SONICWALL®

2021 MID-YEAR UPDATE

SONICWALL CYBER THREAT REPORT

Cyber threat intelligence for navigating today's business reality

sonicwall.com | @sonicwall

Table of Contents

A Note From Bill 3

2021 Global Cyberattack Trends 4

Ransomware Continues its Record-Shattering Run 5

Top Three Ransomware Strains 13

Malware Falls by Nearly a Quarter 16

RTDMI™ Reaches New Heights 19

Malicious PDF and Office Files on the Decline 21

IoT Attacks Jump 59% 22

Cryptojacking Continues to Climb 24

Attacks Against Non-Standard Ports Fall 26

Your New Research Destination: The SonicWall Capture Labs Portal 27

About the SonicWall Capture Labs Threat Network 28

About SonicWall 29

A Note From Bill

In the past 15 months, the world has endured an unprecedented degree of change. As the disruption of a global pandemic impacted everything from the highest levels of federal government down to the way kindergartners learned to read, cybercriminals seized upon the changing environment to institute the "new business normal" *they* wanted.

And halfway into 2021, cybercriminals are impacting businesses worldwide. High-profile attacks on Colonial Pipeline, JBS Foods, Kaseya and hospitals worldwide have proven once and for all that these criminals aren't just *willing* to conduct attacks that have the potential to disrupt our entire way of life — they actively seek to do so.

But in response, the world's defenders, including cybersecurity professionals, law enforcement officials and the judiciary, have been doing plenty disrupting of their own.

In January, European and North American law enforcement worked together to deliver a severe blow to Emotet, and a disruption of NetWalker ransomware by the U.S. and Canada followed soon after. Members of Cl0p, Egregor and the operation formerly known as GandCrab were arrested.

After the Colonial Pipeline attack, the DarkSide group hastily issued a *mea culpa* before announcing that it was closing up shop and releasing their decryption tools.

And for reasons still unknown, REvil — one of the world's most powerful, prolific and ruthless ransomware groups — seems to have simply vanished, with rumors suggesting that pressure from one or more heads of state may have played a role.

At the same time, cybersecurity vendors have been introducing new products, tools and technology that will allow them to keep the upper hand in the escalating cybercrime arms race.

Backed by its 30 years of cybersecurity expertise, SonicWall has spent the past two years completely refreshing its product portfolio, introducing solutions that are already being widely recognized by third-party testing and reporting agencies.

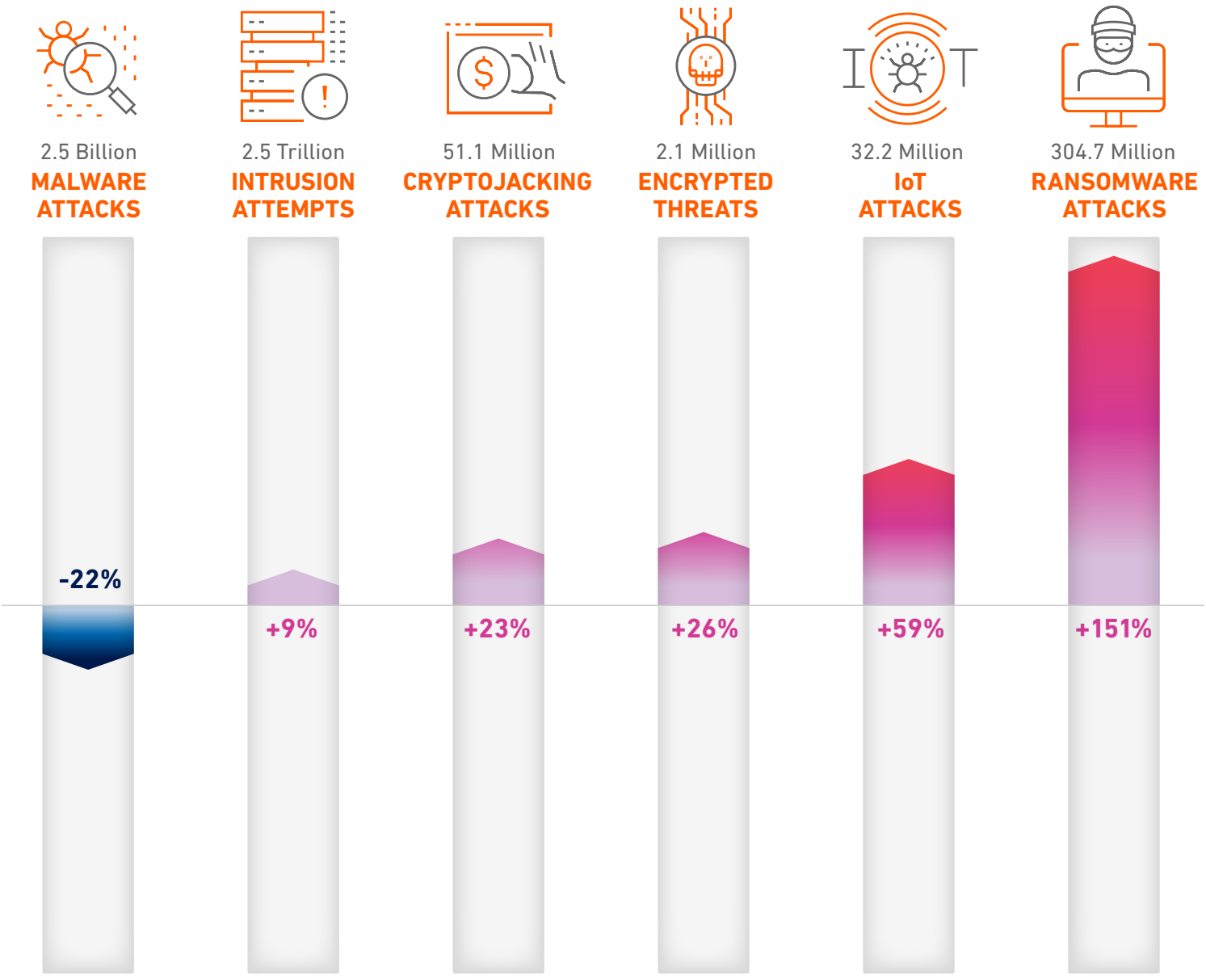
Three factors are essential in ensuring organizations can continue to withstand the rising tide of cybercrime: Unified Visibility and Control, the ability to Know the Unknown, and Disruptive Economics. These form the pillars of SonicWall's Boundless Cybersecurity approach, which has shown great success in protecting organizations worldwide.

The tools needed to maintain a proactive cybersecurity posture and prevent widespread disruption are already at our disposal. But it's crucial going forward that organizations move toward a modern Boundless Cybersecurity approach to protect against both known and unknown threats, particularly when everyone is more remote, more mobile and less secure than ever.

Meanwhile, SonicWall will continue doing everything we can to ensure you have visibility into the nature of the threats you face and the tools you need to defend your organization.

BILL CONNER
PRESIDENT & CEO
SONICWALL

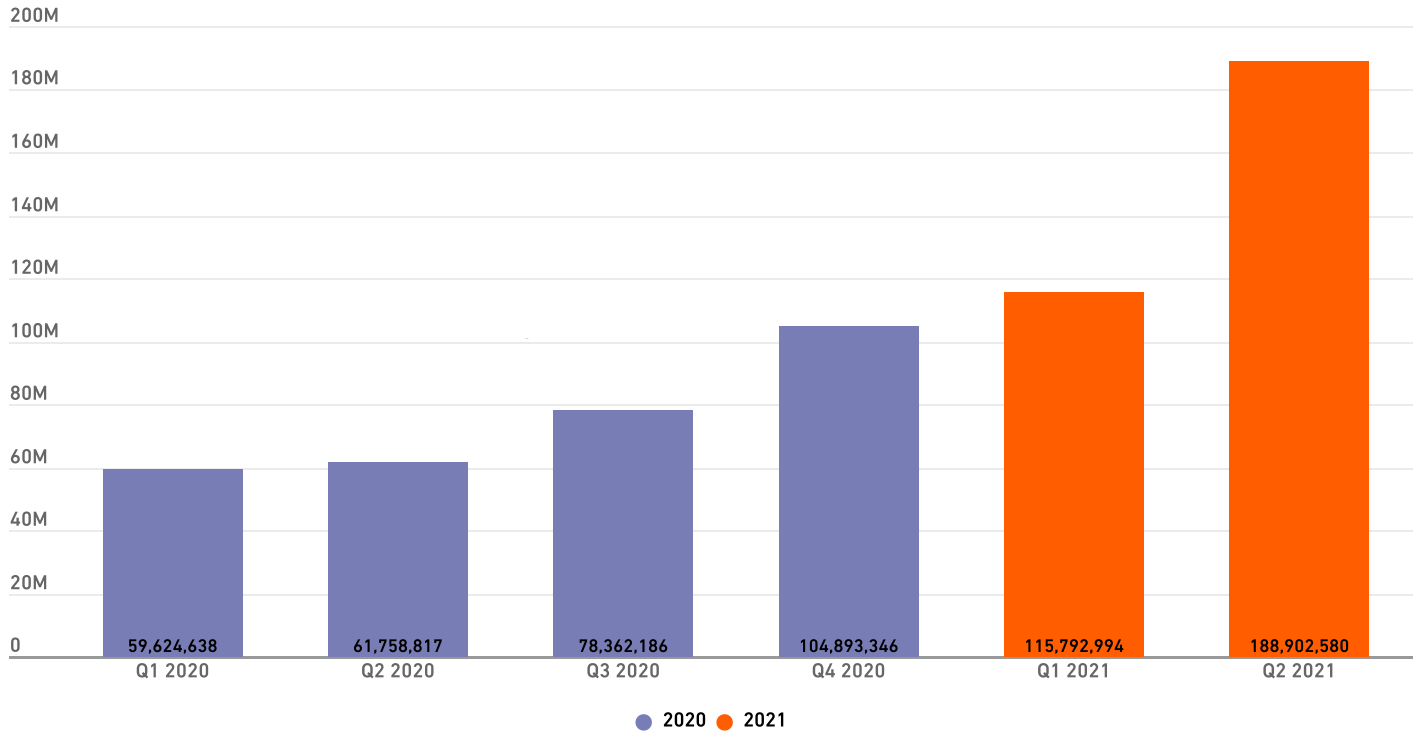
2021 Global Cyberattack Trends



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.

Ransomware Continues its Record-Shattering Run

RANSOMWARE GROWTH BY QUARTER



Q2 2021 was the worst quarter for ransomware since SonicWall began keeping records — and it isn't even close.

In the first six months of 2021, global ransomware volume reached an unprecedented **304.7 million** attempted attacks — already eclipsing the 304.6 million ransomware attempts logged for the entirety of 2020, as recorded by SonicWall Capture Labs.

