojacking attempts, a 43% year-over-year increase.

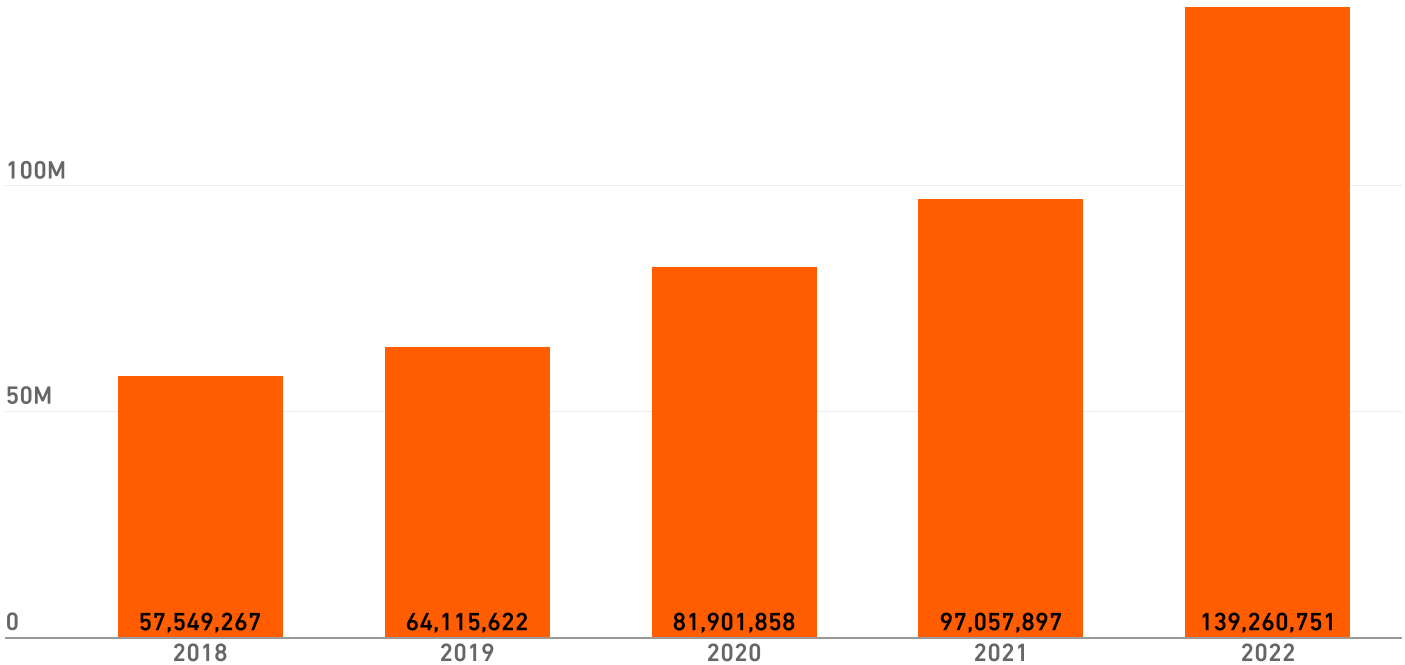
Not only did 2022 mark the first time that yearly attack volume surpassed 100 million, it was also more cryptojacking than SonicWall had ever observed in a single year.

Monthly record totals were set as well: In January, cryptojacking attempts rose to 18.4 million, surpassing the previous monthly record (set in March 2020) by nearly 3 million.

After attack volume dropped dramatically in November, December came with a vengeance, bringing with it 30.4 million cryptojacking attempts. This unprecedented total not only exceeded the previous monthly record by roughly 12 million, it also surpassed the total for all but three *quarters* on record.

Even so, highly suppressed volume in November, combined with sustained high rates of cryptojacking at the beginning of 2022, meant that Q1, not Q4, ended the year with the highest volume on record.

Global Cryptojacking Volume by Year



Cryptojacking by Region

While LATAM recorded a 66% drop in cryptojacking volume year over year, it was the only region to see a drop.

In North America, which typically sees by far the most attacks, volume rose from 78.0 million in 2021 to 105.9 million in 2022 — a 36% increase, and more than the *entire world* saw the year before.

Asia saw an even larger year-over-year increase of 129%, jumping from 3 million to 6.9 million. But it was Europe where cryptojacking grew the fastest: Volume there soared from 3.4 million in 2021 to 22.0 million in 2022, an increase of 548%.

Despite skyrocketing attack volumes in Europe, the United States remained the country with the highest volume. Cryptojacking attempts there rose 41% year over year.

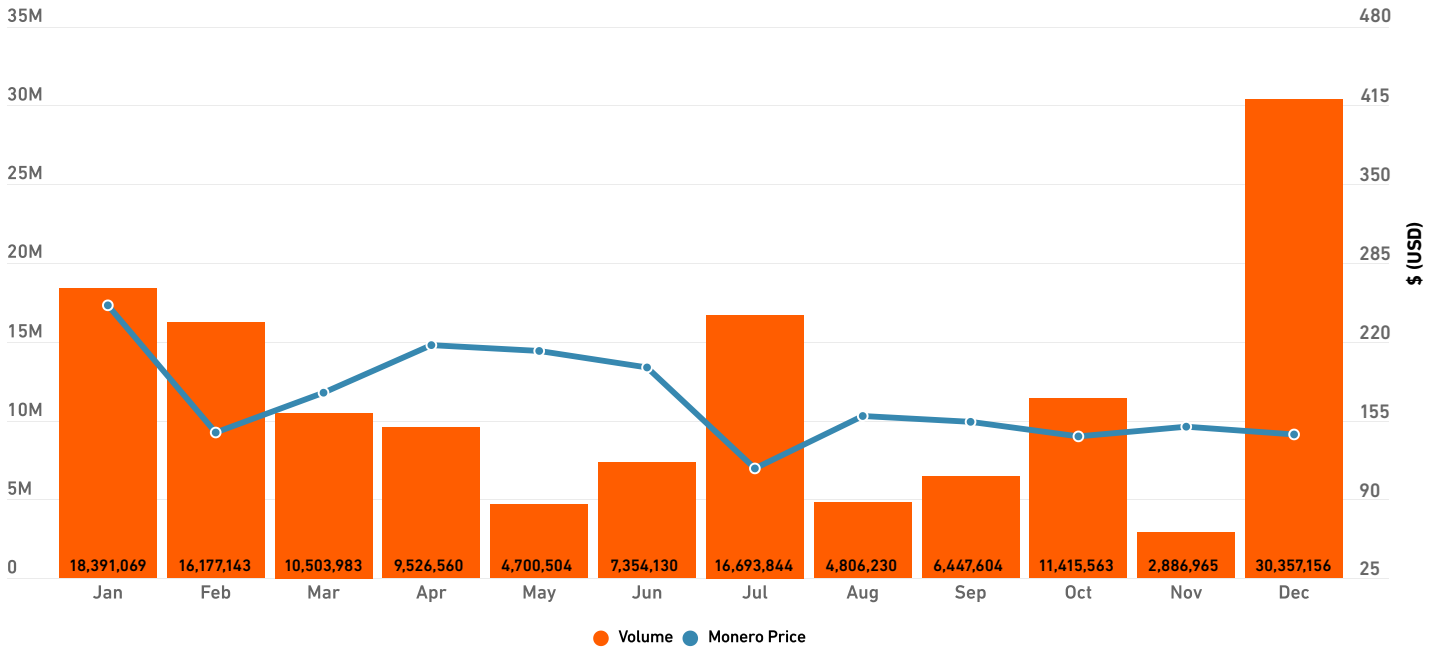
XMRig Now Used in Nearly 90% of Cryptojacking Attempts

Due to its high availability and ease of use, XMRig was once again the cryptominer of choice. In 2022, 89.4% of all cryptojacking attempts recorded by SonicWall were based on XMRig, up from 67.4% in 2021.

XMRig is an open-source, cross-platform miner that, while not malicious on its own, is frequently abused by cybercriminals to illegally mine the privacy coin Monero on victims' computers.

The miner can be dropped on a victim's machine through a variety of means, such as the modular Glupteba malware and, increasingly, malware targeting Linux.

Global Cryptojacking Volume



Linux Increasingly in the Crosshairs

With more than 96% of the world's top web servers running Linux, attackers have been observed targeting the operating system in increasing numbers. Because Linux offers a pathway into multi-cloud environments, it can make the infection process easier: While there are many cloud tenants to choose from (GCP, Azure, AWS, etc.), Linux is a ubiquitous platform across all environments. In other words, there's a much more limited scope of technology that attackers need to be familiar with.

In addition to being faster, this method also tends to be lower risk: Most antimalware solutions focus primarily on identifying and mitigating Windows-based attacks, as opposed to the Linux-based operating systems underpinning many private and public cloud deployments. As a result, a growing amount of sensitive data and infrastructure are left vulnerable to compromise.

Unfortunately, as with traditional cryptojacking, attacks on cloud environments are designed to be as subtle as possible while still achieving the desired output — so it's unlikely there will be any perceptible disruption to operations.

More Diverse Capabilities = More Powerful Campaigns

Cybercriminals aren't just making their attacks more subtle, however. They're also making them more sophisticated.

In November, a Linux-targeting cryptojacking campaign incorporating a remote-access trojan (RAT) was discovered. This free, open-source RAT, called Chaos RAT, adds a diverse set of capabilities to the traditional cryptojacking repertoire — such as the ability to access file explorer; upload, download and delete files; take screenshots; and connect to a command-and-control server that can use used for deploying additional malware.

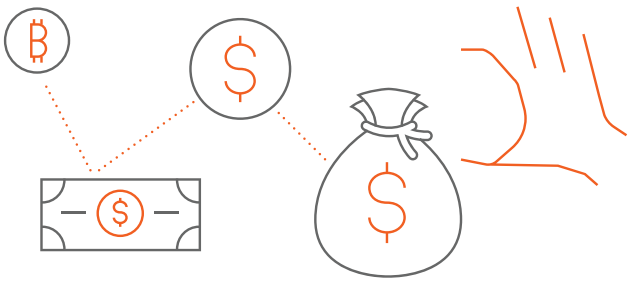
Another cryptomining Trojan was detected by SonicWall in June, this one purporting to be from well-known malware group TeamTNT. After finding, killing and removing any cryptominers that may already be running (a technique pioneered by groups like ROCKE), this variant downloads and installs XMRig, then gains secure access to the victim machine over an unsecured network. Finally, it launches another open-source tool, punk[.]py, which collects usernames, SSH keys, and known hosts from a Unix system, then attempts to connect via SSH to all the combinations found.

Cryptojacking Goes to the "Dogs"

TeamTNT's techniques were also built upon for a campaign spotted in September. Named "Kiss-a-dog" based on the domain used to trigger a shell script payload, this variant targets vulnerable Docker and Kubernetes instances. In addition to installing XMRig, the malware also tries to escape from and create backdoors to compromised containers, move laterally in the network, and gain persistence — while at the same time attempting to terminate and uninstall any cloud monitoring services.

Many of these tactics used in Kiss-a-dog were also present in an earlier campaign wearing the TeamTNT banner, this one detected by SonicWall in May 2022. This variant seems to specifically target Alibaba Cloud/Aliyun Linux deployments, but unlike the Kiss-a-dog campaign, it installs the Xanthe bitcoin-mining software.

Another similar campaign was discovered in June, this one targeting misconfigured Docker Engine API endpoints and Redis servers. The attack involved several payloads and was capable of disabling Alibaba Cloud Agent security and wormlike propagation in addition to XMRig mining. While the scripts feature TeamTNT logos and messages such as "TeamTNT likes the Borg," the mining address and other factors suggest that this campaign is actually the work of the WatchDog group.



CYBERCRIMINALS AREN'T JUST MAKING THEIR ATTACKS MORE SUBTLE. THEY'RE ALSO MAKING THEM MORE SOPHISTICATED.

Secure Your Redis Servers … or Pay

Redis servers are a growing target for opportunistic attackers. Since they're meant to be used inside the network, rather than exposed to the internet, authentication isn't enabled by default. If they aren't secured, they can easily be compromised by malware, such as the Headcrab malware.

In practice a botnet (due to its ability to exploit Redis' SLAVEOF command), this custom malware had already infected at least 1,200 Redis servers as of February 2023. Headcrab runs in memory, bypasses volume-based scans, deletes logs and communicates with legitimate IP addresses. These tactics have made it so stealthy that, until recently, it was virtually undetectable.

The botnet's primary function is to mine Monero, and it seems to be unusually good at it: Researchers estimate that each infected endpoint could be expected to generate around $4,500 per year.

