

MID-YEAR UPDATE

2022 SONICWALL CYBER THREAT REPORT

SONICWALL®

CYBER THREAT INTELLIGENCE FOR NAVIGATING
THE UNKNOWN OF TOMORROW

sonicwall.com | [@sonicwall](https://twitter.com/sonicwall)

 **Marlin**
Communications



Table of Contents

| | |
|---|----|
| Introduction | 3 |
| Malware | 5 |
| Ransomware | 12 |
| Log4j Update | 21 |
| Capture ATP & RTDMI | 23 |
| Malicious PDF/Office Files | 25 |
| Encrypted Attacks | 27 |
| IoT Malware | 29 |
| Cryptojacking | 31 |
| Intrusion Attempts | 34 |
| Attacks on Non-Standard Ports | 36 |
| About the SonicWall Capture Labs Threat Network | 38 |

Introduction

A Note From Bill



Cybercrime has been a global phenomenon for decades. But with geopolitical forces accelerating the reconfiguration of the world's cyber frontlines, the true danger presented by threat actors is coming to the fore — particularly among those that once saw the smallest share of attacks. For many, 2022 has been a wake-up call: there are no safe industries, and there are no safe countries. Cybercrime is everywhere.

And it touches every facet of our lives. During the average day, much of what we interact with — from the clothes that we wear to the cars that we drive, even the water that we drink — has been impacted by a cyberattack. And this already pervasive threat is growing and expanding at an alarming clip.

Already in 2022, we've seen attackers [compromise Microsoft Teams](#), slipping into chats and dropping malicious executables into conversations. We've seen QNAP ransomware specifically designed to seek out and [encrypt backups](#). We've seen cybercrime syndicates attempting to [destabilize entire nations](#).

It's a terrifying prospect, until you consider its corollary: Cybersecurity is also everywhere.

In every state and every country, there are individuals who have dedicated their lives to beating back an ever-encroaching wave of cyberattacks. If you're not one yourself, you probably work with at least one of them; I've been fortunate enough to work with thousands of them.

As the cyber arms race continues to escalate, they're the ones on the front lines, observing and anticipating the global threat landscape from a business perspective to remain proactive against an increasingly volatile global threat environment.

Cybersecurity professionals and their tools are [saving lives](#) in our [hospitals](#), safeguarding our communications networks, forming barricades around [critical infrastructure](#) in war-torn regions and even [hijacking ransomware](#) strains.

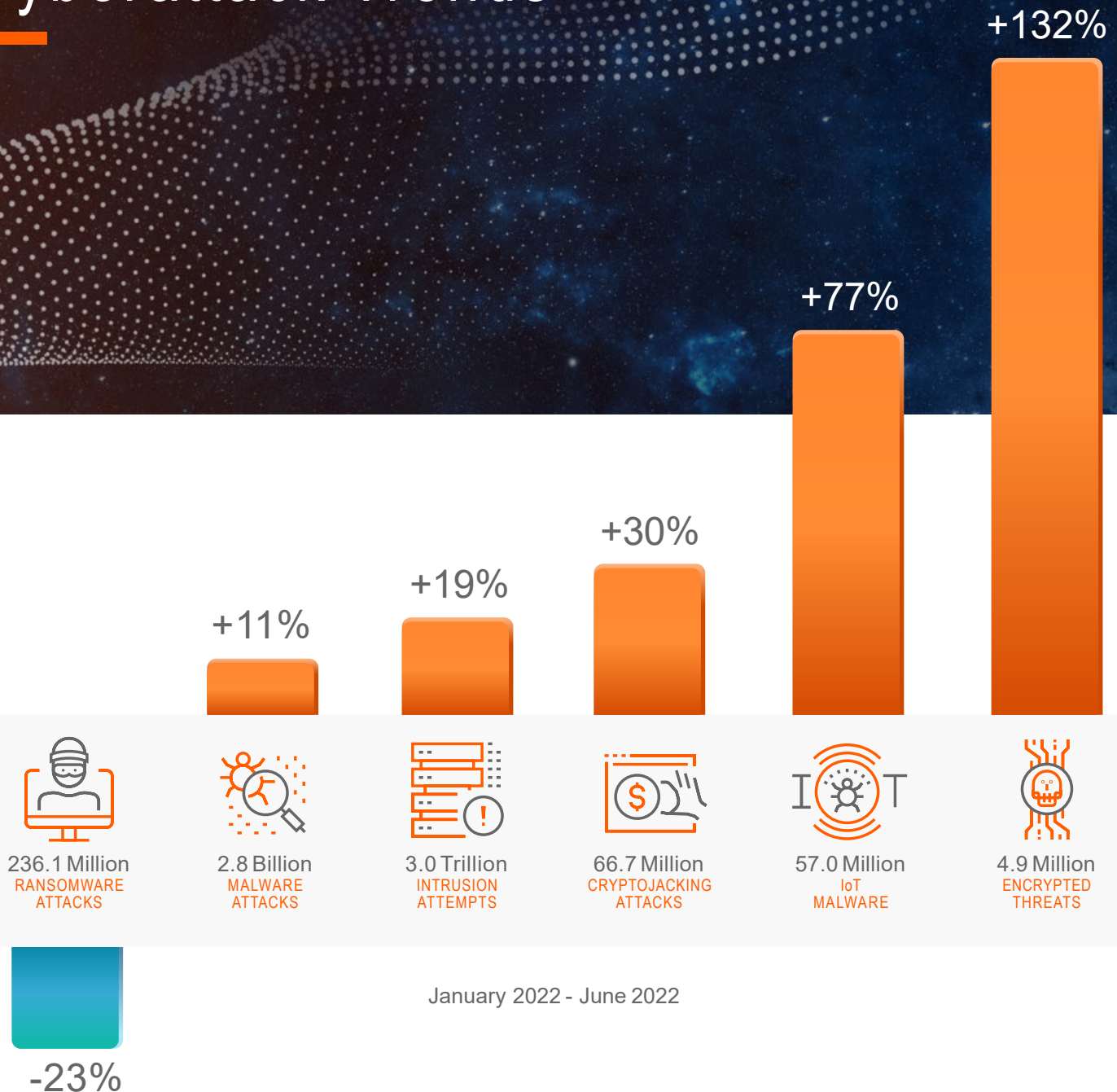
And unlike threat actors, who may be motivated by money, fame, nationalism or any number of other factors, those fighting on the side of good are united in purpose, dedicated to helping build a safer world for everyone.

As the cyber warfare battlefield continues to shift — changing the challenges of Europe, the United States and the rest of the world — cybersecurity professionals at SonicWall and elsewhere will continue communicating, innovating and fostering resiliency among our customer organizations and the world at large. So that when cybercriminals shift strategies and acquire new targets, we'll be prepared with the tools, talent and technology to meet them where they are. And we will ultimately prevail.

A handwritten signature in black ink, appearing to read 'Bill Conner'.

BILL CONNER
PRESIDENT & CEO
SONICWALL

2022 Global Cyberattack 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 Rebounds, Rising 11%

There have been three big comebacks so far in 2022: “Top Gun,” Kate Bush’s “Running Up That Hill” ... and malware.

In the first half of 2022, SonicWall Capture Labs threat researchers recorded 2.8 billion malware hits globally, an 11% increase year-to-date over 2021. This amounts to an average of 8,240 malware attempts per customer.

But paradoxically, buried amid data that shows double-digit increases is actually a tremendous drop. June’s malware volume is so extraordinarily low at 364.7 million that we haven’t seen its equal in more than two-and-a-half years.

Why is Malware Up?

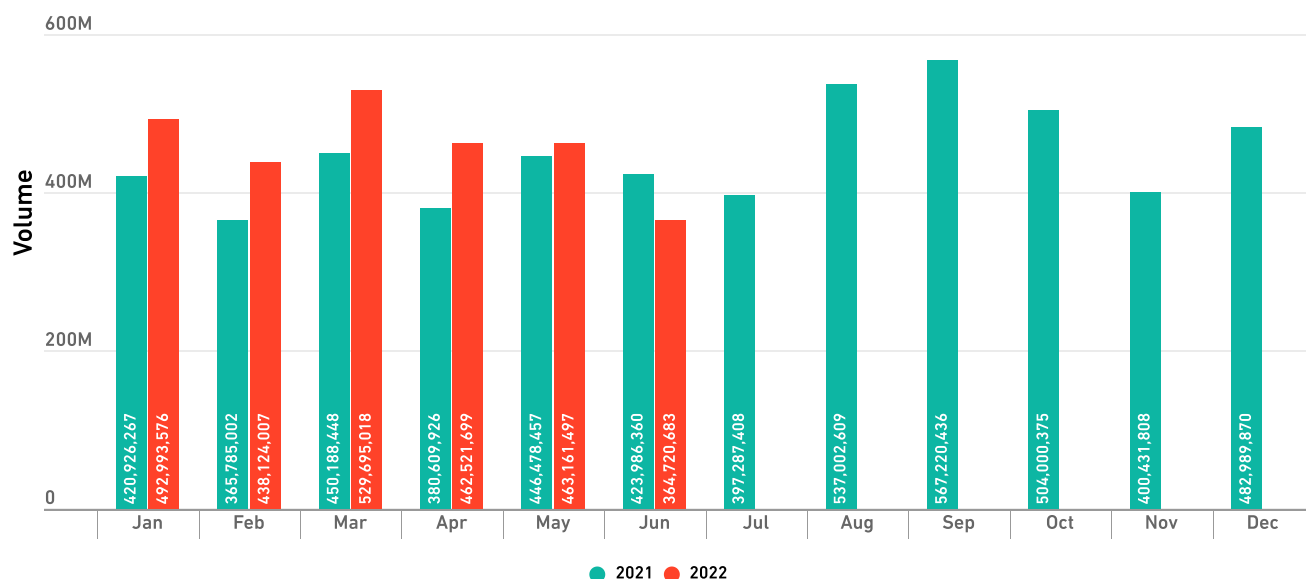
At the end of 2021, we posed the question: Are we seeing more malware because we’re *seeing* more malware, due to people returning to the office and the corporate perimeter?

Or are we seeing more malware because there *is* more malware? At the end of the first half of 2022, we can definitively say that it’s the latter.

Between [September 2021](#) and [March 2022](#), the number of remote-capable workers who were working either a fully remote or hybrid schedule grew from 67% to 81%. So if we were previously seeing more malware because more people were coming back to the office (and thus the protection of the corporate network), we would have expected to then see a corresponding drop as the percentage of remote work arrangements rebounded. Clearly, this has not been the case.

Based on data collected by SonicWall Capture Labs threat researchers, the true culprits behind the rise in malware have been cryptojacking and IoT malware, which have risen 30% and 77%, respectively, year to date.

Global Malware Volume



Malware by Region

Based on regional data, malware seems to not only be increasing, but also changing course.

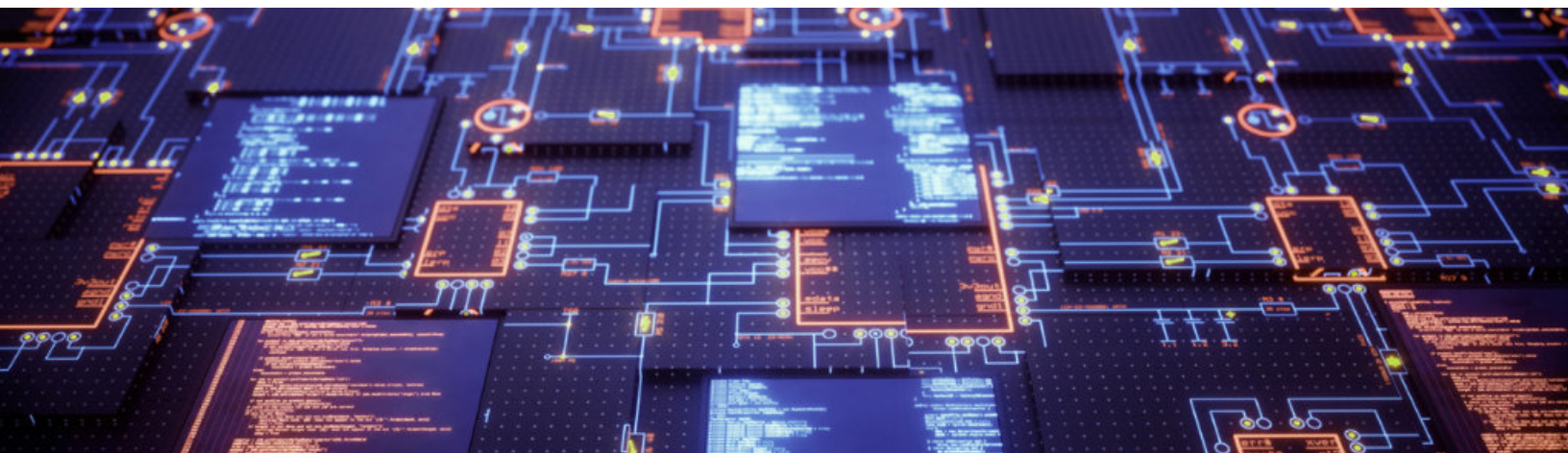
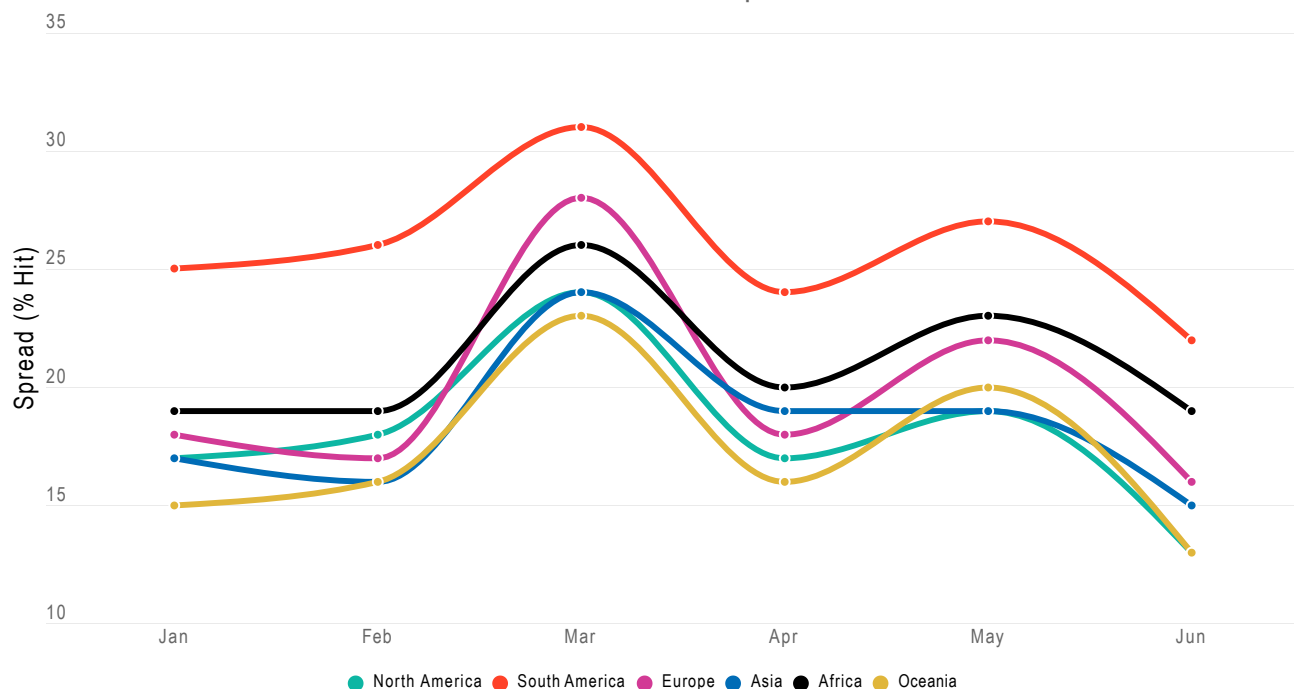
In North America, which typically sees by far the largest malware volume, attacks increased by just 2% — much lower than the global average.

So which regions drove that average up? In short, all the rest of them. Malware in Europe, usually second in terms of volume, rose 29%; while malware volume in Asia, which tends to be lower still, showed an even greater increase at 32%.

The same trend can be observed on a country-by-country basis. For example, the United States actually saw malware *decline* 1% year-to-date (the uptick observed in North America can be attributed to greatly increased malware volumes in Mexico and Canada).

The U.K. and Germany, which also typically have a higher-than-average amount of malware, saw even larger drops of 9% and 13% respectively — each running counter to the nearly 30% *increase* observed for Europe as a whole.

2022 Global Malware Spread Trend



Malware Spread

A look at malware spread data for the first half of 2022 shows a case of history repeating: Just like in 2020, malware spread for every continent peaked in March.

But if the COVID-19 pandemic was the likely driver of the March spike in 2020, what resulted in such a uniform and well-defined March spike in 2022? While we can't know for sure, it's likely another event of worldwide interest, in this case the Russia-Ukraine conflict.