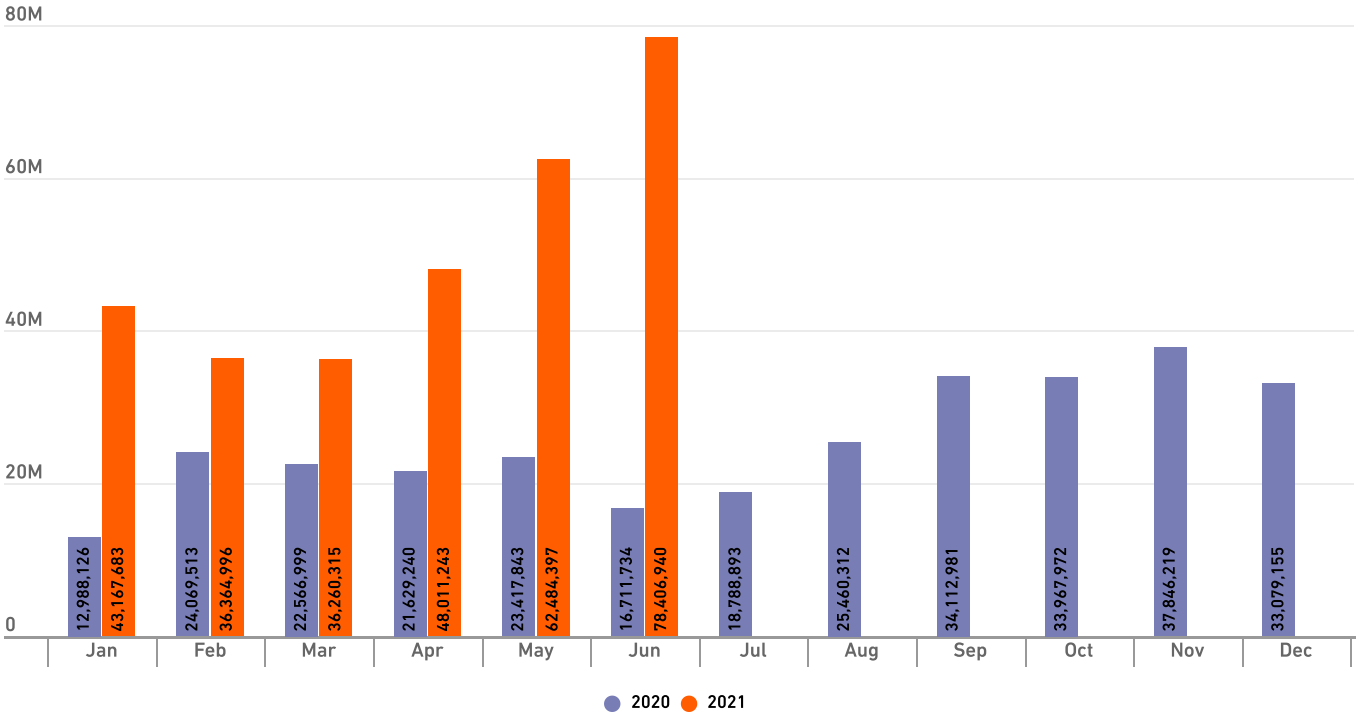
In all, ransomware for the first half of this year is up a staggering 151% over the same time period in 2020.

While Q1 was worrying, Q2 was markedly worse — going into spring, ransomware jumped from 115.8 million to 188.9 million, enough to make Q2 the worst quarter for ransomware SonicWall has ever recorded.

If we're lucky, this will be an aberration. Some years, such as 2019, see ransomware totals high in the first half, then fall off during the second half.

Even if we don't record a single ransomware attempt in the entire second half (which is irrationally optimistic), 2021 will already go down as the worst year for ransomware SonicWall has ever recorded.

GLOBAL RANSOMWARE VOLUME



The month-by-month ransomware data gives a much more nuanced view.

But even if we don't record a single ransomware attempt in the entire second half (which is irrationally optimistic), 2021 will already go down as the worst year for ransomware SonicWall has ever recorded.

While Q2 was record-setting in its own right, every month during the quarter set a new record, too. After rising to a new high in April, ransomware rose again in May, then saw another increase in June. During that month, SonicWall recorded 78.4 million ransomware attempts — more than the entire second quarter of 2020, and nearly half the total number of attacks for the *year* in 2019.

Even 2021's lowest month didn't provide much of a reprieve. With 36.3 million ransomware hits, March 2021 had more ransomware than all but one month in 2020.

Why is Ransomware Rising?

There are several factors behind the recent increase in ransomware, but the fact remains: The more organizations there are that are forced to pay out, the more incentive ransomware groups have to launch attacks.

CYBERINSURANCE

Some organizations are choosing to obtain cyberinsurance, which is intended to shield the purchaser from the effects of cyberattacks. But as these policies generally cover the payment of ransoms, policyholders faced with a ransomware attack are able to pay the ransom and obtain decryption while still avoiding the risk and hardship that comes with making a huge, unexpected payment to criminals.

While this can seem beneficial for insurers, victims and ransomware operators in the short term, this strategy isn't sustainable. Faced with victims forced to pay what's demanded of them, cybercriminals have continued making bigger and bigger demands — and if this trend persists, the losses will eventually become unsustainable for insurance companies.

It also isn't sustainable for victims, who, as we detail on the following pages, are often at greater risk after an attack simply because they've shown willingness to pay. For cybercriminals, however, this model will continue

While ransomware operators are getting better at finding and encrypting backups, they've also found another way to ensure victims pay up despite the existence of current backups: extortion.

to pay off for as long as it exists, giving them no reason to change course.

DOUBLE OR NOTHING

There's another reason ransomware operators may be launching more attacks: Shifting techniques have made it much more likely that doing so will pay off. There are two ways cybercriminals are making more on ransomware now than in the past: double extortion and repeat attacks.

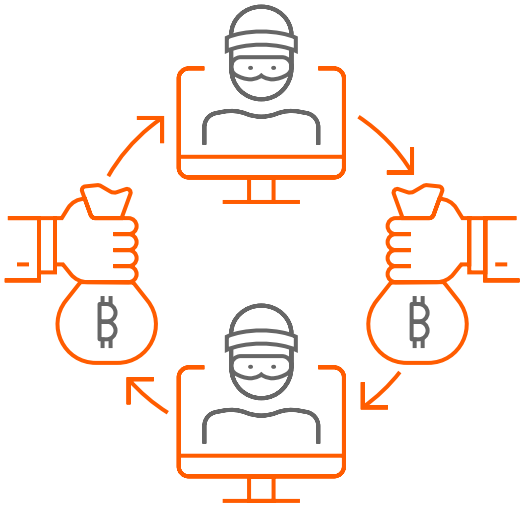
In the past, ransoms were primarily paid to ensure the ability to recover or decrypt data. Victims paid attackers the agreed-upon amount, and the attacker (usually) delivered a decryption tool that (usually, at least mostly) allowed them to recover their files. But amid high-profile attacks like WannaCry, organizations began fortifying their cybersecurity posture to protect against ransomware. These organizations, provided they maintained current backups, were able to rebuild their systems easily without purchasing decryption tools.

While ransomware operators are getting better at finding and encrypting backups, they've also found another way to ensure victims pay up despite the existence of current backups: extortion.

In an increasing number of cases, such the recent attacks on Colonial Pipeline and the city of Tulsa, Okla., attackers are stealing and exfiltrating the data before they encrypt files. This means that even if the victims have ironclad backups and can rebuild their network easily, they may still pay to preserve their reputation, avoid fines and maintain regulatory compliance with regards to personally identifiable information, protect customers, or preserve the secrecy of intellectual property.

Unfortunately, organizations that display a willingness to pay may be opening themselves up to be attacked again soon after, either by the same group of cybercriminals or by another group who heard about the original payment. According to ZDNet, roughly eight in 10 organizations that opt to pay a ransom wind up being attacked again — and of those victims, nearly half believe the second attack was perpetrated by the same cybercriminals as the first.

While it's unclear how many organizations are targeted by repeat attacks — companies are often reluctant to publicly acknowledge ransomware incidents for this very reason — at least three have made headlines in recent years: the city of Baltimore, Australian logistics firm Toll Group and American technology company Pitney Bowes.



Recent Developments

MORE MOVING TO MONERO

The recent increased scrutiny of Bitcoin records, both as a result of cybercrime and in general, has served as a reminder of exactly how traceable the cryptocurrency is — prompting some attackers to shift tactics to better hide their tracks.

REvil, one of the most prominent and prolific ransomware groups prior to its disappearance in July, was recently known for demanding payment in Monero (though, as we saw in the JBS hacking incident, they were clearly still willing to accept Bitcoin).

Others, such as Babuk and Darkside, reportedly *prefer* Monero, but will accept Bitcoin from those willing to pay a premium to compensate for the added risk.

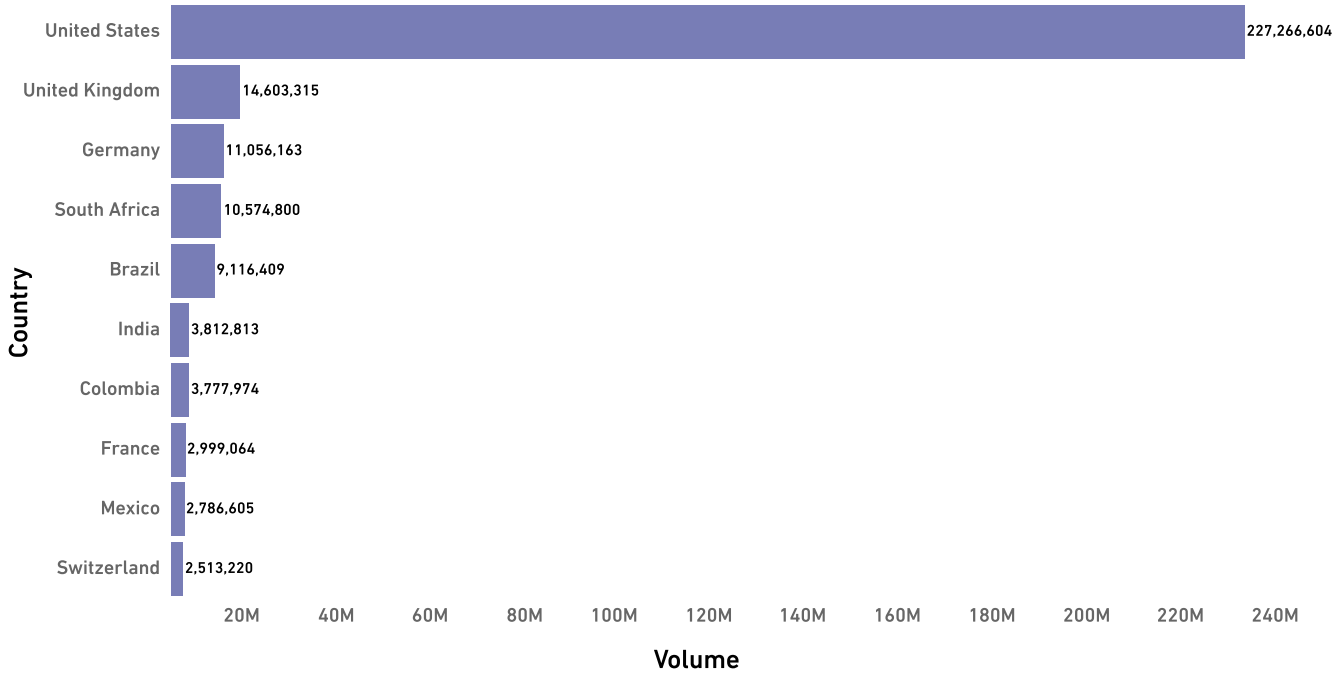
According to Justin Ehrenhofer, a member of the Monero developer community, Monero is used to satisfy an estimated 10% to 20% of ransom demands today. However, he predicts that as many as half of demands will be met with the privacy currency by the end of 2021.

WHAT HAPPENED TO REvil?

On the heels of successful attacks on JBS and Kaseya in the first half of 2021, ransomware giant REvil should have been riding high. But in early July, the Russia-based group suddenly disappeared, taking down sites on both the Dark Web and the clear web and leaving many victims in a lurch.

As of this writing, no one is sure what happened, but there are three prevailing theories: REvil shut down under pressure from Russian President Vladimir Putin; REvil was quietly taken out by U.S. Cyber Command in much the same way it targeted Trickbot in 2020; or REvil itself decided — as a result of investigations into its two recent, large-scale attacks — to either disband, or to lay low for a while. Regardless of the reason, the disappearance of REvil is good news for the industry.

2021 RANSOMWARE VOLUME | TOP 10 COUNTRIES



Ransomware's Rise

BY REGION

Unfortunately, ransomware isn't just getting worse — it's getting worse everywhere. At the top of the list, Europe fell victim to an alarming 234% spike in ransomware, and ransomware volume jumped 180% in North America.

