



MID-YEAR UPDATE | JULY 2020

2020 SONICWALL CYBER THREAT REPORT

Cyber threat intelligence for navigating
the new business normal

SONICWALL®

www.sonicwall.com | @SonicWall



Table of Contents

A Note From Bill	03
2020 Global Cyberattack Trends	04
Profiting off the Pandemic	05
Phishing for Fear	06
What's Hiding in Your Office Files?	07
Malware Falls in 2020	09
What's Your Malware Risk?	11
Ransomware Still on the Rise	17
Non-Standard Port Attacks Gain Ground	21
IoT Attacks Spike 50%	22
Encrypted Threats Make Late Surge	24
Cryptojacking: 2020's Comeback Kid	25
Connection in the Time of COVID	27
About the SonicWall Capture Labs Threat Network	29
About SonicWall	30

A Note From Bill

We're in the midst of one of the most turbulent times in cybersecurity history. Over the past six months, as the COVID-19 pandemic ravaged its way across the globe, we've seen shifts we thought would take decades happen virtually overnight.

Full-scale remote work went from being a long-term plan to an imminent necessity. With traditional work solutions no longer sufficient to protect and enable employees working from home, cybersecurity had to pivot — without precedent and, in many cases, without budget — to secure employees at significantly greater risk than ever before.

In April 2020, SonicWall introduced the new Boundless Cybersecurity model, designed to help organizations navigate a hyper-distributed IT reality where everyone is remote, everyone is mobile and everyone is less secure.

By knowing the unknown, providing real-time visibility and leveraging breakthrough economics, SonicWall enables businesses to close the cybersecurity business gap and guard against the growing ranks of opportunistic cyberattackers.

While the historic disruption accompanying the COVID-19 pandemic has been challenging for businesses, it's been a boon for cybercriminals.

SonicWall Capture Labs threat researchers have detailed at least 20 COVID-19-themed threats aimed at ensnaring worried and distracted victims.

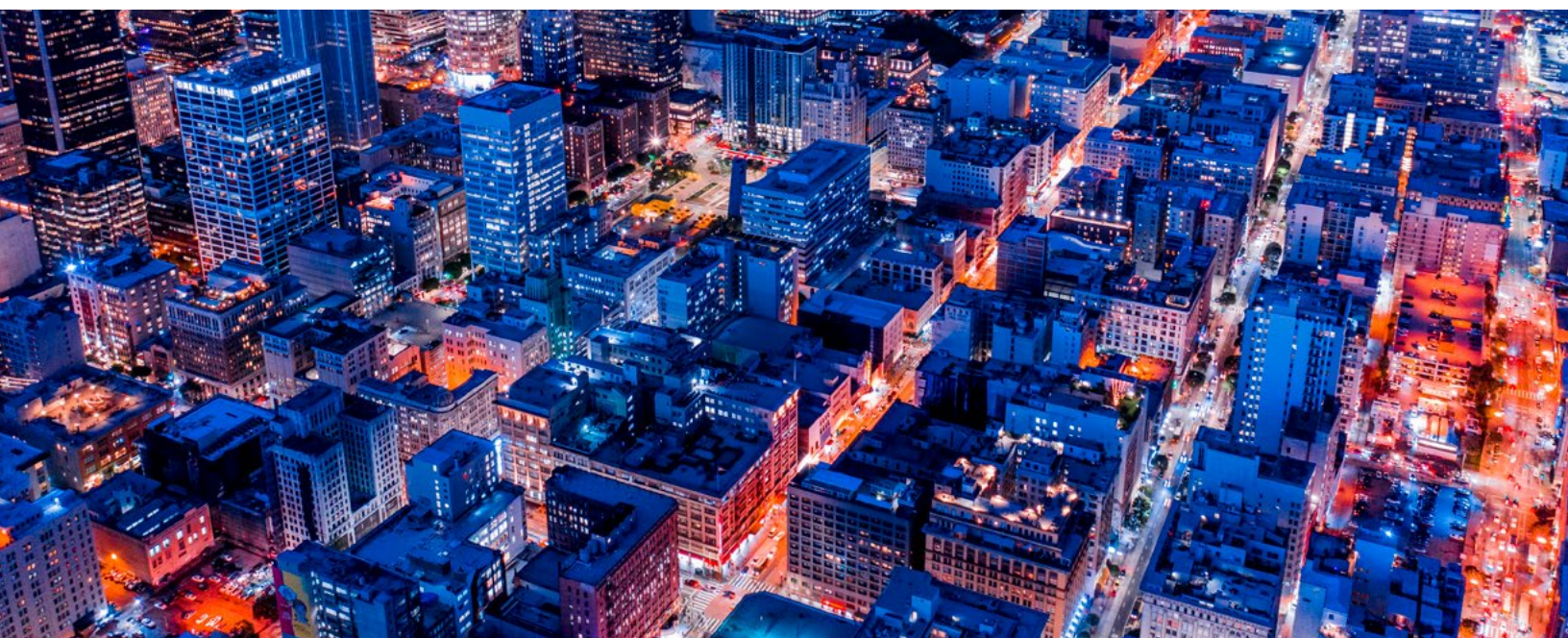
The pandemic's effects can be seen in most every piece of threat data highlighted here — shifting, increasing, decreasing and upending long-standing patterns.

Amid the disruption, a few key takeaways emerge: Malware is down, but changing and spreading. Ransomware is up, particularly in the U.S. (+109%). Office files continue to be leveraged for malicious agenda. SonicWall Capture Advanced Threat Protection (ATP) with Real-Time Deep Memory Inspection™ is catching more attacks than ever. Malware targeting Internet of Things (IoT) devices has risen to 20.2 million, up 50% from this time last year. Cybercriminals are increasingly targeting the massive influx of employees working from home. And intrusion attempts are up 19%, to 2.3 trillion.

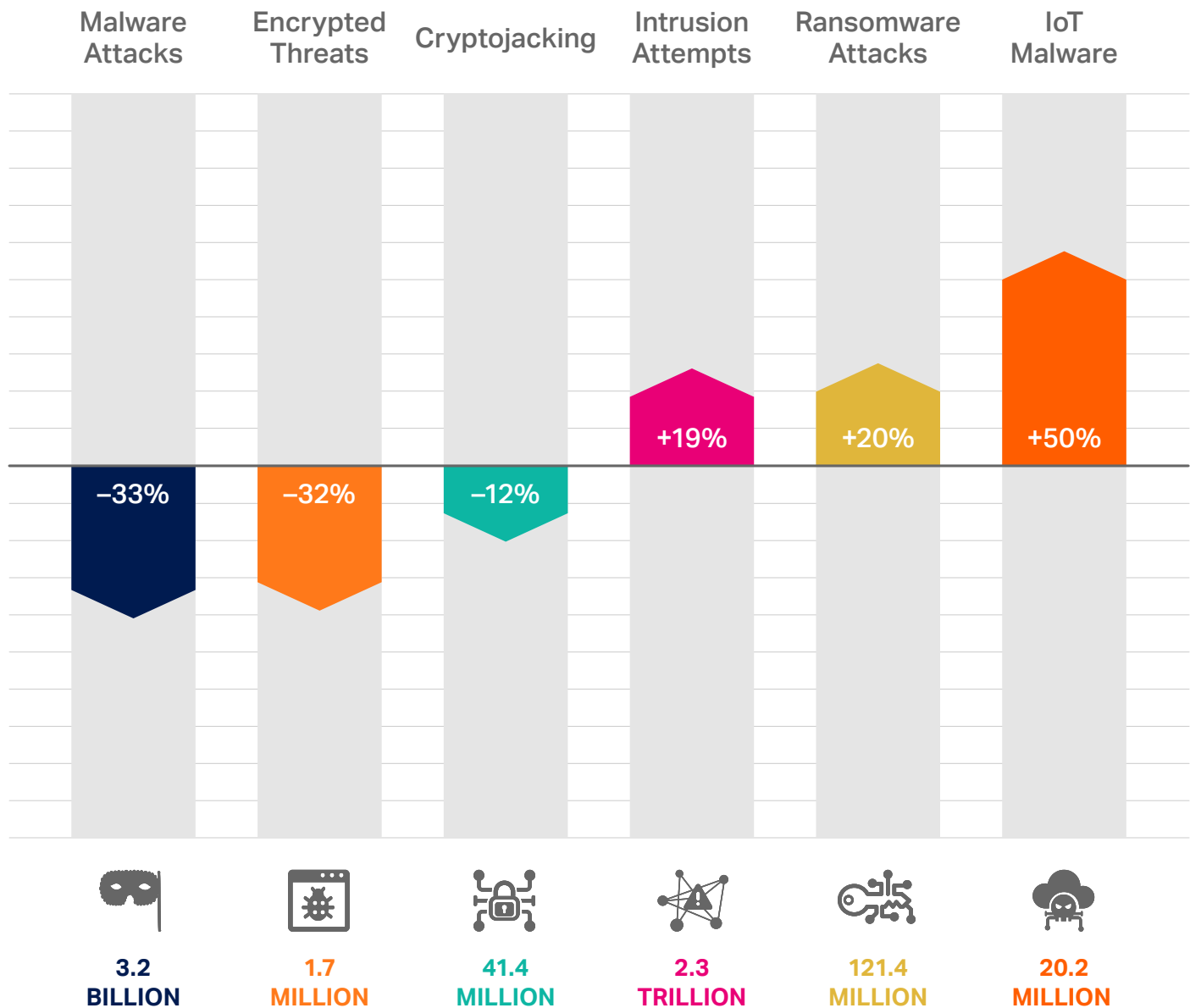
By gaining a fuller understanding about where we find ourselves in 2020, we can move as safely and resolutely as possible toward the future, whatever it has in store.



BILL CONNER
PRESIDENT & CEO
SONICWALL



2020 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.

Profiting off the Pandemic

These are dark days for many businesses and individuals. But they're salad days for cybercriminals. Opportunistic hackers, seeing a chance to take advantage of the confusion and fear surrounding the pandemic, have been out in force.

During a June 16 U.S. House meeting on cybercrime, [representative Emanuel Cleaver stated](#), "We are seeing a 75% spike in daily cybercrimes reported by the FBI since the start of the pandemic."

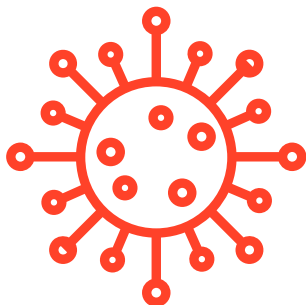
To make matters worse, some are targeting medical facilities, research labs, utilities and other institutions we're relying on for our continued survival.

"It was only a matter of time before a nation state resorted to cybercrime to influence or control global healthcare during a time of great need," Bill Conner [told Newsweek International](#).

"As this pandemic expands and evolves, we stand to see similar attacks in the future. It's incredibly valuable information for millions around the world — IP that would catapult a company's economy if seized," Conner said. "[Cyber] criminals tend to follow the money trail, thus putting a massive bounty on anything vaccine-related."

While COVID-19 continues to drive cybersecurity trends as a whole, it has also inspired new attacks capitalizing on our desire for news, assistance or guidelines that could help keep us safe.

SonicWall Capture Labs threat researchers began seeing attacks, scams and exploits specifically based around COVID-19 on Feb. 4, and since then have detailed at least 20 different types of attacks across just about every category.



- **MALWARE** [Corona Anti-Locker Ultimate](#), a data-stealing malware
- **RANSOMWARE** [Ada Covid](#), which uses WhatsApp to communicate with victims
- **CRYPTOMINER** A [cryptominer trojan](#) that comes as a WinRAR self-extracting archive and is capable of killing and deleting running rival cryptominers
- **ANDROID LOCKER** [Various versions of Android Locker](#), repackaged to look like apps such as WhatsApp, Netflix and others
- **TROJAN** [Infostealer Trojan](#), delivered via an email purportedly coming from the U.S. Centers for Disease Control (CDC)
- **RAT** [Remote Access Trojan](#) distributed via spam attachment disguised as COVID-19 response and preparedness document
- **SPAM SCAM** [Malicious executable file](#) in email supposedly regarding COVID-19 relief package
- **SCAREWARE** [Lansom](#) scareware demands ransom but in reality does not encrypt any files

"It was only a matter of time before a nation state resorted to cybercrime to influence or control global healthcare during a time of great need."