While the countries with the highest malware volume were the U.S., India, the U.K. and Germany, this doesn't mean that a given organization in these countries was more likely to see malware. Once again, we see that most of the top countries for malware volume don't even make the top 10 for malware spread, with one notable exception: Brazil, which is the only country to appear on both lists (No. 5 in terms of volume, and No. 9 in terms of spread).

In the first half of 2022, an organization located in Slovenia had the highest chance of seeing an attack, at 33.3%. In contrast, an organization in Luxembourg had only a 7.3% chance of seeing an attack, making it the "safest" country in terms of malware.

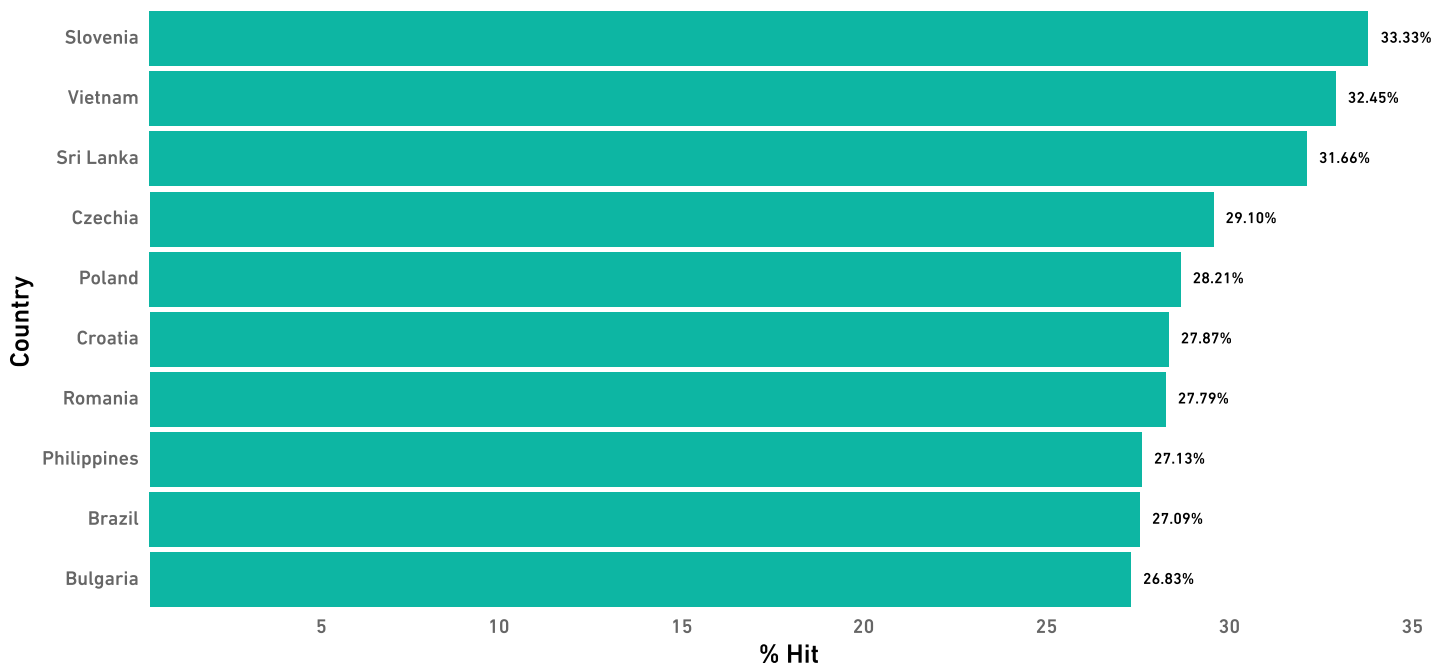
What Is Malware Spread?

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.

2022 Malware Spread | Top 10 Countries



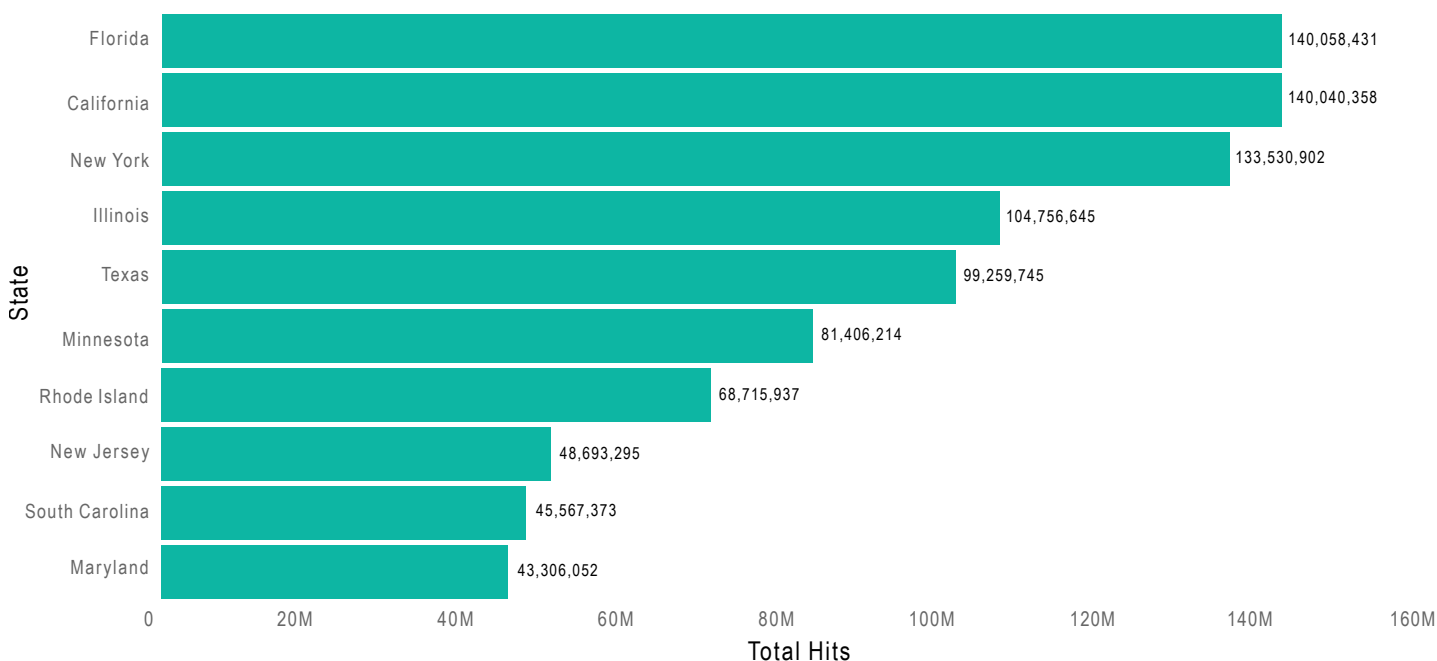
It's worth noting that countries in general are seeing less malware spread in 2022: Last year the riskiest country, Vietnam, saw a malware spread of 36.4%, while an organization in 2021's safest country, the Bahamas, was more than twice as likely to see an attack at 15.87% as Luxembourg is today.

In the first half of 2022, Florida experienced 140.1 million malware hits, enough to retain its position as the worst state for malware volume.

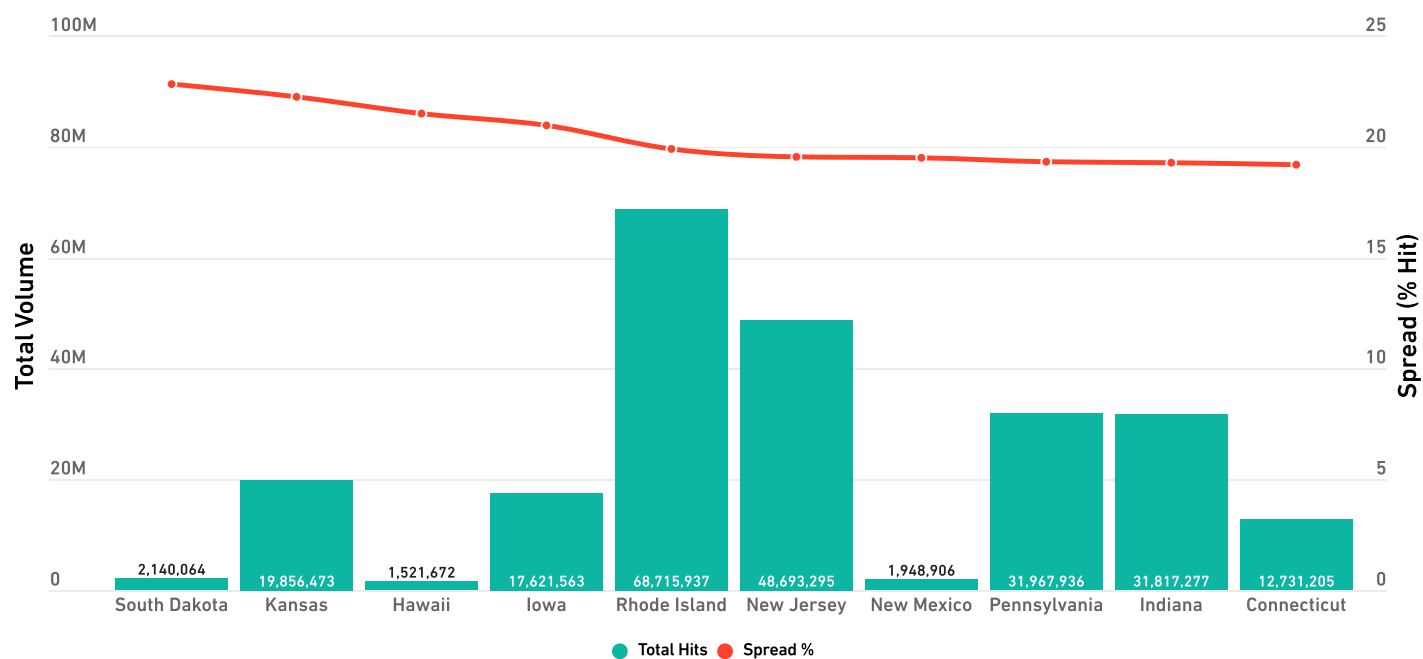
But while New York was No. 2 in 2021, it has now slipped to third with 133.5 million hits — while the 140 million hits recorded in California sent it back up the list to second.

But as we saw with the country-specific data, high malware volume does not necessarily predispose an area to a high malware spread percentage. While the Venn diagram of these datasets is usually two distinct circles, in the first half of 2022 there were two states that made both lists: Rhode Island, which was No. 7 for volume and No. 5 for spread, and New Jersey, which was No. 8 for volume and No. 6 for spread.

2022 Malware Volume | Top 10 U.S. States



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



So which state is the riskiest? South Dakota, where 22.9% of organizations saw a malware attack. Kansas, which was the highest for two years running, has slipped to No. 2, and Hawaii jumped one spot to round out the top three.

On the other side of the spectrum, Texas (which had the fifth-highest volume at 99.3 million) was the safest state: Only 15.5% of organizations there saw an attempted malware attack.

22.9%

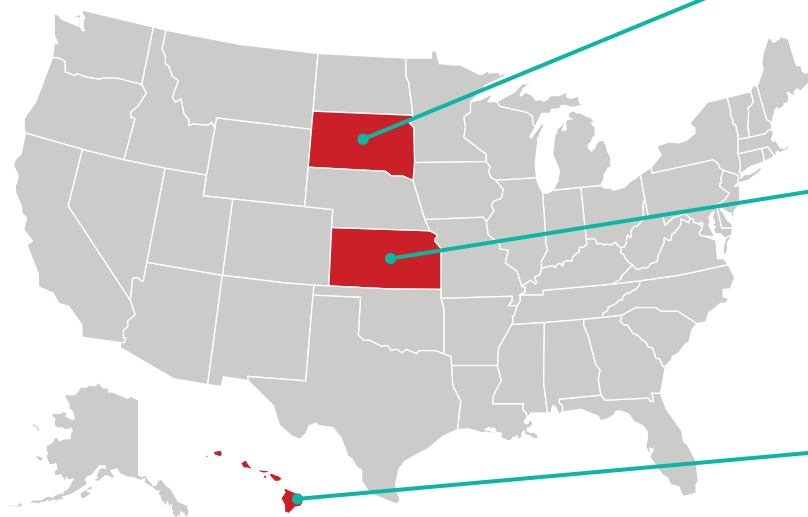
Of organizations in South Dakota saw a malware attack.

22.3%

Of organizations in Kansas saw a malware attack.

21.5%

Of organizations in Hawaii saw a malware attack.

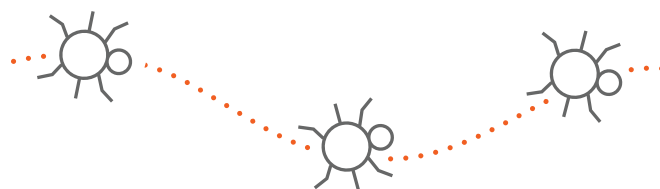


Malware by Industry

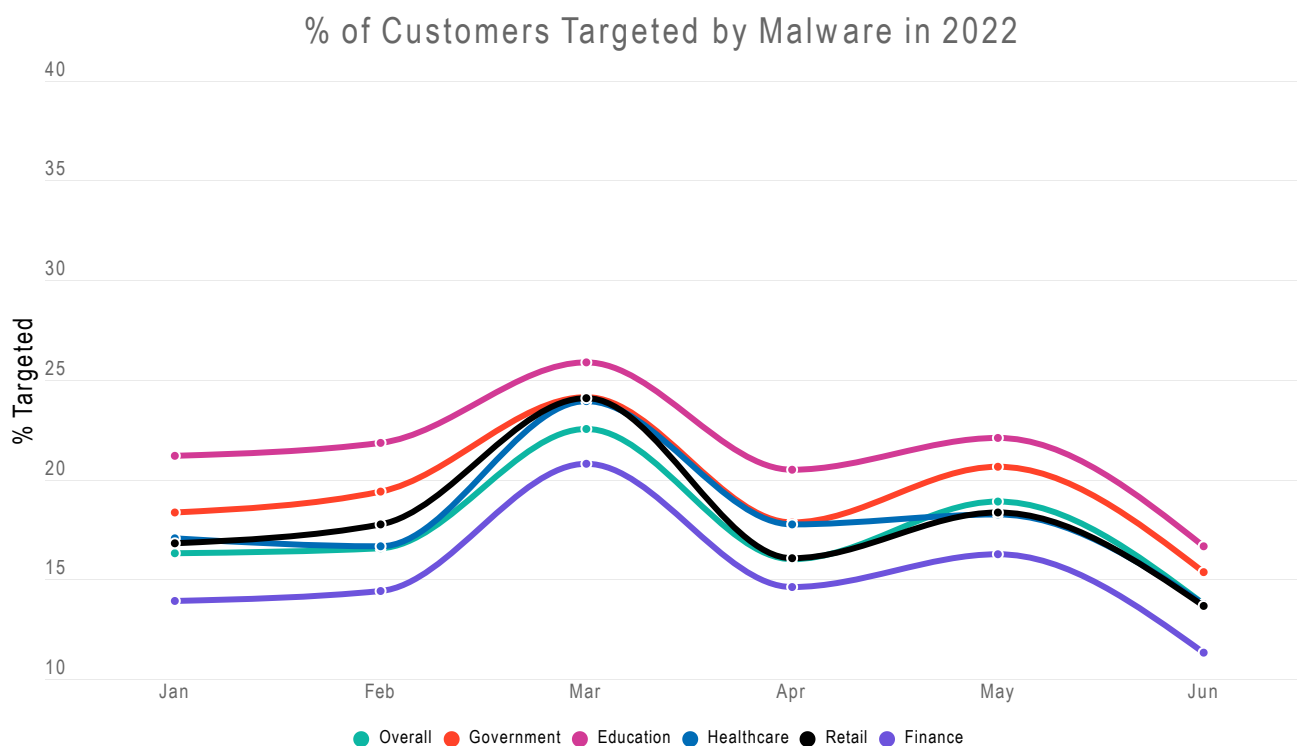
Does the graph below look familiar? In an unusual case of synchronicity, the trend lines for percentage of industry customers targeted by malware follows the same pattern as the malware-spread by continent graph for the first half of 2022, complete with a moderate start, a peak in March, a drop in April, a smaller peak in May, and a bottoming out in June.

Once again, those in education saw the highest percentage of customers targeted, at an average of 21.4% per month, followed by government, with 19.3% of customers targeted. However, there was one bit of good news: both of these percentages are down slightly from last year, meaning there were fewer customers affected overall.

Finance, an industry we began reporting on this year, sat at the other extreme: Only 15.2% of finance organizations on average saw a malware attack.



Those in education saw the highest percentage of customers targeted, at an average of 21.4% per month, followed by government, with 19.3% of customers targeted.