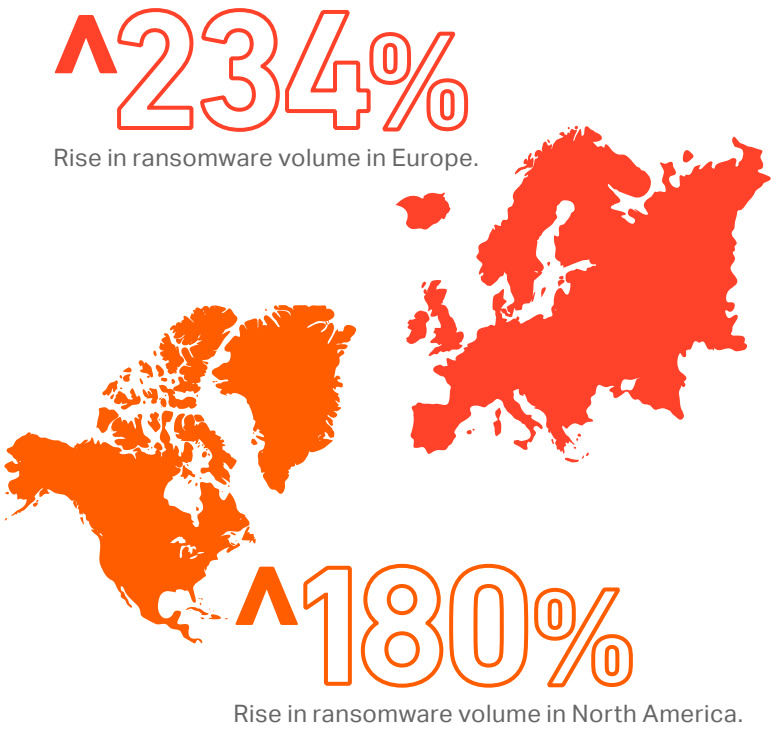
In Asia, ransomware hit a high point in March, then began dropping steadily. By June, there were only about a fifth as many attacks as there had been three months prior.

So while ransomware in Asia is still up 59% year to date, it's at least on a sustained path in the right direction.

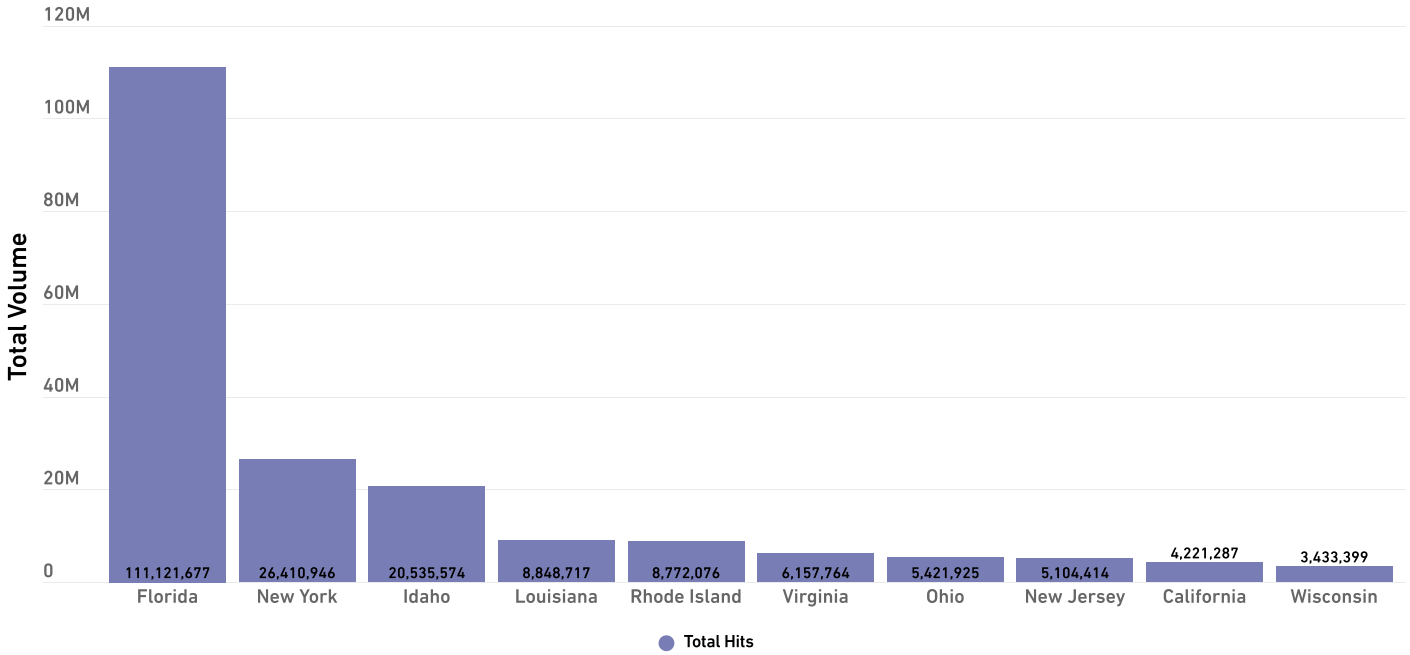
BY COUNTRY

Once again, the U.S. recorded far and away the most ransomware attacks. In fact, of the top 10 countries for ransomware volume, the U.S. had nearly as much ransomware as the other nine put together … *times four*.

But despite already having the lion's share of ransomware, attack volume in the U.S. still rose 185%, while ransomware in the second-ranking country, U.K., rose 144%.



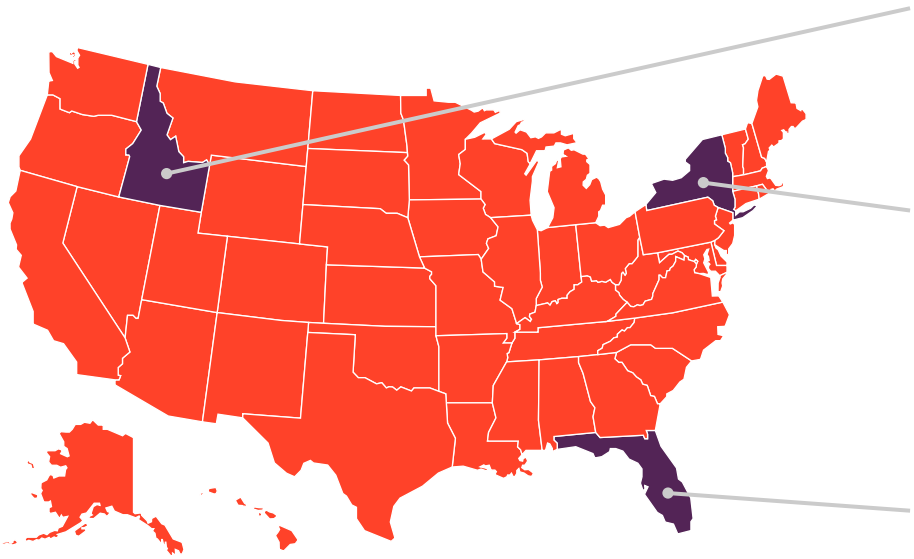
2021 RANSOMWARE VOLUME | TOP 10 U.S. STATES



BY STATE

As with the country-level data, there's one clear outlier at the state level in the U.S.: Florida, which racked up far more ransomware than the other nine states put together.

Surprisingly, California — home to nearly twice as many people as Florida — only recorded about 1/26th the amount of ransomware Florida did.



20M

Total number of malware hits in Idaho.

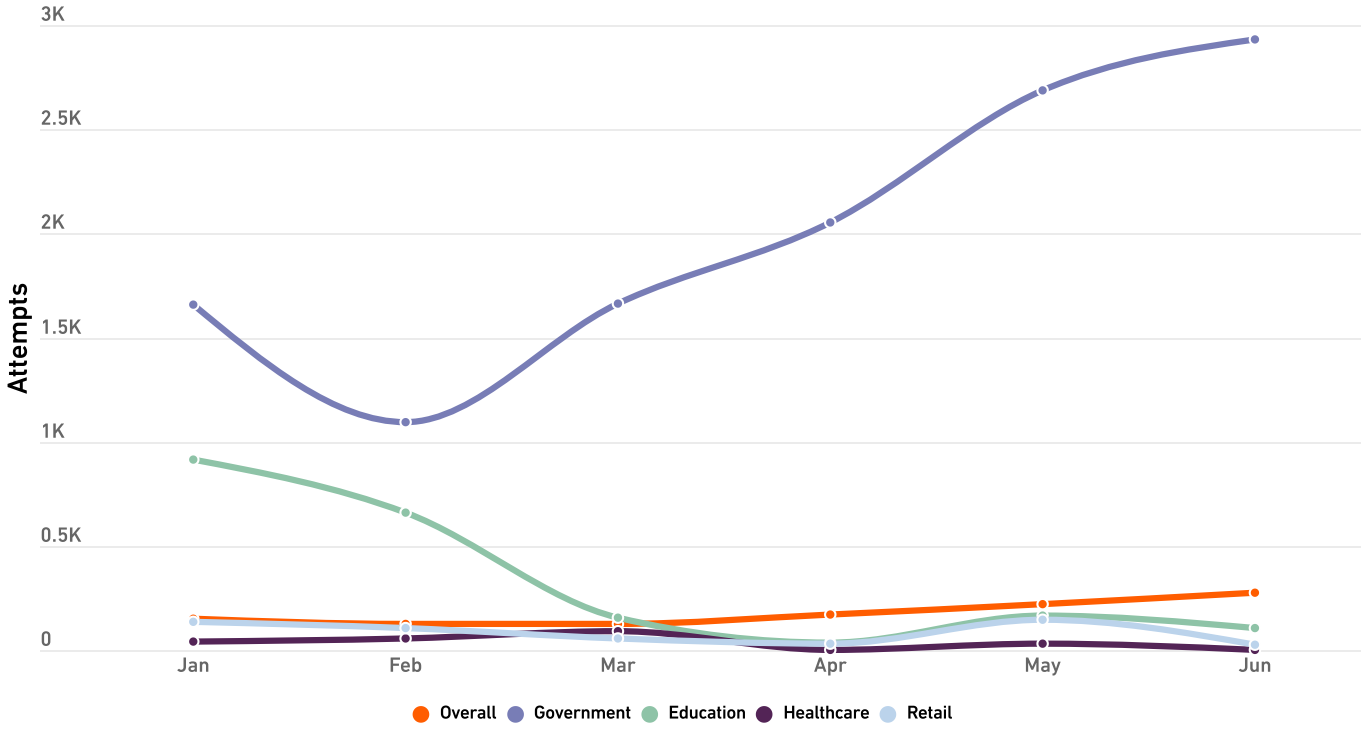
26M

Total number of malware hits in New York.

111M

Total number of malware hits in Florida.

2021 RANSOMWARE ATTEMPTS PER CUSTOMER



Is Your Industry at Risk?

ATTEMPTS PER CUSTOMER

By an overwhelming margin, the most commonly targeted industry in 2021 is government — and so far attacks have risen to **three times last year's high point**.

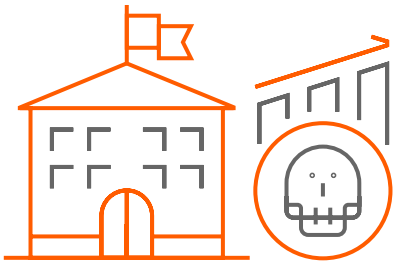
Each month in 2021, there have been far more hits on government customers than any other industry. By June, government customers were getting hit with roughly *10 times* more ransomware attempts than average.

By June, government customers were getting hit with roughly *10 times* more ransomware attempts than average.

