# 2020

# SONICWALL CYBER THREAT REPORT

sonicwall.com | @sonicwall

SONICWALL®

# TABLE OF CONTENTS

# A NOTE FROM BILL

The boundaries of your digital empire are limitless. What was once a finite and defendable space is now a boundless territory — a vast, sprawling footprint of devices, apps, appliances, servers, networks, clouds and users.

For the cybercriminals, it's more lawless than ever. Despite the best intentions of government agencies, law enforcement and oversight groups, the current cyber threat landscape is more agile than ever before.

To survive, you have to be faster, smarter and more decisive. And that's not easy to do alone — even for larger organizations with substantial cybersecurity budgets.

In response, SonicWall and our Capture Labs threat research team work tirelessly to arm organizations, enterprises, governments and businesses with actionable threat intelligence to stay ahead in the global cyber arms race.

And part of that dedication starts now with the 2020 SonicWall Cyber Threat Report, which provides critical threat intelligence to help you better understand how cybercriminals think — and be fully prepared for what they'll do next.

Bill Conner

Bill

President & CEO
SonicWall

## CYBER CRIMINAL

The modern cybercriminal acts with purpose. These criminal operations are business-focused and budget-conscious. If a certain strategy didn't provide the returns expected, they will pivot toward a plan that's more effective. They are efficient enterprises with modern business plans.

For the last five years, cybercriminals overwhelmed organizations with sheer volume. Their objective was simple: cast as big a net as possible and reap the rewards.

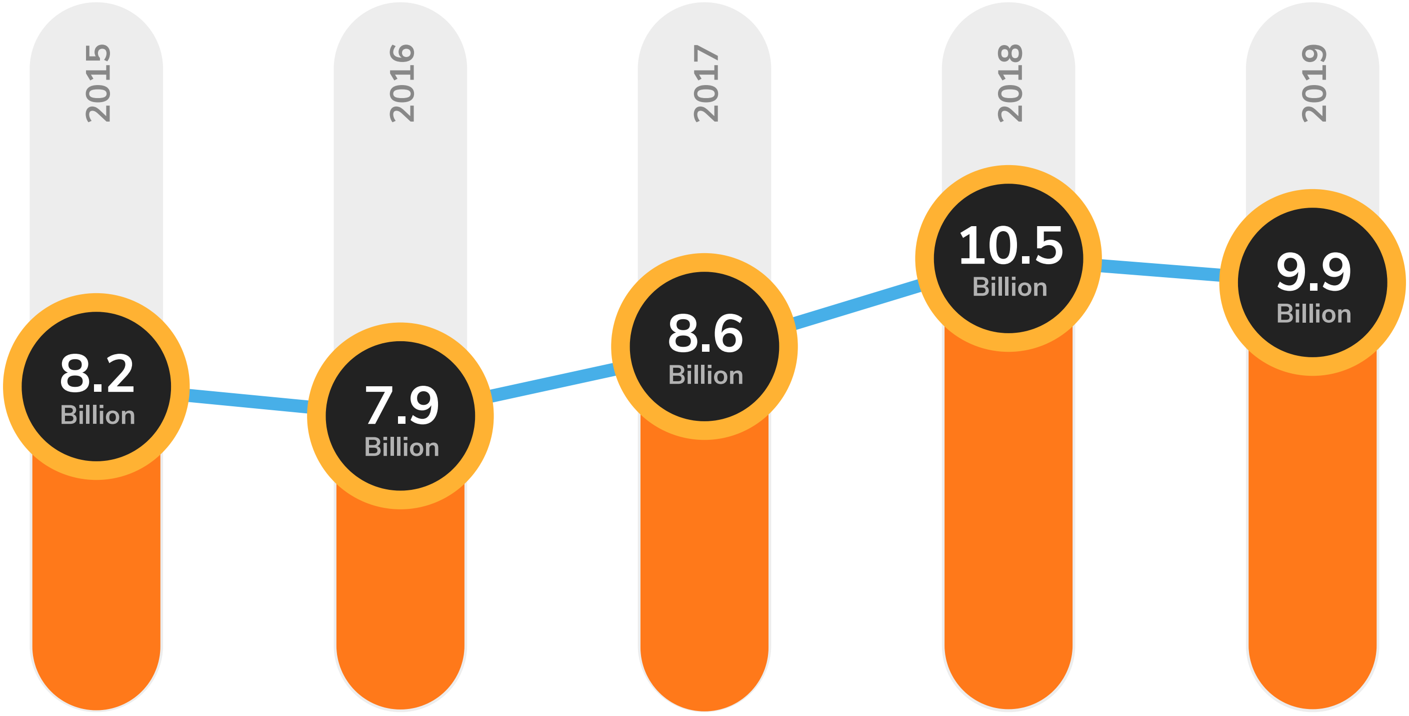
But as cyber defenses evolved, this approach was no longer effective. More volume was not resulting in higher paydays. A change was in order.

In 2018, cybercriminals and threat actors began to dial back untargeted salvos in favor of more evasive attacks against "softer" targets.

This approach was even more recognizable in 2019 as total volume waned, but attacks were more targeted with higher degrees of success, particularly against the healthcare industry, and state, provincial and local governments.

All told, SonicWall Capture Labs threat researchers recorded **9.9 billion malware attacks* in 2019** — a slight 6% year-over-year decrease.

## GLOBAL MALWARE VOLUME



* 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 2019

While data exposures are often caused by malicious cybercriminal activity, many other cases stem from lackadaisical security practices and unintentional human error. Serious data breaches and exposures run the gamut across different industries, verticals and regions. Below is a snapshot of the most egregious data exposures in 2019.

| INSTITUTION | CATEGORY | REPORTED | EXPOSED |
|---|---|---|---|
| **Orvibo** | IoT | 7/1/2019 | **2** Billion |
| **LightInTheBox** | Online Retailer | 12/16/2019 | **1.6** Billion |
| **Verifications.io** | Business | 3/29/2019 | **980** Million |
| **First American** | Banking/Credit/Financial | 5/25/2019 | **885** Million |
| **Collection #1** | Technology | 1/17/2019 | **773** Million |
| **Facebook** | Social Media | 3/21/2019 | **600** Million |
| **Facebook** | Social Media | 4/2/2019 | **540** Million |
| **Facebook** | Social Media | 12/14/2019 | **267** Million |
| **Zynga** | Entertainment | 9/12/2019 | **170** Million |
| **Canva** | Education | 5/24/2019 | **139** Million |
| **Capital One**<br>(American Medical Collection Agency) | Banking/Credit/Financial | 7/19/2019 | **106** Million |
| **Evite** | Entertainment | 2/22/2019 | **100** Million |
| **Poshmark** | Retailer | 8/5/2019 | **50** Million |
| **Chtrbox** | Social Media | 5/20/2019 | **49** Million |
| **BioStar 2** | Other | 8/16/2019 | **27.8** Million |
| **Ascension** | Banking/Credit/Financial | 1/23/2019 | **24** Million |
| **CafePress** | Retailer | 8/5/2019 | **23** Million |
| **Novaestrat** | Government | 9/16/2019 | **20** Million |
| **LifeLabs** | Medical/Healthcare | 12/17/2019 | **15** Million |

# TOP DATA EXPOSURES OF 2019

| INSTITUTION | CATEGORY | REPORTED | EXPOSED |
|---|---|---|---|
| **500px** | Social Media | 2/15/2019 | 14.8 Million |
| **Hostinger** | Technology | 9/25/2019 | 14 Million |
| **Quest Diagnostics**<br>(American Medical Collection Agency) | Medical/Healthcare | 6/3/2019 | 11.9 Million |
| **Emuparadise** | Gaming/Entertainment | 6/10/2019 | 11 Million |
| **TrueDialog** | SMS Service | 12/4/2019 | 10 Million |
| **Bodybuilding.com** | Health/Fitness | 4/22/2019 | 9 Million |
| **LabCorp**<br>(American Medical Collection Agency) | Medical/Healthcare | 6/4/2019 | 7.7 Million |
| **BlankMediaGames** | Gaming/Entertainment | 1/3/2019 | 7.6 Million |
| **Coffee Meets Bagel** | Social Media | 2/14/2019 | 6 Million |
| **Bulgaria National Revenue Agency** | Government | 7/17/2019 | 5 Million |
| **DoorDash** | Business | 9/26/2019 | 4.9 Million |
| **Dominion National** | Medical/Healthcare | 6/21/2019 | 2.9 Million |
| **Wyze Consumer Electronics** | Consumer Electronics | 12/30/2019 | 2.4 Million |
| **Blur** | Technology | 1/2/2019 | 2.4 Million |
| **Federal Emergency Management Agency "FEMA"** | Government/Military | 3/15/2019 | 2.3 Million |
| **Clinical Pathology 14**<br>(American Medical Collection Agency) | Medical/Healthcare | 7/12/14 | 2.2 Million |
| **Martinsburg VA Medical Center** | Medical/Healthcare | 4/11/2019 | 1.8 Million |
| **AMC Networks** | Entertainment | 5/1/2019 | 1.6 Million |
| **Auto Truck Kargo Equipment LLC** | Business | 4/2/2019 | 1.3 Million |
| **T-Mobile Prepaid Customers** | Business | 11/22/2019 | 1 Million |
| **Suprema** | Medical/Healthcare | 8/25/2019 | 1 Million |

# RISKS FROM NEW KITS AND MACROS

## New exploit kits emerging

With the indictments of various cybercriminal gang members, some exploit kits (EK) have emerged to replace older variants. But even the new EKs still utilize fairly old Internet Explorer and Adobe Flash vulnerabilities. Like their predecessors, they also are mainly distributed via “drive-by-download” and malvertizing campaigns.

Newer and more sophisticated EKs, however, use fileless attacks instead of dropping traditional payloads to the disk. Magnitude EK, Underminer EK and Purplefox EK have been known to leverage fileless payloads, many of which are ransomware.

As another example, router-based exploit kits can alter a router’s DNS settings so that users are redirected to phishing and other malicious websites.

## Macros enabling malicious activity

Each year, SonicWall sees an increase in the use of document files as an initial vector for malware infection. Be it targeted attacks, wide-spread infections or marketing-based spam campaigns, Visual Basic for Applications (VBA) macros are involved everywhere because of their versatility and wide range of capabilities.

