MID-YEAR UPDATE

2023 SONICWALL CYBER THREAT REPORT

TRACKING CYBERCRIMINALS INTO THE SHADOWS

SONICWALL®

sonicwall.com | @sonicwall

Table of Contents

INTRODUCTION

A NOTE FROM BOB

It's now been more than a decade since we published the first SonicWall Cyber Threat Report — and in the time since that initial report, the threat landscape has changed dramatically.

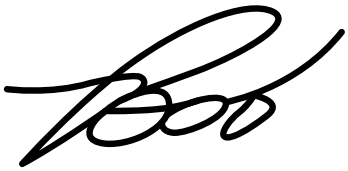
As cyberattacks continue to expand in scale and sophistication, the digital assault on governments, enterprises and global citizens is seemingly endless and evolving at a rapid pace. Threat actors are increasingly seeking out opportunistic targets, such as schools, state and local governments, and retail organizations, and have continued shifting away from enterprise targets in the U.S. to regions such as Latin America and Asia — especially as organizations that are more prepared refuse to pay ransoms.

Unlike the cybercriminal gangs of years past, who relied on reputation and branding, today's attackers are largely operating in secret. This is in part due to advances by law enforcement, which we applaud. By pivoting to lower-cost, less risky attack methods, such as cryptojacking, these attackers hope to reduce their risk of discovery while maximizing their profit.

We've spent the first six months of 2023 tracking the latest cyberattacks, and the result of our research is the Mid-Year Update to the 2023 SonicWall Cyber Threat Report. This report pulls key data and insight from the more than 1.1 million active sensors around the world that report threat information multiple times daily.

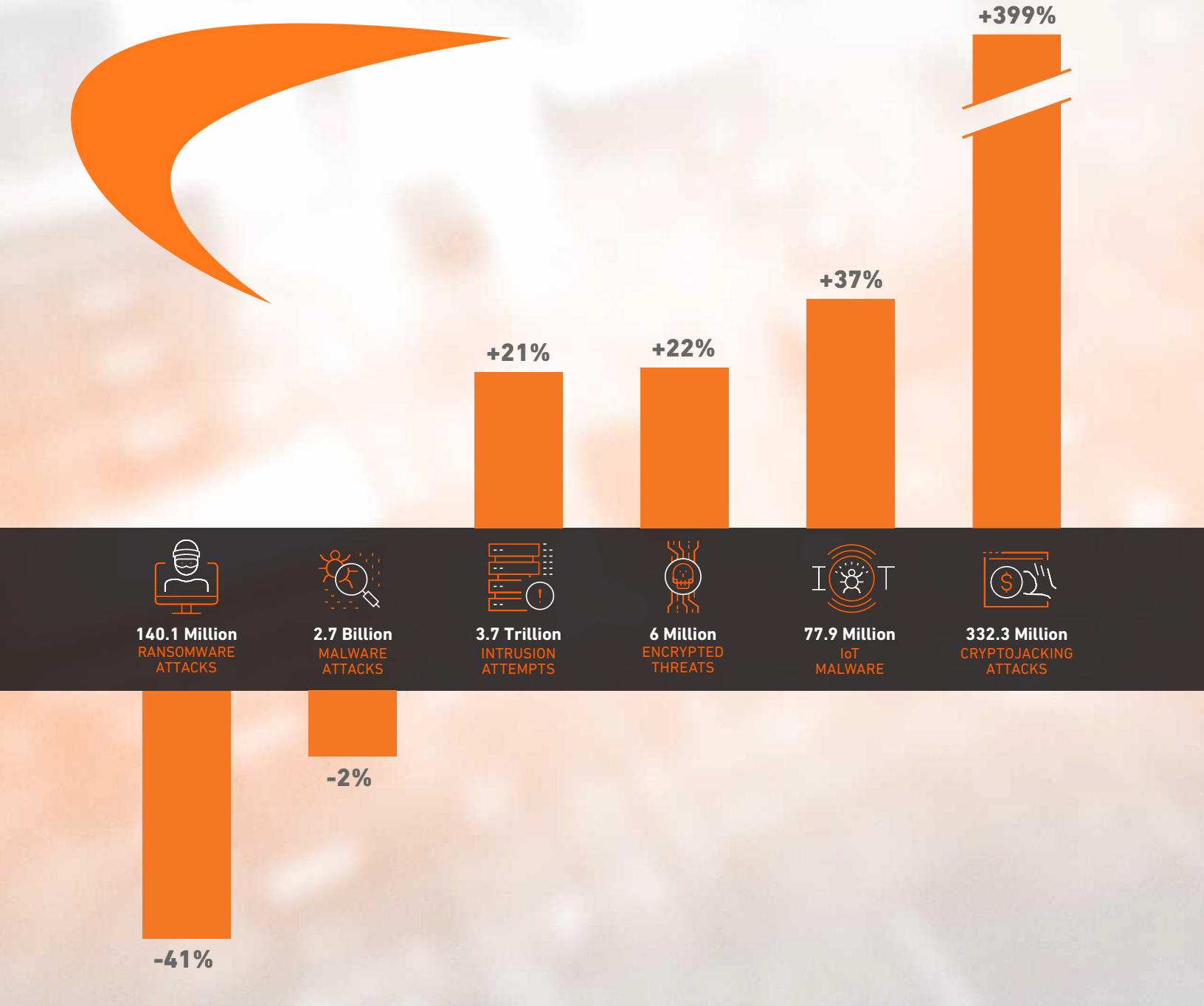
SonicWall has deployed millions of firewalls and endpoints globally, which is a testament to how much our partners and customers depend upon SonicWall every day. The SonicWall team remains focused on providing the highest level of security efficacy at a cost-effective price point for businesses, organizations and governments of all sizes. A key aspect of our world-class security efficacy is observing and using our threat data to build stronger defenses and solutions to guard against malicious activities — particularly at times like these, when threat actors and their attacks continue to evolve and attempt to evade detection.

On behalf of our Capture Labs threat researchers and the rest of the SonicWall team, we're pleased to present this firsthand look into evolving cybercriminal behavior, along with the actionable threat intelligence you need to safeguard your network and your customers against an increasingly volatile threat environment.



Bob VanKirk
President & CEO
SonicWall

2023 GLOBAL ATTACK TRENDS



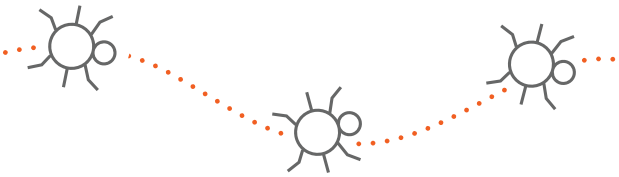
As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time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

MALWARE

Malware Continues Its Migration

During the first six months of 2023, SonicWall Capture Labs threat researchers recorded 2.7 billion malware attempts globally, down just 2% from the 2.8 billion observed during the same time period in 2022.

But while the year-to-date change was essentially flat, the trend line was anything but. While there were both peaks and valleys as the first half wore on, the direction was decidedly upward — leading to a June monthly volume of 576 million. Not only was this 46% higher than the 395 million hits observed in January, it was also the highest monthly malware total recorded since March 2020.

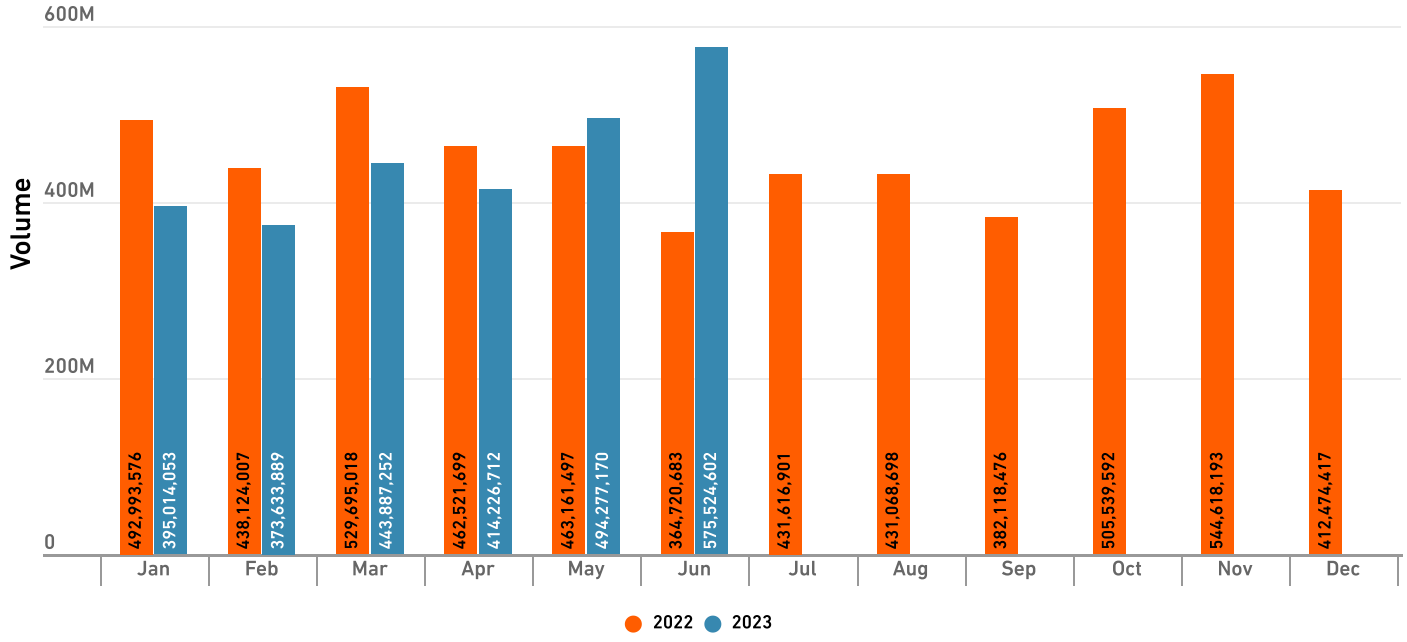


Malware Trends

Based on SonicWall threat data, cybercriminals have continued shifting their sights to new areas — resulting in fewer malware attacks in North America, and more in Europe, Latin America and Asia. Here are some examples of such attacks from the first half of 2023:

- EU governments and agencies have been targeted by spear phishing campaigns spreading PlugX and other malware via malicious Office and PDF files.
- Politically motivated attacks have targeted journalists, government officials and activists in Latin America.
- Several campaigns targeting Asian countries have been identified, including DownEx, FluHorse and DragonSpark.
- Emotet malware is back in full force, and SonicWall has observed a huge spike in Emotet attacks spreading via massive Microsoft Office docs.

Global Malware Volume



SONICWALL

Malware by Region

A look at the areas being attacked also reveals a great deal of change so far in 2023. With 1.3 billion hits (out of a global total of 2.7 billion), North America remains the world's malware epicenter. But this region was also the only one to show a decrease, falling 12% year to date.

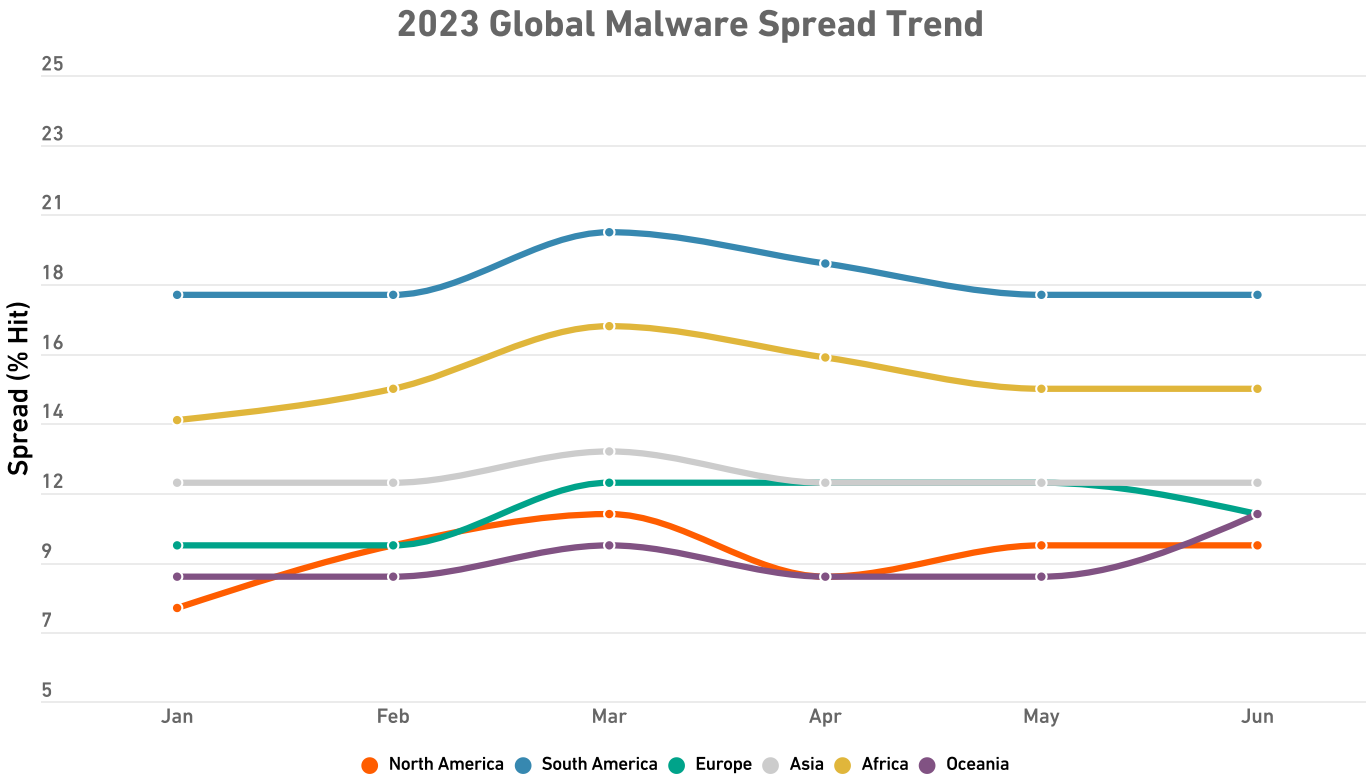
Malware attempts in Asia rose, but only modestly: SonicWall recorded 417 million hits in the region through the end of June, an increase of just 2% over the same time period last year.

In contrast, Europe and Latin America both experienced double-digit growth: Malware in Europe jumped 11% to 707 million hits, and attacks in Latin America spiked 19% to 199 million hits.

Malware Spread

But even as malware ebbs, flows and changes course, there's one thing we've come to count on. Since March 2020, malware spread has peaked in March, and 2023 was no different. Every continent showed a peak in March, and in 5 out of 6 of them, this peak was the highest of the entire first half. (The sole exception, Oceania, was very close: While malware spread there indeed peaked at 10% in March, it rallied again in June, climbing to 11%.)

But that's not the only trend from 2020 that persists to the present day. The other has to do with the malware spread rankings: Each year, South America has the highest malware spread of any other continent. And unlike the back-and-forth we observe among the other continents, South America's trend line is never crossed.



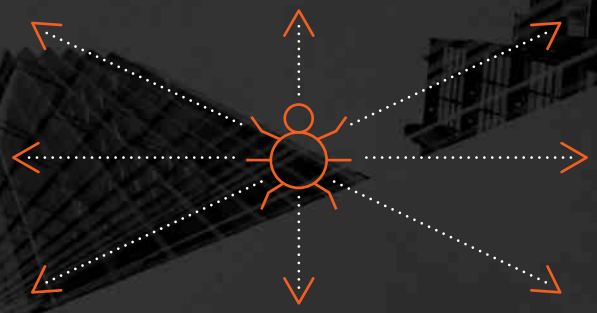
What is Malware Spread?

Malware volume for a given area is useful in calculating trends, but less so when it comes to determining relative risk: This data ignore factors such as size, population, number of sensors and more.

By calculating the percentage of sensors that saw a malware attack, we get much more useful information about whether an organization is likely to see malware in an area. The greater this malware spread percentage, the more widespread malware is in a given region.

