2021

SONICWALL CYBER THREAT REPORT

Cyber threat intelligence for navigating the new business reality

sonicwall.com | @sonicwall

Table of Contents

A Note From Bill

The World Economic Forum asked respondents in a recent study which dangers will pose the largest threat to the world over the next two years.

Unsurprisingly for a pandemic year, "infectious diseases" and "livelihood crises" topped the list. But rounding out the top four were "extreme weather events" and "cybersecurity failure."

And the latter concerns have more in common than you may think, particularly now. In fact, the cybersecurity challenges of 2020 have played out a bit like an extreme weather event: They've come on suddenly, most found themselves unprepared, there was significant damage and, in some cases, businesses are still sorting through the rubble.

While history will note the still-untold number of social, economic and political changes brought by the pandemic, it also brought about a sea change in cybersecurity. As COVID-19 spread across the globe, an unprecedented wave of cybercrime followed in its wake, driving the rates of almost every sort of cyberattack up (sometimes *way* up.)

This culminated in the discovery of a successful breach of software company SolarWinds in December — which has become widely regarded as one of the largest and most extensive cyberattacks of all time. (Read more about the SolarWinds incident on page 7.)

The event also brought lessons, the foremost being the importance of ***cyber resiliency***.

Cyber-resiliency means expanding your focus beyond simply securing your network and your data, to ensuring business continuity in the event of an attack or some other unforeseen event.

Almost all organizations in high-stakes environments — whether it be power plants, government agencies, law enforcement or another group depended on to fulfill a vital need — have a philosophy of resiliency. It may be known as a contingency plan, a fallback, or even by a code name, but the idea is the same: This is how we maintain operations when things don't go as expected.

And 2020 — a year in which *very little* went as expected — highlighted the danger of approaching cyber-resiliency as merely a best practice. It is vital that we expand our thinking from just "How are we going to prevent an attack?" to also include "What will we do when (not *if*) we get attacked?"

We encourage you to review the threat intelligence found only in the *2021 SonicWall Cyber Threat Report*. This latest cyber threat data offers a look at how cybercriminals shifted and refined their tactics in a world greatly changed … and an idea of what they might do amid the uncertain world that lies ahead.

Bill

BILL CONNER
PRESIDENT & CEO
SONICWALL

INTRODUCTION

Cybercriminals' Perfect Storm

Cybercriminals have always been opportunists, and the 2020 COVID-19 pandemic offered more proof of this than perhaps any other event before it.

Threat actors are becoming more powerful, more aggressive and more numerous, increasingly abandoning the tendency to look for the biggest quarry in favor of attacking the least defended.

And 2020 was rife with vulnerable targets.

From a new class of remote workers, millions strong and in many cases completely unaware of the security implications and best practices tied to such a power shift …

… to a panicked and confused populace, some of whom were willing to trust anything claiming to offer more information about COVID-19 …

… to hospitals, overworked and over capacity …

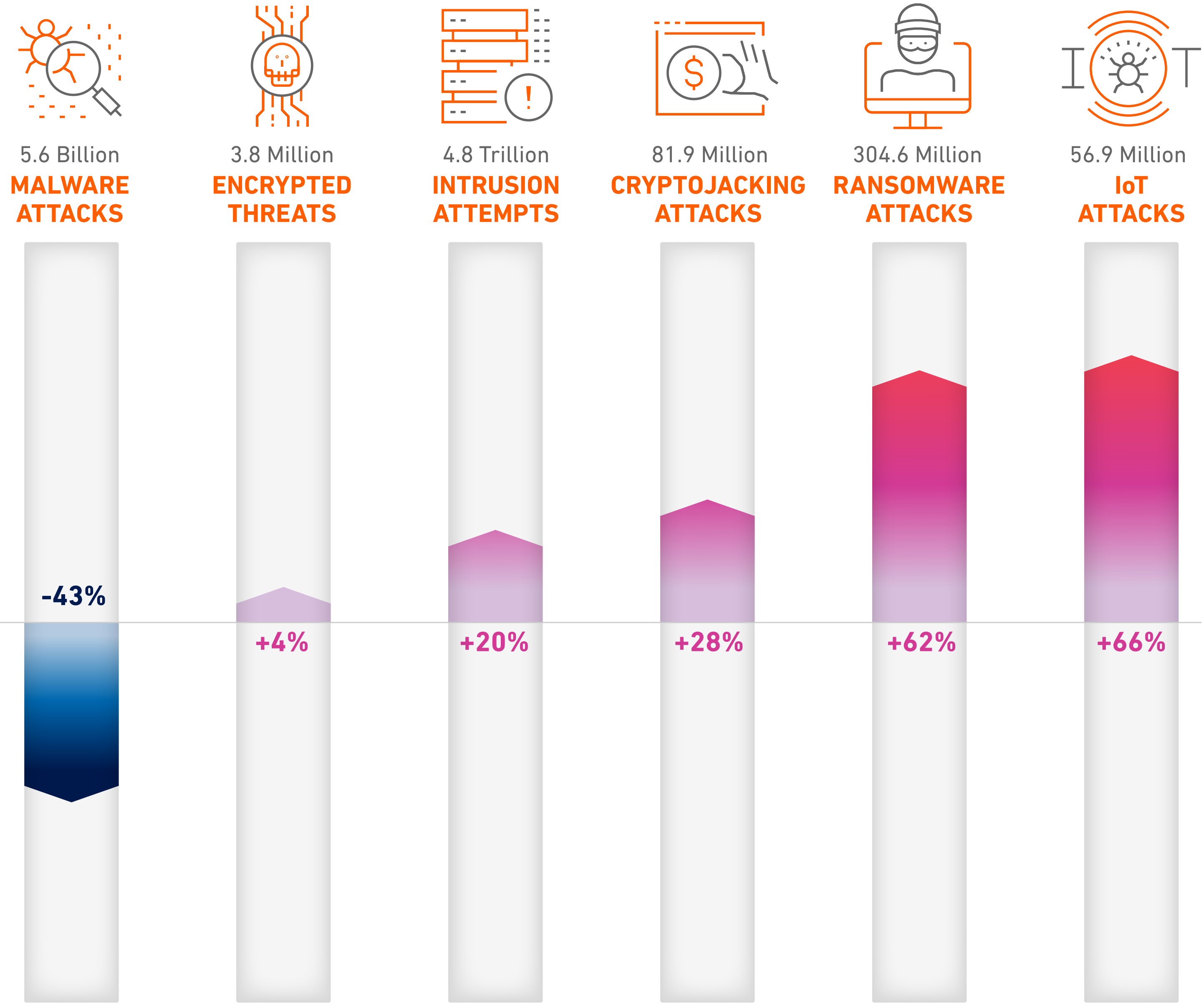
… cybercriminals found themselves in the midst of a perfect storm of opportunity. The combination of cloud-scale infrastructure; widespread availability of attacker tools such as PowerShell, Mimikatz and Cobalt Strike; and anonymous cryptocurrency payment has allowed threat actors of all sizes to inflict the sort of heavy damage typically associated with the most sophisticated nation-state campaigns. And many of them rode this perfect storm to untold riches as their targets faced devastation on many fronts.

In 2020, SonicWall Capture Labs threat researchers recorded 5.6 billion malware attacks — a sharp decrease from the previous year. But this isn't cause for celebration. With many employees working from home, cybersecurity vendors are losing visibility into traffic, and potential attacks along with it. So this number may in fact be much higher.

Worse, almost across the board, we've seen cybercrime numbers pushed up, in several cases to new records.

While it's unclear whether cybercrime's perfect storm will continue to rage into 2021, it's already apparent that the confluence of factors at work over the past year has pushed cybercrime to a new level, requiring increased security, vigilance and cunning as we move into the new year.

2020 Global Cyberattack Trends



Year-Over-Year Change, 2019-2020

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.

Top Data Exposures of 2020

We've alluded to the fact that there aren't many bright spots in this year's Cyber Threat Report — but this is one of them. In 2020, the largest breach affected 440 million — less than a quarter as many as 2019's largest breach, which affected more than 2 billion.

Unfortunately, we can't say this list represents a triumph. While the last two entries on this list may be small in terms of number of records exposed, the ripples of these breaches are shaking large multinational corporations and federal governments to their core, and may be felt for years, if not decades, to come.

Top Data Breaches

NAME	INDUSTRY	REPORT DATE	NUMBER OF RECORDS
Estée Lauder	Skin Care	1/30/20	440 million
Microsoft	Software	1/22/20	280 million
Facebook	Social Networking	4/1/20	267 million
MGM Grand Hotels	Hospitality	7/14/20	142 million
Pakistani mobile users	Telecommunication	5/6/20	44 million
Wishbone	Social Networking	5/20/20	40 million
Vetrafore	Software	11/13/20	27.7 million
Unacademy	Education	5/7/20	22 million
Bigbasket	Online Grocery Store	10/30/20	20 million
Couchsurfing	Social Networking	7/23/20	17 million
Home Chef	Food Delivery	5/22/20	8 million
Marriott International	Hospitality	3/31/20	5.2 million
Dunzo	Delivery Services	7/29/20	3.4 million
Edureka	Education	9/30/20	2 million
Denmark's government tax portal	Government Services	2/10/20	1.26 million
Zoom	Software	4/14/20	500,000
Magellan Health	Healthcare	5/13/20	365,000
WhiteHat Jr	Education	11/25/20	280,000
Defense Information Systems Agency (DISA)	Combat Support	2/24/20	200,000
Nintendo	Consumer Electronics	4/24/20	160,000
U.S. Department of Veterans Affairs	Government Services	9/15/20	46,000
NHS, Wales	Healthcare	9/15/20	18,105
SolarWinds	IT Management Software	12/13/20	18,000
FireEye	Cybersecurity	12/8/20	Red Team Tools

Power Shifts Changing Future of Cybersecurity

During the height of the COVID-19 global pandemic, the threat landscape reached a critical tipping point that will change cybersecurity forever. The new work-from-home reality brought about exponentially greater attack surfaces to introduce an untold number of new vectors and infinite opportunities for disruption.

Cloud-scale infrastructure and widely available attacker tools (PowerShell, Mimikatz and Cobalt Strike, all developed for legitimate use), combined with anonymous payment via Bitcoin, are tilting the playing field and arming threat actors of all sizes. This is empowering criminal groups new and old with the ability to launch both global and targeted cyberattacks — from anywhere in the world — with the same force, volume and damaging impact as nation-state campaigns.

The results of this dramatic shift are resulting in some of the most damaging attacks the industry has ever seen.

Highly Sophisticated Threat Actors Target SolarWinds Supply Chain

In November, FireEye reported an attack on its own network and quickly concluded the attack originated from a compromised version of the Orion product from American software company SolarWinds. Shortly after, in December, SolarWinds confirmed that its product Orion had been targeted in an extensive supply chain attack.

While supply chain attacks have been around for some time in the field of cybersecurity, they took on a minor role in the headlines due to their very targeted and esoteric nature. That, of course, has changed with the massive SolarWinds hack. The Orion software is used to manage IT networks and, therefore, makes a perfect target, since a successful attack places the attacker in a very privileged position on a network, allowing them to burrow and embed themselves further.

According to FireEye, the threat actor was able to hide malicious code in software updates provided to Orion customers, and through these trojanized updates gain a foothold in the network through which to gain elevated credentials.

The trojan family, dubbed SUNBURST, was disguised as a legitimate component of Orion and went to great lengths to evade detection. The trojan was subsequently used to conduct a massive spying and data exfiltration operation on mostly American enterprises and government networks.

The attack was targeted, sophisticated and is considered to be wildly successful. In mid-December 2020, the U.S. Department of Homeland Security (DHS) and the Cybersecurity Infrastructure Security Agency (CISA) determined that the exploitation of SolarWinds products "poses an unacceptable risk," and CISA issued an emergency directive instructing all U.S. federal agencies to disconnect devices immediately.

According to General Paul M. Nakasone, commander of U.S. Cyber Command, the hack actually took place nine months before it was identified by cybersecurity company FireEye — and so far it's believed to have impacted 250 businesses and federal agencies. As of the time of this report, the list of organizations affected by the SolarWinds attack continues to grow, and it comprises targets from hospitals to federal government agencies to software giants.

As the investigation into the attack continues and the true extent of the damage continues to be assessed, there are a few certain takeaways from this attack: the **importance of supply chain integrity** and the reality that organizations should operate under a threat model that assumes at some point they will be breached.

The former is especially critical in today's highly interconnected world, and the latter highlights the necessity and real-world applicability of **zero-trust networking principles**.

In this case, the threat actor doubled down on their success, targeting tech companies in order to turn the victims into further attack vectors on other organizations. For example, even software giant Microsoft wasn't immune — the company has acknowledged that attackers gained access.

What is a Supply-Chain Attack?

Supply-chain attacks are cyberattacks intended to damage organizations by targeting the supply chain, or the process of distributing, handling, manufacturing or processing products. These attacks usually involve sneaking malware into software or electronics in order to gain access or otherwise cause harm to a company somewhere further along in the manufacturing or usage process.

Now other companies, some of which had no relationship with SolarWinds, have said they were attacked via software obtained through Microsoft resellers. According to a recent report from the Wall Street Journal, roughly 30% of the networks found to be infected with back doors did not have SolarWinds software installed.

The attack is likely the work of threat actor APT29 (aka Cozy Bear), believed to be associated with one or more Russian intelligence agencies. Researchers now suspect that Russia exploited several layers of the supply chain.

We should expect a surge in similar attacks in the upcoming few years, as the proverbial flashlight has been pointed on this soft underbelly of global IT systems. For example, while hardware supply-chain integrity was questioned and subsequently tightened in light of the Snowden NSA leaks, the SolarWinds attack exposes the weakness in the IT software space.

So, what will be next? What about third-party software that end-users can install on their machines? What about developers, IT staff and other tech-savvy employees who, in their day-to-day job, may rely on a plethora of highly useful tools available on the internet?

There's no preventing such attacks, but there is the ability to detect, react, contain and remediate. Companies have succeeded in thwarting untold numbers of attacks through things like employee security awareness training, comprehensive cybersecurity solutions and multifactor authentication.

But until organizations stop blindly trusting vendors, cloud services and other third parties, we will continue to see these sorts of attacks proliferate.

In the future, we expect third-party certification of software distribution as another mechanism to develop deeper trust levels in downloadable install packages and software updates. Software packages could soon be digitally signed (or published via hashes) to not only securely confirm it is authentic and from a specific vendor, but also that it has been deemed safe (i.e., uncompromised) by a trusted third-party vendor.

Hafnium Launches Next Salvo

In March 2021, just before publication of this report, researchers discovered that a China-based hacking group, known as Hafnium, spent the past several months breaching Microsoft Exchange email software.

"Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks," Microsoft stated in a real-time blog used to communicate mitigation steps. *"In the attacks observed, the threat actor used these vulnerabilities to access on-premises Exchange servers, which enabled access to email accounts, and allowed installation of additional malware to facilitate long-term access to victim environments."*

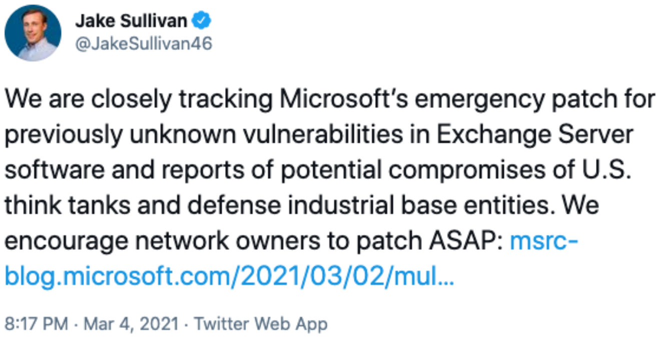
The vulnerability was so concerning, government officials were warning of the ramifications.

"This is a significant vulnerability that could have far-reaching impacts," said U.S. White House Press Secretary Jen Psaki during a March 5 briefing. "First and foremost, this is an active threat. And as the National Security Advisor tweeted last night, everyone running these servers — government, private sector, academia — needs to act now to patch them ... We are concerned that there are a large number of victims and are working with our partners to understand the scope of this."

SonicWall Capture Labs threat researchers tracked the Hafnium exploits of the following Microsoft Exchange vulnerabilities, including CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065, affecting Microsoft Exchange Server 2013, 2016 and 2019. SonicWall released four IPS signatures to protect against such attacks.

While the breach has impacted an estimated 60,000 victims worldwide so far, threat actors also appear to have found a way to automate the attack process, allowing them to target a massive number of victims in a very short period of time.

These changes in criminal access, scale, process and economics are already changing the future of cybersecurity.



Jake Sullivan
@JakeSullivan46

We are closely tracking Microsoft's emergency patch for previously unknown vulnerabilities in Exchange Server software and reports of potential compromises of U.S. think tanks and defense industrial base entities. We encourage network owners to patch ASAP: msrc-blog.microsoft.com/2021/03/02/mul...

8:17 PM · Mar 4, 2021 · Twitter Web App

Published CVEs Nearly Triple Since 2015

According to NIST, 18,353 Common Vulnerabilities and Exposures (CVEs) were published in 2020. This marks the fourth year in a row that a record number of vulnerabilities has been discovered, and amounts to nearly three times the number that were identified just five years ago.

This trend signifies that the industry is working more quickly and more efficiently together to identify critical vulnerabilities and ensure the greater public has guidance to correct any issues.

As one of just 150 trusted CVE Numbering Authorities (CNA), SonicWall closely collaborates with the global cybersecurity industry to help identify vulnerabilities and quickly ensure greater security awareness.

The CVE program is effective because an entire network of certified organizations works together, with the backing of numerous researchers and support personnel, to identify and stay ahead of emerging cyber threats.

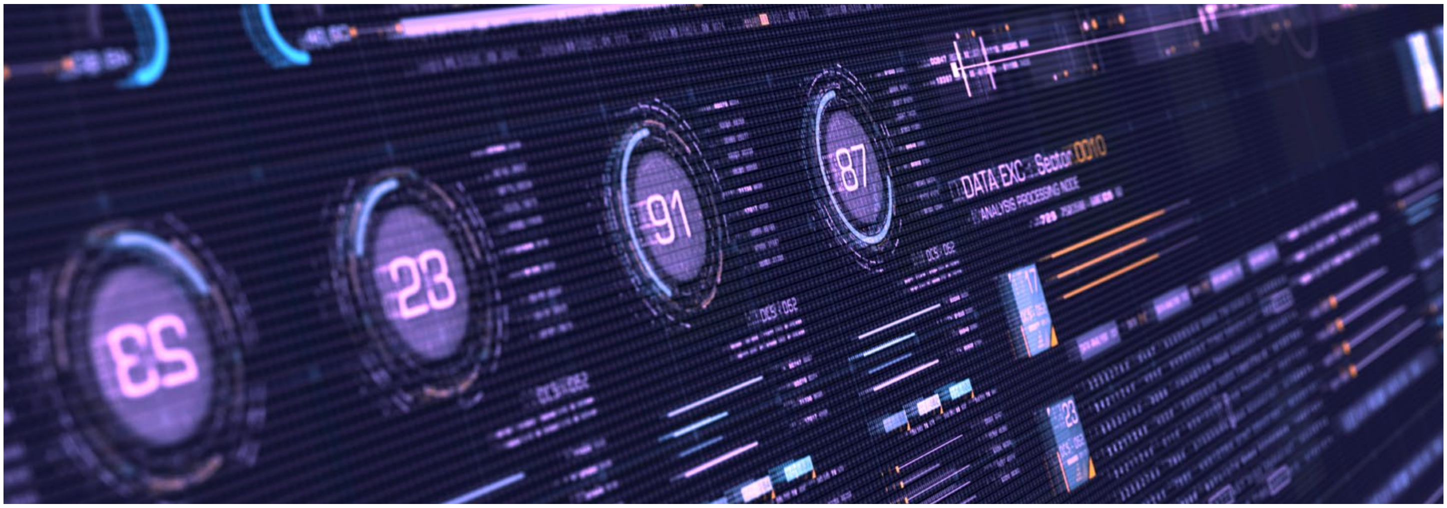
18,353 Common Vulnerabilities and Exposures (CVEs) were published in 2020.

Top 8 CVEs Exploited in 2020

In a perfect world, zero-day vulnerabilities would be patched, fixed or otherwise mitigated before they could result in serious damage.

Unfortunately, this isn't a perfect world. In 2020, SonicWall recorded and analyzed the top eight CVEs that were exploited "in the wild."

These impacted a range of applications, including Microsoft Windows, Oracle WebLogic Server, WordPress and more. SonicWall implemented automatic Intrusion Prevention Service (IPS) or Gateway Antivirus (GAV) signatures for each exploit.



Top 8 CVEs Exploited in 2020

NAME	REFERENCE	DESCRIPTION	PRODUCTS AFFECTED
Zerologon	CVE-2020-1472	A vulnerability in the cryptography of Microsoft's Netlogon process that allows an attack against Microsoft Active Directory domain controllers. This makes it possible for a hacker to impersonate any computer, including the root domain controller.	• Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server Version 1903 • Microsoft Windows Server Version 1909 • Microsoft Windows Server Version 2004
SMBGhost	CVE-2020-0796	A remote code execution vulnerability in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, also known as 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability.'	• Microsoft Windows 10 • Microsoft Windows Server Version 1903 • Microsoft Windows Server Version 1909
SIGRed	CVE-2020-1350	A remote code execution vulnerability in Windows Domain Name System servers in which they fail to properly handle requests, also known as 'Windows DNS Server Remote Code Execution Vulnerability.'	• Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server Version 1803 • Microsoft Windows Server Version 1903 • Microsoft Windows Server Version 1909 • Microsoft Windows Server Version 2004
Curveball	CVE-2020-0601	A vulnerability affecting the certificate verification function in the Crypt32.dll module provided by Microsoft.	• Microsoft Windows 10 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Applications that rely on Windows for trust functionality
F5 TMUI RCE Vulnerability	CVE-2020-5902	A critical vulnerability in the F5 BIG-IP Traffic Management User Interface (TMUI), also known as the Configuration Utility.	• F5 BIG-IP versions 11.6.1 – 11.6.5 • F5 BIG-IP versions 12.1.0 – 12.1.5 • F5 BIG-IP versions 13.1.0 – 13.1.3 • F5 BIG-IP versions 14.1.0 – 14.1.2 • F5 BIG-IP versions 15.0.0 – 15.0.1 and 15.1.0
Oracle WebLogic RCE Vulnerability	CVE-2020-14882	A critical and easily exploitable remote code execution vulnerability in Oracle WebLogic Server.	• Oracle WebLogic Server
Microsoft Exchange Memory Corruption Vulnerability	CVE-2020-0688	A remote code execution vulnerability in Microsoft Exchange software in which the software fails to properly handle objects in memory.	• Microsoft Exchange Server
WordPress 'WP-FILE-MANAGER' Plugin Exploit	CVE-2020–25213	The File Manager (wp-file-manager) plugin before 6.9 for WordPress allows remote attackers to upload and execute arbitrary PHP code.	• WordPress

2020 Zero-Day Vulnerabilities

Of the more than 18,000 new CVEs published in 2020, 24 were published to immediately identify and correct zero-day vulnerabilities.

MONTH	CVE RECORD	VULNERABILITY
January	CVE-2019-17026	Type confusion vulnerability in IonMonkey JIT compiler of Firefox
February	CVE-2020-0674	Microsoft IE scripting engine memory corruption vulnerability
February	CVE-2020-6418	Type confusion vulnerability in v8 of Google Chrome
March	CVE-2020-8467	Remote code execution in Trend Micro Apex One
March	CVE-2020-8468	Content validation escape vulnerability in Trend Micro Apex One
April	CVE-2020-0938, CVE-2020-1020	Windows Adobe Font Manager Library remote code execution vulnerability
April	CVE-2020-6819, CVE-2020-6820	Firefox use-after-free vulnerability
April	CVE-2020-1027	Windows Kernel elevation of privilege vulnerability
April	CVE-2020-12271	SQL injection vulnerability in Sophos XG Firewall
July	CVE-2020-16009	Google Chrome heap corruption via a crafted HTML page
July	CVE-2020-16010	Heap buffer overflow in UI in Google Chrome on Android
August	CVE-2020-1464	Windows spoofing vulnerability
August	CVE-2020-1380	Microsoft IE scripting engine memory corruption vulnerability
August	CVE-2020-17087	Windows Kernel local elevation of privilege vulnerability
August	CVE-2020-1472	Windows Netlogon elevation of privilege vulnerability
September	CVE-2020-3566, CVE-2020-3569	Denial-of-Service (DoS) vulnerability in Cisco IOS XR software
October	CVE-2020-25213	Unauthenticated arbitrary file upload vulnerability in WordPress File Manager plugin
October	CVE-2020-27930	Memory corruption in Apple macOS
November	CVE-2020-15999	Heap buffer overflow in Google Chrome
November	CVE-2020-14871	Buffer overflow vulnerability in Oracle Solaris
November	CVE-2020-27932	Local privilege escalation vulnerability in Apple macOS
November	CVE-2020-27950	Out-of-bounds read in Apple macOS
November	CVE-2020-16013	Memory corruption vulnerability in Google Chrome
November	CVE-2020-16017	Use-after-free in Google Chrome

COVID Threats: Exploiting a Pandemic

Of all the threat types that really took off in March, COVID-19-related threats are perhaps the least surprising. As the mysterious new pandemic spread to country after country, cybercriminals saw an opportunity to take advantage of the fear and confusion in its wake to achieve their own nefarious ends. And in very short order, a deluge of phony COVID-19 tracking apps, malicious "COVID-19 information" docs and PDFs supposedly full of "cures" sprang up.

(It's worth mentioning, though, that COVID-19-related malware doesn't *always* have anything to do with the pandemic. With phishing trends, for example, we can be fairly certain that emails containing words like "coronavirus" are, by definition, pandemic-related. But threat actors can name *any* piece of malware something like "pandemic," "COVID" or "coronavirus," and it'll get flagged — even if there isn't anything related to the virus whatsoever on the front end.)

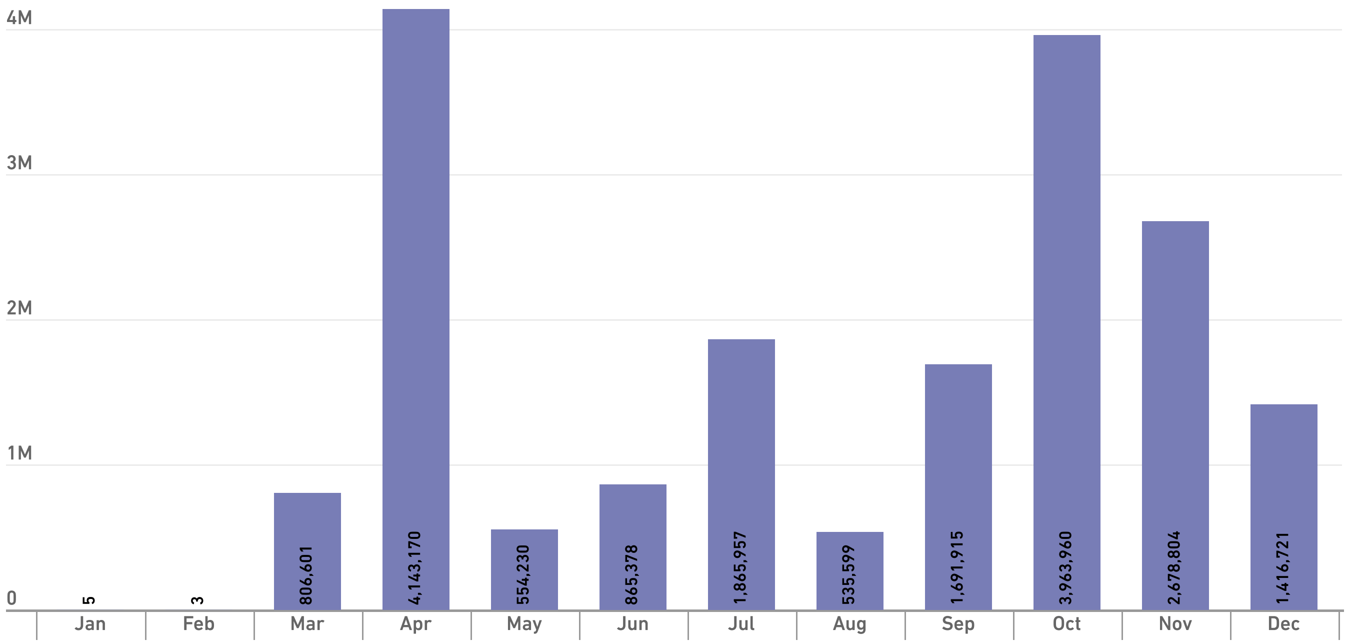
Perhaps unsurprisingly, trends in COVID-19 malware and phishing attempts bear some resemblance with those for COVID-19 case data.

And likely because the vast majority of malware targets the United States, the COVID-19 data it happens to most closely resemble is that for the United States. Everywhere we see jumps in the number of cases — namely, in April, July and October — we see jumps in the number of COVID-19-related malware.

Interestingly, while cases continue to rise in November and December, COVID-19-related malware falls off. There are a few reasons this could be occurring: It's possible that, with a vaccine on the horizon and a much larger body of legitimate sources from which to gather information, people are spending less time researching and thus encountering fewer threats. Perhaps by the end of 2020, some people developed "COVID fatigue" and began to actively avoid anything to do with the virus.

Of course, it's also possible that people began hearing about COVID-19-related threats and became too savvy to fall for many of the methods that had worked before, leading criminals to shift their efforts elsewhere.