TrickBot, Ursnif, Emotet, Lokibot and Remcos are some of the prevalent malware families that use a malicious VBA Macro for their distribution. Even though the Microsoft Office installation process has macros disabled by default, threat actors trick users into enabling them by making use of social-engineering techniques.

And because of the ubiquity of sandbox technology offered by security vendors to understand macro behavior, malware authors now thrive on code obfuscation, sandbox detection and bypass techniques.

Due to the use of code-obfuscation tools, SonicWall sees multiple variants of the same malicious macro. Also, the richness of the document file format is exploited by malware authors as they use components like UserForm, Excel cells and Text Label to hide malicious code.

SonicWall observed a handful other macro execution actions, including general mouse use as well as Image.Click, AutoOpen, AutoClose, AutoExit, AutoNew and AutoExec.

Other evasion tricks observed in malicious macros use the VBA Timer function to warrant sleep (e.g., GetTickCount) to impede execution until the next user logon and then drops malicious scripts in the startup folder.

Throughout 2019 SonicWall also spotted Rich Text Format (RTF) files exploiting Microsoft Equation Editor vulnerabilities. Though a large number of the malicious documents were downloaded, traces of phishing incidents were also recorded.

The use of evasive techniques is not new and is a continuation of the malware evolution we’ve observed over the past few years. We expect this trend to continue as malware cannot act without first bypassing the defensive layers.

# DGAs CONTINUE TO SLOW MALWARE ANALYSIS, INVESTIGATION

## Top Malware Families Using DGAs

| | |
|---|---|
| CCleaner | Necurs |
| WD | Bamital |
| Mirai | Goznym |
| Blackhole | Symmi |
| CryptoLocker | Volatilecedar |
| DNSbenchmark | Rovnix |
| Emotet | Ud2 |
| Locky | Infy |
| Sutra | Ud3 |
| Gameover | Vawtrak |
| Modpack | Beebone |
| Madmax | Shifu |
| Conficker | Qhost |
| DNSchanger | Simda |
| Sphinx | Qakbot |
| Vidro | Tinba |
| Virut | Nymaim |
| Dyre | Padcrypt |
| Ramnit | Gspy |
| Gozi | Feodo |

Malware architects create and leverage sophisticated Domain Generation Algorithms (DGAs) as diversion mechanisms.

The algorithms are designed to overload security researchers, analysts and engineers who need to reverse-engineer the binary in order to discover the true command and control (C&C) structure and communication behind malware.

The DGA is created to hide or mask the location of the C&C so the attacker can hide and protect his design, structure and communication from prying eyes. The DGA will flood the network with DNS requests to random domains.

Meanwhile, only a handful of domains are active at one time. This feature allows connections back to their command and control server.

SonicWall Capture Labs threat researchers are committed to defending against the top DGAs (see top 40 in table ranked by Google popularity) and discovering new DGAs.

# DGAs CONTINUE TO SLOW MALWARE ANALYSIS, INVESTIGATION

| Random<br>Algorithm-Generated Domains |
|---|
| www.ylGntVEPMH.com |
| www.MGtoYca5Mc.com |
| www.f0VrN4HH6A.com |
| www.HL3aPxMS3Y.com |
| www.wsJjcWQQYi.com |
| www.QS41X9DIxP.com |
| www.pNMfQfCMcc.com |
| www.VWG3uvAFJ5.com |
| www.xuOEZYTq59.com |
| www.cO4FBGST1R.com |

The top DGAs will produce billions of domains each year. SonicWall Capture Labs threat researchers discover this real-time DNS traffic and capture the malware activity with proprietary correlation engines and separate malicious DGAs from legitimate DNS traffic. SonicWall uses traditional reverse-engineering and modern machine learning techniques to clearly identify and block these DGAs.

DGAs still stand as one of the most effective and popular algorithms being used by malware architects in 2019 and will be well into the future.

Using domain, seed and random-number generation formulas (e.g., Mersenne Twister), SonicWall is able to identify more than 172 million randomly-generated domains that could be exploited for malicious purposes.

# ATTACKS OVER NON-STANDARD PORTS DOWN, BUT STILL A CONCERN

Each of the last two SonicWall Cyber Threat Reports flagged alarming increases in malware attacks over non-standard ports. At the close of 2018, more than 19.2% of all malware volume was being sent via non-standard ports.

In the first half of 2019, attacks over non-standard ports dropped to 13% globally (based on a sampling of approximately 500 million malware attacks).

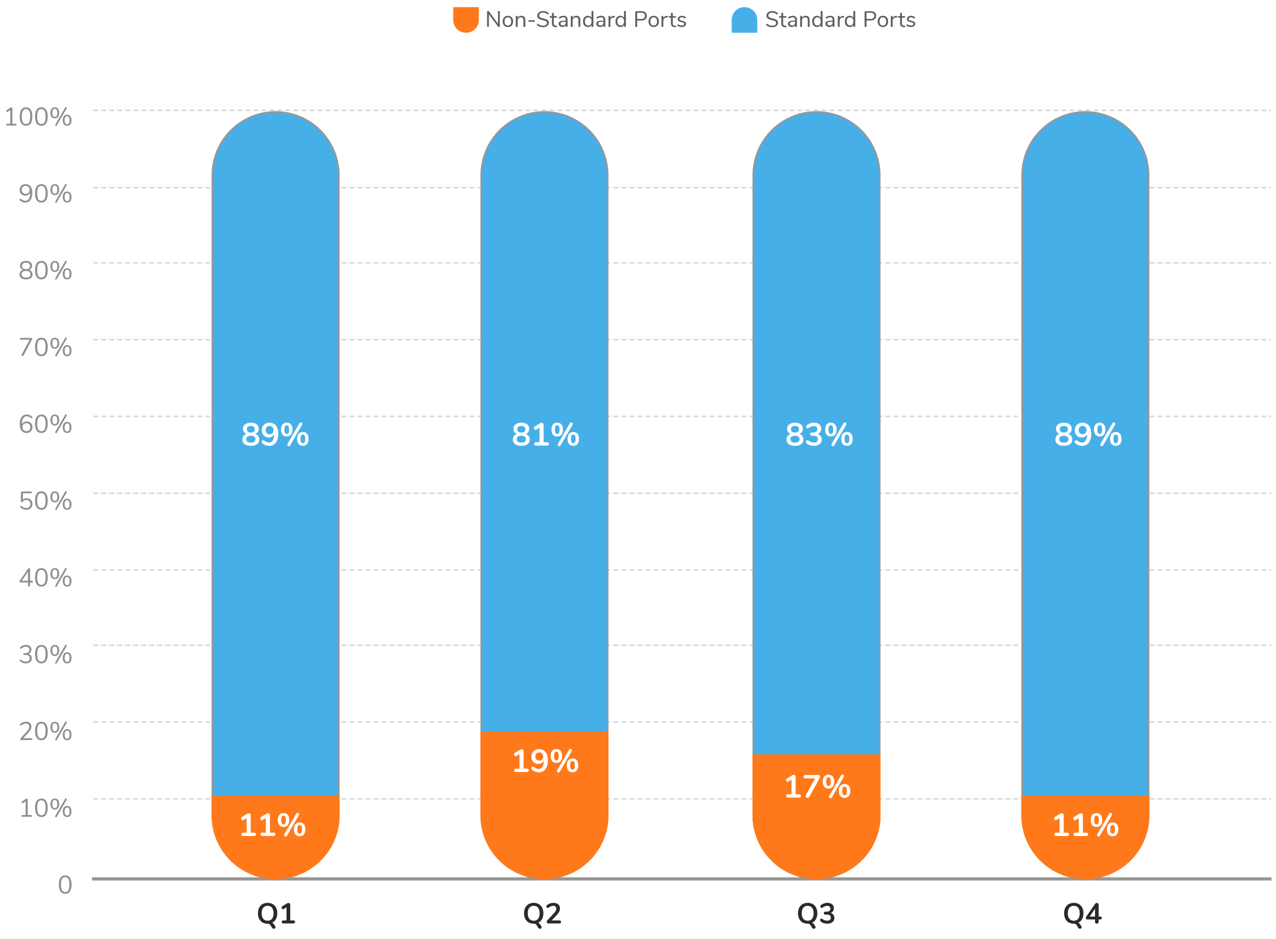
In May 2019, however, SonicWall saw that a quarter of all recorded malware attacks were coming across non-standard ports.

With full-year 2019 data now available, SonicWall Capture Labs threat researchers have found the vector stabilizing, with 15% of all malware attacks coming over non-standard ports.