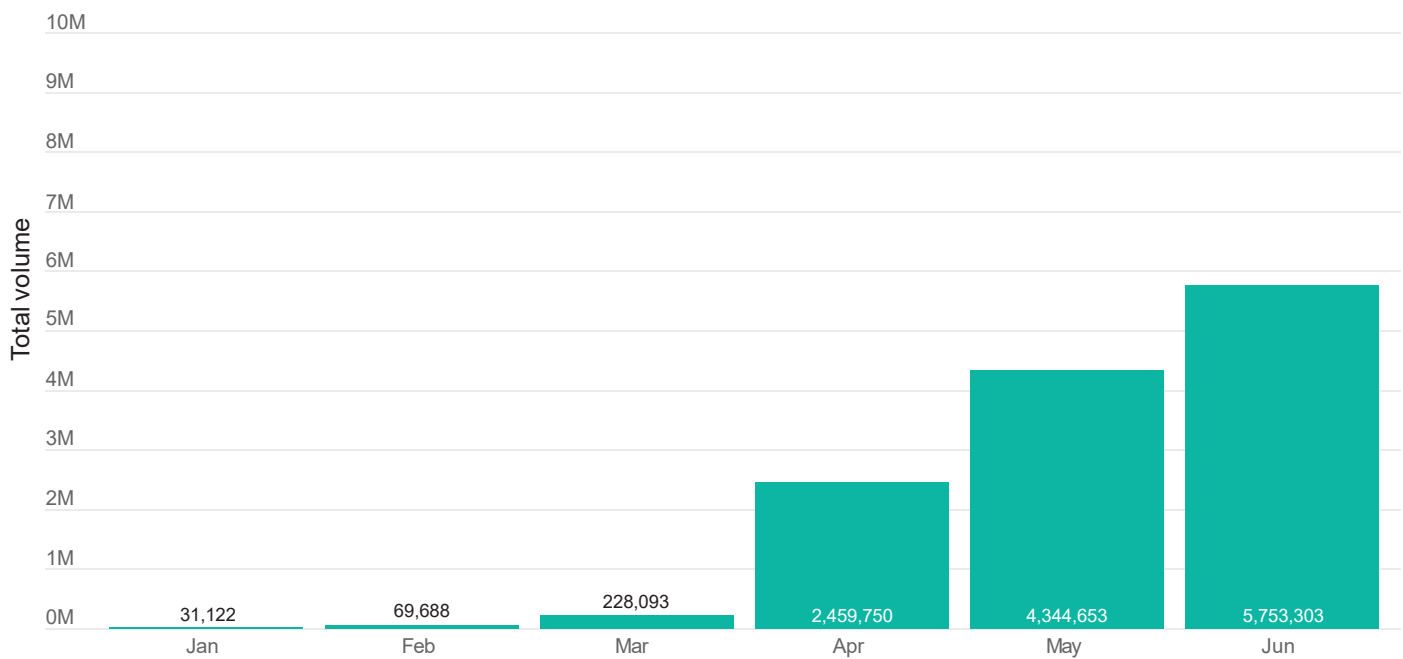


Ukraine Sees Massive Malware Increase

We typically don't report on cybercrime in Ukraine: SonicWall requires a minimum of 1,000 active sensors for public reporting, and our footprint in Ukraine falls far short of this threshold for statistical relevancy.

However, given the ongoing conflict between Ukraine and Russia, a known haven for cybercriminals, we took a closer look at the data gathered from the sensors we do have there, and discovered some anecdotal trends.

2022 Malware Volume | Ukraine



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

During the first half of 2022, the increase in malware has been *extraordinary*. In January 2022, SonicWall Capture Labs threat researchers logged 31,122 malware attempts in Ukraine. By June, monthly malware volume in Ukraine reached 5.8 million, a staggering 18,386% increase.



Ransomware

Ransomware Attacks Down 23% as Geopolitical Landscape Complicates Cybercriminal Activity

SonicWall Capture Labs threat researchers recorded 236.1 million ransomware attempts in the first half of 2022. This represented a 23% drop globally, as geopolitical forces, volatile cryptocurrency prices, and increased government and law-enforcement focus impacted both who cybercriminals chose to attack and how well they were capable of carrying out those attacks.

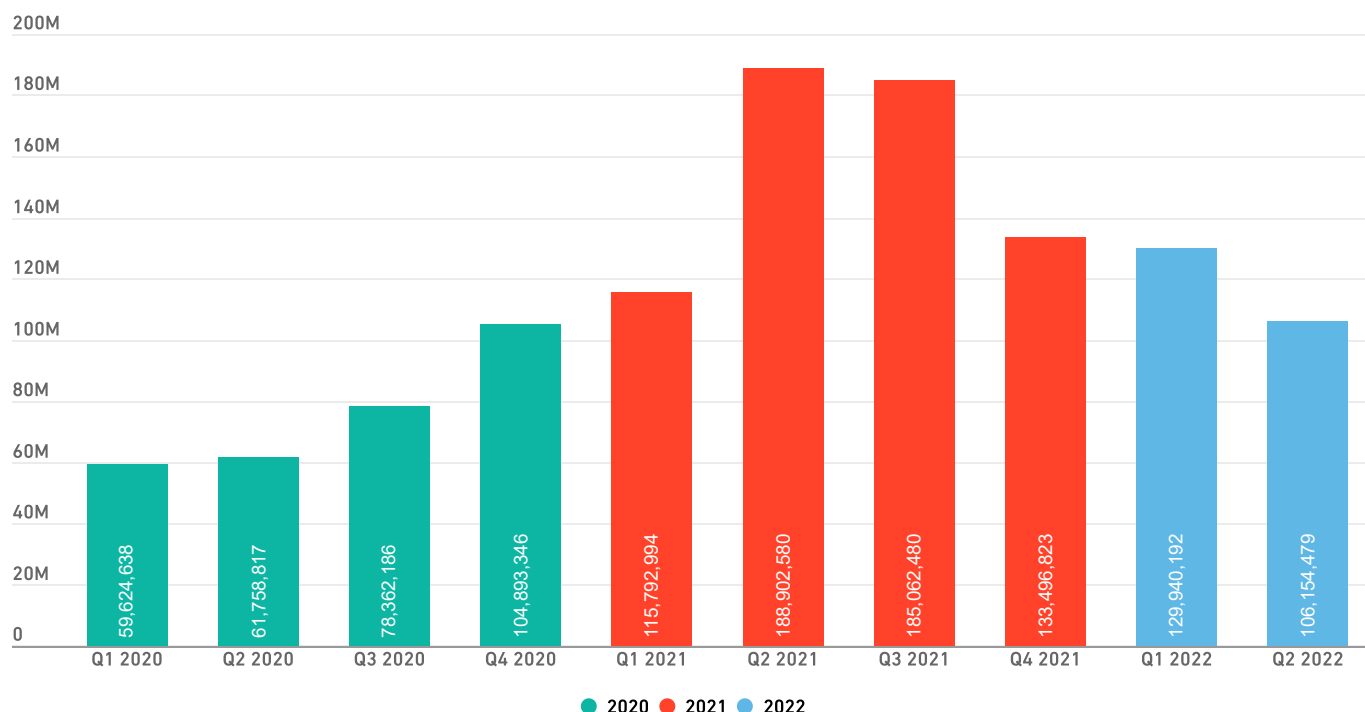
After two straight years of increase, ransomware volume peaked in Q2 2021 at 188.9 million. Combined with Q1, this was already enough to push ransomware to a new yearly high. But mercifully, Q3 and Q4 began a downward trajectory, one which has continued into this year.

Q2 2022 has marked the fourth consecutive quarter of decrease, and the lowest quarter seen since late 2020.

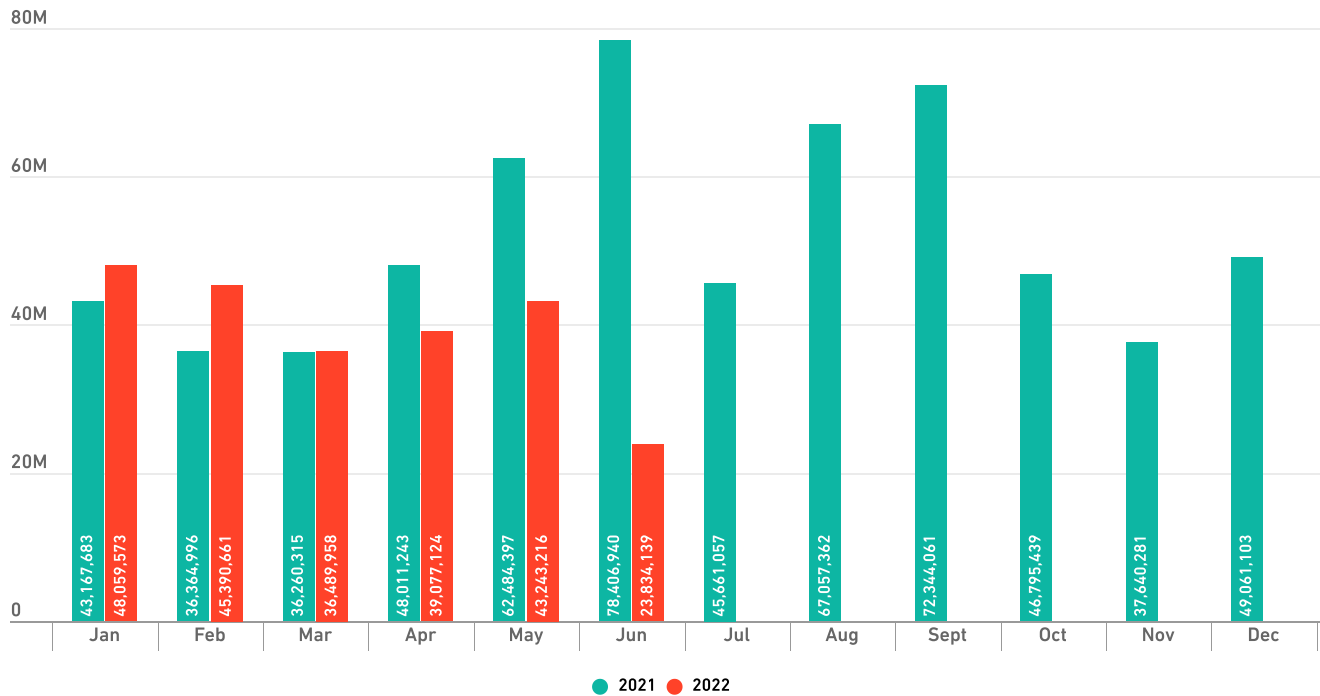
This is noteworthy in its own right, as it breaks an established quarterly trend in ransomware. For four years running, ransomware volume increased from Q1 to Q2. This is the first year since at least 2018 that it didn't happen.

But Q2 was also noteworthy for another reason: June 2022's unexpectedly low ransomware total. That month, SonicWall researchers recorded just 23.8 million ransomware hits, the lowest number in 23 months, and down nearly 45% from the already relatively low levels seen the previous month.

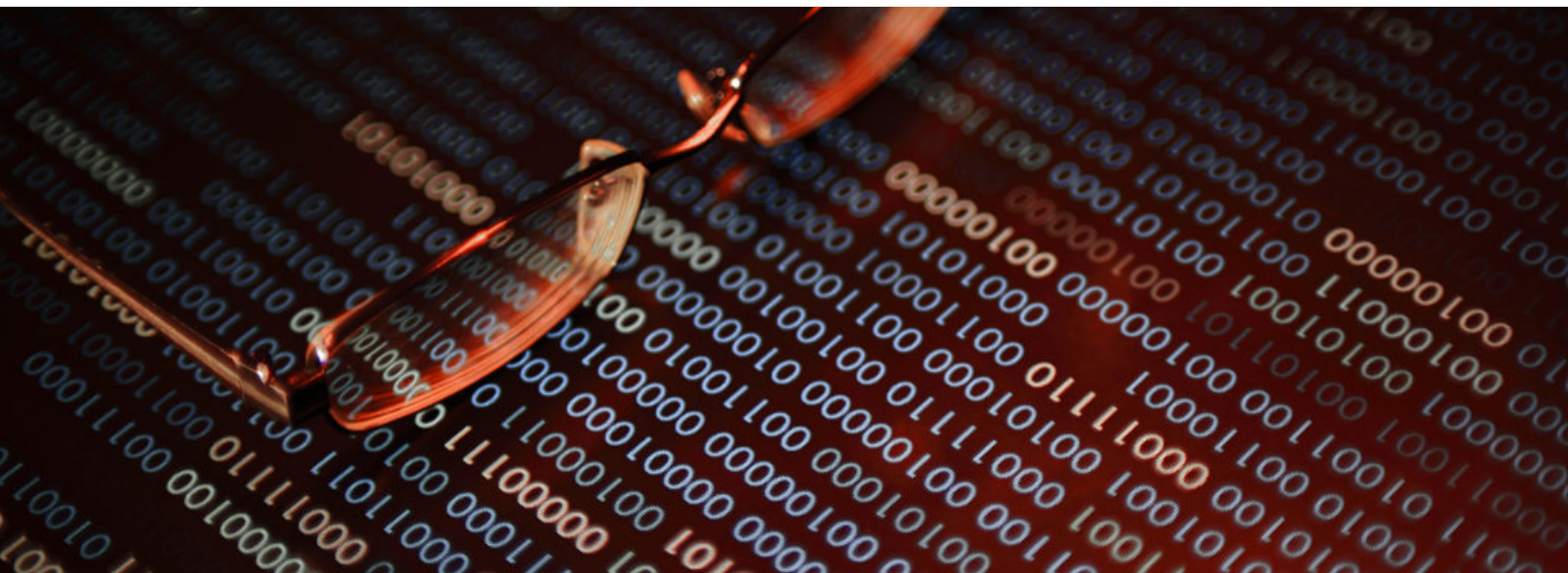
Global Ransomware by Quarter



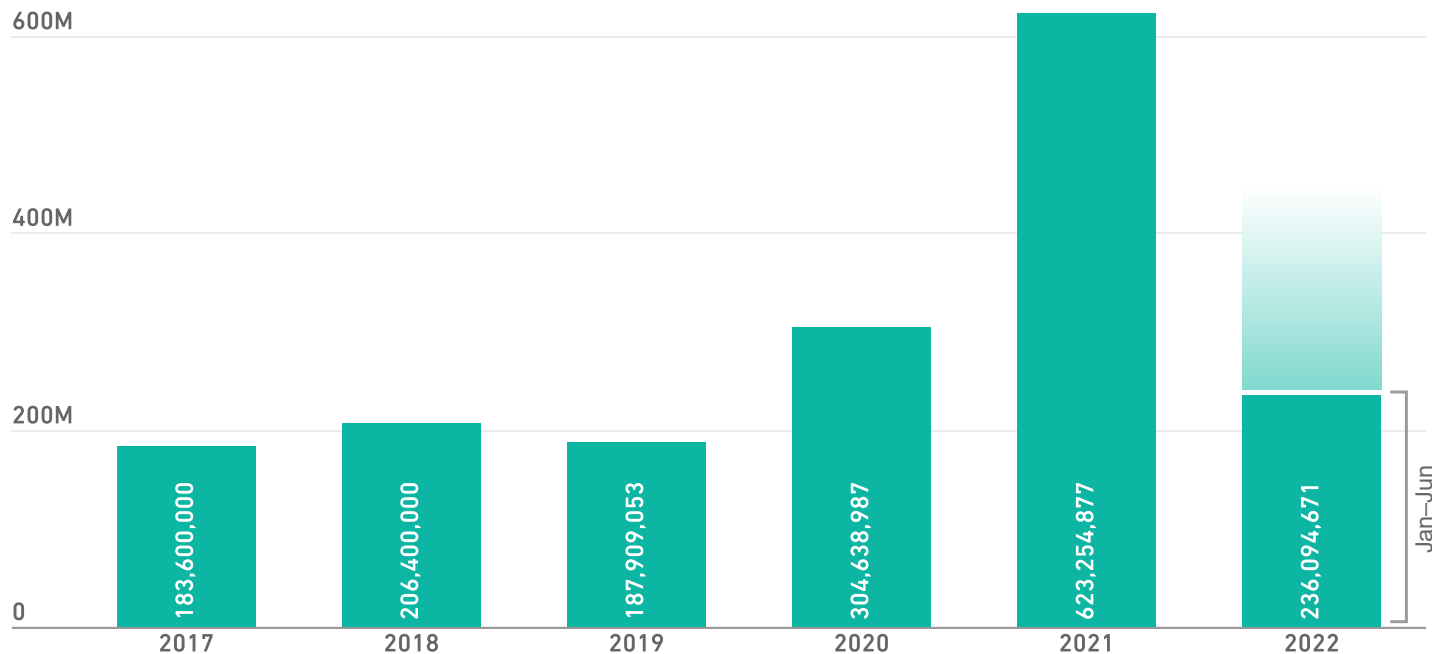
Global Ransomware Volume



But while a decrease in ransomware volume is unquestionably good news, it's important to keep this drop in perspective. The amount of ransomware we've seen in the first half of 2022 has already eclipsed the full-year totals for each of 2017, 2018 and 2019, meaning we're still far above pre-pandemic levels.