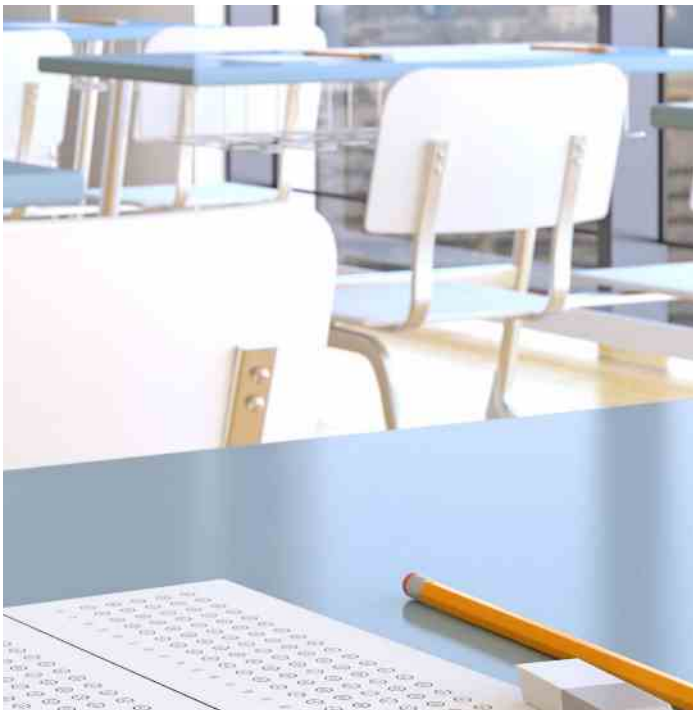
PERCENTAGE OF CUSTOMERS TARGETED

When it comes to the percentage of customers getting hit with ransomware attempts, the data is a bit more mixed. Government customers are still seeing a higher-than-average number of ransomware attempts, but in three out of six months during the first half of 2021, education customers saw even more.

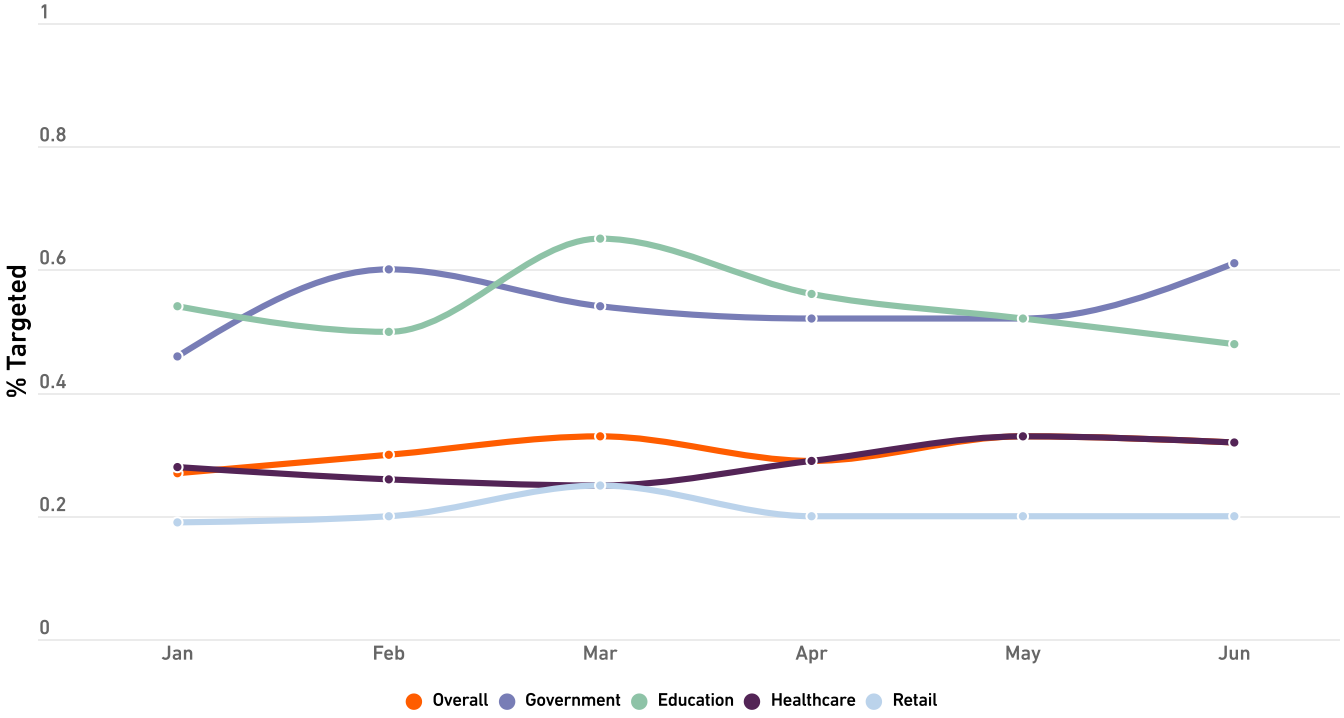
The good news is, the percentage of customers being targeted across all industries has fallen year to date.



In three out of six months during the first half of 2021, education customers saw even more ransomware attempts than government customers.



% OF CUSTOMERS TARGETED BY RANSOMWARE IN 2021



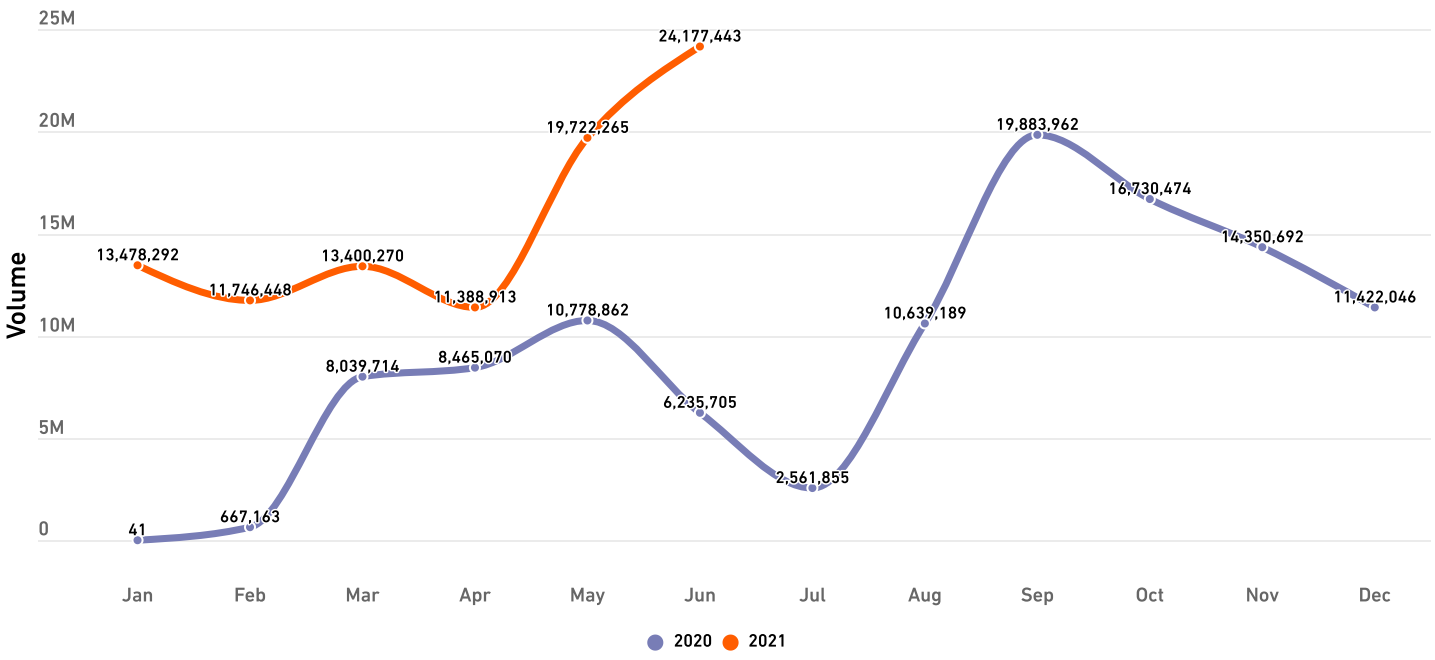
SONICWALL

Who are the Biggest Threats?

For the first half of 2021, the top three ransomware families by volume were Ryuk, Cerber and SamSam.

RYUK

GLOBAL RYUK RANSOMWARE VOLUME



RYUK: BY THE NUMBERS

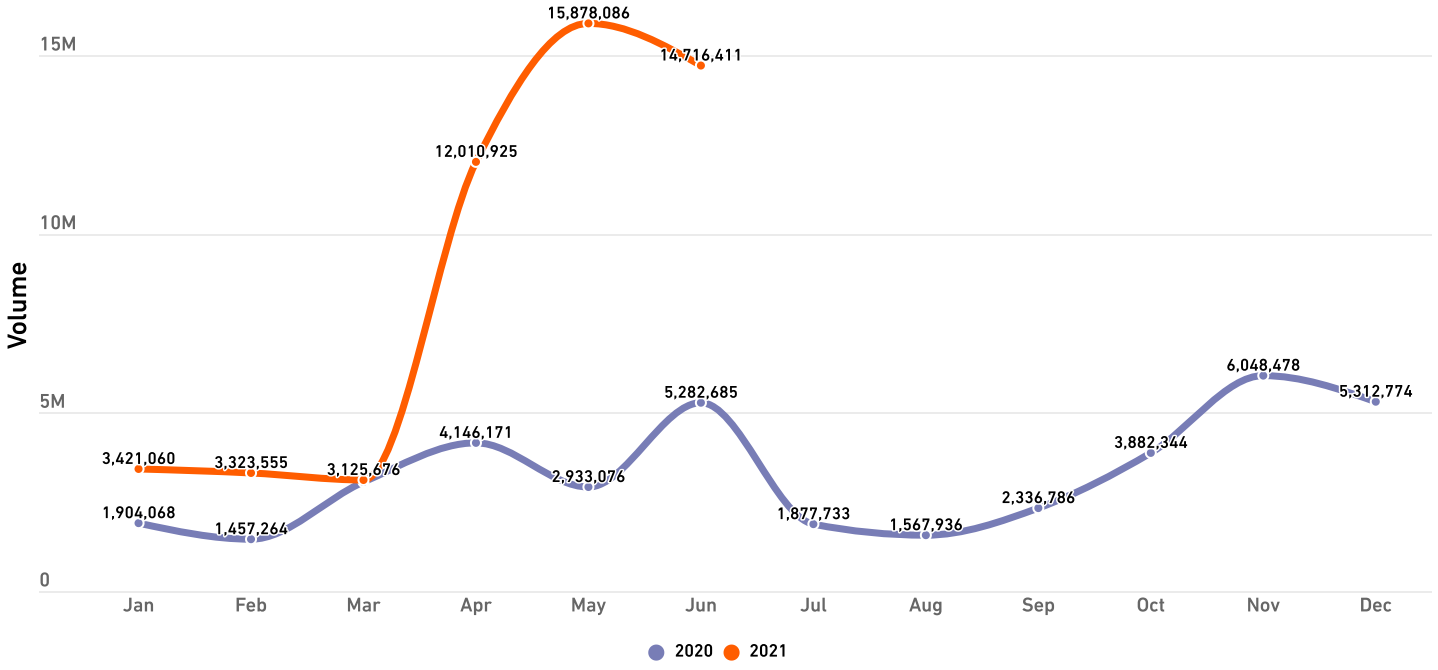
In the first half of the year, SonicWall Capture Labs threat researchers recorded 93.9 million instances of Ryuk. This total doesn't just *exceed* the number of Ryuk attempts in the first six months of 2020 — it nearly *triples* it.

Given the current trajectory of Ryuk going into the second half of 2021, we expect to see the number of Ryuk incidents continue to rise.

SonicWall Capture Labs threat researchers recorded 93.9 million instances of Ryuk in the first half of 2021.