Big Tech Bites Back

Big tech firms, such as Amazon, Alibaba and Google, are well aware of the attacks on their cloud servers. But since the privacy of data and workflows is part and parcel of the product they sell, they're limited in how they can protect customer organizations against cryptojacking.

But the threat is growing. In its 2021 Threat Horizons report, Google Cloud reported that 86% of compromised cloud instances were being used to illegally mine cryptocurrency.

In response, some cloud providers have been working to increase their ability to detect cryptojacking. Microsoft has improved its Defender for Endpoint, and Google Cloud has introduced the Virtual Machine Threat Detection (VMTD).

But with the entry points for cloud-based cryptojacking remaining largely the same as for traditional cryptojacking — such as phishing, misconfigurations and poor patch hygiene — following established best practices will go a long way.

The Bust, the Breaches and the Late Bitzlato

If you started 2022 with one bitcoin, by the end of the year, you'd be … highly disappointed.

After starting 2022 at nearly $50,000 — already down significantly from its peak of nearly $69,000 — bitcoin prices soon sank rapidly, ending 2022 at $16,556, roughly a third of their Jan. 1 value. But while BTC prices were among the most visible aspects of the crash, they were only a symptom.

The true catalysts for 2022's "crypto winter" were macroeconomic uncertainty and the complete collapse of two so-called "stable coins": Luna and TerraUSD.

As investors fled the crypto market, cybercriminals upped the ante, resulting in a record-breaking year for both the number of heists and — with an estimated $3.56 billion (USD) stolen — the amount of losses.

In the first week of August, the Nomad cryptocurrency bridge was attacked, resulting in a loss of almost $200 million of its funds. The very next day, attackers reportedly exploited a vulnerability in Slope wallets to steal at least $6 million worth of crypto tokens from more than 9,000 wallets.

In October, the Binance Smart Chain network saw an attack bigger than both of these combined, when criminals stole $570 million. But the biggest heist — not just of 2022, but of all time — took place in March. That month, attackers breached the Ronin bridge and stole a staggering $650 million. Researchers now believe the Lazarus group, who was responsible for stealing $100 million in an attack on Harmony's Horizon bridge in June, was also behind this breach.

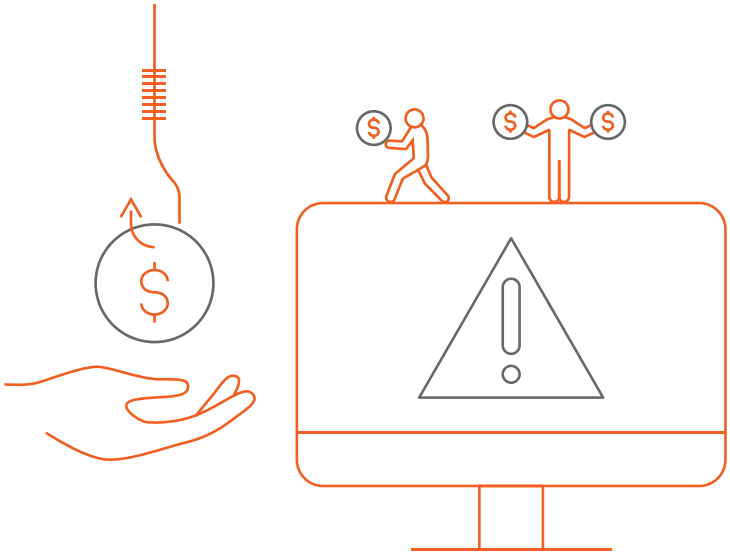
But while several crypto companies were a target for cybercriminals, one was reportedly a haven for them. In January 2023, Anton Shkurenko, founder of cryptocurrency exchange Bitzlato, was arrested after an investigation found Bitzlato had violated U.S. anti-money laundering regulations.

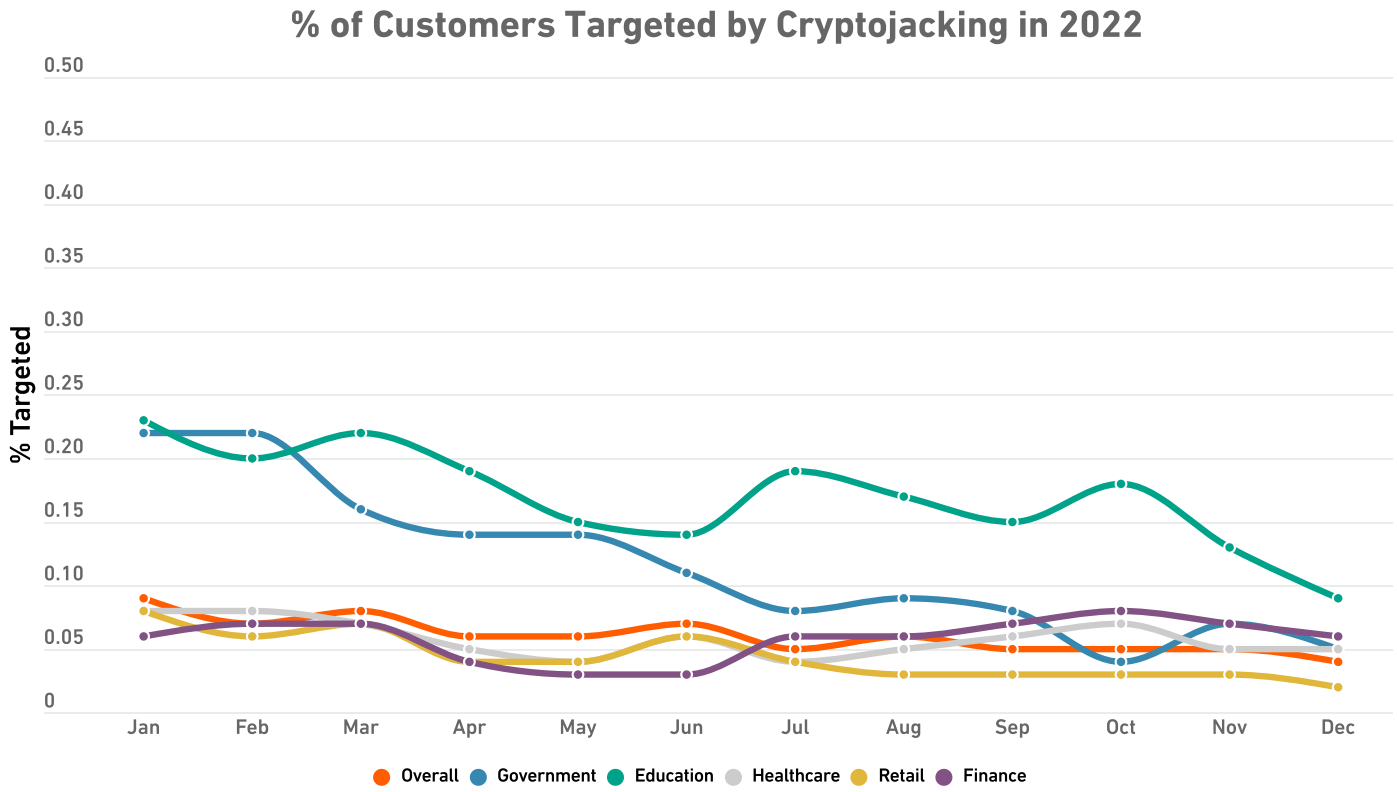
According to U.S. Attorney Breon Peace, the exchange "sold itself to criminals as a no-questions-asked cryptocurrency exchange," and processed over $4.5 billion in cryptocurrency transactions, including more than $15 million in ransomware proceeds.

Bitzlato was reportedly associated with several cybercriminal groups, including DarkSide, Phobos and Conti. It also worked closely with Hydra, which, prior to its shutdown, was the world's biggest and longest-running darknet marketplace, specializing in stolen financial information, fraudulent identification documents, money laundering services and narcotics.

According to the U.S. Justice Department, "Hydra buyers routinely funded their illicit purchases from cryptocurrency accounts hosted at Bitzlato, and in turn, sellers of illicit goods and services on the Hydra site routinely sent their illicit proceeds to accounts at Bitzlato."

In February 2023, Bitzlato's CEO, a sales executive, the marketing director and others were apprehended in Spain, bringing the total number of arrests to six. But despite ongoing enforcement efforts, Shkurenko has vowed that this isn't the end, and that the new Bitzlato would be based out of Russia and "out of the reach of law enforcement authorities."





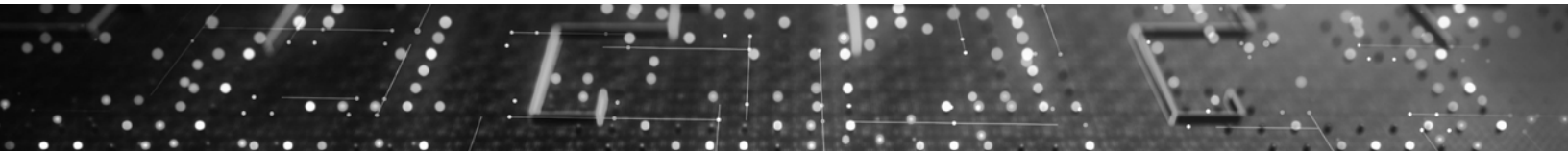
Cryptojacking by Industry

Among the most volatile of our data sets, 2022's data on cryptojacking by industry highlights the rapid evolution of cybercriminal behavior. The least movement was seen in education, where total attack volume increased 20% over 2021's totals. Government and healthcare also saw double-digit movement, with attack volumes falling 83% and 76% respectively.

Attacks on finance customers increased 352% in 2022, enough to move it from No. 4 to No. 3 for attack volume. But even this triple-digit spike wasn't the worst observed: **those in retail saw year-over-year attack volume jump a staggering 2,810%**. But despite retail having the highest total attack volume, these customers were the least likely to see an attack: it was education customers that had the highest percentage of customers targeted.

Cryptojacking Attack Volumes by Industry

2021	2022
1. Healthcare	1. Retail
2. Education	2. Education
3. Government	3. Finance
4. Finance	4. Healthcare
5. Retail	5. Government



ENCRYPTED ATTACKS

Encrypted Attacks Fall 28%

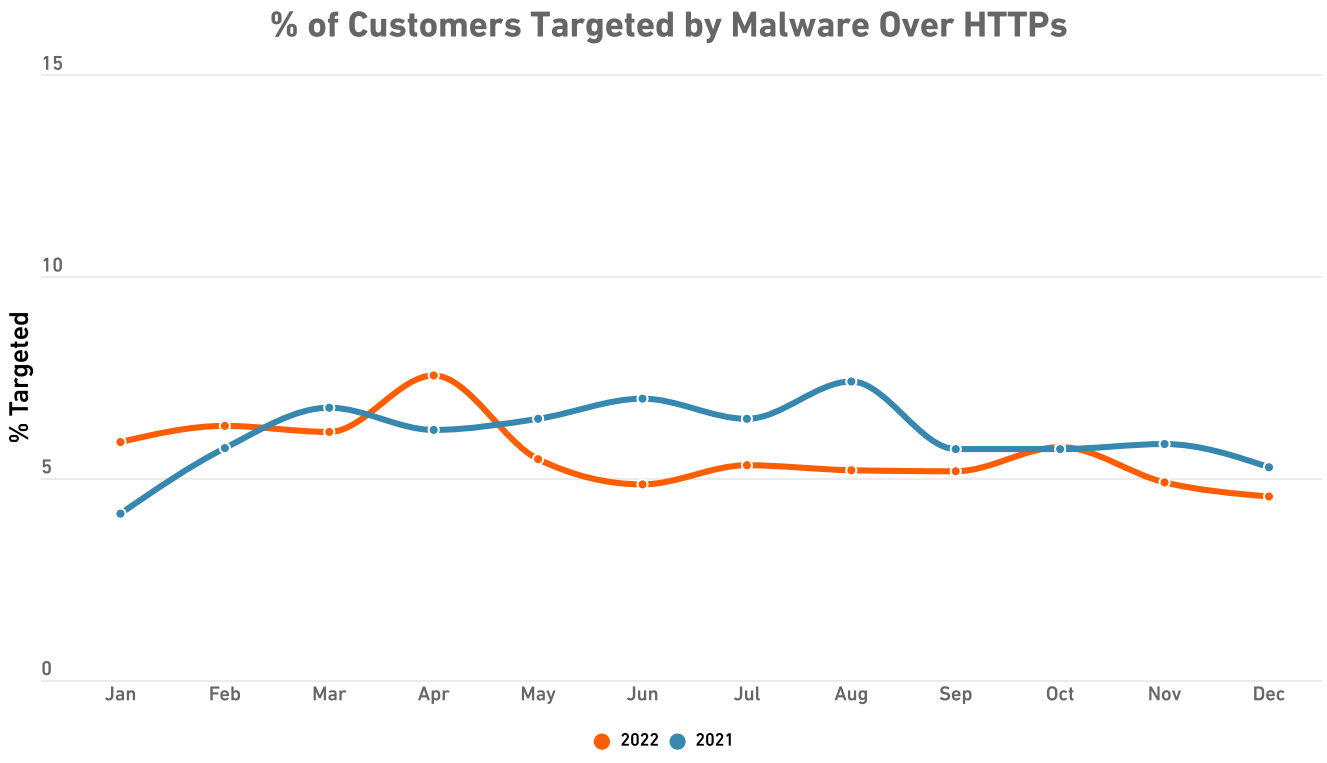
In 2022, SonicWall Capture Labs threat researchers recorded 7.3 million encrypted attacks, down from 10.1 million in 2021. But in 2022, the total was closer to last year's record high than to the volumes seen in 2019 (3.7 million) and 2020 (3.8 million).