Global Ransomware Volume by Year



Note: 2017-2021 full-year data; 2022 only includes six months of data

More importantly, we're already 77.5% of the way to reaching 2020's full-year ransomware totals. Barring an extreme and unprecedented dip in volume during the second half of this year, 2022 will surpass 2020's ransomware totals to become the second-worst year for ransomware since SonicWall began tracking.

What's Behind the Reduction in Ransomware?

There are likely several factors contributing to the drop in ransomware, such as [continued volatility of cryptocurrency prices](#) and more stringent [requirements from cybersecurity insurance underwriters](#). There's also been an increased hardening of organizations, both in response to high-profile attacks such as JBS Foods and Colonial Pipeline, and in light of increased guidance from governments around the world.

But according to the U.S. National Security Agency (NSA) Director of Cybersecurity Rob Joyce, the biggest factor in ransomware's decline [is likely political conflict](#).

"One interesting trend we see is, in the last month or two, ransomware is actually down. There's probably a lot of different reasons why that is, but I think one impact is the fallout of Russia-Ukraine," Joyce said at the July 2022 National Cyber Security Centre Cyber UK event in Wales.

In July, U.S. Cyber Command and NSA chief Gen. Paul Nakasone corroborated this statement, noting that U.S. Cyber Command [is seeing fewer ransomware attacks](#).

"I would echo Rob Joyce's comments," Nakasone said at the International Conference on Cybersecurity. "We're seeing Russians much more focused on activities related to Ukraine."

Despite continued denials that the country is harboring cybercriminals, roughly two-thirds of state-sponsored cyberattacks [have been traced back to Russia](#) in the past few years, according to various sources. And 74% of all money generated by ransomware last year — nearly \$400 million — went to groups ["highly likely to be affiliated with Russia."](#)

In other words, what affects Russia also affects cybercriminals, and what affects cybercriminals also affects *cybercrime*. According to Joyce, sanctions against Russia in response to attacks on Ukraine have affected ransomware groups in a variety of ways.

"As we do sanctions and it's harder to move money and harder to buy infrastructure on the web, we're seeing them be less effective — and ransomware is a big part of that," Joyce said.

According to Joyce, cybercriminals [have been complaining](#) about an inability to use credit cards and other means to purchase the infrastructure needed for their attacks from Western countries, as well as increased difficulty moving money around.

"We've seen that have an impact on their operations," Joyce explained, noting that these actions have helped to drive down ransomware rates.

There's also increasing pressure on the other side of the equation. The number of organizations willing to pay a ransom demand has [been trending downward](#), from 85% of targets in the first quarter of 2019 to less than half in the first quarter of 2022.

Due to [press coverage of the conflict](#) and warnings about [possible cyberattacks from Russian cybercriminals](#), people are increasingly aware of the Russia/ransomware connection. Some may be worried that the money could fund the Russian government's actions, and object to paying a ransom on ethical grounds. Others may fear the double jeopardy that could result from paying a ransom, only to incur civil penalties from their own government [for violating sanctions](#).

But governments aren't just relying on sanctions to combat ransomware. They're stepping up their response to ransomware in a big way. In February 2022, the U.S. FBI [launched the Virtual Asset Exploitation Team](#) to track ransomware and ransomware profits, just months after the formation of the Justice Department's National Cryptocurrency Enforcement Team late last year. These teams follow on the heels of a series of high-profile busts in 2021, [some involving millions of dollars](#). All of these initiatives should serve to further suppress ransomware rates.

Why Ransomware Won't Be Going Away

But readers should be cautious not to mistake these happenings for harbingers. Ransomware may be down, but it certainly isn't out.

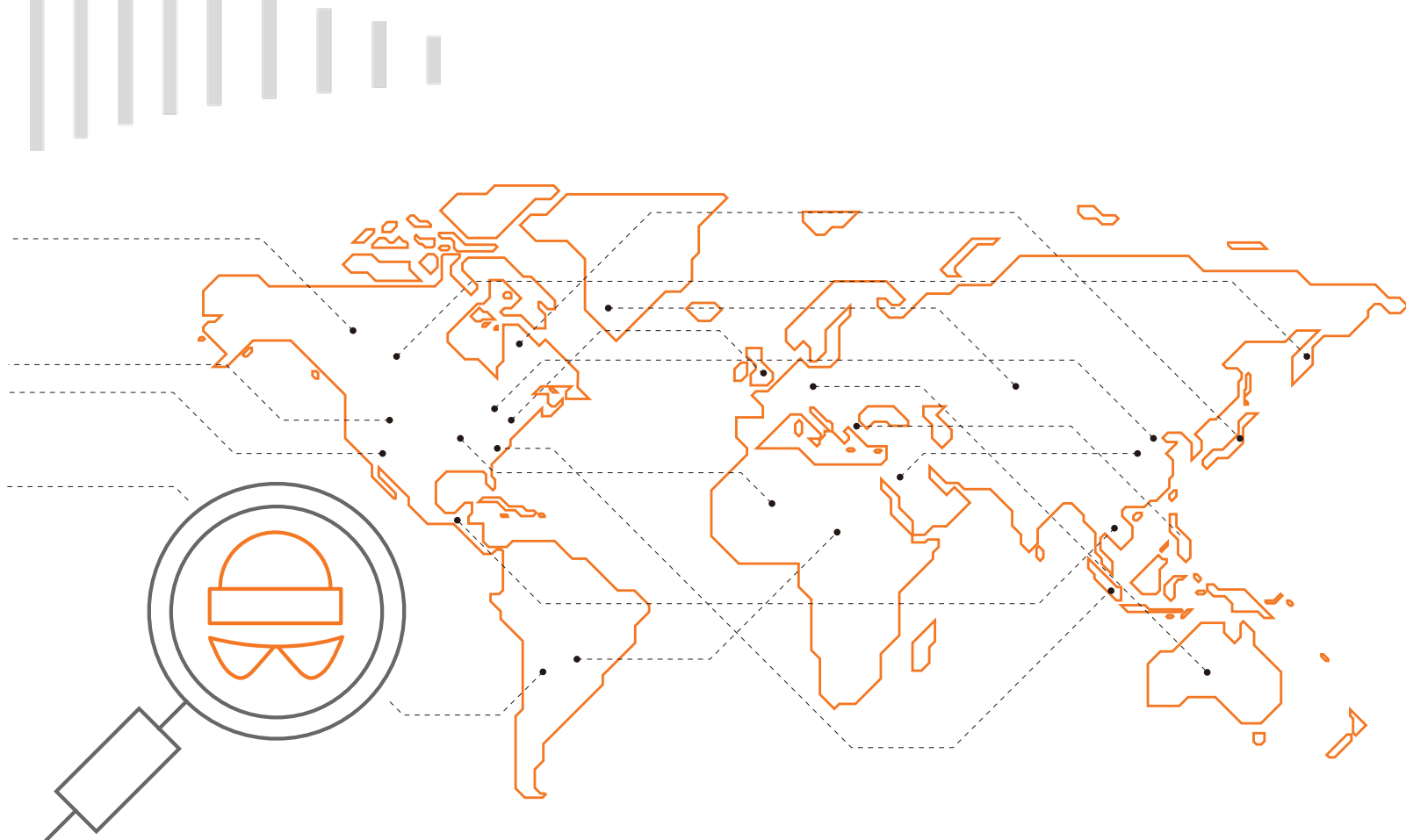
FBI Director Christopher Wray, who attended the International Conference on Cybersecurity along with Gen. Nakasone, [confirmed that the FBI is still seeing a variety of ransomware attacks](#), covering a range of motives and



affecting almost every critical infrastructure sector in the United States. And even with a decrease in ransomware, SonicWall still recorded an average 707 ransomware attempts per customer in the first half of 2022.

As long as there's a financial incentive, there will still be ransomware. And while the number of targets paying ransoms may be falling, ransom amounts are still rising dramatically. These ventures are currently so lucrative that, according to Joyce, ransomware gangs [are now able to buy zero-day exploits](#) and bankroll research into vulnerabilities that they can then exploit.

"As bad actors diversify their tactics, and look to expand their attack vectors, we expect global ransomware volume to climb — not only in the next six months, but in the years to come," said SonicWall President and CEO Bill Conner. "With so much turmoil in the geopolitical landscape, cybercrime is increasingly becoming more sophisticated and varying in the threats, tools, targets and locations."



Ransomware by Region

Ransomware in North America dropped by 42% in the first half of 2022. That's nearly 100 million ransomware attacks — or 556,000 ransomware attempts a day — that happened last year, but didn't happen this year.

Because of the high percentage of global ransomware that occurs in North America, this drop pulled the global average down into the negative range. But this paints an unrealistic picture of how most places experienced ransomware in the first half.

In Asia, ransomware went up 4%, a much smaller increase than last year. In contrast, ransomware in Europe shot up 63% year-to-date to 63 million. Much of this was due to unusually high attack volume in May, when ransomware reached 24.7 million — more than three times what it was in May 2021, and more than *10 times* the volume in May 2020.

There were tremendous shifts at the national level, as well. In last year's mid-year update, we noted a 185% increase in the U.S. (then ranked first for ransomware) and a 144% increase in the U.K. (at that time, second), accelerating a steady upward trend.

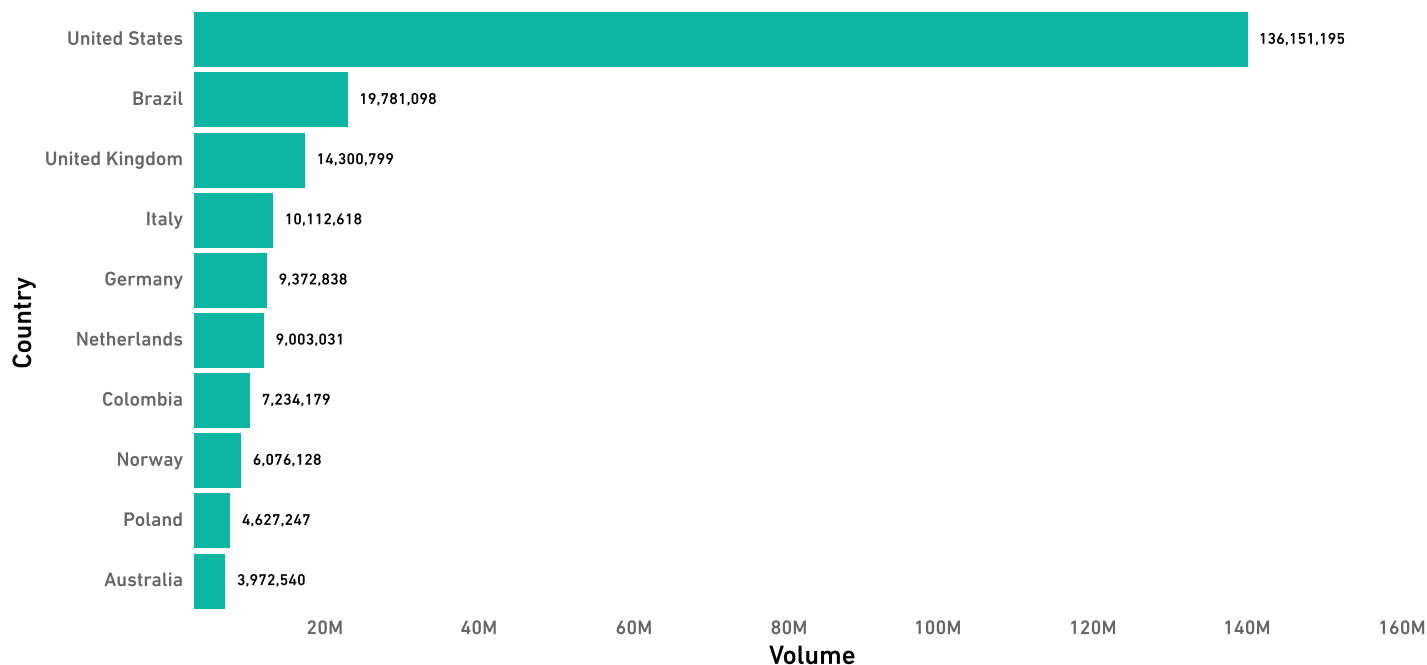
But in the first half of 2022, these trends completely reversed. The U.S. has now seen a 42% *decrease* in ransomware, while ransomware in the U.K. fell 2%.

But while the news is good for the U.S., U.K., and the other typical hotspots that saw decreases, much of this ransomware didn't actually disappear — it was simply redistributed. In the first half of 2022, many countries that typically see less ransomware have seen their ransomware volumes increase.

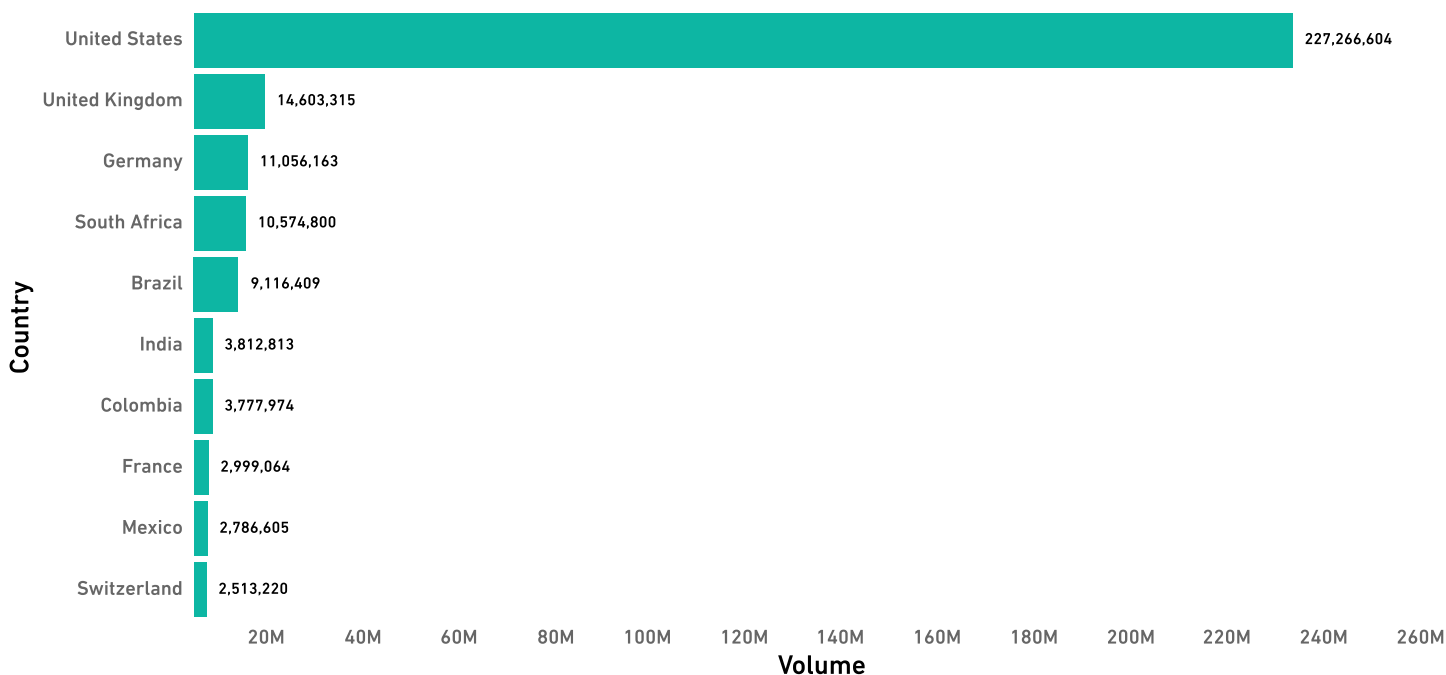
This becomes clearer when comparing 2021's list of top 10 countries for ransomware to that of the first half of 2022. Even though ransomware was much higher last year overall, the entire second half of that list had less than 4 million hits each. This year, only Australia (No. 10) has fewer than 4 million hits — and only barely, at that.

Comparing these lists illustrates the rise of Europe as a ransomware hot spot: At the midpoint of last year, only five of the top 11 countries for ransomware volume were in Europe. In 2022, that number has risen to seven.