CERBER

GLOBAL CERBER RANSOMWARE VOLUME



CERBER: BY THE NUMBERS

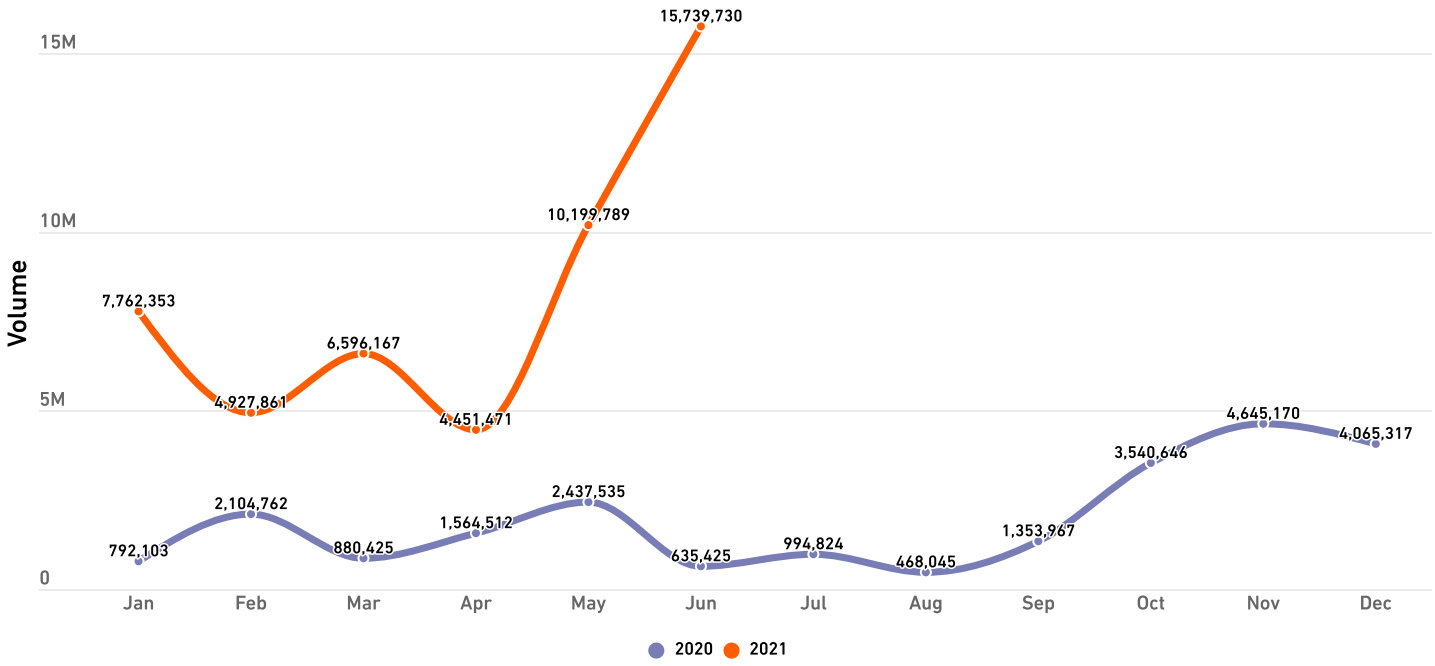
At the end of 2020, Cerber was the No. 2 ransomware family — and so far it's held onto its spot, with 52.5 million recorded hits in the first half of 2021.

While Cerber hits remained fairly steady in Q1, the number of hits nearly quadrupled in April, and by May it had risen to nearly five times the levels seen in January.

The number of hits nearly quadrupled in April, and by May it had risen to nearly five times the levels seen in January.

SAMSAM

GLOBAL SAMSAM RANSOMWARE VOLUME



SAMSAM: BY THE NUMBERS

So far in 2021, SonicWall Capture Labs threat researchers have recorded 49.7 million instances of SamSam — more than double the volume seen during the entire year of 2020. In fact, June alone saw 15.7 million hits — more than two-thirds the 23.5 million hits seen for all of last year.

June alone saw 15.7 million SamSam hits — more than two-thirds the 23.5 million hits seen for all of last year.

Malware Falls by Nearly a Quarter

A year and a half into the 2020s, it's starting to seem like the halcyon days of malware may be behind us. After routinely recording malware volumes of 8 billion a year in the 2010s, the threat type peaked at 10.5 billion in 2018.

Since then, there have not been more than two consecutive months of rise at any point, and the overall trend has been overwhelmingly down — sometimes like a feather, other times more like a rock.

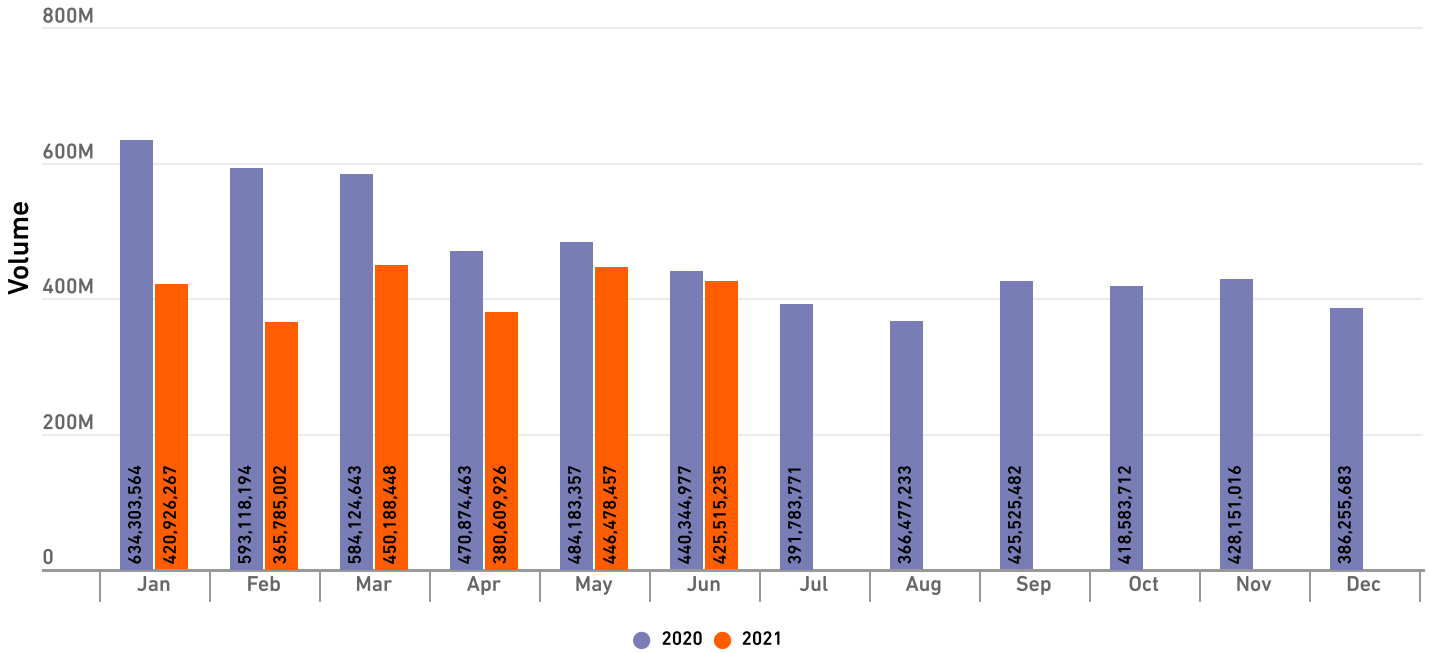
In 2020, SonicWall recorded 5.6 billion malware attempts, a six-year low, and so far 2021 has fallen even further. **SonicWall Capture Labs threat researchers recorded just 2.5 billion malware attempts in the first six months of this year, down from 3.2 million at this time last year — a decrease of 22%**.

But as it will become apparent by reading the rest of this report, less malware isn't the same as less cybercrime. Instead, it's a sign that the traditional malware associated with spray-and-pray attacks of yesterday is being abandoned ... usually in favor of more specialized, more sophisticated and more targeted attacks, capable of making criminals much more money and leaving much more devastation in their path.

Regional Malware Trends

While the general malware trend was slightly downward, there was a lot of variation from region to region. North America and Europe saw malware volume dip 25% and 13%, respectively. Contrast that with Asia, which actually saw a 23% *increase* in malware.

GLOBAL MALWARE VOLUME



The U.S. and the U.K. — two countries that have long been burdened with the lion's share of malware — fell in line, dropping 23% and 17%, respectively.

But something interesting happened in India and Germany during the first part of the year. In these two countries in particular, malware didn't just rise, it skyrocketed.

During the first half of 2020, India saw 80.6 million malware attempts, and Germany noted 26.6 million attempts. In the first half of 2021, India saw 147.2 million malware attempts, an increase of 83% year over year. But in Germany, researchers noted 150.4 million malware attempts — meaning malware attempts there increased a staggering 465%.

These increases rocket both countries up into the neighborhood of the U.K., which saw 188.6 million malware attempts in the first half of the year (but still far behind the 1.5 billion recorded during that period in the U.S.)

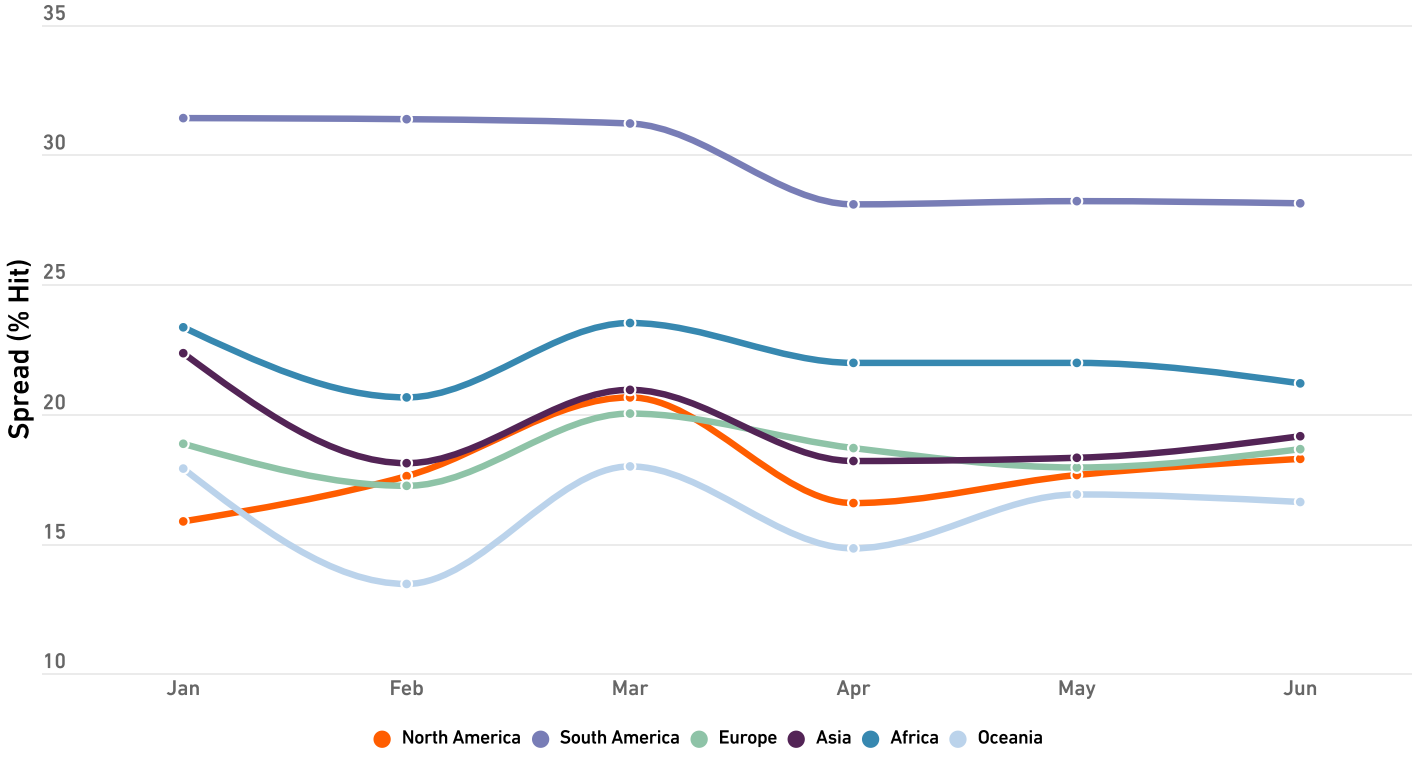
Malware Spread

In 2020, malware spread spiked dramatically in March across every region, likely as a result of the COVID-19 pandemic. Oddly, in the absence of such a universally disruptive event in 2021, four out of six regions still saw the highest malware spread in March. (The other two, South America and Asia, saw malware spread peak in January.)