2020 Global COVID-Themed Malware Attacks



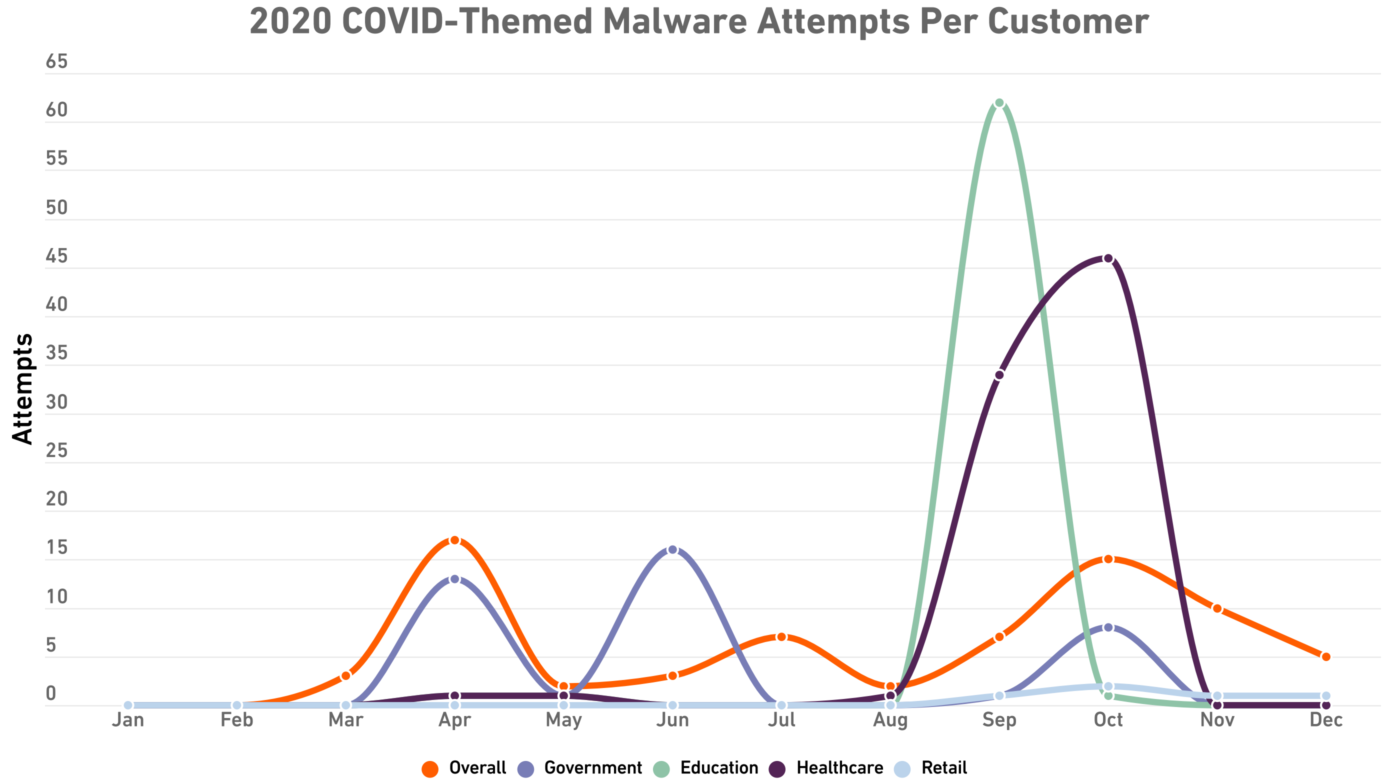
COVID-19-Related Attacks By Industry

While there was no shortage of attempted COVID-19-related attacks in 2020, that doesn't mean that *everyone* necessarily saw a lot of attempts.

That the number of COVID-19 malware attempts per customer overall began to spike in March isn't surprising. Nor is the fact that those in the education industry saw a spike in attempts right around the time school started back in the fall.

But the fact that healthcare saw very little COVID-19-related malware until it skyrocketed in September and October, only to crash just as spectacularly to finish out the year, is a bit more puzzling — particularly since COVID-19 case levels continued to rise through the end of the year, straining hospitals already struggling amidst the pandemic and creating exactly the sort of situation cybercriminals love to exploit.

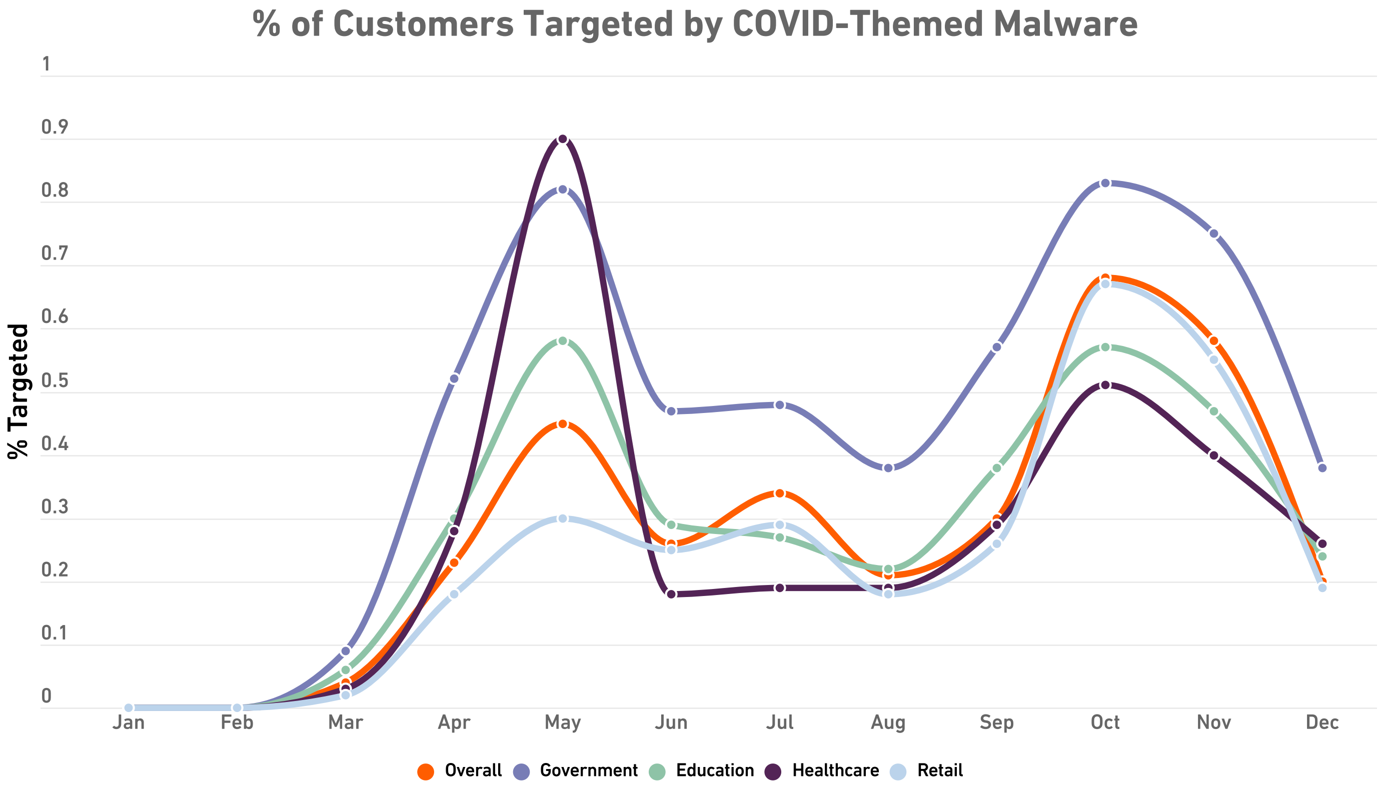
While the healthcare industry saw 15% more COVID-19-related malware attempts per customer than average, customers in the rest of the verticals examined fell below this baseline, with education 8% lower, government 44% lower and retail 92% lower.



While the data for number of attempts per customer was fairly lopsided in terms of industries targeted, the trends for percentage of customers targeted by COVID-19-themed malware are much more egalitarian.

This doesn't mean there weren't still winners and losers, however. Those in government were roughly 1.83 times more likely to be targeted by COVID-19-related malware than those in retail, who were the least likely to see an attempt.

While the highest number of attempted COVID-themed malware attacks per customer in the first half occurred in April, we don't see a peak in the percentage of customers targeted until May — suggesting that cybercriminals ramped up attacks on their existing targets before widening their nets.



2020's Biggest Cybersecurity Events

2020

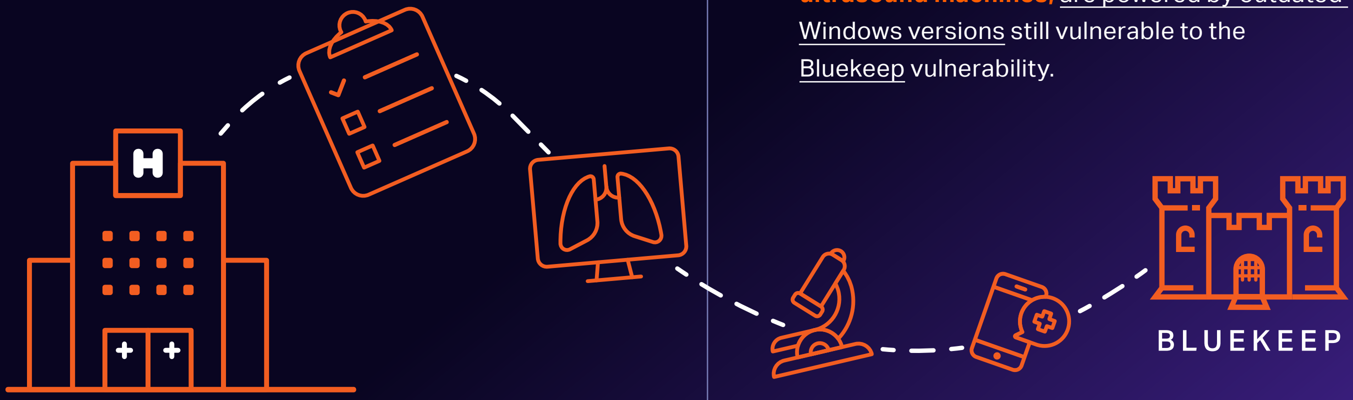
While the biggest news in 2020 was, of course, the spread of COVID-19, the pandemic set into motion a wave of cybersecurity incidents, the ripples of which are still being felt nearly a year into the so-called "new normal."

JANUARY

- The U.S. Army banned TikTok from government devices over concerns about the platform's relationship with China.
- Authentication bypass bugs in two WordPress plugins allow anyone with the admin username to access a site's backend.

FEBRUARY

- Security researchers identified a JavaScript vulnerability in WhatsApp that could allow malware, ransomware or phishing to be spread through notification messages that appear completely normal to users.
- Researchers find that over **55% of medical imaging devices, such as X-rays, MRIs and ultrasound machines,** are powered by outdated Windows versions still vulnerable to the Bluekeep vulnerability.



MARCH

- As COVID-19 spreads and countries around the world enter lockdown, cyberattacks rapidly double, including a sophisticated hacking attempt against the World Health Organization (WHO).

APRIL

- A vulnerability is discovered in Apple iPhones and other iOS/macOS devices that causes them to crash when loading messages or posts in the Sindhi language.

2020's Biggest Cybersecurity Events

2020

MAY

- German Chancellor Angela Merkel implicates Russia in a series of hacking attempts on her emails and those of other German lawmakers.
- Cell towers in several states are burned or otherwise damaged by conspiracy theorists who believe 5G is responsible for the spread of the novel coronavirus.
- 15-year-old hacker Ellis Pinsky and a group of friends steal $24 million in cryptocurrency from blockchain advisory firm Transform Group.

JULY

- Millions of Microsoft Office 365 users, including business leaders across a variety of industries and 62 countries, are targeted in a massive phishing campaign.
- In a bid to steal invaluable vaccine research data, Chinese government-linked hackers target U.S.-based biotech company Moderna.
- The Twitter accounts of U.S. politicians Joe Biden and Barack Obama, musician Kanye West, businessmen Bill Gates and Elon Musk, and other high-profile individuals are hacked and used in an attempt to scam Bitcoin from followers.

JUNE

- With many employees working remotely full time during the pandemic, mobile phishing increases 37%.
- A large German multinational corporation charged with procuring PPE for front-line healthcare workers is targeted in a massive phishing attack.
- Researchers discover an unpatched, zero-day vulnerability in Netgear router firmware, leaving 79 device models at risk for full takeover.
- An unidentified European bank is the target of an 809 million packet-per-second DDoS attack, believed to be the largest to hit any network.
- The U.S. Federal Communications Commission (FCC) formally designates China's Huawei Technologies Co. and ZTE Corp. as threats to national security.

AUGUST

- Researchers discover social media app TikTok used encryption to conceal its tracking and collecting of unique identifiers from millions of Android users without their consent.
- FritzFrog, a unique and advanced worming P2P botnet that drops backdoors and cryptominers, attacks millions of SSH servers.

2020’s Biggest Cybersecurity Events

2020

SEPTEMBER

- A woman dies after a ransomware attack on Germany’s Dusseldorf University Clinic leads to her being diverted to a distant facility, resulting in care being delayed for over an hour.
- Cybercriminals threaten thousands of organizations, from various industries around the world, with DDoS attacks within six days unless they pay a ransom.

OCTOBER

- A politically motivated spear-phishing attack targets hundreds of U.S. organizations with emails that claimed to be from the Democratic National Committee, but were in reality vehicles for Emotet malware.
- Iranian state-sponsored hackers exploit the Zerologon vulnerability, which allows attackers to take over domain controllers and gain full control over their targets.
- The Maze cybercrime gang, among the most prominent ransomware groups, announces it is shutting down operations.

NOVEMBER

- In a unique and highly targeted cyberattack, suspected state-sponsored attackers steal cybersecurity firm FireEye’s Red Team assessment tools.
- A cyberattack on UVM Health Networks halted chemotherapy, mammogram and screening appointments, and led to 300 staff being furloughed or reassigned.
- Manchester United, one of the wealthiest and most popular soccer clubs in the world, is targeted in a suspected ransomware attack.

DECEMBER

- A compromised update to tech company SolarWinds’ Orion software enables state-sponsored attackers to access government and other systems. According to Dmitri Alperovitch, head of the Silverado Policy Accelerator think tank, the SolarWinds intrusion **had the greatest impact of any cyberattack in American history**.

KEY FINDINGS FROM 2020

∨43%

MALWARE HITS LOW POINT

In 2020, malware fell dramatically, reaching 5.6 billion attacks— **a 43% decrease from 2019's totals.**

READ MORE ON PAGE 21

∧62%

RANSOMWARE HITS RECORD HIGH

The effects of a global pandemic, combined with record highs in the price of cryptocurrency, drove ransomware to a **staggering 62% increase over 2019.**

READ MORE ON PAGE 35

∧20%

INTRUSION ATTEMPTS RISE, ATTACK PATTERNS CHANGE

The number of intrusion attempts in 2020 was **20% higher than in 2019**, but year-over-year attacks in Europe nearly quadrupled. Meanwhile, changes in attack types and patterns evolved over the year.

READ MORE ON PAGE 44

∧74%

DEEP MEMORY INSPECTION: BETTER THAN EVER

SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) found 268,362 'never-before-seen' threats in 2020— **an increase of 74% from 2019**.

READ MORE ON PAGE 48

KEY FINDINGS FROM 2020

+1D

FASTER IDENTIFICATION OF 'NEVER-BEFORE-SEEN' MALWARE

The sooner new threats can be identified, the sooner they can be neutralized. Based on VirusTotal data, on average **SonicWall is identifying never-before-seen malware variants a full day before VirusTotal receives samples** — sometimes much earlier.

READ MORE ON PAGE 50

∧ 25%

MALICIOUS OFFICE FILES OVERTAKE MALICIOUS PDFs

In 2019, cybercriminals preferred malicious PDFs and malicious Office files in roughly equal numbers. But in 2020, malicious Office files were the clear choice: **They now make up more than a quarter of all malicious files**.

READ MORE ON PAGE 51

∧ 3YH

REPORTS OF CRYPTOJACKING'S DEATH HAVE BEEN GREATLY EXAGGERATED

Despite all predictions to the contrary, the death of Coinhive wasn't enough to kill illegal mining. Instead, record cryptocurrency prices drove **cryptojacking up from its low point in 2019 to a three-year high**.

READ MORE ON PAGE 52

∧ 66%

IoT MALWARE SKYROCKETS

When the pandemic sent workers home, their unsecured personal devices were there waiting for them — and so were cybercriminals. Recognizing the potential to use compromised devices for personal gain, **attackers pushed IoT malware to a 66% increase**.

READ MORE ON PAGE 58

Malware Hits Low Point

In 2019, malware began to slip downward. In 2020, it fell like a rock, reaching 5.6 billion total attacks — a mind-blowing 43% *decrease* from last year's total.

Where Did The Malware Go?

SonicWall is exercising caution when using the 2020 global malware data. During the pandemic, fewer employees were accessing corporate networks through traditional means, thereby relying solely on whatever security is included in their ISP's consumer-grade hardware. This reduced visibility for corporate networks worldwide, and by extension reduced visibility for cybersecurity vendors, including SonicWall.

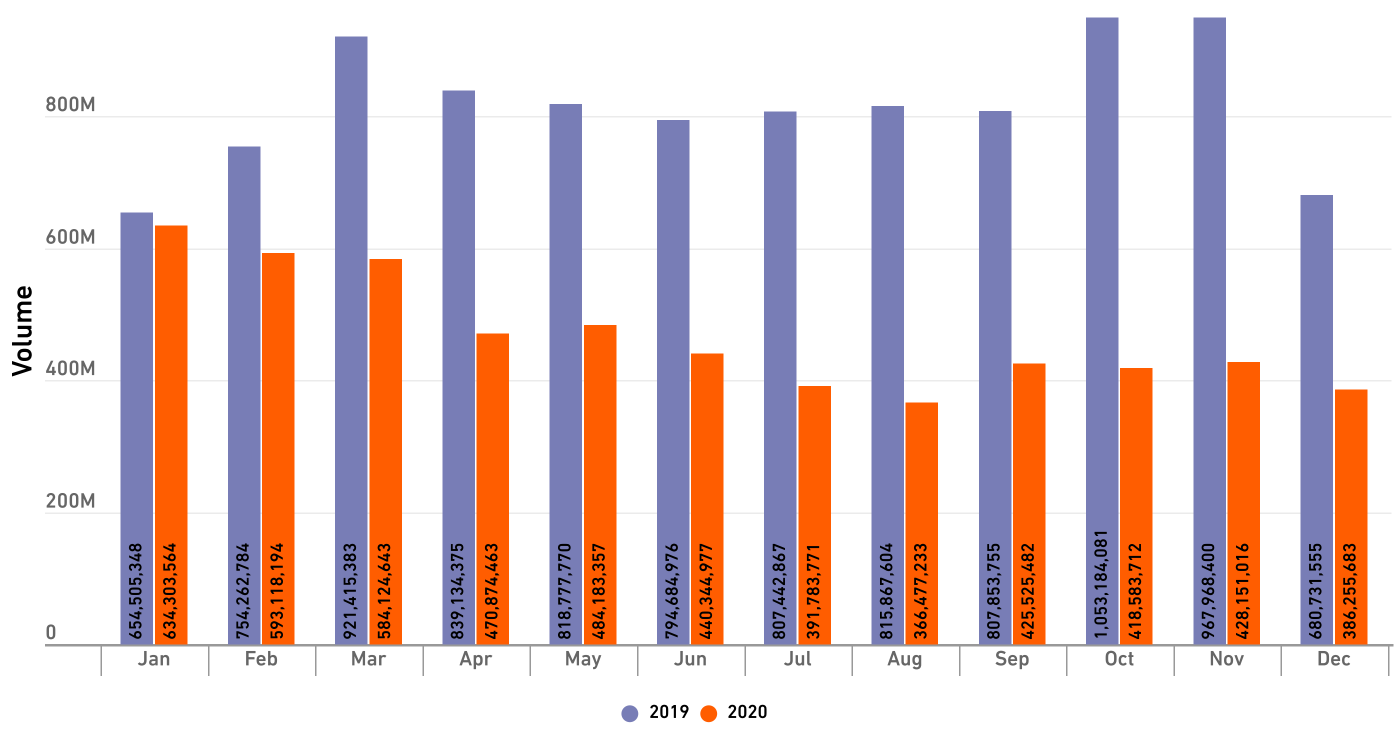
But as contrarian as malware was in its overall trends, it was equally so from month to month.

Unlike most other forms of cybercrime in 2020, SonicWall observed malware starting high in January and then dropping — and this decrease was so pronounced that even a rebound through September and all of Q4 couldn't reverse it.

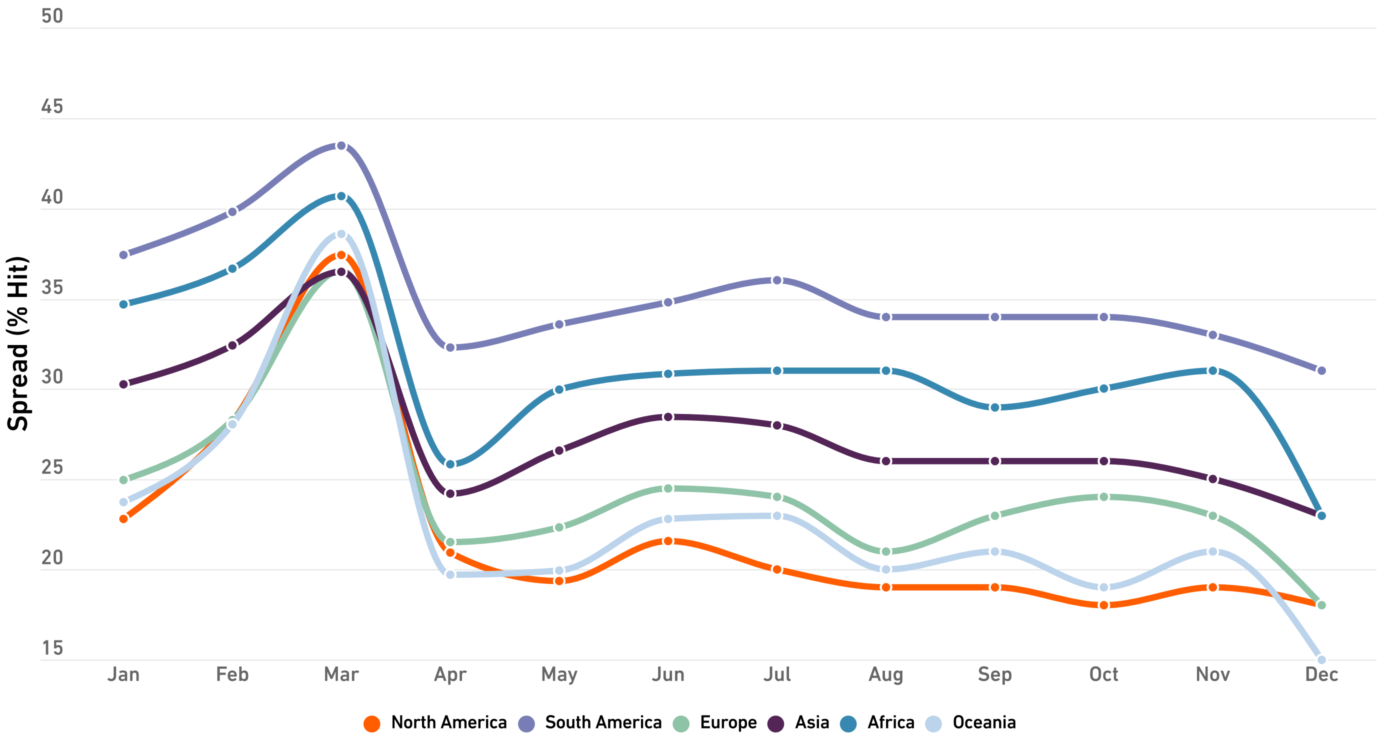
But even though malware is ending 2020 at near-historic lows, criminals continue to refine their tactics to be even more targeted and effective than ever, requiring fewer total attacks to be successful.

Worse, as we'll see later on, the decreases in malware coincide with record or near-record *highs* in other forms of attack — meaning cybercriminals aren't calling it a day, but simply switching their strategies yet again.

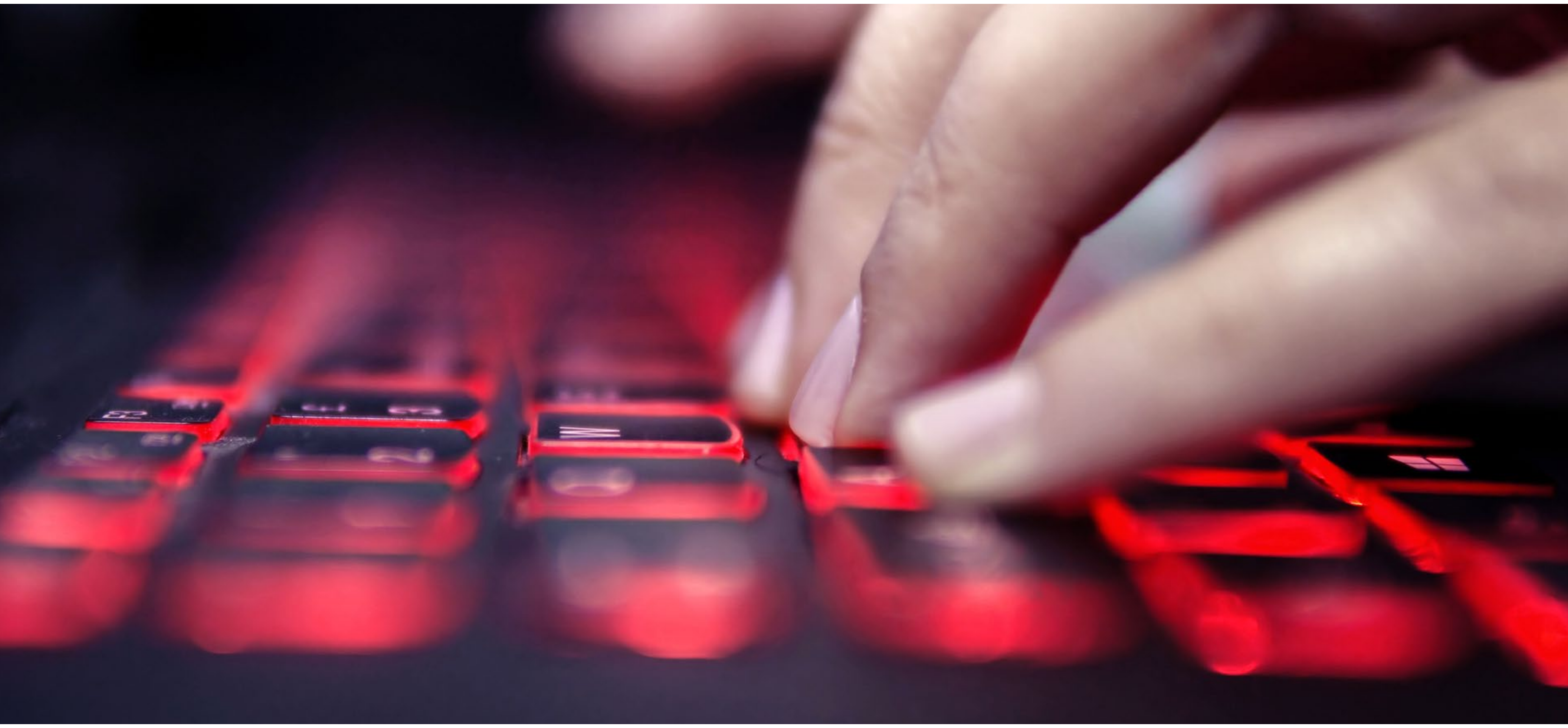
2020 Global Malware Attacks



2020 Global Malware Spread Trend



The COVID-19 pandemic caused a worldwide spike in malware, pushing the chance any given organization would see a malware attack above 35%. By December, the odds had fallen considerably, to about 21%.



Want to get a sense for how much malware dropped in 2020? Consider this: **In 2019, every region had more than 1 billion malware hits total. In 2020, only one did.**

In both 2019 and 2020, SonicWall observed by far the most malware in North America, but it fell 42% in 2020, from 5.86 billion to 3.40 billion. Unfortunately for North America, however, its percentage share of total malware actually increased: in 2019, malware in North America made up 59% of all malware, but in 2020 that rose to 61%. With 984 million malware hits in 2020, Europe saw a 44% drop in overall malware. Asia, meanwhile, experienced a 53% decrease in malware attempts.

▼42%

SonicWall saw total malware volume in North America fall in 2020, from 5.86 billion to 3.40 billion.

What is Malware Spread?

SonicWall recorded 2.8 billion malware hits in the United States in 2020 — nearly nine times the next-highest ranked (U.K., with 322 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.

To find out the odds that an organization will see malware in a particular area, we use the malware spread percentage — a calculation of what percentage of sensors saw a malware attack.

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

Think of it this way: Annual precipitation numbers can be useful in determining whether your area has seen more rain than it did last year, but they don't tell you whether your umbrella will see heavier use than your tube of SPF. Like the "chance of rain," malware spread percentage considers a variety of additional factors to provide a more meaningful risk assessment.