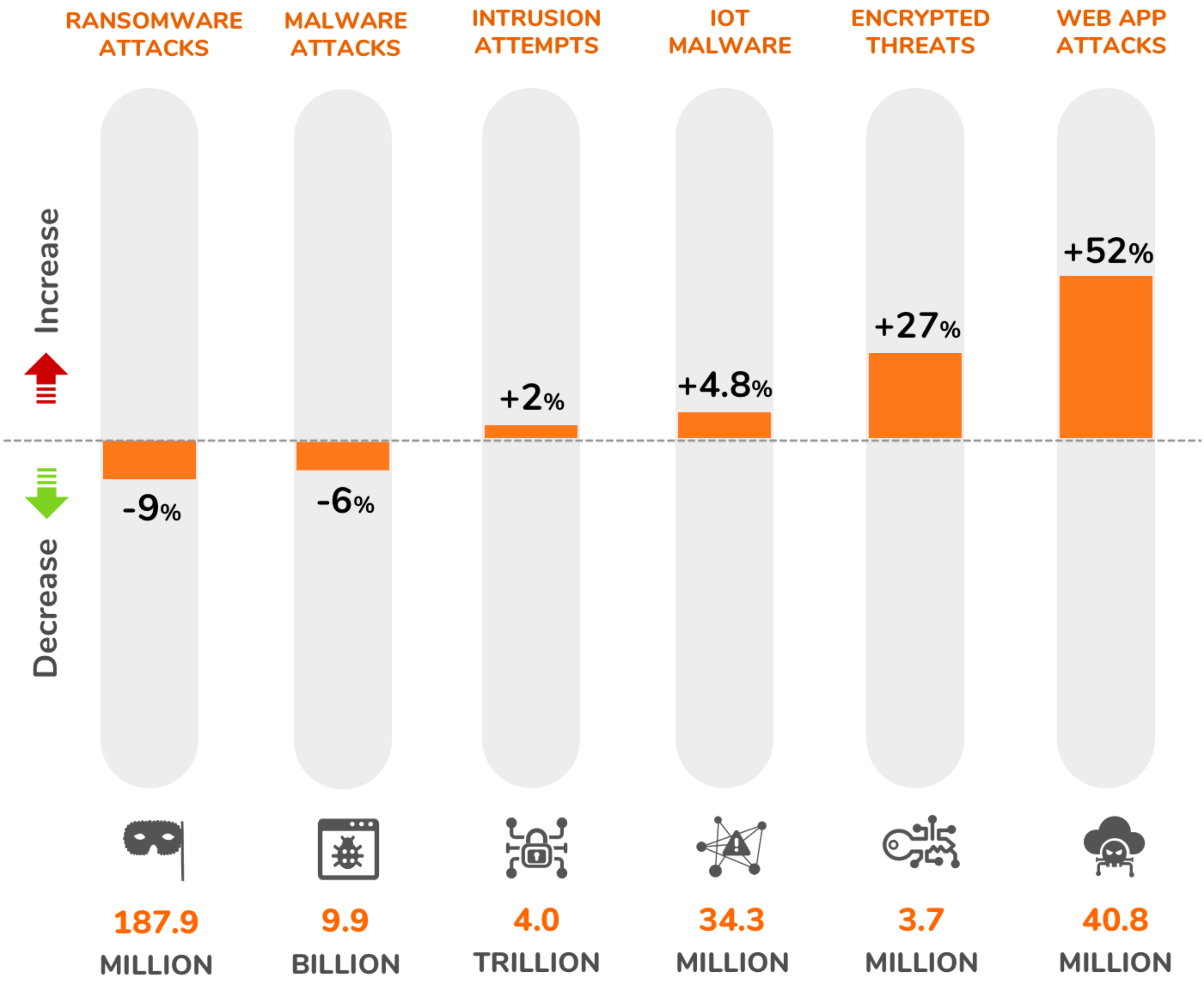
A 'non-standard' port is leveraged by services running on a port other than its default assignment, usually as defined by the IANA port numbers registry. Ports 80 and 443 are standard ports for web traffic.

As such, this is where traditional proxy-based firewalls focus their protection. Knowing this, cybercriminals target non-standard ports to help ensure their payloads are deployed undetected in a target environment.

## 2019 Malware Attacks



## Attack Volume



# INSIDE THE SONICWALL CAPTURE LABS THREAT NETWORK

Intelligence for the 2020 SonicWall Cyber Threat Report was sourced from real-world data gathered by the SonicWall Capture Threat Network, which securely monitors and collects information from global devices and resources including:

- More than 1.1 million security sensors in nearly 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

**1.1 MILLION**
Global Sensors

**215+**
Countries & Territories

**24x7x365**
Monitoring

**<24 HOURS**
Threat Response

**100,000**
Malware Samples Collected Daily

**27 MILLION+**
Malware Attacks Blocked Daily

● Sensors per region

# KEY FINDINGS FROM 2019

## Security Advances

### Faster Identification of 'Never-before-Seen' Threats

Speed and accuracy are critical attributes in identify and mitigating zero-day threats. New intelligence suggests that some security vendors — and respective innovative technology — are setting new standards for protection against unknown threats.

### Phishing Down for Third Straight Year

Despite its effectiveness as an attack vector, phishing dips again in 2019. Like changing tactics for malware, attacks are now more targeted and require much less volume to be successful.

### Advancements in Deep Memory Inspection

Announcements of new processor threats and side-channel attacks make the chip a critical battleground in 2020. Fortunately, the rapid evolution of deep memory inspection technology could help mitigate weaponized side-channel attacks until vendors are able to properly correct and patch.

### Cryptojacking Crumbles

In early 2019, the price of bitcoin and complementary cryptocurrencies created an untenable situation between Coinhive-based cryptojacking malware and the legitimate Coinhive mining service. The shuttering of the latter led to the virtual disappearance of one the year's hottest malware.

### Adoption of Perimeter-Less Security

Unlearning what has become trusted and commonplace is never easy. But new momentum toward perimeter-less architecture is helping redefine the future of cybersecurity.

# KEY FINDINGS FROM 2019

## Criminal Advances

### Ransomware Targets State, Provincial & Local Governments

‘Spray and pray’ is over. Now it’s all about ‘big-game hunting.’ Cybercriminals are using ransomware to surgically target victims that are more likely to pay given the sensitive data they possess or funds at their disposal (or both).

### Fileless Malware Spikes in Q3

The use of fileless malware ebbed and flowed in 2019. But exclusive SonicWall data shows a massive spike mid-year for this savvy technique.

### Encrypted Threats Growing Consistently

Another year, another jump in the use of encrypted threats. Until more organizations proactively and responsibly inspect TLS/SSL traffic, this attack vector will only expand.

### IoT Malware Volume Rising

From hacked doorbell cameras to rogue nanny cams, 2019 was an alarming year for the security and privacy of IoT devices. Trending data suggests more IoT-based attacks are on the horizon.

### Web App Attacks Double in 2019

The ubiquity of web applications offer cybercriminals and threats actors enticing pathways to valuable data. Does new data represent a pivot for their malicious behavior?

# FASTER IDENTIFICATION OF ‘NEVER-BEFORE-SEEN’ MALWARE

It’s logical that the faster a new attack can be identified, analyzed and blocked, the less likely it is to cause damage to a business or organization.

As such, SonicWall Capture Labs threat researchers and engineers have worked to increase the speed and accuracy in identifying 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 a full 1.9 days before VirusTotal receives the samples.

In some cases (see table below), SonicWall is discovering new threats months before samples are submitted.

This is accomplished by leveraging the SonicWall Capture Advanced Threat Protection (ATP) sandbox service, as well as patent-pending Real-Time Deep Memory Inspection$^{TM}$, which works to stop these never-before-seen malware variants.

The solution identifies more than 1,200 new malware variants each day. SonicWall immediately deploys signatures for these samples to protect active customers.

## 1.9 Days Faster

SonicWall is identifying ‘never-before-seen’ malware variants a full 1.9 days before samples are submitted to VirusTotal.

| Type | RTDMI Detection | VirusTotal Submission | File Hash |
|---|---|---|---|
| **PE32 Executable Malware** | Mar. 21, 2019 | Nov. 25, 2019 | 05012b6c975b253e9e0e61075b868d7df9d0d93fc6807d2e368512a0b1c4e343 |
| **PDF Phishing URL** | Mar. 11, 2019 | July 9, 2019 | 957a0f906c00c6dd409a76d768a00f47a26d857320b8e6749e0ed5da46c4f4d1 |
| **PDF Phishing URL** | Mar. 11, 2019 | July 9, 2019 | 11301d0dc44798263da9e3ba6a0f3693cec5af473bdd6fa612456d8756dd9cff |
| **PDF Phishing URL** | Mar. 12, 2019 | July 9, 2019 | 6051ede972c26fbc74b924b41778aafbe0cb602cd67e9349fcf1bdcec3b1e25d |
| **PDF Phishing URL** | Mar. 12, 2019 | July 9, 2019 | 56cd9b8d028276cd048dc72ff02258f5b590d391a0dc3a963d7316c0e943b034 |
| **PE32 Executable Malware** | May 5, 2019 | Dec. 12, 2019 | 0785243aec4c6791c7a87ee00a5917928bdb6f6a36b3b2bf82155fd725f85acf |

# TOP 10 CVES EXPLOITED IN 2019

In many cases, zero-day vulnerabilities are patched, fixed or otherwise mitigated before attacks can cause serious damage. Unfortunately, the inverse is also true. In 2019, SonicWall recorded and analyzed the top 10 CVEs that were exploited "in the wild." These impacted a range of applications, including SharePoint, Atlassian Confluence, Drupal Oracle WebLogic, Microsoft Windows GDI and more. SonicWall implemented Intrusion Prevention Service (IPS) or Gateway Antivirus (GAV) signatures for each exploit.

Top 10 CVEs Exploited in 2019

| Name | Reference | Description | Products Affected |
|---|---|---|---|
| BlueKeep | CVE-2019-0708 | A remote code execution vulnerability exists in Remote Desktop Services (formerly known as Terminal Services) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, also known as 'Remote Desktop Services Remote Code Execution Vulnerability.' | • Microsoft Windows 7<br>• Microsoft Windows XP<br>• Microsoft Windows Server 2008<br>• Microsoft Windows Server 2003 |
| SharePoint Server | CVE-2019-0604 | An unsecure deserialization vulnerability, this Microsoft SharePoint Server vulnerability is due to insufficient validation usersupplied data to EntityInstanceIdEncoder. | • Microsoft SharePoint Enterprise Server 2016<br>• Microsoft SharePoint Foundation 2010 & 2013<br>• Microsoft SharePoint Server 2010, 2013 & 2019 |
| Win32k | CVE-2019-0859 | An unsecure deserialization vulnerability, this Microsoft SharePoint Server vulnerability is due to insufficient validation usersupplied data to EntityInstanceIdEncoder. | • Microsoft SharePoint Enterprise Server 2016<br>• Microsoft SharePoint Foundation 2010 & 2013<br>• Microsoft SharePoint Server 2010, 2013 & 2019 |
| Atlassian Confluence | CVE-2019-3396 | A server-side template injection vulnerability was reported in Atlassian Confluence Server. This vulnerability is due to improper validation of the _template JSON parameter. | • Atlassian Confluence Server 6.12.x prior to 6.12.3<br>• Atlassian Confluence Server 6.6.x prior to 6.6.12 |

# TOP 10 CVES EXPLOITED IN 2019

| Top 10 CVEs Exploited in 2019 | | | |
|---|---|---|---|
| Name | Reference | Description | Products Affected |
| Drupal | CVE-2019-6340 | A remote code execution vulnerability was reported in the web services components of Drupal Core. The vulnerability is due to improper sanitization of data for certain Field Types from non-form sources prior to deserialization. | • Drupal Drupal 8.5.x prior to 8.5.11<br>• Drupal Drupal 8.6.x prior to 8.6.10<br>• Drupal Drupal 7.x |
| Oracle WebLogic | CVE-2019-2725 | An insecure deserialization vulnerability was reported in Oracle WebLogic. This vulnerability is due to insufficient validation of XML datawithin the body of HTTP POSTrequests. | • Oracle WebLogic Server 12.1.3.0.0<br>• Oracle WebLogic Server 10.3.6.0.0 |
| Exim Server | CVE-2019-10149 | A remote command execution injection vulnerability was reported in Exim server. This vulnerability is due to insufficient handling of recipient address in the deliver_message() function. | • Exim versions 4.87 to 4.91 |
| Microsoft GDI | CVE-2019-0903 | A remote code execution vulnerability was reported in the GDI component of Microsoft Windows. The vulnerability is due to the way GDI handles objects in memory. | • Microsoft Windows 7, 8.1 & 10<br>• Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016 & 2019 |
| Webmin Server | CVE-2019-15107 | A command injection vulnerability was reported in Webmin. The vulnerability is due to improper validation of user-supplied input within password_change.cgi. | • Webmin prior to 1.930 |

# ADVANCEMENTS IN DEEP MEMORY INSPECTION

The processor has been a fluid and emerging battlefield for the last 24 months.