BILL CONNER
PRESIDENT & CEO
SONICWALL

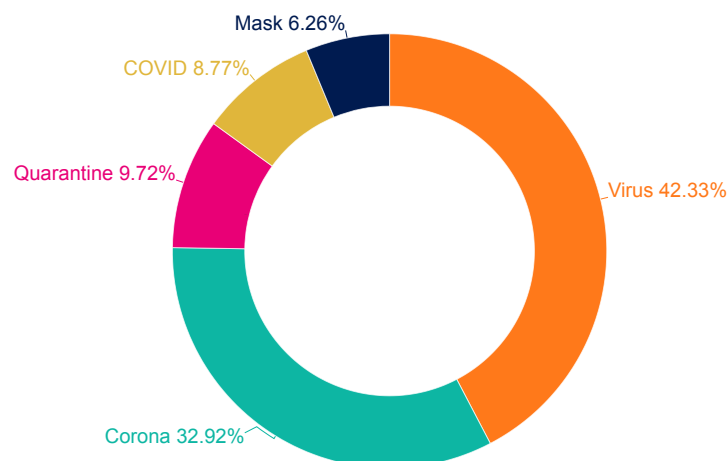
[NEWSWEEK INTERNATIONAL, JULY 16, 2020](#)

Phishing for Fear

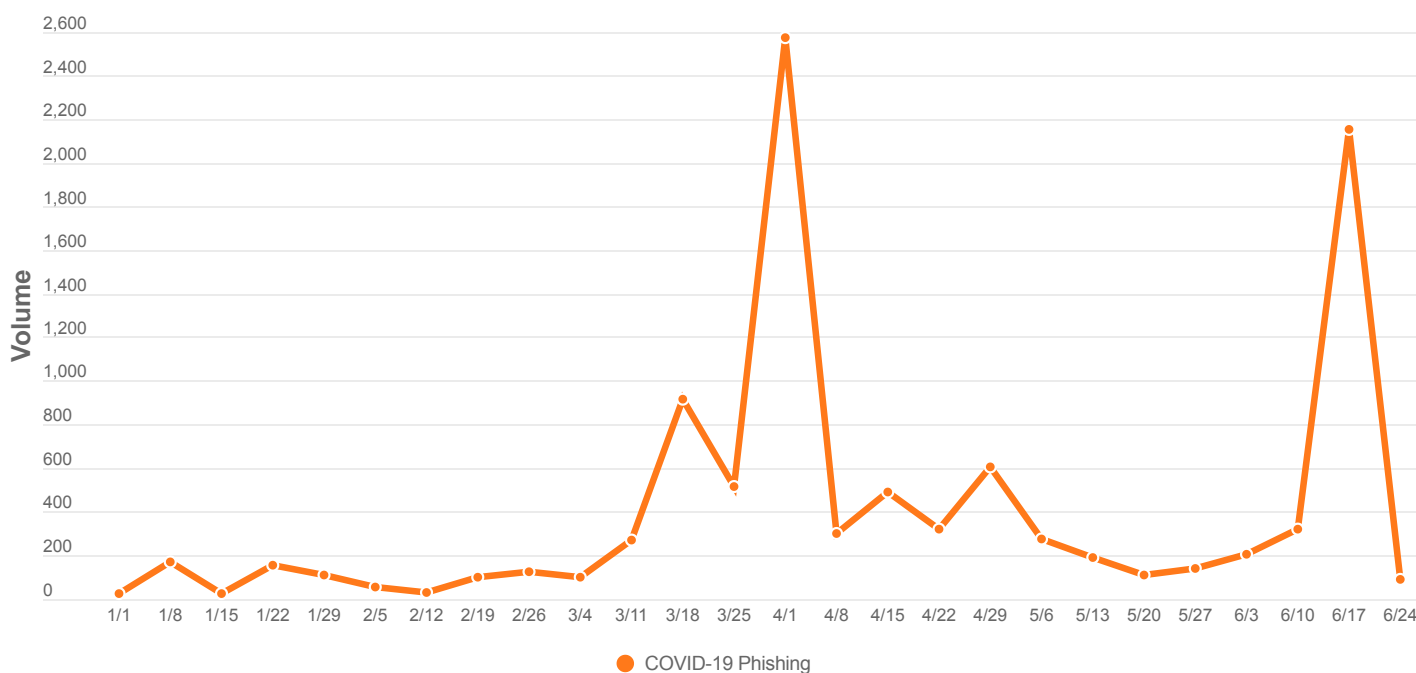
In the first half of 2020 global phishing volume was down 15%, but roughly 7% of those attacks leveraged fears around COVID-19. SonicWall phishing intelligence derived this figure from a large sample of spam emails containing COVID-19-related search terms. The safe, or non-phishing, emails about COVID and related terms were filtered out and omitted.

As expected, COVID-19 phishing began rising in March, and saw its most significant peaks on March 24, April 3 and June 19. This contrasts with phishing as a whole, which started strong in January and was down by the time the pandemic phishing attempts began to pick up steam.

TOP 5 COVID-19 PHISHING KEYWORDS



2020 COVID-19 PHISHING TRENDS



* Not representative of total phishing volume. Weekly data based on sample pool of SonicWall phishing intelligence. Safe emails related to COVID-19 filtered and omitted.

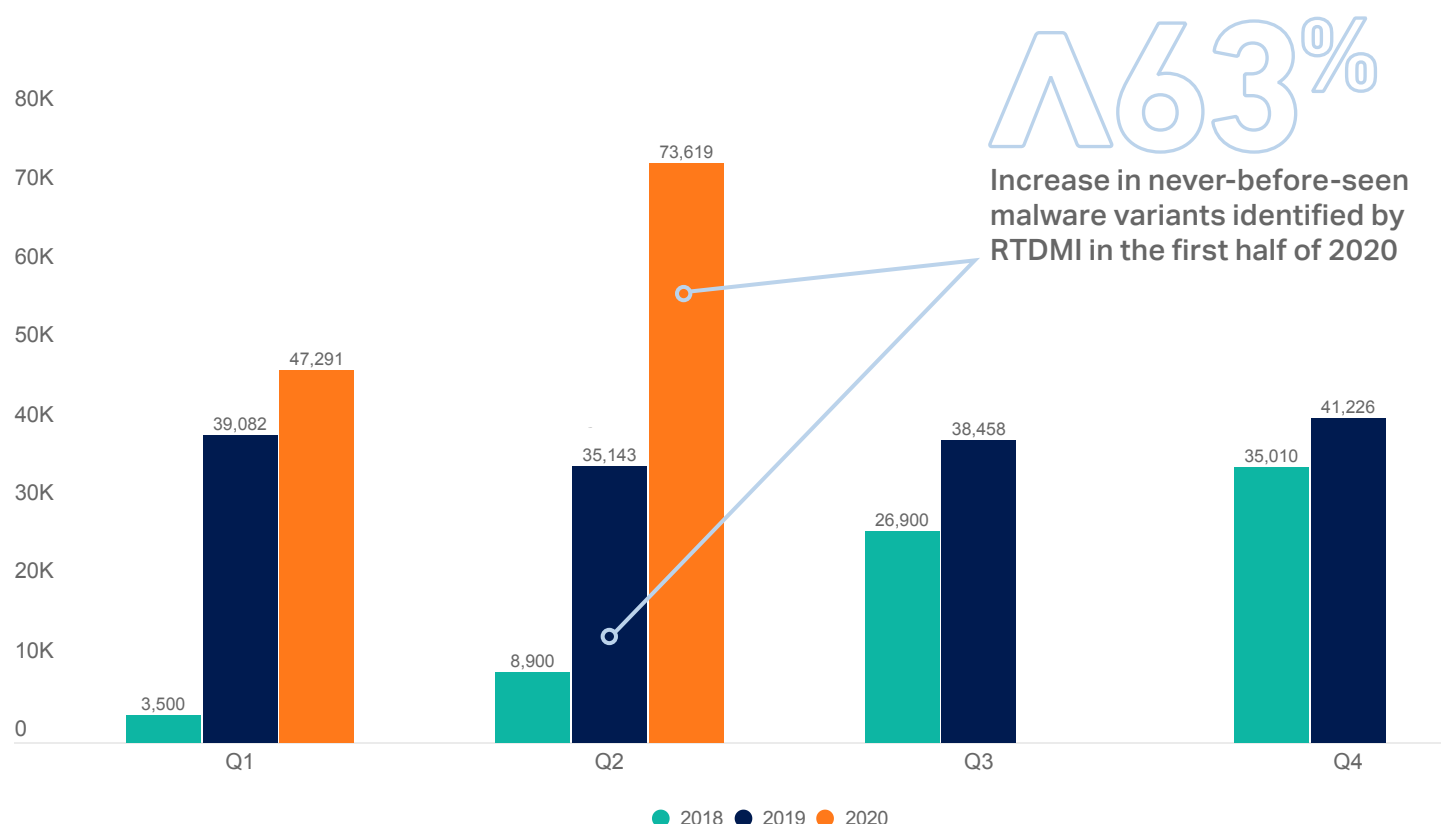
What's Hiding in Your Office Files?

The number of new malware variants found by SonicWall Capture Advanced Threat Protection (ATP) with Real-Time Deep Memory Inspection™ continues to rise: During the first six months of 2020, the pair discovered 315,395 new malware variants.

Each year has brought significant advancements, and the first half of 2020 is no exception.

So far in 2020, every month has seen significant year-over-year increases in the number of malware variants found — combined, they represent a 62% increase over 2019's first half totals.

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



Of these, 120,910 were detected by SonicWall Real-Time Deep Memory Inspection. Included as part of Capture ATP, RTDMI™ leverages proprietary memory inspection, CPU instruction tracking and machine learning capabilities 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. These are attacks that traditional sandboxes likely missed.

Overall, 63% more never-before-seen malware variants were identified by RTDMI in the first half of 2020 than were identified in the first half of 2019.

Microsoft Office Files Overtake PDFs

In the first half of 2020, Office files and PDFs made up a third of all new malicious files identified by Capture ATP. For the first half of 2019, PDFs showed an edge over Office 365 files, outpacing them 36,488 to 25,461.

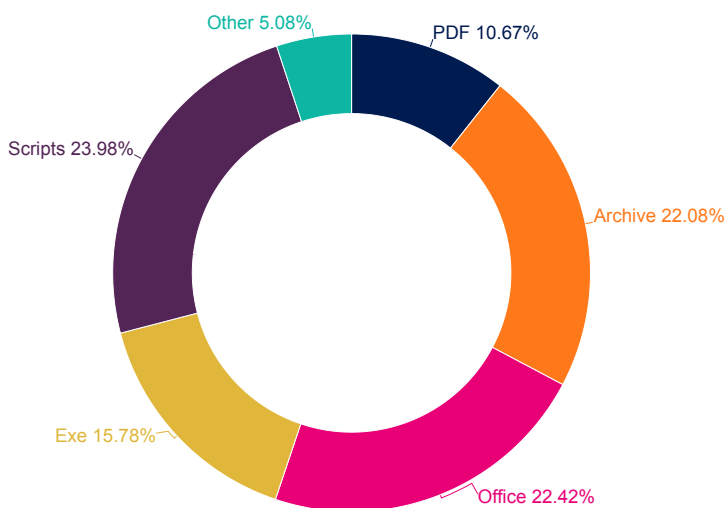
So far in 2020, we've seen a major reversal: While 8% fewer PDF files were uncovered, the number of Office files identified has exploded, climbing to 70,184 — a 176% increase.

While the overall number of new threats identified over the past six months is up significantly, there is some good news. As we've moved through the first half of 2020, both the number of malicious PDF files and the number of malicious Office files seem to have dipped slightly in the second quarter.

The bad news: just six days into the second half of 2020, SonicWall Capture Labs threat researchers have begun [observing advances in the way malicious Excel files distribute malware](#) — including new techniques to evade signature-based, anti-malware engines and hinder sandbox debugging and analysis.

This tells us: 1) The aforementioned respite will likely be brief, 2) Attackers are still focusing a significant amount of time and energy into these sorts of attacks, so we shouldn't expect a sustained drop anytime soon, and 3) Threats are becoming more evasive and more nefarious, particularly those leveraging PDF and Office files — making advanced technology like RTDMI more critical than ever.