But while a 28% decrease is somewhat modest compared with some of the movement we've seen elsewhere, it hides a great deal of regional variation.

In Asia, attack volumes fell dramatically in 2022, dropping 85% year over year. For most of the year, LATAM appeared to be going the same direction. By November, attack volumes for 2022 were less than half that seen in 2021.

But then December came, bringing with it more than twice the number of attacks that LATAM recorded in the other 11 months combined. This late-year blitz was enough to singlehandedly push encrypted attacks in the region from a 62% year-over-year decrease to a 29% increase.

While it lacked the volatility seen in other regions, double-digit movement was also seen in North America and Europe, which experienced a drop of 39% and an increase of 22%, respectively.



* Organization must have a SonicWall firewall with DPI-SSL activated.

Encrypted Attacks by Industry

For the industries studied, the news ranged from good, to bad, to worse. Retail and finance received a welcome reprieve from encrypted attacks, with attack volumes for these industries falling 79% and 45%, respectively.

In contrast, healthcare saw a 35% jump in malware attacks over HTTPs — but this was small compared with what was experienced by customers in education and healthcare. Both of these industries experienced triple-digit attack volume increases, with attacks on education rising 411% and attacks on government spiking 887%.

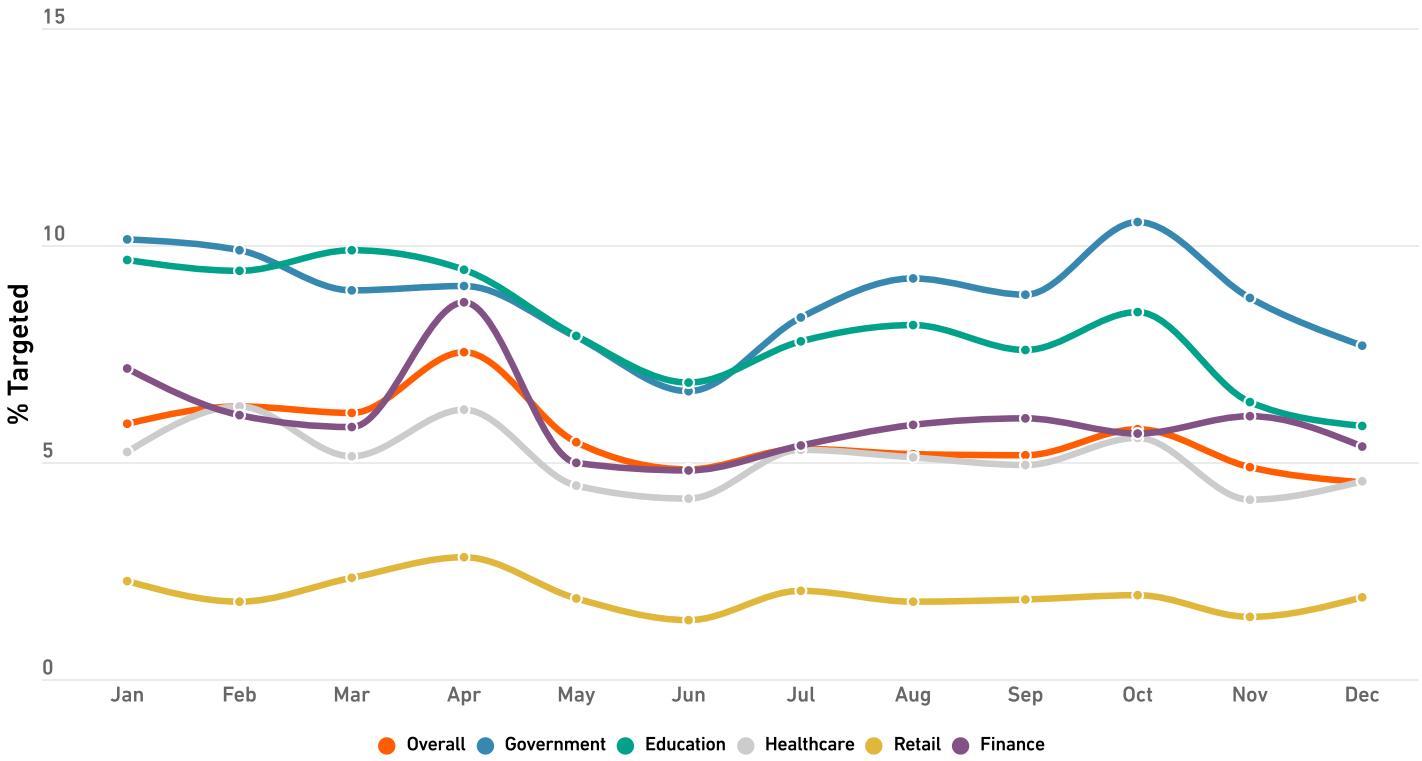
The huge increase in attacks on government organizations can also be observed in the per-customer data. Government was the only industry studied to see a year-over-year increase in the average percentage of customers targeted. This increase pushed it above education, the industry that saw the most attacks per customer in 2021.

What Are Encrypted Threats?

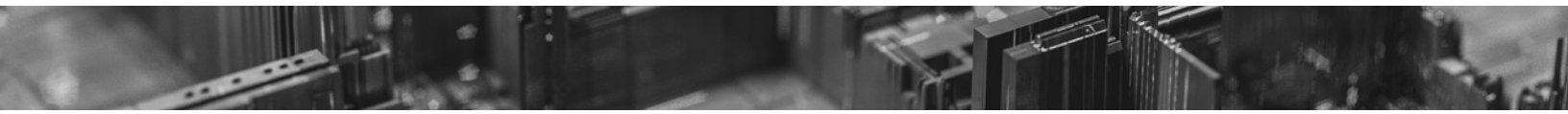
Put simply, TLS (Transport Layer Security) is used to create an encrypted tunnel for securing data over an internet connection. While TLS provides security benefits for web sessions and internet communication, this encryption protocol is also increasingly used by cybercriminals who want to hide malware, ransomware, zero-day attacks and more.

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

% of Customers Targeted by Malware Over HTTPs in 2022



* Organization must have a SonicWall firewall with DPI-SSL activated.



INTRUSION ATTEMPTS

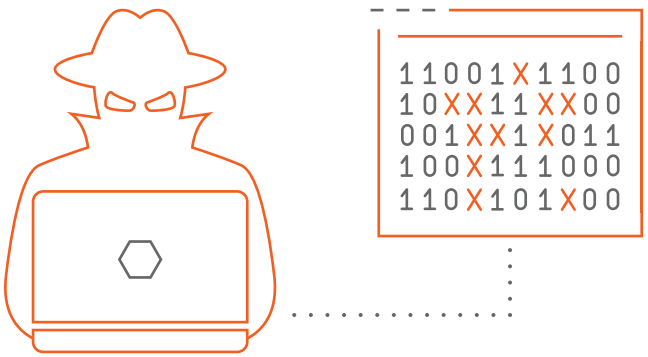
Overall Intrusion Attempts Up

Intrusion attempts continued to climb in 2022, hitting a new high of 6.3 trillion. This represents a 19% increase over 2021's total, and is roughly six times the number of overall attempts observed in 2013, the first year SonicWall recorded this data.

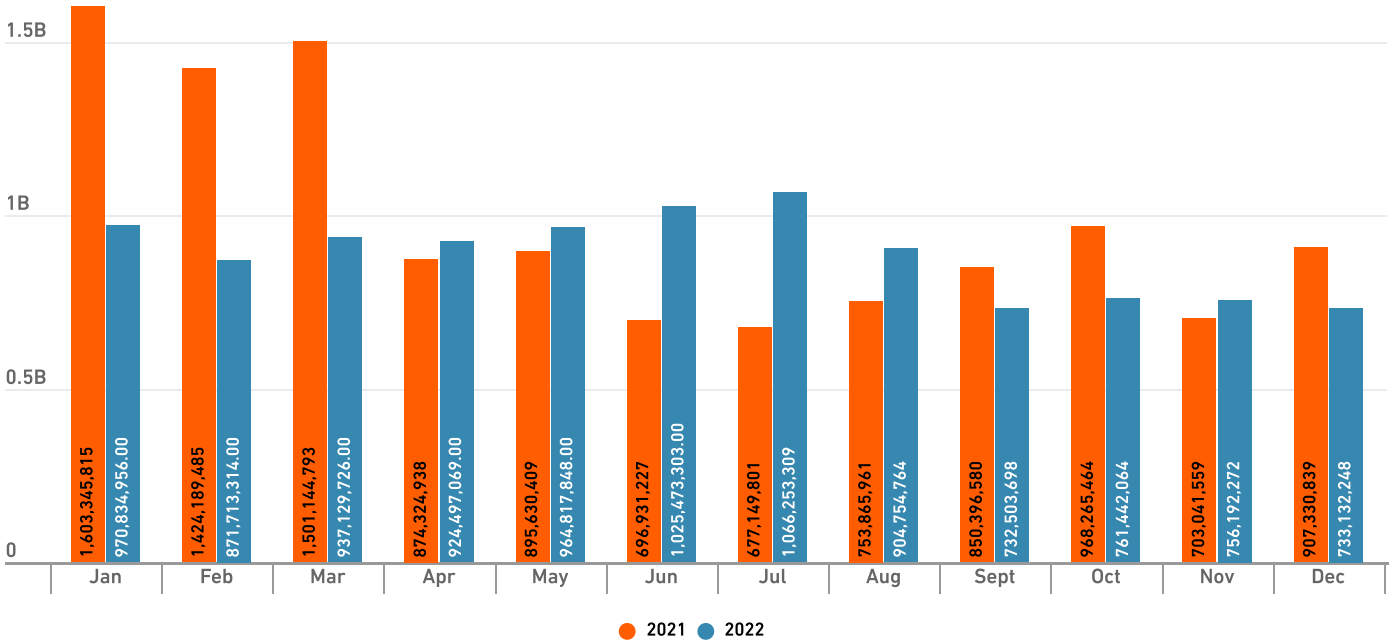
But while there may be more overall intrusions, a majority of this increase is due to low-severity hits associated with pings and other actions that are typically benign. The number of moderate- or high-severity intrusion attempts, also known as malicious intrusion attempts, observed in 2022 actually fell, dipping to 10.6 billion — a 10% year-over-year drop.

Even larger decreases were recorded in Europe and Asia, where malicious intrusions fell 28% and 17%, respectively. In North America, malicious intrusion attempts remained essentially unchanged from 2021 levels. Only LATAM saw a statistically significant increase: Malicious intrusion attempts there rose 8%.

But while there was no reshuffling of the regions with regards to who was hardest hit, the gap between North America and Europe, which had the second-highest attack volume, is continuing to grow — making it likely that malicious intrusion attempts will continue to disproportionately affect this region for the foreseeable future.



Global Intrusion Attempts



Note: Only includes malicious medium- and high-risk intrusion attempts.

What is an Intrusion Attempt?

A malicious intrusion attempt is a security event in which a cybercriminal, hacker, threat actor or intruder tries to gain access to a system or resource by exploiting a vulnerability without authorization. Such vulnerabilities are generally public and published as CVEs (see page 10). While these vulnerabilities are public, not everyone patches at the same rate, giving attackers an opportunity to take advantage of unpatched software or appliances that can be used as an entry point into a network.

Malicious intrusions also include the exploitation of vulnerabilities that are not yet well publicized or haven't been published — the dreaded zero-day vulnerabilities.