Malware Risk by Country

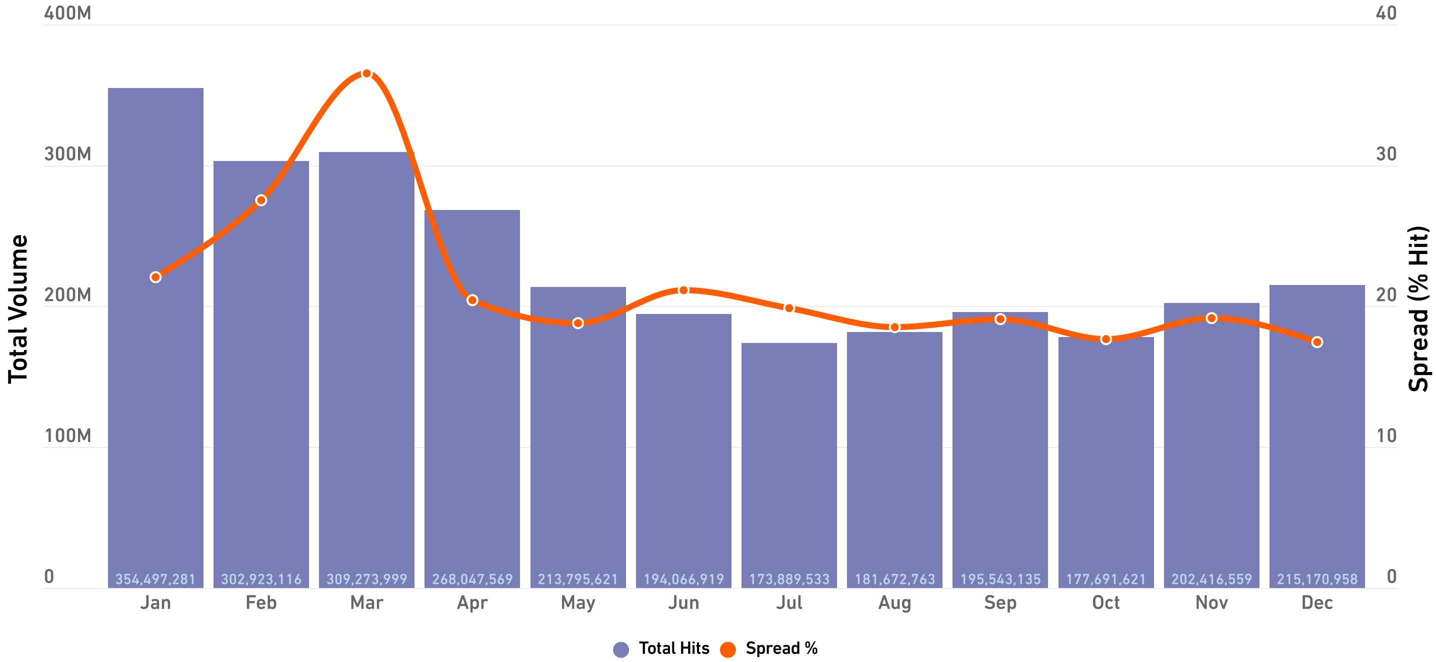
In a relatively small sample size of eight countries, there's still a huge variation in outcomes. But one thing remains remarkably consistent regardless of where the country is located, what its total malware volume is, or how its trend lines fall.

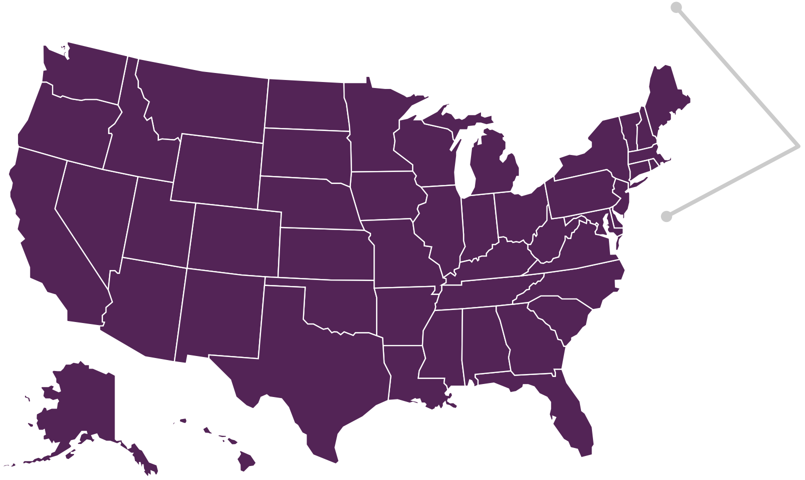
When looking at SonicWall's exclusive malware spread percentage data — which tells us how widespread malware is in a given region (see next section) — the highest malware spread percentage occurred in March, at the peak of the initial pandemic lockdown.

This is one of several places you can see the direct effects of COVID-19 on the threat data.

Interestingly enough, in all but one country, malware spread was *lowest* in December. We'll see in 2021 whether this proves to be a seasonal blip or a further sign of malware losing ground.

2020 Malware Attacks | United States

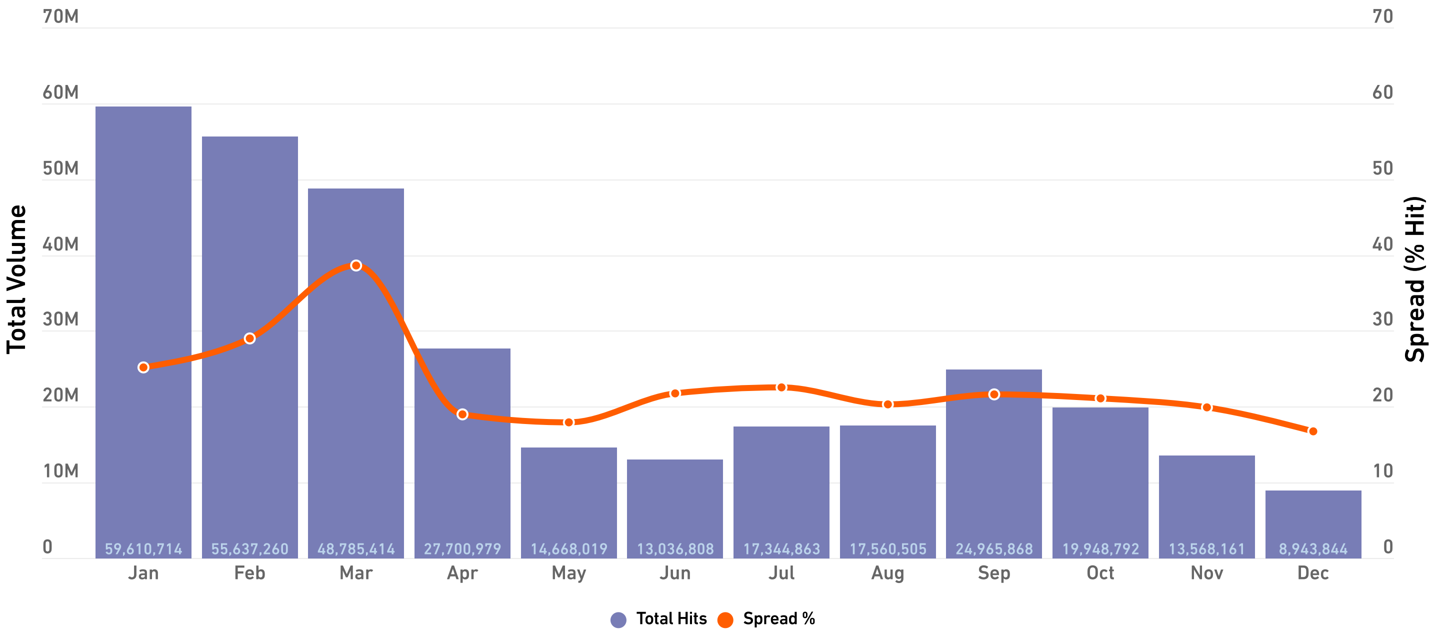




9x

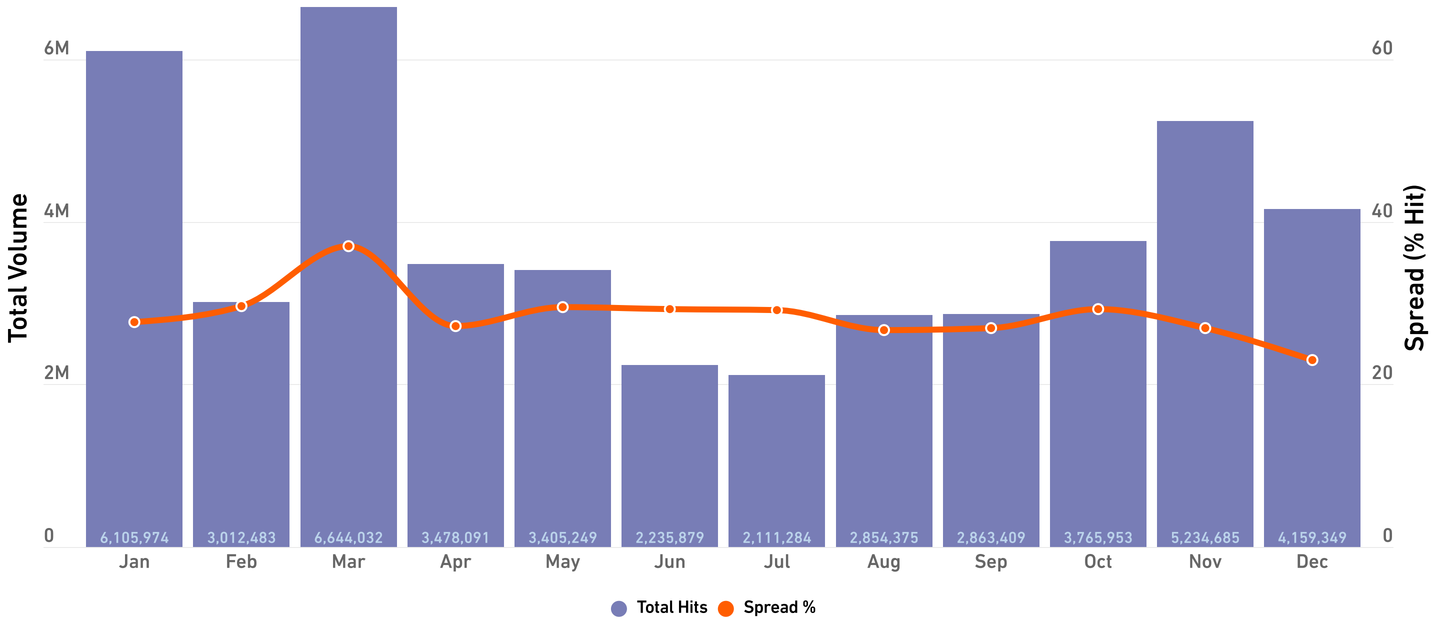
Once again, SonicWall observed the highest volume of malware in the United States, with nearly nine times the volume seen in No. 2 U.K.

2020 Malware Attacks | United Kingdom



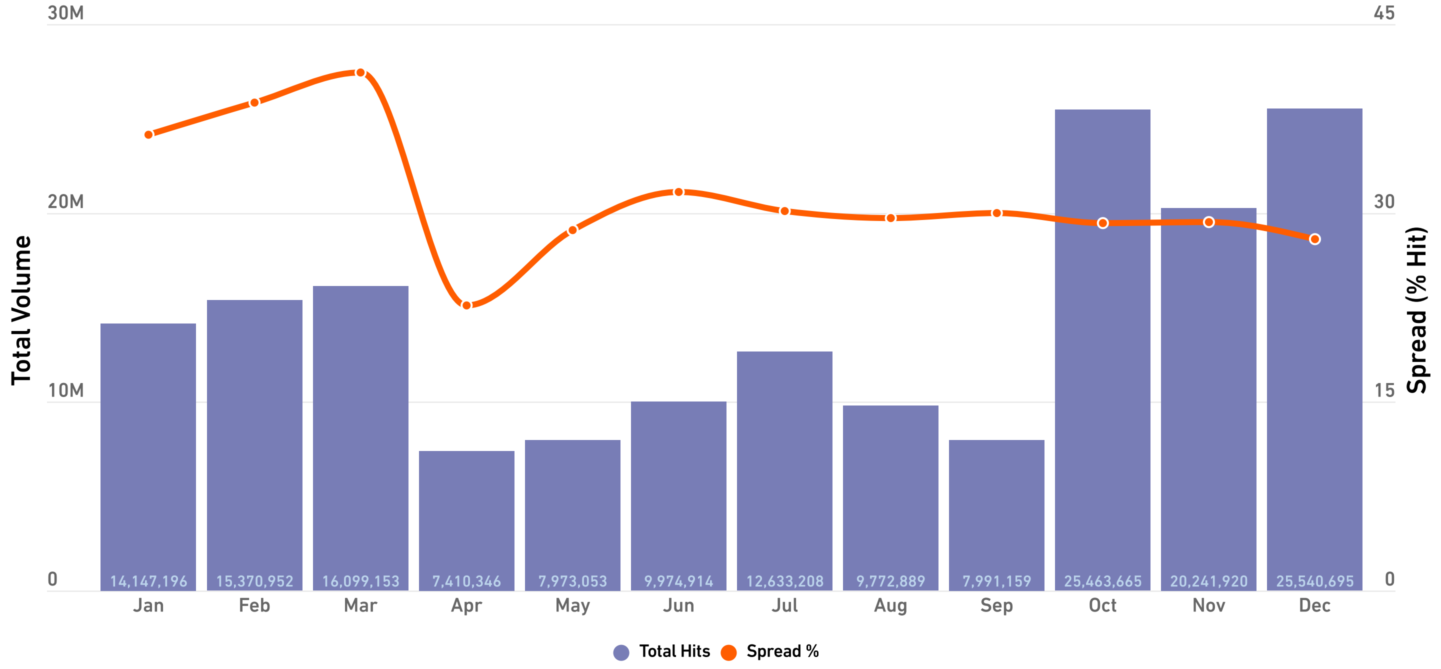
In the U.K., over half of all malware hits occurred within the first three months of the year, another indication of the impact of COVID-19.

2020 Malware Attacks | Germany



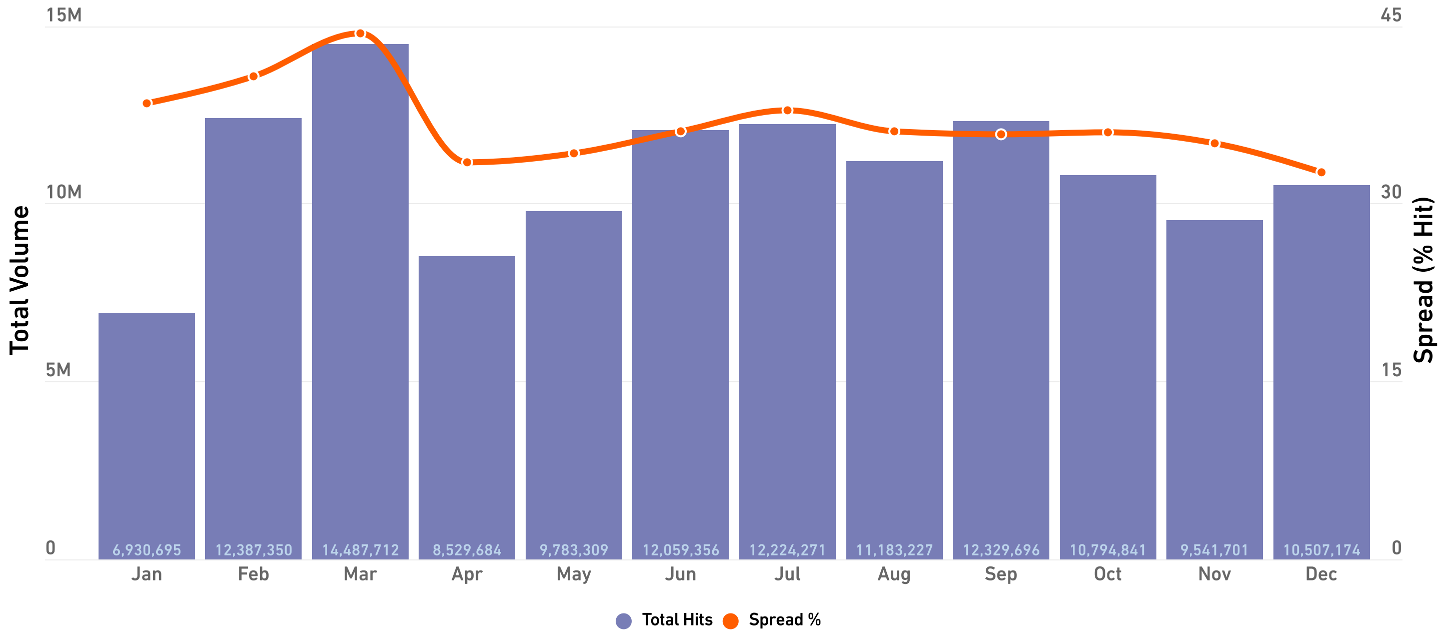
Malware dropped more in Germany than in any other country, falling by a remarkable 67%. Its roughly U-shaped graph is a complete departure from 2019, when volume was highest in spring and summer.

2020 Malware Attacks | India



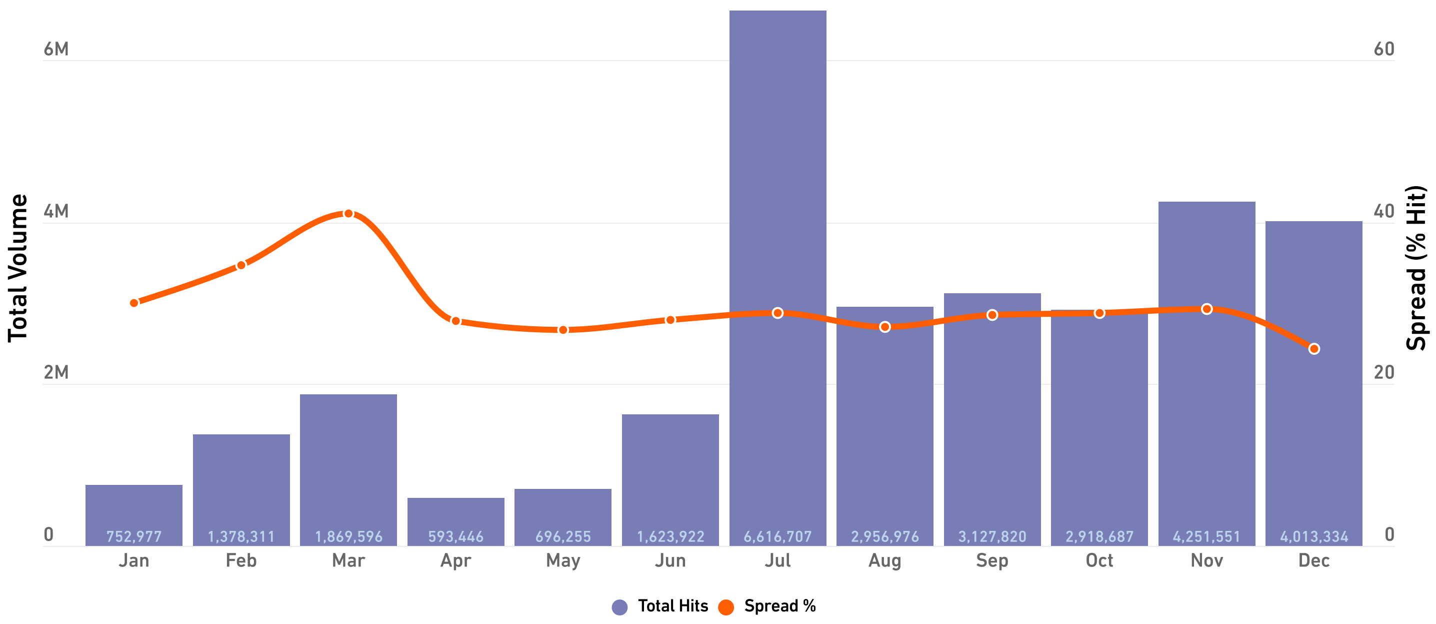
India was the only country to see its lowest spread percentage in a month other than December. Instead, malware spread was lowest in April, meaning it saw both its highest malware spread percentage and its lowest within a 60-day period. India also experienced the largest spike, with monthly volume more than tripling between September and October.

2020 Malware Attacks | Brazil



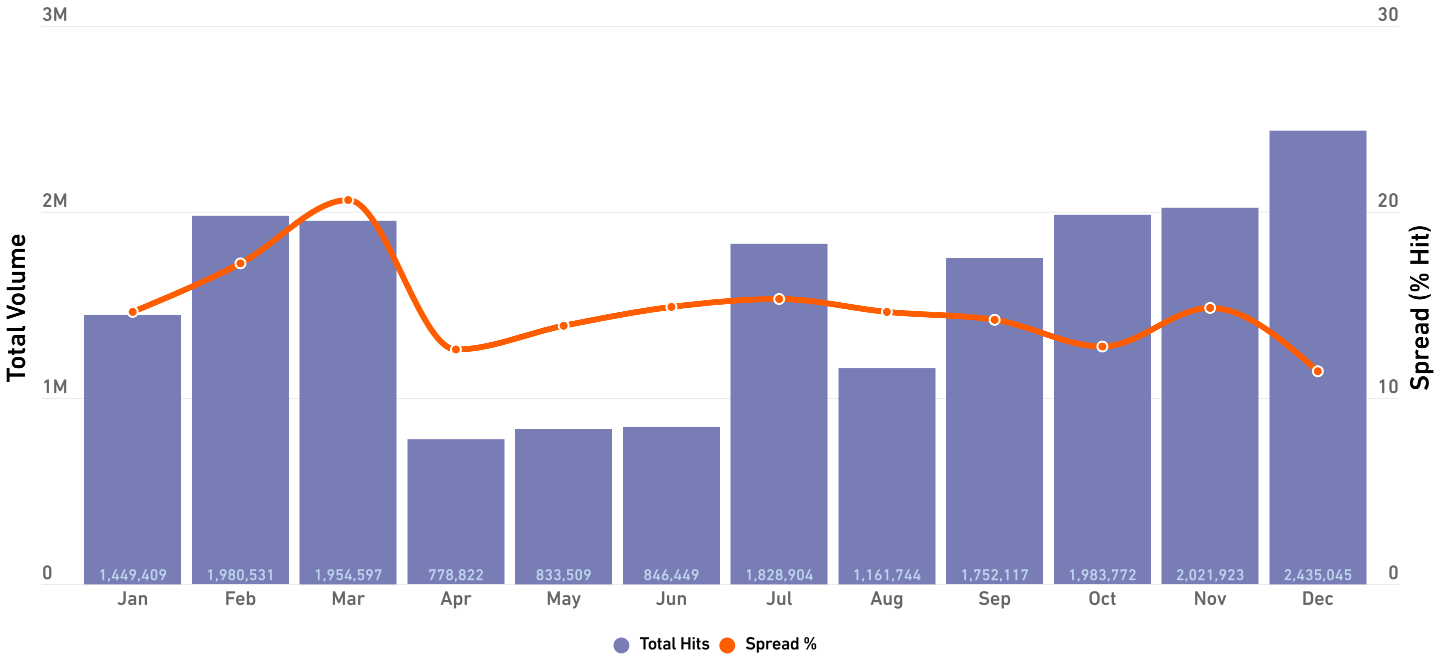
Brazil, which experienced a 46% overall drop in malware, saw both its lowest malware volume and highest malware spread in Q1.

2020 Malware Attacks | Mexico

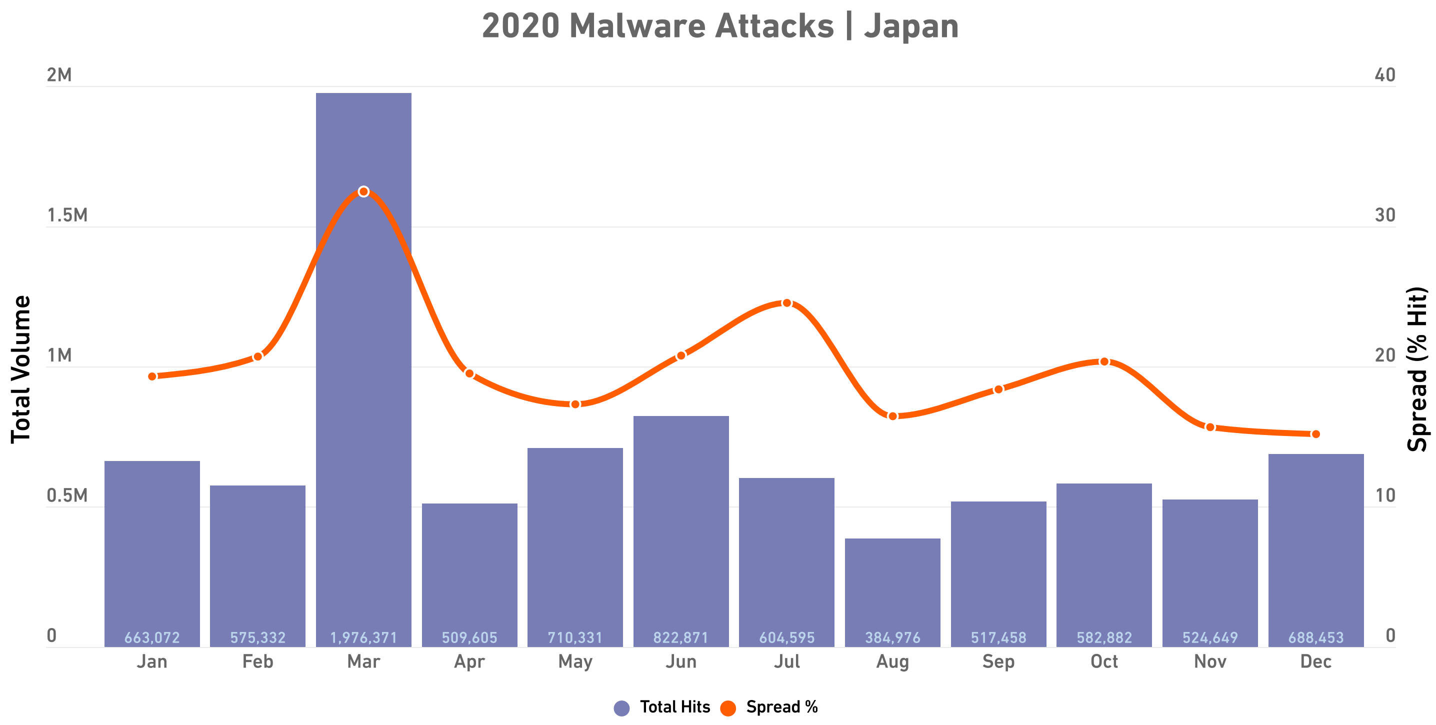


In Mexico, malware actually *rose,* spiking 73% over 2019's volume.

2020 Malware Attacks | United Arab Emirates

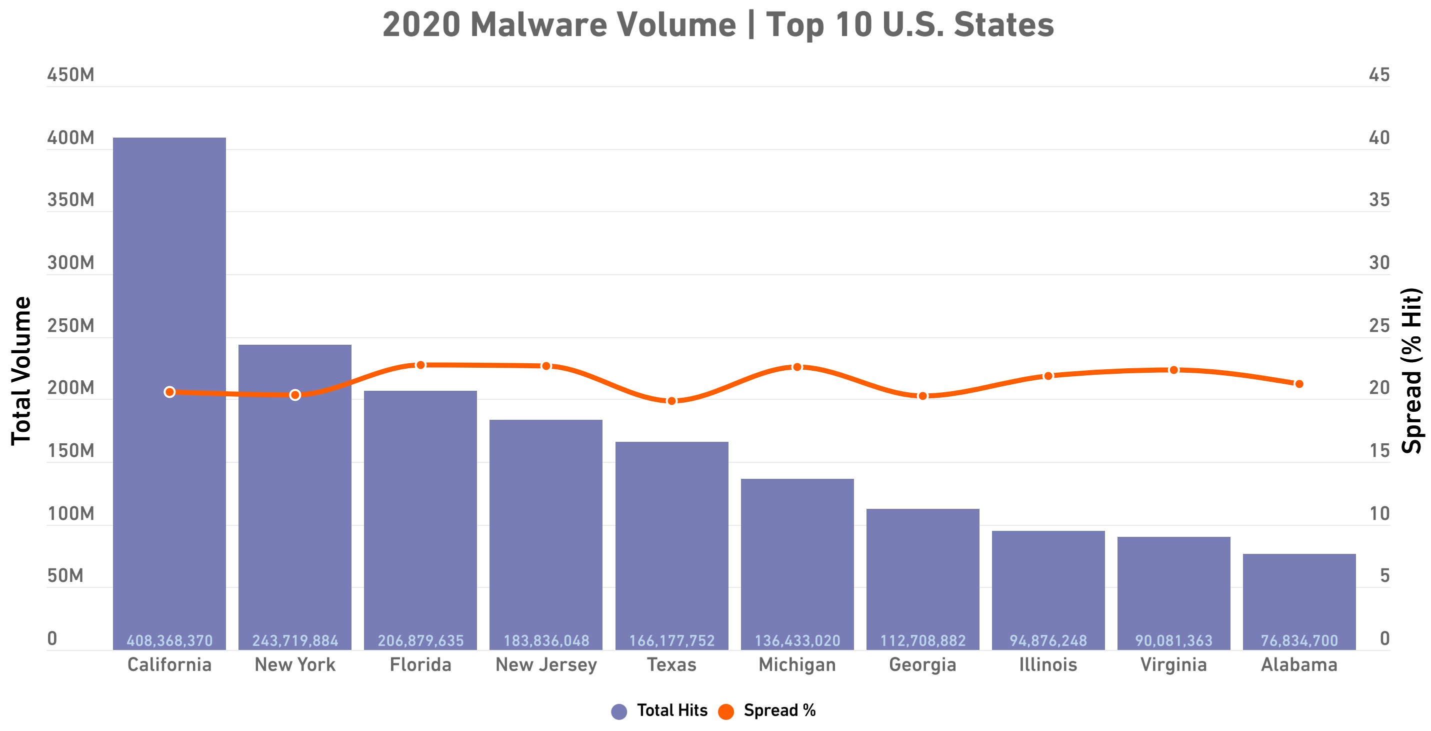


Malware volume in the UAE was largely suppressed by a very favorable Q2, when numbers fell to their lowest point and stayed there the entire quarter.