2022 Ransomware Volume | Top 10 Countries



2021 Ransomware Volume | Top 10 Countries



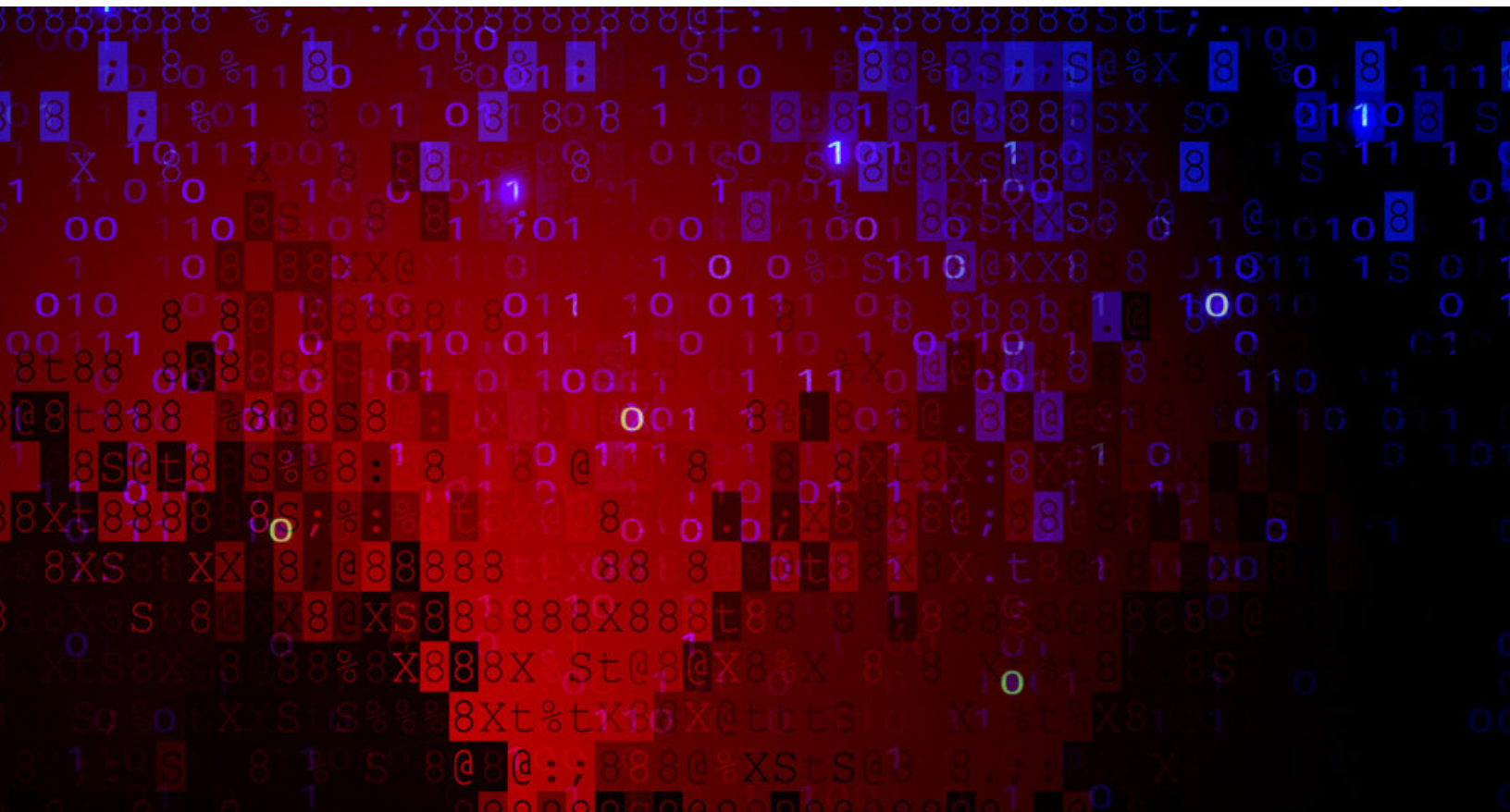
But there's an important geopolitical distinction here as well. *Every one of the countries on the top 10 list for ransomware in 2022 has condemned Russia's actions in Ukraine.*

It's also important to note which countries from last year's list are missing from this year's, such as South Africa, India and Mexico.

The fact that they've fallen off the list is likely due to ransomware's overall shift to Europe, as these are not European countries. But despite the fact that they're thousands of miles apart, these countries all share one interesting thing in common.

[South Africa](#) and [India](#) have both refused to condemn Russian President Vladimir Putin's actions in Ukraine. And while Mexico did condemn the attacks, it has [refused to participate in sanctions](#) and has criticized other countries' censorship of Russian media.

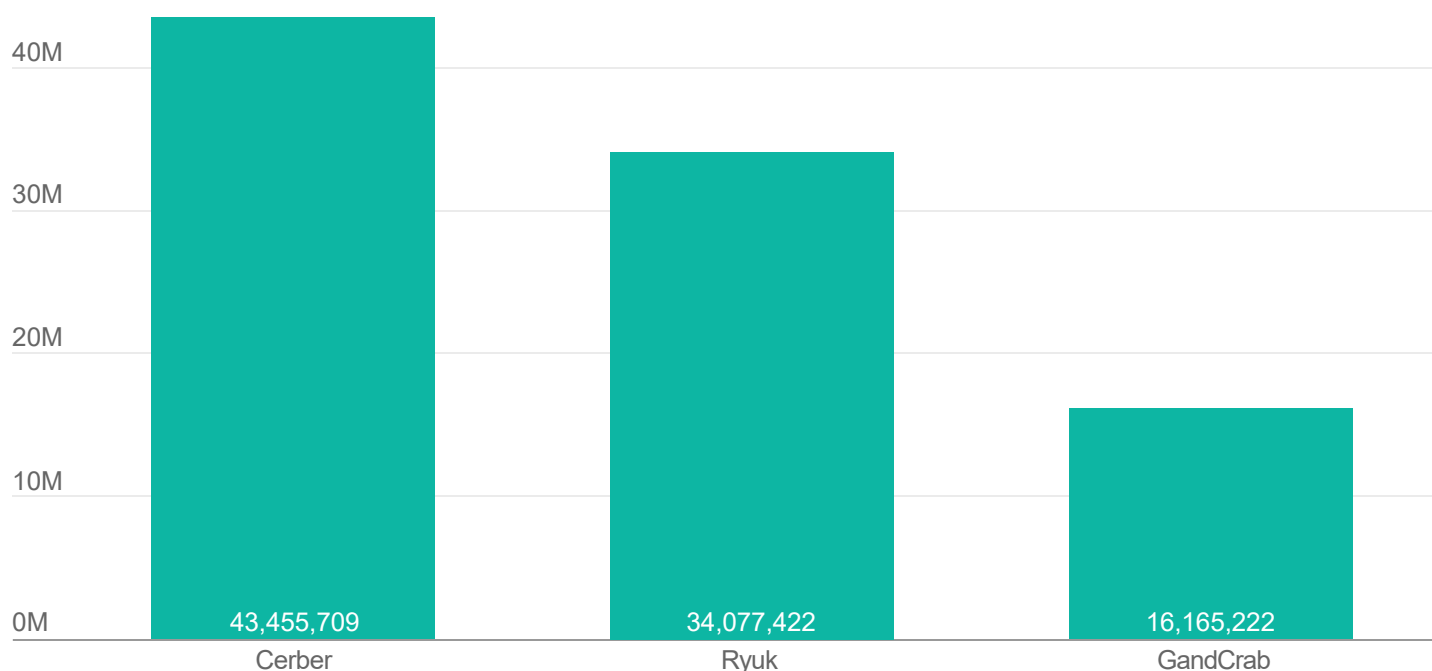
As for Ukraine itself? Even though SonicWall's sensor footprint there is too small to be statistically significant, it just barely missed making this year's list: It came in at No. 11.





The top ransomware families for the first half of 2022 were Cerber, Ryuk and ...GandCrab.

Top 3 Ransomware Families of 2022

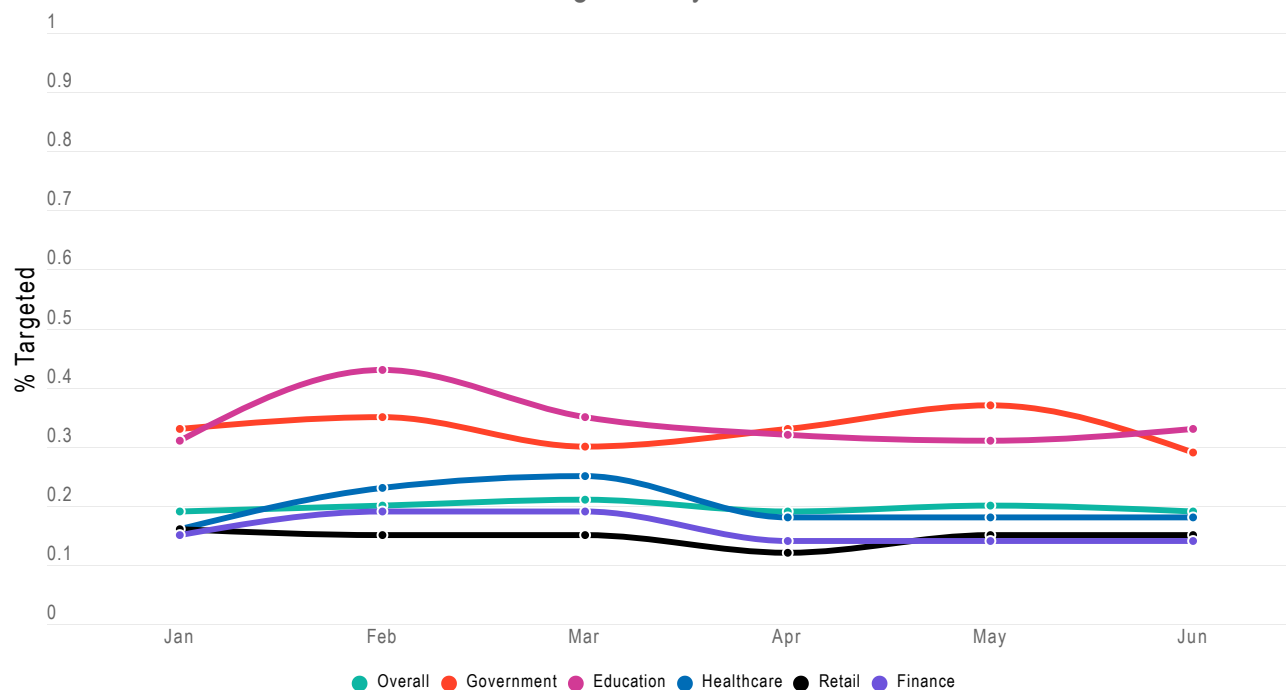


Rates of Ryuk fell dramatically in the first half of this year, pushing it into second place and allowing Cerber to reclaim the top spot. And with the volume for other ransomware families falling, GandCrab was able to move from fourth back into the top three.

This doesn't mean we're seeing some sort of GandCrab renaissance, however. While it's possible "GandCrab" has been rebranded or otherwise resurrected, it's more likely that what we're seeing is the remnants of old campaigns.

At the time GandCrab shut down in 2019, it accounted for roughly half of the global ransomware market. But as Gandcrab was a Ransomware as a Service (RaaS) offering, the shuttering of GandCrab HQ had no effect on automatic campaigns, many of which were never turned off — and many of which are still running today.

% of Customers Targeted by Ransomware in 2022



Ransomware by Industry

While *overall ransomware* might be down, the view for the industries SonicWall analyzed was much less rosy. In fact, there was only one bright spot — ransomware targeting government organizations dropped 84%.

Everyone else saw an increase: Education and retail rose 51% and 90% respectively, while finance and healthcare saw triple-digit increases of 243% and 328%.

But while ransomware continued to rise in the majority of industries examined, all of these industries saw their percentage of customers targeted year-to-date drop.

The Rise of Cross-Platform Ransomware

Throughout the first half of 2022, ransomware groups have continued to target large enterprises.

Because the networks of these enterprises are often complex, encompassing various types of hardware and operating systems, ransomware operators have begun writing their code in cross-platform languages.

This allows the code to easily be ported between Linux, iOS and Android — thus ensuring the ransomware can wreak maximum havoc by encrypting as many systems as possible. And as an added bonus, these languages can prove challenging to researchers.

As of the first half of 2022, Blackcat/ALPHV ransomware is written in the Rust language, and Babuk, Hive, HelloKitty and many others are currently written in Golang.

Log4j Update

Log4Shell Still Being Exploited

When the Log4j zero-day vulnerabilities were disclosed in December 2021, cybercriminals were quick to attack: Despite being the final major vulnerability identified in 2021, a CISA report from early January 2022 revealed it to be [the most exploited vulnerability](#) of the entire year.

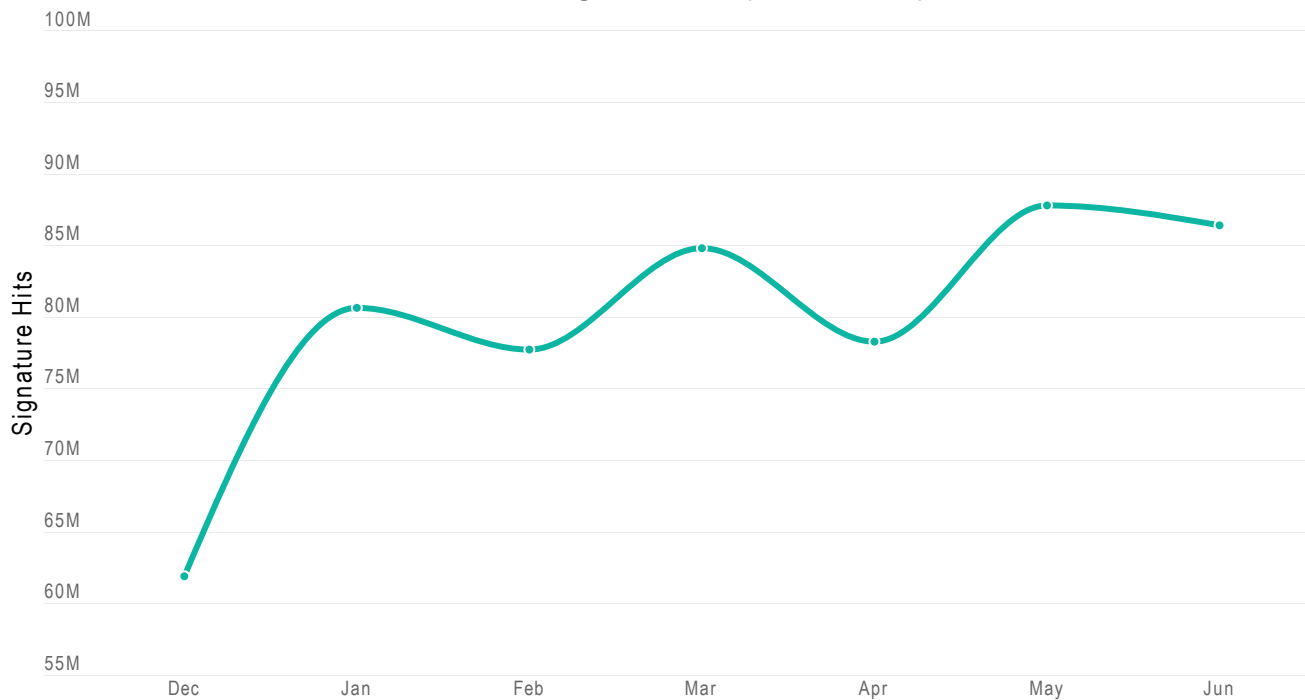
At the time, [CISA director Jen Easterly said](#) that the Log4j vulnerabilities were “one of the most serious I’ve seen in my entire career, if not the most serious.” And Jay Gazlay, also of CISA, reported that [hundreds of millions of endpoints](#) would likely be impacted.

What’s Happened Since Then

Between December 11, 2021, and June 30, 2022, SonicWall recorded 557.5 million Log4Shell exploit attempts, an average of 2.8 million each day.

While SonicWall Capture Labs threat researchers noted an already extraordinary number of attacks in December, the pace has only picked up since then. There were 252.5 million hits in Q1 and 243 million in Q2, and so far each month in 2022 has had more attempts than December 2021 saw.