Vulnerability exploitation doesn't stop once attackers get inside the network. In fact, it usually accelerates. Attackers attempt to gain network persistence and lateral movement by exploiting other, internal vulnerabilities in unpatched systems and software inside the network.

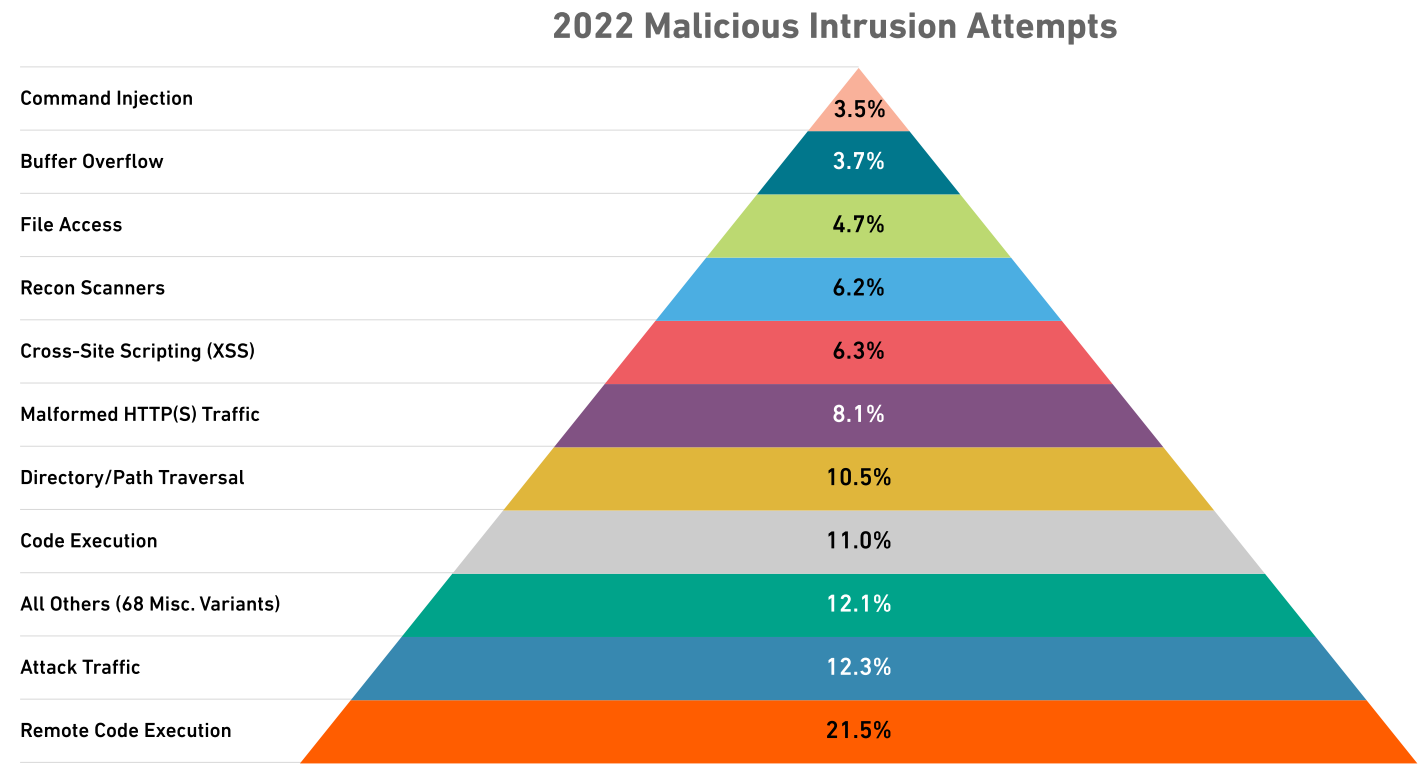
What SonicWall records is detection and prevention of vulnerabilities coming from both external and internal sources. When a piece of code that constitutes a vulnerability passes a firewall with Intrusion Prevention enabled, and the firewall detects and neutralizes that code, an intrusion attempt is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

As noted, malicious intrusions consist of moderate- and high-severity intrusion attempts — low-severity intrusion attempts are typically harmless.

The Rise of RCEs

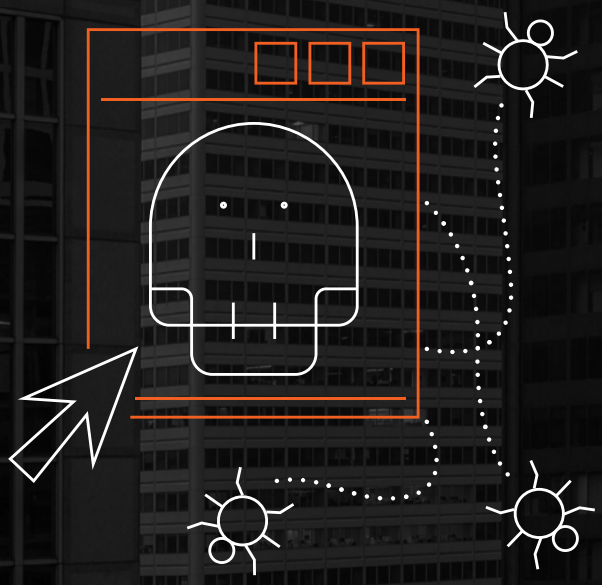
While very little in the cybersecurity world has returned to its 2019 state, malicious intrusion types are one exception: Just like we saw four years ago, Remote Code Executions (RCEs) are once again the most common form of malicious intrusion we observed.

While this type of intrusion attempt made up less than 10% of total malicious intrusions in 2021, their numbers grew tremendously in 2022, and they now make up 21.5% of malicious intrusion attempts globally.



What is an RCE?

An RCE attack takes place when a threat actor uses a vulnerability to remotely run malicious programming code, usually in an unexpected path and with system-level privileges. (The infamous Bluekeep vulnerability is one example of this.) These vulnerabilities are among the most dangerous on software systems and are frequently used to spread ransomware.



Here are some of the RCEs SonicWall Capture Labs threat researchers reported in 2022:

EmbedThis Goahead Web Server CGI RCE	2/4/22
Samba vfs_fruit Module RCE Vulnerability	3/4/22
Java Spring Framework Spring4Shell RCE Vulnerability	4/1/22
VMware Workspace One Access & Identity Manager RCE Vulnerability	4/22/22
WSO2 API Manager RCE Vulnerability	4/29/22
Parse Server Databasecontroller RCE Vulnerability	5/6/22
Follina MS-MSDT RCE Vulnerability	6/1/22
Atlassian Confluence OGNL Vulnerability	6/10/22
Oracle MySQL NDB Cluster RCE	7/22/22
Ivanti Avalanche RCE Vulnerability	8/5/22
Zimbra Collaboration RCE Vulnerability	9/2/22
Microsoft Exchange Server Zero-Day Vulnerabilities	9/30/22
Zimbra Collaboration Suite TAR RCE	10/20/22
Follina Vulnerability Is Being Used to Deliver Redline Info Stealer	11/2/22

Malicious Intrusions by Industry

The industry-specific intrusion data for 2022 showed less volatility than some other threat types, but that doesn't mean there weren't still some significant upticks.

Government organizations saw the worst of it: malicious intrusion attempts on these customers spiked 74% year over year. With a 55% increase, the finance industry didn't fare much better. Healthcare and retail saw significantly more modest increases of 5% and 3%, respectively. Only education saw a decrease — total malicious intrusions targeting these organizations dropped 17% from 2021's levels.

But a look at the per-customer data shows that while most of the industries studied saw an increase, that doesn't necessarily mean more of these customers are seeing an attack. In fact, we observed the opposite.

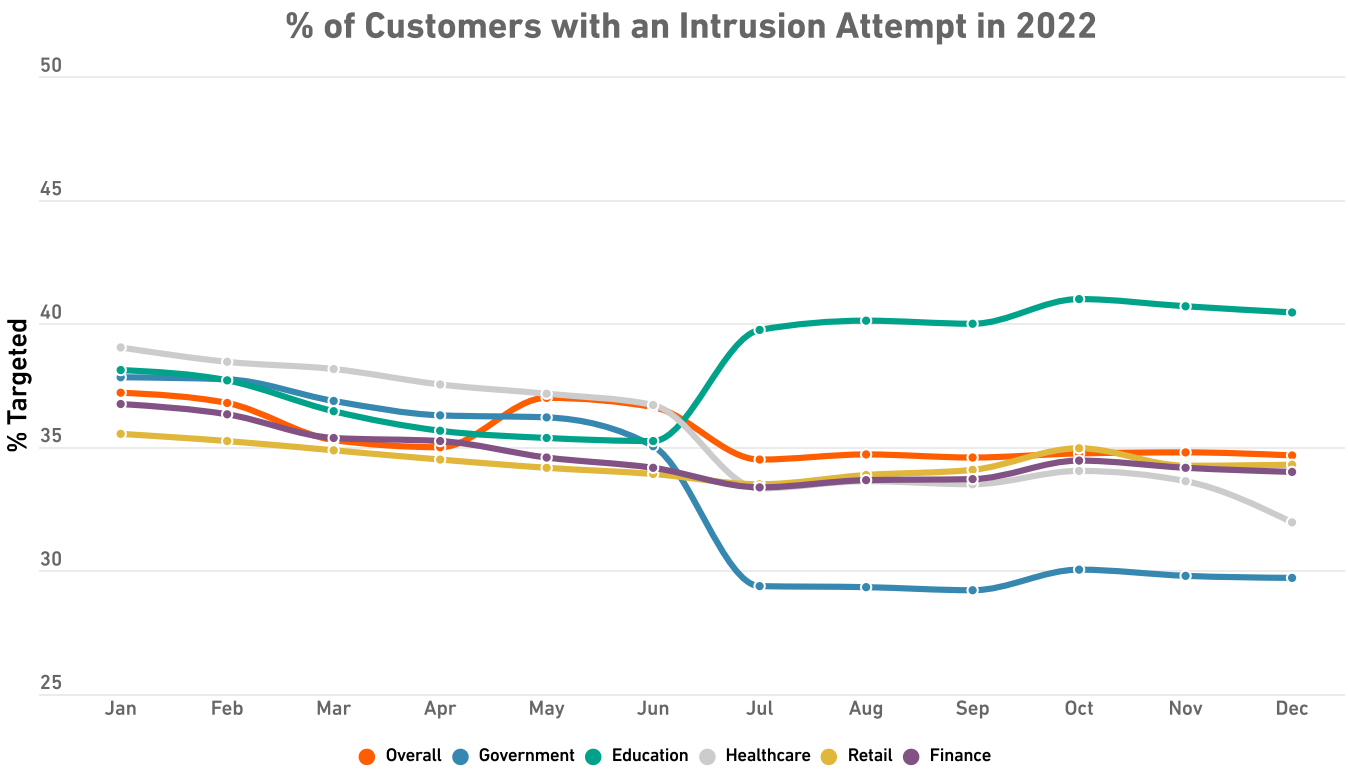
The biggest decrease in percentage of customers targeted by malicious intrusion attempts was for government: In 2021, 40.7% of these customers saw an attack, but in 2022, only 33.1% did.

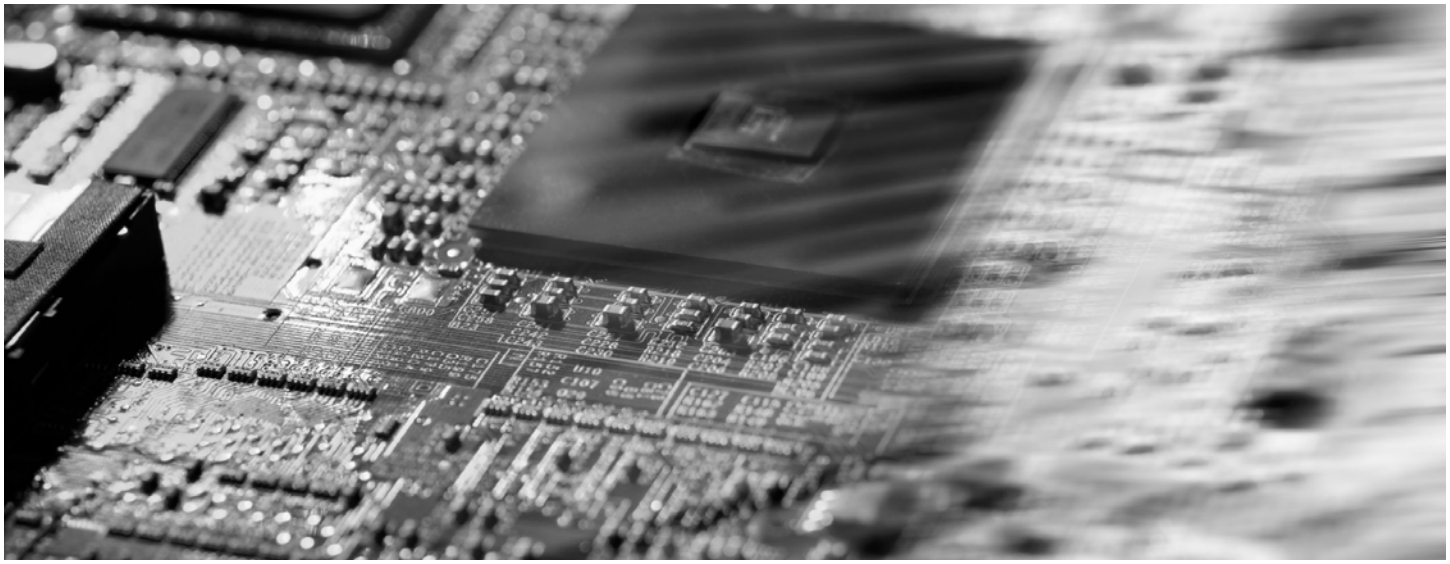
Combined with the 74% increase in attacks on government overall, this suggests that malicious intrusion attempts on government are becoming much more targeted.