2020 NEW MALICIOUS FILE TYPE DETECTIONS | CAPTURE ATP



▲176%

Increase in the number of malicious Office files

120,910

Number of never-before-seen malware variants identified by SonicWall RTDMI™ so far in 2020

'ZERO-DAY' VS. 'NEVER BEFORE SEEN' ATTACKS

The 'zero-day attack' is among the most well-known cybersecurity terms due to its connection to high-profile breaches. These attacks are completely new and unknown threats that target a zero-day vulnerability without any existing protections (e.g., patches, updates, etc.) from the target vendor or company.

Conversely, SonicWall tracks detection and mitigation of 'never-before-seen' attacks, which are the first time SonicWall Capture ATP identifies a signature/SHA256 as malicious. These discoveries often closely align with zero-day attack patterns due to the volume of attacks analyzed by SonicWall.

[VIEW ATTACK DATA](#)

Malware Falls in 2020

Instituting widespread work-from-home policies in response to the COVID-19 pandemic was the right thing to do, both from a business continuity standpoint and from an employee safety standpoint.

The downside is that organizations are more distributed than ever before — and this is having an impact on how cybercriminals approach the targeting and deployment of malware.

During the first half of 2020, malware fell from 4.8 billion to 3.2 billion cases, a drop of 33% over 2019's mid-year total. This drop is the continuation of a downward trend that began last November.

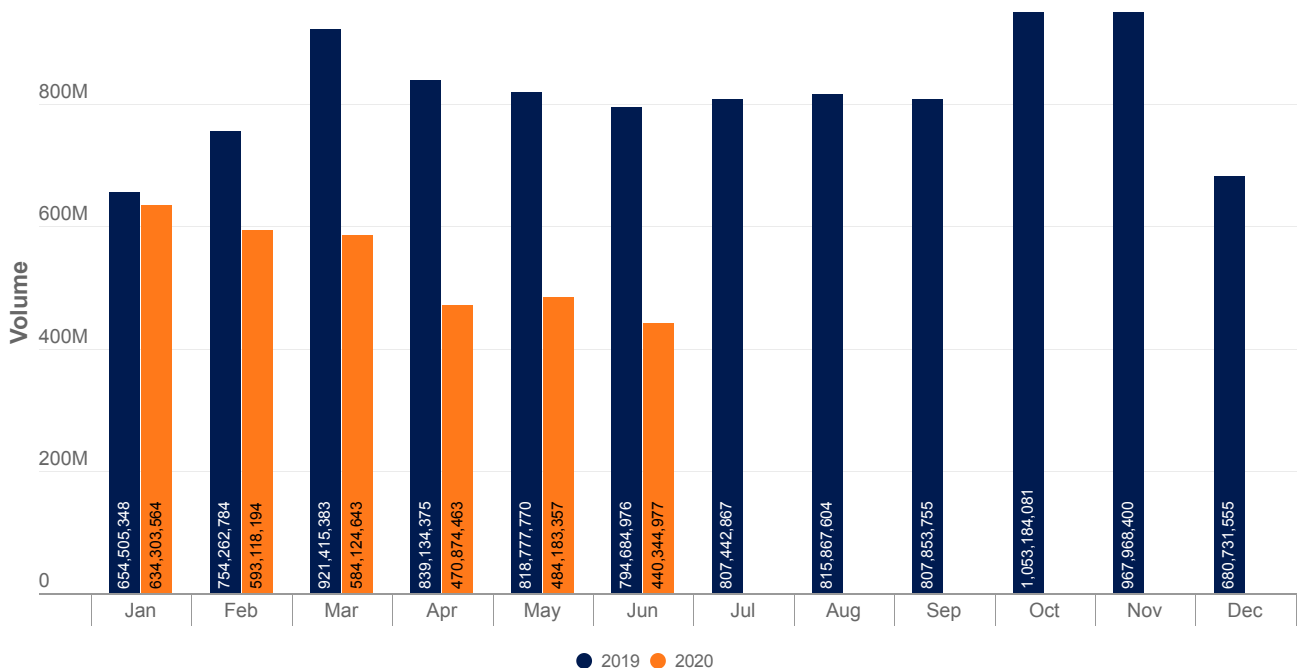
Remarkably, every month in 2020 has seen less total malware volume than *any* month in 2019. The latest malware data available, from June 2020, shows 440.3 million total malware hits — less than half of 2019's high of 1.1 billion set in October.

A WORLD OF DIFFERENCE

There are many reasons one region may see more malware than another, including:

- Allocation of cybersecurity resources
- More targeted attacks run by specific advanced persistent threats (APT)
- Attacks related to regional events such as elections, civic actions, natural disasters, etc.
- The severity of penalties levied against cybercriminals in a specific region

2020 GLOBAL MALWARE ATTACKS



Malware is clearly trending downward. Not shown: What's picking up the slack.

It's worth noting, however, that less malware doesn't necessarily mean a safer world. As we'll explore later in this report, ransomware has seen a corresponding jump over the same time period.

And across all categories of malware, SonicWall researchers have noted that attacks are both more tactical and more targeted than ever, giving them a greater chance of success.

2020 First-Half Malware Volume

COUNTRY	TOTAL HITS	YTD CHANGE
U.S.	1,899,310,121	-24%
U.K.	228,187,476	-27%
India	80,587,000	-64%
Brazil	69,583,407	-56%
Germany	26,606,635	-60%
Mexico	9,903,771	-3%
UAE	7,073,783	-74%
Japan	5,298,028	22%

The malware that we are seeing is evolving to be sneakier and more malicious. As detection tools are refined, hackers are increasingly turning to fileless malware attacks that operate in memory and [take advantage of legitimate tools such as Microsoft Windows Powershell.](#)

As the table shows, there's a large regional difference in both the amount of malware and the percentage change year over year.

But looking at SonicWall's exclusive malware spread percentage data, which tells us how widespread malware is in a given region (see next section), reveals one very important thing these countries have in common. In every case, the highest malware spread percentage occurred in March.

What's so special about March? In a typical year, nothing: This is one of the more extreme examples of the COVID-19 pandemic affecting cybercriminal behavior.



What's Your Malware Risk?

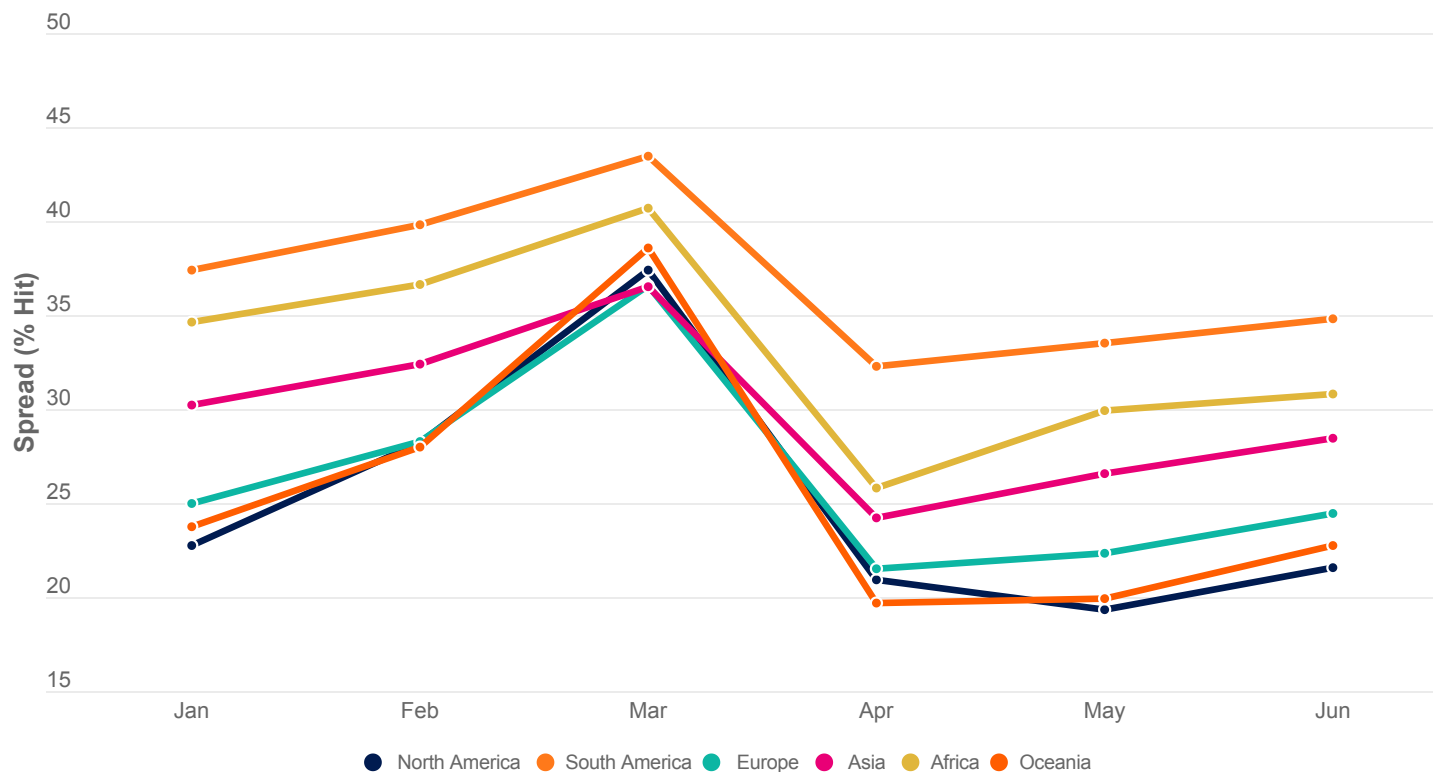
Depends on where you are.

After a spike in March, malware took a dive in April. Over the last few months, however, it's begun to rise again. This shows some connection with the rate at which COVID-19 cases are being diagnosed. As protective measures began to be lifted in May and June, cases began rising again, as did malware attacks.

There are also regional differences in both the amount of malware and the percentage change year over year, highlighting shifting cybercriminal focus.

For example, the United States (-24%), United Kingdom (-27%), Germany (-60%) and India (-64%) all experienced reduced malware volume. As cybercriminals continue shifting their focus to ransomware and more insidious and stealthy forms of malware, we may continue to see these numbers fall.

2020 GLOBAL MALWARE ATTACK TRENDS



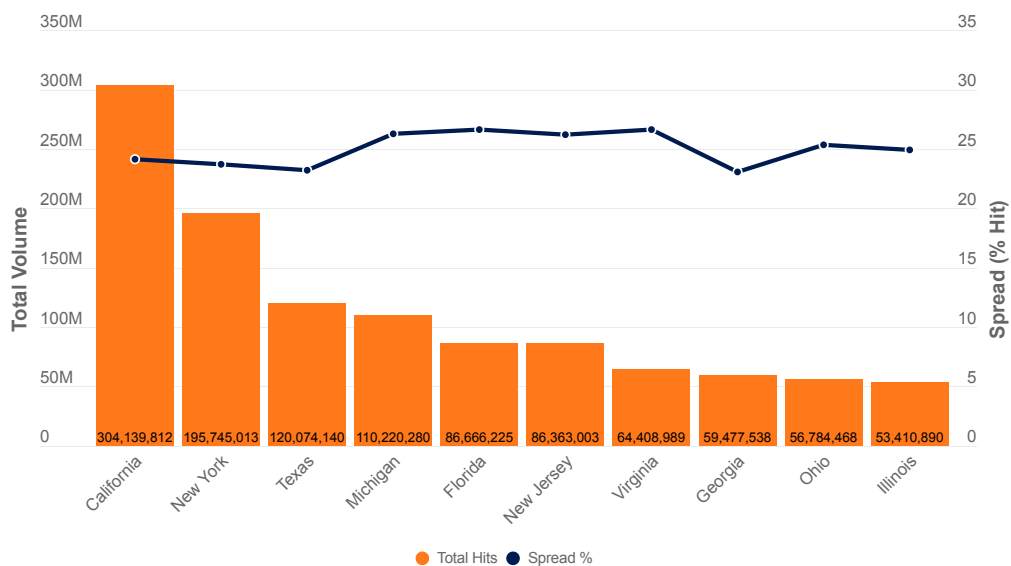
The COVID-19 pandemic sparked malware across all continents, pushing the chance an organization would see a malware attack above 35%.