Although chip-based vulnerabilities have been difficult for traditional cybercriminals to exploit, advanced side-channel attacks have proven even more challenging for organizations and enterprises to mitigate.

Simply, the steps required to correct processor vulnerabilities are much different than a simple software patch — and they're much more difficult to implement across large user populations, too.

As such, once these attacks are weaponized by mainstream criminal groups, we will see critical damage across infrastructure, servers, security appliances, data repositories, mobile devices and a wide range of endpoints.

For this reason, SonicWall has been at the forefront of deep memory inspection technology.

In early 2018, SonicWall announced its patent-pending Real-Time Deep Memory Inspection$^{\text{TM}}$ engine, which detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption.

In 2019, the multi-engine SonicWall Capture Advanced Threat Protection (ATP) cloud sandbox identified **439,854 new malware variants**, a 12.3% increase over 2018.

Of those, RTDMI discovered **153,909 'never-before-seen' malware variants in 2019** — attacks that traditional sandboxes likely missed.

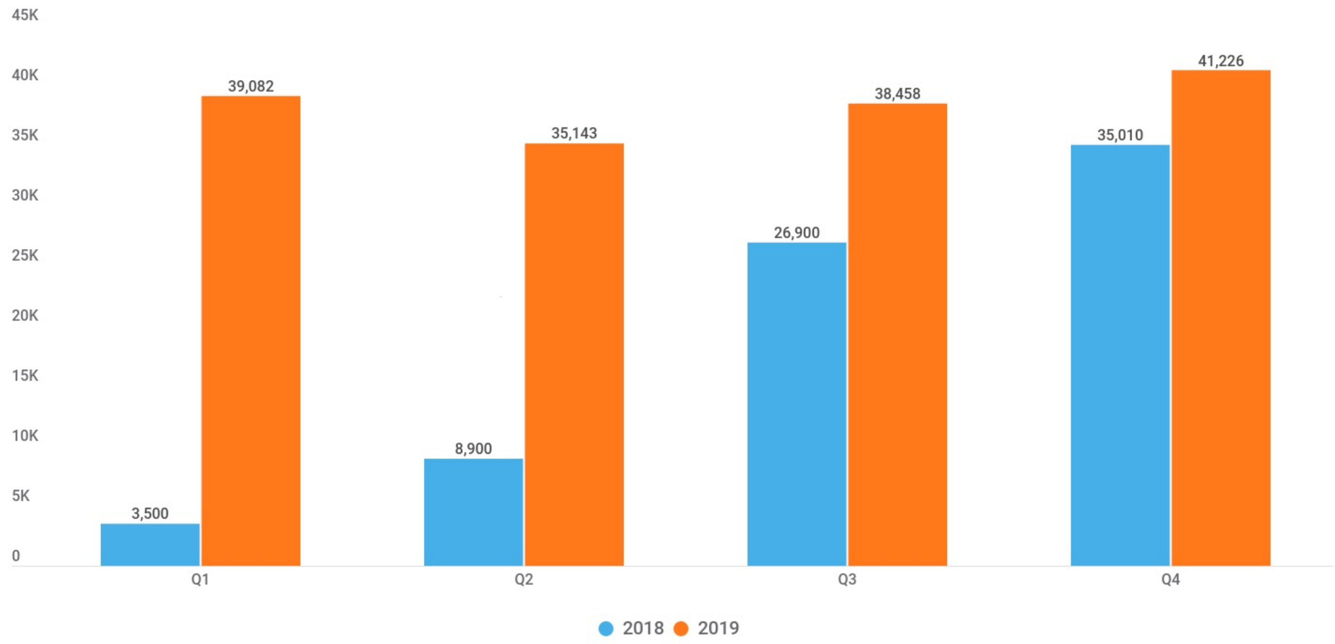
Each year, RTDMI leverages proprietary memory inspection, CPU instruction tracking and machine learning capabilities to become extremely efficient at recognizing and mitigating cyberattacks never seen by anyone in the cybersecurity industry.

## Pioneers of Machine Learning

In 2004, SonicWall Capture Labs researchers pioneered the use of machine learning for threat analysis. Today, SonicWall's machine learning technology powers the protection provided by the Capture Cloud Platform.

# ADVANCEMENTS IN DEEP MEMORY INSPECTION

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



By forcing malware to reveal its weaponry in memory, RTDMI™ proactively detects and blocks mass-market, never-before-seen threats and unknown malware, including attacks against processor vulnerabilities and malicious PDFs and Office files.

### What are 'never-before-seen' malware variants?

SonicWall tracks the detection and mitigation of 'never-before-seen' malware. These attacks mark the first time SonicWall Capture ATP identifies a signature/SHA256 as malicious.

Conversely, a 'zero-day' vulnerability is completely new or unknown and doesn't have any existing protections (e.g., patches, updates, etc.), usually from the target vendor or company.

This means that zero-day attacks against these vulnerabilities are unmitigated and, therefore, a critical threat to the global landscape.

Due to malware writers heavily investing in obfuscation and evasion techniques, the variants of existing, remixed or slightly modified malware have grown exponentially.

Therefore, these are attacks that may use existing, previously classified malware families, but are sufficiently mutated and modified as to evade detection by the majority of security tools in the industry. Thus, many have never been logged as malicious by Virus Total.

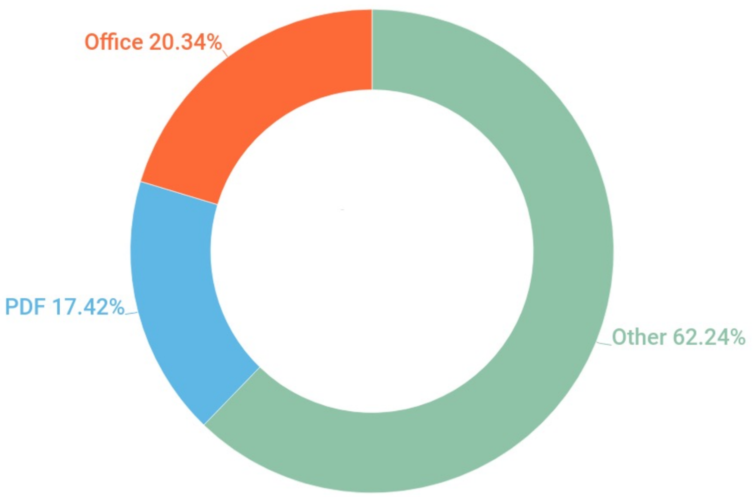
# ADVANCEMENTS IN DEEP MEMORY INSPECTION

### PDFs, Microsoft Office files among top new file types

In 2019, SonicWall observed that most new threats are based on malicious PDFs or Office files, followed by Archives.

In fact, Office (20.3%) and PDFs (17.4%) represent 38% of new threats detected by Capture ATP.

Capture ATP | New Detections by File Type



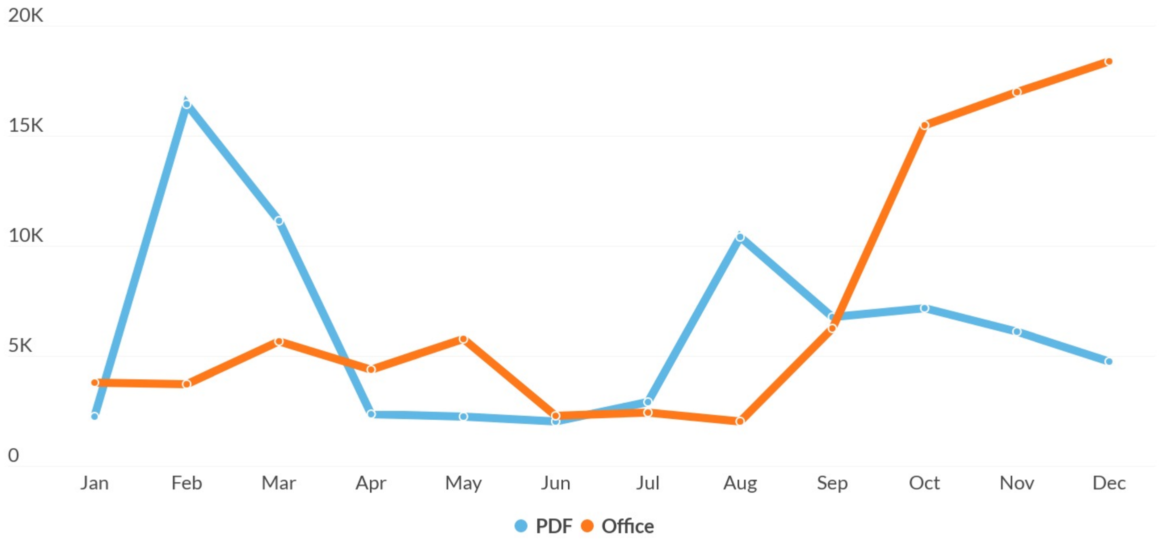
PDF files are popular because they are searchable, can be viewed on any device, are easy to create and may be encrypted for security, password-protected and/or digitally signed for authentication.

The file type's ubiquity makes them an attractive delivery mechanism for cybercriminals, who use them to spread phishing URLs, scripts, embedded malicious files and other PDF-based exploits.

Popular Microsoft Office/Office 365 files (e.g., Word, Excel, PowerPoint) are leveraged in similar fashion.

The graph below shows the popularity of using PDF to deliver malicious payloads, particularly during the beginning of 2019; malicious Office files were then leveraged later in the year.