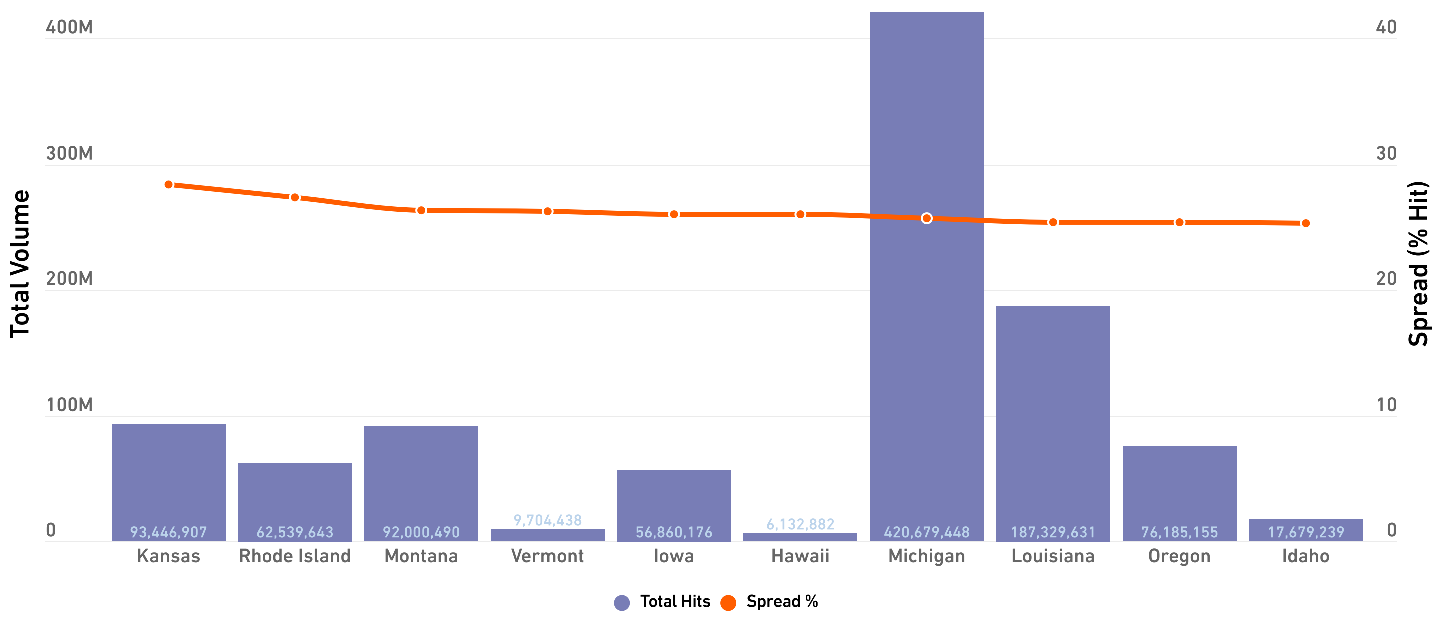


Japan was the only country that had roughly the same amount of malware in January as in December. Aside from a large spike in March (the second largest in any country), malware in Japan remained the most consistent throughout the year.

Malware Risk Across U.S. States



2020 Malware Spread | Top 10 Riskiest U.S. States



If California's malware volume — at 408.3 million, nearly 70% more than the next-highest state — has you wondering how Californians have time to do anything besides battle malware, it might be a good time to also take a look at California's malware spread percentage.

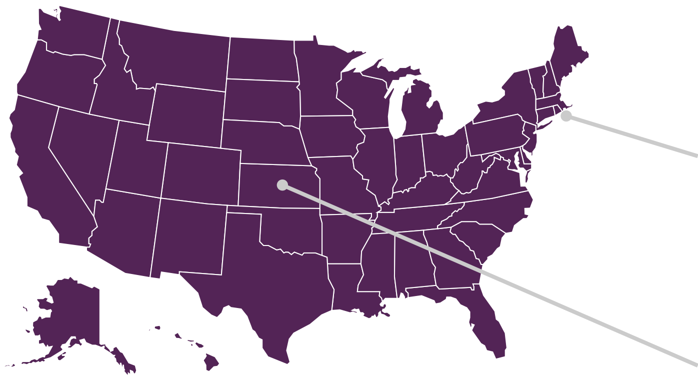
Keep in mind that there are a *lot* of Californians: 39.5 million at last count, making it the most populous state by far. Moreover, its $3.2 trillion economy (if it were a country, it'd be the fifth-largest GDP on Earth) needs a massive number of devices to power it.

Taking these factors into consideration, California isn't anywhere close to being the riskiest state — it's actually near the bottom of the list, at No. 43.

So what state *is* the riskiest? Kansas, where 26.7% of SonicWall sensors saw a malware hit. Fortunately for those in the Sunflower State, though, this stat appears to be trending in the right direction: In our 2020 Mid-Year Update, 31.3% of sensors saw a hit.

At the other end of the spectrum, in North Dakota only 18.5% of sensors logged an attempted malware attack.

On a per-person basis, the riskiest state in 2020 was Rhode Island, where there were 37 malware attempts for each resident. In contrast, Mississippi and Delaware each saw just a single attempt per person on average.



37/👤

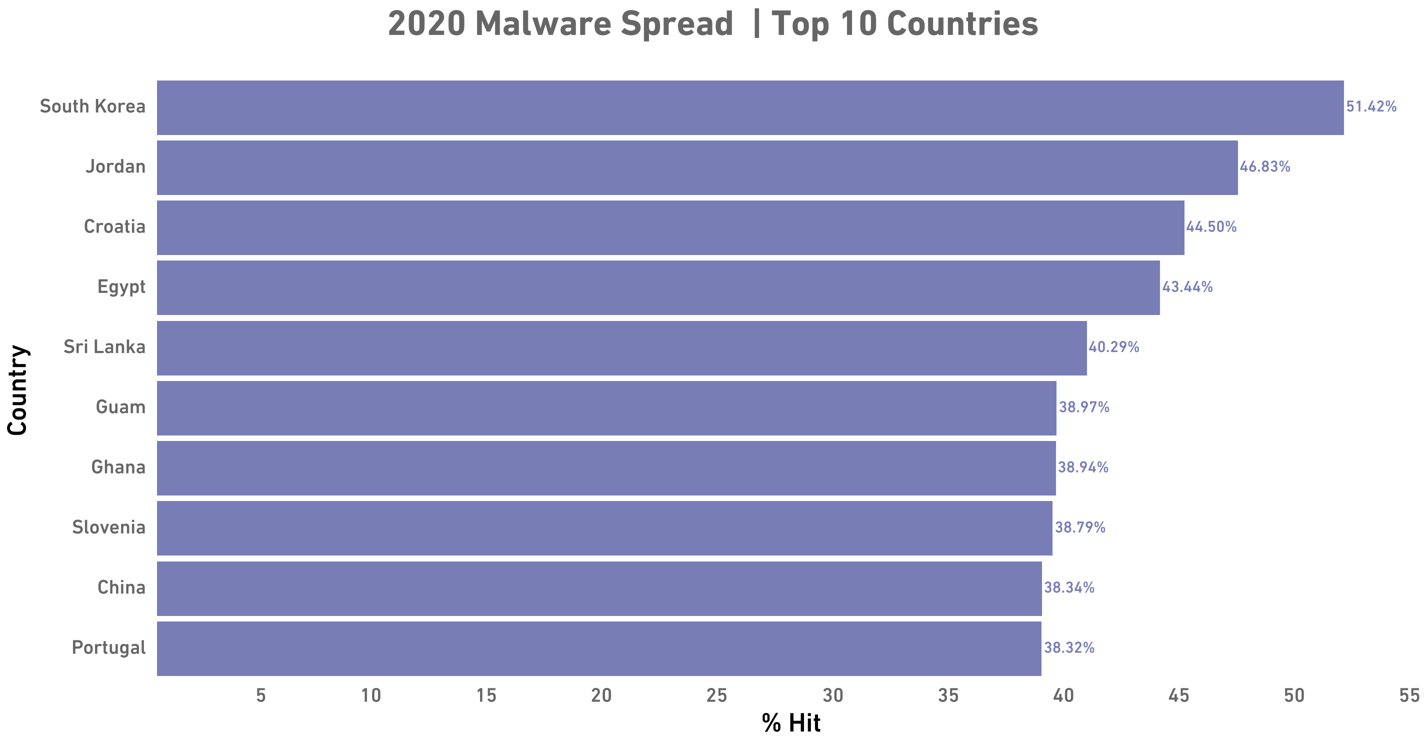
Malware attempts for each resident in Rhode Island.

26.7%

of SonicWall sensors saw a malware hit in Kansas.

Malware Spread by Country

Based on the malware spread data, an organization is not most likely to see malware in the U.S. *or* the U.K. An organization in South Korea, however, is actually more likely to see malware than not, as the spread percentage there is 51.4%. (Conversely, in the Bahamas, you've only got about a 16% chance of seeing malware.)



Which Industries Saw the Most Malware?

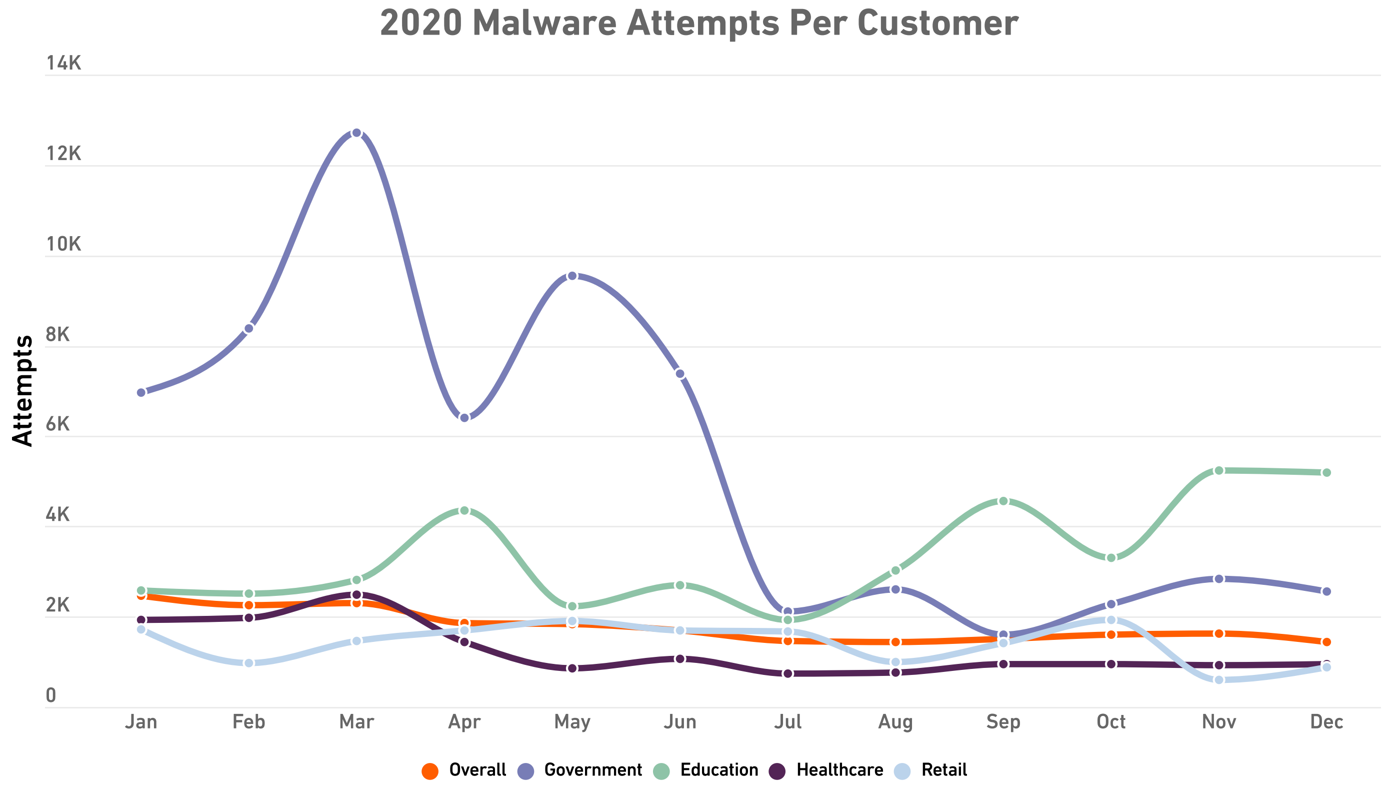
In the first half of 2020, the number of attempted malware attacks per government customer started at more than double other industries, and only rose from there. In March, government customers saw an unbelievable 12,725 attempted malware attacks each on average — that's 17 *every hour*.

Fortunately, this spike was short-lived, but the rates for government stayed (un)comfortably above all other industries for the entire first half of the year.

But in late summer — just in time for schools to reopen — a surge in the number of attempted attacks targeting the education sector coincided with a drop in attacks on government. By September, there were nearly triple the number of attempts on education as on government. Education would remain far ahead of the pack for the rest of the year.

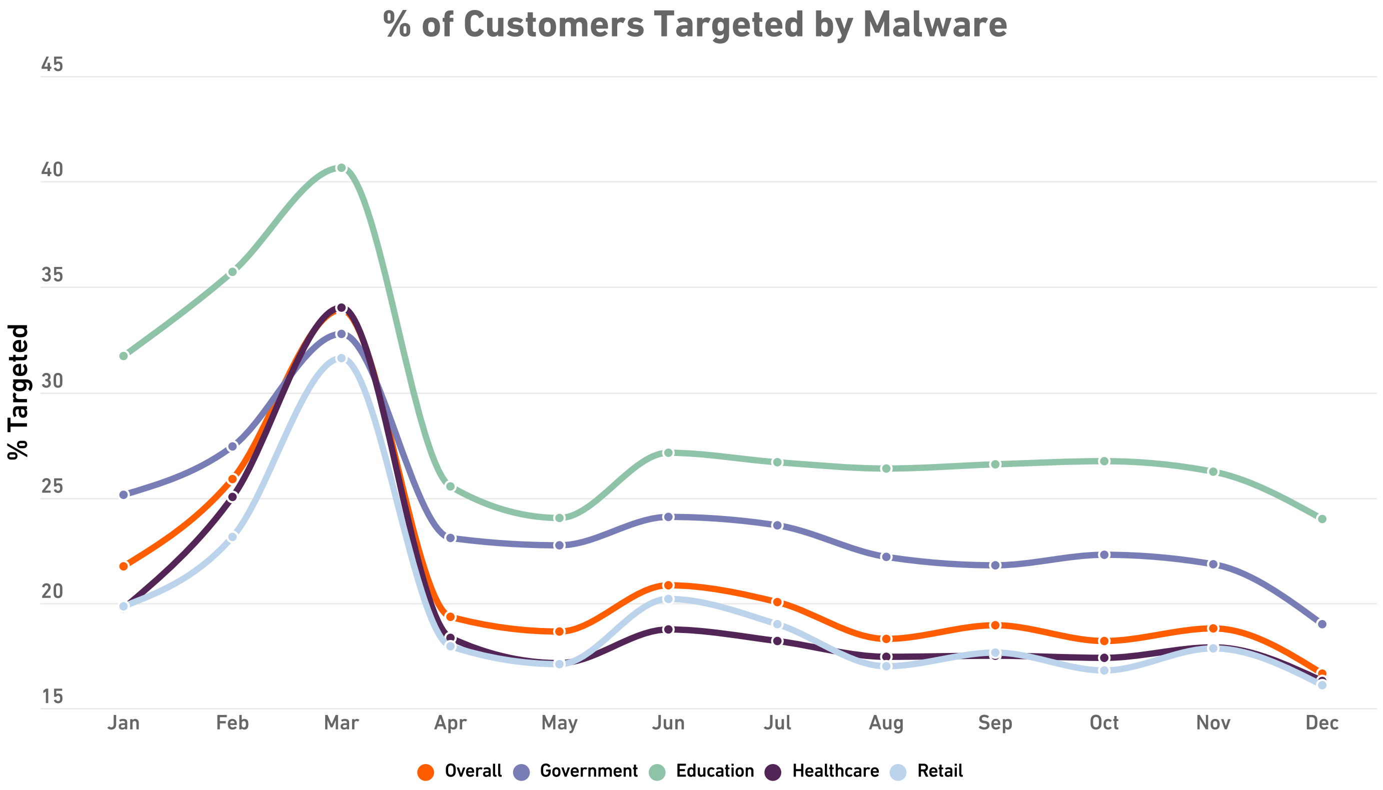
On a longer timeline, however, these spikes are of much less concern. Across every industry, year-over-year attempted malware attacks per customer were way down. This decrease ranged from 22% for retail, to 78% for government.

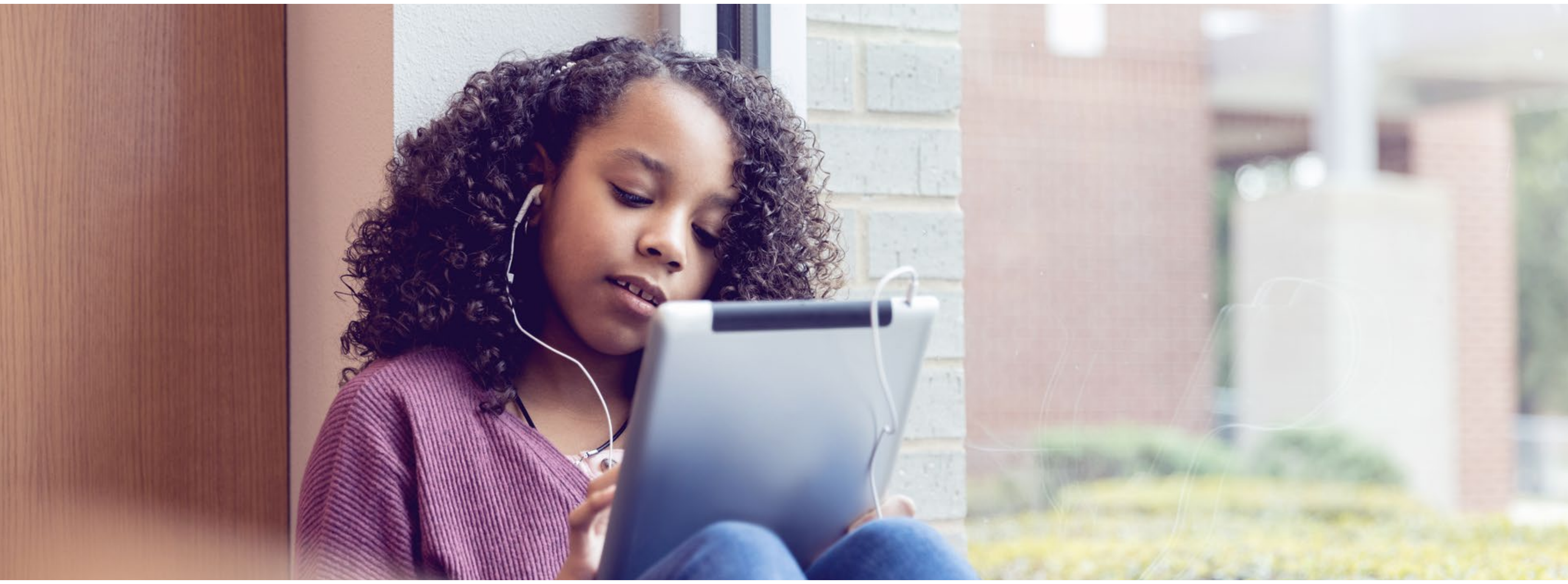
> **In March, government customers saw an unbelievable 12,725 attempted malware attacks each on average — that's 17 *every hour*.**



But even though the government customers being targeted saw the most malware attempts overall, not all government customers were targeted — or even close. In fact, the highest percentage of customers targeted in a given industry was in education, and this held true for every single month in 2020.

Those working in healthcare and retail were least likely to be targeted, as both fell below the overall average for the majority of the year.





Encrypted Attacks Rise Slightly

In an ordinary year, a rise in any given threat category is cause for concern. But this is 2020 — and with cybercriminals ramping up activity across the board, any report that doesn't require a new synonym for "skyrocketing" can be considered a bright spot, even if it isn't technically *good* news.

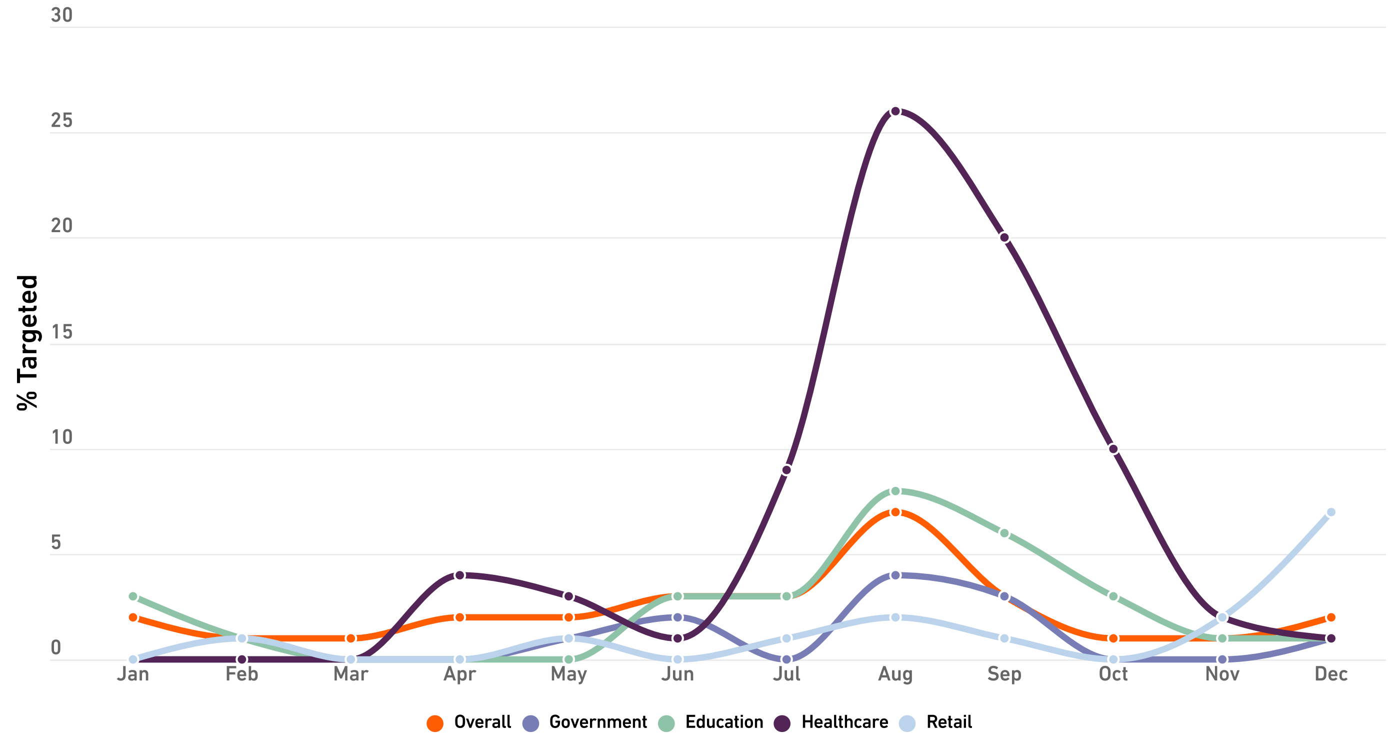
Over the past year, SonicWall Capture Labs threat researchers recorded a 4% increase in encrypted threats (i.e., malware sent across HTTPs traffic). During each month from January through June, the number of encrypted attacks fell short of 2019's corresponding monthly total.

An Uneven Upswing

While there was an overall increase of 4% in encrypted attacks in 2020, due to large variations in regional totals, this number doesn't really represent the experiences of anyone outside North America (where attacks increased 3%).

For example, Europe saw an average of 21% more encrypted attacks — while in Asia, year-over-year totals increased 151%. However, most other places in the world actually saw *fewer* encrypted attacks in 2020, with an average 16% drop over 2019's totals.

% of Customers Targeted by Malware over HTTPs



This 4% increase in encrypted attacks can be attributed in no small part to two industries: education and healthcare, which rose 292% and 351% year over year, respectively.

Of the industries we focused on in the scope of this report, one seems to be driving overall trends in encrypted threats more than any other: Healthcare. Not only did it post a huge increase, it was also the only industry to show a huge spike in August.

This makes the data for encrypted attacks an outlier: For other threat types, those working in government and education tended to be targeted at a higher rate. Encrypted attacks are the only threat type that saw a higher percentage targeted in healthcare.

Another thing makes this data unique: It's the only threat type for which those in government have the *least* chance being targeted.

What Are Encrypted Threats?

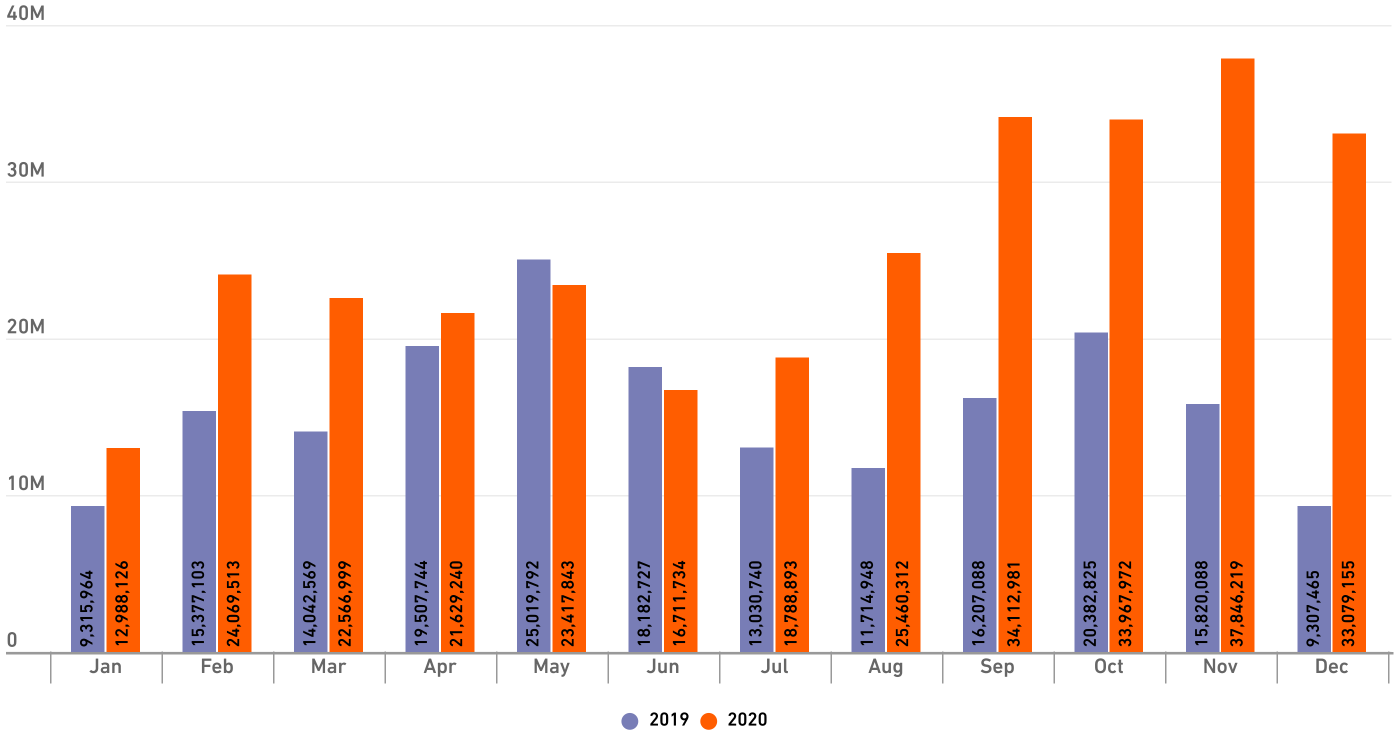
In simple terms, TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer) are used to create an encrypted tunnel for securing data over an internet connection. TLS is the replacement of SSL. When one encounters the technical term "SSL" in products or solutions, one must assume the TLS protocol is being used unless specified.

While TLS provides legitimate security benefits for web sessions and internet communications, cybercriminals are increasingly using this encryption protocol to hide malware, ransomware, zero-day attacks 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.

Ransomware Runs Rampant

2020 Global Ransomware Attacks



It didn't look *too* bad at first: In the Mid-Year Update to last year's SonicWall Cyber Threat Report, we noted a 20% year-over-year jump in ransomware. With numbers for July trending downward and people settling into the "new normal" brought by the pandemic, we hoped for the best.

By the time we released our Q3 threat data, however, that 20% increase had turned into a 40% increase. But with past years showing a dropoff toward the end of the year, there was still room for some (*very* cautious) optimism that things might yet turn around.

Unfortunately, they never did, and 2020 ended with ransomware up a staggering 62% worldwide.

How unusual was 2020 in terms of ransomware? When graphed and visualized, ransomware hit data from previous years shows mostly gentle rises and falls, with the two halves of the year fairly balanced in terms of quantity. 2019's graph, with its sine-wave consistency, is a prime example of this.

But all the usual balance and predictability that can usually be found in ransomware data went out the window in 2020.

For example, in 2019, there was a general upward trend until May, when numbers peaked, dropping until August. At that point they reversed and peaked again in October, before falling off for the rest of the year.

In 2020, the peak happened three months earlier, in February. While it remained on a downward trajectory until June, it would never again return to its low pre-COVID level of 13 million. And while ransomware levels showed a late-summer increase in both 2019 and 2020, in 2020 they soared to unprecedented heights — and then stayed there.

December is a good case in point. In 2020, December was the fourth-highest month (and it was close, at that). But in every single other year since we began tracking, December was in the bottom half for monthly ransomware totals — and in all but one year, it was in the *bottom quarter*.

But if the pandemic can explain some of the increase, why did numbers rise to a new high in July, at the same time that COVID-19 cases began a two-month drop?

To understand the behavior of ransomware in 2020, we have to look at another factor.

For ransomware to be lucrative, you need a pool of likely victims — which the pandemic provided in spades, in the form of employees working from home for the first time, many oblivious to security best practices and distracted by a rapidly changing world.

But you also need a profit motive. And as it turned out, there was enough happening on the profit side to cancel out any pandemic-related trough altogether.

Just as COVID-19 numbers were hitting their lowest point since late spring, something else was hitting its highest point all year: Bitcoin. Bitcoin rose roughly 300% in 2020, and as Bitcoin went and stayed up during the second part of the year, ransomware followed.