Malware Risk Across U.S. States

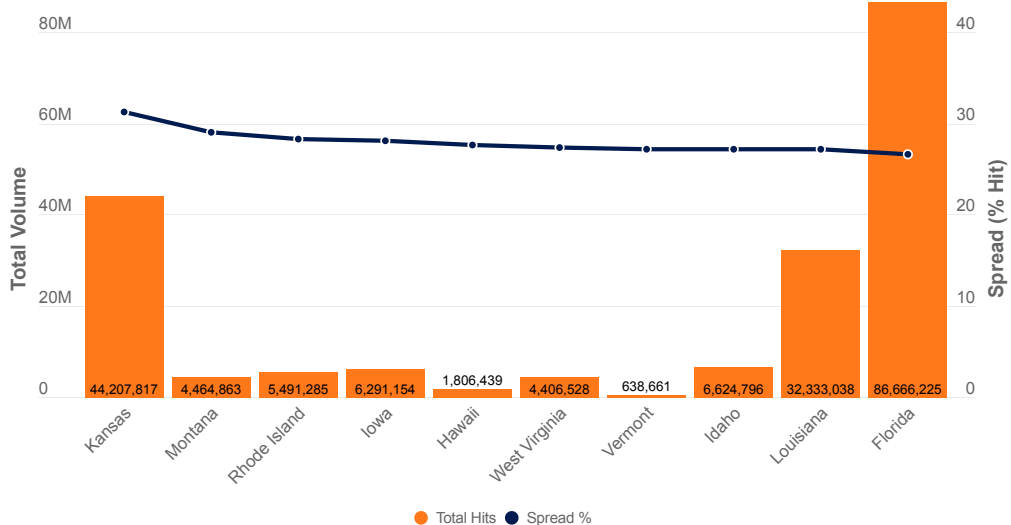
In the U.S., California had by far the largest number of malware hits, with 304.1 million total. But it isn't the riskiest state — or even in the top *half*.

You're most likely to encounter malware in Kansas, where nearly a third, or 31.3%, of sensors saw a hit. In contrast, just over a fifth of the sensors in North Dakota (21.9%) logged an attempted malware attack.

2020 MALWARE VOLUME | TOP 10 U.S. STATES

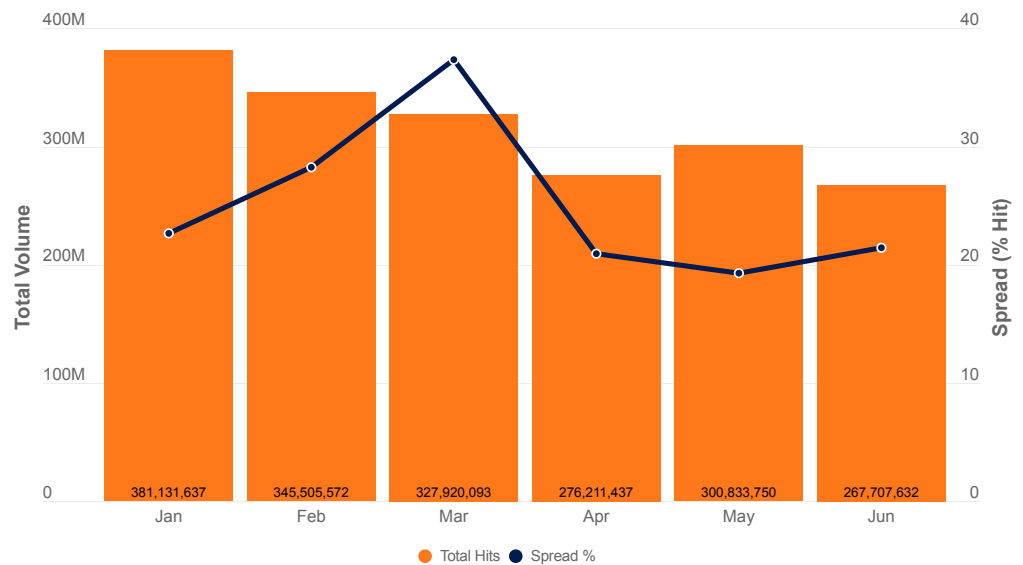


2020 MALWARE SPREAD | TOP 10 RISKIEST U.S. STATES



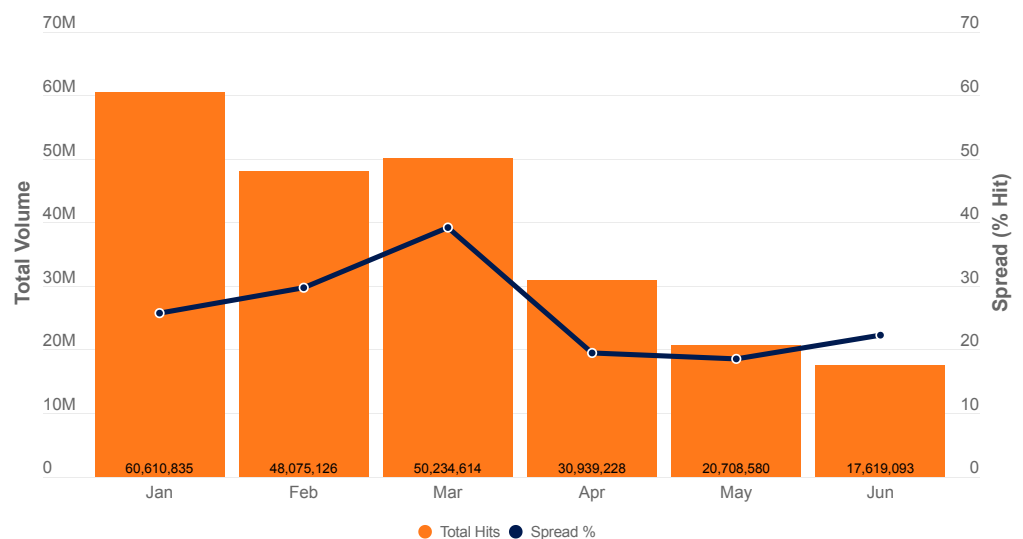
Regional Malware Volume & Risk

2020 MALWARE ATTACKS | UNITED STATES



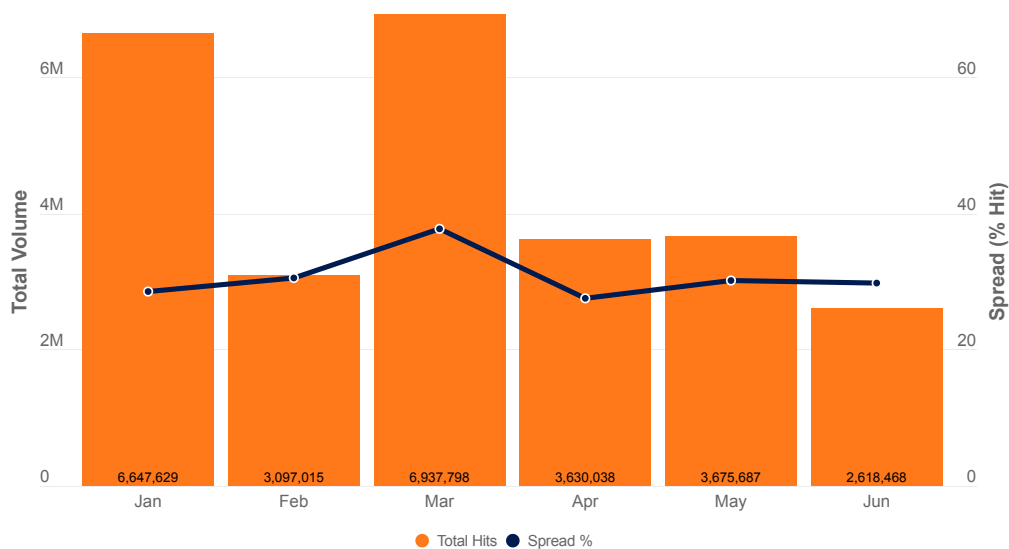
Once again, the U.S. leads in total malware, with January showing the highest volume, but March showing the largest spread.

2020 MALWARE ATTACKS | UNITED KINGDOM



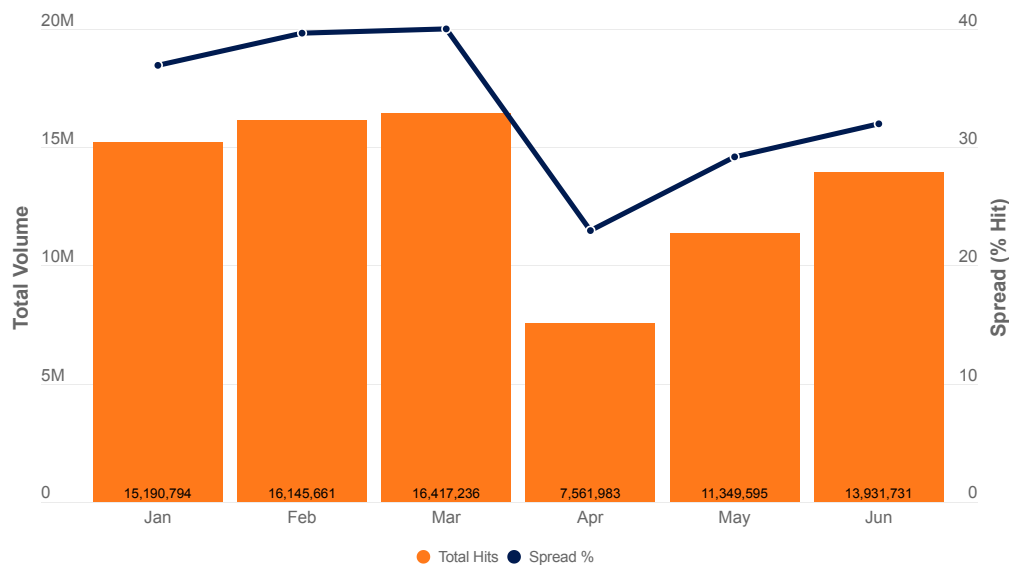
Malware spread in the U.K. has begun to rise again in Q2, but still remains well below Q1. Meanwhile, total malware continues to drop.

2020 MALWARE ATTACKS | GERMANY



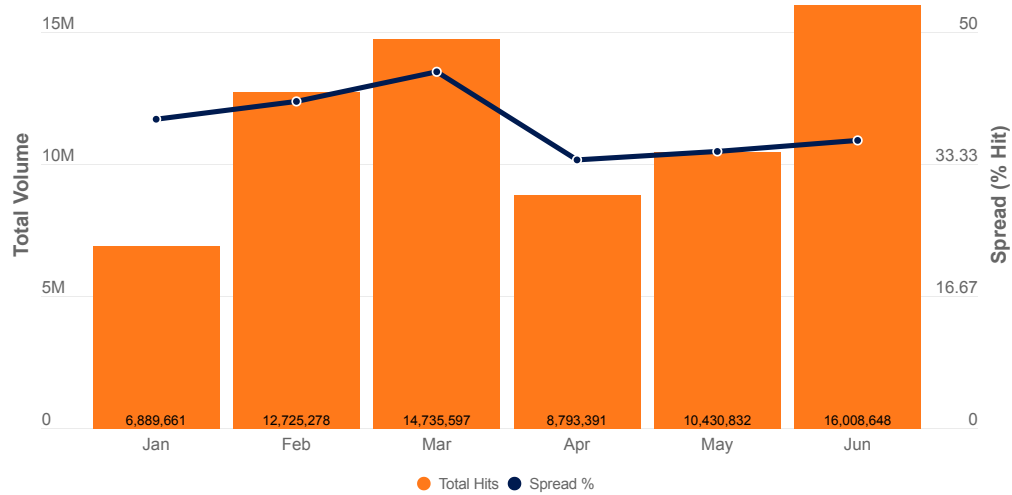
In Germany, like many other countries, malware volume hit its highest point in March — but it showed an uncharacteristic drop between January and February.