Capture ATP Detection | Malicious PDF & Office Files



# ADVANCEMENTS IN DEEP MEMORY INSPECTION

### Tracking the evolution of malware strains

The collective power of Capture ATP and RTDMI also helps SonicWall Capture Labs threat researchers track the evolution of malware variants — even when authors obfuscate their payloads, such as using scripts inside of archives.

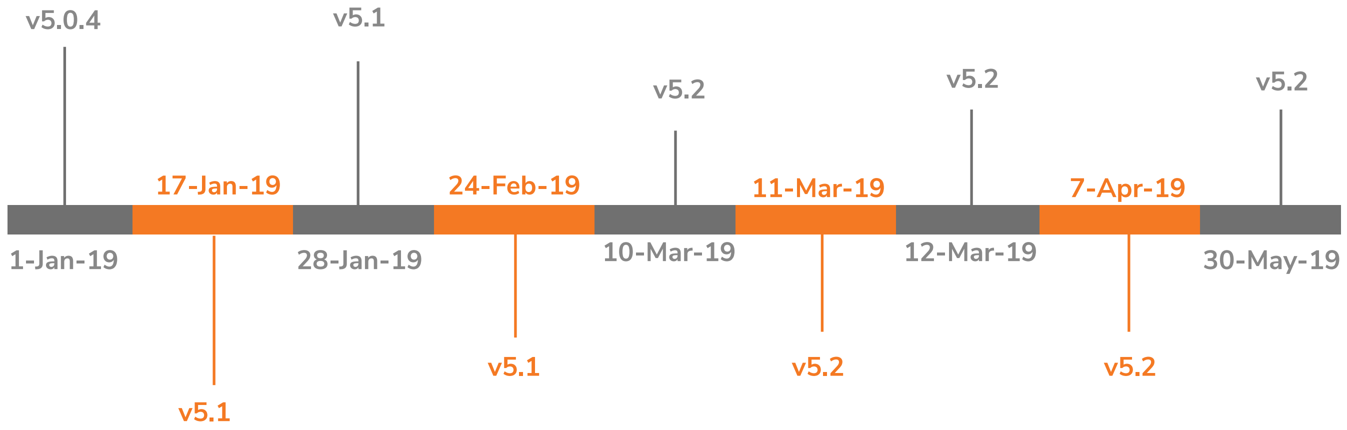
In this example, SonicWall tracked the evolution of GandCrab as it spread in the wild. The authors of the GandCrab ransomware eventually announced they were shuttering the project in June 2019 after a “successful” 16-month run.

### Side-channel attacks continue to be ripe for security research

In November 2019, four researchers from three universities — Worcester Polytechnic Institute (U.S.), University of Lübeck (Germany) and the University of California (U.S.) — published new findings that side-channel timing and lattice attacks could be executed against Trusted Platform Module (TPM) chips, specifically Intel fTPM and STMicroelectronics TPM chips.

Dubbed TPM-FAIL, this group of vulnerabilities are the next variation of side-channel attacks following Meltdown/Spectre, Foreshadow, PortSmash, MDS, etc. The details of the TPM-FAIL vulnerabilities are outlined in CVE-2019-11090.

GANDCRAB RANSOMWARE V5.X TIMELINE



The above timeline highlights changes SonicWall observed to GandCrab Version 5 in 2019, including alterations to payloads, malicious URLs, etc., even if the version number remained the same. (i.e., Version 5.2 could have different download URLs).

In this snapshot, SonicWall identified and logged different versions of GandCrab through the first half of the year, but didn't record any attacks after May 2019 as the malware authors terminated the illegal affiliate program.

The latest attacks on the TPM chip shows an evolution of side-channel attacks. Unlike the first-generation side-channel threats that would result in damage to the "immediate" target (i.e., the targeted data centers, cloud providers, etc.), TPM-FAIL could impact unpatched devices "down the line" — everything from security appliances to end-user laptops.

This exploit could be leveraged to forge digital signatures. If an operating system or the application use TPM to issue digital signatures, the private signing key used for signature generation can be compromised.

With compromised signing keys, forged signatures can help criminals bypass authentication protocols, tamper with operating systems, sign malicious software, etc.

SonicWall stands by its position that while these types of side-channel attacks have yet to be publicly weaponized, they continue to present a significant potential threat to organizations, such as cloud providers and hosting companies, running virtualized or multi-tenant environments that allow execution of arbitrary payloads. SonicWall continues to test and refine detection techniques in preparation for when side-channel attacks evolve from theoretical to practical.

SonicWall has confirmed that Capture Advanced Threat Protection (ATP) sandbox customers are protected from certain TPM-FAIL side-channel attacks via the solution's patent-pending Real-Time Deep Memory Inspection$^{TM}$ (RTDMI) technology.

| Vulnerability | Publicly Announced | RTDMI Detection Confirmed |
|---|---|---|
| Meltdown | 1/3/2018 | 1/30/2018 |
| Spectre | 1/3/2018 | 6/13/2018 |
| Foreshadow | 8/14/2018 | 8/15/2018 |
| PortSmash | 11/2/2018 | 11/15/2018 |
| Spoiler | 3/5/2019 | 3/5/2019 |
| MDS<br>(ZombieLoad, RIDL, Fallout) | 5/14/2019 | 5/15/2019 |
| TPM-FAIL<br>(CVE-2019-11090) | 11/12/2019 | 1/7/2020 |

# MOMENTUM OF PERIMETER-LESS SECURITY

For decades, protecting networks was entirely focused on defining perimeters and setting up defense layers to keep threats out. And for years, this approach served businesses well, with finite exposure points and attack vectors that were guarded with some investment and adherence to established best practices and frameworks.

Today, it's a different story. The boundaries of organizations' networks are borderless and expanding to limitless endpoints. Simultaneously, the threat landscape is becoming increasingly evasive.

These evolving and persistent cyberattacks create boundless points of exposure to organizations. But new momentum toward perimeter-less architecture is helping redefine the future of cybersecurity — a safer future not restrained by undefendable perimeters.

Much of this new thinking was first based on a zero-trust security model, which requires organizations to verify and authenticate any device, user or application, regardless if it is inside or outside the network perimeter.

From there, organizations could segment data across different 'trust zones' and further vet access depending on the sensitivity of the data. But more guidance was needed to bring this theory into reality.

### Introduction of SASE

The cybersecurity and network security solution spaces are highly segmented with an endless number offerings and vendors. This creates a massive headache for organizations trying to smoothly integrate these solutions into their network environment.

Instead, the entire cybersecurity space needs to converge to provide a more holistic cybersecurity approach. This is where secure access service edge (SASE), a new network security model coined by Gartner in 2019, comes into play.

SASE may help shape how organizations secure their networks and data in the coming years. SASE platforms combine software- and service-based networks, which will provide a unification of different security solutions.

"With an endless field of exposure points, the traditional network security model is outdated. With the adoption of many different cloud services, we need a more holistic approach," said Sagi Gidali, co-founder of Perimeter 81, a SonicWall technology partner. "Designing a new way forward — a future without network perimeters — was the only way to properly manage and mitigate tomorrow's most innovative cyberattacks."

A modern SASE platform will empower organizations to simply connect to a single platform for access to a secure network while gaining access to physical and cloud resources, regardless of their location.

Some of these new solutions have a range of overlapping benefits, so the naming conventions do vary: zero-trust network access, secure network as a service, firewall as a service, secure SD-WAN as a service and so on.

The new perimeter-less security movement could also replace the need for traditional virtual private networks (VPN) that so many employees have (begrudgingly) learned to adopt.

Unlike hardware-based legacy VPN and firewall technology, the more advanced and secure zero-trust network as a service offerings use the software-defined perimeter (SDP) model to offer greater network visibility, seamless onboarding and full compatibility with all major cloud providers.

> “With an endless field of exposure points, the traditional network security model is outdated ... Designing a new way forward — a future without network perimeters — was the only way to properly manage and mitigate tomorrow's most innovative cyberattacks.”

**Sagi Gidali**
**Co-Founder**
**Perimeter 81**

# PHISHING DOWN FOR THIRD STRAIGHT YEAR

Mirroring how malware is being leveraged, cybercriminals are being more targeted with phishing than ever before, too. So much so, SonicWall Capture Labs threat researchers recorded a 42% decline in overall phishing volume, the third straight year the attack vector declined.

Also like malware, volume is only part of the story. Phishers are being measured, pragmatic and patient. Besides the usual phishing campaigns that attempt to steal login credentials, SonicWall observed new practices using old tricks.

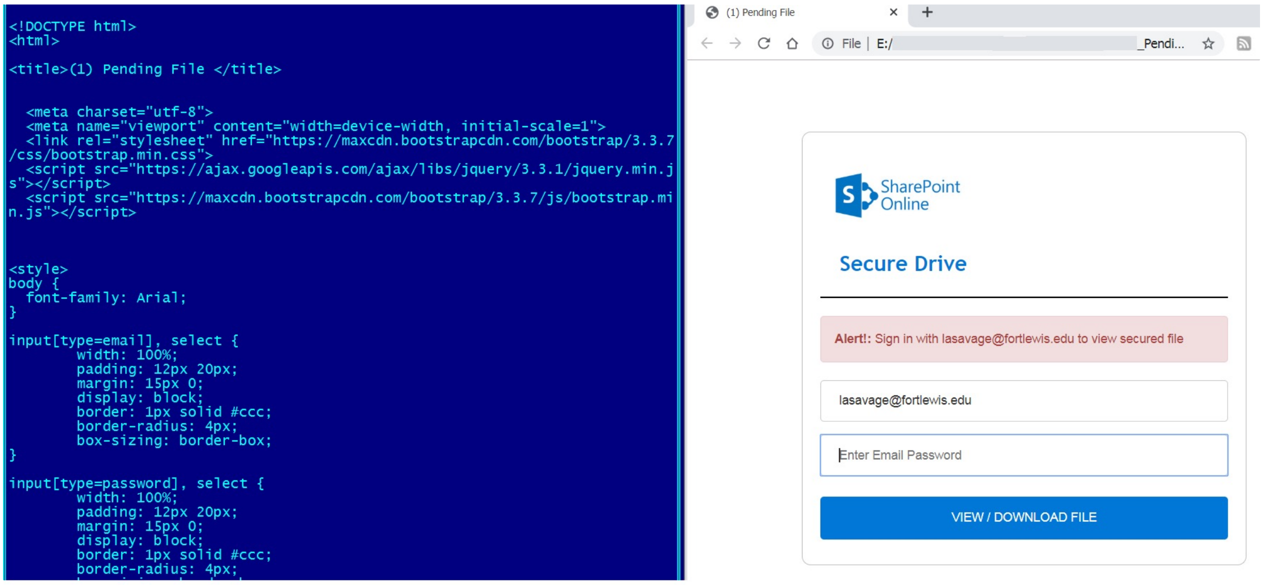
One such example is the use of HTML files leveraging legacy data uniform resource identifier (URI) methods other than JavaScript, which upon rendition displays a fraudulent webpage or form to the victim to illegally obtain usernames and/or passwords from unsuspecting victims.