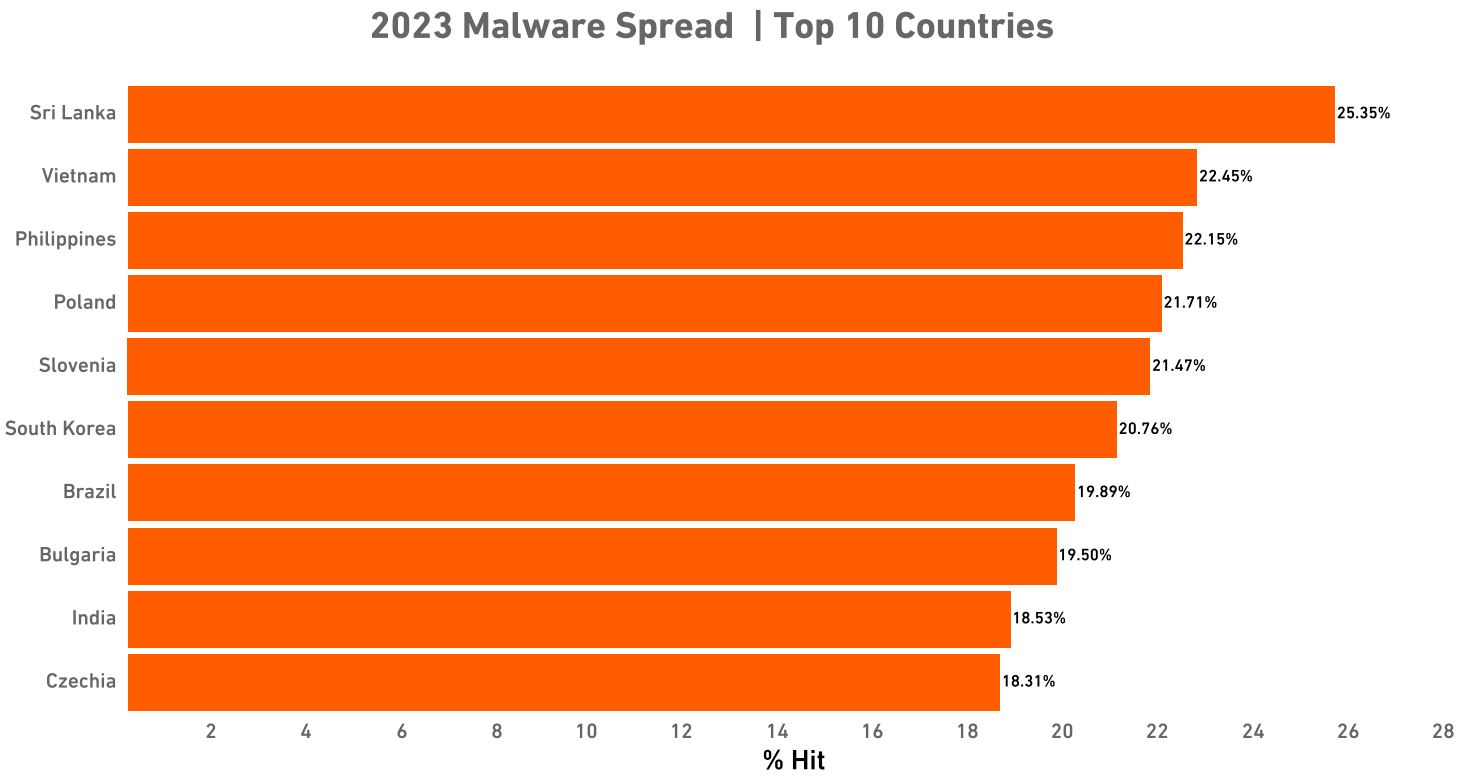
It can be helpful to compare malware spread with how we explain precipitation. Knowing the total amount of rainfall in an area can be useful for year-over-year comparisons, but it can't tell you whether you're likely to need an umbrella.

For that, you need the Probability of Precipitation, or the "chance of rain." Like the malware spread percentage, this calculation considers a number of other factors to provide a more meaningful risk assessment.



SonicWall also tracks volume and spread metrics on a by-country basis — though these often don't show as much correlation as you'd expect. The countries with the highest malware volume so far in 2023 are U.S., India, Spain, U.K., and Germany. But this doesn't mean that a given organization in these countries was more likely to see malware.

As in most years, we see that most of the highest-volume countries don't even make the list for malware spread, though this year there's a greater amount of crossover than usual. Four countries — India (No. 2), Brazil (No. 6), Vietnam (No. 7) and Philippines (No. 10) — also made the top 10 list for malware spread, as you can see in the graph below:

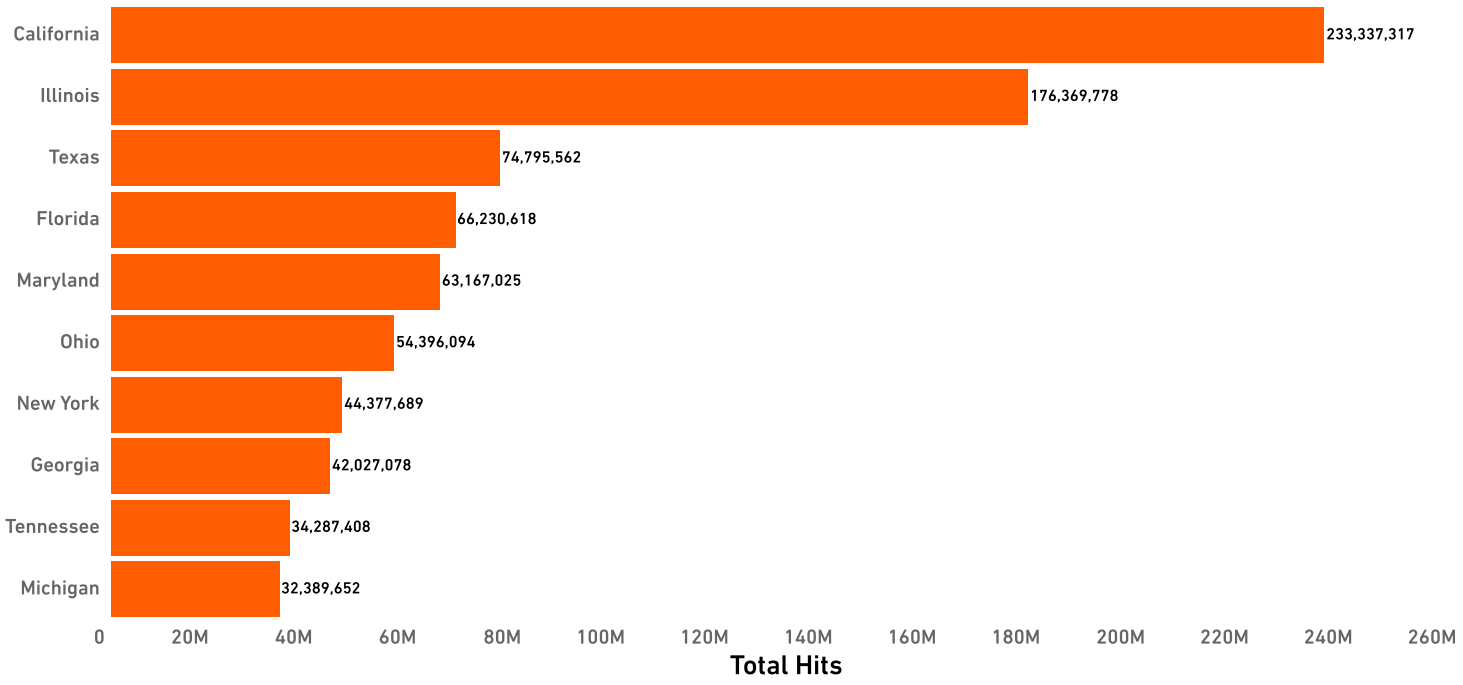


In the first half of 2023, an organization located in Sri Lanka had the highest chance of seeing an attack, at 25.4%. In contrast, for the second year in a row, Luxembourg was the "safest" country in terms of malware: An organization there had only a 4.5% chance of experiencing an attack.

Malware By State

A look at malware volume rankings by state shows that cybercriminals are shifting targets here, too. The state with the highest malware volume last year, Florida, fell all the way to No. 4 this year. No. 2 California moved up into the top position, No. 3 New York fell to No.7, No. 4. Illinois is now No. 2, and No. 5 Texas is the new No. 3.

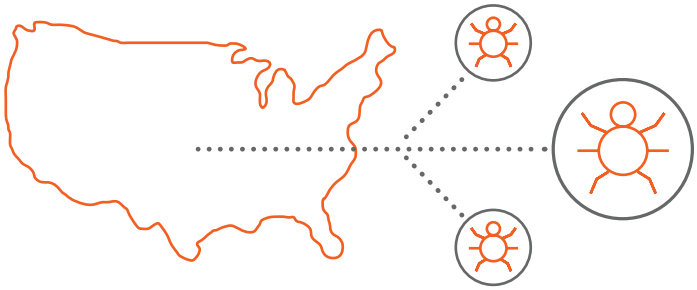
But while all of last year's top 5 found themselves on this year's list, most of the other states from the 2022 Top 10 did not: Minnesota, Rhode Island, South Carolina and New Jersey all fell off the list, and were replaced by Ohio, Georgia, Tennessee and Michigan.



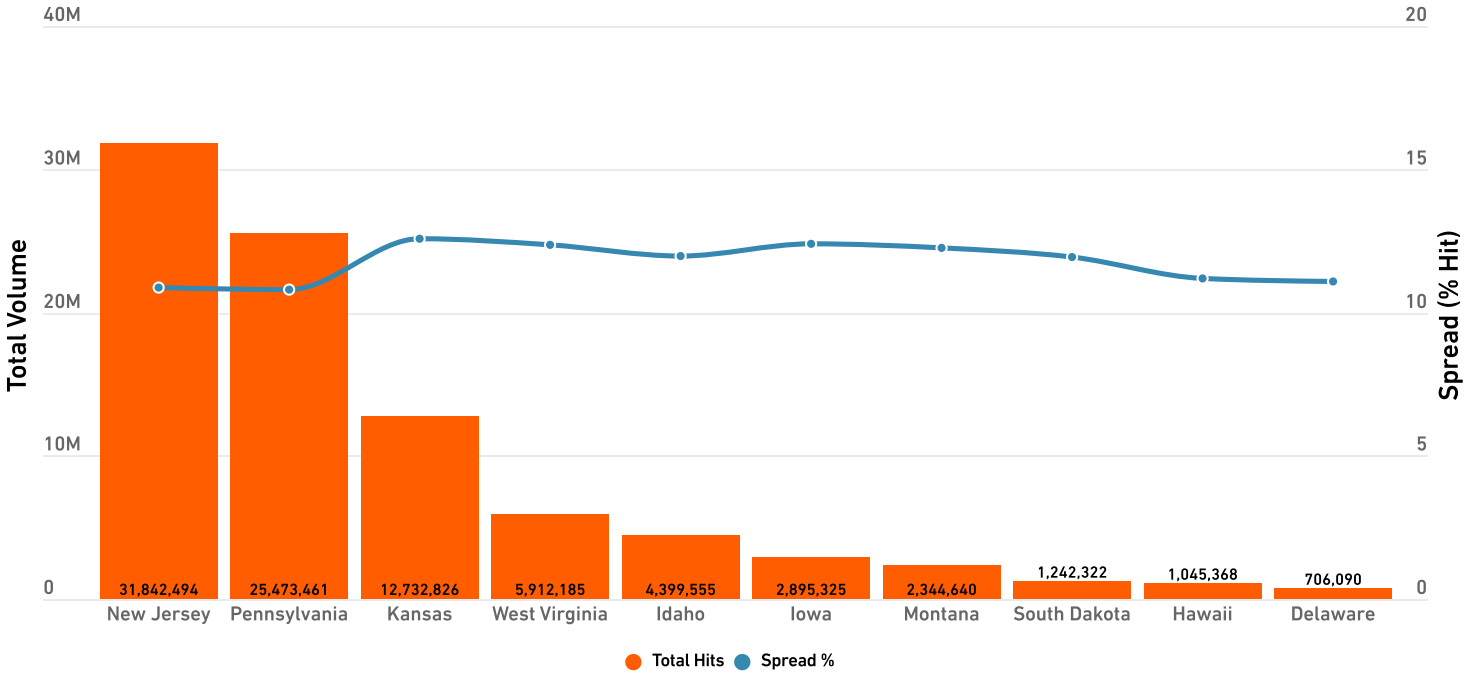
But as we saw with the country-specific data, larger malware volumes don't necessarily predispose an area to higher malware spread percentages. In fact, none of the top-ten states for volume also made the top-ten for malware spread.

So if none of the top ten states for volume are the riskiest in terms of malware, which state is? Once again, it's Kansas, where 12.6% of SonicWall sensors registered a malware attempt. 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.

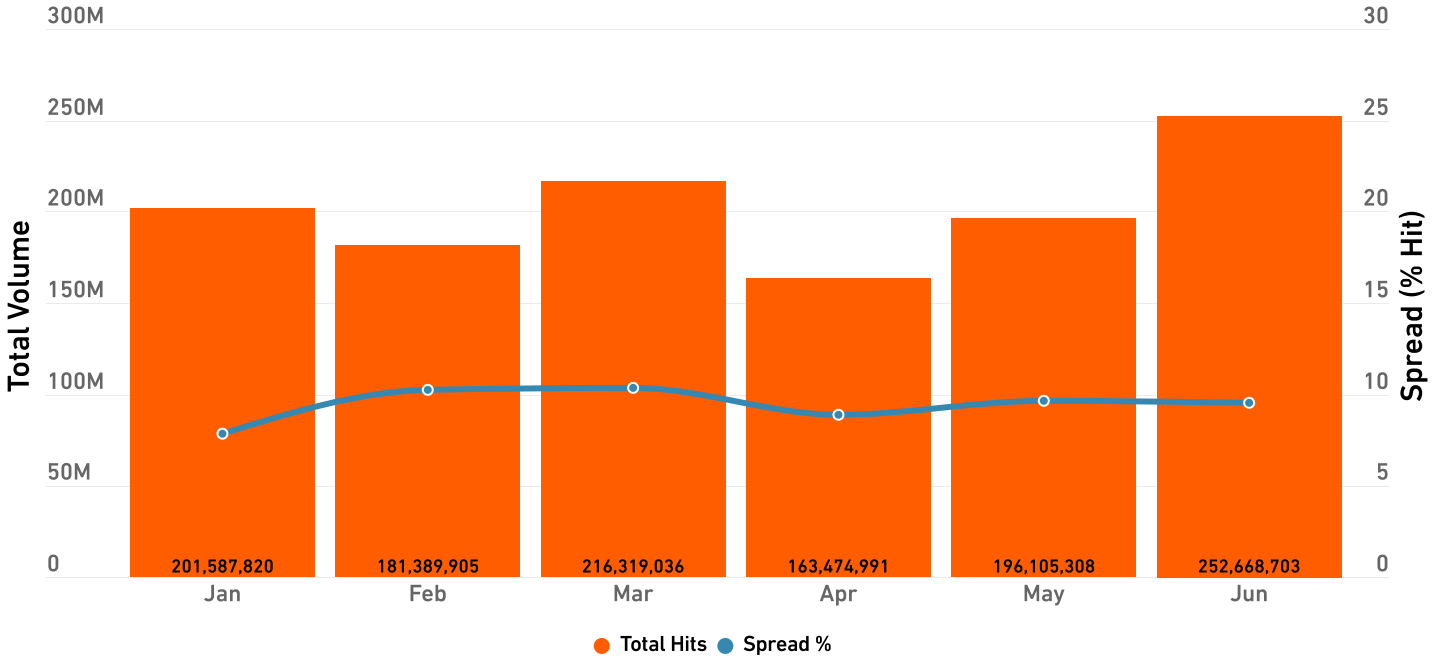
At the other end of the malware spread spectrum was Maine, where only 7.4% of sensors logged a malware attempt.



2023 Malware Spread | Top 10 Riskiest U.S. States



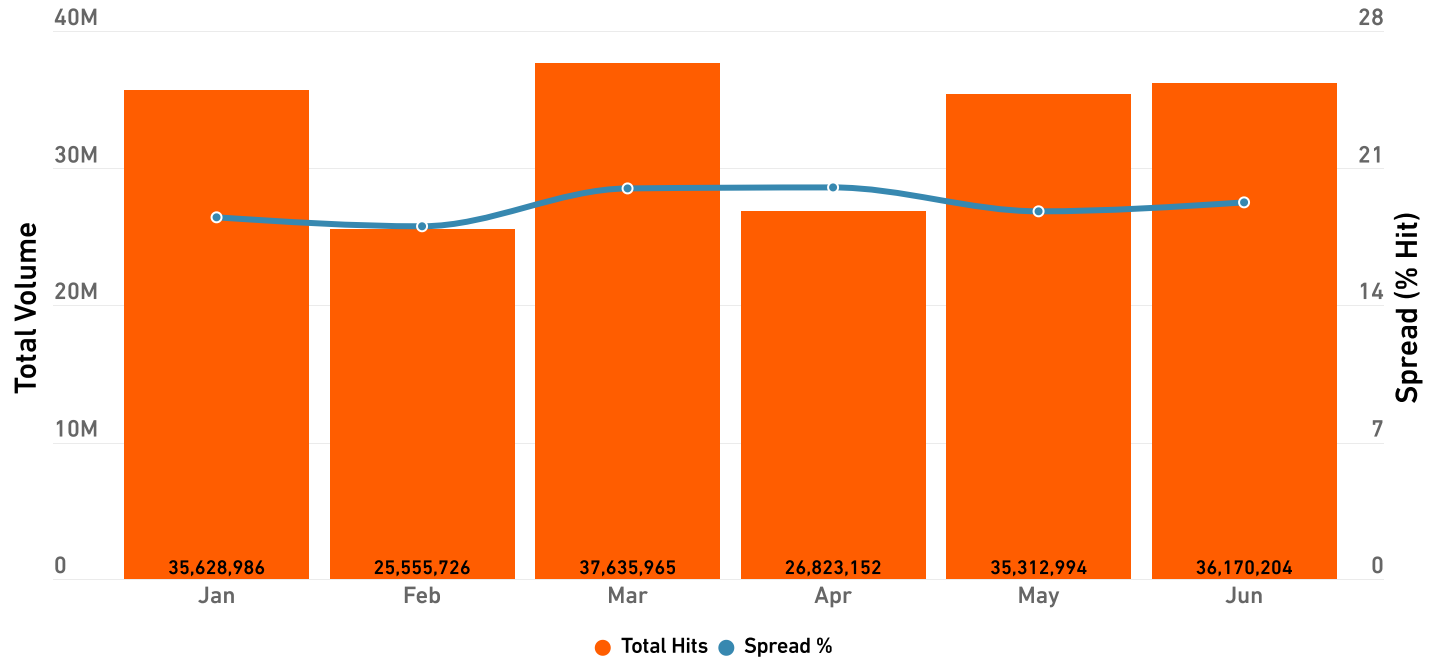
2023 Malware Attacks | United States



MALWARE RANK
1

With 1.2 billion hits (out of a global total of 2.7 billion), the U.S. remains the world's malware epicenter, but attacks there fell 14% year-to-date.