2020 MALWARE ATTACKS | INDIA



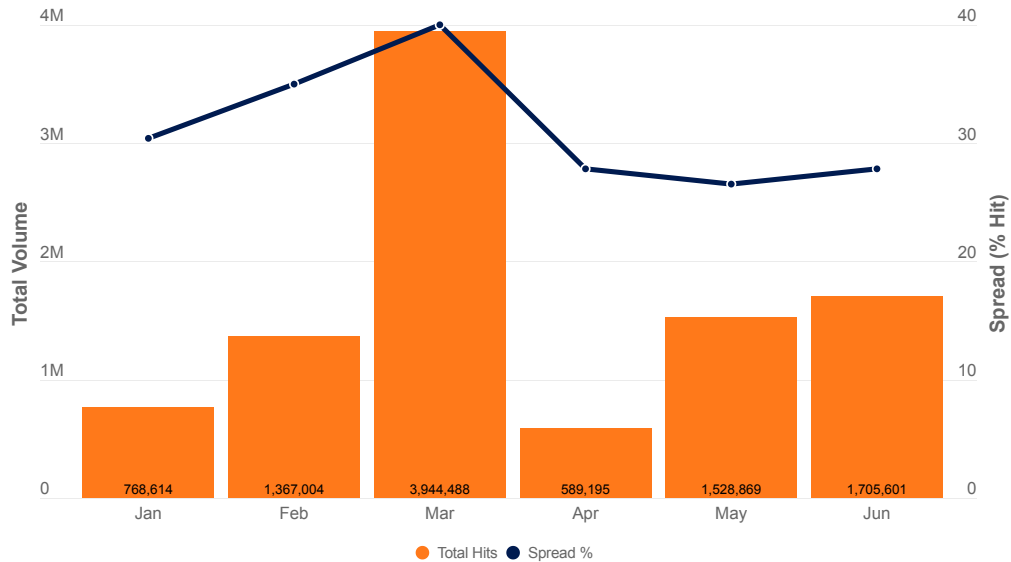
India's malware rates plummeted in April, but by June had nearly reached Q1 levels.

2020 MALWARE ATTACKS | BRAZIL



Total malware volume in Brazil hit its highest point in June, a departure from trends in other countries.

2020 MALWARE ATTACKS | MEXICO



In Mexico, malware spread is disproportionately higher than total malware numbers, with totals remaining low in every month but March.

WHAT IS MALWARE SPREAD?

SonicWall recorded 1.8 billion malware hits in the United States through June 2020 — more than four times the next-highest ranked (U.K., with 231.9 million). So why aren't these countries the riskiest?

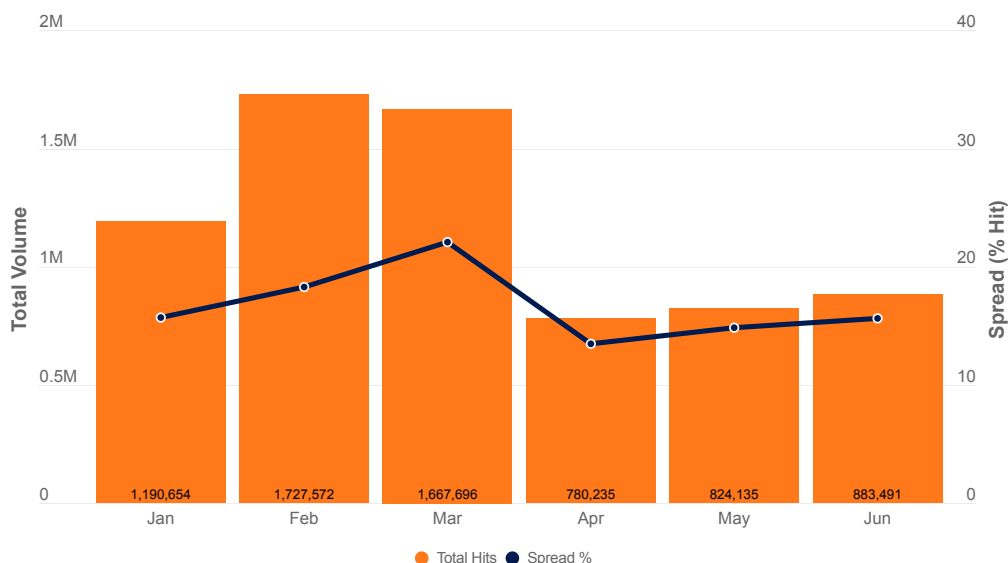
Malware totals are useful in calculating trends, but they're of limited usefulness when determining relative risk: They ignore factors such as size, population, number of sensors and more.

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.

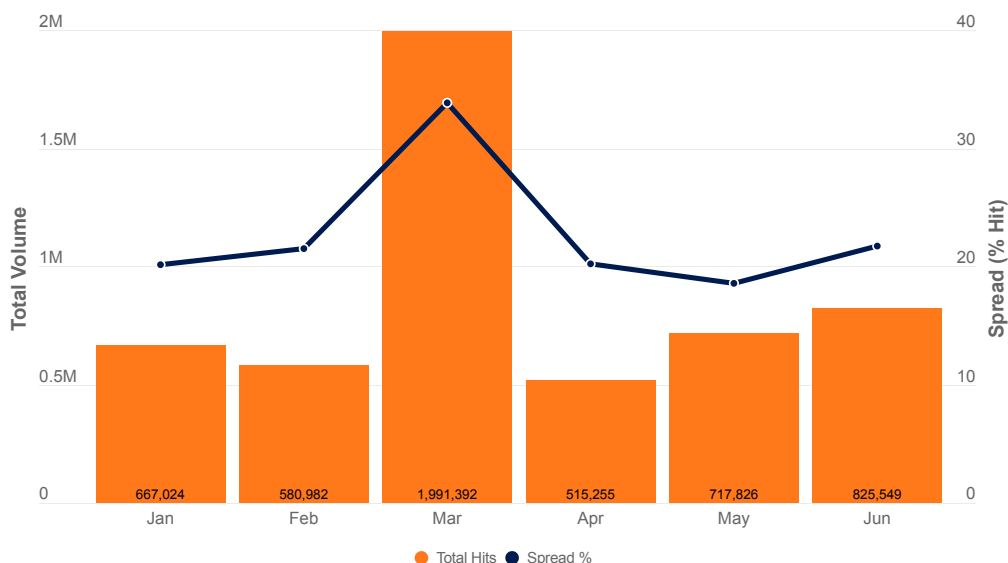
For that, you need the Probability of Precipitation, or the "chance of rain." Like the malware spread percentage, this calculation takes into account a number of other factors to provide a more meaningful risk assessment.

2020 MALWARE ATTACKS | UNITED ARAB EMIRATES



There is plenty of malware in UAE, but fortunately spread remains comparatively low.

2020 MALWARE ATTACKS | JAPAN



Japan showed the biggest month-over-month percentage change in total malware volume.

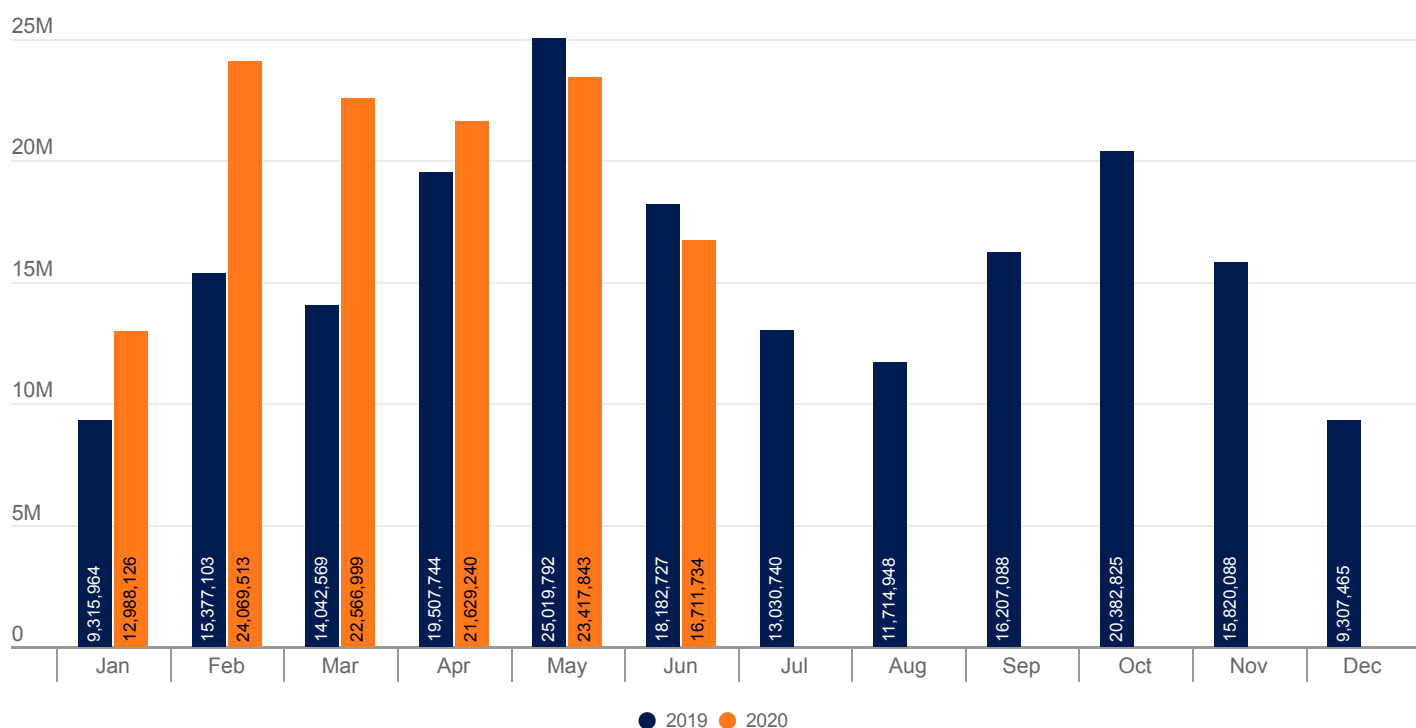
Ransomware Still on the Rise

Due to its low barrier of entry, ease of use and anonymous payouts, ransomware continues to grow — and is growing at an increasing clip. By mid-year 2019, global ransomware was up 15%. This year, it's up 20%.

Within this 20% lies a great deal of variation, however. Ransomware in the U.K. has fallen by 6% year over year, to 5.9 million, and in other places it's dropped by nearly half.

In North America, ransomware is up 105% — including a 109% increase in the United States, where it rose to 80 million.

2020 GLOBAL RANSOMWARE ATTACKS



When asked what type of cyberattacks influenced their decision to purchase a SonicWall TZ firewall, 79% of surveyed organizations said “ransomware.”



While it's impossible to determine causation, a strong correlation can be found in the ransomware graph and the patterns of COVID-19 infections. Asia saw the first COVID-19 cases, and ransomware numbers there spiked in January and March. The pandemic hit Europe next, and we see corresponding spikes there in February and April.

In North America, ransomware attacks started low in January, but by March they had nearly tripled, continuing to make more modest gains through April and May before showing a slight decrease in June, when numbers fell to their lowest point since March.