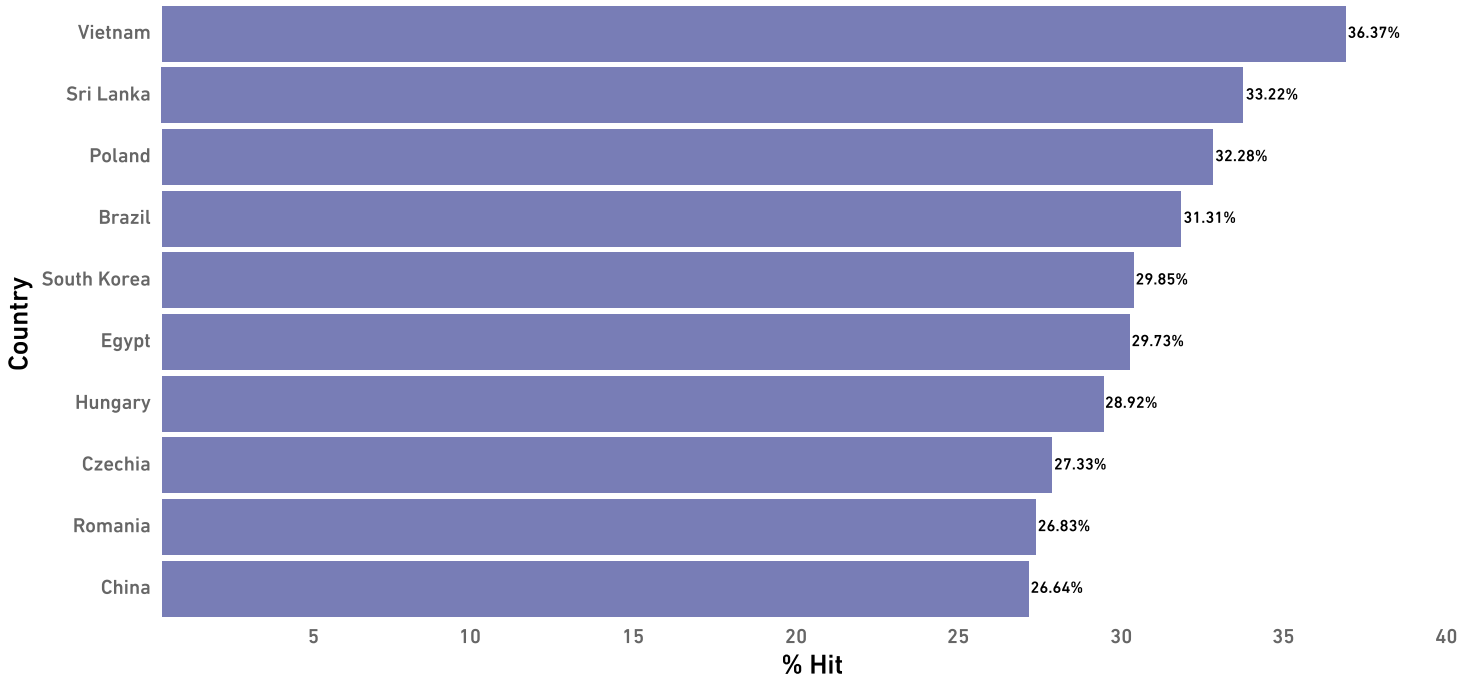
While the countries with the highest malware volume were the U.S., U.K., Germany and India, this doesn't mean a given organization in these countries is more likely to see malware. Once again, we see that the top countries for malware *volume* don't even make the top 10 when it comes to malware *spread*.

In the first half of 2021, an organization located in Vietnam had the highest chances of seeing attack, at 36.4%. In contrast, the safest country was the Bahamas, where only 15.87% of organizations saw a malware attempt.

2021 GLOBAL MALWARE SPREAD TREND



2021 MALWARE SPREAD | TOP 10 COUNTRIES



What is Malware Spread?

Malware totals are useful in calculating trends, but less so when it comes to determining relative risk: They 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.

RTDMI™ Reaches New Heights

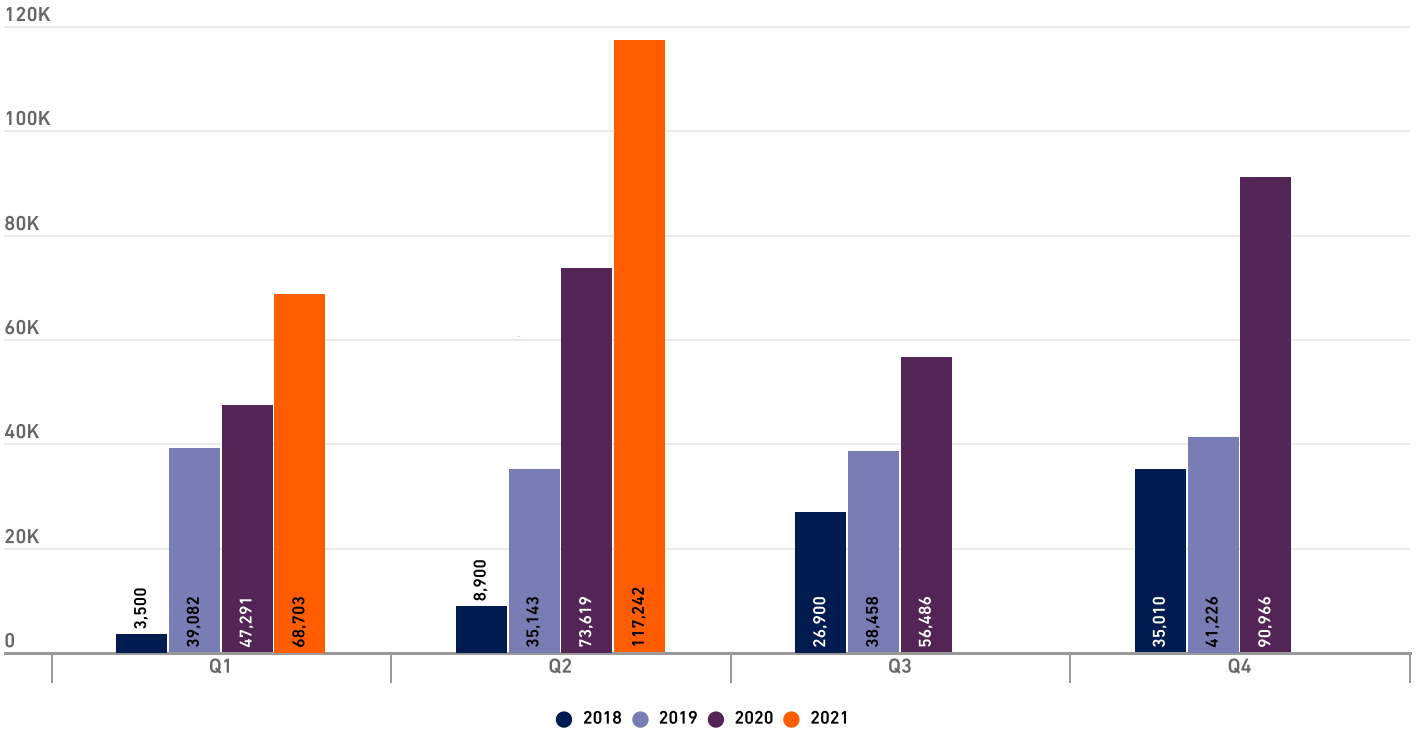
The number of new malware variants found by SonicWall's Real-Time Deep Memory Inspection™ (RTDMI) continues to rise. **In the first half of 2021, this patented technology discovered 185,945 "never-before-seen" malware variants, up 54% from the first half of 2020**.

While RTDMI has been continuously getting better at finding unknown threats since its introduction in 2018, comparing the first and second quarters of 2021 offers a striking example. Seventy-two percent more threats were found in Q2 than in Q1 — among the biggest increases we've ever recorded.

Included as part of SonicWall Capture Advanced Threat Protection (ATP), RTDMI leverages proprietary memory inspection and CPU instruction tracking with machine learning capabilities. This allows it to become increasingly efficient at recognizing and mitigating cyberattacks never seen by anyone in the cybersecurity industry — including threats that do not exhibit any malicious behavior and hide their weaponry via encryption.

72% more threats were found by RTDMI™ in Q2 than in Q1 — among the biggest increases SonicWall has ever recorded.

'NEVER-BEFORE-SEEN' MALWARE VARIANTS FOUND BY RTDMI™



100% Detection. No False Positives.

The power of RTDMI capabilities has been proven already this year — not once, but twice — in ICSA Labs Advanced Threat Defense testing. These tests evaluate vendor solutions designed to identify new threats that other traditional security products do not detect, and focus on how effectively solutions detect these unknown and little-known threats while minimizing false positives.

In February, after 35 days of testing and 1,741 tests, **SonicWall Capture ATP received a 100% score** with no false positives on the ICSA Labs Advanced Threat Defense test for Q1 2021.

Then in May, after a further 33 days of testing and another 1,144 tests, the solution earned a second 100% score in a row, still without a single false positive.