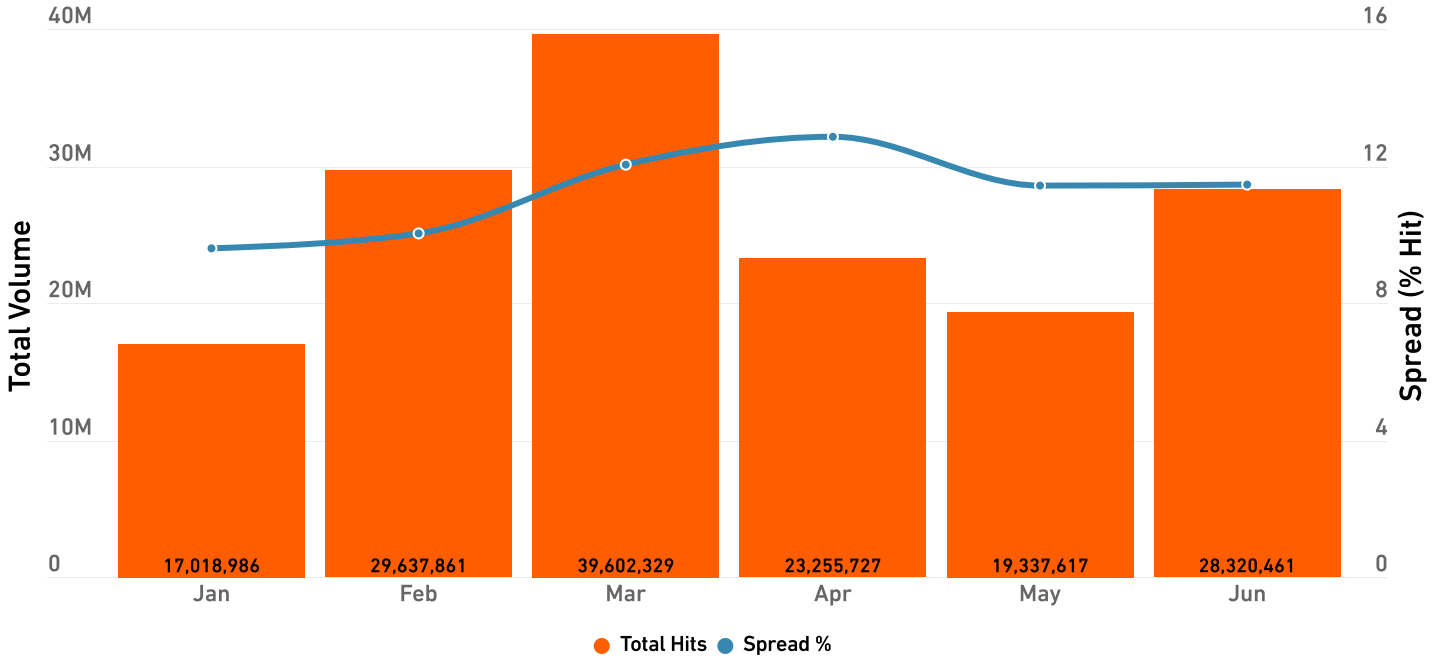
2023 Malware Attacks | India



MALWARE RANK
2

In the first half of 2023, malware in India was nearly flat, falling from 197.9 million to 197.1 million, a .5% drop.

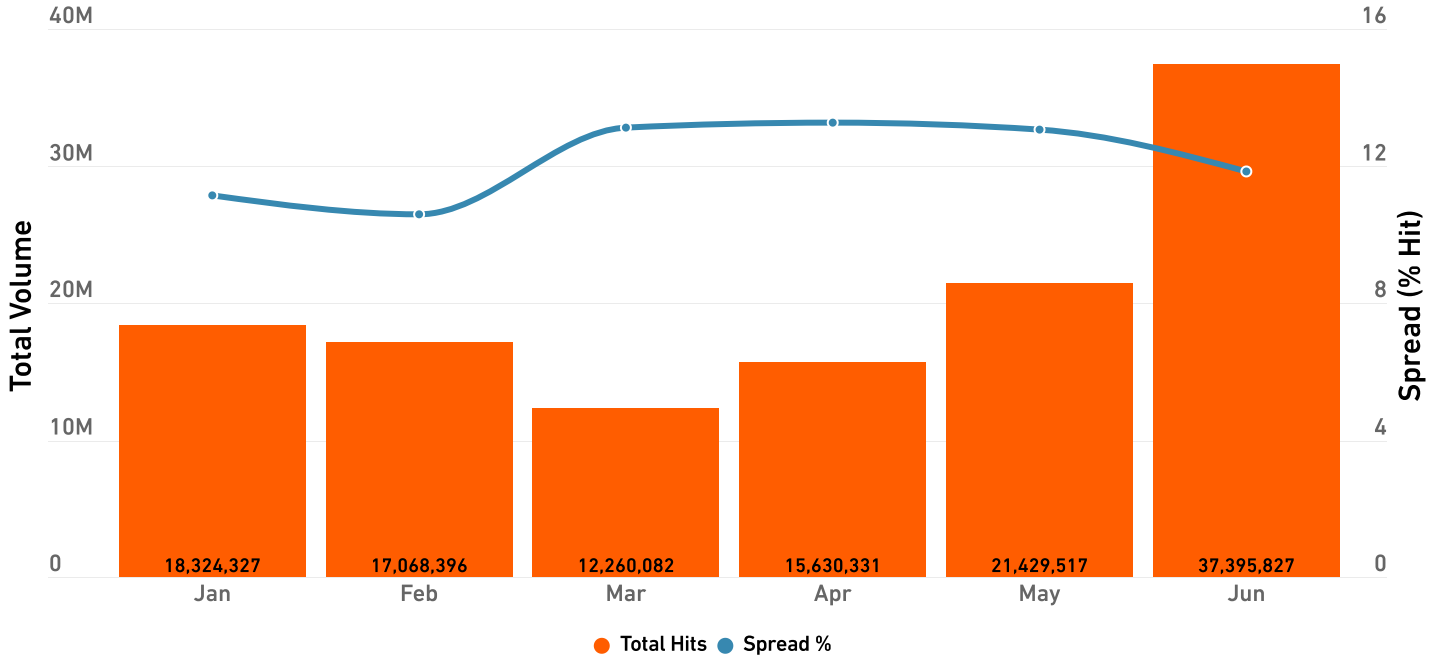
2023 Malware Attacks | United Kingdom



MALWARE RANK
4

The malware volume for U.K. decreased 8% year-to-date, falling from 171.2 million to 157.2 million.

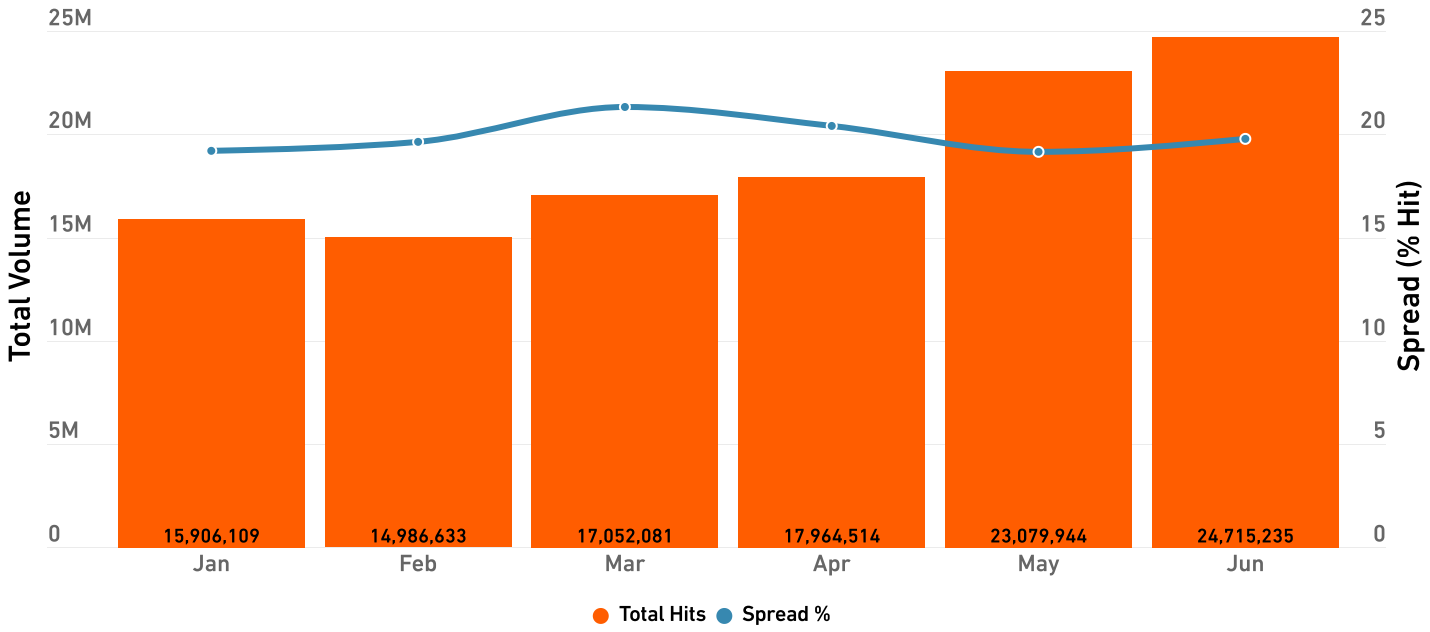
2023 Malware Attacks | Germany



MALWARE RANK
5

2023 brought a 7% drop in malware for Germany, where attack volumes fell from 131.2 million to 122.1 million.

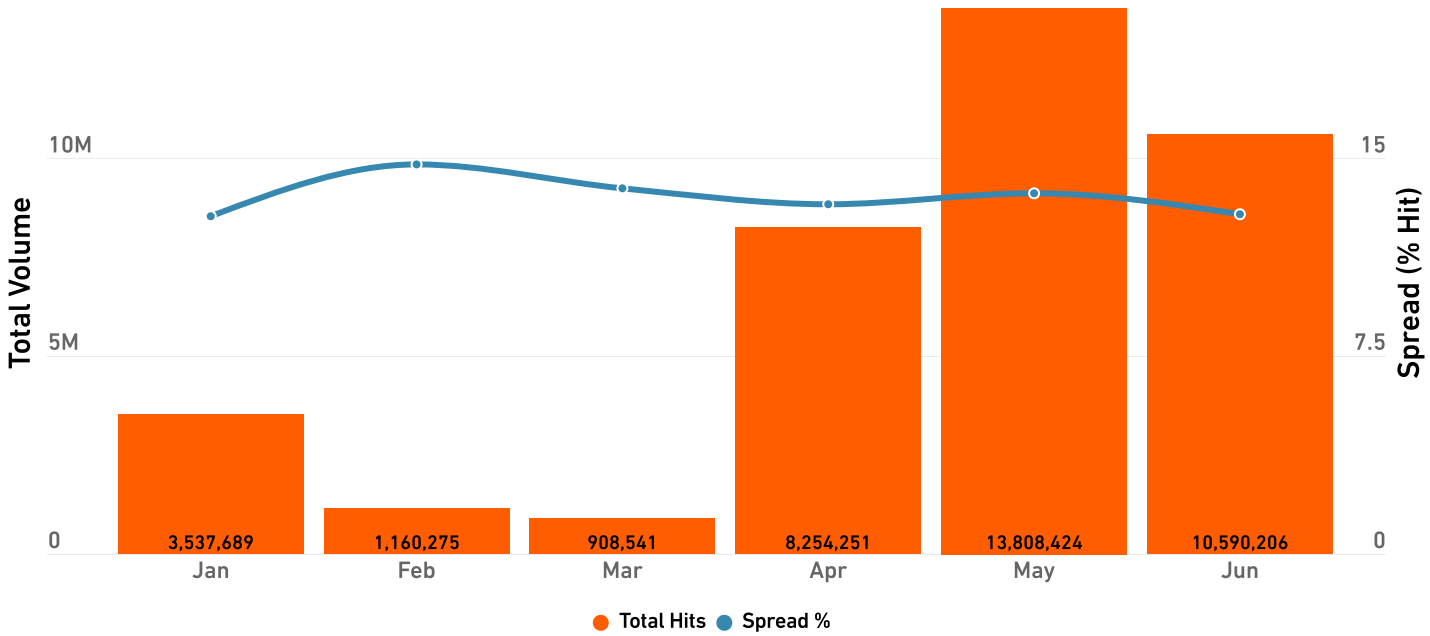
2023 Malware Attacks | Brazil



MALWARE RANK
6

Brazil saw an even smaller change: Attack volume there dropped from 115.4 million to 113.7 million, down just 1.5%.

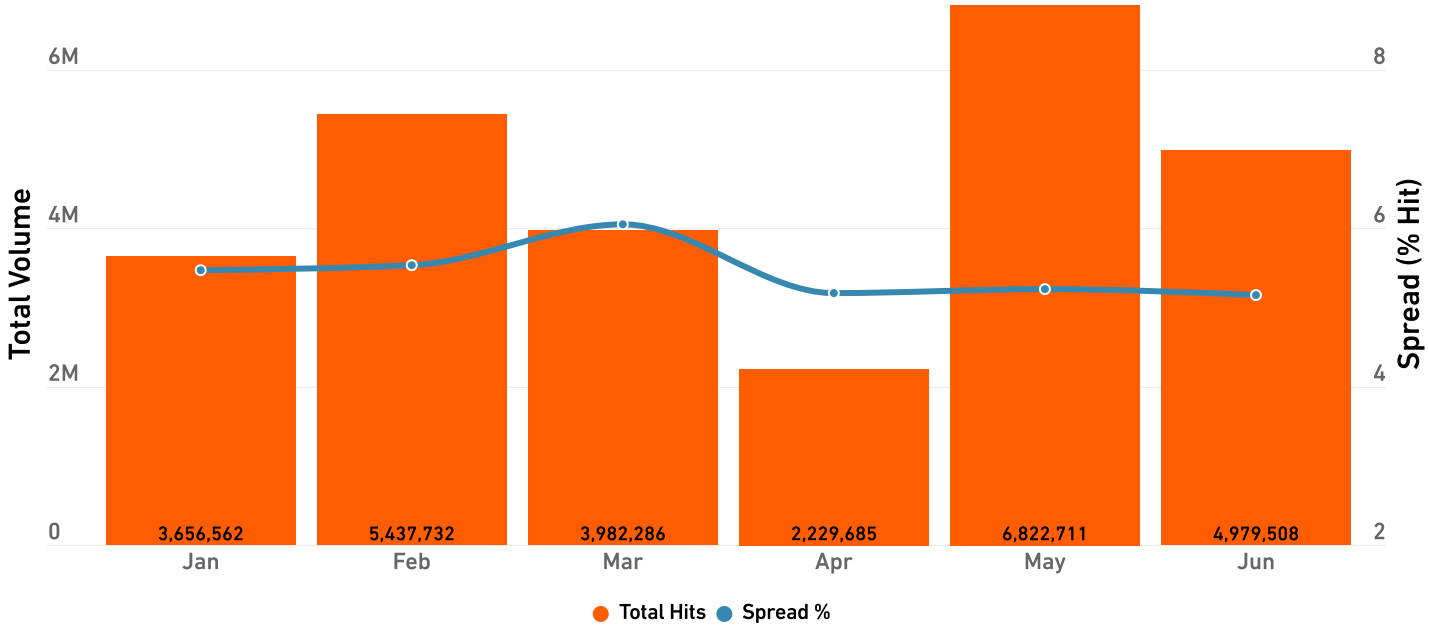
2023 Malware Attacks | Mexico



MALWARE RANK
13

Highly unbalanced quarters fueled a huge malware spike in Mexico, the only country we studied to see an increase. Attack volume there jumped 90.5%, from 20.1 million in 1H 2022 to 38.3 million in 1H 2023.