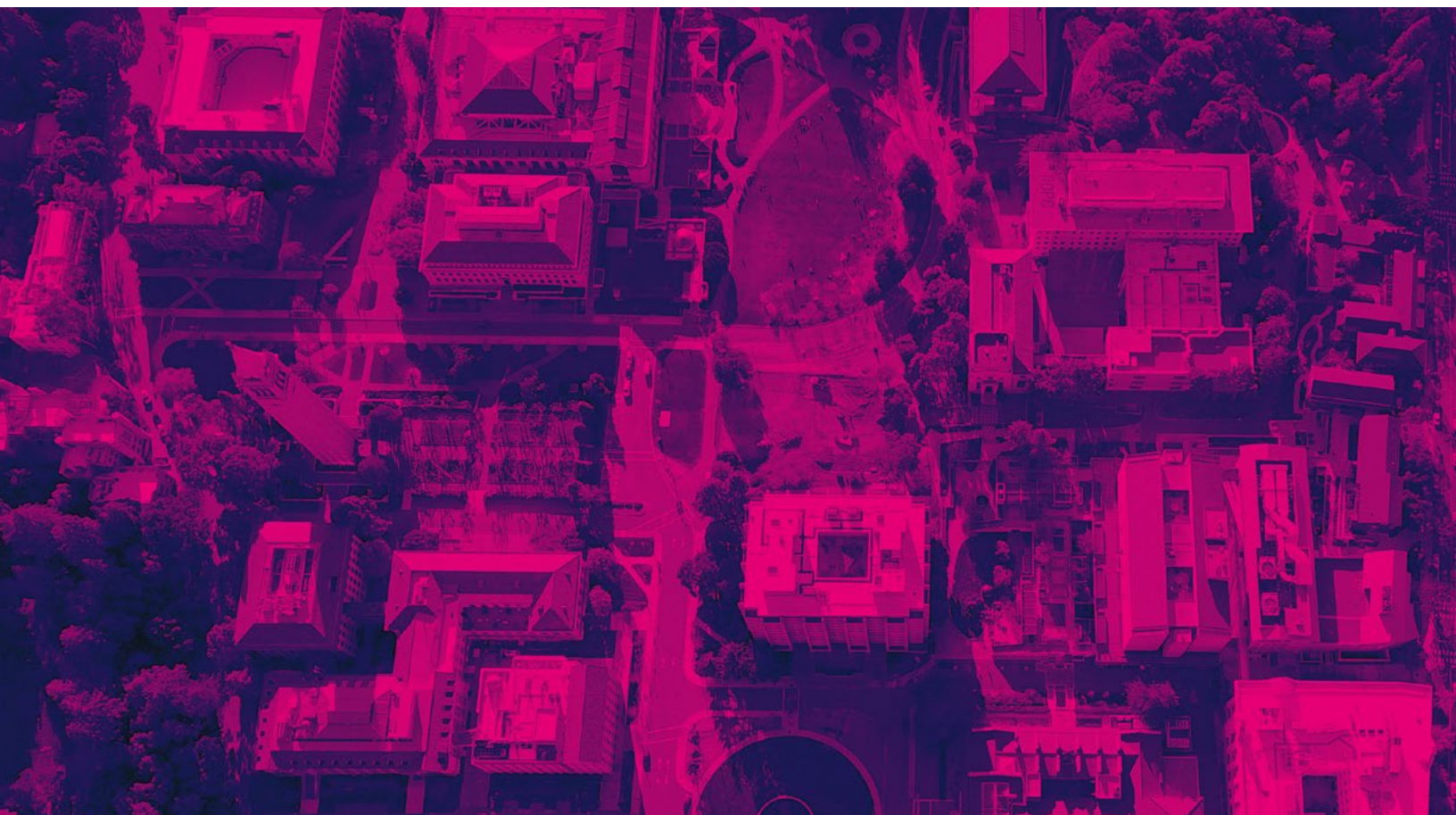
Unfortunately, COVID-19 rates have been rising again, this time even higher than before — so if this pattern holds true, North America may soon be dealing with the one-two punch of COVID-19 and rampant ransomware.

Effects of the pandemic can also be seen in global trends. In the first half of last year, ransomware peaked in May. This year, it peaked in February.

Unfortunately, exploiting a global pandemic isn't the only reprehensible thing ransomware operators did in 2020. They've also been increasing focus on so-called "soft targets" — local governments, public administration agencies, education, and even hospitals. Due to their small size and generally tight budgets, they often lack the security of larger companies.

But perhaps more importantly, the work many of these organizations do isn't just vital to the company itself — it's vital to the functioning of our society. These attacks have taken down websites, email, payroll, phone services and dispatch services, and have even attempted to toxify municipal water supplies.

"In most cases, these are not brand new exploits; [attackers] are not creating new malware," SonicWall President & CEO Bill Conner said in an interview with the *San Jose Mercury News* [regarding a \\$1.14 million ransom demand recently paid by UC San Francisco](#). "There's more easy access from home than there was in a building because you have multiple layers of security in your office."



Ransomware by Location

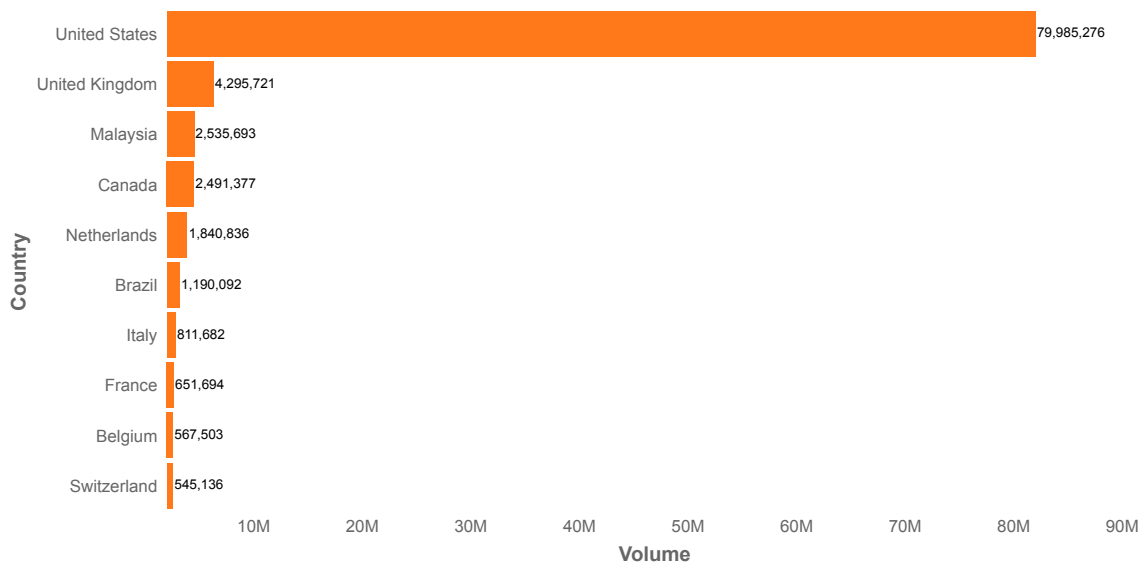
In some places ransomware is getting better. But in others, it's getting *much* worse. In terms of total ransomware, the United States had far more than any other country, with nearly 80 million ransomware attacks.

This is more than 13 times the number of ransomware attacks in the next-highest country, U.K.

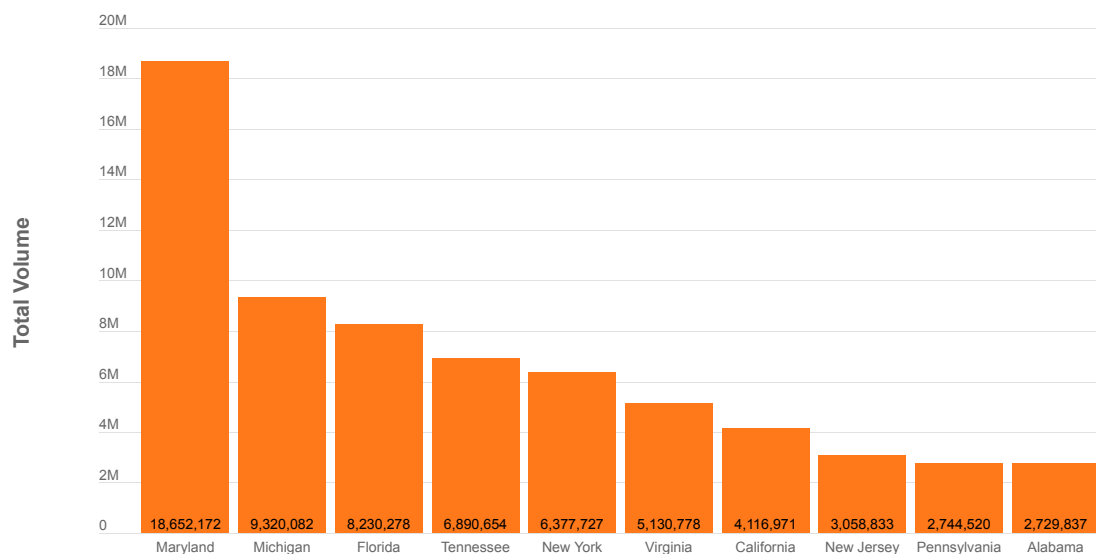
Like the country-level data, the state-level data shows one region far outpacing the rest when it comes to total ransomware attacks. Maryland had roughly twice as many ransomware attacks as the next-highest state, Michigan.

In response to a string of high-profile ransomware attacks, including one that [held the city of Baltimore's computer systems hostage for 36 days](#), Maryland has been [working to pass laws strengthening penalties for ransomware operators](#) in an attempt to reverse this trend.

2020 RANSOMWARE VOLUME | TOP 10 COUNTRIES



2020 RANSOMWARE VOLUME | TOP 10 U.S. STATES





SMALL, BUT MIGHTY

While these ransomware numbers may seem small, it's worthwhile to remember a few things. One, they're growing — and two, the stakes are rising.

According to [The New York Times](#), ransom demands are skyrocketing: the cities of Riviera Beach and Lake City, both in Florida, [recently paid out \\$600,000 and \\$500,000 ransoms respectively](#), and in early July, cybercriminals [demanded a staggering \\$14 million ransom from Brazilian power company, Light S.A.](#)

To make matters worse, many ransomware operators have taken to selling or otherwise releasing company data if the organization refuses to or cannot pay.

Even for companies that cooperate with the criminals' demands, the trouble often doesn't stop when the ransom is paid. Many organizations pay the ransoms, only to find their files are irretrievably corrupted or have been wiped out altogether. Ransomware attacks are so devastating that they've forced a number of companies out of business.



Non-Standard Port Attacks Gain Ground

Cybercriminals are increasingly using non-standard ports to evade detection and deploy malware. SonicWall found that Q1 and Q2 each set new quarterly records for these attacks.

Two new monthly records were set during this time as well: In February, non-standard port attacks reached 26% before climbing to an unprecedented 30% in May.

During that month, there was a surge in many specific attacks, such as VBA Trojan Downloader, that may have contributed to the spike. Overall, an average of 23% of attacks took place over non-standard ports so far in 2020.

While there are more than 40,000 registered ports, only a handful are commonly used. They are the 'standard' ports. For example, HTTP uses port 80, HTTPS uses port 443 and SMTP uses port 25. A service using a port other than the one

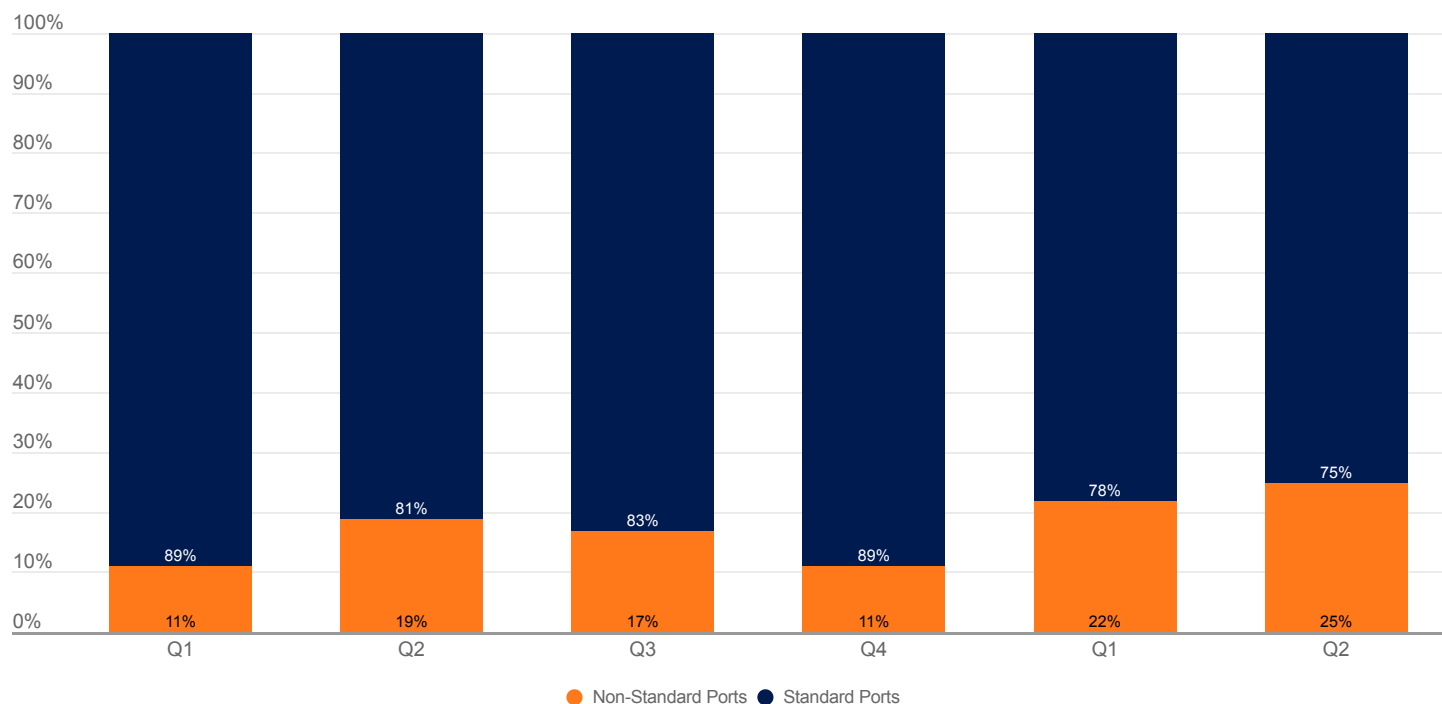
assigned to it by default, usually as defined by the IANA port numbers registry, is using a non-standard port.