The opposite held true for education customers. While education saw a sizeable drop in overall attacks, per-customer data showed the least-favorable trend, with the percentage of customers targeted falling only 3.2% year-over-year.

These averages (and their accompanying rankings) are largely courtesy of an odd divergence that began in Q3.

After remaining in the middle of the pack for the first half of the year, in July the percentage of education customers targeted rose several percentage points — and the percentage of attacks on government customers fell by nearly the same amount. Both trends persisted through the end of the year, suggesting a sustained change in cybercriminal behavior.





MALICIOUS PDF/OFFICE FILES

Malicious PDFs Up by More than a Third

In 2022, SonicWall Capture Advanced Threat Protection (ATP), which includes patented Real-Time Deep Memory Inspection™ (RTDMI), logged 119,549 new PDF-based attacks. This 35% increase pushed the number of attacks past the 100,000 mark for the first time since SonicWall began tracking these threats.

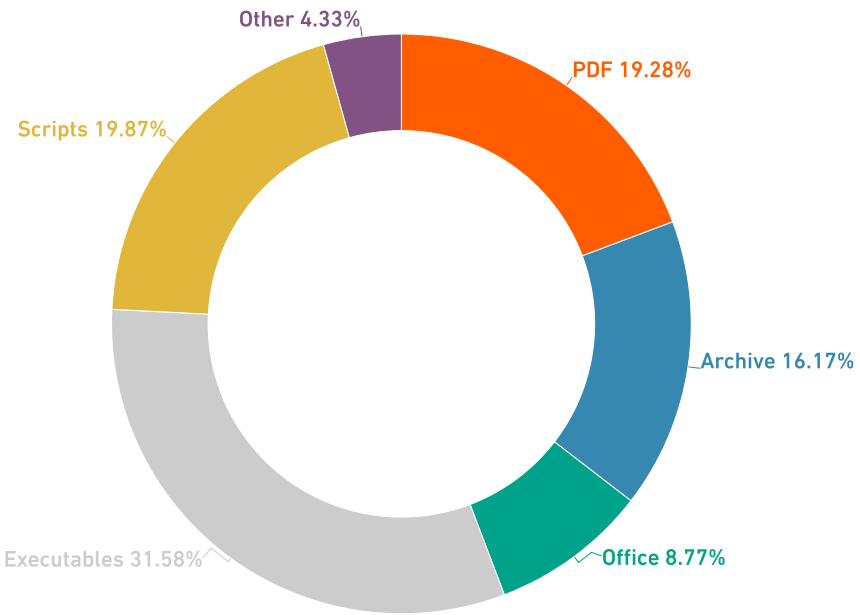
The number of malicious Microsoft Office files rose too, but just barely — the total number of malicious Office files in 2022 was 54,371, just 3% higher than 2021's total.

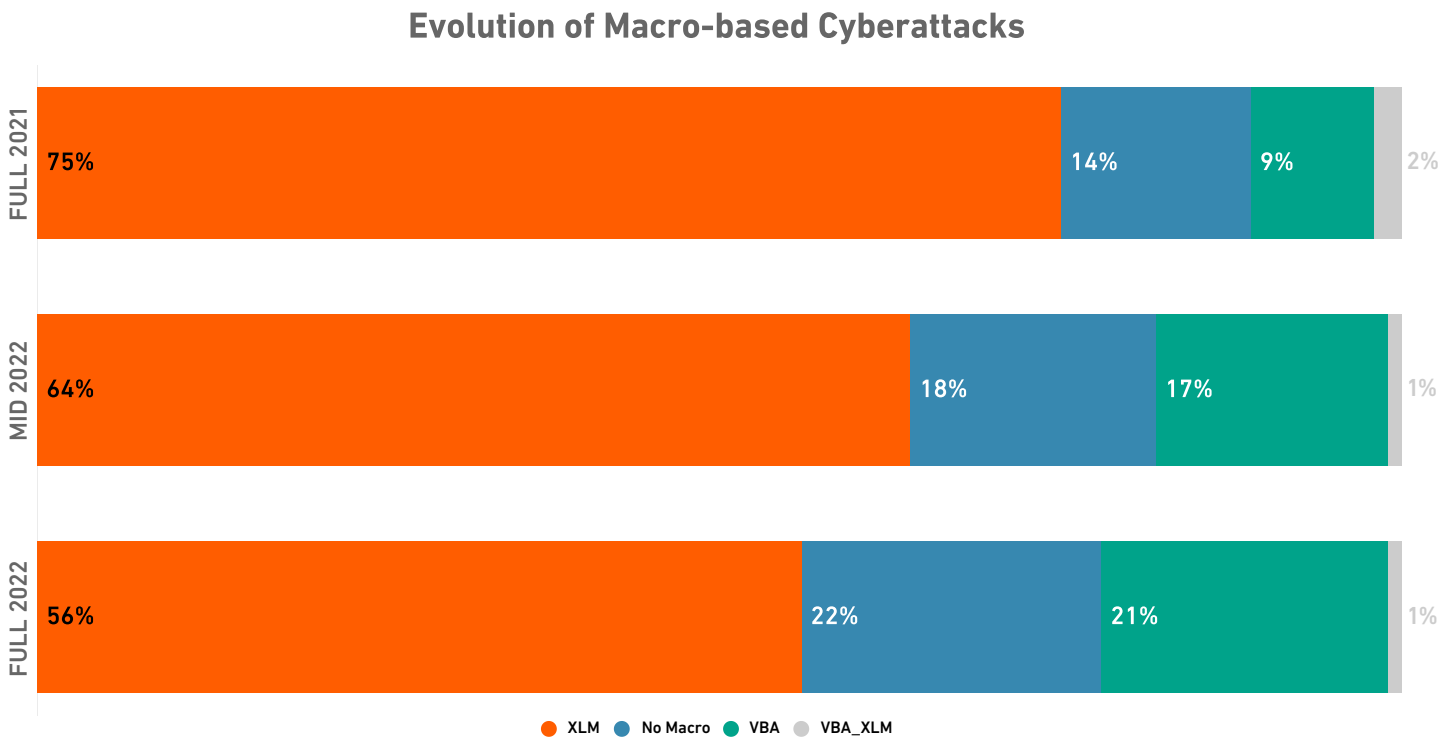
2021 turned out to be an inflection point in attacks using PDF versus attacks using Office files. Weaponized office files were the preferred means of attack in 2018, 2019 and 2020.

But in 2021, the trend began to shift in favor of PDFs — and in 2022, the number of malicious PDFs was double the number of malicious Office files.

But while malicious PDFs and Office files are among the most dangerous malicious filetypes, due to their ability to blend in with legitimate and expected attachments in a work environment, they aren't the most common. For the second year in a row, that dubious distinction belonged to .exe files.

2022 New Malicious File Type Detections | Capture ATP





A Macro-Level Difference

For the past several years, XLM macros, also known as Excel 4.0 macros, have been a popular tool for cybercriminals. These macros were first included in Microsoft Excel in 1992, but were quickly replaced by XLM's successor, VBA.

For decades, XLM was little more than a relic — but in 2015, Microsoft released its Antimalware Scan Interface (AMSI), which included the capability to scan for malicious use of VBA macros. Ever on the lookout for ways to circumvent defensive measures, threat actors seized on the less capable but largely forgotten XLM macros as a way to continue to slip under the radar.

That year, researchers began to observe coordinated attempts by cybercriminals to exploit these macros, but it would be another five years before widespread attacks leveraging Excel 4.0 macros really took off. In 2020, the use of this tactic accelerated dramatically, and eventually included campaigns utilizing the macros to spread Emotet, Trickbot, Zloader and more.

But between 2021 and 2022, SonicWall Capture Labs threat researchers observed that the use of XLM dropped from three-quarters to not much more than half. What happened?

Deciphering the Drop

Two things, actually. In October 2021, Microsoft announced it would begin disabling Excel 4.0 macros by default in Microsoft 365 — a measure that was rolled out in January 2022.

Then, in February 2022, the company announced that VBA macros obtained from the internet would soon be blocked by default on Windows devices running its Access, Excel, PowerPoint, Visio and Word apps. This change was rolled out in mid-July.

So what we're likely seeing reflected in these graphs is, first, the announcement regarding XLM causing the number of XLM macros to drop 11% in the first six months of 2022, accompanied by a corresponding near-doubling in the use of VBA files.

Then, in the next six months — during which time the announcement regarding VBA was made — we see a significant slowdown in the growth of VBA macros, but sustained growth in malicious Excel files using no macros.

The Future of Malicious Office Files

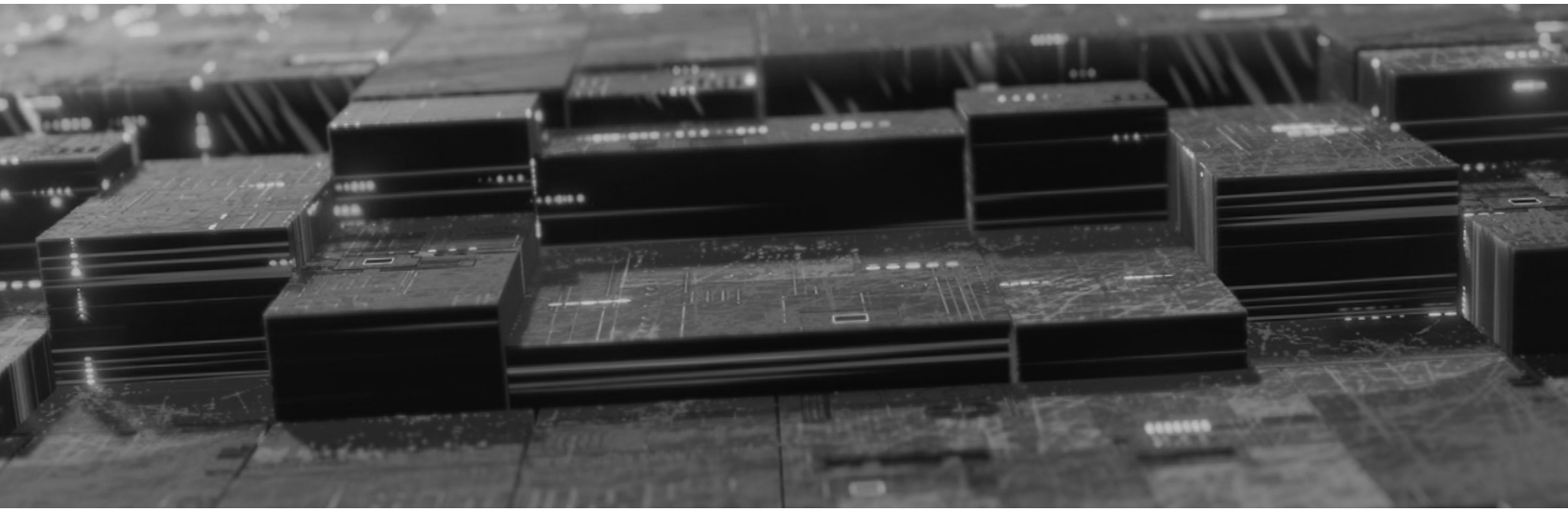
Unless new evasiveness tactics are developed, it's likely that we'll continue to see a drop in XLM macros and the beginnings of a drop in VBA macros as we make our way through 2023. In their place, we're likely to see accelerating growth in the use of malicious files without *any* macros, such as those exploiting vulnerabilities in MS-Office, making use of things like Dynamic Data Exchange (DDE) fields, or requiring a victim to click on a phishing link.