> ***"It's a milestone moment to see our technology reach this level and to receive such a wonderful score when tested against some of the most unknown and rigorous threats today. These third-party, real-world tests play a vital role in ensuring that we continue to strive for and deliver excellent products and services."***
>
> *Alex Dubrovsky*
> *Vice President of Software Engineering & Threat Research, SonicWall*

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

SonicWall tracks the detection and mitigation of "never-before-seen" attacks, which are recorded the first time SonicWall Capture ATP 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 PDF and Office Files on the Decline

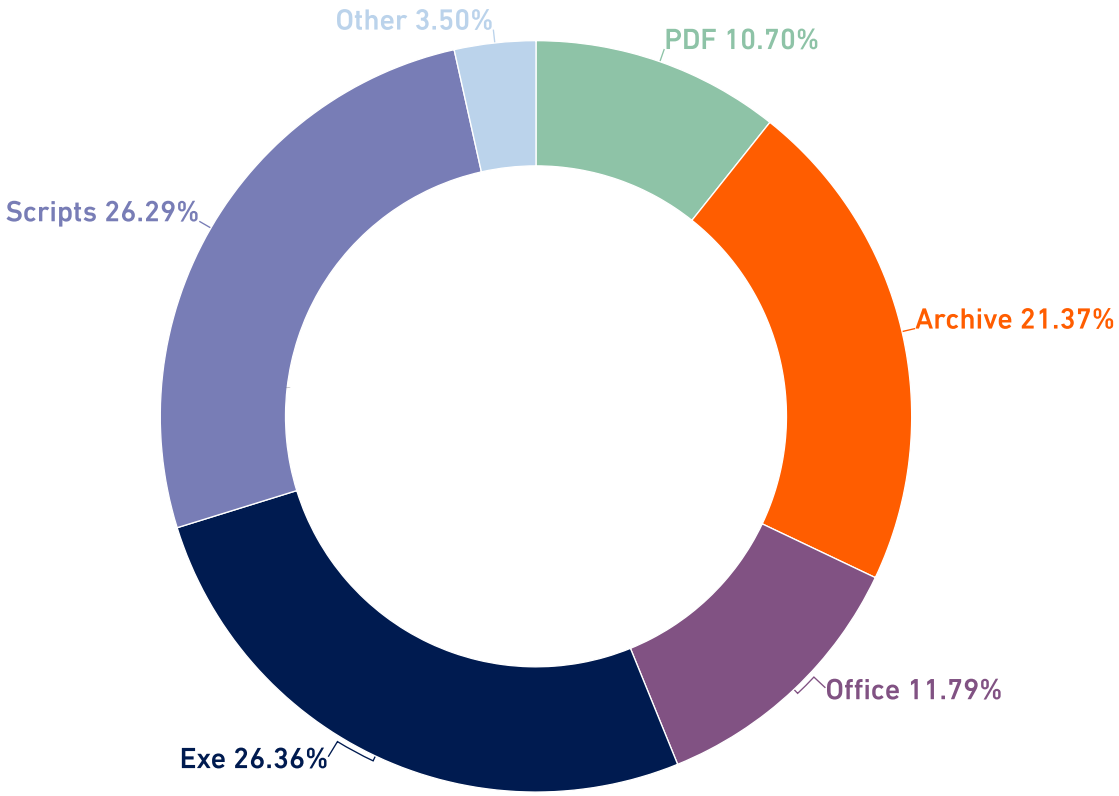
There aren't many bright spots to report on during what's been a record-setting year for cybercrime, but here's one: For the first time since at least 2018, the volume of both malicious PDF files and malicious Office files has dropped.

At the beginning of 2020, there were nearly as many malicious PDFs as Office files. But over the course of 2020, the number of malicious Office files began to skyrocket. By midyear, there were 110% more malicious Office files than malicious PDFs, and by the end of the year, that gulf had widened to 150%.

So far in 2021, as restrictions have eased and offices have reopened worldwide, malicious Office files have dropped 54%, while malicious PDFs have fallen only 13%. Both filetypes together make up 23% of all malicious files detected by Capture ATP.

.Exe files gained most of the ground malicious Office files lost, rising from 15.5% to 26%.

2021 NEW MALICIOUS FILE TYPE DETECTIONS | CAPTURE ATP



IoT Attacks Jump 59%

IoT malware has shown continued growth since 2018. But in the first half of 2021, these attacks have increased even faster. IoT attack volume in the first six months of 2021 rose 59% over the first six months of 2020 — a period which itself showed a 50% increase over the same time in 2019.

In all, 32.2 million IoT attacks have been recorded so far this year, compared with 20.2 million during the same time period last year.

In the U.S., IoT malware attempts rose 15% to 9.4 million. In other words, attacks on targets in the U.S. now make up nearly a third of all attacks worldwide.

This unfortunate news does come with a couple of bright spots. First of all, while IoT attacks are up most places — including North America, which saw a rise of 21%; Europe, which recorded an increase of 113%; and Asia, where attacks skyrocketed 190% — they weren't up *everywhere*. South America, Africa and Australia saw IoT attacks decrease 9%.

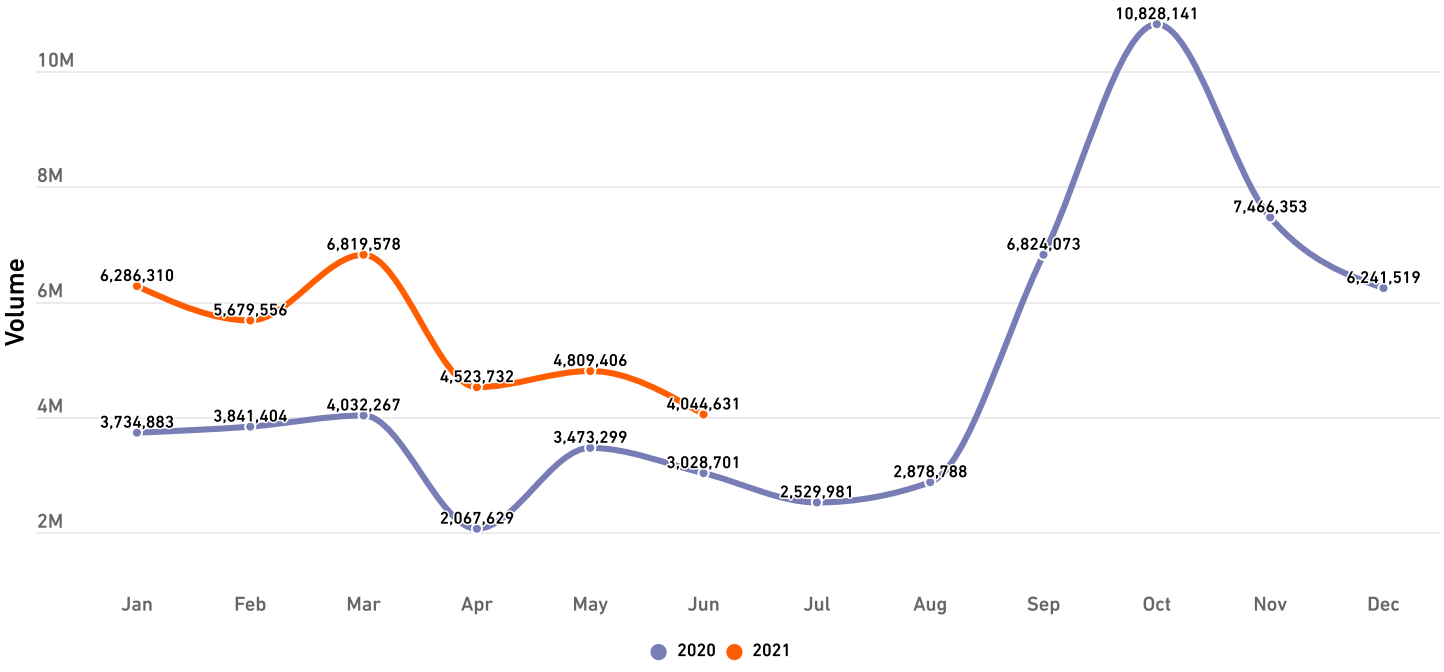
Secondly, attacks were higher in Q1 than they were in Q2, meaning that rates are trending downward, at least for now.

On the other hand, the first half of 2021 still recorded numbers far above those seen in the first half of 2020. If, instead of continuing to fall, attack volume in 2021 follows the pattern established in 2020, we may be on track to see a quarter with far more IoT attacks than any we've experienced before.

With 41 billion IoT devices projected to be online by 2027, and with nearly three-quarters of enterprises reporting either full or trial IoT deployments, cybercriminals are clearly seeing attacks on IoT devices as a growth industry ripe for exploitation.

And some of these criminal exploits have had far-reaching impacts. In February, an attacker took control of the systems running Oldsmar, Florida's water supply, increasing the amount of sodium hydroxide, or lye, in the water to 110 times normal levels.

GLOBAL IoT MALWARE VOLUME



Just two months later, vulnerabilities affecting over 100 million enterprise, consumer and industrial IoT devices were identified that could allow attackers to take control of them remotely and gain wider access to connected networks.

While the nine vulnerabilities, collectively known as "Name:Wreck," all have patches available as of the time of this writing, many IoT devices lack the ability to be easily patched (or patched at all), meaning we may see attacks arising from these vulnerabilities for years into the future.

And in early July, researchers discovered a vulnerability in millions of Schneider Electric programmable logic controllers — used in automation, manufacturing, utilities and more — that could enable remote attackers to take control and deploy malware, perform remote code execution attacks and more.

Vulnerabilities in devices like these — which are connected to systems that could result in large-scale disruption if breached — shine a light on why industries need to act now to ensure that IoT devices are not only more secure, but are also easily patchable.

Regulation to the Rescue?

With the specter of IoT attacks continuing to grow, many legislative bodies opted to consider legislation strengthening cybersecurity on these devices during the first half of 2021:

U.K.

In late January, the U.K. Department for Digital, Culture, Media and Sport announced a new law that would ban the use of easy-to-guess default passwords in IoT devices. Manufacturers would be required to disclose the length of time they planned to continue offering security updates for these devices. The law would also mandate the creation of a public point of contact for reporting vulnerabilities, and would require devices have the ability to receive software updates.

Australia

Due to a lack of response from manufacturers of lower-cost goods, the Australian government announced it is considering making mandatory a suite of voluntary regulations introduced last September. These regulations would outline a set of minimum cybersecurity requirements for consumer-grade smart devices.

U.S.

In late March, legislation known as the Cyber Shield Act was reintroduced in Congress. If passed, the law would create security standards for IoT devices based on recommendations from an advisory committee made up of cybersecurity experts from the government, academia and the private sector. Devices meeting these regulations would be allowed to label their products with a mark indicating they had met the standards and their products were more secure.

Cryptojacking Continues to Climb

As cryptocurrency prices go, so goes cryptojacking. And with crypto prices reaching the stratosphere in the first half of 2021, SonicWall recorded a higher volume of cryptojacking in Q1 than any quarter since it began reporting these attacks in 2018.

These unusually high levels of cryptojacking at the beginning of the year pushed total cryptojacking attacks for the first six months of 2021 to 51.1 million, an increase of 23% over the first half of 2020.

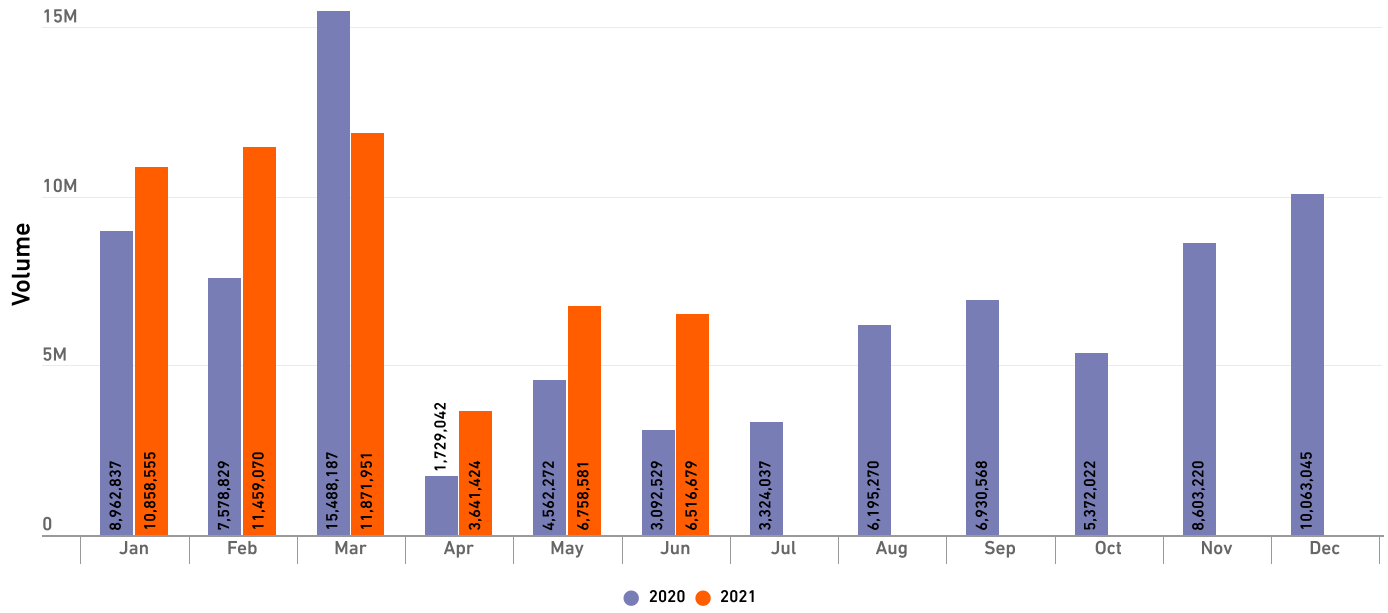
While cryptojacking rose worldwide, there was a lot of regional variation. In North America, attack volume rose by 22% — a significant increase, but an order of magnitude less than the 252% increase recorded in the region in the first half of 2020.