And while ransomware operators usually wrap their year up early, leading to lower numbers in November and December, staying in the game in 2020 was simply too lucrative.

Bitcoin's Big Score

A number of things happened in 2020 to influence the price of Bitcoin. The media, no doubt hungry for stories about anything not related to pandemic or politics, covered the uptick in Bitcoin prices extensively, attracting others looking to cash in.

At the same time, Bitcoin began to shake a lot of its shady associations. While none other than Warren Buffet referred to Bitcoin as "probably rat poison squared" as recently as May 2018, in mid-2020 institutional finance firms began investing in Bitcoin, bringing the currency an increased sense of legitimacy.

Meanwhile, other investors — wary of 2020's unprecedented stock market volatility stemming from a swirling mass of political unrest, skyrocketing unemployment and the uncharted territory of a post-COVID world — wanted someplace a little more stable to invest their money.

And Bitcoin fit the bill. While no one knows whether we will be going to the movies, buying jeans, or favoring drive-through restaurants in 2021, Bitcoin will always be a rare and limited resource. And unlike the literal standard of rare and limited resources (gold), Bitcoin is easier to store and transfer, and is more divisible.

To put Bitcoin's rise into perspective, if you owned one Bitcoin on March 14, it was worth $5,304 — enough to finance a nice vacation (not that anyone was going anywhere).

If you resisted the urge to sell and rang in the New Year with that same Bitcoin, its value would have grown to $29,112 — almost six times its original value, and enough to buy a brand-new Toyota RAV4 (with enough left over to finance your Netflix, Hulu, Disney+ and Amazon Prime streaming habits for an entire year afterward.)

By the end of the first week in January, Bitcoin had jumped even higher, breaking the $40,000 mark for the first time in history and continuing to rise in fits and starts thereafter, ultimately reaching $50,000 in February. If the Bitcoin-ransomware connection continues to hold, historic highs in ransomware are unfortunately likely to follow.

Ransomware by Region

Ransomware trends by region ran the gamut in 2020. In Europe, there was no increase, but other areas weren't as fortunate: ransomware volume spiked 158% in North America, and a mind-boggling *455%* in Asia, according to SonicWall's sensor network.

In terms of total ransomware volume, the United States once again had more than any other country, with over 203 million ransomware hits. This is more than 13 times the volume of ransomware in South Africa, the next-highest country.

Like the country-level data, the state-level data shows one region far outpacing the rest when it comes to total ransomware attacks. With 53.5 million ransomware hits, Florida had almost twice as many ransomware attacks as the next-highest state, New Jersey.

With 53.5 million ransomware hits, Florida had almost twice as many ransomware attacks as the next-highest state.

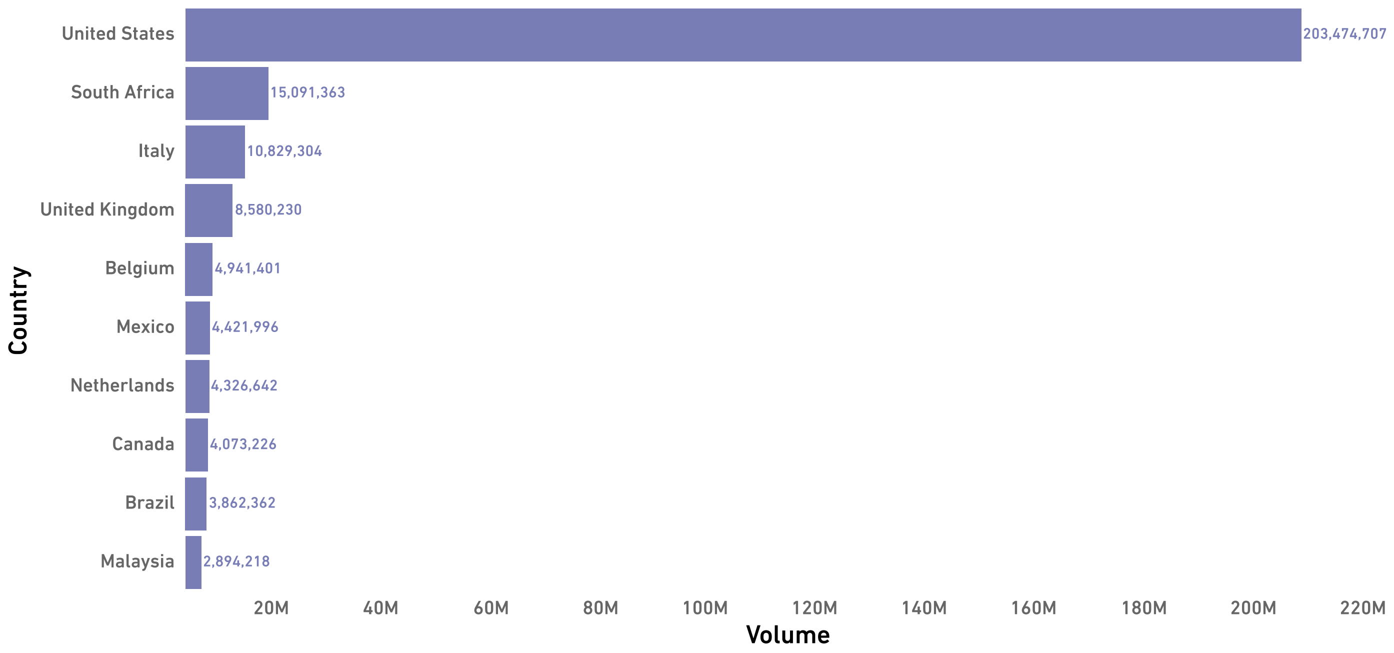
Florida saw an unusually large number of attacks in the second half, on diverse targets such as state and local governments, one of the largest healthcare provider chains in the U.S., nonprofit organizations, Miami-based Carnival Cruise Lines and more.

A New Safe Haven?

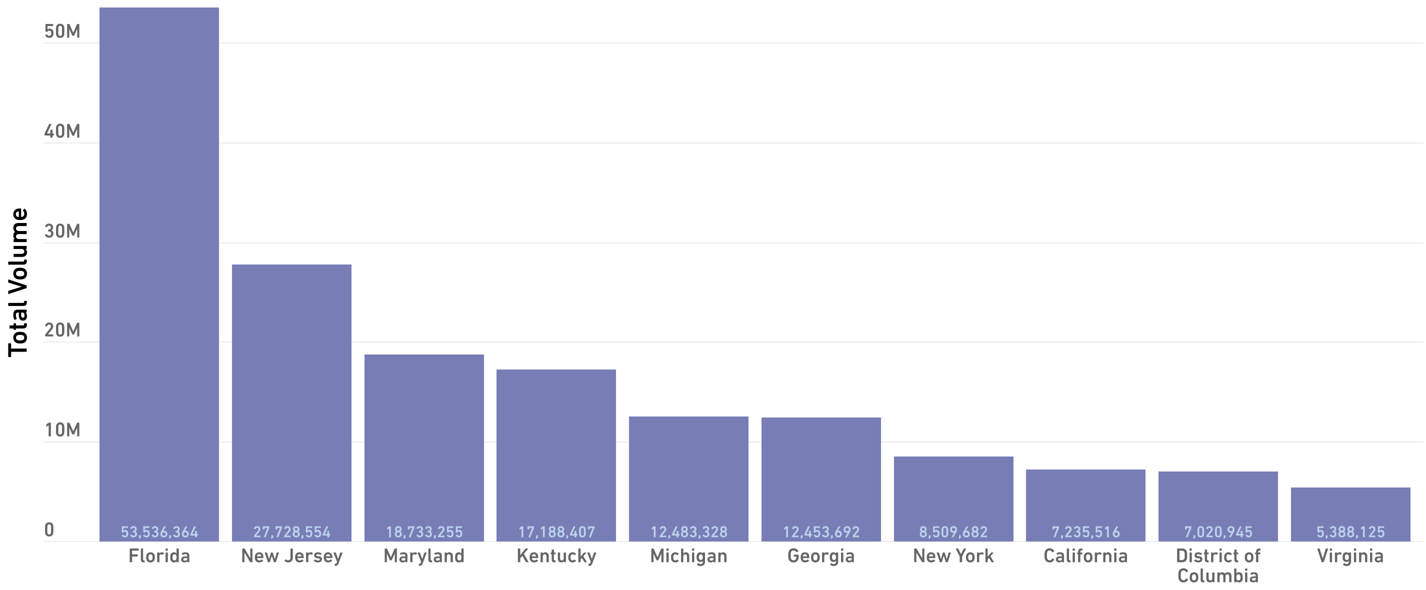
In 2020, SonicWall Cyber Labs threat researchers noticed an unusual characteristic in some of the ransomware identified. In at least two cases, Exorcist ransomware and Erica ransomware, the software is designed to spare those living in certain Eastern European countries.

In the case of Exorcist, the malware performs a check to avoid encrypting systems in Commonwealth of Independent States countries. In the case of Erica, files are encrypted regardless of the victim's location, but according to the ransomware note left in each directory, the ransomware operators promise to help with decryption if a victim lives in Russia, Kazakhstan or Ukraine, with no time limit on these requests for assistance.

2020 Ransomware Volume | Top 10 Countries



2020 Ransomware Volume | Top 10 U.S. States



Top Ransomware by Signature

Cybercriminals continued to rely on readily available ransomware kits in 2020, but there has been some movement in the rankings since last year's Cyber Threat Report. Cerber, last year's No. 1 ransomware family, slipped to second place as a new ransomware family shot up the rankings: **Ryuk**.

	Top Ransomware Signatures of 2020
1	Ryuk.RSM_27
2	CryptoJoker.RSM
3	Samsam.RSM_9
4	Cerber.RSM
5	JScript.Nemucod.AW_10
6	Cerber.RSM_20
7	Ryuk.RSM_28
8	MalAgent.RSM_99
9	JScript.Nemucod.D_2
10	GandCrab.RSM_5

Two Ryuk signatures made it into the top 10, including Ryuk.RSM_27, which was No. 1. The fact that we recorded so many hits for this signature is especially remarkable when considering that there were no hits at all recoded in January, and (comparatively) very few in February, when researchers recorded 667,000 hits, compared with an average of about 9.5 million for every month thereafter.

While Ryuk signatures got their start in 2020, no signatures died out, or even came close — in fact, only one signature family, Nemucod, ended the year at a lower point than where it started in January.

A note on GandCrab: In mid-2019, the creators of the GandCrab Ransomware-as-a-Service (RaaS) announced that they were shutting down their operation, giving those using the software a month to cease operations and cash out.

Indeed, as SonicWall threat researchers noted in last year's Cyber Threat Report, few attacks were recorded after summer 2019. So why are we seeing GandCrab now at all — let alone in the list of top 10 signatures?

It turns out the GandCrab authors are still active, and researchers are reasonably sure they're the same group responsible for the REvil/Sodinokibi ransomware, a more sophisticated form of ransomware created just before GandCrab shut down.

So while the *operation* GandCrab as we knew it is truly defunct, it's likely that the GandCrab *software* has been rebranded to some other RaaS, which could trigger detection from our signatures. This would also explain how new signatures are still being created for "GandCrab" (the most recent in October 2020).

Notable Ransomware Identified in 2020

JANUARY	
Jan. 7	MZP Ransomware Actively Spreading in the Wild
Jan. 17	New Version of Cryakl Ransomware Demands $10k for File Decryption
Jan. 28	Maze Ransomware That Contains A Maze of Code

FEBRUARY	
Feb. 7	ENC Ransomware Actively Spreading in the Wild
Feb. 14	Ako Ransomware Demands $3,000; Operators Hide Behind Tor

MARCH	
Mar. 5	Marracrypt Ransomware Actively Spreading in the Wild
Mar. 13	Legion Ransomware Variant, King Ouroboros, Charges $3,000 for File Recovery

APRIL	
Apr. 2	Project23 Ransomware Actively Spreading in the Wild

MAY	
May 4	Project Zorgo Ransomware Actively Spreading in the Wild
May 8	Instabot Ransomware Demands $490 in Bitcoin After 50% Discount
May 28	DragonCyber Ransomware Actively Spreading in the Wild

JUNE	
Jun. 5	Fake Image File Containing JavaScript Leads to Avaddon Ransomware
Jun. 18	Fake Ransomware Decryptor Spreads Zorab Ransomware
Jun. 25	CobraLocker Ransomware Actively Spreading in the Wild

JULY	
Jul. 1	BadBoy Ransomware, Variant of Spartacus, Charges $1,000 for Decryption
Jul. 23	Reha Ransomware Targeting Arabic-Speaking Countries
Jul. 31	Exorcist Ransomware Casts Triple Punishment for Non-Payment

AUGUST	
Aug. 14	VoidCrypt Ransomware Actively Spreading in the Wild
Aug. 28	Darkside Ransomware Targets Large Corporations, Charges Up to $2M

SEPTEMBER	
Sep. 4	Jackpot Ransomware Actively Spreading in the Wild
Sep. 25	Zhen Ransomware Actively Spreading in the Wild

OCTOBER	
Oct. 2	Operator of New Phobos Variant Gives Blunt Response During Negotiation
Oct. 22	Nibiru Ransomware Actively Spreading in the Wild
Oct. 26	A New Variant of Clop Ransomware Surfaces

NOVEMBER	
Nov. 6	Ragnar Locker Ransomware
Nov. 25	Exerwa Ransomware Leaked from CTF Hacker Event

DECEMBER	
Dec. 7	Egregor Ransomware
Dec. 18	Mobef Ransomware Actively Spreading in the Wild

Ryuk on a Rampage

First identified in August 2018, Ryuk got off to a slow start. In 2019, SonicWall Capture Labs threat researchers recorded 5,000 cases of Ryuk worldwide all year long. In February and September, researchers recorded zero cases of Ryuk *anywhere*. And no matter where you were in the world, you spent at least a quarter of the year Ryuk-free.

Even as late as January 2020, Ryuk didn't appear outside of North America, Europe or Asia. At the time researchers noted a mere 41 cases *total* — or a little more than one case of Ryuk a day in the entire world.

The very next month, there were more than 16,272 times as many.

February's total of 667,163 continued to climb. It crossed the 1 million threshold on its way to March, and would stay there the rest of the year, overtaking Cerber as the top ransomware family.

While Ryuk and ransomware as a whole both slumped in the summer, Ryuk rebounded more quickly: In September, researchers noted a record 19.9 million cases of Ryuk — equivalent to nearly eight cases of Ryuk *each second*.

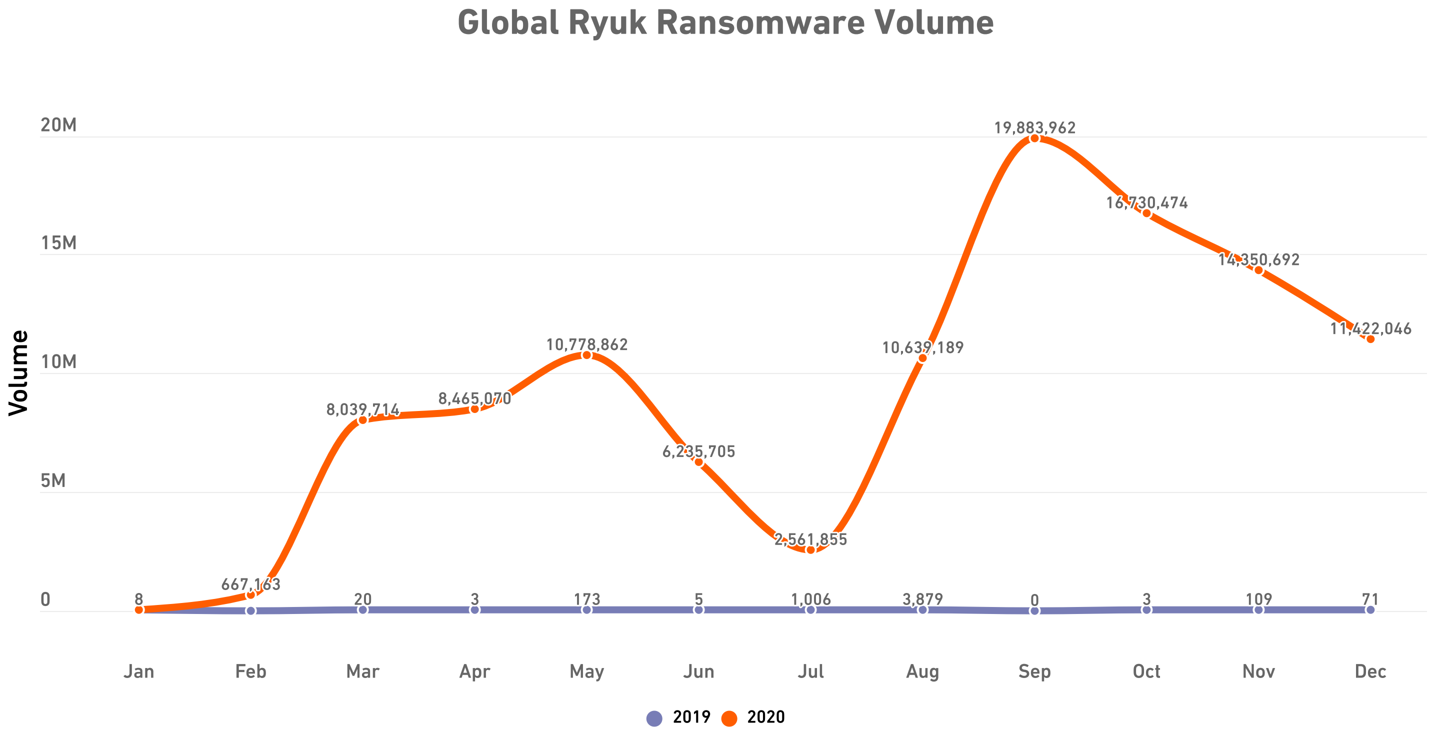
But while Ryuk was quicker than ransomware in general to rise, it was also quicker to fall. While ransomware levels in general tenaciously remained near the top of the graph as 2020 drew to a close, Ryuk did what ransomware *usually* does and fell through the end of Q4.

Despite ending on a down note, Ryuk still had 11 million more hits in December than it had in January, suggesting we're likely to continue seeing plenty of it in 2021.

Ryuk's Astronomical Growth

January 2020: Just over one case of Ryuk a day

September 2020: Nearly eight cases of Ryuk every second


Global Ryuk Ransomware Volume

Ryuk on the Rebound?

Ryuk finished the year down somewhat from the meteoric heights it reached in autumn. However, in January, the U.S. Cybersecurity and Infrastructure Security Agency warned that it had been seeing a fresh surge in Emotet attacks.

What does this have to do with Ryuk? Well, Ryuk is often leveraged via a multi-stage attack (Emotet > Trickbot > Ryuk.) So a surge in Emotet may mean that a surge in Ryuk may not be far behind.

Cerber Slips to No. 2

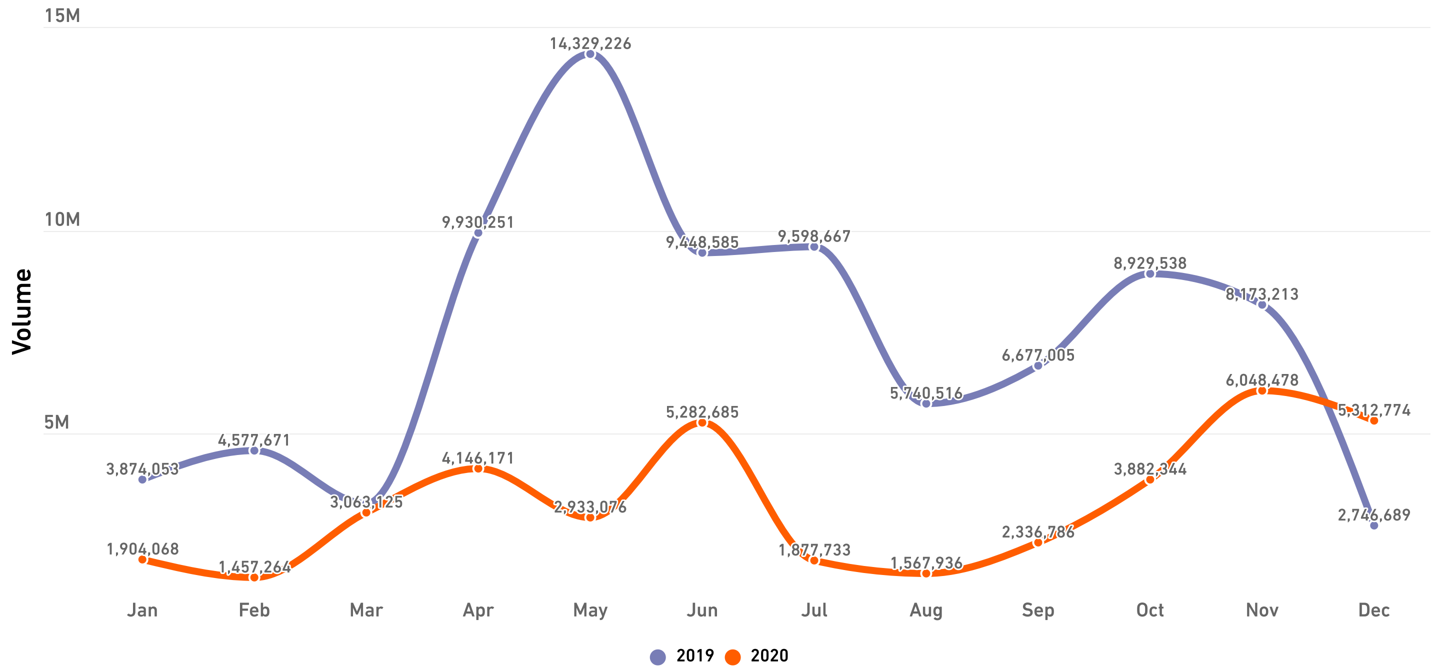
When looking at signatures, Cerber is Nos. 4 and 6 (Cerber.RSM and Cerber.RSM_20 respectively). But when looking at the top 10 *families*, Cerber's two entries on the list combine to catapult it above SamSam and CryptoJoker to No. 2.

In 2019, Cerber was the No. 1 ransomware family identified by SonicWall Capture Labs threat researchers. It boasted four of the top 10 ransomware signatures of the year, making up 33% of all ransomware attacks.

In contrast to Ryuk, the current No. 1 signature (and family), Cerber has been around for quite a while — it was originally discovered in March 2016. It follows the RaaS model: As one of the first examples of this business model, the operators of Cerber originally offered their ransomware for a 40% cut of any ransoms paid.

Cerber has been known to spread via exploit kits, malicious JavaScript attached to spam, infected websites, fake software downloads and malvertising (infected ads placed on legitimate websites.)

Global Cerber Ransomware Volume



Ransomware by Industry

In the industry-specific data for ransomware, we see the effects of the pandemic, just as we do in the overall 2020 ransomware data. But a closer look shows this expected outcome playing out in an unexpected way.

In other threat types, such as malware, IoT malware attacks and encrypted threats, spikes in the overall data usually coincide with spikes in each industry, as they rise and fall more or less in concert.

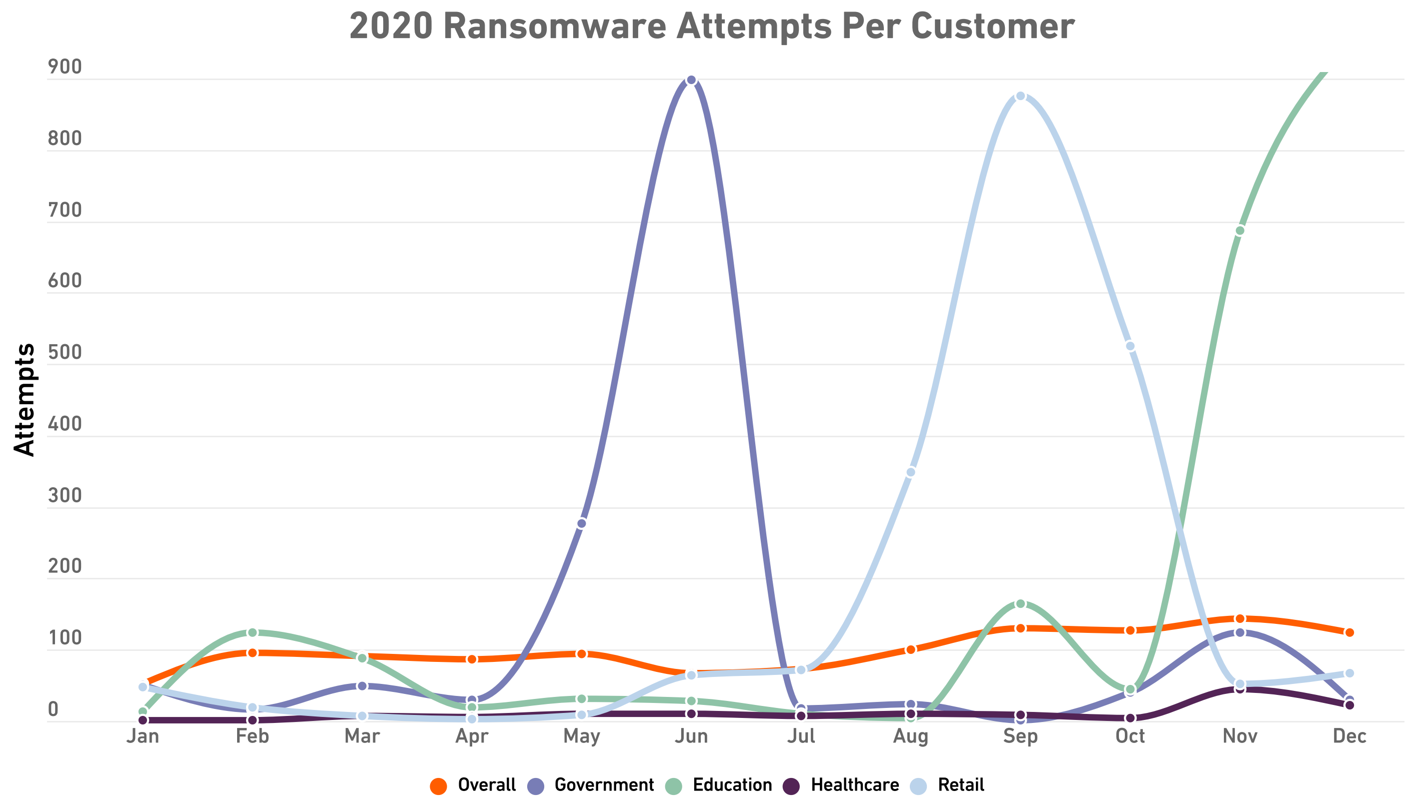
The number of attempted ransomware attacks per customer, however, shows something very different. Instead of across-the-board increases, we see three distinct instances in which one industry peaks, while the others remain nearly or completely inert. No other data set collected in 2020 shows a pattern quite like this.

In the case of government and retail, these spikes translated to overall year-over-year ransomware increases of 21% and 365%, respectively. But even with a sizable jump in the number of ransomware attempts per customer in Q4, the total volume of ransomware targeting education was still down 14% over 2019's levels.

What about the healthcare-related ransomware attacks widely reported on in the media? Those attacks tend to grab the headlines — and, in most cases, rightfully so — since they were both successful and are critical in nature.

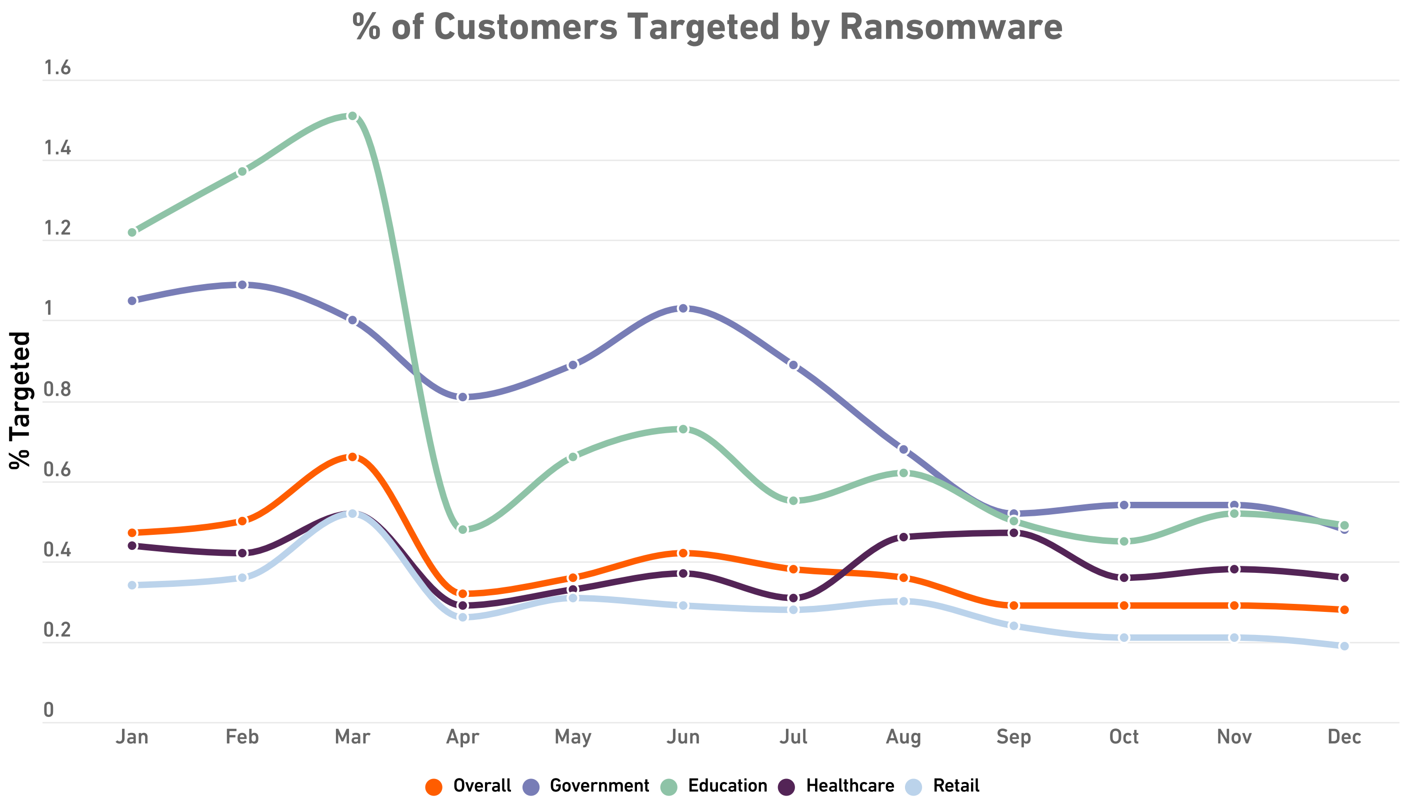
But unlike government, retail and education, there were no huge spikes in healthcare ransomware attempts — just a widespread, overall increase.