Rabota Retires, Posik Punches In

In last year's Cyber Threat Report, we noted that the most commonly observed author of malicious Office files was Rabota: Nearly 50% of those with an author listed were credited to this name.

In 2022, however, Rabota fell off the Top 10 list altogether. The heir apparent? Posik, who allegedly authored roughly as many files in 2022 as Rabota did in 2021.

The shakeup was apparently widespread: Aside from expected aliases like Admin, Test and User, the only author from 2021's list to appear on the list for 2022 is "brian."



IoT MALWARE

IoT Malware Nearly Doubles

When IoT malware attack volume rose just 6% in 2021 — after jumping 218% in 2019 and another 66% in 2020 — it offered hope that wild acceleration might be giving way to slower and more stable growth. Unfortunately, this easing would prove temporary: In 2022, SonicWall Capture Labs threat researchers recorded 112.3 million instances of IoT malware, an 87% increase over 2021.

This spike easily exceeded the previous record for IoT malware attacks observed by SonicWall in a single year, and it also pushed the number of attacks past the 100 million mark for the first time.

Within this overall yearly record were several smaller records. The global attack volume for January reached 12.54 million, surpassing the previous high-water mark by nearly 2 million. And in June, attack volume soared even higher, reaching 12.98 million. These higher-than-usual monthly attack volumes pushed quarterly totals to new records, as well. The only quarter not to set a new attack volume record was Q3 — and it wasn't far off, at that.

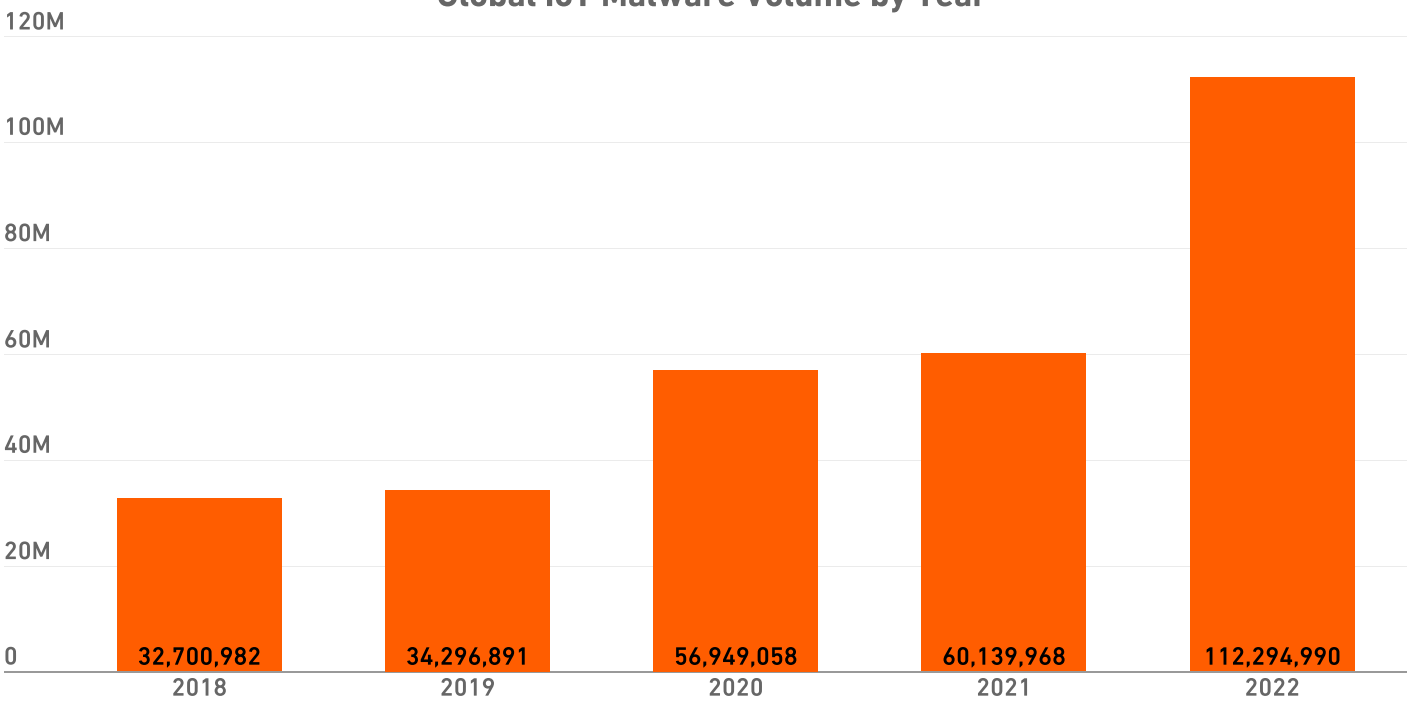
What is IoT Malware?

IoT malware is a type of malware specifically designed to take over connected, or IoT, devices. This malware gains entry through vulnerabilities, exploit kits, weak or compromised credentials, and other means. Because these devices are often not very powerful on their own, IoT malware is generally deployed en masse with the intention of creating botnets of many infected IoT devices. These botnets are controlled either via a command-and-control server that connects to each infected device, or through the use of peer-to-peer networking.

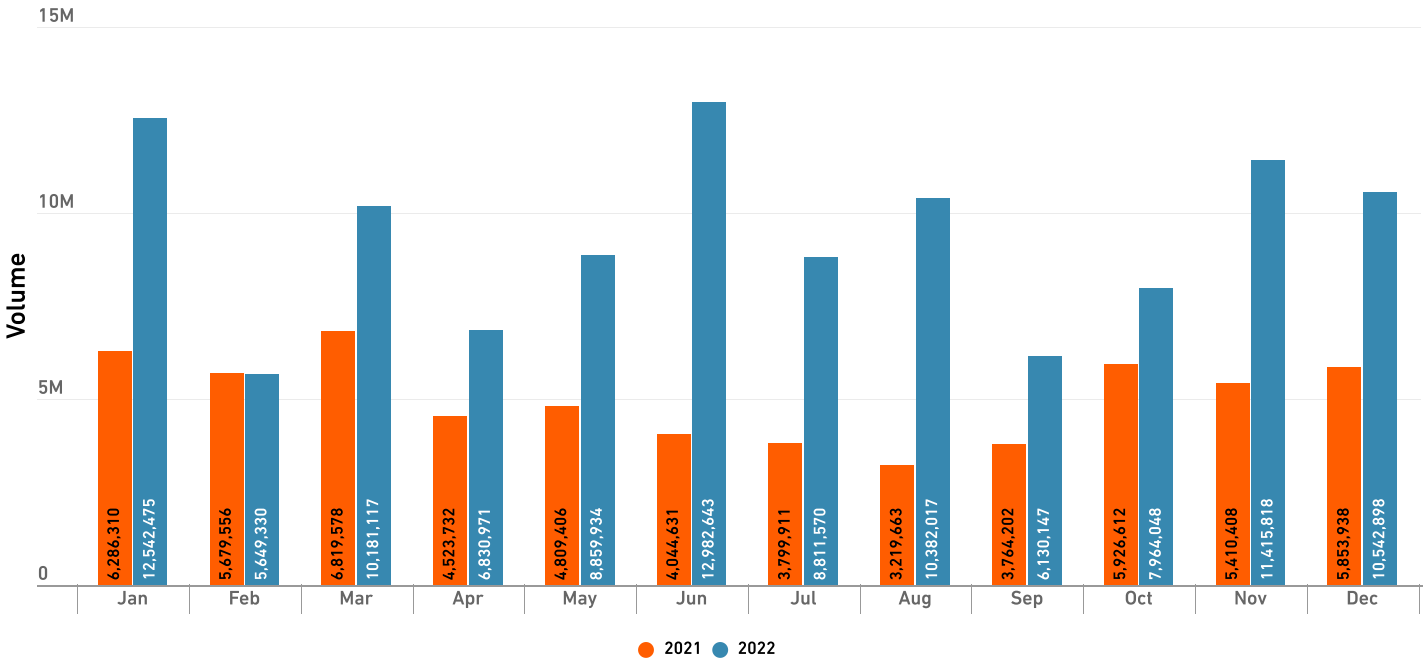
Once connected, these devices can work together to perform malicious activities, such as launching of Distributed Denial of Service (DDoS) attacks, installing and running cryptojacking malware, conducting brute-force attacks to deploy ransomware or steal data, or sending spam emails.

The Mirai botnet is the most famous example of this type of malware, but there have been many others.

Global IoT Malware Volume by Year



Global IoT Malware Volume



IoT Malware by Region

Given the global IoT malware increase, it's unsurprising that there were significant, across-the board increases at the regional level. IoT malware volume in Europe increased 21%, followed by the LATAM (65%) and Asia (73%) regions.

And while overall malware, ransomware and other threat types saw attacks fall in the hardest-hit regions, IoT malware did not follow this pattern. North America, which experienced the biggest increase at 145% year-over-year, already led the pack in IoT malware attacks — and it has for three years running.

As cybercriminals doubled down on attacking targets in North America last year, the gulf between it and the second-highest region widened from just a few million to roughly *40* million: By the end of 2022, North America had recorded 62.9 million attacks, versus 23.2 million in Europe.

On a country-by-country level, the two countries that typically see the highest IoT malware attack volume also saw triple-digit increases. The U.K., which has the second-highest attack volume, saw IoT malware increase 163%. And in the U.S., which typically sees the most attacks, attack volume rose 169%.

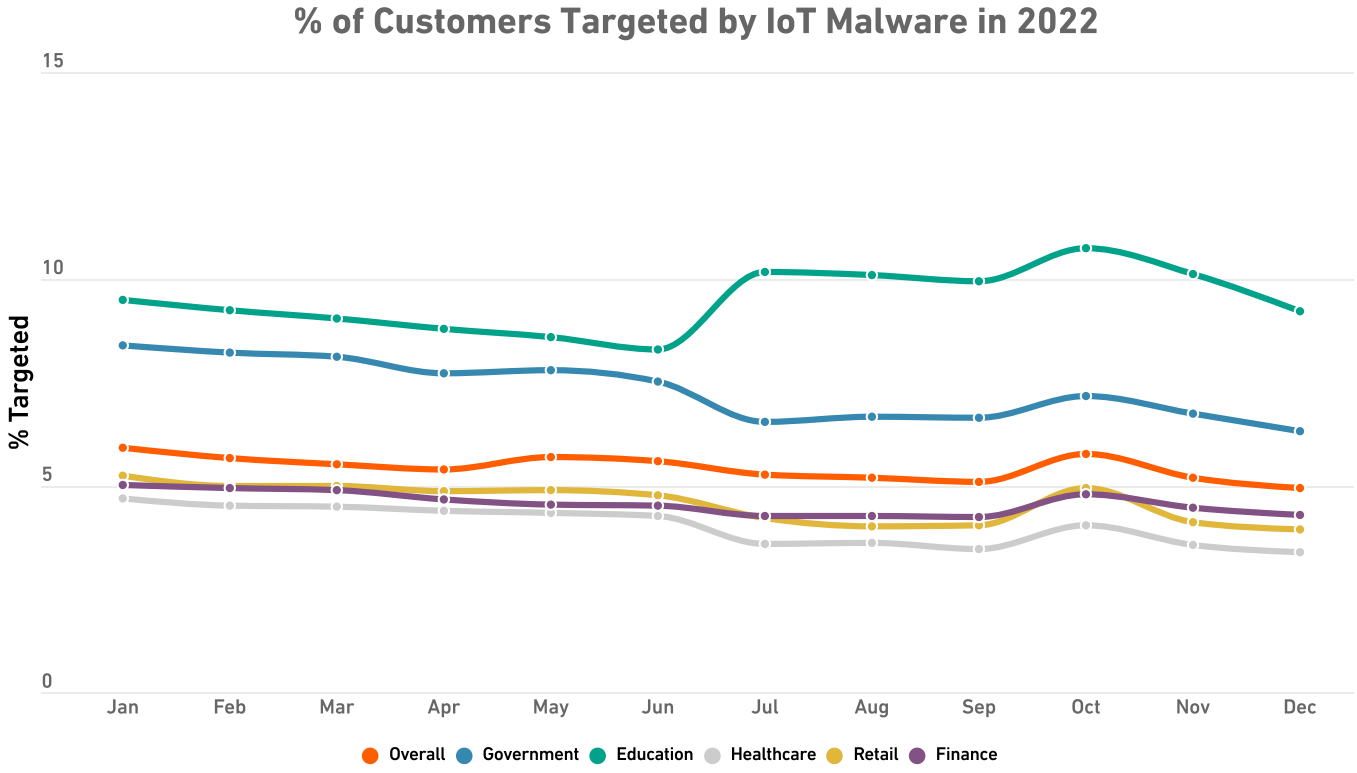
IoT Malware by Industry

For the second year in a row, SonicWall Capture Labs threat researchers observed increases in IoT malware volume across every industry studied — and this year, the increases were even bigger.