Employees across a range of organizations, including educational, banking, computer, government, airlines, agriculture, travel, machinery, construction, among others, are often the target of this prevalent phishing tactic.

As was covered in a previous section, PDFs and Microsoft Office files are the delivery vehicles of choice for the modern cybercriminal.

Unfortunately, these files are universally trusted and abundant in the modern workplace.

Threat actors are hoping this trust, coupled with busy work schedules, is enough to trick unsuspecting victims into clicking links or downloading attachments included within phishing emails. In many situations, this click is the only barrier preventing the delivery of the cybercriminal's payload.



```
<!DOCTYPE html>
<html>

<title>(1) Pending File </title>


  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7
/css/bootstrap.min.css">
  <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.j
s"></script>
  <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.mi
n.js"></script>



<style>
body {
  font-family: Arial;
}

input[type=email], select {
        width: 100%;
        padding: 12px 20px;
        margin: 15px 0;
        display: block;
        border: 1px solid #ccc;
        border-radius: 4px;
        box-sizing: border-box;
}

input[type=password], select {
        width: 100%;
        padding: 12px 20px;
        margin: 15px 0;
        display: block;
        border: 1px solid #ccc;
        border-radius: 4px;
```

Secure Drive

**Alert!:** Sign in with lasavage@fortlewis.edu to view secured file

lasavage@fortlewis.edu

Enter Email Password

**Old tricks are new again.** The example above, found in 2019, shows how data URI methods can be leveraged to present target victims with fraudulent web pages or forms to steal user credentials.

# CRYPTOJACKING CRUMBLES

The shuttering of the Coinhive mining operation in March 2019 dealt a devasting blow to the nefarious cryptojacking racket that abused the service.

Coinhive was not inherently malicious; it was an alternative method for websites to earn revenue instead of showing advertisements. Coinhive-enabled websites allocated a small portion of visitors' processing power to legitimately mine cryptocurrency.

**78%**

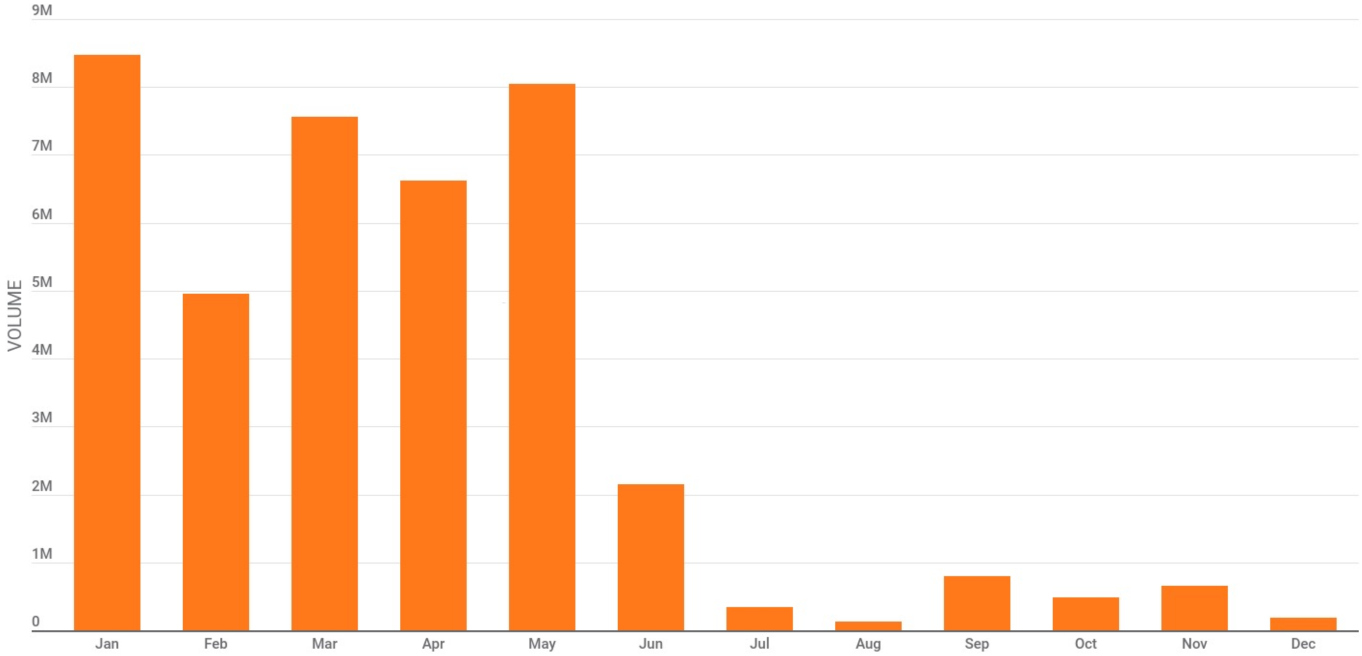
After the shuttering of Coinhive, the volume of cryptojacking hits dropped 78% during the second half of 2019.

Unfortunately, attackers misused this technology by infecting a large number of websites with Coinhive scripts and used the processing power of unsuspecting victims to mine cryptocurrency for themselves (without users' knowledge). The cryptocurrency of choice was usually Monero.

While the ebb and flow of cryptocurrency prices didn't help encourage authors to write new cryptojacking malware, the loss of Coinhive was too much for the malicious movement to overcome.

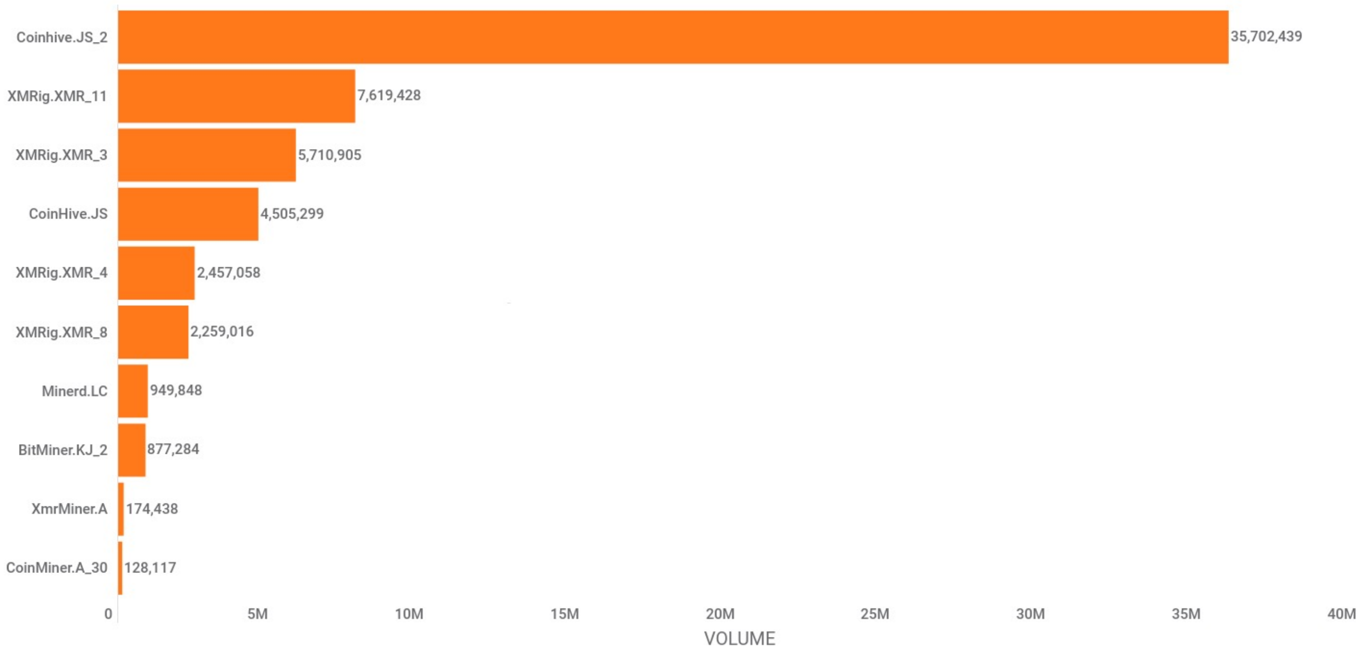
In fact, bitcoin even made a surge halfway through 2019 to help cryptojacking stay relevant as a lucrative option for cybercriminals.

## 2019 Cryptojacking Signature Hits



# CRYPTOJACKING CRUMBLES

## 2019 Top Cryptojacking Signatures



SONICWALL

But crypto prices slumped again in late 2019 and remnant Coinhive malware faded with it. XMRig and Bitminer were the primary cryptojacking malware remaining, but their collective volume was a fraction of Coinhive.

To put the decline in perspective, SonicWall reported that total **cryptojacking hits reached 52.5 million** for the first six months of 2019.

Despite a late surge in December (expected seasonal attack spike), the malware finished with 64.1 million total hits in 2019, a **78% drop** since the start of July 2019.

# RANSOMWARE TARGETS STATE, PROVINCIAL & LOCAL GOVERNMENTS

In 2019, there was an increase in ransomware used in targeted attacks toward state, provincial and local governments, as well as large corporations.