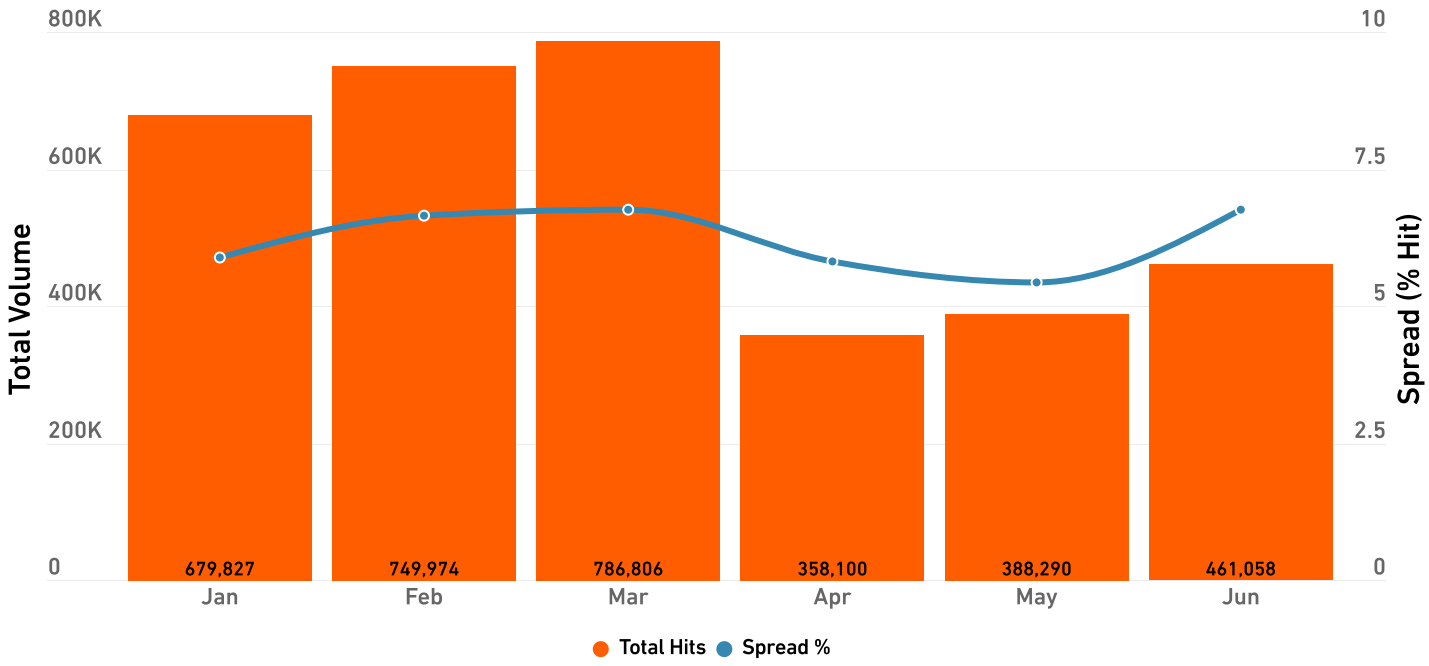
2023 Malware Attacks | UAE



MALWARE RANK
15

Malware in UAE dipped 41% year to date, from 45.9 million in the first six months of 2022 to 27.1 million so far this year.

2023 Malware Attacks | Japan



MALWARE RANK
31

Of all the countries we examined in depth, Japan experienced the largest decrease in malware, going from 9.4 million in the first six months of last year to 3.4 million in the first half of 2023 — a 64% drop.

Malware by Industry

While malware was down slightly overall, this wasn't the case in any of the industries we studied. In fact, malware was one of three threat categories in which every industry we looked at experienced an increase in malware volume. (The other two were cryptojacking and encrypted threats.)

But while these industries shared that in common, the similarities ended there — outcomes ranged from a near-negligible uptick to a near-*tripling* in attack volume.

Government: Government customers saw the smallest year-to-date increase out of the industries listed here, with volumes creeping up just 2%. An average of 11.3% of government customers were targeted by a malware attack each month.

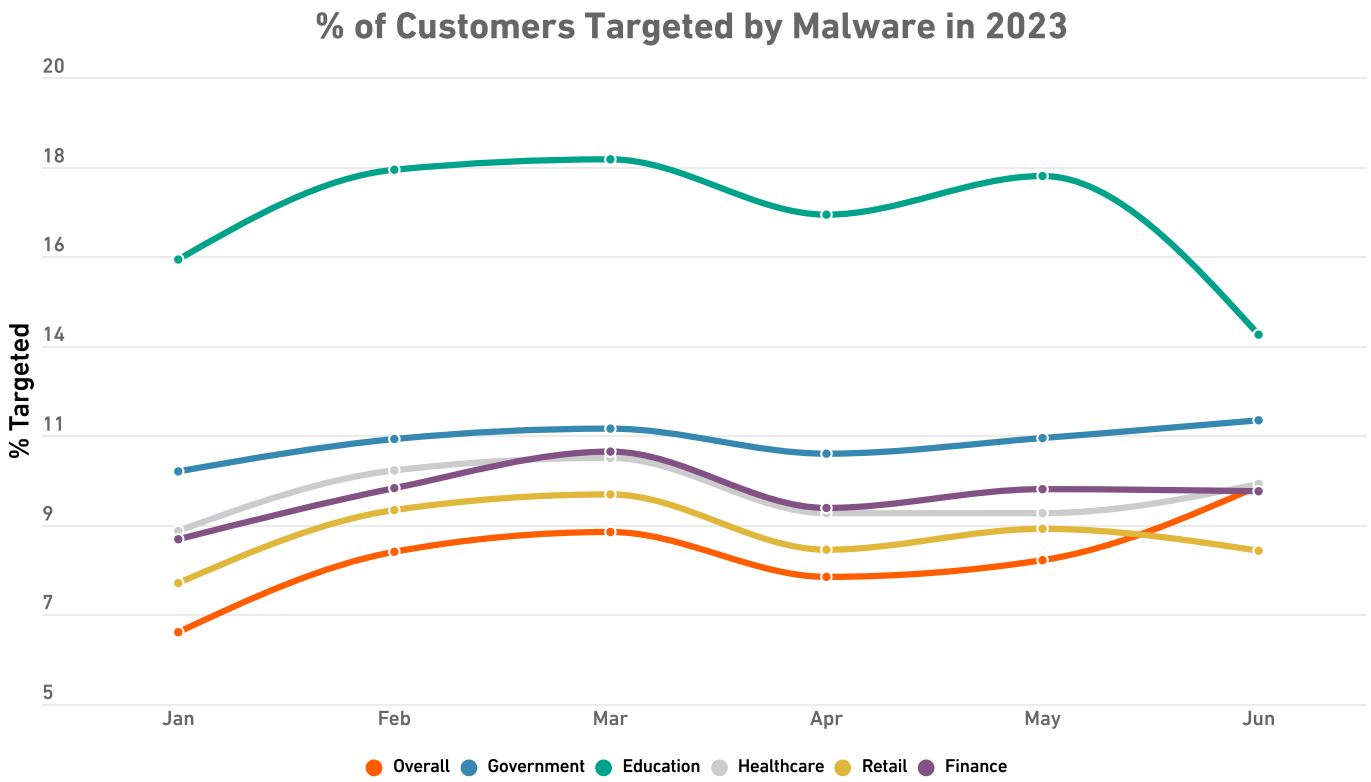
Retail: Retail customers ended June with the second-lowest malware volume, and also experienced the second-lowest increase: Attacks on these customers jumped 39% over the first six months of 2022. Roughly 9% of retail customers saw an attack each month.

Finance: So far in 2023, customers working in finance have experienced a 59% overall increase in malware volume. An average of 10% of these customers were targeted in a given month.

Healthcare: While customers working in healthcare ended June with the second-highest malware attack volume, they saw a slightly smaller increase of 46% year to date. Approximately 10% of healthcare customers saw an attack each month.

Education: In the first six months of 2023, education customers saw a staggering 179% increase in attack volume compared with the same time period in 2022. These customers were also the most likely to see an attack: An average of 16.6% were targeted every month.

It's worth noting that the malware trends we're seeing in education are the result of two disparate trends. Higher education actually saw a *decrease* in malware attempts in the first half of the year, bringing their total attack volume down 42%. But this was more than offset by a massive spike in malware among K-12 organizations, which saw a staggering 466% increase in attacks year to date.



RANSOMWARE

Ransomware Still Falling, but Poised for a Rebound

So far in 2023, SonicWall Capture Labs Threat Researchers have recorded 140.1 million ransomware attacks, down 41% year-to-date.

March, in particular, saw lower-than-expected ransomware. At just 13.2 million hits, that month had the lowest attack volume since January 2020. But it also turned out to be an inflection point: Ransomware rose in April, more than doubled in May, and jumped again in June.

This led to two very unbalanced quarters: Q1 2023 had the smallest number of attacks since Q4 2019 at just 51.2 million hits, but Q2 was 74% higher, at 88.9 million. Taken with the monthly trends, this suggests ransomware could rebound as we continue moving through 2023.

Why is Ransomware Decreasing?

In 2020 and 2021, it seemed ransomware would never stop increasing. But as history has shown, most threat trends are cyclical (Remember in 2019 when headlines announced the death of cryptojacking?)

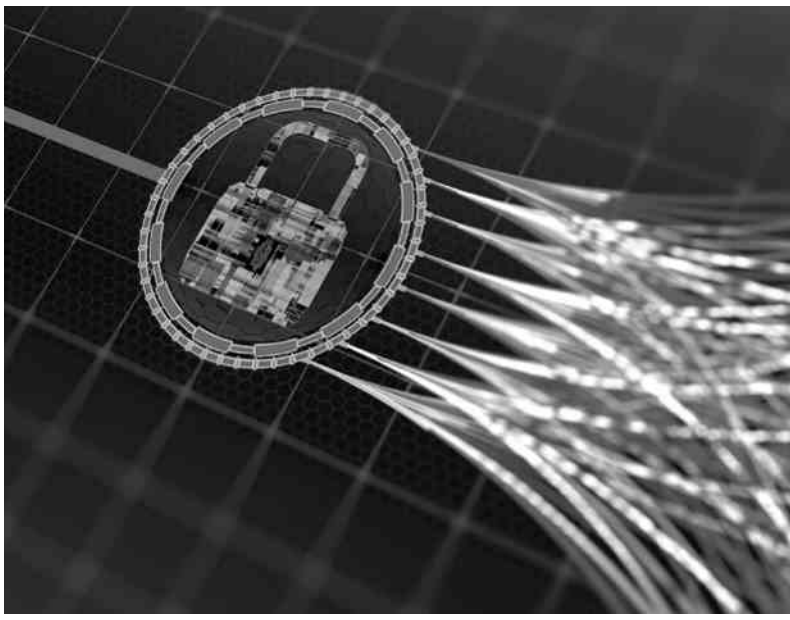
These trends also don't exist in a vacuum. They're pulled in various directions by everything from economic headwinds to technological developments. Here are a few of the factors that may be contributing to the year-to-date decline in ransomware:

The Hive Takedown: In January 2023, the U.S. FBI announced it had infiltrated and taken down the Hive ransomware operation — previously the third-most active ransomware gang.

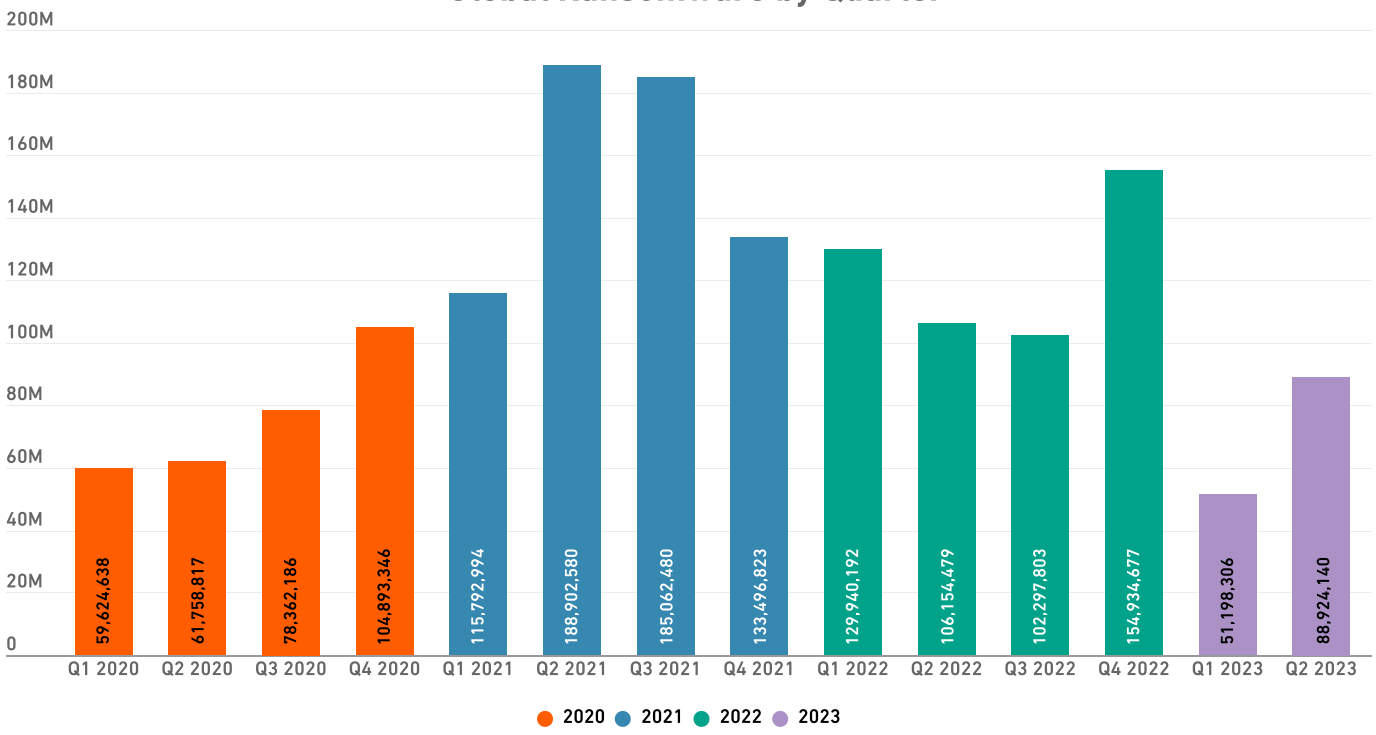
Increased Law Enforcement Scrutiny: Hive wasn't the only group that faced a bust. In addition to the high profile busts in 2022, in February the U.S. and U.K. sanctioned Trickbot operatives, March brought the arrest of two members of the prolific DoppelPaymer ransomware group, April saw the disruption of hacker marketplace Genesis Market, and May came with news that the FBI had seized nine crypto exchanges that were used to launder ransomware payments.

Political and Economic Climate: As news of a possible recession clouded late 2022 and early 2023, cost-cutting measures taken by companies in the U.S. and elsewhere began making headlines. Combined with better incident response measures and the growing awareness that paying a ransom could be supporting Russia in its ongoing conflict with Ukraine, the number of organizations willing to pay a ransom dropped dramatically — prompting hackers to begin conducting layoffs of their own.

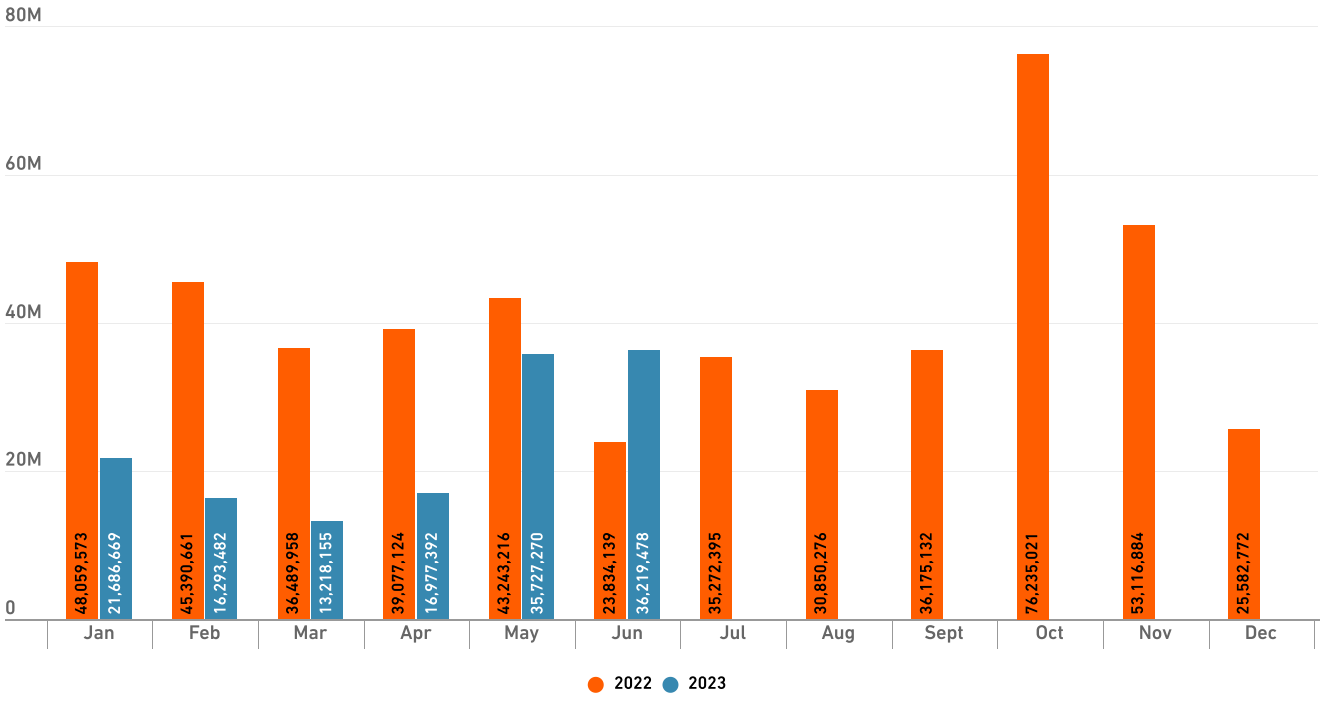
Pure Extortion Attacks: As cybercriminals continue to rely on the threat of data leaks in addition to the sale of decryption keys to make their money, some are abandoning the encryption part altogether — leading to an uptick in what are referred to as "pure extortion attacks." For instance, the BianLian ransomware group made news in March for switching to pure extortion after a free decryptor for their victims was released. As these extortion schemes do not trigger a ransomware detection, they're not counted as part of our ransomware total.