Malicious Log4Shell Exploit Attempts



What's In Store for Log4j

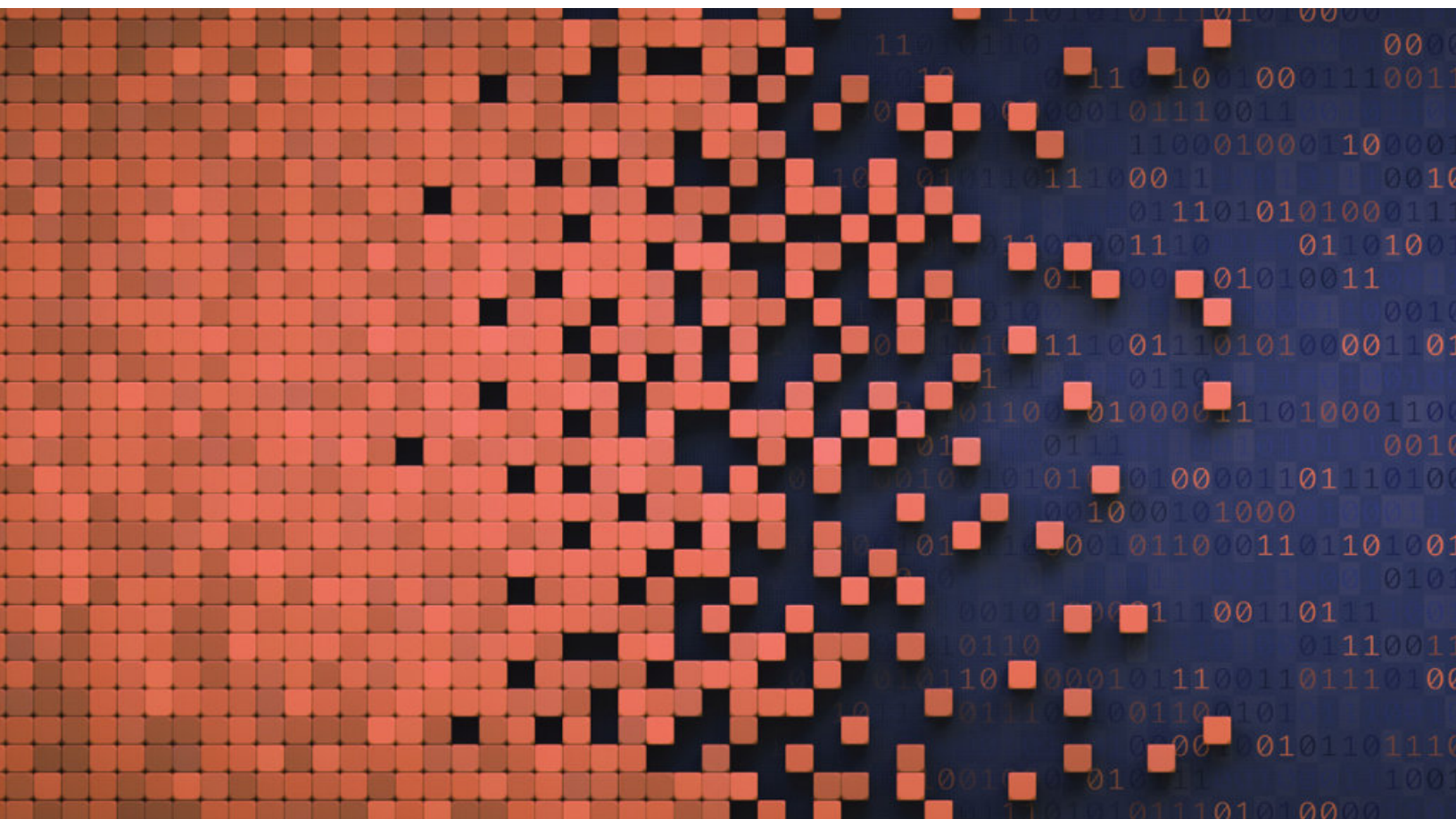
Based on current data, we may not see attack volumes fall, or even *peak*, any time soon. According to Dark Reading, more than 40% of the Log4j packages downloaded from early February to early March — months after fixed versions of the software became available — [were still vulnerable versions](#). Worse, many instances have remained vulnerable because organizations are simply unaware of them, and sometimes even [dependency analysts can't find them](#).

Despite a lack of [any "significant" attacks](#) on critical infrastructure thus far, the continued presence, distribution and exploitation of these vulnerabilities led the U.S. Cyber Safety Review Board to classify the vulnerability as "endemic" [in a report](#) released in July 2022.

Unfortunately, cybersecurity experts say these vulnerabilities will be exploited for years to come.

"Log4j is one of the most serious software vulnerabilities in history," Department of Homeland Security Undersecretary Rob Silvers [told reporters](#). "This event is not over."

Despite being the final major vulnerability identified in 2021, a CISAreport from early January 2022 revealed it to be the most exploited vulnerability of the entire year.



Capture ATP & RTDMI

RTDMI™ Detections Rise Dramatically

In the first half of 2022, the number of never-before-seen malware variants found by SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) rose 45% year-to-date, setting several new records in the process.

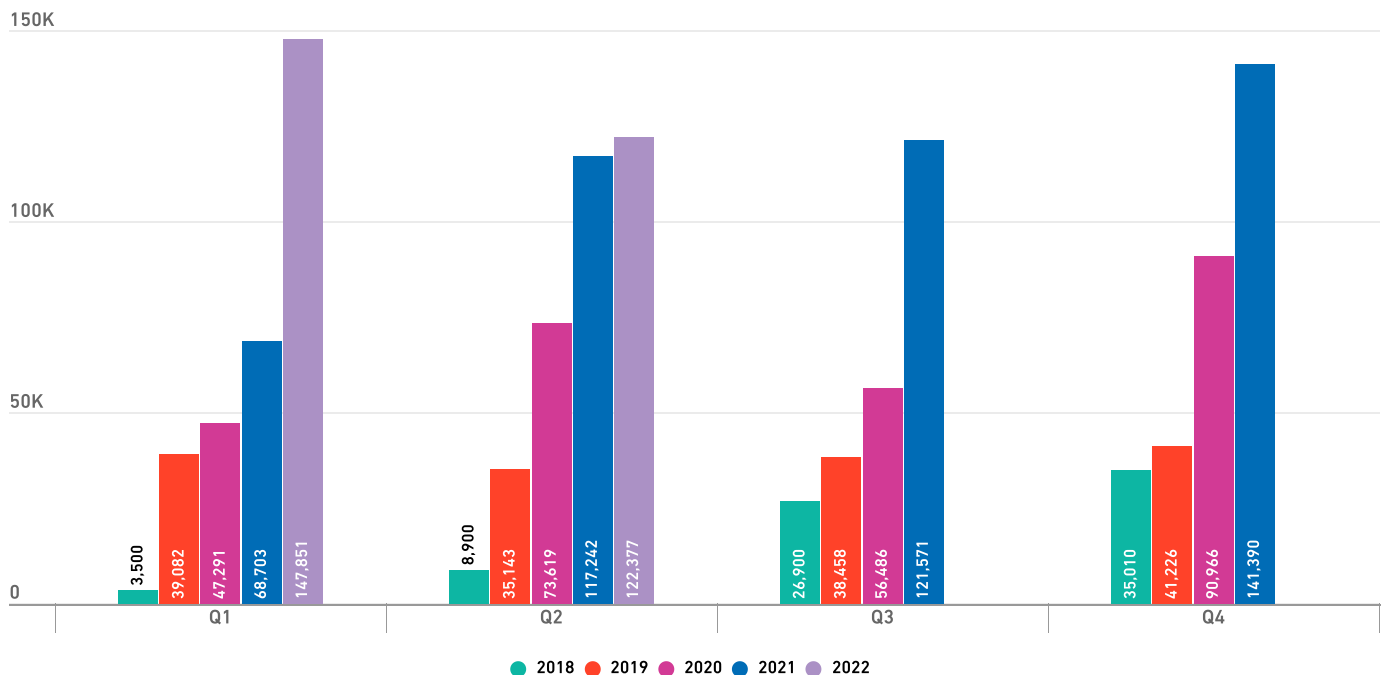
A total of 270,228 never-before-seen malware variants were detected in the first half of 2022, an average of 1,501 each day.

In March, RTDMI™ detected 59,259 new malware variants, the most ever identified in a single month.

Along with higher-than-average detections in January and February, this resulted in Q1 becoming the largest-ever quarter for new detections in RTDMI's history, with 147,851 never-before-seen variants.

SonicWall has now reported an increase in the number of variants discovered by RTDMI in 14 of the last 18 quarters. Taken cumulatively, this represents a dramatic evolution in the technology over time: Since it was introduced in early 2018, the number of new variants discovered has skyrocketed 2,079%.

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



An illustration in orange lines showing a folder with a magnifying glass over a warning sign (a triangle with an exclamation mark). Dotted lines connect the folder to four virus-like icons (circles with spikes) scattered around it.

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.

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.

24 | Mid-Year Update: 2022 SonicWall Cyber Threat Report | Capture ATP & RTDMI

Malicious PDF/Office Files

Malicious PDFs, Office Files on the Rise

In last year's mid-year update, SonicWall Capture Labs threat researchers noted a 54% drop in the number of malicious Office files, along with a 13% drop in the number of malicious PDFs.

Unfortunately, these drops seem to have been short-lived. In the first half of 2022, we saw malicious Office files rise 18% and malicious PDFs rise 9%, taking back a fair amount of the ground gained last year.

Combined with an unusual amount of volatility, these increases are pushing both threat types to rare heights. In March 2022, the number of new malicious Office files hit 12,471 — the highest point recorded since October 2020.

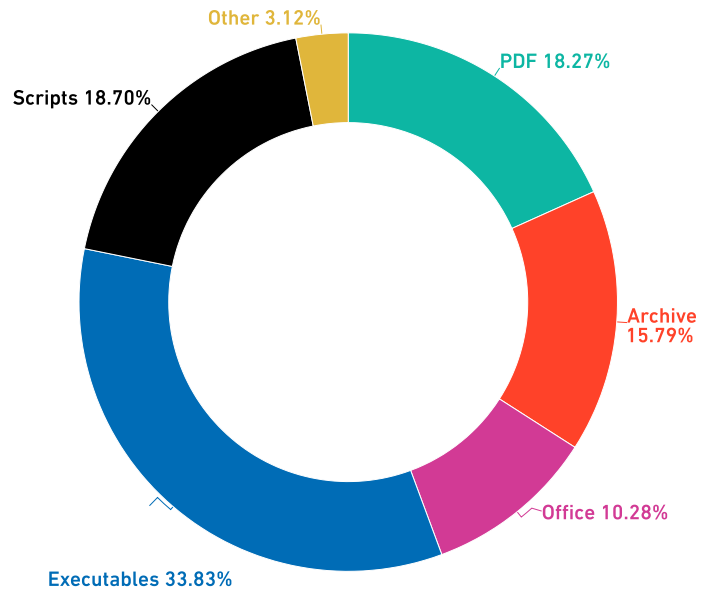
From April to May, the number of new malicious PDFs rose a staggering 486% to 27,127 — by far the highest level recorded by SonicWall.

PDFs now make up 18% of all new malicious filetypes, while Office files make up 10%. The largest share of new malicious file types, however, remains executables: During the first half of 2022, executables made up 34% of new malicious files — an appreciable increase over last year, when they represented 26.4% of malicious files.

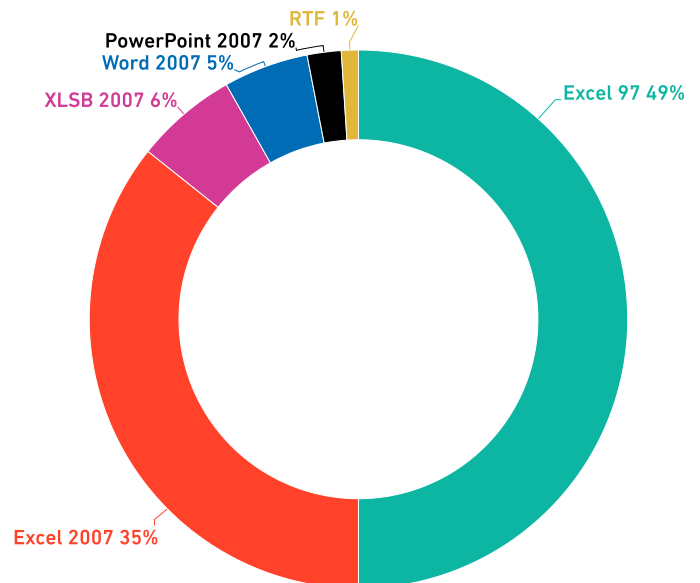
These increases were made possible by declining rates of both malicious scripts and archive files, which showed moderate drops over 2021.

Microsoft Excel files made up a majority of the malicious Office files observed.

2022 New Malicious File Type Detections | Capture ATP



2022 Malicious Office Files





New Developments in Malicious Files

In the first half of the year, researchers observed Emotet being distributed using malicious Microsoft Office files.

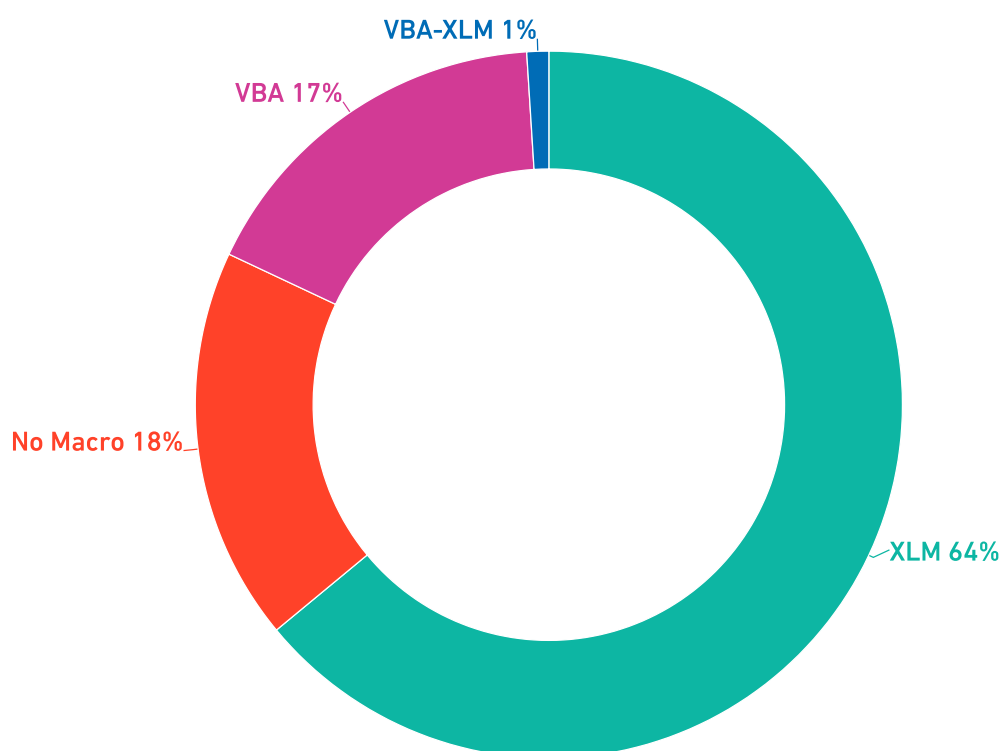
Threat actors have also been leveraging files with Excel Macro 4.0 (XLM), the predecessor of the current VBA programming structure, to install and execute payloads. XLM is popular among cybercriminals because XLM macro code utilizes formulas regularly used in normal Excel spreadsheets, making malicious patterns more difficult to detect. XML macros can also spread between sheets or be added during runtime.

In response to Microsoft's recent addition of a security warning for XLM macro, threat actors have begun developing samples that use both VBA and XML to perform malicious activity.

This is done by adding a malicious XLM macro sheet dynamically when the VBA is executed, causing control to pass from VBA to XLM, which then performs the malicious activity.

To date, XLM is still being used in a majority of malicious Office files.

2022 Malicious Excel Macros



Encrypted Attacks

Encrypted Threats Jump 132%

Encrypted attacks showed a 132% year-to-date increase from January to July, bringing attack volume to near-record highs.

While January started off unusually low at just 280,896 attacks, by May, attack volume had reached 1.5 million, making it second only to December 2021 for most malware over HTTPs SonicWall has recorded in a single month.

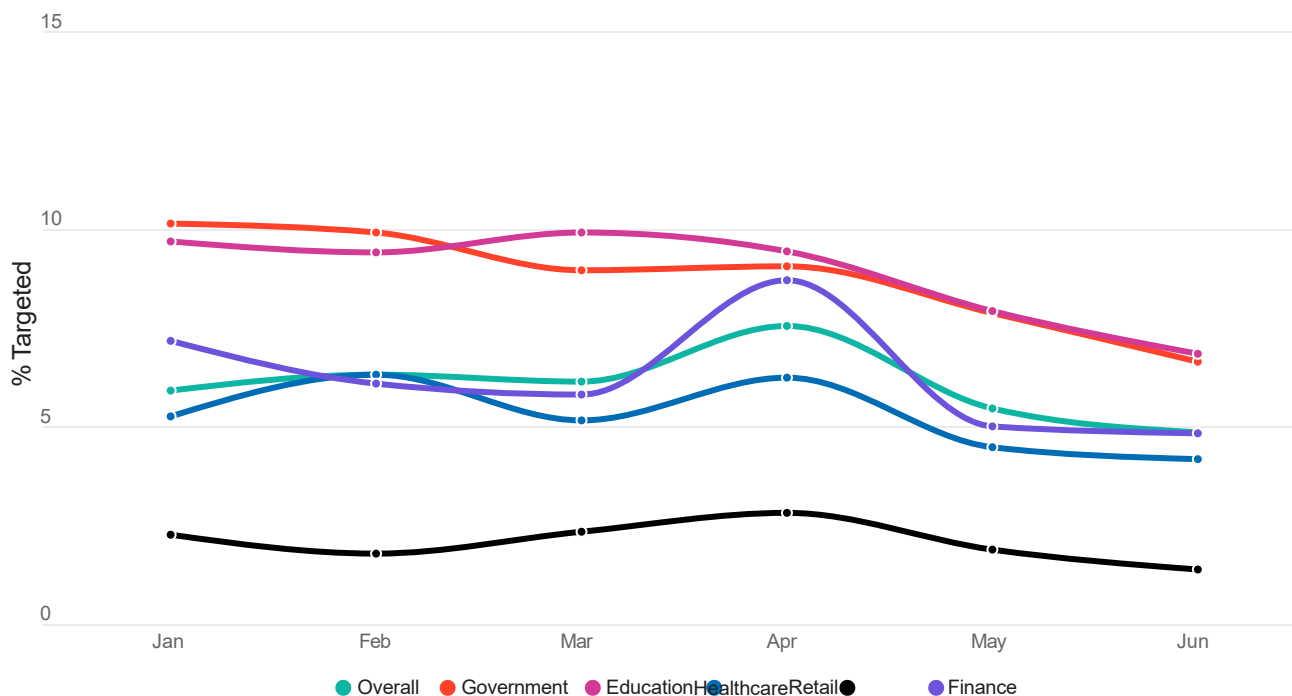
In North America, encrypted threats rose to 3.34 million, a 284% increase year-to-date. Much of this was due to May's massive spike, when monthly attack volume for the region hit 1.4 million.