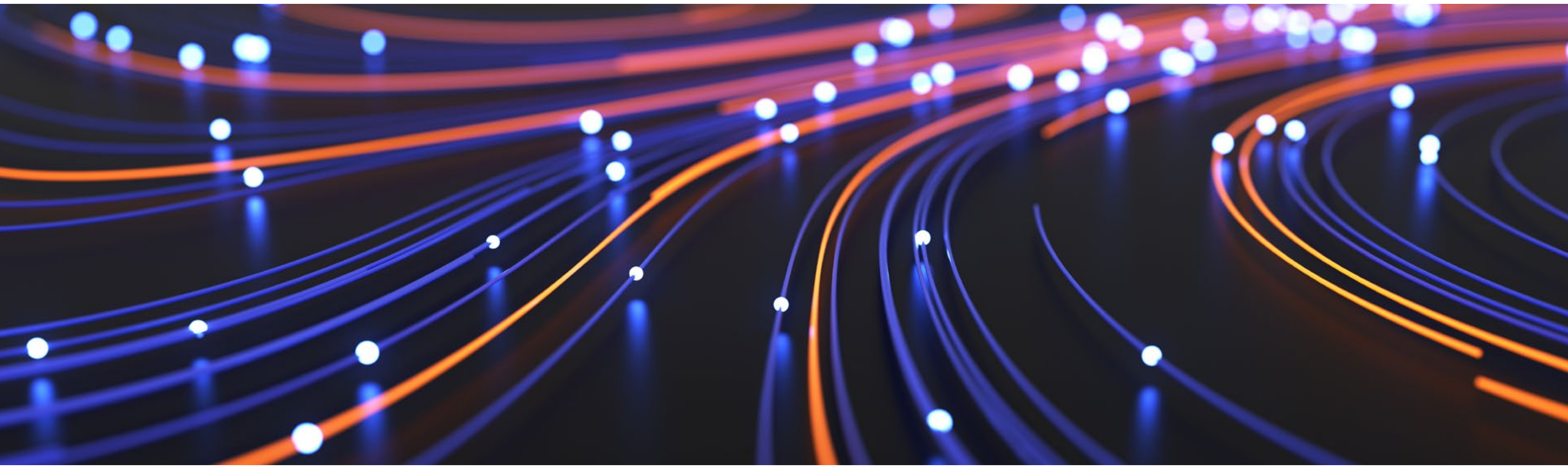
The number of ransomware attempts per customer for healthcare jumped 123% year-over-year.



It's one thing to say that attempted ransomware attacks are getting more targeted, but industry data gives us an opportunity to see this in action — as a relatively high number of attempts per customer combined with a relatively low percentage of customers targeted tends to indicate precisely that.

As ransomware as a whole shows a great deal of increase toward the end of the year, we actually see the percentage of customers targeted fall throughout the year, with every industry showing a lower percentage of customers targeted in Q4 as in Q1 — the opposite of what we would expect based on the graph of global ransomware volume.





Intrusion Attempts Rise, Upending Existing Patterns

In 2020, SonicWall Capture Labs threat researchers noted a slow and (relatively) steady rise in intrusion attempts, marked by uniform growth across regions. With every month but January exceeding 2019's high point, intrusion attempts as a whole (including low, medium and high severity) for the year were up an average of 20% overall — with malicious intrusion attempts (medium and high severity) up *112%* overall.

While this is itself unremarkable compared with past years, a closer look reveals changes in the month-to-month pattern.

In 2019, intrusion attempts started the year at roughly 345 billion and then dropped, not again reaching January's heights until October. In 2020, however, we see the yearly distribution of attacks take on an entire new character, possibly as the result of the changes wrought by the COVID-19 pandemic.

2020 also started with around 345 billion attacks. But then they *rose*, increasing by 14% in February and another 6% in March, before dipping slightly and then leveling off through late spring and summer.

From that point on, each month saw more hits in 2020 than the same month saw in 2019.

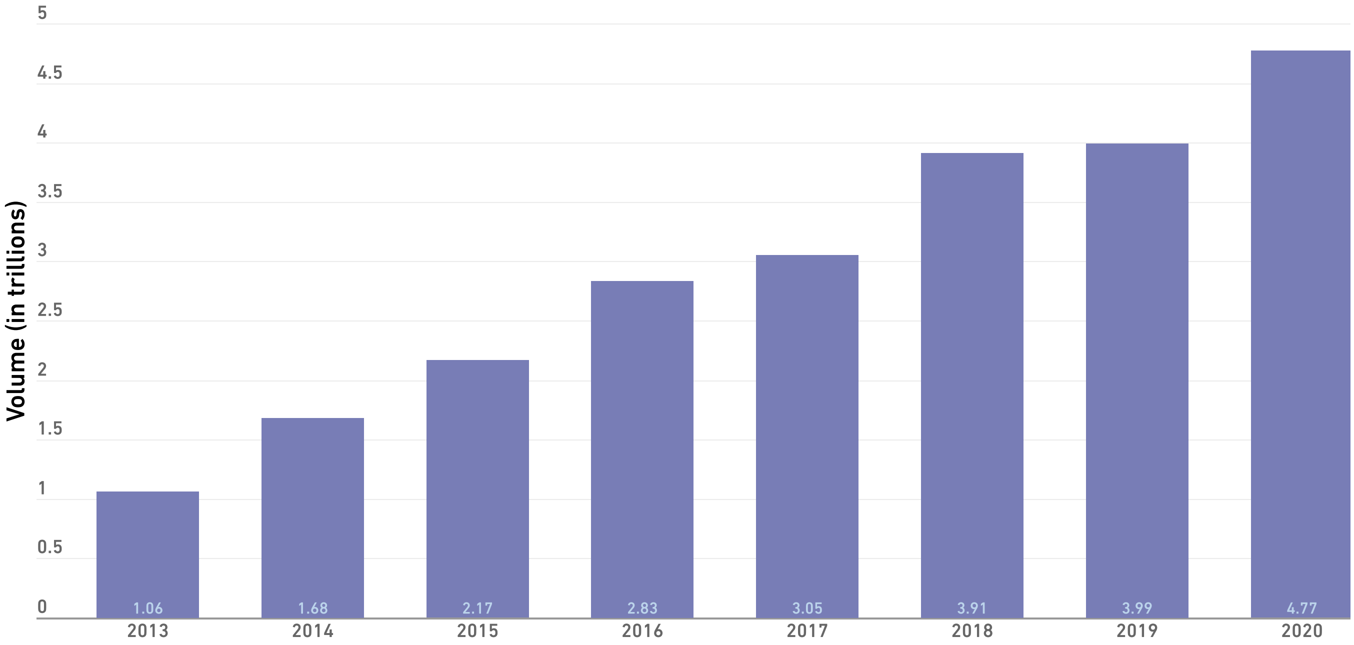
But monthly totals for the second half of the year were especially concerning: they averaged nearly double their 2019 counterparts.

September saw numbers once again on the rise — but instead of topping out in October and falling off, like they did in 2019, they kept rising, and did so at an increasing pace.

This culminated in a December with 422.4 billion intrusion attempts, by far the largest number all year. This stands in contrast with the 296.2 billion intrusion attempts seen in December 2019 — that year's low point.

It's important to note that the intrusion attempt data here is a combination of three severity types: low, moderate and high. Low-severity hits generally consist of things like scanners and pings — these are non-malicious and pose no threat to the target.

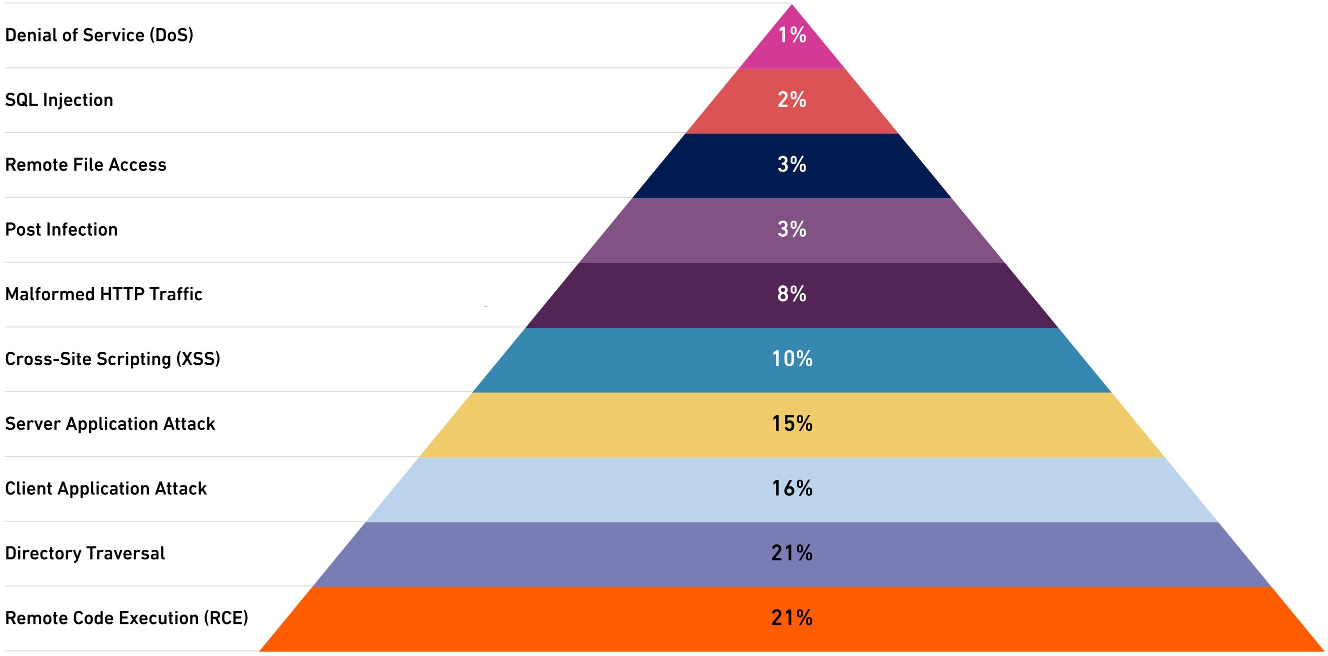
Intrusion Attempts by Year



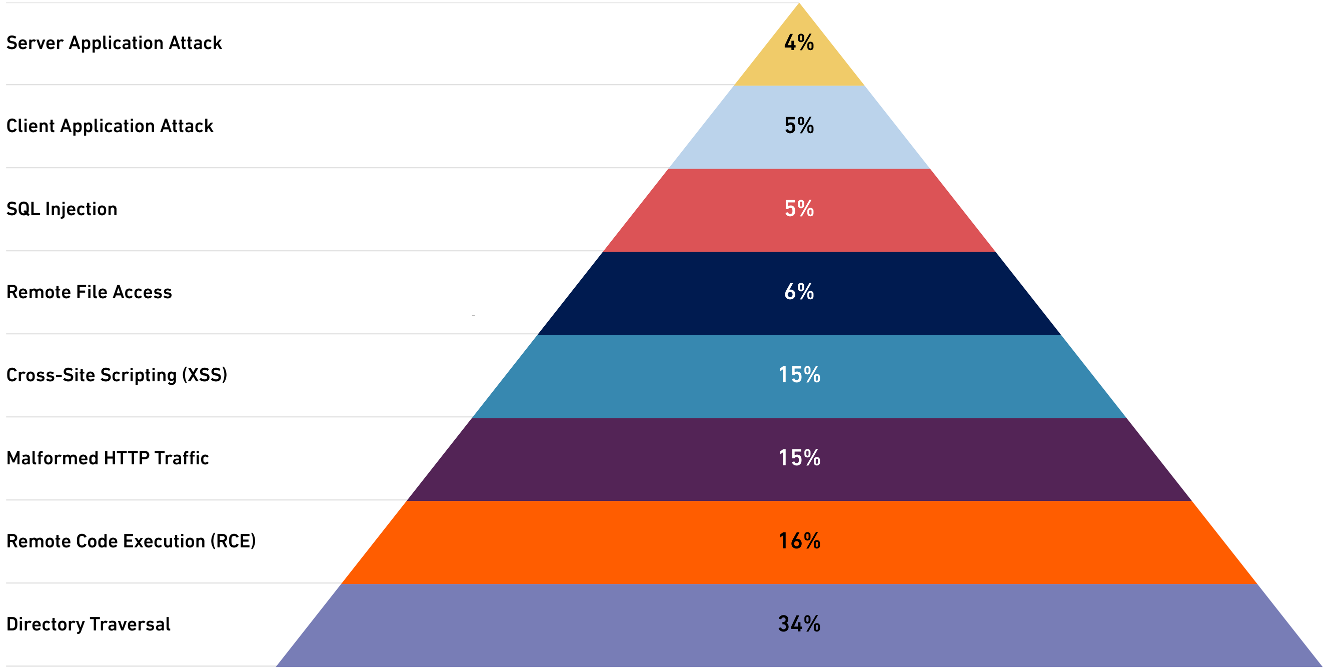
After removing low-severity intrusions, the behaviors of malicious actors — and how these behaviors are changing over time — become much clearer. In 2020, Directory Traversal attacks grew dramatically, going from 21% of total attacks in 2019 to 34% percent in 2020.

A lot of this gain came at the expense of server-application attacks (whose share fell from 15% to 4% of attacks) and client application attacks (which fell from 16% of attacks to 5%).

2019 Malicious Intrusions



2020 Malicious Intrusions



Top Intrusion Attacks

Directory Traversal

Also known as a path traversal attack, a directory traversal attack is an exploit that aims to access files and directories that are not located under the root directory. This is done by manipulating file variables, so that characters representing "traverse to parent directory" are passed through to the operating system's file system API. This allows attackers to obtain sensitive files.

Remote Code Execution (RCE)

An RCE attack takes place when a cybercriminal actor uses a vulnerability to run malicious programming code, usually in an unexpected path and with system-level privileges. The Bluekeep vulnerability is an example of this.

Malformed HTTP Traffic

Malformed HTTP traffic consists of patterns not seen in legitimate HTTP requests or responses — for example, oversized HTTP headers.

Cross-Site Scripting (XSS)

XSS attacks are client-side code injection attacks that insert malicious code, most commonly JavaScript, into the script of legitimate applications or websites. When a user visits these hacked pages or apps, the malicious code is executed, sending the malicious script to the victim's browser, with the ultimate goal of stealing the victim's information.

Remote File Access

Remote file access refers to an unauthorized individual gaining access to a file meant to be accessed by authorized individuals only.

SQL Injection

SQL injections occur when malicious SQL statements are injected into vulnerable applications or websites. This allows attackers to manipulate backend databases and retrieve or alter database information that was not meant to be accessible, in some cases giving the attacker complete control over your database.

Client-Application Attack

Client-application attacks occur when attackers target client applications directly — for example, memory leaks.

Server-Application Attack

Server-application attacks include attacks in which a threat actor targets server applications — for example, authentication bypasses.

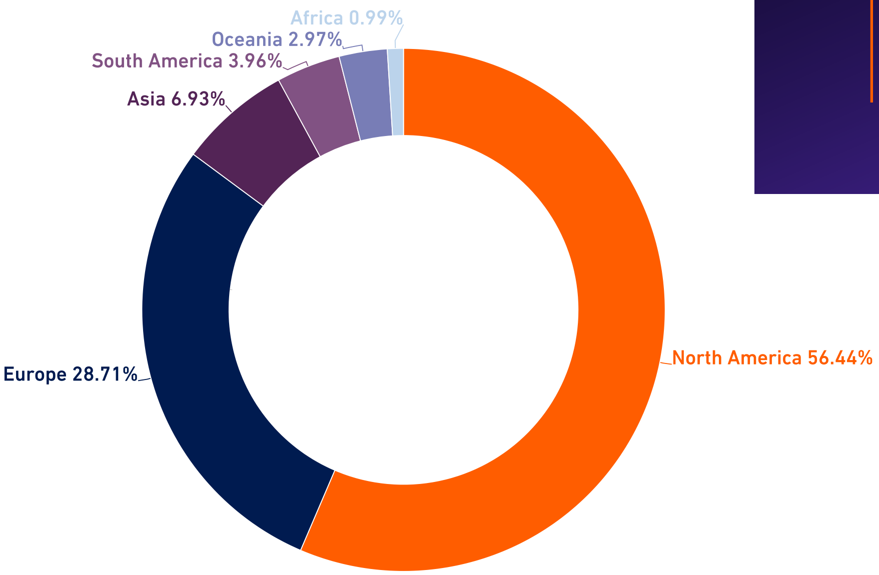
Intrusion Attempts by Region

In 2019, North America had roughly twice as many attacks as Europe (3.08 billion vs. 1.57 billion). While attacks in North America rose only slightly in 2020, to 3.99 billion, attacks in Europe *nearly quadrupled*, reaching 6.02 billion. This huge increase in attacks propelled Europe to the top of the list for IPS attacks in 2020.

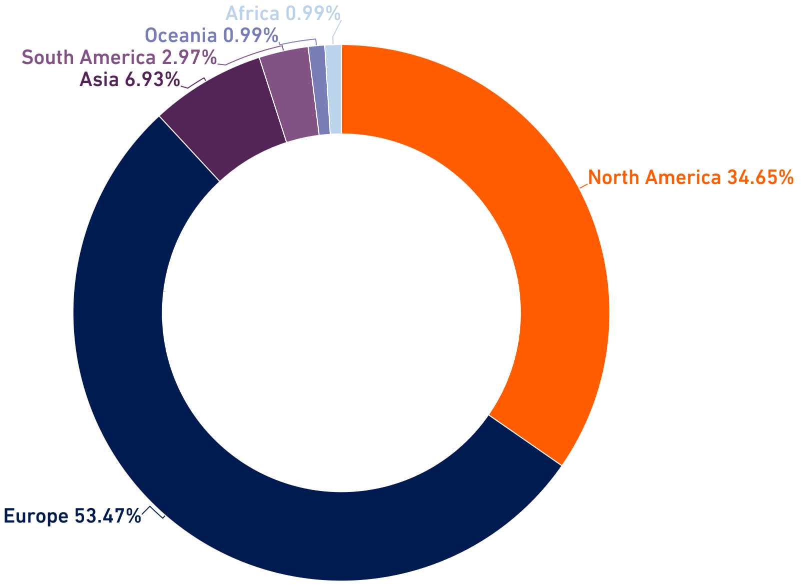
What is an Intrusion Attempt?

An intrusion attempt is a security event in which an intruder, hacker, cybercriminal or threat actor attempts to gain access to a system or resource without authorization.

2019 Intrusion Attempts by Region



2020 Intrusion Attempts by Region



In 2020, intrusion attempts in Europe *nearly quadrupled*, reaching 6.02 billion.

Capture ATP and RTDMI: Better than Ever

In 2004, before SIEM, widespread encryption and the cloud, few could anticipate threats such as Zeus, Petya and WannaCry — let alone the generation of threats that would come after.

If you were SonicWall, however, you'd already seen more than a decade of the worst cybercriminals had to offer and had a good idea of where they were going. That's why, just four years into the new millennium, SonicWall was already pioneering the use of machine learning for threat analysis.

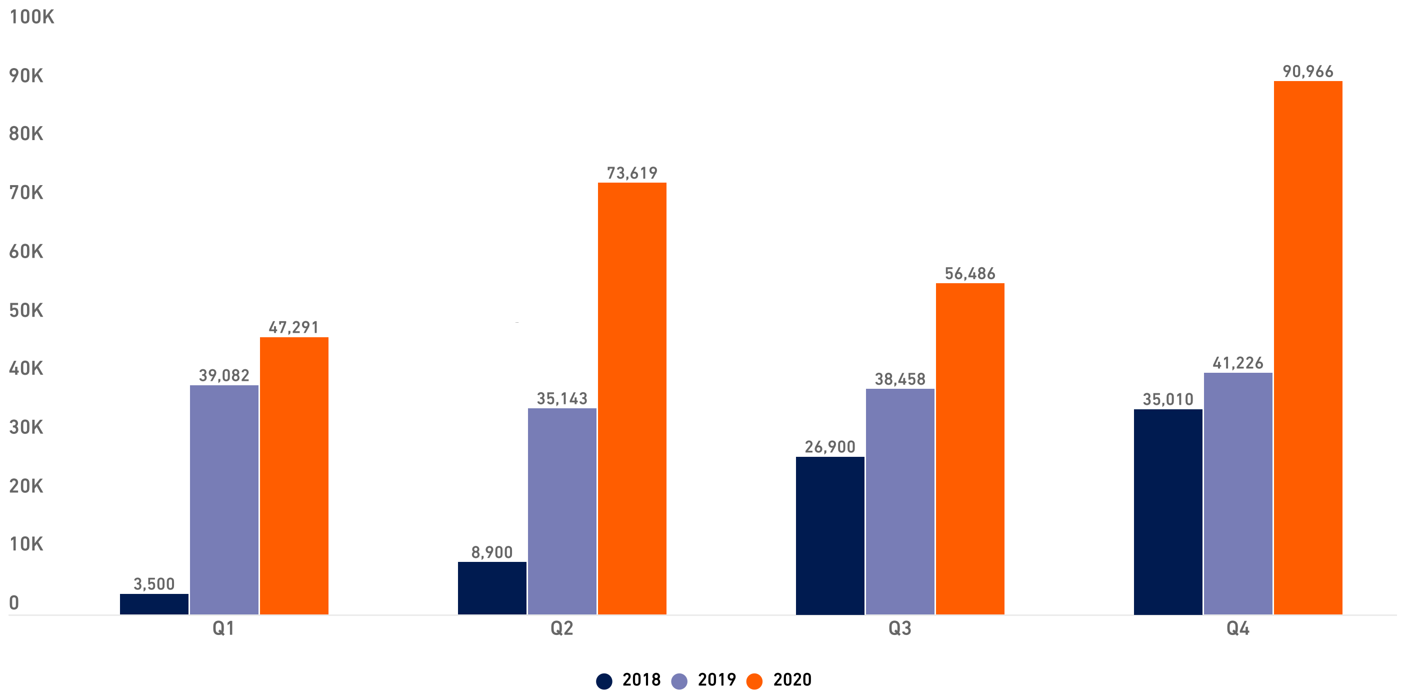
Today, an evolved form of this early machine learning technology powers SonicWall's threat intelligence. And each year, this technology grows faster, more vigilant and more intelligent, making it progressively better at identifying new malware variants.

Each year since the introduction of the SonicWall Capture Advanced Threat Protection (ATP) sandbox service with Real-Time Deep Memory Inspection™ has brought significant increases in the number of threats identified, and 2020 was no exception: **the pair found a combined 589,313 new malware variants**.

In all but three months of 2020, Capture ATP with RTDMI found not only more, but *significantly* more, threats than it had during the same time in 2019, driving a 34% increase in the number of new malware variants found.

Of the 589,313 new malware variants found in 2020, 268,362 were detected by SonicWall Real-Time Deep Memory Inspection.

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



Overall, **an unprecedented 74% more never-before-seen malware variants** were identified by RTDMI in 2020 than were identified in 2019, which recorded 153,909.

Patented RTDMI Ready for First Weaponized Side-Channel Attack

Researchers and security experts predicted that the first weaponized side-channel attack was still two to three years away. In March 2021, however, the first side-channel attack was discovered against Apple M1 Chips.

SonicWall's newly patented Real-Time Deep Memory Inspection™ (RTDMI) is able to mitigate devastating side-channel attacks. Patching systems against side-channel and memory-based vulnerabilities often requires organizations to update BIOS/firmware and software, which are not easy to deploy across large workforces or user populations.

SonicWall Capture ATP with RTDMI identifies and stops more than 1,600 new malware variants each day.

What are Capture ATP and RTDMI?

Introduced in 2016, the SonicWall Capture Advanced Threat Protection (ATP) sandbox service was designed to mitigate millions of new forms of malware that attempt to circumvent traditional network defenses via evasion tactics. It was built as a multi-engine architecture in order to give the malicious code different environments to detonate within.

To improve the speed and accuracy of determinations, SonicWall developed Real-Time Deep Memory Inspection, a patented technology that allows malware to go straight to memory and extract the payload within the 100-nanosecond window in which it is exposed. 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.

Since it can detect malicious code or data in memory and in real time during execution, no malicious system behavior is necessary for detection. In other words, the presence of malicious code can be identified prior to any malicious behavior taking place, allowing for a quicker verdict.

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.

Faster Identification of ‘Never-Before-Seen’ Malware

To minimize the damage done by a new threat, it must be identified, analyzed and blocked as quickly as possible.

That’s why SonicWall Capture Labs threat researchers and engineers are dedicated to increasing the speed and accuracy with which they identify attacks leveraging never-before seen malware variants.

Based on data from VirusTotal, a market-leading malware repository, SonicWall is identifying never-before-seen malware variants on average an entire day before VirusTotal receives the samples. This extends to 1.81 days for PDF files, 1.9 days for PE files, and 5.4 days for APK files.

In some cases (see table below), SonicWall is discovering new threats nearly half a year before samples are submitted.

This is accomplished by leveraging the SonicWall Capture ATP with RTDMI. Together, they identify and stop more than 1,600 new malware variants each day. SonicWall immediately deploys signatures for these samples to protect active customers.

Fast Detection in Action: A Sample of SonicWall’s Never-Before-Seen Malware Variants

TYPE	SONICWALL DETECTION	VIRUSTOTAL SUBMISSION	FILE HASH
PE32 executable (GUI)	Jan. 28, 2020	July 21, 2020	26a422e8ae54096f64ddf2fabd4d8da550cf74cbdfb43a11cca3353a4109714f
PE32 executable (GUI)	Jan. 29, 2020	July 21, 2020	486d956b449cf689aebeb251b0455b352da7c1191bd9985f65074f376c6fa2bb
PE32 executable (GUI)	March 5, 2020	Aug. 13, 2020	18f35b06a7cf09062a51987819c415b510285491d2d9ad4e244a3dc3cb230a9d
PE32 executable (GUI)	May 20, 2020	Aug. 22, 2020	2a8c6937aa3fd0ace698ad7e12fc2cc354a76bffdae65c5e6182bbc16119e673
PE32 executable (GUI)	Jan. 8, 2020	April 12, 2020	28618c5e0244682e7f98a6b51ccbc9904cef5b32145caadc6a403e2ca9f13967
PE32 executable (GUI)	July 30, 2020	Oct. 13, 2020	029e4e886a3001167319dc2095f47e36881b4f9e600742bf32e2b95a8890b8cb
PE32 executable (GUI)	Feb. 13, 2020	April 17, 2020	18577a4c15b6c78d62be3a4f8086a36313b5dcc44c5a55ac4d78b3691bceaf9d
PE32 executable (GUI)	July 3, 2020	Aug. 13, 2020	0886a52a4f08c32b3e7a75f38345600bc6aa0296c8f7cc1b372e5ed5c7cc78f1
PDF	June 22, 2020	June 29, 2020	65fac50a84aca7b8ae9102ec1da54c7cda4d7a4cad8e64cfdbc9ba504df7cff4
Composite Document File V2	June 3, 2020	July 5, 2020	e6f6add79b87507658b0a254f2f51fbca3f00b63cdd926f7d9667d94e15b500f
PE32 executable (GUI)	March 2, 2020	April 10, 2020	501fcc0cbb3a4057c638d5c3e4d249133f40573295683acae44b07b08b096ba0
PDF	June 17, 2020	June 29, 2020	793a1e5b017e7275e5193b3a56dc90546832ffe22e1f1d822644b727492c240f

Malicious Office Files Overtake Malicious PDFs

In 2019, cybercriminals utilized new malicious Office files and new malicious PDFs in fairly equal number (20% and 17% of total malicious files, respectively.) The two filetypes went back and forth the entire year, with each spending about six months ahead of the other.

But in 2020, this gap widened significantly. By the end of the year, the share of new malicious Office files had risen 67%, to roughly 1 in 4. In contrast, the share of new malicious PDF files actually fell 22%, to 1 in 10.

Looking at the trend graph for 2020, there's none of the volatility of the previous year, and Office files led by a significant number from September 2019 until November of the following year.

There are several reasons Office files may have taken such a definitive lead in 2020, but a lot of it likely had to do with working from home. In spring 2020, Microsoft announced its total number of active commercial Office 365 users had topped 258 million. That's a lot of Office files flying back and forth, making a malicious Office file more likely to blend in with legitimate files. As people collaborate at a distance, they're unlikely to see an Office file that appears to come from their boss or coworker as being suspicious.