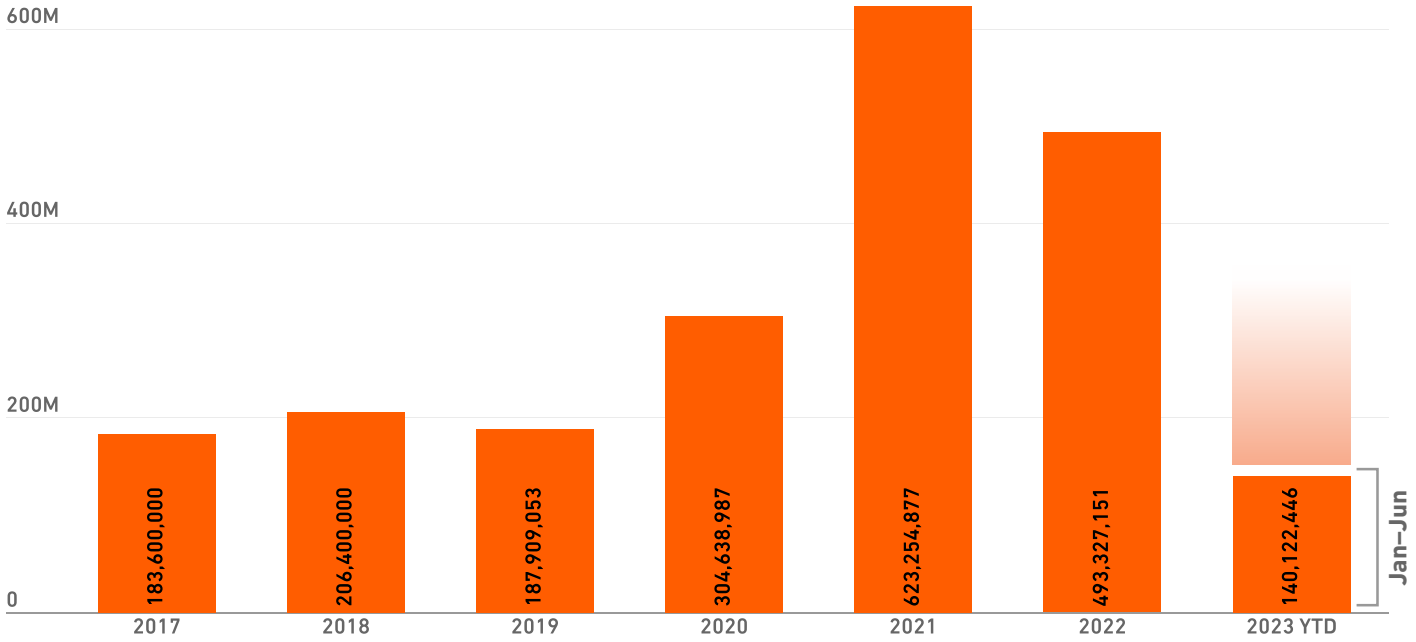
Global Ransomware by Quarter



Global Ransomware Volume



Global Ransomware Volume by Year



Ransomware by Region

The decrease in ransomware was observed across every region, but there was a lot of variation in these dips.

As with many other threat types, North America showed a significant drop over the first half of 2023, dipping to just 72.8 million hits, a decrease of 45% over the same time period last year. February in particular brought lower-than-expected ransomware volume — at just 4.2 million, *one-tenth* of the volumes we were recording in mid-2021, ransomware for the region was lower than at any point since December 2019. But surprisingly, June brought a rally as attack volumes jumped to more than 25 million.

Europe also saw a decline in ransomware, but at 11%, it was much smaller. Correspondingly, six out of the top 10 countries for ransomware volume in the first half of 2023 were in Europe. As we continue to see ransomware operators shift away from the U.S. and to Europe and other regions, this number could continue to grow.

Latin America saw the largest decrease in ransomware at 77%, but, paradoxically, it also saw the biggest amount of growth. After bottoming out in February at just 66.7 *thousand* hits, attacks crept up in March, then spiked sharply in both April and May to end June at 2.5 million — *37 times* the volume seen just four months before.

While most regions saw ransomware volumes trending up on a month-to-month basis despite a year-to-date drop, Asia was the sole exception: Volumes in the region in the first half of 2023 totaled 4.1 million, but based on a trend line that pointed unambiguously down for most of that time, we expect to see this total continue to fall.

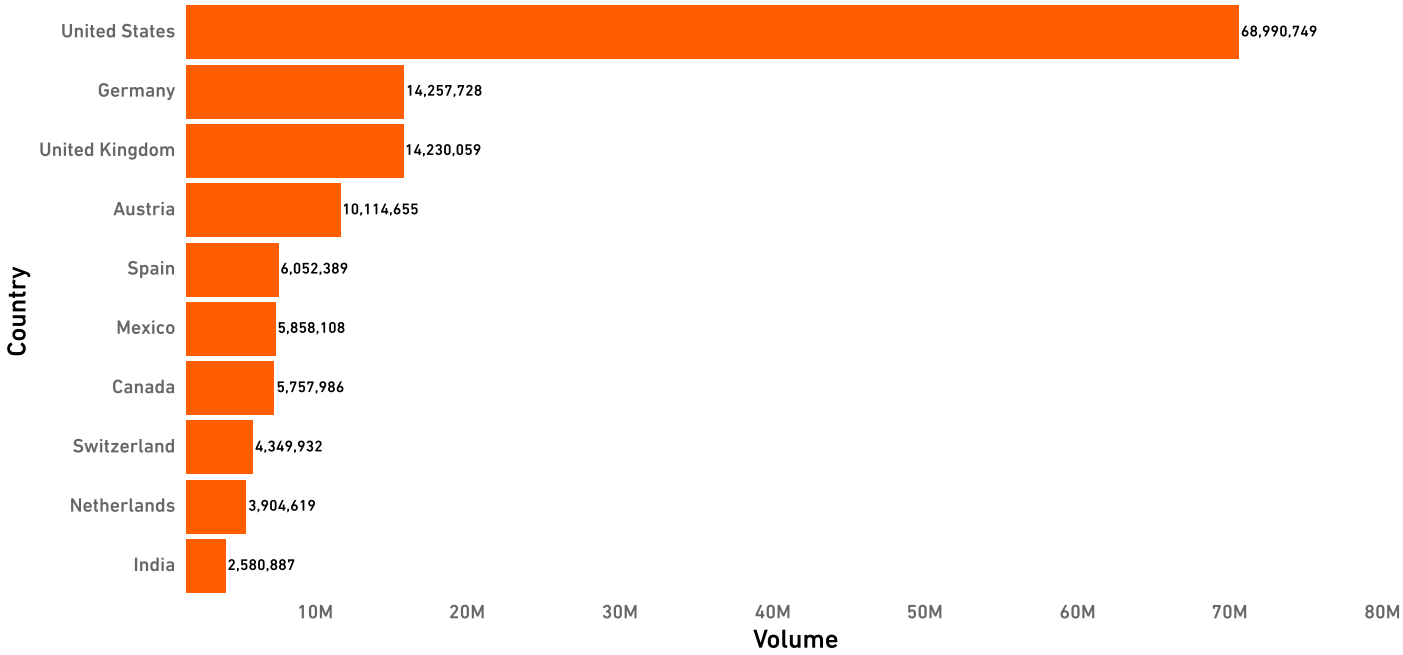
Ransomware by Country

But while ransomware by region was down across the board, the country-by-country data was much more of a mixed bag.

SonicWall researchers recorded 67 million ransomware hits in the U.S. during the first six months of 2023, a 49% drop year to date. In the U.K., ransomware was basically flat at 14.2 million, down just .5% over this time in 2023.

But several countries bucked the lower-ransomware trend. One of them was Germany: With 14.3 million hits so far in 2023, ransomware is up 52% over the first six months of 2022. And India saw an even larger jump, with attack volumes rising 133% to 2.6 million.

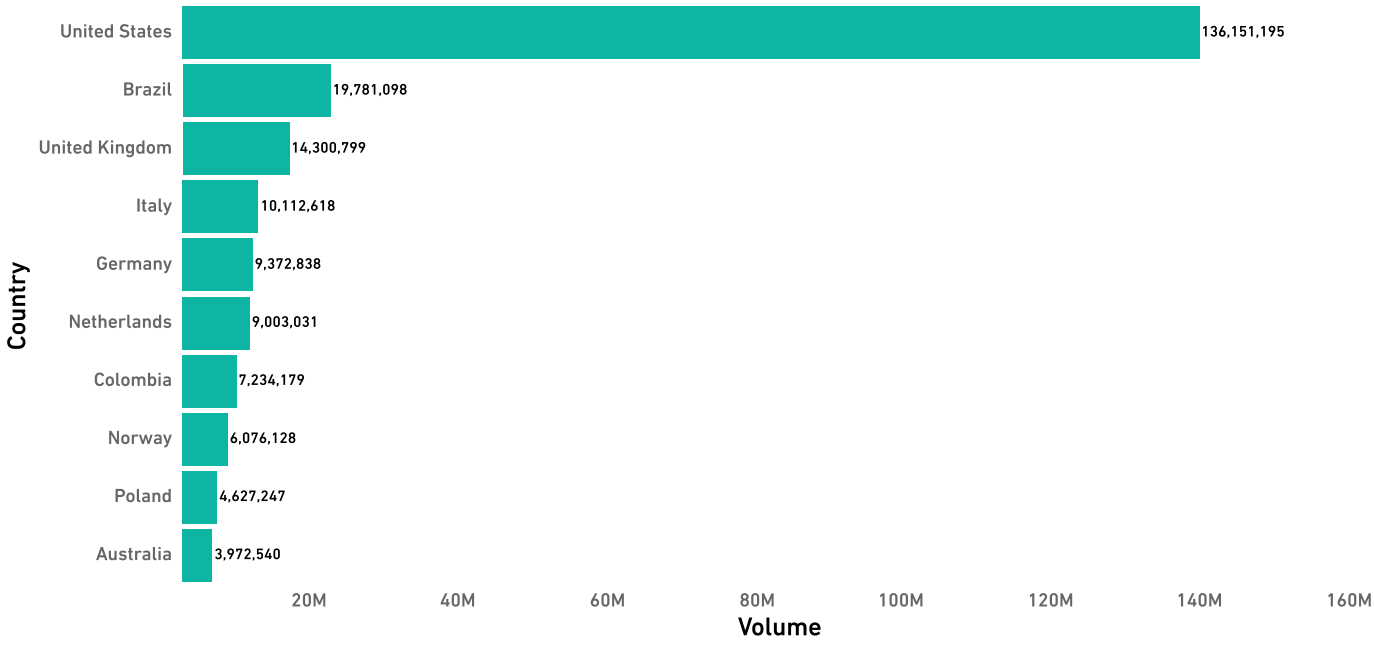
2023 Ransomware Volume YTD | Top 10 Countries



Comparing the Top 10 Countries for Ransomware graphs allows us to observe the change in ransomware trends over time. While the U.S. still has the highest ransomware attack volume, other countries are continuing to catch up: This year, the No. 2 country (Germany) saw 21% of the total ransomware recorded in the U.S. Last year, that percentage was 15%. And in 2021, it was just 6%.

And as threat actors target new regions, we've seen a sizeable amount of shuffling in the list. Only four of the countries on June 2022's list appeared on the 2023 list.

2022 Ransomware Volume 1H | Top 10 Countries

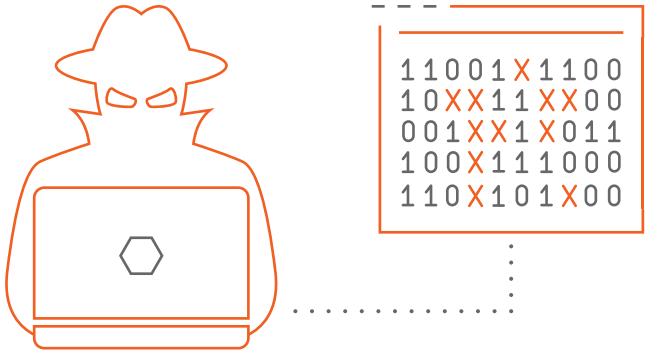


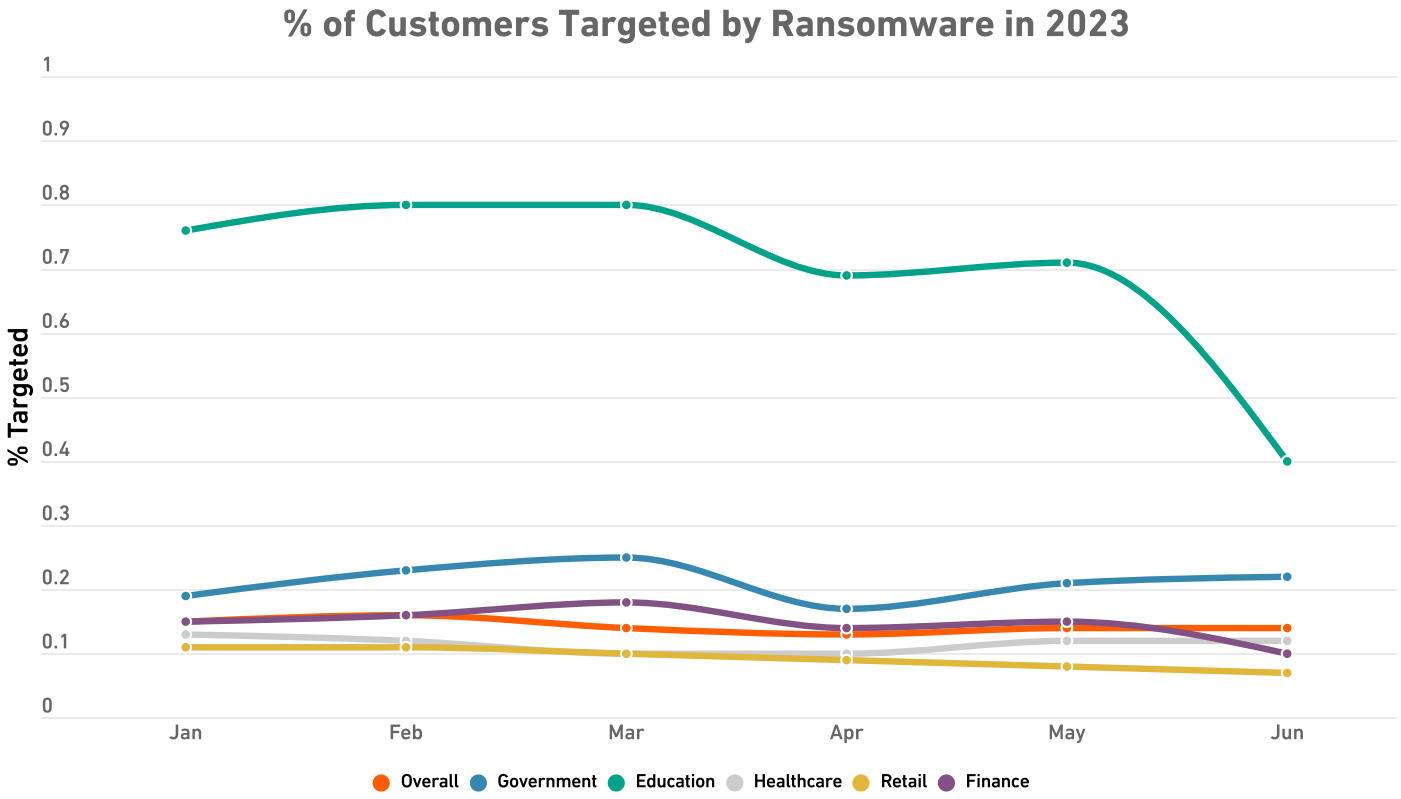
Ransomware by Industry

Across all but one of the industries we studied, ransomware dropped. The sole exception was government, where ransomware rose a modest 6%.

Attacks on higher-ed organizations also increased by 6% in 1H 2023. But a 19% decrease in ransomware attacks on K-12 organizations easily offset this rise — and an astounding 95% drop among other educational organizations* brought the total year-to-date change to -38%.

Healthcare, finance and retail organizations saw an even larger drop than education: Total attack volume for these customers decreased 60%, 93% and 96%, respectively.





*Defined as fine arts schools, exam prep and tutoring, automobile driving schools, educational support services, and traditional education institutions that are not easily classified.

CRYPTOJACKING

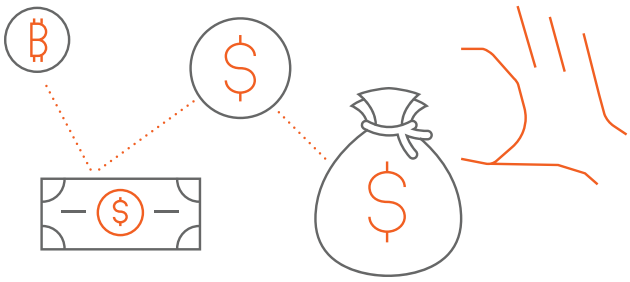
Cryptojacking's Record Surge Continues

In 2022, cryptojacking surpassed 100 million for the first time ever. In the first six months of 2023, attack volumes have not only eclipsed that milestone, they've more than *tripled* it, rising 399% to more than 332 million hits — compared to just 66.7 million during the first half of last year.