To put this in perspective, North America saw more encrypted attacks in May than were recorded in the entire world in January, February, March or April — and more attacks than January, February, March and April of last year *combined*.

This is pushing attack volumes in North America, already the hardest hit, even higher: In the first half of 2021, encrypted threats there made up 41% of the global total. In the first six months of this year, that share rose to 68%.

While Europe showed a smaller increase of 75%, Q2 hit the region particularly hard. In April, attack volumes rose 247% over the previous month to reach their highest point since before 2019.

% of Customers Targeted by Malware over HTTPs in 2022



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



Encrypted Attacks by Industry

In the first half of 2022, industries saw wildly different trends. Healthcare and retail fared the best, with decreases of 6% and 79% respectively. But attack volumes rose in government (9%), finance (27%) and education (42%).

Education had the largest average percentage of customers targeted in the first half of 2021 at 8.9%, just exceeding the average 8.8% of government customers targeted. And as usual, the retail industry saw by far the lowest percentage of customers targeted, averaging just over 2% of customers targeted per month.

These numbers may be on their way down, however: In each of these industries, the percentage of customers targeted in Q2 was lower than in Q1 — meaning that while overall *volume* of attacks may be on the rise, at least fewer customers are being affected.

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 Up 77%

The first half of 2022 got off to a rough start: In January, IoT malware attacks had already doubled from the December immediately preceding it. Persistently high attack volumes over the next five months resulted in a total of 57 million IoT malware attacks in the first half of 2022 — a 77% increase year to date.

The first half of 2022 also saw a new record set — twice. January exceeded the previous monthly record of 10.8 million, set in October 2020, to become the month with the largest IoT malware volume SonicWall had ever recorded. Then, in June, attack volume rose even higher, to 12.9 million, setting yet another new monthly record.

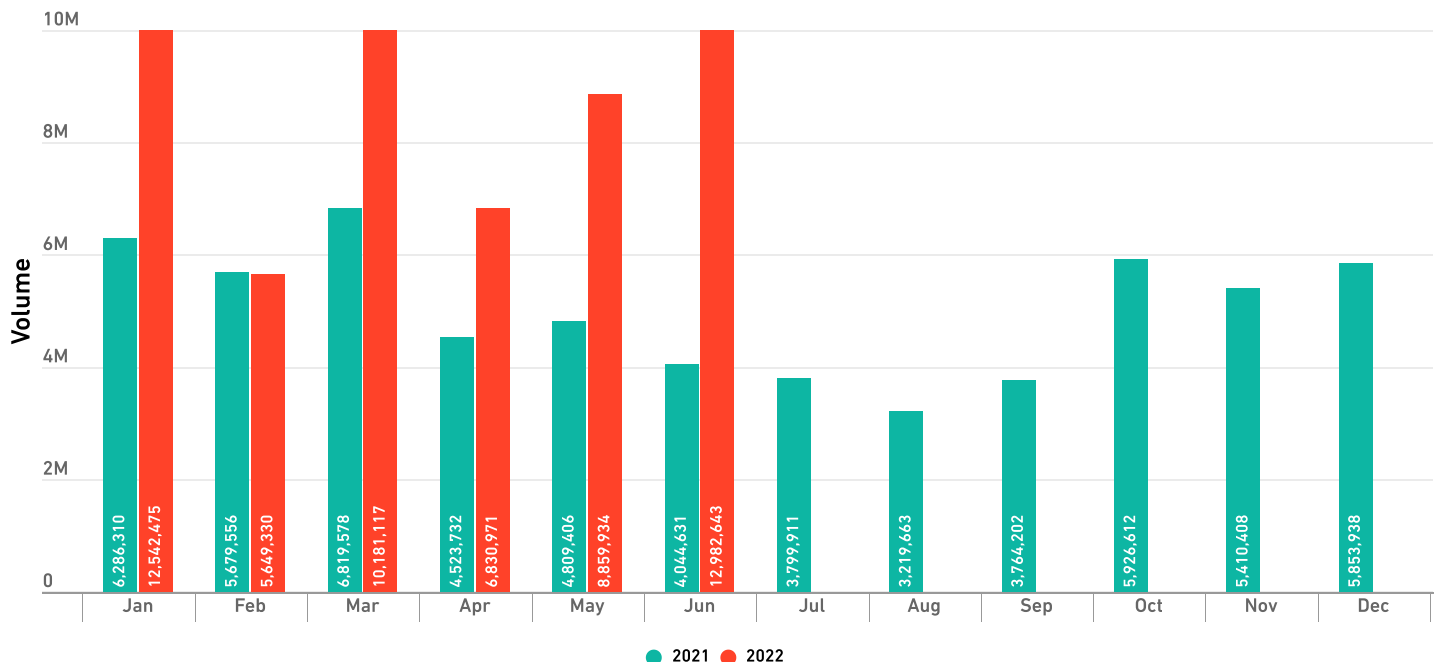
The quarterly trends echoed the monthly trends: After the first quarter became the new *worst* quarter at 28.4 million hits, Q2 2022 immediately surpassed it, reaching 28.7 million. Each quarter so far in 2022 has seen more IoT malware attacks than the *entire last half* of 2021.

In fact, IoT malware has increased so much in the first half of 2022 that we've already seen a higher attack volume than 2018, 2019 or 2020 recorded for the entire year. And while last year was itself a record-breaking year for IoT malware, by the end of June 2022 we're already 95% of the way to surpassing the full-year total for 2021.

IoT Malware by Region

The 77% increase in attack volumes represents a wide variety of outcomes. Despite passing the 2 million mark for the first time in January, Asia's 74% increase was slightly better than the global average. And in Europe IoT malware attacks actually *decreased* by 19%.

Global IoT Malware Volume



North America, however, had it much, much worse: IoT malware there skyrocketed 222% and set several new records of its own. In January, IoT malware attacks in North America surpassed 5 million for the first time ever, setting a new record at 6.7 million. It didn't last long, though — after remaining lower for the next four months, attack volumes increased dramatically in June, making 8.1 million the new high-water mark.

During the first half of 2021, IoT malware in North America made up 33% of global IoT malware volume. During the first half of 2022, that percentage rose to 59%. And with IoT malware ending on an upward trajectory both globally and for North America specifically, this makes for an inauspicious start to the second half of the year.

The U.S. and U.K. saw similar patterns. After starting at a new record high in January, IoT malware in the United States peaked even higher in June, setting a new record at 7.7 million and bringing the U.S.'s total IoT malware volume for the half to 30.8 million — a 228% increase year-to-date.

Attacks in the U.K. started out strong in January, before rising even higher in March ... then May ... then June. June's attack volume of 508,039 earned the U.K. its own new record, and this dubious distinction helped push volume for the first half to 2.6 million — a 134% increase from the same time period last year.

IoT Malware by Industry

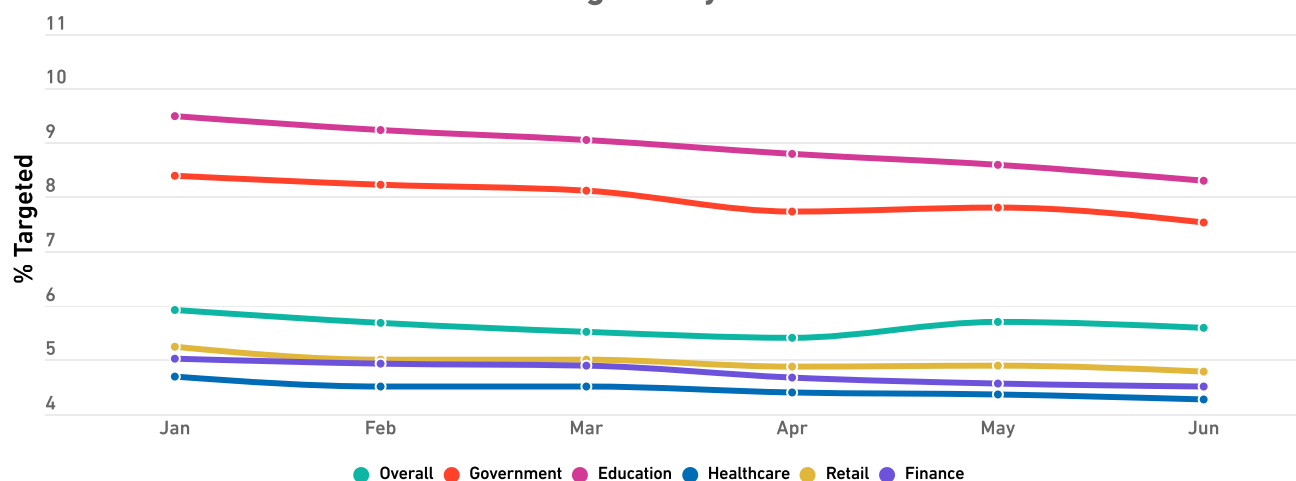
Unlike with the regional data, there were no bright spots in the industry-specific IoT malware counts: *Every industry we analyzed showed triple-digit attack volume increases.* Finance got the worst of it, with a 151% increase in IoT malware volume, followed by healthcare (up 123%), retail (up 122%), government (up 114%) and education (up 110%).

That doesn't mean there isn't any good news, however: Surprisingly, these massive increases don't seem to have resulted in corresponding jumps in the percentage of customers targeted. In fact, the opposite has happened: across every industry examined, the percentage of customers targeted in the first half of 2022 actually *fell* compared with the first half of 2021.

Education, which has consistently seen more IoT malware than any other industry, saw the biggest drop: During the first half of 2022, the average percentage of education customers targeted was 8.91%, down from 11.33% during the first half of last year. While this drop is good for education as a whole, given the massive increase in the amount of IoT malware targeting education customers, those who *are* being targeted can expect to see even more IoT malware attempts than before

One other small bit of good news: For education, along with every other industry, January had the highest percentage of customers targeted, and June had the fewest. If this trend continues, we'll probably see the percentage of customers targeted each month continue to drop as we head into 2022's second half.

% of Customers Targeted by IoT Malware in 2022



Cryptojacking

Cryptojacking Reaches Record High

Despite a precipitous drop in the price of cryptocurrency, global cryptojacking volume rose to 66.7 million in the first half of 2022, up 30% over the first half of 2021.

While such an increase is obviously concerning, it's a lot better than it looked from the outset. In January, cryptojacking volume reached 18.4 million. This represented a new monthly high, exceeding the previous record — 15.49 million, set in March 2020 — by nearly 3 million hits.

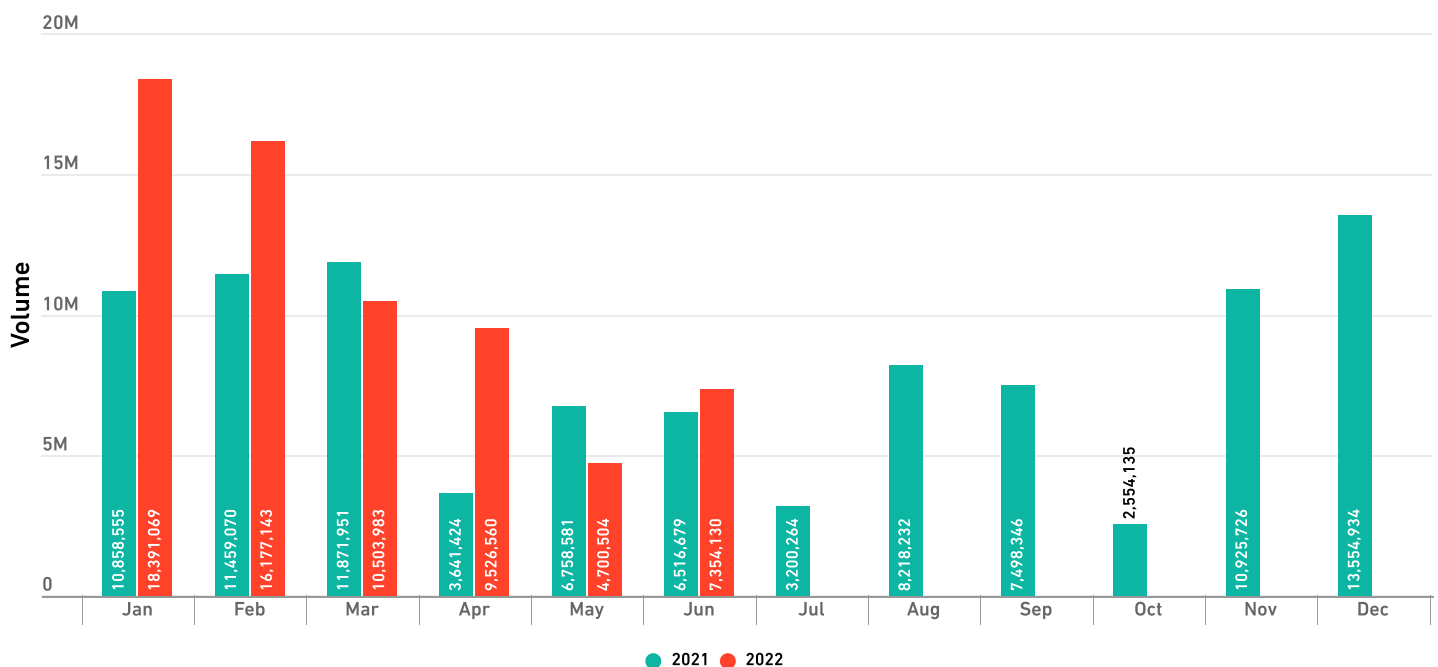
Fortunately, it proved to be all downhill from there, and this sustained drop resulted in two very uneven quarters. Bolstered by January's spike, SonicWall recorded 45.1 million attacks in Q1, the most ever observed in a single quarter.

But by April, cryptojacking was already down by half from its peak, and in May it was even lower, resulting in a second-quarter attack volume of just 21.6 million, less than half the amount seen in the preceding three months.

While falling cryptocurrency prices may have a lot to do with this, keep in mind that what we're seeing follows a well-established pattern. Every year since SonicWall began tracking cryptojacking, researchers have recorded significantly higher cryptojacking volumes in Q1 than in Q2, resulting in the "cryptojacking summer slump." If prior years are any indication, volumes will remain lower in Q3, only to peak again in Q4.



Global Cryptojacking Volume



Cryptojacking by Industry

While overall cryptojacking increased, the three industries typically most affected — government, healthcare and education — saw attack volumes *drop* 78%, 87% and 96% respectively. This represents a long-awaited reprieve for education customers, who have gone from seeing the most cryptojacking of any industry on our list, to seeing the least.

In contrast, cryptojacking targeting the retail industry increased 63% year-to-date, while attacks on the financial industry skyrocketed 269%. This represents a dramatic reshuffling: Previously near the bottom, finance customers now experience significantly more cryptojacking than any other industry we examined. In fact, the number of attacks on the finance industry is *five times greater* than the second-highest industry — retail, which used to be at the very bottom of the list.

There were some trends that benefitted all industries, however. In every case, the average percentage of customers targeted by cryptojacking in the first half of 2022 was down over the same period in 2021. And every industry saw a Q2 with fewer customers targeted than Q1, and a June that ended in a better place than January started.

Cryptojacking targeting the retail industry increased 63% year-to-date, while attacks on the financial industry skyrocketed 269%.