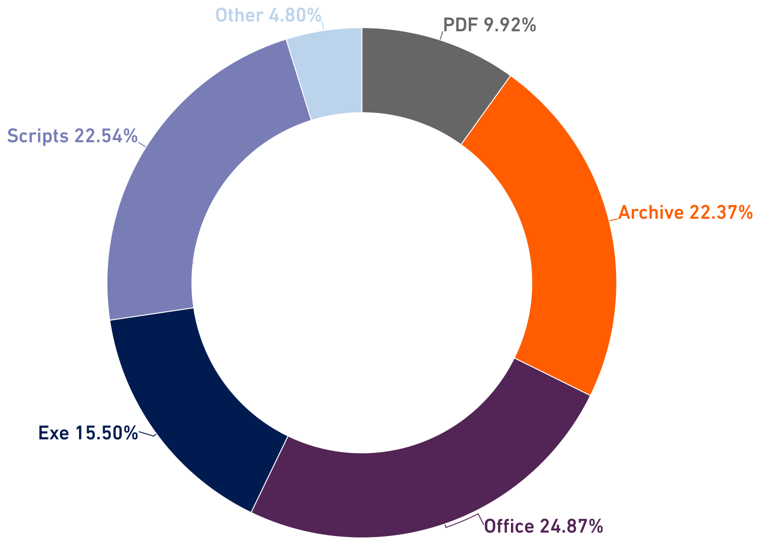
On the other hand, PDF files are searchable, can be viewed on any device, are easy to create, and may be encrypted for security, password-protected or digitally signed for authentication.

By the end of 2020, the share of new malicious Office files increased 67%, to roughly 1 in 4.

Criminals use both file types to spread phishing URLs, embedded malicious files and other exploits. Unlike .exe files, which used to make up a larger share of total malicious files, businesses tend not to restrict the ability of Office files or PDF files to be sent and received.

Unfortunately, cybercriminals have gotten better and better at fooling their targets by imitating trusted individuals and businesses. And with malicious PDFs and Office files now able to infect unrelated files on a target's devices, even completely legitimate files from known senders aren't necessarily safe.

2020 New Malicious File Type Detections | Capture ATP



Reports of Cryptojacking's Death Have Been Greatly Exaggerated

In March 2019, Coinhive, by far the largest legitimate cryptocurrency mining operation, shut down. Headlines around the world predicted the subsequent death of cryptojacking, and indeed, attacks fell 78% between July and Dec. 31 of last year.

When attacks then tripled between December 2019 and March 2020, reaching a three-year high, it seemed like little more than a swan song — one last cash-out before shifting to other attack vectors.

After all, Coinhive was (still) dead, with no heir apparent, and the number of cryptojacking hits crashed hard in April. When we published our mid-year update to the *2020 SonicWall Cyber Threat Report*, cryptojacking volume was hovering at around 20% of that (seemingly) anomalous high-water mark.

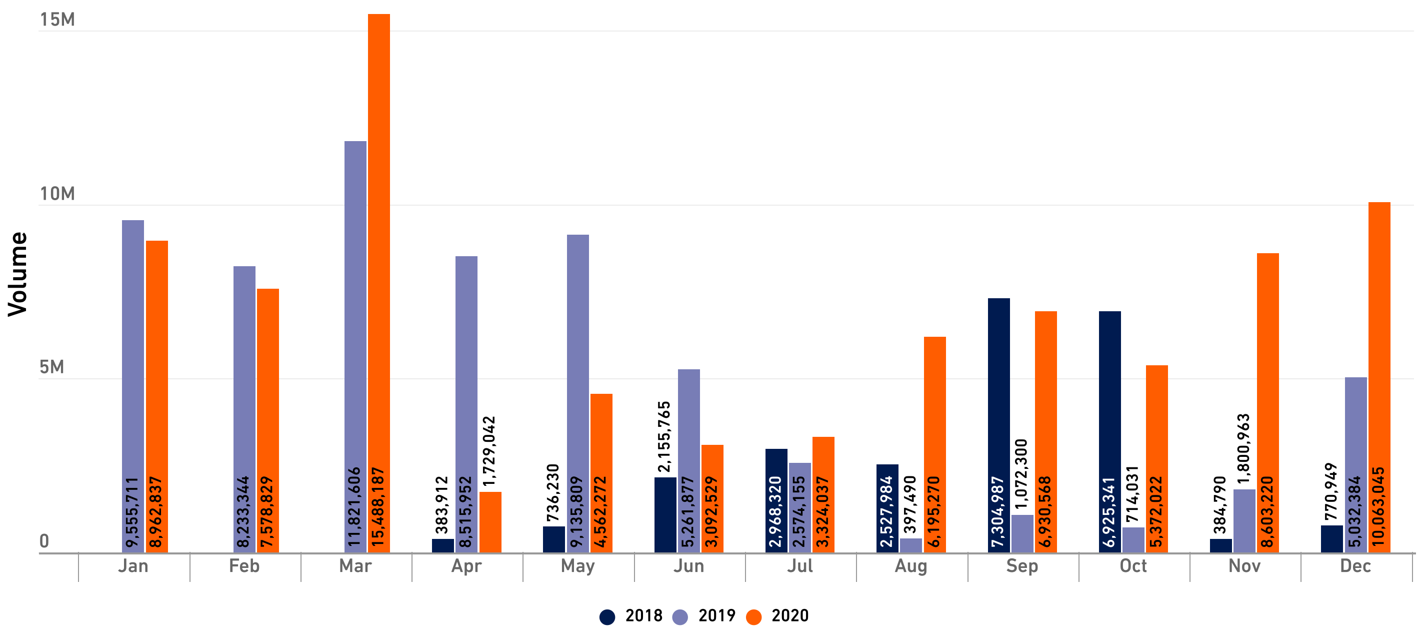
But during the second half of 2020, something curious happened. Cryptojacking pulled out of its stagnation and began to rise, with five of the six months in the second half of 2020 showing an appreciable increase. Defying all reports of its demise, December 2020 had twice the volume as December 2019, and wound up being the second-highest point since SonicWall began recording cryptojacking.

These unexpected spikes in Q1 and Q4 pushed total cryptojacking for 2020 to 81.9 million, up 28% from last year's total of 64.1 million. In fact, Q2 was the only quarter in 2020 that didn't register an increase over 2019.

Last year, Asia had 35.7 million cryptojacking hits, while North America had 19.4 million. But in 2020, the tables turned, as cryptojacking fell 87% in Asia and rose 260% in North America.

This reversal is actually the continuation of a long-established trend. In 2018, the first year SonicWall tracked cryptojacking, North America was third out of four regions, trailed only by Europe and only recording half of Asia's total cryptojacking volume.

2020 Global Cryptojacking Volume



What's Responsible for the Rise?

The data for cryptojacking bears little resemblance to any of the COVID-19 data — that may be a factor, but it doesn't appear to be the driving factor here. And a look at historical Bitcoin data might make it tempting to assume the vagaries of the coin market aren't having much of an impact, either.

But unlike with ransomware, Bitcoin doesn't tell the real story here.

When it comes to ransomware, cybercriminals depend on people who are often cryptocurrency novices to find, obtain and remit coin to pay the ransom. While Bitcoin isn't as anonymous as other forms of cryptocurrency, this additional level of risk is justified by the fact that using Bitcoin is easier and more palatable for ransomware marks.

But cryptojacking, also known as malicious mining, makes its money in the shadows. The process starts 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. By mining cryptocurrency directly rather than demanding it, cryptojacking groups can forego the risks of using the more transparent Bitcoin, and focus their attention on so-called "privacy currencies" — particularly Monero.

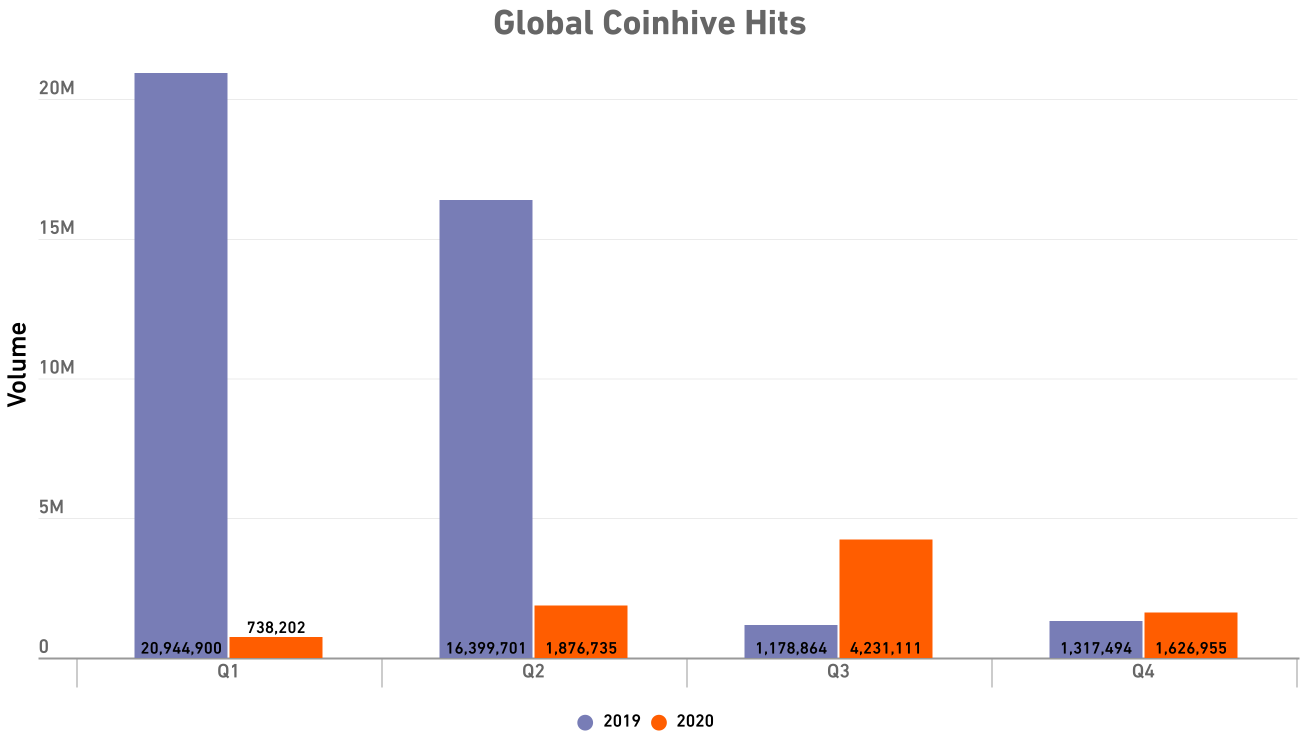
Indeed, comparing the graph of cryptojacking with that of Monero shows a much closer correlation that can be seen throughout the year — only a week or two removed. Cryptojacking's largest fall, between March and April, corresponded with a freefall in the price of Monero. This pattern was also seen in the shared dip in early autumn, and a sustained rise through the end of the year.

The Fall of Browser-Based Cryptojacking

Coinhive started as a legitimate way for websites to earn revenue without showing ads. Coinhive-enabled websites allocated a small portion of visitors' processing power to legitimately mine cryptocurrency.

Unfortunately, attackers instead used this technology to infect a large number of websites with Coinhive scripts, using the processing power of unsuspecting victims to surreptitiously mine cryptocurrency for themselves.

While cryptojacking wasn't directly implicated in Coinhive's decision to shutter (operators cited the drop in hash rate and an 85% depreciation in the price of Monero), the shuttering of Coinhive *was* expected to kill cryptojacking.



This prediction wasn't entirely wrong: the closing of Coinhive *did* succeed in helping lower the amount of browser-based cryptojacking (though internet browsers that check for cryptojacking-related JavaScript files also deserve some of the credit.)

A good example of what's happened to browser-based malware can be seen in the trends of Coinhive signatures themselves. In 2019, there were 39.8 million Coinhive hits, 37.3 million (94%) of which occurred in Q1.

In 2020, there were 8.5 million Coinhive hits all year, a 79% year-over-year drop (though, paradoxically, the second half of 2020 finished with more hits than second half of 2019.)

And the Rise of File-Based Cryptojacking

As mentioned before, the death of cryptojacking was widely predicted from the moment Coinhive announced it would be ceasing operations. However, as early as the 2019 SonicWall Cyber Threat Report, which was released just a couple months after the February announcement, SonicWall Capture Labs threat researchers predicted there would "still be a surge in new cryptojacking variants and techniques to fill the void."

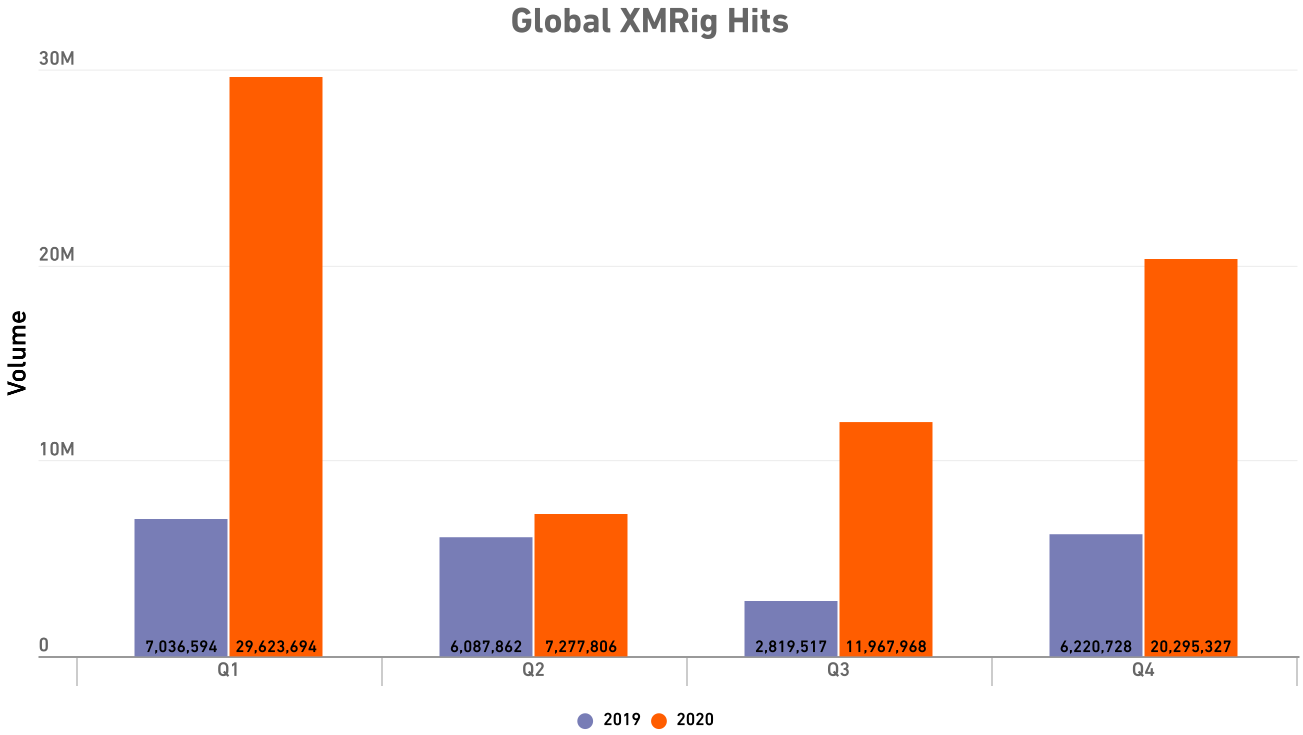
Cryptojacking, the report noted, "could still become a favorite method for malicious actors because of its concealment; low and indirect damage to victims reduces chances of exposure and extends the valuable lifespan of a successful attack."

Unfortunately, this prediction has come true, as we've seen a drastic rise in file-based cryptojacking, which works by compromising a device in order to download and deploy payloads designed to mine cryptocurrency.

While the easy-money era of Coinhive was over and a new era of browser crackdowns had dawned, cryptocurrency prices were still rising and cybercriminals still wanted to cash in.

So they began increasingly turning to file-based cryptojacking such as XMRig, an open-source cross-platform miner. XMRig, whose name is a play on the symbol for Monero, "XMR," is dropped on the victim's machine by a number of different types of malware, like Vivin and BlueMockingbird.

XMRig signatures hit an all-time high in Q1, reaching 29.6 million and almost singlehandedly accounting for the spike in overall cryptojacking we see in March. In the second quarter, XMRig hits fell to roughly a fourth of that total (handily accounting for the mid-spring drop.) XMRig hits rose to nearly 12 million in Q3, and remained more or less steady through Q4 (11,742,081).



Top Cryptojacking Signatures

2019	
Coinhive.JS_2	35,702,439
XMRig.XMR_11	7,619,428
XMRig.XMR_3	5,710,905
CoinHive.JS	4,505,299
XMRig.XMR_4	2,457,058
XMRig.XMR_8	2,259,016
Minerd.LC	949,848
BitMiner.KJ_2	877,284
XmrMiner.A	174,438
CoinMiner.A_30	128,117

2020	
Coinhive.JS_2	77,585,213
XMRig.XMR_11	43,243,304
XMRig.XMR_3	15,481,435
XMRig.XMR_4	10,065,366
CoinHive.JS	6,814,769
CoinMiner.OF_3	6,413,194
BitCoinMiner.CA	5,672,621
CoinMiner.IA	3,425,952
XMRig.XMR_8	3,015,872
CoinMiner.C_4	1,965,274

The Crushing Cost of Cryptocurrency

In the beginning, mining cryptocurrency was accessible to anyone with a decent rig. But after a while, mining became complex enough that even those with top-of-the-line PCs and high-end processors had trouble making much money.

But as cybercriminals soon discovered, the costs of cryptomining become much less of a drawback when they're borne by someone else.

And there are actually a number of costs associated with the illegal mining of cryptocurrency. First of all, there are the enormous energy bills: Mining Bitcoin alone uses up the energy equivalent of a country of more than 200 million people, or seven nuclear power plants worth of power.

There's also the loss of productivity due to diverted resources, potential damage to systems, and risk of data compromise and other security dangers.

Unfortunately, unlike with other forms of malware, cryptojacking can take place entirely in secret — meaning these costs can compound for a significant amount of time without the victim becoming aware.

Gamers Vs. Miners: The Other Battle for Resources

In early February, NVIDIA released its GeForce RTX 3060, a highly anticipated GPU (graphics processing unit) that touted unprecedented performance for its price point. While gamers flocked to retailers to purchase the card, they soon found themselves in competition with cryptominers, who had discovered it could be programmed to mine cryptocurrency, particularly Ethereum.

To help ease the shortage and ensure the card found its way into the hands of its intended market (i.e., gamers), NVIDIA took two drastic steps. First, it modified the software to detect the Ethereum mining algorithm. If identified, the card would limit the hash rate by roughly half, making the GPU much less desirable to miners while maintaining performance for gaming and other applications.

At the same time, NVIDIA announced the introduction of NVIDIA CMP, or Cryptocurrency Mining processor, designed specifically to mine Ethereum. These cards feature the improved airflow and lower peak core voltage and frequency that miners look for in a card — and because these improvements were made possible by eliminating the card's graphics component, there's no worry that gamers will turn around and monopolize the CMP market.

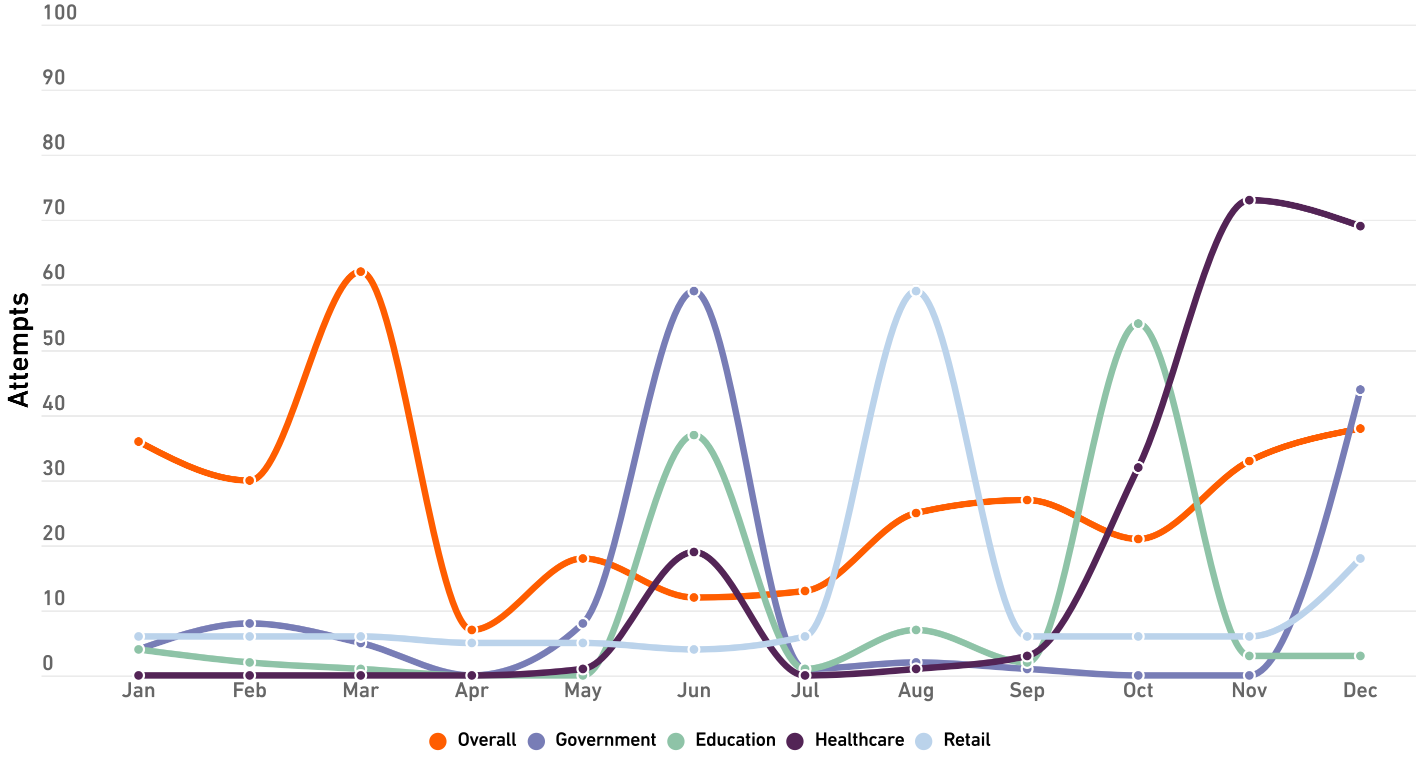
Cryptojacking Attempts by Industry

As previously noted, Cryptojacking is up, but within this category lay a lot of variation.

Large year-over-year decreases were recorded for government and retail (68% and 67% respectively). Education saw an even larger change, but in the other direction, with 110% more attempts per person than in 2019 — a figure fueled almost entirely by spikes in June and October.

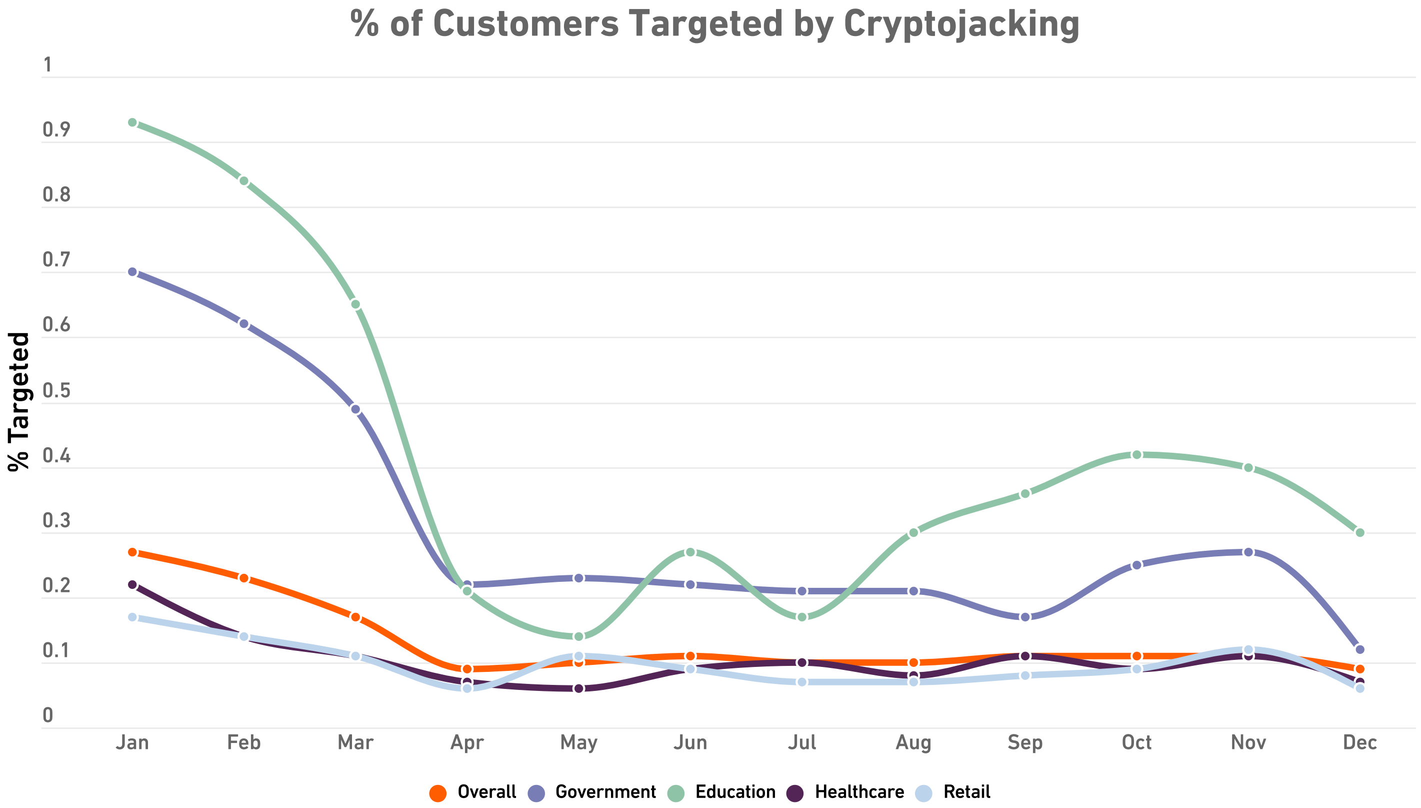
Healthcare saw an astounding 1,391% increase in numbers of attempted attacks per customer.

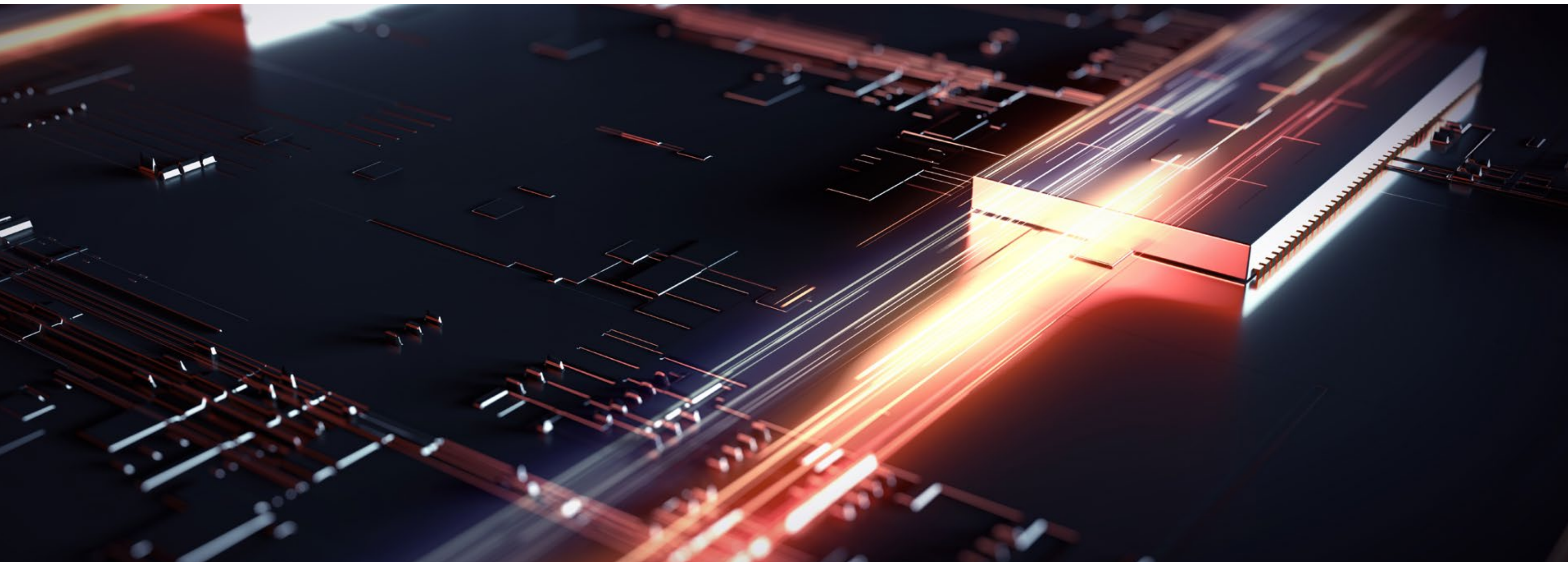
2020 Cryptojacking Attempts Per Customer



The data for the percentage of customers in a given industry targeted by cryptojacking shows an odd phenomenon: while cryptojacking as a whole peaked in late Q1 and late Q4, these are precisely the periods in which we see the percentage of customers targeted contracting.

This suggests that the increases in total cryptojacking volume were fueled almost entirely by an increase in the number of attempted *attacks*, rather than the number of targets — and were driven by industries not examined in the scope of this report.





IoT Malware Attacks Skyrocket

When the COVID-19 pandemic struck, work went home — and cybercriminals followed, propelling IoT malware attacks to new heights. While IoT malware attacks have been rising since SonicWall began tracking them in 2017, in 2020 they skyrocketed, based on a number of factors, including the use of compromised home IoT devices for personal gain.

In 2019, SonicWall Capture Labs threat researchers recorded 34.3 million IoT malware attacks. In 2020, that number rose to 56.9 million, a 66% increase.

The circumstances surrounding the pandemic did more than add to the total, however. They also upended some longstanding trends. In 2017, 2018 and 2019, IoT malware attacks dropped from January to February. 2020 bucked this trend, however, as February's numbers marked a climb that would persist until April. Rather than occurring in February, 2020's dip occurred two months later, as April's totals fell to 2.1 million, roughly half the 4.0 million attacks recorded in January.