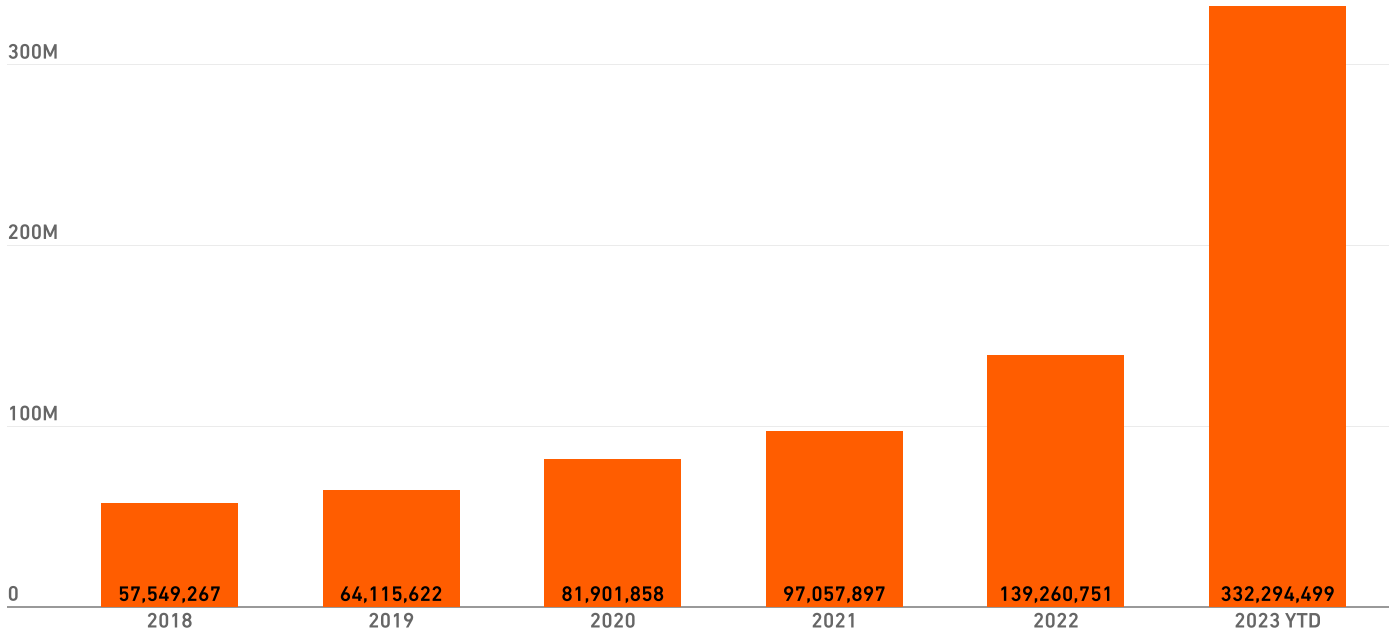
This massive spike in cryptojacking was fueled by record highs in January, February, April and May, with monthly totals for the latter reaching 77.6 million — more than the entire first six months of 2022 *and* more than in all of 2018 or 2019.

By the end of June 2023, the total number of cryptojacking hits had sailed past the 200 million mark *and* past the 300 million mark, reaching a new record high that exceeded the *full* year totals for 2020, 2021, and 2022 (themselves all record-breaking years) combined.

The 332 million hits recorded so far in 2023 represents an unprecedented high, but that's not all. If this growth continues apace—*or even if it slows dramatically*— SonicWall could record more cryptojacking attempts in 2023 than in the entire period between 2018 and the end of 2022.



Global Cryptojacking Volume by Year



Top 10 Countries For Cryptojacking

1. United States
2. Denmark
3. Germany
4. France
5. United Arab Emirates
6. South Africa
7. Mexico
8. Canada
9. India
10. Brazil

Unsurprisingly, every region showed an increase in cryptojacking — and most of these jumps were dramatic. The sole exception was Asia, where SonicWall researchers recorded 5.2 million hits — up just 1% from the same time period in 2022.

At 4.1 million hits, Latin America saw slightly less cryptojacking than Asia, but this total represented a larger year-to-date increase of 32%.

In contrast, cryptojacking in Europe and North America *skyrocketed*. North America experienced 214.7 million hits in the first six months — well over the 139 million recorded globally in all of 2022 and a 345% increase year to date. Worse, this wasn't the product of a single monthly spike: instead, it was month after month of stable, yet relentless, cryptojacking totals.

But while North America still had the highest total cryptojacking volume, it was Europe where hits jumped most dramatically. Cryptojacking there had soared to 88.3 million hits by the end of June 2023, a staggering 788% year to date.

The number of hits recorded in most countries tracked with these patterns. In the U.S., cryptojacking jumped from 48 million to 211.7 million, a 340% increase year to date. Germany also experienced a triple-digit jump, rising 139% from 3.1 million to 7.4 million. And in the U.K., a 479% spike brought the total number of cryptojacking hits to 6.8 million, compared with 1.2 million last year.

A notable exception to this trend was India: Hits there actually *fell* by nearly three-quarters, from 4 million to 1.1 million. Despite this drop, however, India still saw enough cryptojacking attempts to make the Top 10 list.

Cryptojacking Trends

As we've seen, cybercriminals continue to shift away from the quick payout of ransomware in favor of the slower, behind-the-scenes approach of stealing compute power to mine digital currency. To help their chances of success, these cybercriminals constantly shift their tools, tactics and procedures.

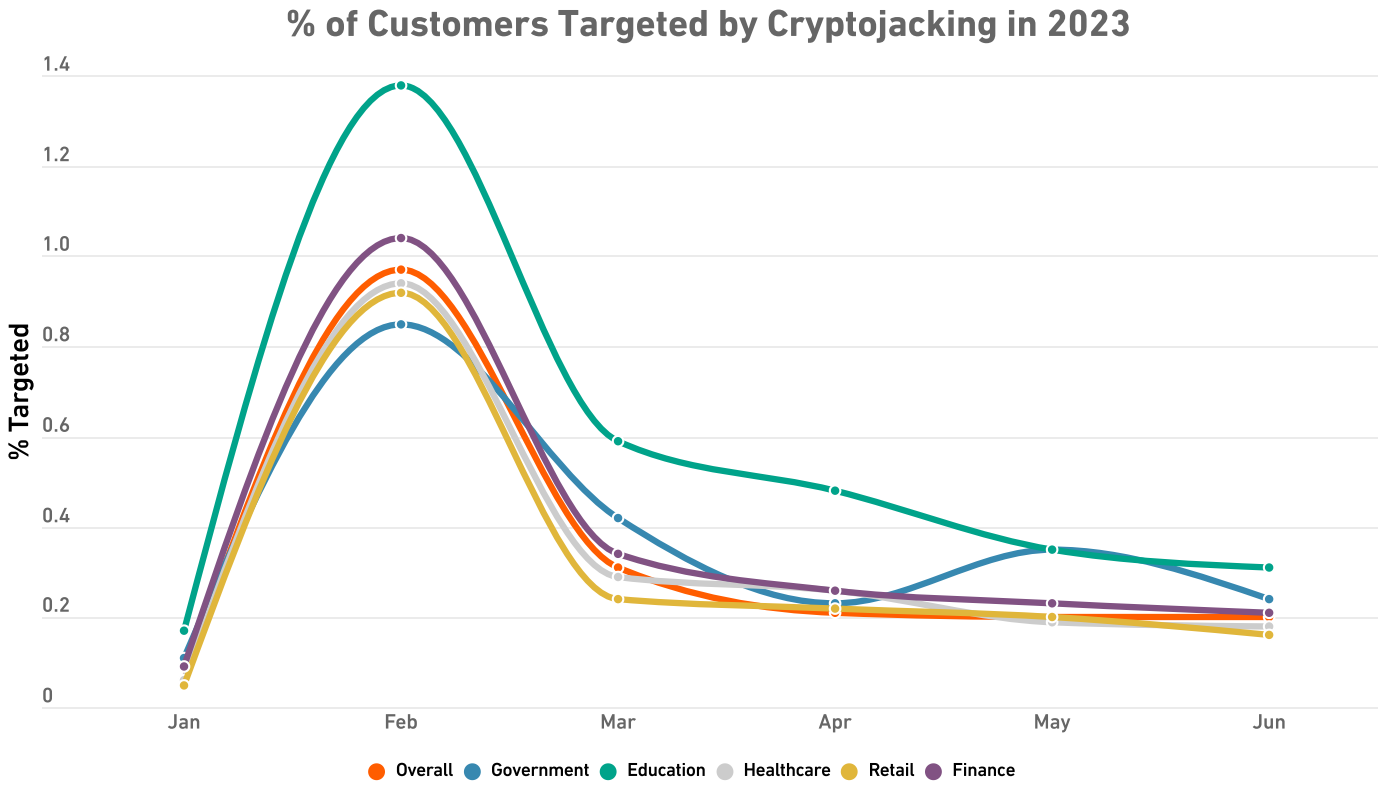
Here are some of the major developments in cryptojacking observed in the first half of 2023:

- Threat actors have accelerated their shift from targeting endpoints to targeting cloud services, including one leveraging Kubernetes clusters to mine Dero
- MacOS endpoints have also been in the crosshairs, with cracked versions of FinalCutPro being used to distribute HonkBox cryptojacking malware
- Oracle WebLogic servers are the target of a new crypter known as ScrubCrypt, designed to evade Windows Defender protections
- SonicWall has continued to observe attackers skipping cryptojacking altogether in favor of stealing crypto directly: In late March, we observed a new variant of AsyncRAT designed to steal Bitcoin, Ethereum and Tether

Cryptojacking by Industry

The number of cryptojacking hits rose across every industry we studied — and many of these jumps were *massive*. Given the very small number of cryptojacking hits several of these industries saw over the first half of 2022, as well as the speed with which these totals are growing, it makes more sense to speak about these changes in terms of factor increases versus percentage increases.

The number of cryptojacking hits targeting those in retail more than doubled in the first half of 2023, and the average percentage of customers targeted each month rose from .06% to .30%. Finance customers saw 4.7 times the number of cryptojacking attempts in the first six months of 2023, and the percentage of customers targeted rose from .05% to .36%. Customers working in healthcare were targeted by 69 times more cryptojacking than in 1H 2023, and the percentage of customers affected jumped from .06% to .32%. Government customers saw 89 times the amount of cryptojacking, with .37% targeted per month on average. But it was education that saw the biggest jump: the number of cryptojacking hits recorded by education customers increased 320 times year-to-date, and the average percentage of customers targeted each month rose from .19% to .55%.



ENCRYPTED THREATS

Encrypted Threats Up 22%

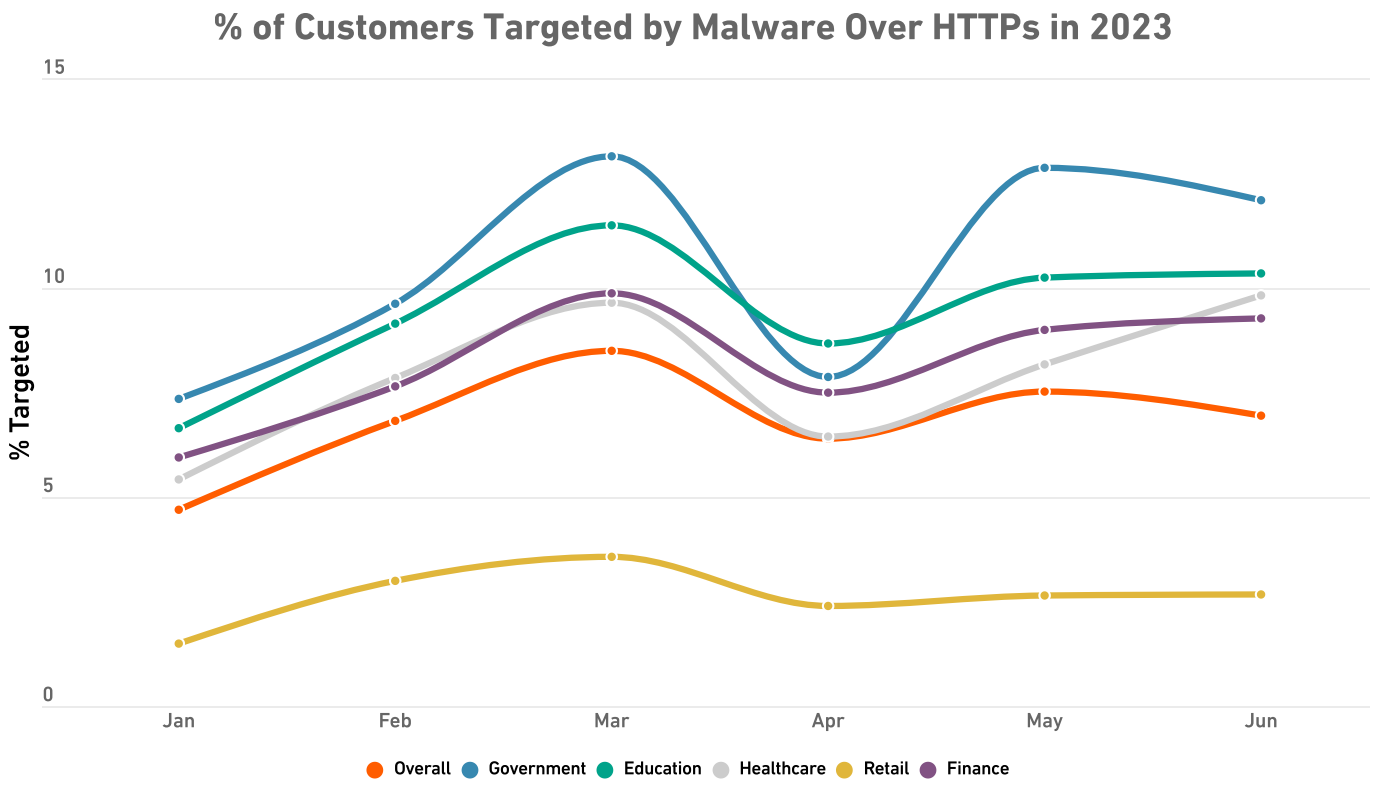
As threat actors continued shifting to stealthier means of attack in 2023, SonicWall has observed a significant increase in encrypted threats. Malware over HTTPS jumped by nearly a quarter in the first six months of this year, enough to give 1H 2023 the highest year-to-date volume of any year since SonicWall began tracking this threat type.

We previously mentioned that cybercriminals have begun shifting their attention outside North America, and encrypted attacks were no exception. While the region still saw the most attacks, it was the only one to register a decrease, with 28% fewer hits in the first half of 2023 than the same period in 2022.

But this drop was more than made up elsewhere. Europe saw attack volumes spike 119% year-to-date, enough to begin eclipsing volumes observed in North America.

While Europe's monthly totals had only exceeded North America's twice before 2023, it's already happened *three* times this year — including in February, when attacks in Europe more than doubled those in North America, pushing the region to a new record high.

While attack volumes are significantly lower in Asia and Latin America, they both saw huge increases, of 287% and 2,851% respectively. By the end of January, total attacks in Latin America had already exceeded 72% of 2022's *full year* totals, but this was just the beginning: May set a new monthly record for the region, followed by yet another in June.



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

Encrypted Threats by Industry

Encrypted attacks rose across every industry we examined — and not by just a little bit. Spikes were observed in both total volume and percentage of customers targeted, resulting in more customers seeing more attacks than ever before.

Government

Customers working in government experienced the biggest spike in encrypted threats: these attacks skyrocketed a staggering 5,677% year to date. This outsized increase also drove a rise in the percentage of customers targeted, with an average of 10.5% of government customers seeing malware over HTTPs (compared with 8.8% in the first half of 2022.)

Education

Customers working at K-12, higher-ed and related organizations also saw a four-digit spike in malware over HTTPs: Attacks on these customers jumped 2,580% over the same time period in 2022. A corresponding increase in percentage of customers targeted was also observed: about 9.4% of education customers saw an attack in the first six months of 2023, compared with 8.9% a year before.

Retail

Retail customers were slightly more fortunate: Attacks on these organizations rose a (comparatively) smaller 676% year-to-date. But even with a triple-digit increase in total volume, the overall percentage of customers targeted remained at the lowest level of any industry examined, albeit slightly higher this year (2.6% vs 2.1%)

Finance

With a 122% increase, finance customers also experienced significantly more encrypted attacks in the first half of 2023 than they did in the first half of 2022, with the percentage of customers seeing an attack averaging 8.2%, compared with 6.3% last year.

Healthcare

SonicWall recorded a 94% increase in encrypted attacks on healthcare organizations, the lowest of any industry studied. But while they saw the lowest total volume increase, they were hit by the *highest* increase in percentage of customers targeted, with 7.9% in 1H 2023 versus 5.3% in 1H 2022.

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 added security for web sessions and internet communications, attackers increasingly use this encryption protocol to hide malware, ransomware, zero-day attacks and more.