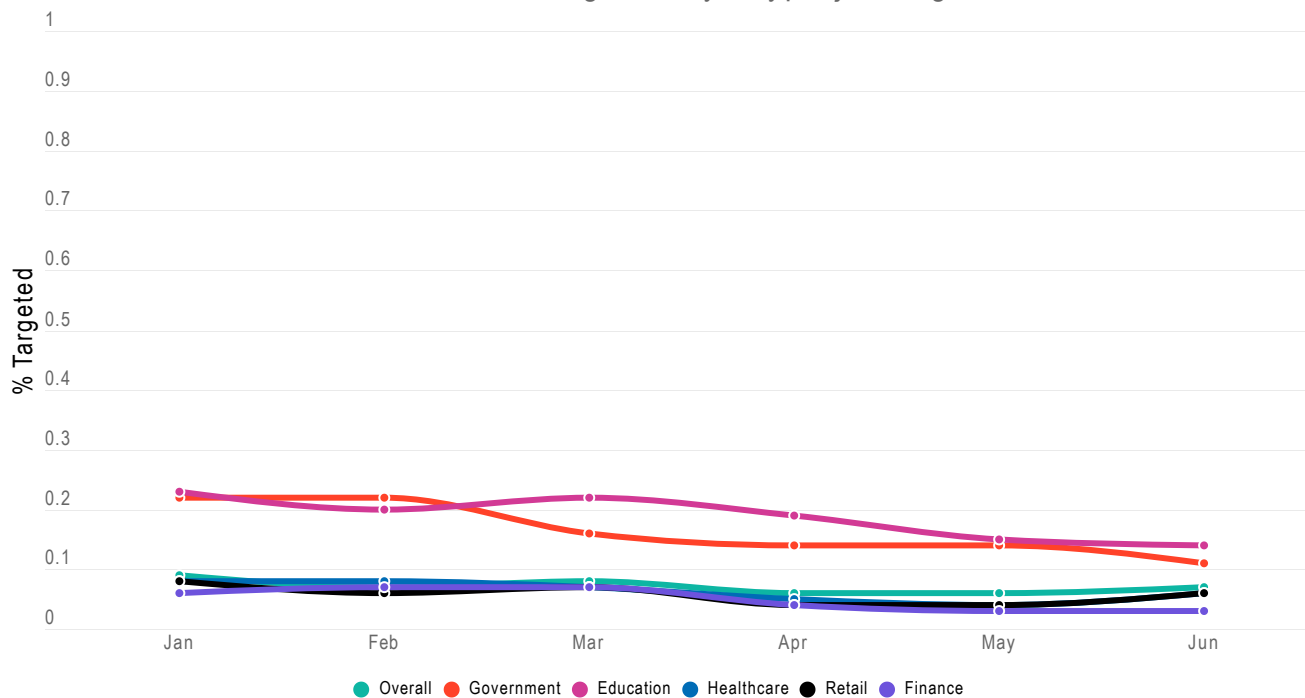
Cryptocurrency Crumbles

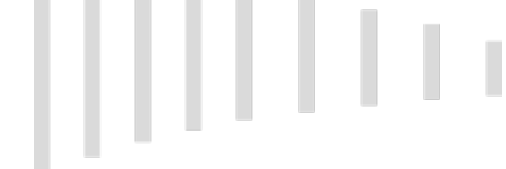
If you had a Bitcoin last November, the world was yours. The price had risen to an all-time high of \$68,990 — enough to purchase a 2021 Porsche 718 Cayman or a Jaguar F-Type, or for a standard down payment on the average house in most states.

That is, if you were lucky enough to sell.

Those who weren't would see a dramatic reversal of fortunes, as prices in June fell to less than a third of that value, [bottoming out at \\$17,601.58](#).

% of Customers Targeted by Cryptojacking in 2022





In other words, that same Bitcoin would barely buy you a sub-compact economy car by mid-year 2022 (and that's assuming you didn't want to pay for any bells and whistles ... such as tag, tax or title.)

So what happened to Bitcoin? In short, the same thing that happened to stocks and other risky assets: [Macroeconomic uncertainty](#). With inflation at historic highs, interest rates and living costs on the rise and the specter of recession looming over the year, middle-class investors have less to spend in general — and wealthier investors and corporations, fearing the worst is yet to come, are choosing to play it safe.

As a result, Bitcoin and others tumbled, two coins collapsed altogether, crypto exchange Binance paused withdrawals, crypto lenders Celsius and Voyager Digital filed for bankruptcy, and Coinbase laid off nearly 20% of its workforce. When people heard about this, they panicked and sold off more coin, pushing prices down even further.

Why Cryptojacking is Growing

Changing careers is tough, and this goes for cybercriminals, too. When the price of coin drops like a rock, it's still easier to hustle harder than it is to find a new line of work. And for many, leveraging the Log4j vulnerability and deploying attacks in the cloud are presenting newer and more lucrative opportunities.

But there's something else that might be bolstering cryptojacking levels: ransomware operators.

After governments stepped up ransomware awareness and enforcement efforts, and ransomware attacks such as those against Colonial Pipeline and Kaseya led to high-profile busts, some ransomware operators have decided they're ready for a quieter life.

Unlike ransomware, which announces its presence and relies heavily on communication with victims, cryptojacking can succeed without the victim ever being aware of it. And for some cybercriminals feeling the heat, the lower risk is worth sacrificing a potentially higher payday.

"It 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](#).

At least one ransomware gang [has publicly announced](#) its intentions to shift to cryptojacking so far, and as long as there's still lower-risk money to be made, others could still follow. If they do, it [won't be the first time](#) cryptojacking has made inroads on ransomware.

The Consequence of China's Coin Ban: Dirtier Crypto

When the Chinese government banned cryptocurrency mining in 2021, it [cited concerns](#) about mining's effect on the environment. Mining generates a lot of waste and requires a tremendous amount of energy — more than [many countries](#). But paradoxically, in the aftermath of the ban, crypto mining appears to have gotten even dirtier.

When the ban went into effect, crypto miners didn't stop mining, they just moved elsewhere — many to places like Kazakhstan and the United States. In so doing, they no longer had access to China's plentiful and renewable hydroelectric power, and now rely on much dirtier energy produced with natural gas and coal.

For example, Bitcoin, which got an average of 42% of its power from [renewable sources](#) in 2020, was only able to get a quarter of its energy from renewable sources in August 2021. Carbon emissions from all cryptomining activities are estimated to have risen [by 17%](#) since the ban went into effect, alarming scientists and environmentalists alike — especially now that cryptomining operations have taken to purchasing their own [personal coal and gas plants](#).

Intrusion Attempts

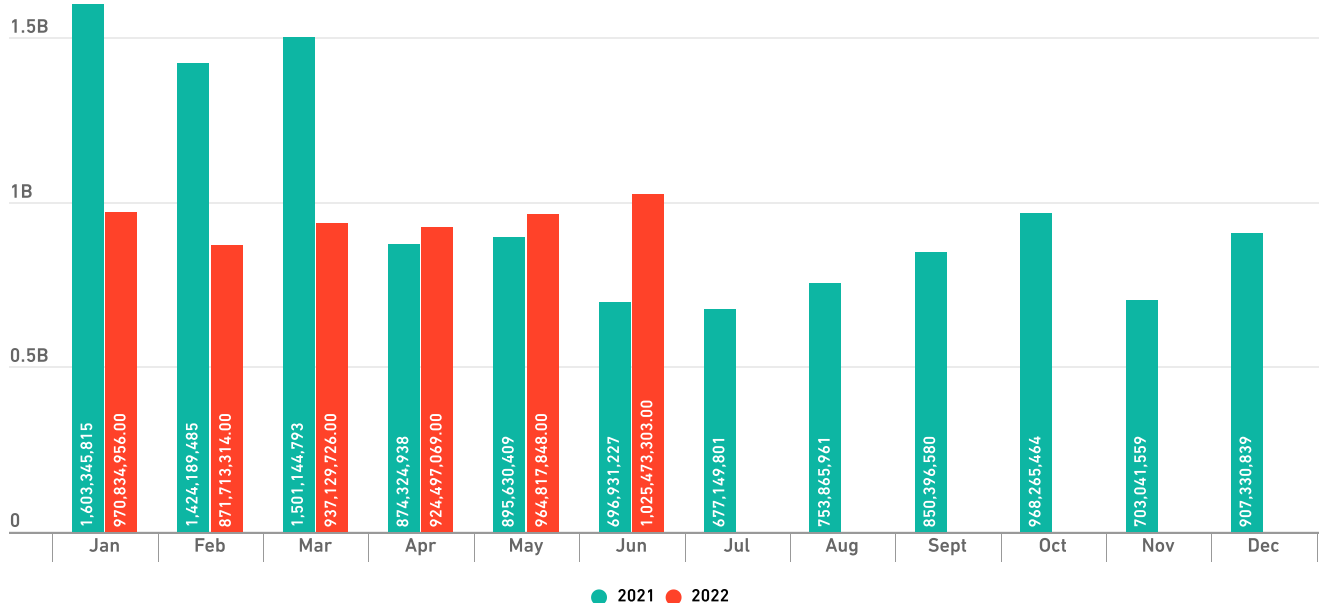
Malicious Intrusion Attempts Fall Nearly 20%

While intrusion attempts in general rose 18% in the first half of 2022, the number of malicious intrusions (those of medium and high severity) actually dropped, falling 19% over the same period in 2021 to 5.7 billion.

Compared with January 2021, January 2022 brought a much lower attack volume. Malicious intrusion attempts then stayed even lower until June, when they passed the 1 billion mark for the first time in over a year to peak at 1.03 billion attacks.

The number of malicious intrusions (those of medium and high severity) dropped, falling 19% over the same period in 2021 to 5.7 billion.

Global Intrusion Attempts



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

Intrusion Attempts by Region

Despite the overall downward movement in malicious intrusion attempts, both North America and Asia recorded increases. In Asia, attacks trended in the opposite direction as everywhere else, peaking in January at 161.1 million attempts. From this high point, attacks fell throughout most of the first half to bottom out in June, which saw 66.3 million attempts. In spite of this drop, malicious intrusions increased 13% year-to-date in Asia.

Things looked a bit better in North America. Attacks there peaked in June at 608 million, the highest since January 2021 — but lower volumes preceding this peak limited the year-to-date increase there to just 2%.

It was Europe that saw the largest drop, however. Despite ending the first half of 2022 at a peak of 288.2 million, the highest intrusion attempt volume seen in 14 months, malicious intrusion attempt volume remained low enough to result in a 52% decrease from the first half of 2021.

Intrusion Attempts by Industry

Despite an overall decrease in the number of malicious intrusion attempts, most industries actually saw an increase in attack volume. Healthcare, government, finance and retail saw spikes of 39%, 46%, 94% and 200%, respectively. The sole exception was education, which saw an 11% decrease in malicious intrusions.

But regardless of these increases, however, the average percentage of customers targeted in every industry was lower in the first half of 2022 than it was in 2021 — and that percentage continued to go down as the first half of 2022 went on. Even so, in any given month, you could still expect to see over a third of the customers in each industry targeted by an intrusion attempt.

The industry that experienced the highest average percentage of customers targeted so far in 2022 was healthcare. Interestingly, this is the only threat type we examined in which healthcare had the highest percentage of customers targeted.



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.

Attacks on Non-Standard Ports

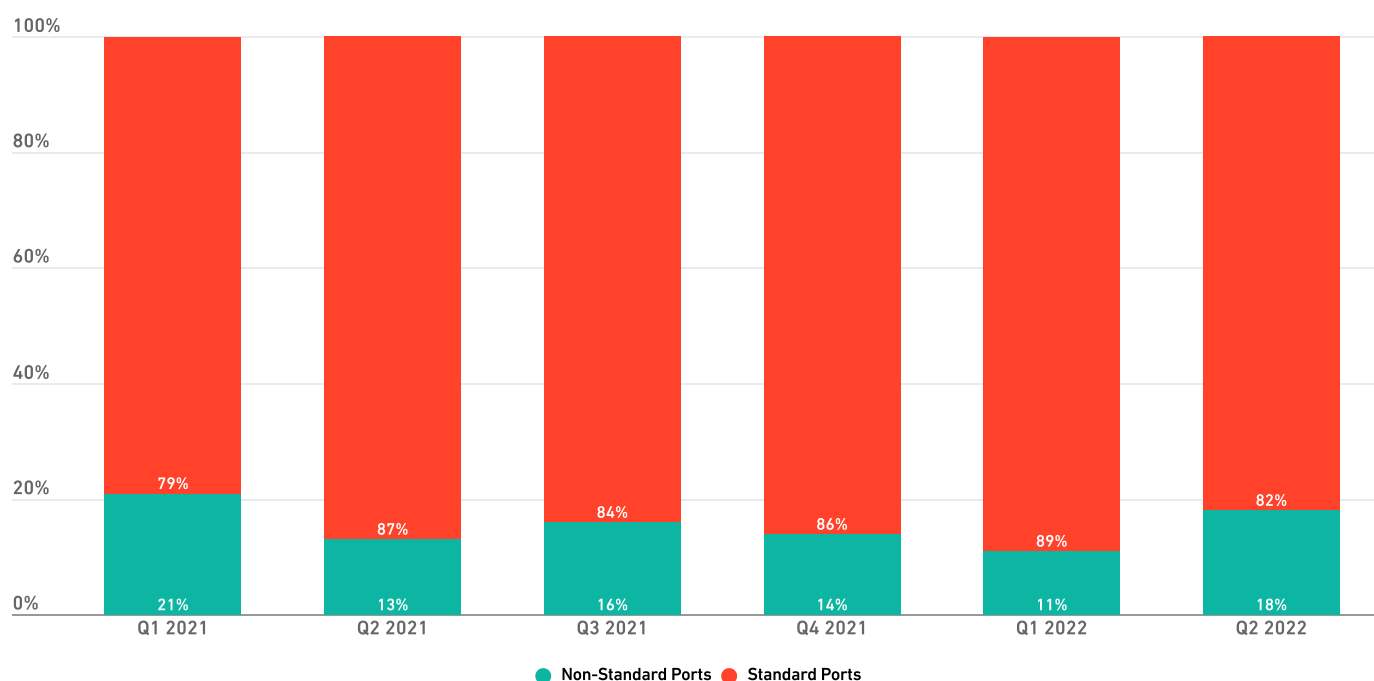
Non-Standard Port Attacks Remain Steady

The beginning of 2022 brought a welcome drop in non-standard port attacks. In January, the percentage of malware attacks over non-standard ports sank to 11% and stayed there the entire quarter, resulting in Q1 having the lowest average percentage of non-standard port attacks since Q4 2019.

This trend would prove to be short-lived, however. Malware traffic over non-standard ports shot up dramatically in April and rose even higher in May, making up the largest share of total attacks recorded in 15 months.

In January, the percentage of attacks over non-standard ports sank to 11% and stayed there the entire quarter, resulting in Q1 having the lowest average percentage of non-standard port attacks since Q4 2019.

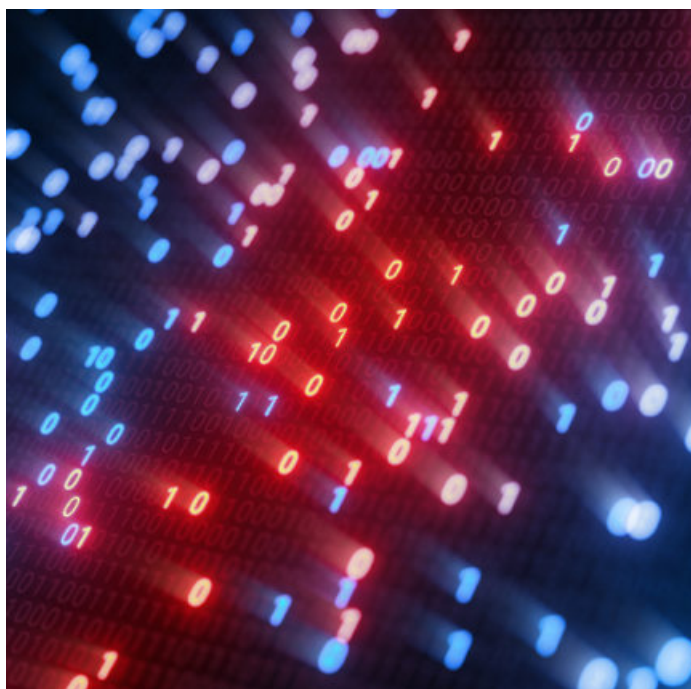
2021-22 Global Malware Attacks



When averaged with the unusual lows recorded in the first quarter, the peaks seen in Q2 brought us right back to the average yearly percentages we saw in 2021: 85% of malware sent across standard ports, 15% of malware sent across non-standard ports.

But non-standard port attacks follow established cadences not seen in other attack types. In 2019 and 2021, there were more attacks via non-standard ports in the first half of the year than the last half. In 2018 and 2020, we saw the opposite. If this holds, we'll see non-standard port attacks rise in the second half, resulting in a higher percentage of non-standard port attacks in 2022 than in 2021.

And based on the other pattern these attacks follow — namely, that non-standard port attacks rise in even numbered years and fall in odd years — this would put us on track to be exactly where we would expect to be.



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.

About the SonicWall Capture Labs Threat Network

Intelligence for the mid-year update to the 2022 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

© 2022 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.

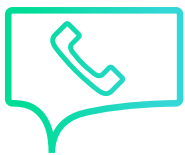
2022-MidYearThreatReport-JK-6641



Their Words, Not Ours

"The key to having a great service provider is that you become part of each other's business family. The collaboration should be mutual. Marlin have totally achieved this – they are approachable, helpful and provide the right solutions."

Group Projects Manager, Time Finance



Voice



Video



Connectivity



Security



Mobile

Get In Touch

For more information and to book a free discovery call with one of our experts, contact us.