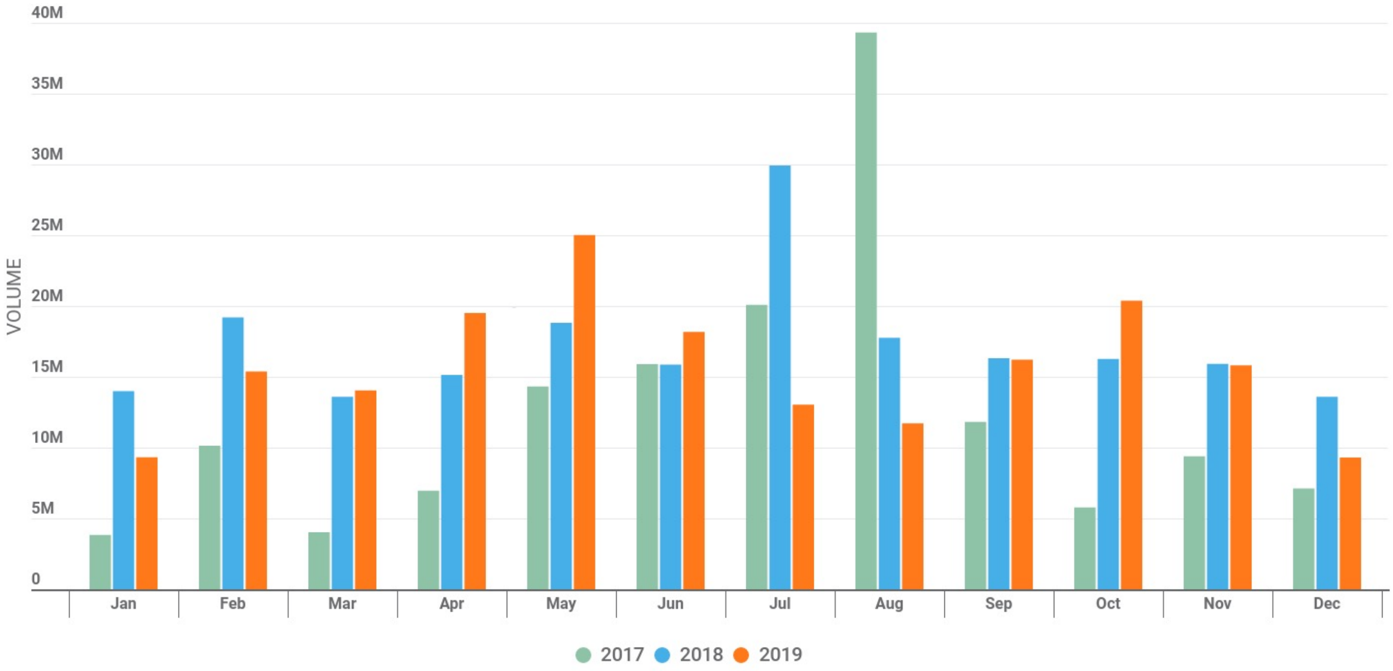
Attacks have ranged from hospitals, police stations and educational institutions to aluminum factories (Norsk Hydro, Norway) and power grids (City Power, Johannesburg).

“In a modern, citizen-centric environment, successful ransomware attacks are highly disruptive,” SonicWall President and CEO Bill Conner wrote for Forbes. “Networks from city hall, law enforcement agencies, sanitation, courthouses or the DMV could be compromised in minutes and everyday operations held for ransom, often at exorbitant costs.”

Following the same trend as global malware volume, ransomware attacks were down slightly in 2019.

SonicWall Capture Labs threat researchers recorded **187.9 million in total ransomware volume** for the year, a 6% drop from the record-breaking 2018 volume.

Global Ransomware Volume



# RANSOMWARE TARGETS STATE, PROVINCIAL & LOCAL GOVERNMENTS

But volume shouldn't be confused with effectiveness. Cybercriminal organizations that leverage ransomware continue to focus on the quality of their attacks over sheer quantity. It's no longer the size of the organization, but rather their likeliness to pay.

Unfortunately, in 2019 that meant a number of highprofile attacks against various state, provincial and local governments. More than 140 state and local governments are reported to have been hit with ransomware in 2019, although the actual number is likely much higher.

Another study stated that ransomware infected some 621 schools and hospitals through September 2019.

The year saw ransomware attacks across the U.S. bring city services to a halt, including those in Arizona, Florida, Georgia, Indiana, Maryland, Nevada, New York, Texas and more.

Larger organizations remain the most lucrative targets as they are more likely to pay higher sums of money for data restoration compared to the average end-user. Bitcoin remains the dominant currency for ransom payments because of its anonymity (when used correctly).

## Schools under siege by ransomware

K-12 districts and higher education institutions across the world were also targeted with ransomware in 2019. And it's very much a global epidemic.

In the U.S., ransomware attacks took down schools across the country, from New York, New Jersey, Louisiana and Oklahoma to California and back again.

In some cases, like Livingston Public Schools in New Jersey, classes were delayed because of ransomware infection. That attack even took down the district's payroll system. Similar delays were felt by districts in Michigan, Alabama and New York.

In the U.K., penetration testing conducted by JISC, the government agency that provides many computerized services to U.K. academic bodies, tested the defenses of over 50 British universities.

The results were unflattering: the pen testers scored a 100% success rate, gaining access to every single system they tested. Defense systems were bypassed in as little as an hour in some cases, with the ethical hackers easily able to gain access to information such as research data, financial systems as well as staff and student personal information.

> “In a modern, citizen-centric environment, successful ransomware attacks are highly disruptive. Networks from city hall, law enforcement agencies, sanitation, courthouses or the DMV could be compromised in minutes and everyday operations held for ransom, often at exorbitant costs”

**Bill Conner**
**President & CEO**
**SonicWall**

In Australia, the head of the local intelligence agency was recruited to inform universities about cyber threats and ways of prevention. This was one of the initiatives put in place after an extremely sophisticated threat actor compromised the Australian National University (ANU) and persisted within the university's network for months at a time.

### Small targets, end-users not safe

Although there has been a continued shift toward higher profile targets, ransomware attacks against average end-user remain steady.

This year SonicWall found that ransomware operators are more willing to chat and negotiate with their victims. In fact, SonicWall has studied ransomware crime groups and operators via several live conversations, including one well-documented, two-week dialog with a Russian ransomware cell.

Most interactions between victim and operator is via email, but everything from Telegram to built-in, custommade chat applications are being used to contact victims for payment.

The past 12 months have also seen an increase in sextortion scams, where attackers claim to have obtained highly sensitive personal information — usually images — of their victims.

These attacks take the form of a simple email claiming that personal information or photos will be released to the victim's contacts if the ransom demand is not met. In most cases, the false claims are scare tactics and no security compromise or malware have been used.

SonicWall also observed that cybercriminals favor using readily available ransomware kits for their attacks. Like SonicWall highlighted in the 2019 mid-year report, the most detected ransomware are variants available via ransomware-as-a-service (RaaS) offerings.

Other popular options include ransomware apps that are based on open-source code.

# CERBER CONTINUES REIGN AS TOP RANSOMWARE STRAIN

Once a malware author creates something eloquent, effective and easy to deploy, others leverage the code and follow the money.

In fact, SonicWall Capture Labs threat researchers detected 1,202 different ransomware signatures in 2019 alone.

Not only was Cerber the top ransomware family of 2019 (making up 33% of all ransomware attacks), it also boasted four of the top 10 ransomware signatures of the year, including the top two spots totaling more than 77 million hits.

Other notable or high-profile ransomware variants for the year include Jigsaw, HiddenTear, GlobeImposter, Sodinokibi, GandCrab and LockerGoga.

2019 Top Ransomware Signatures

| Signature | Hits |
|---|---|
| Cerber.G_5 | 46,046,011 |
| Cerber.RSM | 31,956,607 |
| GandCrab.RSM_5 | 7,901,296 |
| Cerber.RSM_20 | 6,030,471 |
| GandCrab.RSM_23 | 5,486,502 |
| HiddenTear.RSM_18 | 5,385,355 |
| BadRabbit.CM | 3,814,511 |
| Cerber.FLFJ | 3,371,611 |
| JobCrypter.RSM | 3,302,828 |
| Locky.A_140 | 2,799,119 |
| Termite.RSM | 2,633,405 |
| CryptoJoker.RSM | 2,413,649 |

# FILELESS MALWARE SPIKES IN Q3

Fileless malware is a type of malicious software that exists exclusively as a memorybased artifact (i.e., RAM).

Fileless malware does not write any part of its activity to the computer's hard drive, making it very resistant to existing computer forensic strategies that incorporate file-based whitelisting, signature detection, hardware verification, pattern-analysis, time-stamping, etc.

Simply, fileless malware leaves very little by way of evidence that could be used by digital forensic investigators or threat researchers to identify illegitimate activity. This type of malware attack has become commonplace as malware authors become more creative in evading detection.

A typical fileless malware can use PowerShell scripts (located within the Microsoft Windows Registry system) to launch an attack. Others, like IcedId, combine PowerShell scripts and malicious Microsoft Word documents to distribute malware.

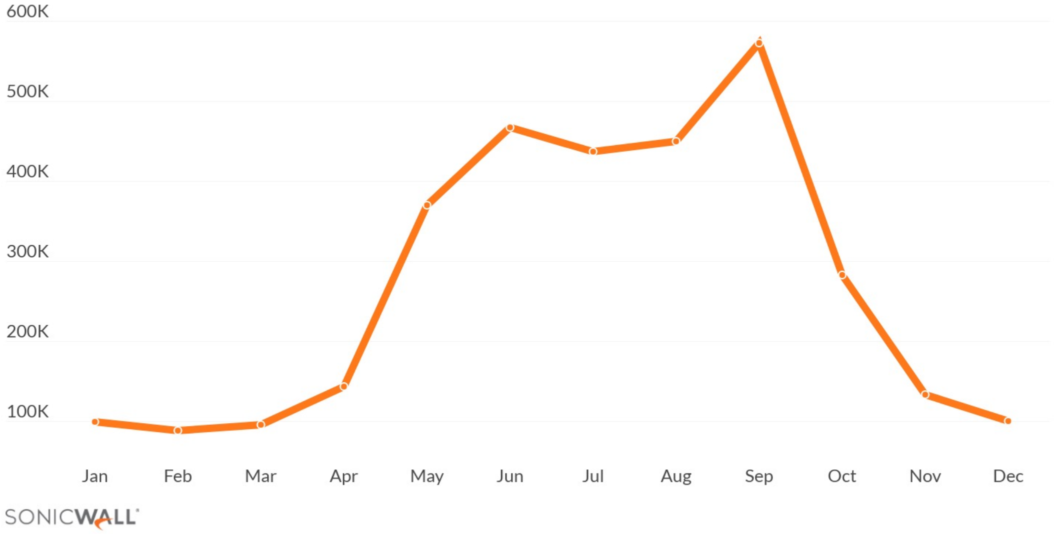
Given that attacks involve several stages for functionalities like execution, persistence, or information theft, some parts of the attack chain may be fileless, while others may involve the file system in some form.