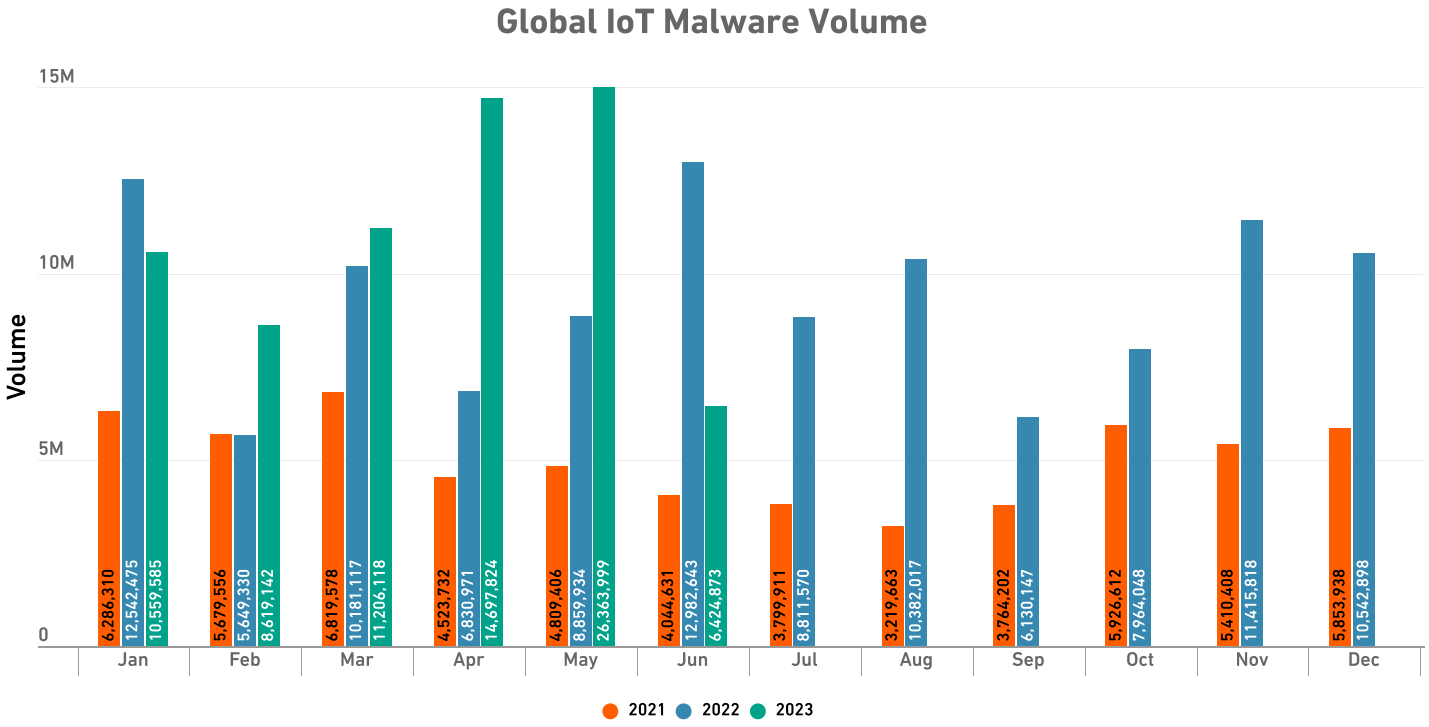
Legacy firewalls and other traditional security controls lack the capability or processing power to detect, inspect and mitigate threats sent over HTTPs traffic, making this a highly successful avenue for cybercriminals to deploy and execute malware.

IoT MALWARE

IoT Malware Jumps by More than a Third

In the first six months of 2023, SonicWall Capture Labs threat researchers recorded 77.9 million IoT malware attacks, up 37% year to date and higher than any other six-month period on record. This total not only exceeds the midyear total of 2022 by more than 20 million, it also exceeds the full-year total for both 2020 and 2021, and is more than 2018 and 2019 combined.

This record half was fueled by high attack volumes in Q1, followed by *abnormally* high attack volumes in Q2. When the monthly total for April reached 14.7 million, it set a new record — but in May, attack volumes nearly doubled, surpassing the 20-million mark for the first time and resulting in a second-straight record-breaking quarter.



IoT Malware by Region

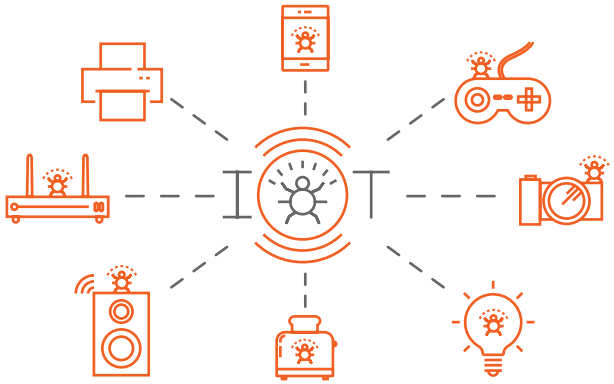
Cybercriminals spent the first half of 2023 shifting their sights away from North America, and IoT malware was no exception: While the region still saw the highest overall attack volume, it was also the only one to experience a decrease, falling 3% to 32.2 million.

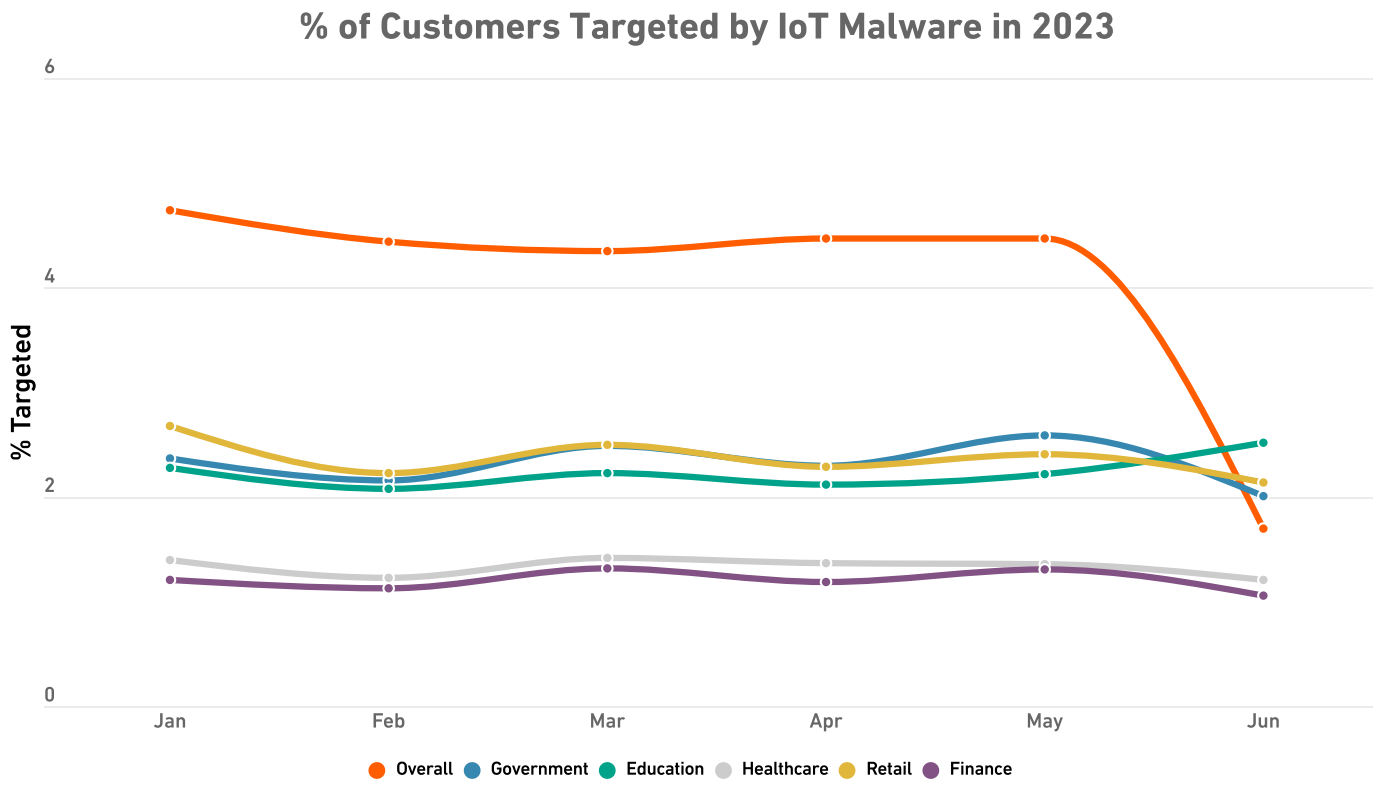
Meanwhile, a corresponding increase was occurring in Europe, Latin America and Asia. In Europe, first-half attack volume reached 12.1 million, an increase of 10% year-to-date. But it was Latin America and Asia that saw the biggest growth: In Latin America, IoT malware increased 164% to 8.5 million, and in Asia, attack volume soared to 23 million, an increase of 170%.

The by-country data followed the same general trends as the regional data: The U.S. saw a 2% drop, bringing attack volume to 30.4 million, and the U.K. (up 53% to 4 million) and India (up a staggering 311% to 19.4 million) also fell in line with regional patterns. Only Germany bucked the trend: IoT attacks there dropped 30 percent, to 1.3 million attacks.

IoT Malware by Industry

Despite an overall increase in IoT malware, all but one of the industries we studied experienced a double-digit drop in the first half of 2023. Government and education both saw a steep decline of 73%, followed by a 70% decrease in finance and a 60% drop in healthcare. Only the retail industry saw an increase: SonicWall observed a 13% jump in attacks on these customers compared with the first six months of 2022.





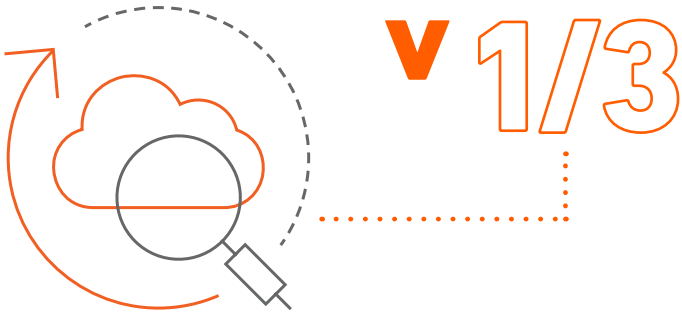
CAPTURE ATP & RTDMI™

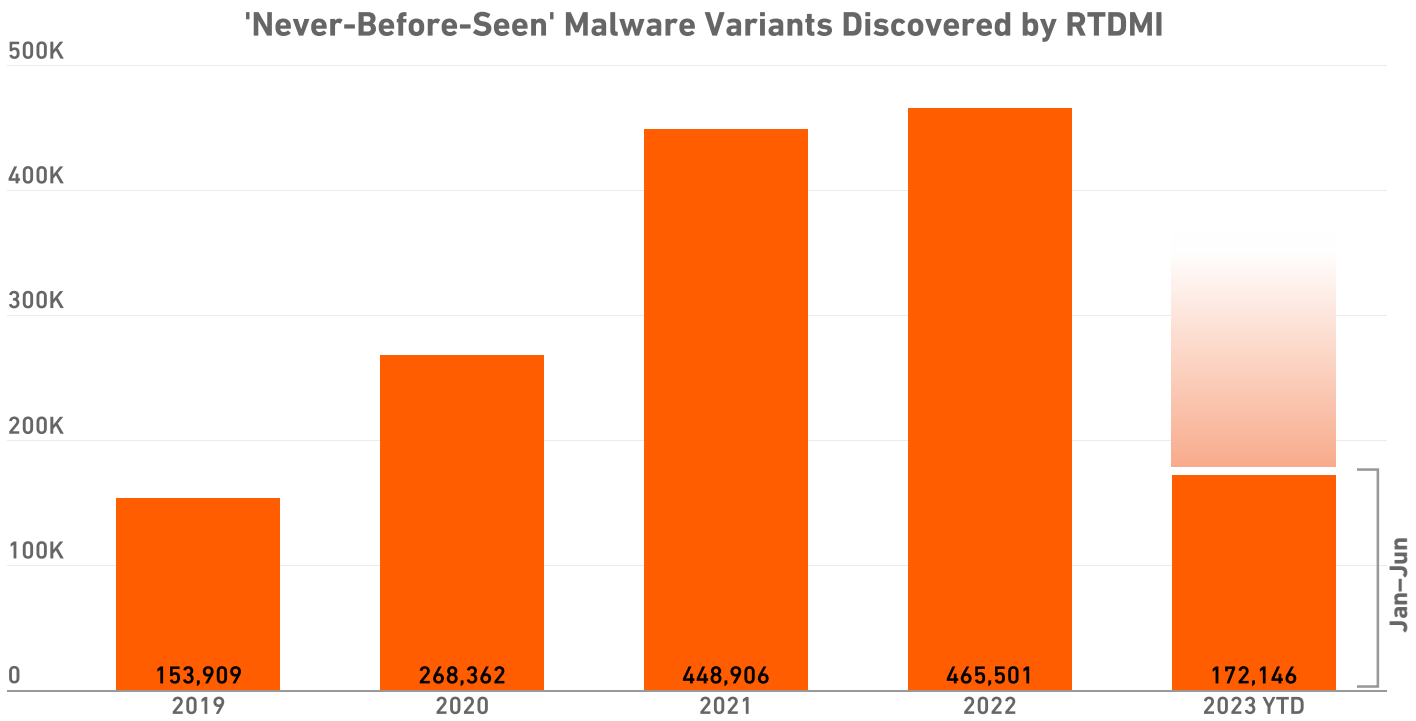
RTDMI™ Detections Fall By Roughly a Third

SonicWall's patented Real-Time Deep Memory Inspection (RTDMI™) technology identified a total of 172,146 never-before-seen malware variants in the first six months of 2023, an average of 956 per day. This total is down 36% year-to-date, and when compared with the smaller drop in malware detected overall, it offers possible insight into cybercriminal behavior.

The U.S. has long seen the lion's share of just about every type of malware. Not only has this reality directly motivated many organizations in the U.S. to take major steps to harden their networks against attacks, it's also provided incentive via cyber-insurance policies: Many policies today have minimum cybersecurity requirements that must be met before obtaining a policy.

In the places where there has been less emphasis on hardening networks, however, there's a greater chance that attackers using "proven" variants will be successful — and this reliance on tried-and-true attack techniques could be driving a drop in never-before-seen variants.





While fewer new malware variants is good news, it's important to look at it within the context of the past few years. The 172,146 never-before-seen variants detected so far this year may be down more than a third from 2022, but the second half of 2021 and 2022 had an unusually high number of detections. 172,146 is down just 7% from 2021's mid-year total of 185,945, and exceeds both 2020's mid-year total and 2019's *full*-year total.

Despite this caveat, a closer look at 2023 data suggests this total may continue to drop. Detections fell by a quarter from Q1 to Q2, and June had the fewest detections since February 2021.

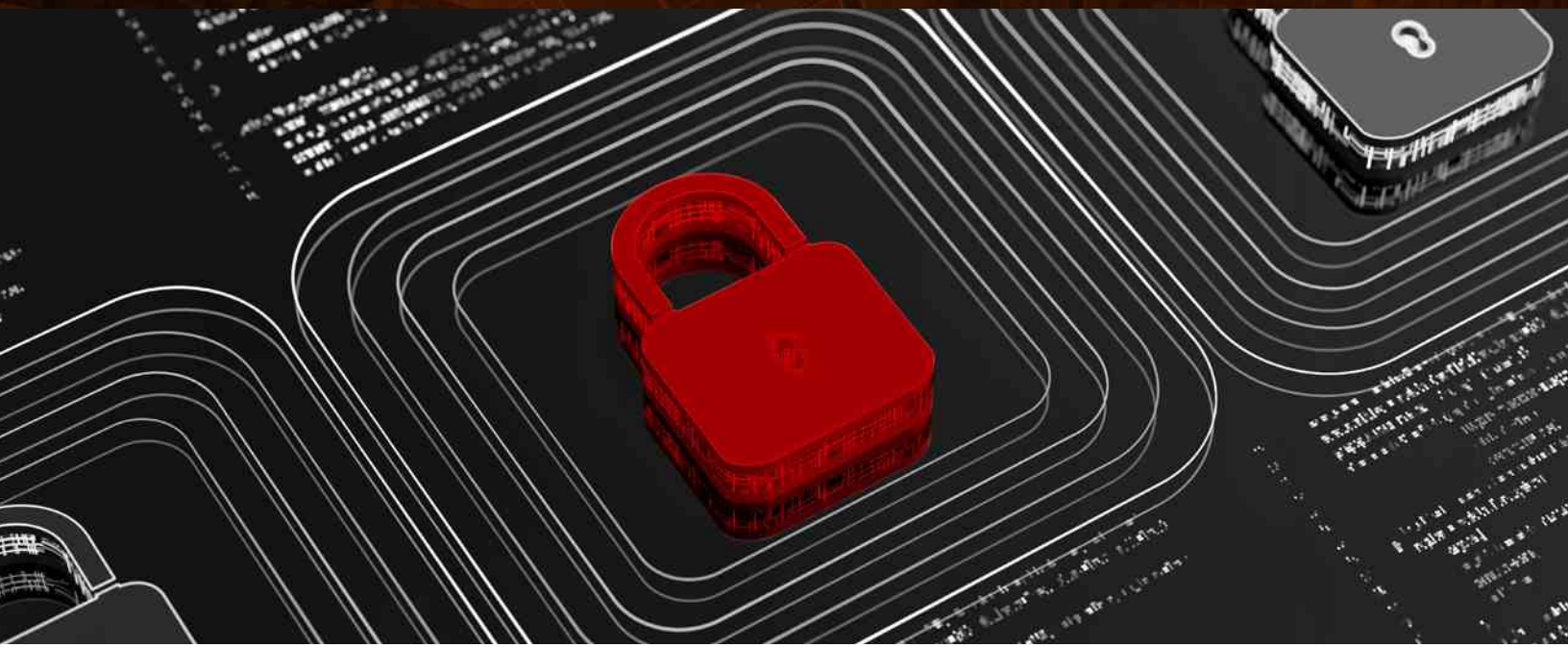
THE 172,146 NEVER-BEFORE-SEEN VARIANTS DETECTED SO FAR THIS YEAR MAY BE DOWN MORE THAN A THIRD FROM 2022, BUT 2022 HAD AN UNUSUALLY HIGH NUMBER OF DETECTIONS.