Healthcare customers saw the least change, with a 33% year-over-year increase in attacks. Government, which saw a jump of 40%, wasn't far behind.

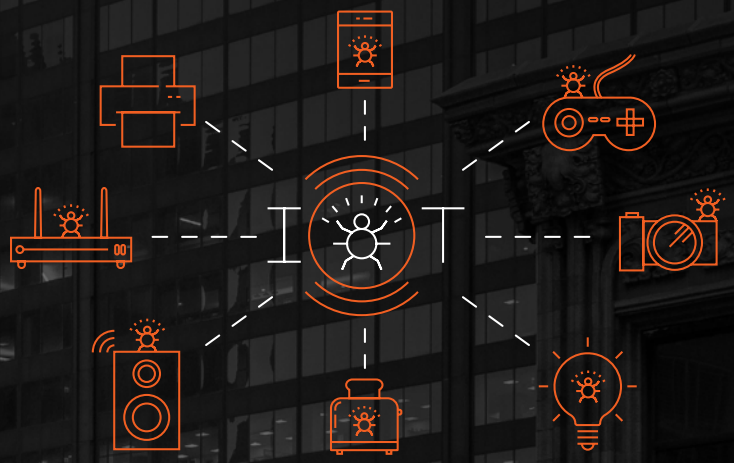
The news gets considerably worse from here, however: Retail experienced a 159% increase in attack volume, and education wasn't much better off at 146%. But it was finance that saw the brunt of the increase: attacks on finance customers skyrocketed 252% year over year.

On a per-customer basis, the rankings remained mostly the same in 2022 as they were in 2021, with the only exceptions being retail and finance. Always close in terms of the percentage of customers targeted, this year retail surpassed finance, but only by the tiniest margin.



Safeguarding Your Smart Devices

While the number of connected devices coming online continues to grow — currently estimated at 17 billion and counting — the types of devices most targeted for attack remains roughly the same year after year. In 2022, SonicWall continued to observe the highest attack volumes targeting routers, cameras, firewalls, load balancers and Network Attached Storage (NAS) devices. As of February 2023, SonicWall has 438 signatures protecting more than 136 IoT device families from various threats, including the device types seen here:



PRODUCT LINE	NUMBER OF SIGNATURES	HITS
D-Link Router	9	31,016,331
Hikvision IP Camera	2	19,251,146
NETGEAR DGN	2	14,451,612
Dasan GPON Router	3	7,823,114
ZyXEL Firewall/NAS	11	4,381,335
Cisco Adaptive Security Appliance	8	4,161,243
D-Link products	21	3,626,533
F5 BIG-IP	8	3,366,830
Vacron NVR	1	1,140,007
Draytek Vigor	2	1,119,891

PRODUCT LINE	NUMBER OF SIGNATURES	HITS
Yealink	1	1,067,806
Drobo products	1	990,225
Tenda Router	5	867,765
NETGEAR products	9	353,208
WIFICAM	1	261,672
Buffalo Routers	1	152,545
HiSilicon-based Devices	1	149,151
Netlink GPON Router	1	137,718
TP-Link Router	4	133,183
Wavlink	2	115,765

The Ever-Evolving Landscape of IoT Regulations

For anyone putting their trust in IoT devices, 2022 was an eye-opening year. Microsoft announced in December that 75% of industrial control devices — such as the ones used in water treatment facilities, power plants and more — have severe, unpatched vulnerabilities.

Not that our increasingly connected vehicles are much safer. In January, a 19-year-old researcher announced he could exploit a bug on the TeslaMate dashboard to run commands on over 25 vehicles in 13 countries. Five months later, another researcher used a Bluetooth device to enroll his own NFC key and take control of a vehicle.

And as the year drew to a close, we learned our robot vacuums and other IoT devices could record us doing … well, pretty much anything.

Given the persistent and egregious lack of security in many connected devices, it's no wonder that in 2022, many governing bodies around the world set their sights on tightening regulations around IoT security. Here are just a few:

United States

In February, the National Institute for Standards and Technology (NIST) published its Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things. Based on these recommendations, private sector leaders, academic institutions and the U.S. government convened in October to advance a national cybersecurity labeling program for IoT devices. Discussions centered around how to best implement the labeling program, how to generate a globally recognized label, and how to work toward improved security standards for connected devices. Rollout for the program is expected to begin in spring 2023.

United Kingdom

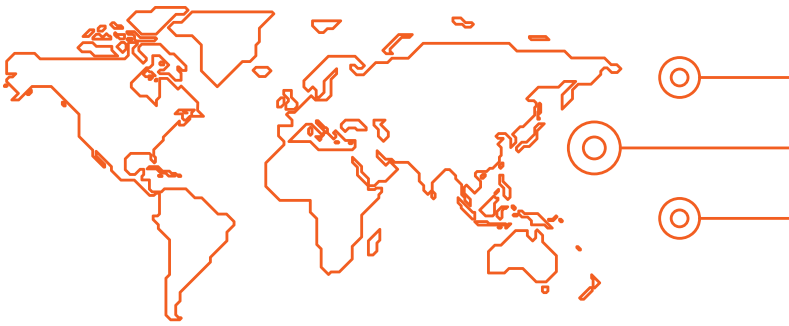
On Dec. 6, the Product Security and Telecommunications Infrastructure Act of 2022, or PSTI Act, became law. These new regulations ensure that consumer IoT devices are more secure against threats by banning default passwords and stipulating that manufacturers disclose how long they plan to offer product security updates. To ensure compliance with the new regulations, the law sets up an enforcement regime that includes civil and criminal sanctions, and also ensures that manufacturers have a point of contact for reporting issues and vulnerabilities.

Singapore, Canada and United Kingdom

A collaborative effort between Singapore, Canada and the U.K. was announced in November 2022. The three countries plan to work together to support and promote the creation of international standards and security requirements to replace the current fragmented patchwork of regulations worldwide. "Through this global alignment," the announcement read, "we can reduce duplication of testing and similar assessments and the challenge for industry of needing to apply to multiple schemes underpinned by identical or very similar requirements."

European Union

The European Union's Cyber Resilience Act was proposed in September 2022. This legislation aims to address the lack of cybersecurity in consumer IoT products, as well as a lack of updates or patches to address vulnerabilities. Unlike the voluntary guidance issued by some nations, the Cyber Resilience Act allows for large fines and penalties for violators, and it specifies that products failing to meet the outlined safety requirements will not be permitted to go to market.



NON-STANDARD PORTS

Non-Standard Port Attacks Defy Expectations

In past cyber threat reports, we've noted that non-standard port attacks have followed a predictable pattern since SonicWall began tracking them in 2018. Attacks would rise in even-numbered years and fall in odd-numbered years, with odd-numbered years seeing more attacks in the first half and even years seeing more in the second half.

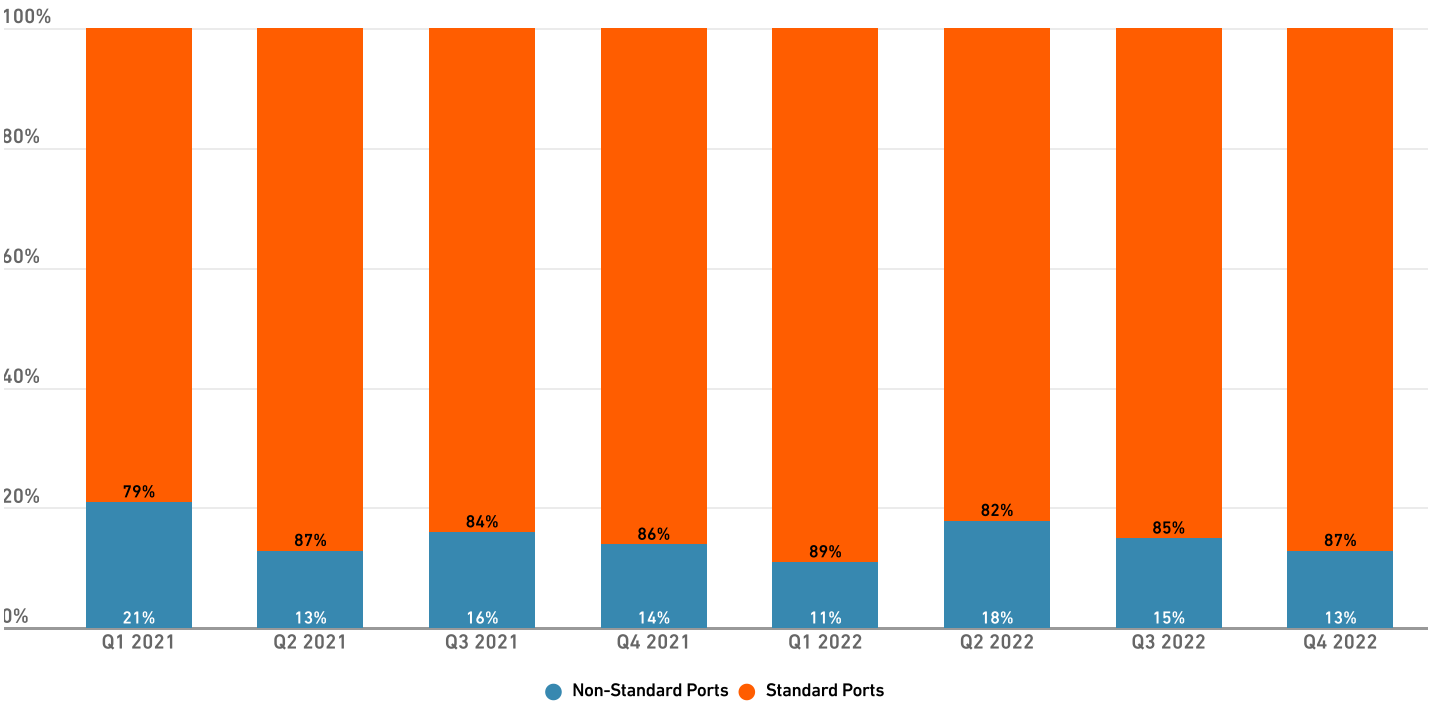
Based on how many other longstanding trends fared in 2022, you may have some idea of where this is going.

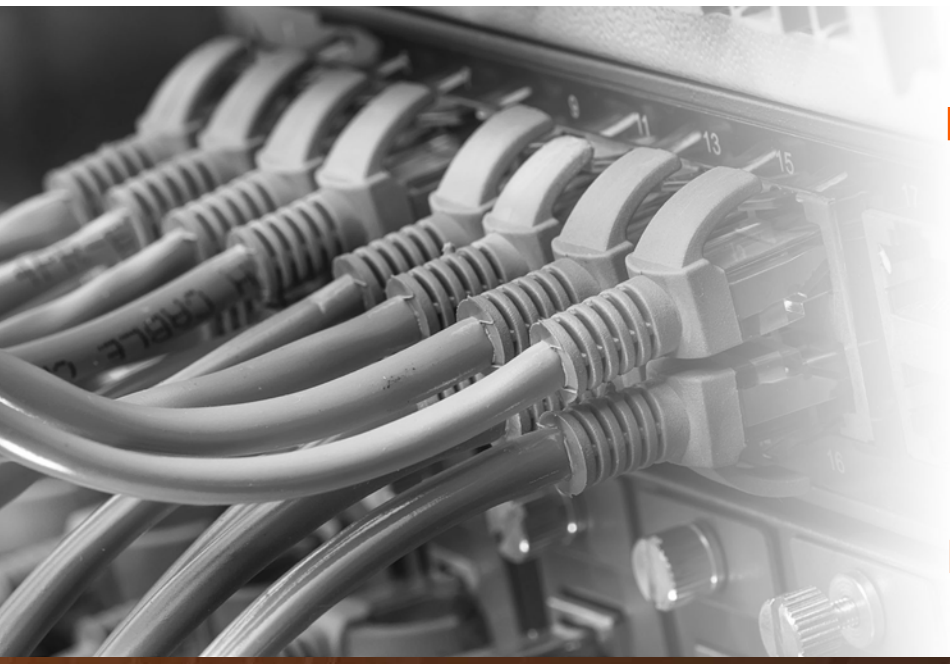
In the first half of 2022, SonicWall Capture Labs threat researchers found, on average, that 14.5% of attacks came through non-standard ports — more or less in line with expectations. But in the second half, something unusual happened: Attacks began to fall instead of rise.