There is nothing inherently wrong with using non-standard ports. But traditional proxy-based firewalls typically focus their protection on traffic going through the standard ports.

Because there are so many ports to monitor, these legacy firewalls can't mitigate attacks over non-standard ports. Cybercriminals are well aware of this and target non-standard ports to increase the chances their payloads can be deployed undetected.

Newer firewalls that are capable of analyzing specific artifacts (as opposed to all traffic) can detect these attacks. But until the number of organizations deploying these more advanced solutions rises considerably, we're likely to see a continued increase in these sorts of attacks.

2019-2020 GLOBAL MALWARE ATTACKS



IoT Attacks Spike 50%

A remote workforce can introduce many risks — some of them obvious, some of them less so. While the increased dangers of things like phishing attacks have been widely reported on, few are talking about the dangers presented by refrigerators, doorbells or gaming consoles.

While most people have at least some IoT devices, many don't have the time or expertise to adequately secure them. But when these devices connect to endpoints that connect to corporate networks, they can provide cybercriminals an open door into what may otherwise be a well-secured organization.

IoT attacks were rampant the first three months of 2020, as January, February and March each racked up more attacks than their 2018 and 2019 counterparts *combined*.

Since January, SonicWall recorded 20.2 million IoT attacks (+50%). If the current pattern holds, total IoT attacks will surpass both 2018 and 2019 levels.

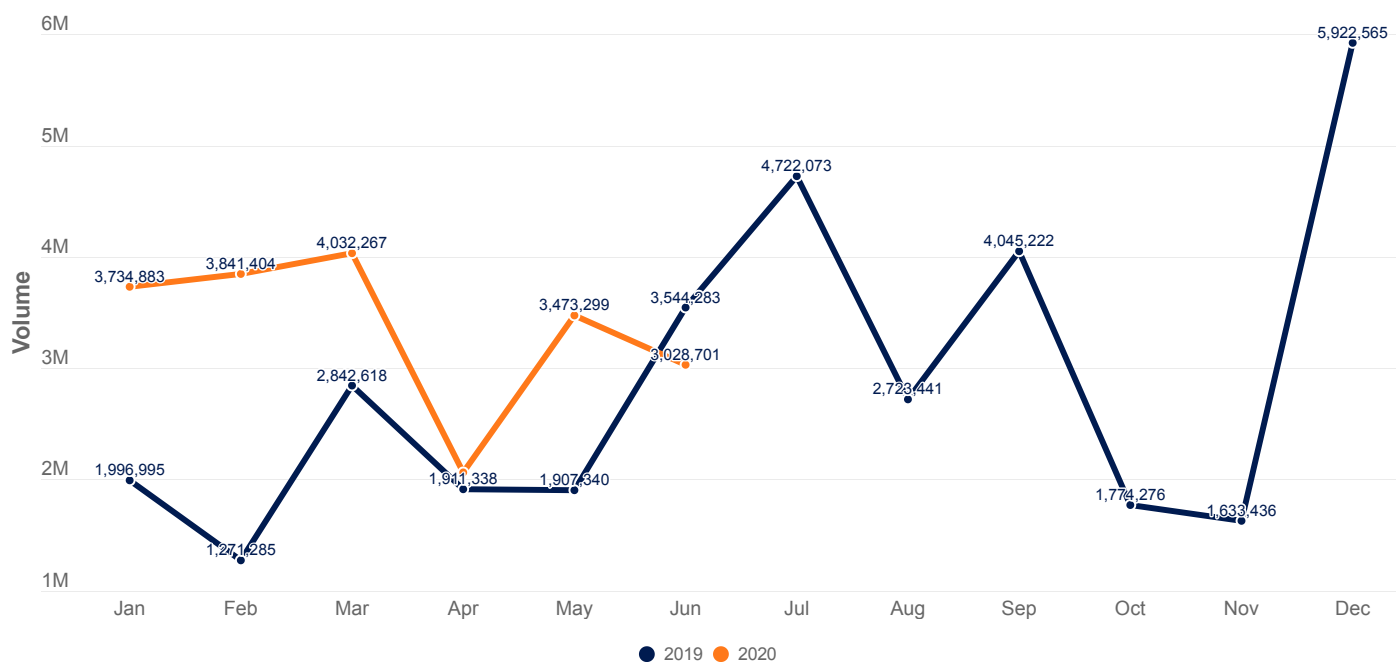
If, on the other hand, 2020 follows the pattern of previous years — which saw a greater number of IoT attacks in the latter half of the year than the first — this year's attack total could wind up surpassing the totals for 2018 and 2019 put together.

According to one source, [31 billion IoT devices will be connected to the web this year](#), and roughly 93% of enterprises and 80% of industrial manufacturing companies will adopt IoT technology.

This widespread adoption — combined with lax manufacturing standards and the difficulty IT has traditionally had in being able to see, let alone control and secure, some of these devices — makes them an attractive target for criminals.

Though there have been cases where IoT devices have been compromised for their own sake, the primary motivation is to use these devices as a back door into the network, allowing them to deploy serious forms of compromise with lower chances of detection.

2020 GLOBAL IoT MALWARE VOLUME





HOPE ON THE HORIZON?

At the end of June the European Telecommunications Standards Institute, the organization responsible for the standardization of information and communications technologies, released a new cybersecurity standard for IoT devices.

Developed in collaboration with governments, academic institutions and industries, [ETSI EN 303 645](#) is intended to curb the epidemic of attacks resulting from criminals gaining control of these devices.

These standards will apply to connected children's toys and baby monitors; door locks; smart cameras and TVs; health trackers; smart appliances and home assistants; and more. The label has already been awarded to a number of products that merit these standards.

While this may mark a sea of change in how IoT devices are secured going forward, the large number of smart devices sold prior to these standards mean IoT device attacks will continue being a problem for a long time.



Encrypted Threats Make Late Surge

During the first half of 2020, 1 in 12 SonicWall customers with DPI-SSL turned on (8.46% average) saw malware on encrypted traffic. While the total number of encrypted malware attacks is down 32% over this time last year, a closer look shows some disturbing trends.

Aside from a large slide between January and February and a tiny dip in May, these attacks have been on an upward trajectory — sometimes a steep one.

Moreover, the total amount of encrypted malware in June, 378,736, is not only the highest number of encrypted threats recorded in all of 2020, it's also higher than at any point in the latter half of last year.

Most regions echo the overall drop in encrypted threats, but Asia was a huge exception. Encrypted threats in Asia didn't just rise, they skyrocketed, resulting in an increase of 175%. Most of this was driven by the month of January, which racked up roughly 10 times the average number of encrypted threat hits as the rest of 2020.

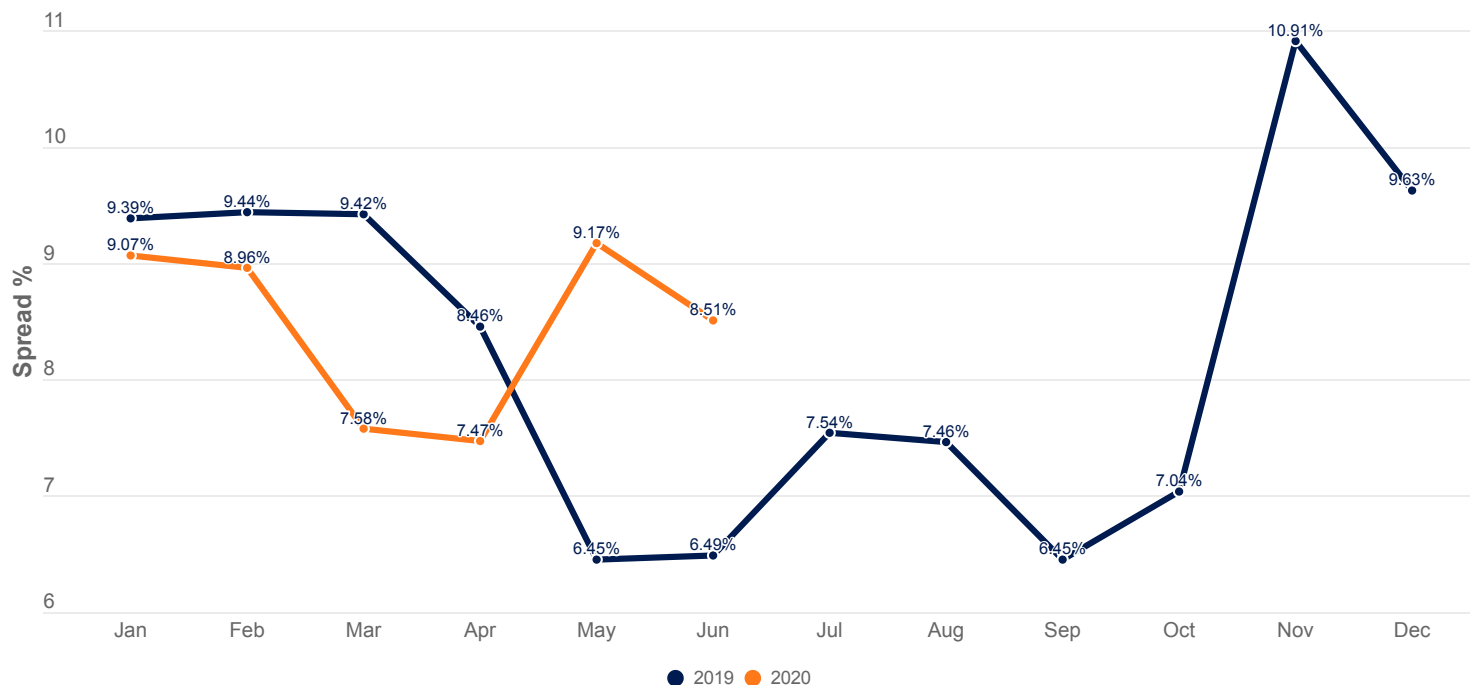
WHAT ARE ENCRYPTED THREATS?

In simple terms, SSL (Secure Sockets Layer) can create an encrypted tunnel for securing data over an internet connection. TLS (Transport Layer Security) is a newer, more secure version of SSL.

While TLS and SSL provide legitimate security benefits for web sessions and internet communications, cybercriminals are increasingly using these encryption standards to hide malware, ransomware, zero-day and more.

Traditional security controls, such as legacy firewalls, lack the capability or processing power to detect, inspect and mitigate cyberattacks sent via HTTPS traffic, making this a highly successful avenue for hackers to deploy and execute malware within a target environment.

2020 ENCRYPTED MALWARE SPREAD



Cryptojacking: 2020's Comeback Kid

When Coinhive, by far the largest legitimate cryptocurrency mining operation, closed down in March 2019, the death of cryptojacking seemed imminent — and the 78% drop in attacks between July 1 and Dec. 31 of last year seemed to drive the final nail into its crypto coffin.