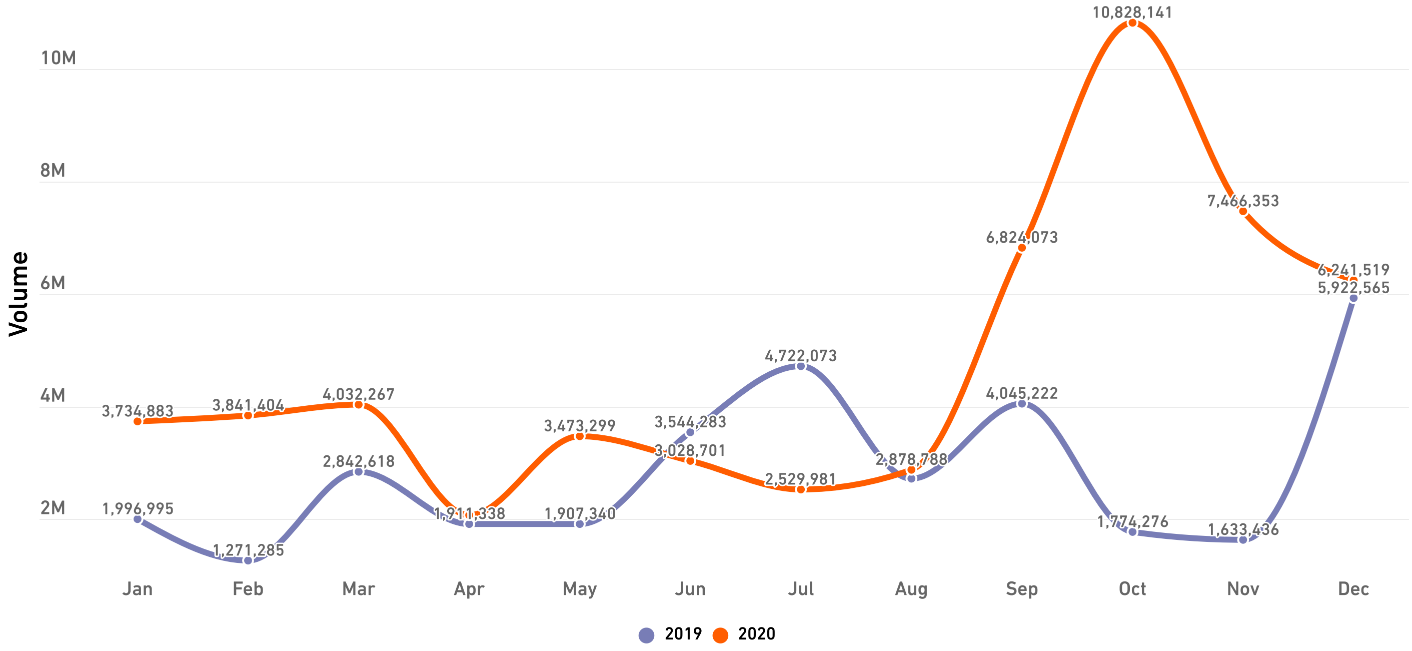
This anomalous behavior persisted into Q2, as the summer spike exhibited in 2018 and 2019 never arrived. Instead, we see a trough in the data, with its low point in July — the month that in previous years has been a high-water mark.

This may be due to the reopening efforts that began in early summer — as employees sporadically headed back to the office, the amount of time they spent connected to the corporate network from home would fall, perhaps driving cybercriminals back to other, more sure ways of making money.

But in fall, two things happened: COVID-19 cases began rising more rapidly, and children returned to school, both of which may have brought more employees back home. Suddenly, cybercriminals had two options to exploit — the corporate network, and that of any schools or universities that were also connected to through that network.

IoT attacks generally reach their highest point in fall, as can be seen in 2017 and 2018 data; 2020 was no different.

2020 Global IoT Malware Volume



But with attack levels in 2020 already much higher, October's spike set a new record. During that month, there were 10.8 million IoT malware attacks — more than the October totals for 2018 and 2019 put together. Even more shockingly, this number is higher than the number of IoT malware attacks SonicWall recorded for the *entirety* of 2017.

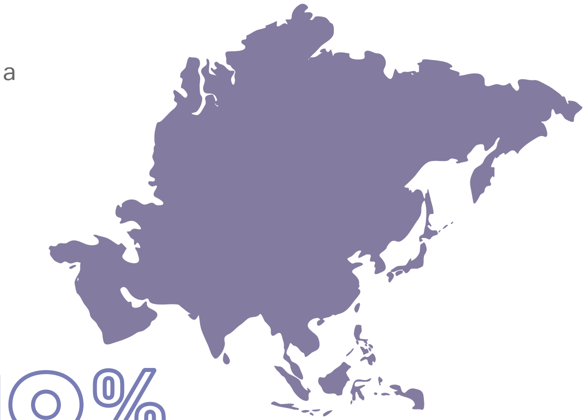
IoT Malware by Region: Europe Sees a Boom, North America Sees an *Explosion*

IoT attacks rose in every region in 2020, but it wasn't an even rise. Asia saw an increase of 18%, slightly edging out Africa, Australia and South America, where IoT malware attacks increased 17%. In Europe, attacks increased an alarming 48% — but that was nowhere near the increase recorded in North America, where IoT malware attacks rose a staggering *152%*.

Oddly enough, given this inconsistency, three out of four regions recoded their highest month in October, including North America, Europe and Asia — where October's numbers were more than double the average for the rest of the year, and largely drove the region's more modest year-over-year increase.

^17%

In Africa, Australia and South America, IoT malware attacks increased 17%

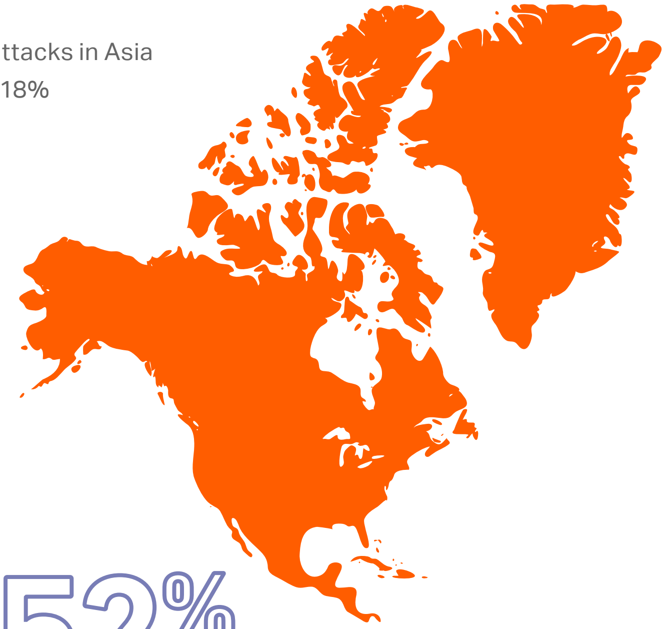


^18%

IoT malware attacks in Asia increased by 18%

^48%

IoT malware attacks in Europe increased by 48%



^152%

IoT malware attacks in North America increased by 152%

More Devices, Greater Reward … Same Security

While the spike in IoT attacks is alarming, it isn't surprising, for a number of reasons. For starters, there's never been more IoT devices to target. According to Security Today, from 2018 through 2020, the number of devices jumped from 7 billion to 31 billion, with an average of 127 new devices coming online every second.

By the end of 2020, IoT technology was projected to be present in the designs of 95% of new electronics products. And over the next five years, the number of connected devices is forecasted to climb to 41.6 billion and generate a mind-boggling 79.4 zettabytes (ZB) of data (for reference, the entirety of the World Wide Web, as it existed in 2009, was estimated to be less than half of one ZB.)

And while the variety and complexity of IoT devices grows, there's one area that remains largely ignored: the means by which to secure them.

There is still no standard for securing IoT devices — meaning that companies are free to make them as secure or unsecure as they want, though this is beginning to change (see page 62).

Many times, particularly with lower-cost items, security is scant or nonexistent to save money on manufacturing. Even when this isn't the case, if vulnerabilities are discovered, in many cases updates to address them are never pushed out, leaving these devices open to exploitation for their entire lifespan.

But the growth in IoT devices has been ongoing for years, in a fairly predictable manner. And we've been talking about the need for greater IoT security for *over a decade and a half* now. So why would attacks suddenly spike in 2020?

As with a lot of what has happened in cybersecurity in 2020, you can thank COVID-19.

Until recently, IoT attacks have generally been thought of as "low risk, low reward." Sure, it isn't hard to hack into an individual's internet-enabled coffeemaker. But aside from knowing how and when you enjoy your brew, what would there be to gain? Even if they used that as a back door into your home computer, the potential financial gains are likely to be minuscule even compared to other forms of attacks on private individuals (e.g., ransomware, cryptojacking, social engineering) — let alone attacks on large organizations.

But when the COVID-19 pandemic forced offices to close, it changed this calculus completely. According to Gallup, by April the remote workforce jumped from 7% to 62%. As people began accessing corporate networks from their often unsecure home network — which also connected to countless, often unsecure devices — cybercriminals began seeing attacks on home networks less as small potatoes, and more as the whole enchilada.

But even as vaccine efforts have begun to turn the tide in the fight against COVID-19, experts are predicting remote work is here to stay. If this holds true — particularly if the number of poorly secured IoT devices continues to increase — we are likely to continue seeing elevated rates of IoT attacks into 2021 and beyond.

The Tempest in Your (Wi-Fi Enabled) Teapot

In 2020, SonicWall Capture Labs threat researchers identified 72 new signatures associated with IoT threats. Here are the top 15:

SIGNATURE NAME	HITS	IoT DEVICE TYPE
NETGEAR DGN Devices Remote Command Execution 2	19,081,149	Router
D-Link HNAP Request Buffer Overflow	16,517,156	Router
NETGEAR DGN Devices Remote Command Execution	5,889,012	Router
Cisco RV320 and RV325 Information Disclosure	4,188,984	Router
NVMS-9000 Digital Video Recorder Remote Code Execution	3,173,477	DVR/NVR
Dasan GPON Routers Command Injection	2,758,616	Router
D-Link DSL-2750B Remote Code Execution	1,498,603	Router
Vacron NVR Remote Command Execution	1,002,542	Camera
ZyXEL Products Command Execution (CVE-2017-18368)	645,793	Camera
Hikvision IP Cameras Authentication Bypass	523,828	Camera
Netlink GPON Router Remote Command Execution	344,079	Router
Wireless IP Camera (P2P) WIFICAM Authentication Bypass 1	308,853	Camera
Avtech IP Camera Command Injection 1	285,407	Camera
NUUO NVRMini2 Authenticated Command Injection	265,905	DVR/NVR
Linksys Smart Wi-fi Information Disclosure	222,150	Router

While IoT technology has continued to expand into new device categories, including socks, cookware and even toilets, routers are still at the top of the list when it comes to attack targets. This is because routers are mostly internet accessible, compared to other devices that either are not directly accessible on the internet, or sit behind the VPN.

Routers also have relatively static IP addresses, putting them at risk for consistent attacks.

However, despite the longstanding tendency to not change router passwords from factory defaults, routers still have stronger security protection than other IoT devices, such as IP cameras or home automation devices.

For example, once exploited, IoT devices, such as cameras, could be leveraged to form massive malicious botnets to launch DDoS attacks against larger companies or organizations.

A Year in IoT Malware Attacks

Linear eMerge E3 Access Controller Actively Being Exploited

While Nortek Security and Control's Liner eMerge E3 access controller is generally used to control access to designated places based on identity and time of day, remote unauthenticated attackers can exploit it to alter or corrupt databases, steal records, launch DDoS attacks or even compromise other parts of the housing infrastructure. This access may be retained even after the vulnerability is fixed.

BlueKeep Flaw Plagues Outdated Connected Medical Devices

While patches for the BlueKeep vulnerability were released in early 2019, researchers discovered that, due to running outdated versions of Windows, roughly half of an average hospital's medical devices are still vulnerable.

Your Philips Hue Light Bulbs Can Still Be Hacked — And Until Recently, Compromise Your Network

An update was thought to have addressed the vulnerability in the firmware of Phillips Hue bulbs, but the actual bulbs may still be at risk from anybody with a laptop and an antenna — even as far as 300 feet away.

Hackers Actively Exploit Zero-Day in CCTV Camera Hardware

Injection vulnerabilities in commercial DVRs manufactured by LILIN were exploited by hackers, who then deployed malware on the devices to execute Chalubo, Moobot and FBot botnets.

Hackers Actively Targeting Remote Code Execution Vulnerability on Zyxel Devices

Researchers observed attackers targeting Zyxel Network Attached Storage (NAS) and firewall products affected by a remote code execution vulnerability. By sending a specially crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code with root privileges on the device.

Netgear Zero-Day Allows Full Takeover of Dozens of Router Models

79 models (and 758 firmware versions) of Netgear routers are discovered to be vulnerable to a flaw that allows attackers to bypass authentication and gain root privileges.

Ripple Vulnerability affecting millions of IoT Devices

A TCP/IP library released in 1997, which has been used ever since to allow software and devices to connect to the internet, was found to contain 19 vulnerabilities, including some that are highly dangerous and could result in hackers remotely taking over affected systems. Using the CVSSv3 vulnerability severity scale, the Department of Homeland Security has assigned two of these vulnerabilities a 10/10 rating, and a further two a 9.8/10.

Attackers Actively Targeting Tenda Wi-Fi Router Vulnerability

The SonicWall Capture Labs threat research team observed attackers exploiting the arbitrary remote code execution vulnerability reported in TENDA AC15 router. The vulnerability can result in attackers exploiting it to allow arbitrary code execution. When the *usb.sh* command is executed, it downloads payloads from the attacker server and executes them one by one.

Attackers Actively Targeting Vulnerable AVTECH Devices

Researchers observed attacks exploiting old vulnerabilities in AVTECH devices. By exploiting this issue, attackers can execute any system command with root privileges without authentication. By exploiting another, attackers can execute arbitrary system commands with root privileges. Both of these exploits connect to malicious domains and download a shell script, which is used to change file permissions and connect to the attacker-controlled server to download more malicious files.

Attackers Actively Targeting Vulnerable Dasan GPON Home Routers

The SonicWall Capture Labs threat researchers also observed attackers exploiting old vulnerabilities in Dasan GPON home routers. One allows attackers to bypass authentication simply by appending "?images" to any URL of the device that requires authentication. The other can be used to inject and execute commands that can download and execute malicious executables.

A New Tool in the Fight Against IoT Attacks: Legislation

The abundance of IoT devices — combined with the ease of exploitation and ever-increasing rewards for doing so — has created something of a Wild West atmosphere for attackers. But there are a number of new regulations dedicated to bringing this era of lawlessness to a close.

EUROPE

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, home assistants and more. The label has already been awarded to a number of products that merit these standards.

UNITED STATES

On January 1, 2020, the first IoT security law in the U.S., the California Internet of Things Security Law, went into effect. It requires that all connected devices sold in the state have "reasonable" and appropriate security measures, such as a preprogrammed password unique to each device and extra layers of authentication when accessing a device for the first time.

In December, the IoT Cybersecurity Improvement Act of 2020 was signed into law. Under the legislation, the National Institute of Standards and Technology (NIST) will issue standards for IoT devices owned or controlled by federal agencies. NIST will also work with cybersecurity researchers, industry experts and the Department of Homeland Security to publish guidelines on federal IoT security.

New IoT devices purchased by the federal government must comply with the new NIST standards. Contractors will also be required to comply with the standards, and agencies must confirm compliance before obtaining an IoT device from a contractor.

IoT Malware Attacks by Industry

Compared to other threat vectors, the industry-specific data for attempted IoT malware attacks per customer is fairly straightforward. The dip in April, spike in October and dropoff at the end of the year that we see in the overall IoT malware data are also visible here, and, particularly after Q1, the industries generally trend in sync with one another.

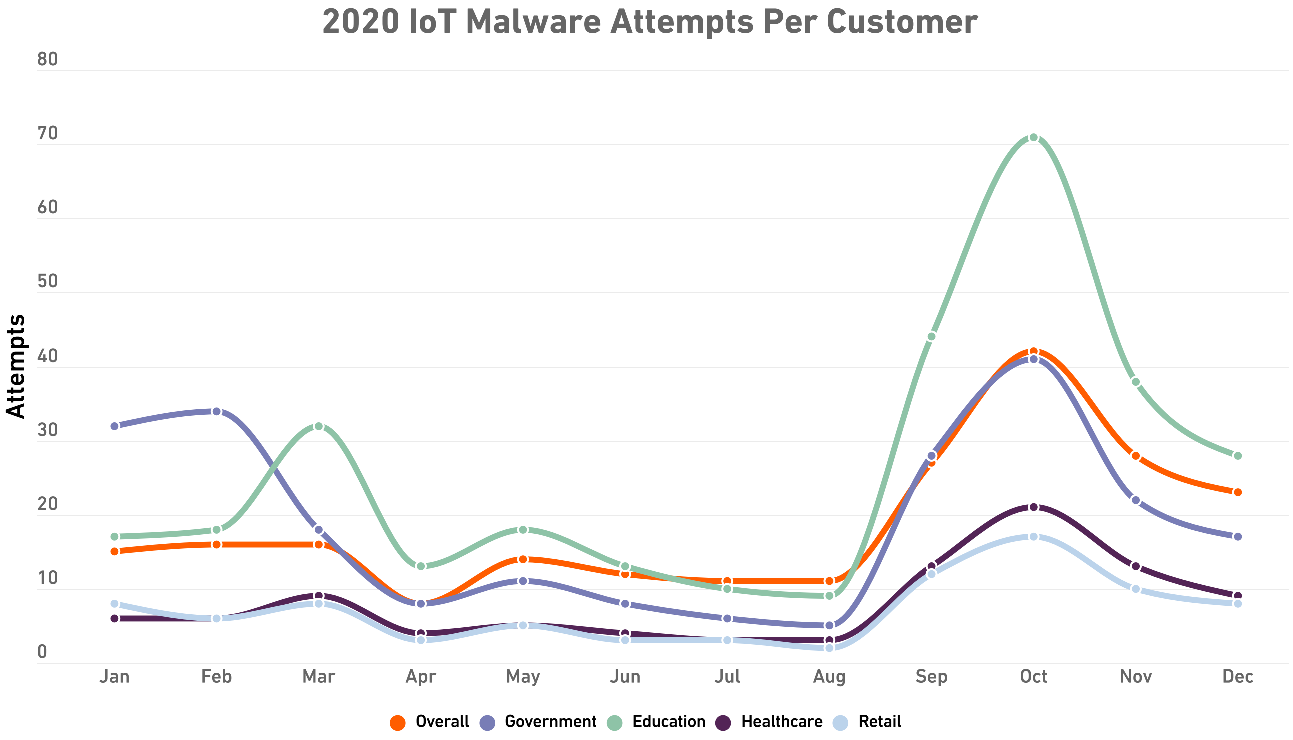
In October, every single industry — as well as the overall per-customer average — had the highest number of attacks per customer it would see all year. Those working in the education industry were hit the hardest, with an average of 71 IoT malware attempts a month.

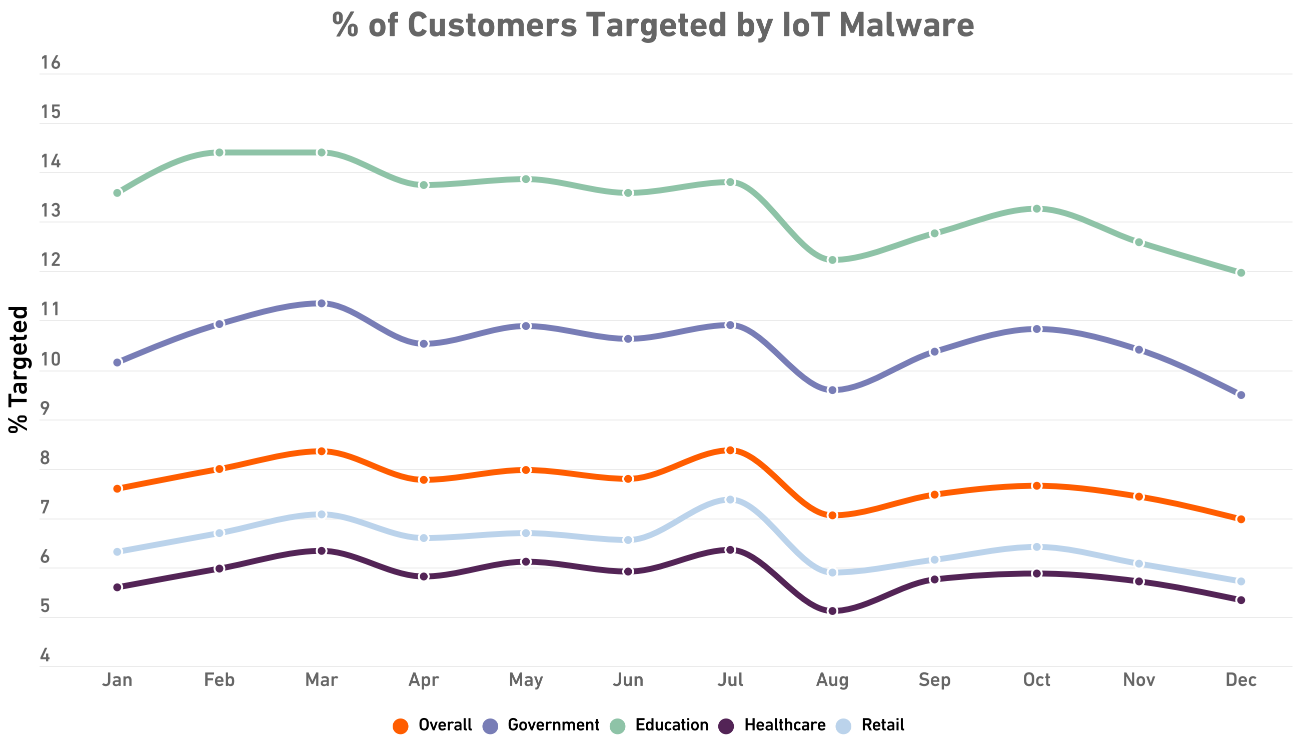
But while October stands out for having the highest number of IoT malware attempts per customer, we don't see a corresponding spike in the percentage of customers targeted. In fact, across industries, October marked the beginning of a *decrease* in the percentage of customers targeted.

This suggests that, while cybercriminals were clearly working harder in October, their energies were focused on doubling down on existing targets, rather than seeking out new ones.

Alternatively, it could also indicate that, while there might be more devices behind each firewall, they are often on the same network and therefore wouldn't increase the *percentage of customers* targeted — just the number of targets.

Looking at the data for percentage of customers targeted by IoT malware attacks suggests that these threat actors are nothing if not creatures of habit. We see none of the sharp peaks and valleys and none of the crisscrossing as one industry falls out of favor with attackers and another comes into vogue.




% of Customers Targeted by IoT Malware
% Targeted
16
15
14
13
12
11
10
9
8
7
6
5
4
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
● Overall
● Government
● Education
● Healthcare
● Retail

Attacks on Non-Standard Ports Reach All-Time High

In 2020, SonicWall Capture Labs threat researchers saw the percentage of attacks across non-standard ports grow from 2019's 13% to 25% in 2020.

In July, 46% of all malware attacks came via non-standard ports — the highest level since SonicWall began tracking these attacks. The volume of non-standard port attacks in July exceeded those of the two highest months in 2019 — themselves record-breaking — put together.

The percentages for Q3 and Q4 were down slightly from the highs we saw at midyear, but not much — they still managed to tie one another for second-highest quarter of all time, a sure sign that nonstandard port attacks aren't going away anytime soon.

What is a Non-Standard Port Attack?

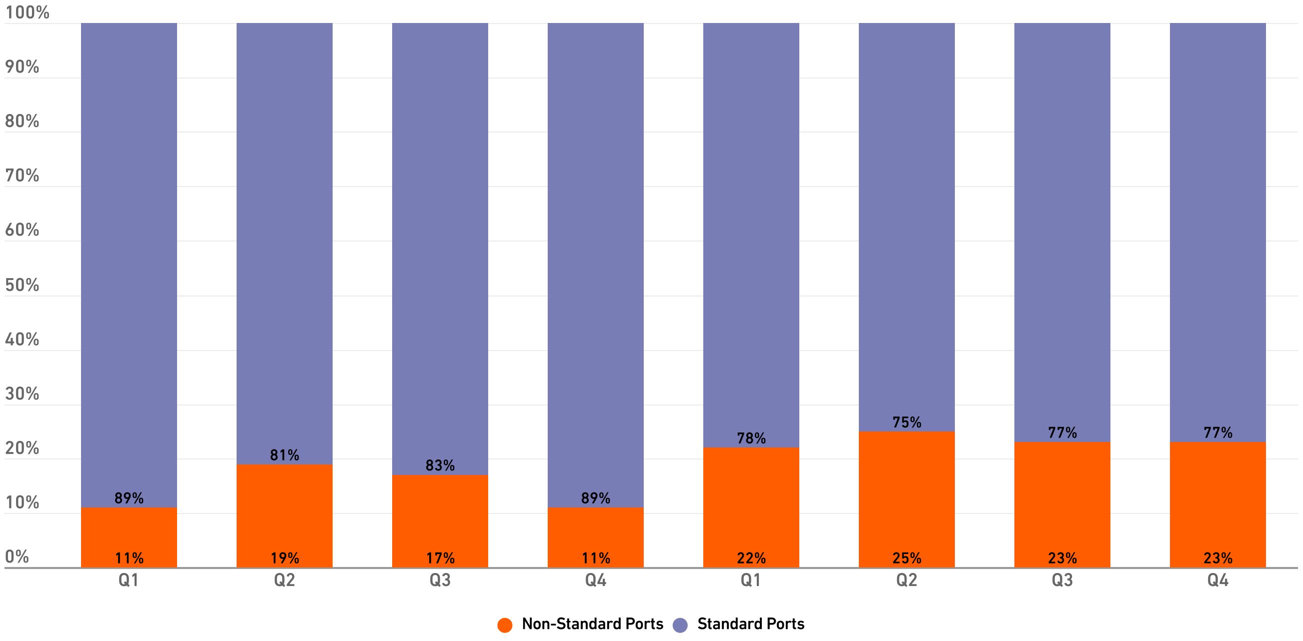
While there are more than 40,000 registered ports, only a handful are commonly used. They are the 'standard' ports. For example, HTTP uses port 80, HTTPS uses port 443 and SMTP uses port 25. A service using a port other than the one assigned to it by default, usually as defined by the IANA port numbers registry, is using a nonstandard 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.

New 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



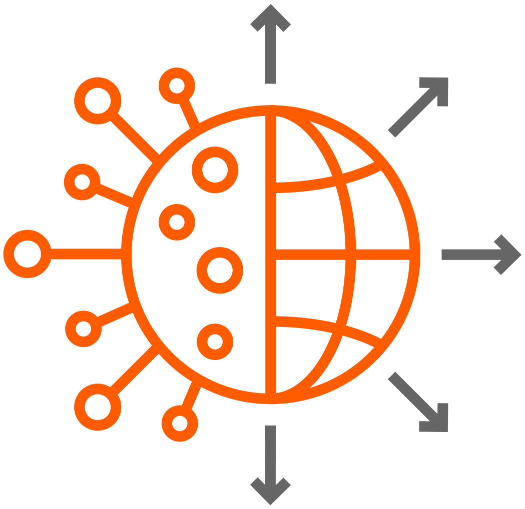
CONCLUSION

Cybersecurity in a Post-Pandemic World

2020 taught the world more about cybersecurity than perhaps any year before it. While we don't know yet how many of those lessons will be generalizable to a time when COVID-19 is no longer seen as a clear and present danger, what we do know is that the fundamentals of cybersecurity will continue on as they always have:

The cybersecurity business gap will continue to grow over time. Threats will become more evasive, and skilled staff will only get harder to find. Businesses will ultimately be faced with two options: Bridge the gap, or fall in.

While knowledge, such as that found in this *2021 SonicWall Cyber Threat Report*, can help fill some of the voids, to truly protect yourself in tomorrow's threat landscape, you'll need a new way of looking at cybersecurity — and solutions that can detect and prevent even the most advanced threats.



At SonicWall, we're dedicated to providing industry-proven solutions at a lower total cost of ownership — allowing you to know the unknown, and unify visibility and control for less. Plus, every solution we sell is backed by our team and partners, who make it their mission to exceed your business and security objectives.

To learn more, visit sonicwall.com

ABOUT THE SONICWALL CAPTURE LABS THREAT NETWORK

SONICWALL
CAPTURE LABS

Intelligence for 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

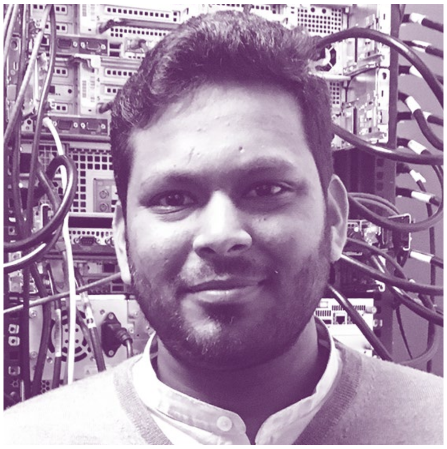
28m+

Malware Attacks Blocked Daily

FEATURED THREAT RESEARCHERS

Terry He
Director
Software Engineering

Rhoda-Mae Aronce
Senior Engineer
Software Development



Lalith Dampanaboina
Principal Engineer
Software Development

Justin Jose
Senior Manager
Software Engineering

Michael King
Senior Engineer
Software Development

Edward Cohen
Vice President
Strategy & Operations

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 NONINFRINGEMENT. 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. If you have any questions regarding your potential use of this material, contact:

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 and a work reality where everyone is remote, mobile and unsecure. 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.