With full-year data tabulated, 2022's second half had *fewer* attacks via non-standard ports, not more. And with 14% of attacks going through non-standard ports in 2022, it was the first time SonicWall had ever seen these attacks drop two years in a row.

While it's too early to say what the new paradigm will be, there are some emerging trends. Our prediction that attacks likely wouldn't dip back into the single digits held true in 2022, but nor did they come close to approaching the heights we've seen in previous years. This decrease in variation, coupled with just a 2% year-over-year change, indicates we may be seeing attacks begin to stabilize.

2021-22 Global Malware Attacks





IN THE FIRST HALF OF 2022, SONICWALL CAPTURE LABS THREAT RESEARCHERS FOUND, ON AVERAGE, THAT 14.5% OF ATTACKS CAME THROUGH NON-STANDARD PORTS.

What is a Non-Standard Port Attack?

In networking, a port number uniquely identifies the endpoint of a connection and directs data to a particular service. While around 40,000 ports are registered, only a handful — the "standard" ports — are generally used. For instance, HTTP uses port 80, HTTPs uses port 443, and SMTP uses port 25. Any service using a port other than the one assigned to it by default, usually as defined by the IANA port numbers registry, is using a non-standard port.

There's nothing inherently wrong with using non-standard ports, but they can present cybersecurity challenges.

Traditional proxy-based firewalls generally focus their protection on traffic going through the standard ports — but with so many ports to monitor, these legacy firewalls are unable to mitigate attacks coming over non-standard ports.

As a result, threat actors target non-standard ports to increase the odds of remaining undetected as they deploy their payloads. That's why it's important to ensure your network is secured by a modern firewall capable of analyzing specific artifacts (as opposed to all traffic), and thus able to identify these attacks.

PHISHING

Health and Finances Top Phishing Topics for 2022

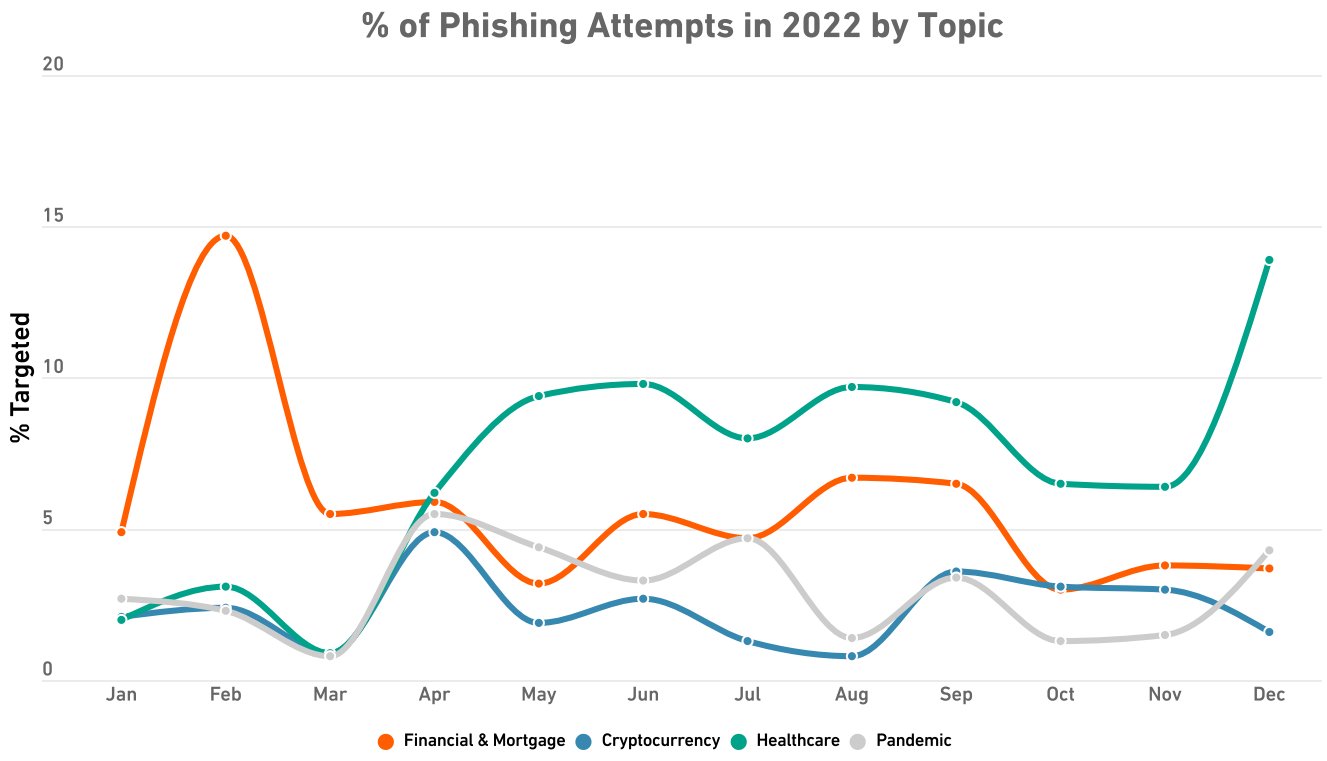
In 2022, phishing topics again tracked closely with current events. The top themes were Financial/Mortgage, Cryptocurrency, Healthcare and Pandemic.

As COVID-19 continued to shift from pandemic to endemic, SonicWall observed a drop in pandemic-related phishing, which contributed to a 17% decrease in phishing globally.

But attackers aren't just sending fewer emails, they're sending different ones: the number of finance- and mortgage-related phishing sent in 2022 saw a corresponding increase. These emails spiked in February, as falling economic indicators in many countries stoked recession fears and homebuyers found themselves caught between increased interest rates, a record low in housing supply and still-rising home prices.

In December, we see a similar spike in health-related emails, coinciding with the open enrollment periods of many insurance programs and headlines warning of a flu, RSV and COVID-19 "tripledemic."

In contrast, while we see an uptick in cryptocurrency-related emails in April, around when Bitcoin began to fall, cryptocurrency (and related topics such as NFTs) were hot topics all year, corresponding with a fairly steady and sustained rate of crypto-related phishing.



Ready to Test Your Phishing IQ?

With over 90% of data breaches starting with a phishing attack, it's never been more critical to know how to spot a phish. But today's phishing attacks are more subtle and sophisticated than ever before. Will you be able to spot the imposters?

TAKE THE QUIZ

CONCLUSION

The Next Step is Up to You

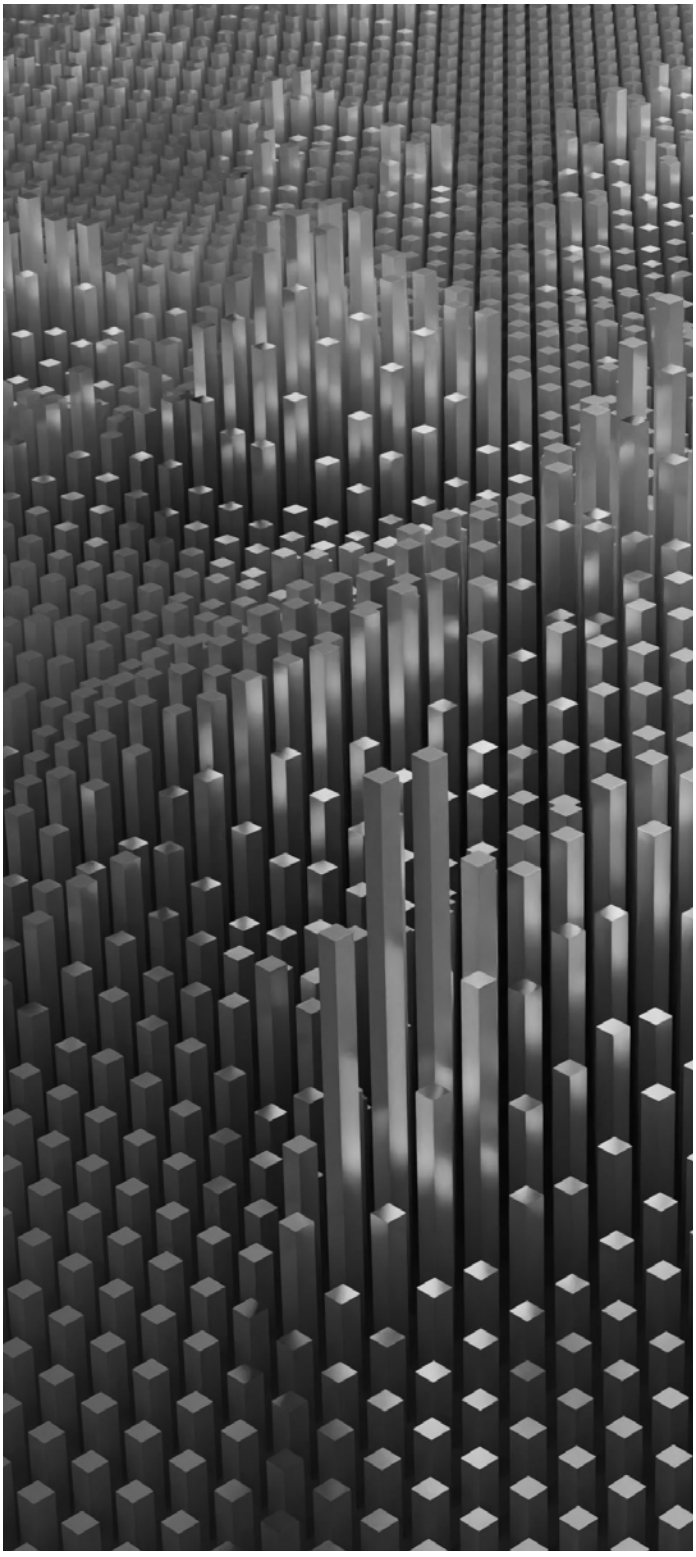
While threat research is a vital part of a larger cybersecurity plan, it's what you do with these insights that will make or break your security strategy. In conjunction with the 2023 SonicWall Cyber Threat Report, SonicWall threat researcher Immanuel Chavoya is offering an in-depth discussion on some of the best ways to put this data to work for your organization.

This webinar covers the importance of:

- Performing regular security assessments and penetration testing to identify vulnerabilities and weaknesses
- How to choose the best security monitoring and log management tools for your network
- Improving incident response plans and protocols to quickly and effectively contain attacks
- Developing a comprehensive disaster recovery (DR) plan
- How and when to regularly review and update security policies, standards and procedures to align with the latest threat information and best practices
- Why communication — with your employees, other organizations and industry groups — is key to upleveling your security posture
- And more

As cyber threats continue to evolve, it's essential for organizations to have a comprehensive understanding of the behaviors and tactics of threat actors. This webinar covers the importance of implementing and enhancing countermeasures based on the latest data. By understanding and addressing the specific tactics and techniques used by threat actors, organizations can more effectively prepare for, defend against and respond to cyberattacks.

RESERVE YOUR SEAT



ABOUT THE SONICWALL CAPTURE LABS THREAT NETWORK

Intelligence for the 2023 SonicWall Cyber Threat Report was sourced from real-world data gathered by the SonicWall Capture Threat Network, which securely monitors and collects information from global devices including:

- More than 1.1 million security sensors in 215 countries and territories
- Cross-vector, threat-related information shared among SonicWall security systems, including firewalls, email security devices, endpoint security solutions, honeypots, content filtering systems and the SonicWall Capture Advanced Threat Protection (ATP) multi-engine sandbox
- SonicWall internal malware analysis automation framework
- Malware and IP reputation data from tens of thousands of firewalls and email security devices around the globe
- Shared threat intelligence from more than 50 industry collaboration groups and research organizations
- Analysis from freelance security researchers

1.1m+
Global Sensors

215+
Countries & Territories

24x7x365
Monitoring

<24hrs
Threat Response

140k+
Malware Samples Collected Daily

28m+
Malware Attacks Blocked Daily

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com

© 2023 SonicWall Inc.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products.

EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/ OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION)

ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

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.

The materials and information contained in this document, including, but not limited to, the text, graphics, photographs, artwork, icons, images, logos, downloads, data and compilations, belong to SonicWall or the original creator and is protected by applicable law, including, but not limited to, United States and international copyright law and regulations.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

SONICWALL

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.

2023-CyberThreatReport-JK-7606