But in what is perhaps 2020's most dramatic reversal, cryptojacking rallied in the first half, showing modest increases in Europe and a number of other regions. More surprising still, North America recorded an increase of 252%, defying all expectations. By June, there was only one region where figures met last year's predictions: In Asia, cryptojacking has ceased almost entirely, falling 97% year over year.

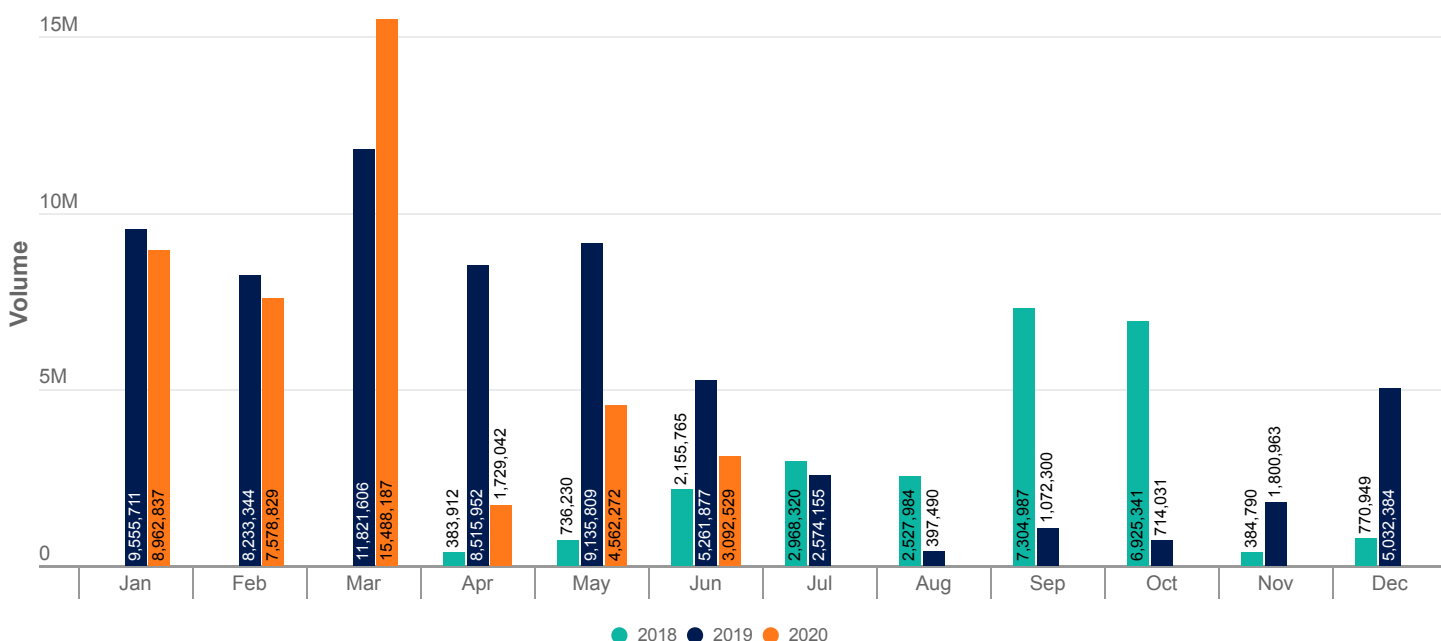
Based on SonicWall analysis, not only did the shuttering of Coinhive fail to kill cryptojacking — it didn't even properly kill Coinhive.

During the first half of 2020, *nine months* after Coinhive ceased operation, two of the top 10 cryptojacking signatures SonicWall identified belonged to Coinhive, demonstrating that this malware is still alive — even if they are just leftover relics of past attacks.

An ongoing shift has been observed, however, from Coinhive to XMRig, another Monero cryptocurrency miner. An open-source code that is readily available, iterations of XMRig malware accounted for nearly 30 million of the 32.3 million total cryptojacking hits SonicWall observed in 2020.

These miners are becoming more sophisticated, with the addition of abilities such as being able to target and kill rival miners. It's also becoming more versatile: In April, [an XMRig cryptominer infected Kubeflow, a machine-learning toolkit for Kubernetes](#), and in June, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) [announced that XMRig was among the three detection signatures](#) that make up over 90% of identified potential threats.

2020 GLOBAL CRYPTOJACKING VOLUME



It remains difficult to fully align cryptojacking attempts (and criminal intentions) with cryptocurrency value, but correlation can frequently be observed. In most of the first half of 2020, prices of Monero and ZCash, two anonymous cryptocurrencies used in the overwhelming majority of cryptojacking cases, were up.

While it might be tempting to attribute March's huge jump in cryptojacking to the pandemic, that doesn't seem to be the case here. Comparing the first half of 2020 with the first half of 2019, you can see that the past six months basically follow the same pattern. While the pandemic may have contributed to the severity of the spike, the spike itself was right on time.

Notable Cryptojacking Malware in the First Half of 2020

- **JAN 24** – The SonicWall Capture Labs team [encountered a cryptominer](#) that pretends to be a media player, even loading a .wav file to hide its real intent.
- **APRIL 18** – A malicious Zoom videoconferencing app installer [bundled with a cryptocurrency miner](#) was identified. It installs the genuine program, but also installs the cryptominer, which runs in the background.
- **JULY 10** – A [cryptominer that comes as a WinRAR self-extracting archive](#) and can connect and download additional files, manipulate access controls and file attributes, change network configuration, and more was identified. Notably, the file is capable of killing and deleting running rival cryptominers.

Cryptojacking, also known as malicious mining, occurs when cybercriminals install malicious programs on target computers without the user's knowledge, allowing them to harness the victim's processing power to mine cryptocurrency. This can be done through fileless malware, through a website with a mining script embedded in the browser, and more.

Cryptojacking delivers something of a one-two punch to victims — not only are they at risk of data compromise, they're also stuck with the enormous energy bills that accompany mining cryptocurrency. [According to Ars Technica](#), cryptomining is thought to consume almost half a percent of the world's energy consumption.

Top 10 Cryptojacking Signatures in 2020

1.	XMRig.XMR_11	27,887,268
2.	CoinMiner.C_4	1,629,068
3.	XMRig.XMR_4	1,420,685
4.	Coinhive.JS_2	728,519
5.	XMRig.XMR_8	314,789
6.	XMRig.XMR_3	313,667
7.	CoinMiner.BRL	27,447
8.	CoinMiner.A_39	11,225
9.	BitCoinMiner.IY	5,714
10.	Coinhive.JS	2,445

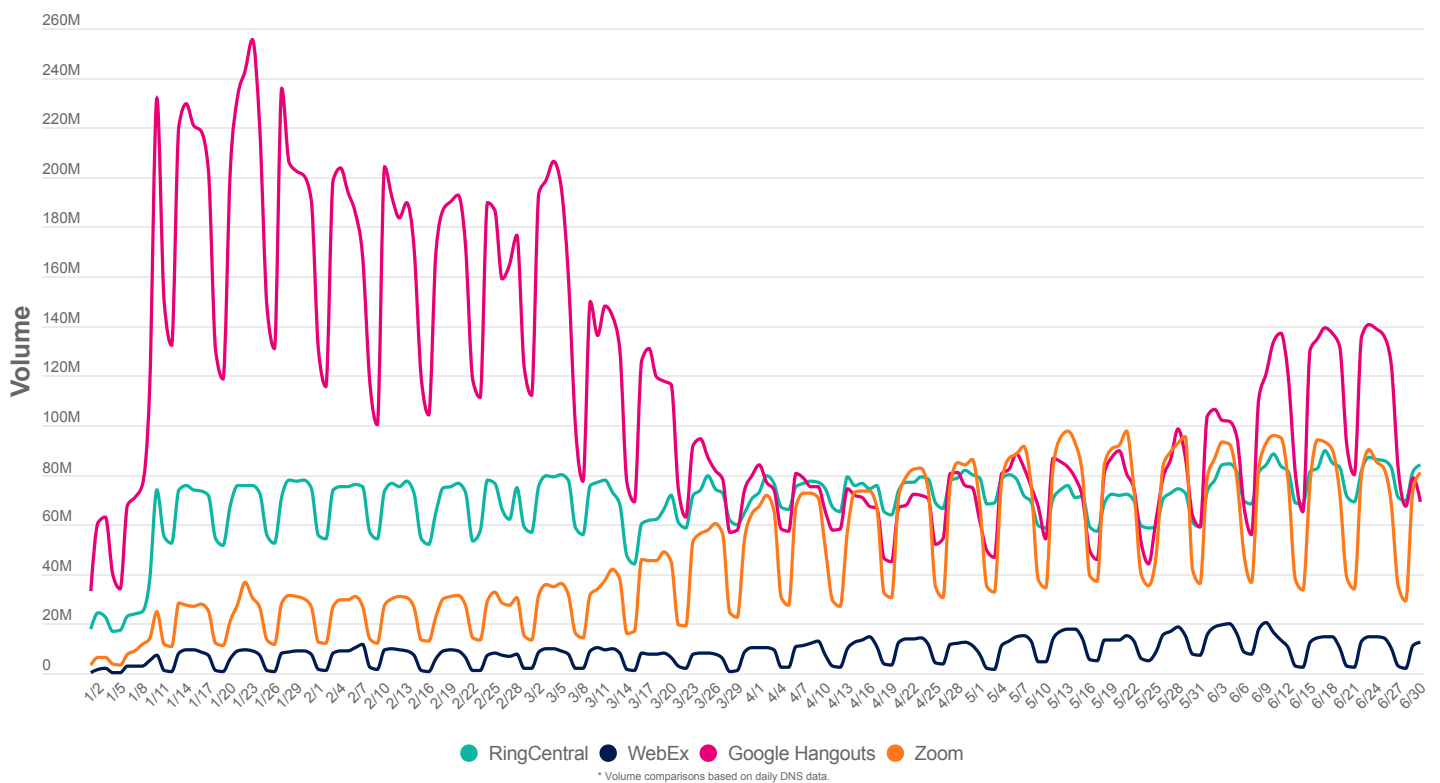
Connection in the Time of COVID

As expected, the COVID-19 pandemic has massively influenced the adoption and use of video-conferencing software, but it has affected different solutions in different ways.

Based on SonicWall's daily DNS and traffic data, Google Hangouts — one of the most popular globally before the onset of the pandemic — lost 73% of its traffic by mid-April. Clearly this wasn't the result of fewer meetings, however. WebEx, while remaining remarkably consistent, still recorded a slight rise in overall usage. RingCentral also showed a modest increase.

The real success story here is Zoom. Now a household name, Zoom had eight times as much traffic by mid-June, a 632% increase.

2020 GLOBAL VIDEO CONFERENCE SERVICE USAGE



It's worth mentioning, however, that the app is not without its security risks. Its popularity has been a double-edged sword, as [hackers](#), [pranksters](#) and [other bad actors](#) wrongfully exploited the solution to wreak havoc.

Despite Zoom lagging significantly behind Google Hangouts for most of the year, the SonicWall Capture Labs threat research team spotted at least five types of malware aimed at defrauding users attempting to use Zoom:

- **APRIL 23** – SonicWall Capture Labs threat researchers observed several malicious Android apps that use the name, user interface (UI) elements and parts of code of the legitimate Zoom app to infect unsuspecting users.
- **APRIL 18** – A malicious Zoom videoconferencing app installer bundled with a cryptocurrency miner installs the legit program to avoid suspicion, while the cryptominer runs in the background.

In response to a series of high-profile attacks, [Zoom has instituted new password protection measures and added a new layer of encryption](#) to help make its platform safer and more secure.

Video-conferencing software traffic also reveals a lot about our habits. Perhaps unsurprisingly, Sunday is the slowest day of the week for videoconferencing software — though Sundays still show significant traffic, giving credence to the idea that we've shifted to an "anywhere, anytime" work reality.

RingCentral illustrates the most extreme example of this: Despite having less of a consumer reputation as a social app than either Zoom or Google Hangouts, the percentage difference between its heaviest traffic days and lightest traffic days was the smallest of the four.

So when *are* people meeting? Across all four videoconferencing solutions, the most popular meeting day was Tuesday.





About the SonicWall Capture Labs Threat Network

Intelligence for the mid-year update to the 2020 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



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

Refer to our website for additional information.

www.sonicwall.com



© 2020 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.