What is a 'Never-Before-Seen' Malware Attack?

SonicWall tracks the detection and mitigation of 'never-before-seen' malware variants, which are recorded the *first* time SonicWall Capture Advanced Threat Protection (ATP), which includes RTDMI, identifies a signature as malicious.

This differs from 'zero-day' attacks, which are new or unknown threats that target a zero-day vulnerability without existing protections, such as patches or updates.

Due to the volume of attacks SonicWall analyzes, however, the discovery of never-before-seen attacks often closely correlates with zero-day attack patterns.



MALICIOUS FILE TYPES

Malicious PDF & Office Files Fall by Double Digits

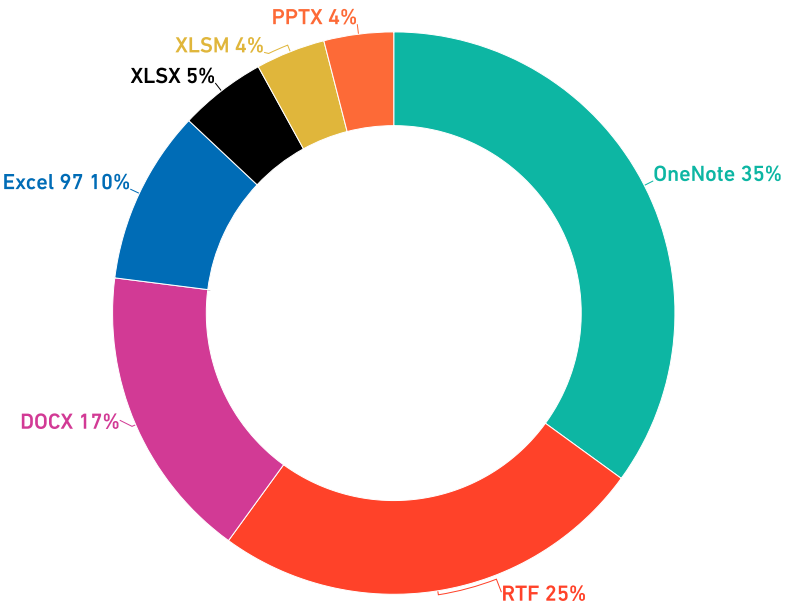
The first half of 2023 brought a drop in the number of both malicious PDFs and malicious Office files.

Malicious PDFs fell 10% year to date — but this doesn't mean that most months are seeing fewer malicious PDFs. Instead, this is a result of comparing 2022, which had a huge jump in May, to 2023, which never saw such a spike. If we remove May from both datasets — or even eliminate the highest month from each — we actually see a slight year-to-date increase.

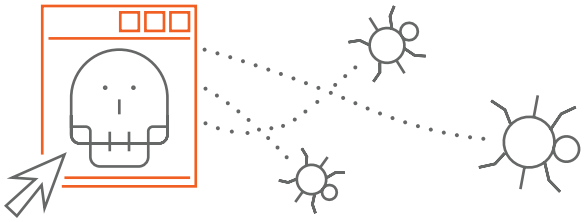
The same can't be said of malicious Microsoft Office files, however. The use of this attack type fell 75% compared with the same time period in 2022, with April's attack volume falling to the lowest point in five years. To put this drop in perspective, the total attack volume for the entire *first half* is only three-quarters of the number of attacks observed in March 2022.

Encouragingly, use of both file types continued to fall as the quarter went on, suggesting we may see even fewer of these in the second half.

2023 Malicious Office Files



As we've mentioned in previous reports, Microsoft has put new restrictions in place to prevent the malicious use of Excel files. As a result, the first half of 2023 saw the number of these files plummet. In its place, we've observed a jump in malicious Word files and malicious PowerPoints, as well as the rapid adoption of a new type of initial vector.



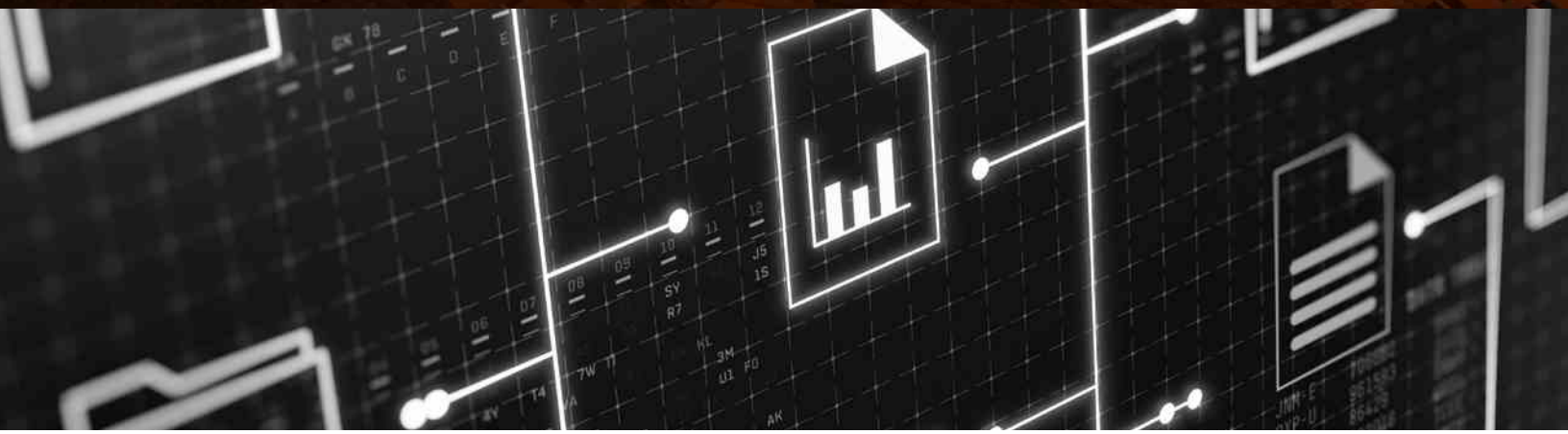
OneNote to Rule Them All?

The SonicWall Capture Labs research team has been tracking the use of malicious OneNote files since February 2023. These files, which weren't commonly used by cybercriminals until recently, have been observed delivering a wide variety of malware, including AgentTesla, AsyncRat and QakBot.

In the beginning, cybercriminals were hiding the malware payloads behind an image in the OneNote file. The target would then be enticed to click on the image, triggering the payload execution.

Shortly after, vendors began adding detections for these payloads, and various security researchers have released tools that can scan a OneNote file and list the embedded files present. As a result, later iterations shifted away from attaching the malware directly to the OneNote file, to instead including a URL within the file that pointed to the payload.

In an attempt to continue evading detection, many of the most recent versions have incorporated large quantities of null bites at the end of the OneNote file, then compressing it to appear smaller. The unarchived file size, which is greater than 500 MB, is then capable of bypassing AV scanning.



INTRUSION ATTEMPTS

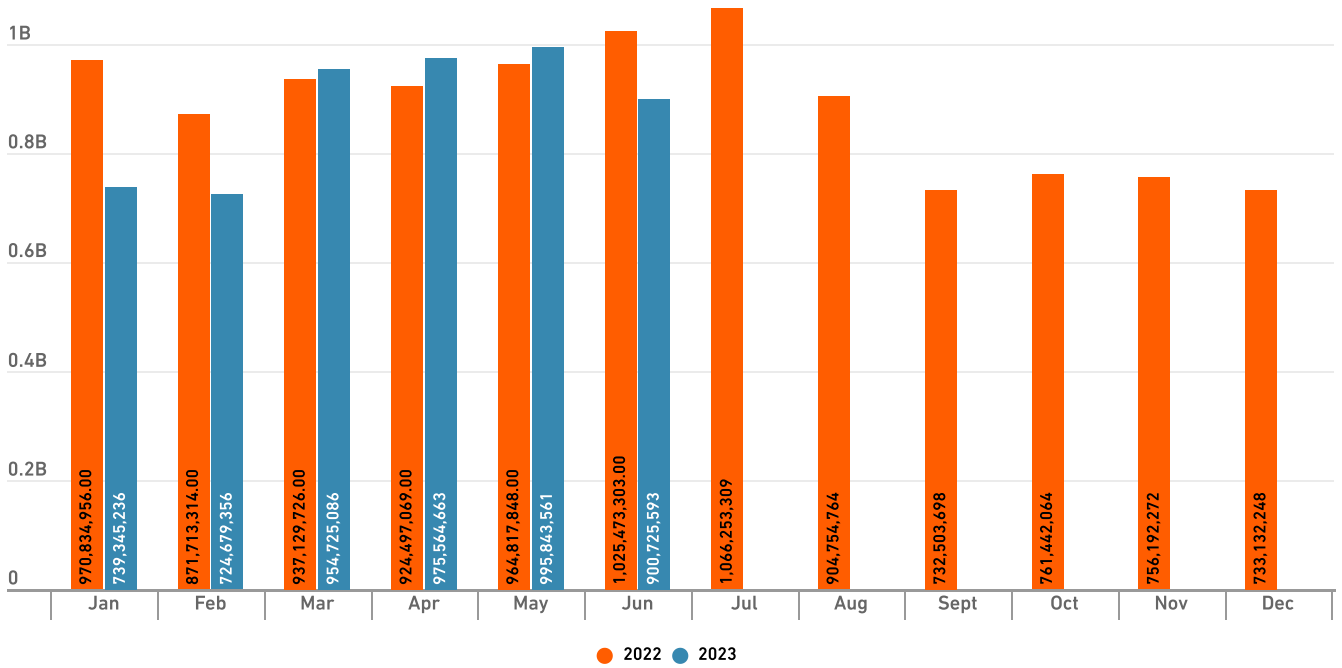
Overall Intrusion Attempts Rise

In the first six months of 2023, SonicWall threat researchers recorded 3.7 trillion overall intrusion attempts globally, a 21% increase over the first half of 2022. But a closer look at these attempts shows two divergent trends: An increase in low-severity intrusion attempts such as pings and other generally benign actions, and a *decrease* in medium- and high-severity intrusions. These attempts, also referred to as "malicious intrusions," fell 7% in the first half of 2023, to 5.3 billion.

While monthly attack volumes never matched the sky-high totals observed at the beginning of 2022, the trend was generally upward in the first half — so we may see them rise to these levels as the year goes on.

IN THE FIRST SIX MONTHS OF 2023, SONICWALL THREAT RESEARCHERS RECORDED 3.7 TRILLION OVERALL INTRUSION ATTEMPTS GLOBALLY, A 21% INCREASE OVER THE FIRST HALF OF 2022.

Global Intrusion Attempts



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

Intrusion Attempts by Region

But while the global trend line was relatively stable, with just gentle ebbs and flows, there was much more movement beneath the surface.

While North America still had the highest total attack volume, it also saw the largest decrease: intrusion attempts here fell 26% to 2.5 billion. This decrease was fueled by far-below-average monthly attack volumes: Since 2019, monthly attack volumes in North America have only dipped below 400 million three times — and two of those were January and February 2023.

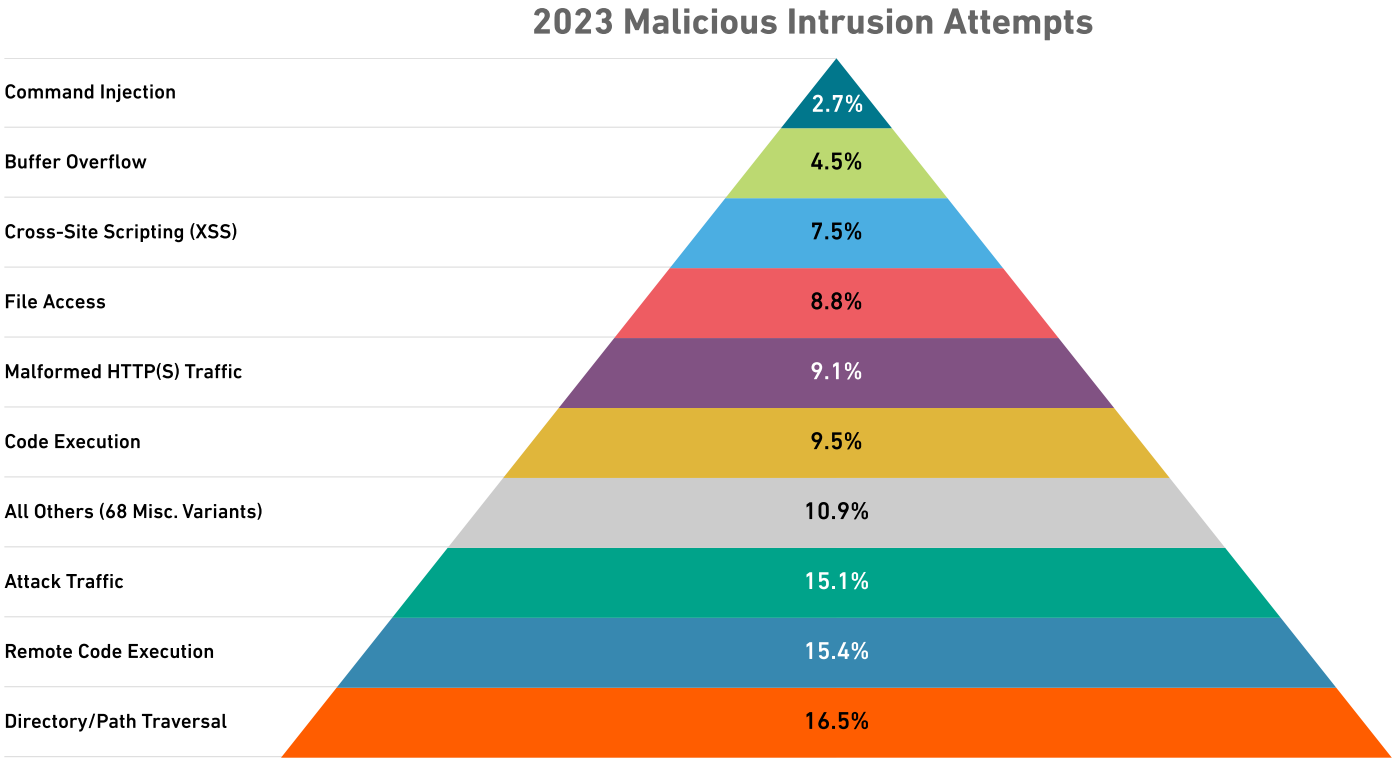
Asia also saw a decrease, albeit a smaller one. Despite reaching a four-year low of just 49.3 million in January, attack volumes in both May and June nearly tripled that. This sharp increase pushed total attacks for the region past 520 million, 18% less than the first half of 2022.

In contrast, Europe and Latin America both saw significant *increases* in malicious intrusions. Through the end of June, SonicWall threat researchers recorded 1.8 billion intrusion attempts in Europe, up 37% over mid-year 2022. Latin America saw an even bigger year-to-date increase of 43%. A new record high of 63.6 million in May, the highest monthly total since 2020, helped push total attacks for that region to 295.1 million so far in 2023.

Intrusion Attempts by Industry

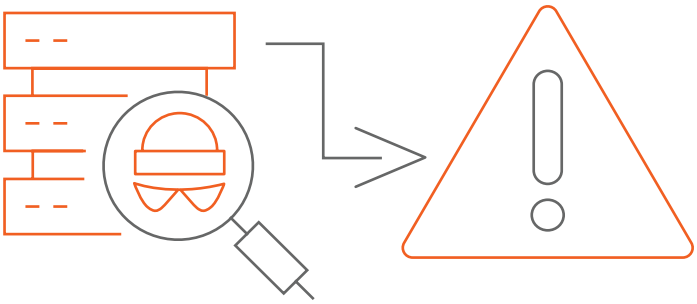
On average, around a third of customers in the industries we examined saw an intrusion attempt each month, as outlined in the table below. Something else you might notice: The industries with the highest attack volume aren't necessarily the ones with the highest percentage targeted. When an industry has high attack volume and a lower percentage of customers targeted, it often signals an increase in highly targeted attacks for that industry.

RANK BY VOLUME YTD	% CHANGE IN 2023	AVERAGE % OF CUSTOMERS TARGETED EACH MONTH	RANK BY VOLUME YTD 2022
Retail	↓15%	33.18%	1
Finance	↓13%	33%	3
Education	↓59%	38.5%	2
Government	↑45%	28.6%	5
Healthcare	↓46%	30.7%	4



What Was the Top Intrusion Type?

We're only halfway through 2023, but it's already brought significant changes in threat actor behavior — and intrusion types were no exception. While Remote Code Executions were on top in 2022, these attacks have decreased in 2023. At the same time, Directory/Path Traversal attempts (only the fifth-most preferred method in 2022) have increased, pushing this attack type into the top spot.



What Are Intrusion Attempts?

SonicWall categorizes intrusion attempts by three severity types: low, medium and high.

Low-severity hits typically consist of things like scanners and pings, actions which are not malicious and pose no threat to the target. Medium and high severity intrusions — also called malicious intrusion attempts — occur when a hacker or threat actor attempts to gain access to a system or resource by exploiting a vulnerability or weakness without authorization.

The vulnerabilities that are being exploited are typically public, but since not everyone patches at the same rate, attackers can take advantage of unpatched appliances or software to enter a network. (A more serious and dangerous scenario occurs when a vulnerability is not yet well publicized or has not been published: These are the dreaded zero-day vulnerabilities.)

Once inside the network, attackers can move laterally and establish persistence by exploiting other internal vulnerabilities in unpatched systems and software.

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

14m+
Malware Attacks Blocked Daily

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

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

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

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-MidYearCyberThreatReport-JK-8744