In Asia, attacks rose a more worrying 118%, but it was Europe that saw the largest increase. **In Europe, cryptojacking rose 248%, with attack volume in May and June spiking to 50 and 23 times what was seen during these months last year.**

Cryptojacking in the U.S. rose 22% year over year and followed a similar pattern as 2020, with a higher Q1 and a low point in April. However, instead of falling in June and staying low, June 2021 cryptojacking levels remained almost static. Whether this indicates threat levels are stabilizing remains to be seen.

SonicWall recorded a higher volume of cryptojacking in Q1 than any quarter since it began reporting these attacks in 2018.

GLOBAL CRYPTOJACKING VOLUME



SONICWALL

THE CRYPTOCURRENCY CONNECTION

In the full-year *2021 SonicWall Cyber Threat Report*, we noted that if you had one Bitcoin in March 2020, you could finance a nice vacation — but that if you had held onto that same Bitcoin through the end of the year, it would have increased in value enough to purchase a 2021 Toyota RAV4.

In early 2021, however, the price of Bitcoin rose even faster. If you still had that Bitcoin in mid-April, when prices doubled to a peak of nearly $64,000, you could have flipped it for a 2021 Porsche 718 Cayman or a Jaguar F-Type (and still had a little left over to go on the road trip of your life.)

Monero prices followed a similar trajectory, cresting in April to hit a new all-time high. **But if Q1 was about the rise of cryptocurrency, Q2 was equally about its fall.**

Spring brought with it headlines warning of the environmental impacts of mining, which preceded two sea-changing announcements. In May, Elon Musk announced that Tesla would no longer accept Bitcoin as payment. Less than a week later, China banned mining altogether in some provinces.

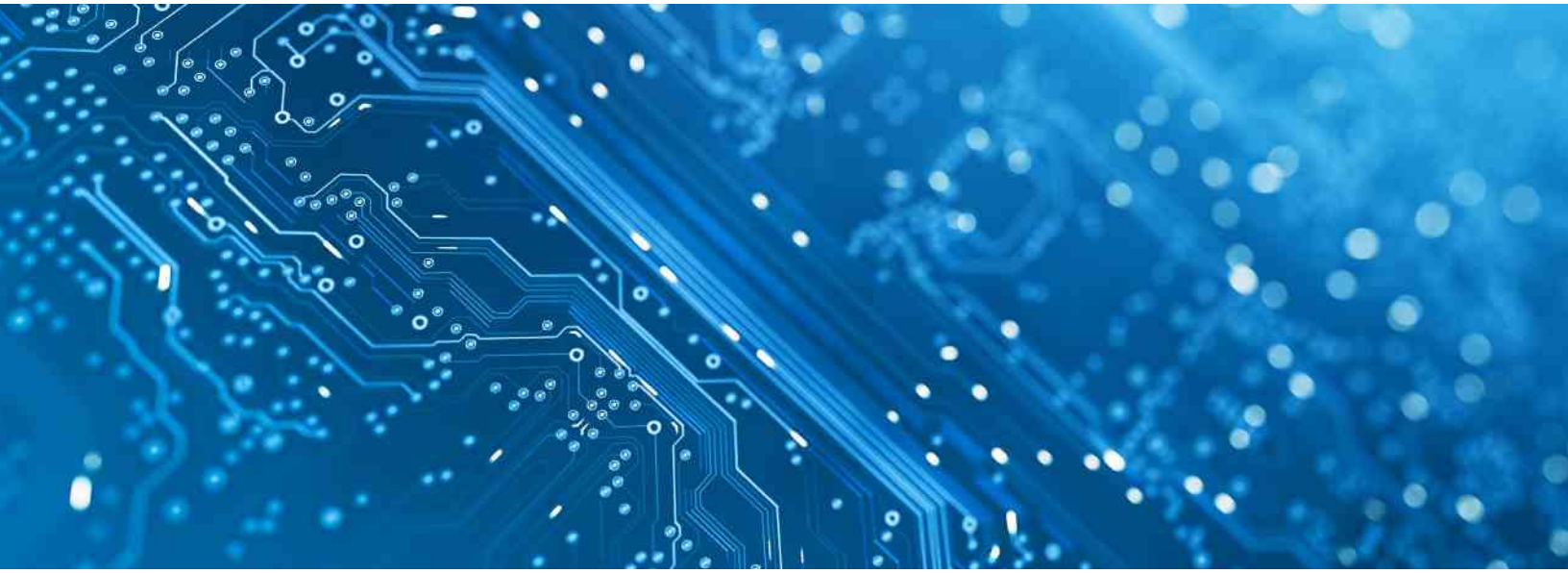
Just days after that, the IRS warned it would step up tax enforcement on cryptocurrency traders — and prior court summonses by federal judges on opposite sides of the country demanding that cryptocurrency purchase records be surrendered gave the warning teeth.

Faced with the growing suspicion that crypto may be both a poor investment and a poor tax shelter going forward, diamond hands turned to paper hands and cryptocurrencies crashed hard.

Faced with the growing suspicion that crypto may be both a poor investment and a poor tax shelter going forward, diamond hands turned to paper hands and cryptocurrencies crashed hard.

But why did cryptojacking crash in April, just as many cryptocurrencies were peaking? Whether it was due to closer federal scrutiny, a shift toward cashing out while the market was hot, or a sudden desire to get in touch with their Earth-loving side, cryptojacking fell hard in April. It bottomed out at a little over a third of the heights it reached in March, and — much like the price of crypto itself — still hasn't fully recovered.

As large-scale mining operations continue to fall around the world amid government crackdowns, it'll be interesting to see whether cryptojacking soars again to fill the void.



Attacks Against Non-Standard Ports Fall

While we haven't seen many big reversals so far in 2021, a major one has been in the use of non-standard ports to launch attacks.

While the percentage of attacks on non-standard ports held remarkably steady throughout 2020, this number fell to 21% for the first quarter of 2021 — a level not seen in more than a year.

This was just a hint of the drop that would occur in Q2, when non-standard port attacks dropped sharply to 13%. The low-water mark for that quarter came in April, **when attacks fell to 9% — the lowest since January 2019**. Interestingly, this drop comes less than a year after non-standard port attacks reached a new *high* of 46%, in July 2020.

Whether this is a temporary blip as criminals focus on other methods, or a more permanent shift resulting from ramped-up cybersecurity measures, remains to be seen.

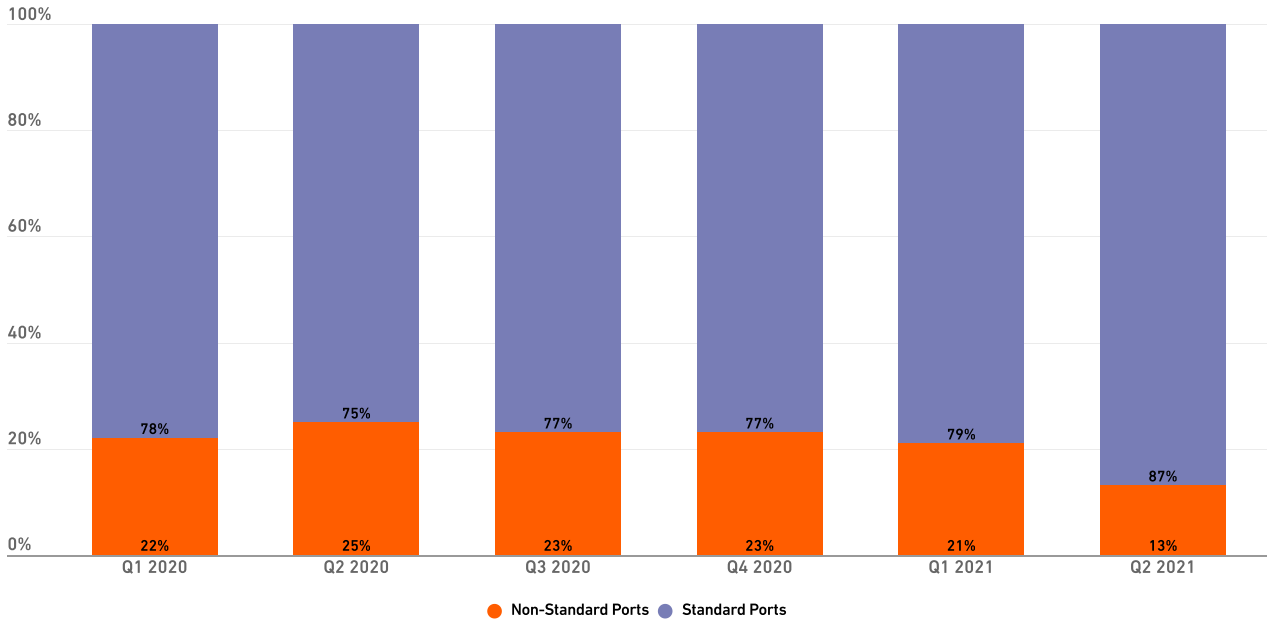
What is a Non-Standard Port Attack?

While around 40,000 ports are registered, just a few — the "standard" ports — are generally used. For example, HTTP uses port 80, HTTPS uses port 443 and SMTP uses port 25. When a service uses a port other than the one assigned to it by default, usually as defined by the IANA port numbers registry, it is using a non-standard port.

While there's nothing inherently wrong with the use of non-standard ports, it can present cybersecurity challenges. Traditional proxy-based firewalls typically focus on protecting traffic going through standard ports — but because there are so many ports to monitor, these legacy firewalls can't mitigate attacks over non-standard ports. Cybercriminals have long been aware of this and target non-standard ports to help avoid being detected as they deploy their payloads.

Modern firewalls that are capable of analyzing specific artifacts (as opposed to all traffic) can identify such attacks, and as more organizations continue to adopt these newer security solutions, we may see the volume of attacks coming over non-standard ports continue to fall.

2020-21 GLOBAL MALWARE ATTACKS



YOUR NEW RESEARCH DESTINATION: THE SONICWALL CAPTURE LABS PORTAL

With threats of almost every type on the rise, SonicWall in June introduced the Capture Labs Portal, an important tool for partners, customers and the cybersecurity community at large.

The SonicWall Capture Labs Portal is a free-to-use centralized repository for comprehensive research that combines new and previously available tools into one easy-to-access portal.

This portal offers direct access to information gathered by SonicWall's Capture Threat Network — consisting of over a million security sensors in over 215 countries and territories, SonicWall's internal malware analysis framework, shared threat intelligence and exploits from industry groups and research organizations, and information from third-party researchers.

With the introduction of the Capture Labs Portal, researchers can perform the following actions from a single organized and easy-to-access portal:

- Use Security Center in near real time
- View the latest security news and research CVE lists
- Research SonicWall's product advisory databases
- Report new SonicWall product vulnerabilities online
- Research SonicWall's rich application, IPS, Anti-Virus and Anti-Spyware threat databases
- Easily gauge the safety of URLs and IP addresses with reputation lookup tools

As the Capture Labs threat research team grows and adds more tools, we will be augmenting this portal with additional capabilities.

The Capture Labs Portal is free to use and can be accessed by anyone at

capturelabs.sonicwall.com

ABOUT THE SONICWALL CAPTURE LABS THREAT NETWORK

SONICWALL CAPTURE LABS

Intelligence for the mid-year update to the ***2021 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

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.

2021-MYThreatReport-COG-4776