SonicWall Capture Labs threat researchers found that fileless malware incidents increased in the second and third quarters of 2019 when compared to the same period in 2018, but trailed off in the fourth quarter.

### Most Common Fileless Malware in 2019

- GandCrab Ransomware
- Kovter
- Ursnif Banking Trojan
- IcedId Banking Trojan
- Divergent
- PCASTLE Monero-Mining Malware
- Astaroth Backdoor Trojan
- Nodersok

### 2019 Fileless Malware Attack Volume



# ENCRYPTED THREATS GROWING CONSISTENTLY

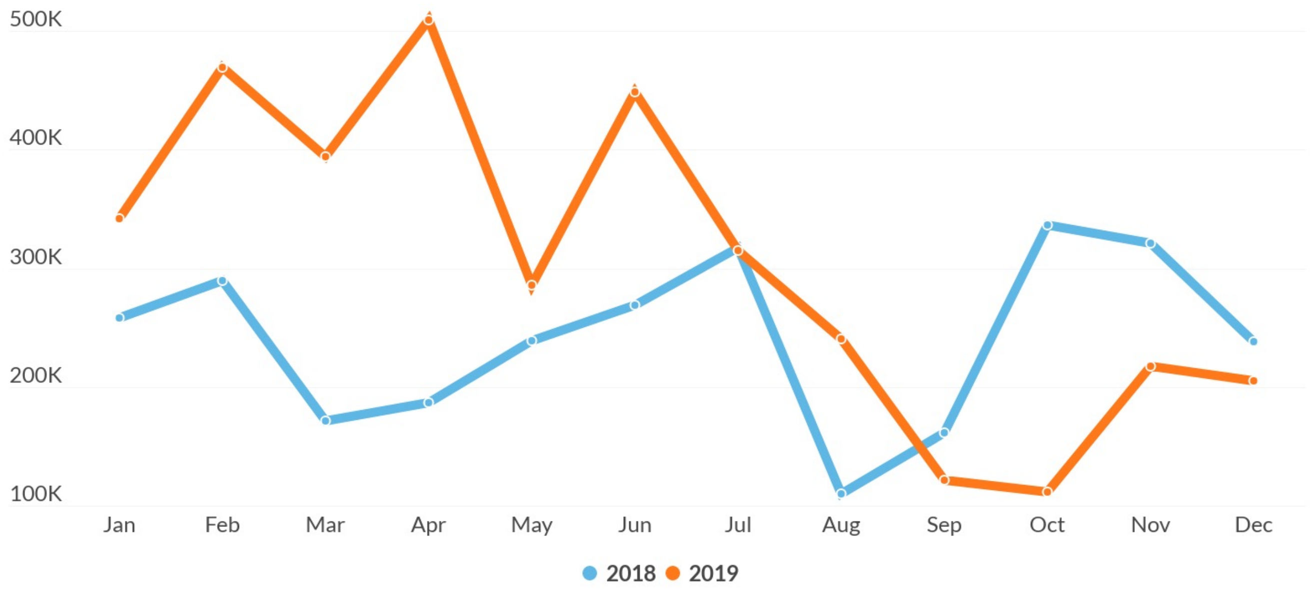
To increase the chances of a malware deploying and executing within a target environment, savvy cybercriminals use transport layer security (TLS) and secure sockets layer (SSL) encryption standards to mask their attacks from inspection by traditional security controls.

In 2019, SonicWall Capture Labs threat researchers recorded **3.7 million malware attacks sent over TLS/SSL traffic, a 27.3% year-over-year increase.**

Launching malware across encrypted traffic works for threat actors because many firewall appliances do not have the capability or processing power to responsibly detect, inspect and mitigate cyberattacks sent via HTTPS traffic.

This is a mounting concern. Despite the dip to close the year, the consistently upward volume trends suggest the use of this attack vector will only increase in the future.

Encrypted Malware



SONICWALL

# ENCRYPTED THREATS GROWING CONSISTENTLY

### Hiding among the pack

Malware comes in many flavors. While ransomware attacks, including Cerber, have commonly been encrypted the last two years, SonicWall Capture Labs threat researchers are seeing an influx of malicious packers encrypted by TLS or SSL standards.

Although intended for legitimate purposes, packers are used by malware authors to circumvent detection.

At a basic level, packers compress a range of files into a single executable, which is later decompressed to create the original file set. Common packers include Aspack, Armadillo and UPX.

For malware, however, packers are used to obfuscate the executable, evade detection and make it challenging for threat researchers to analyze a sample.

### Importance of SSL/TLS inspection

Encrypted traffic is a growing attack vector for cybercriminals. Unfortunately, there is a fear of complexity and a general lack of awareness around the need to responsibly inspect SSL and TLS traffic — particularly using deep packet inspection (DPI) — for malicious cyberattacks.

It's important to consult with your security or firewall provider to ensure you have this capability and that it is properly enabled.

| Encrypted Threat | Type | Hits |
|---|---|---|
| Suspicious#Aspack.G | Packer | 689,240 |
| ARMADILLO packed executable_2 file | Packer | 589,385 |
| Kryptik.C_53 | Packer | 328,571 |
| UPX_Packed_Executable_0 | Packer | 116,100 |
| Parite.A.gen | Malware | 54,109 |
| MalScript.EML | Malware | 53,263 |
| Samsam.RSM | Ransomware | 33,287 |
| Downloader.CCQ | Malware | 29,169 |
| Emotet.XML | Malware | 14,453 |
| Suspicious#mpress.2 | Malware | 14,320 |
| Sality.AN.gen | Malware | 11,542 |
| Suspicious#RLPack | Malware | 11,383 |
| Inject.HHWB | Malware | 10,353 |

# IOT ATTACK VOLUME RISING

According to one industry study, the global IoT security market is expected to reach or exceed $35.2 billion (USD) by 2023, a spike of 33.7% based on compound annual growth rate (CAGR).

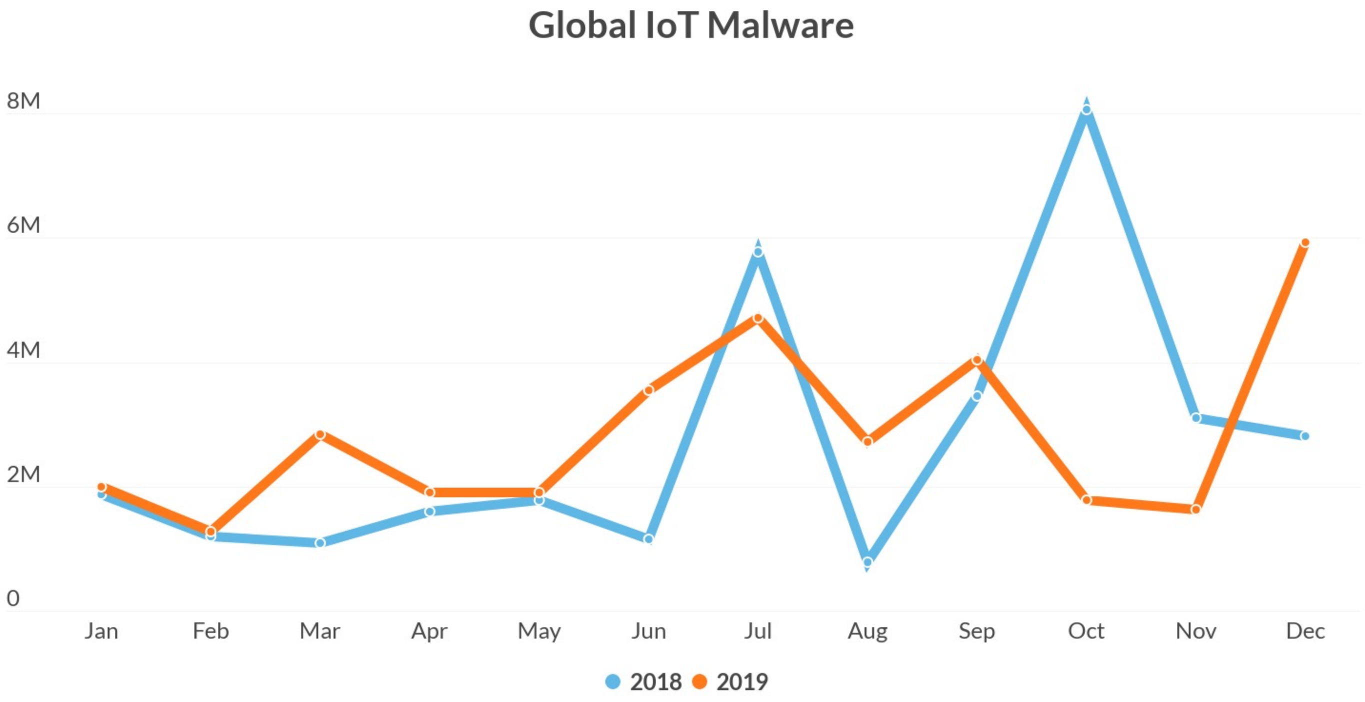
As witnessed in global news headlines, concerns over IoT device security — and respective IoT security regulations — are driving the high market forecasts.

Given the tenuous landscape regarding data privacy, and the fact that everything from nanny cams to doorbells are connected, IoT-focused attacks will only increase in 2020 and beyond.

In 2019, SonicWall Capture Labs threat researchers discovered a moderate 5% increase in IoT malware, with **total volume reaching 34.3 million attacks**.

But with a deluge of new IoT devices connecting each day, increases in IoT malware attacks should not only be expected, but planned for.

Common IoT security weakness include weak or hard-coded passwords, insecure networks and interfaces, and lack of secure update mechanisms.



SONICWALL

# WEB APP ATTACKS DOUBLE IN 2019

Web applications make the digital world spin, particularly in a hyper-connected, clouddominant landscape. They help deliver the client-side experience most end-users know and use within their favorite browser.

Everything from Office 365 and G Suite, to Salesforce and Dropbox, either deliver cloud-first interfaces or offer web versions that complement a software offering.

But for all their convenience, web applications can introduce pathways for cybercriminals or threat actors to illegally access networks or systems full of sensitive data.

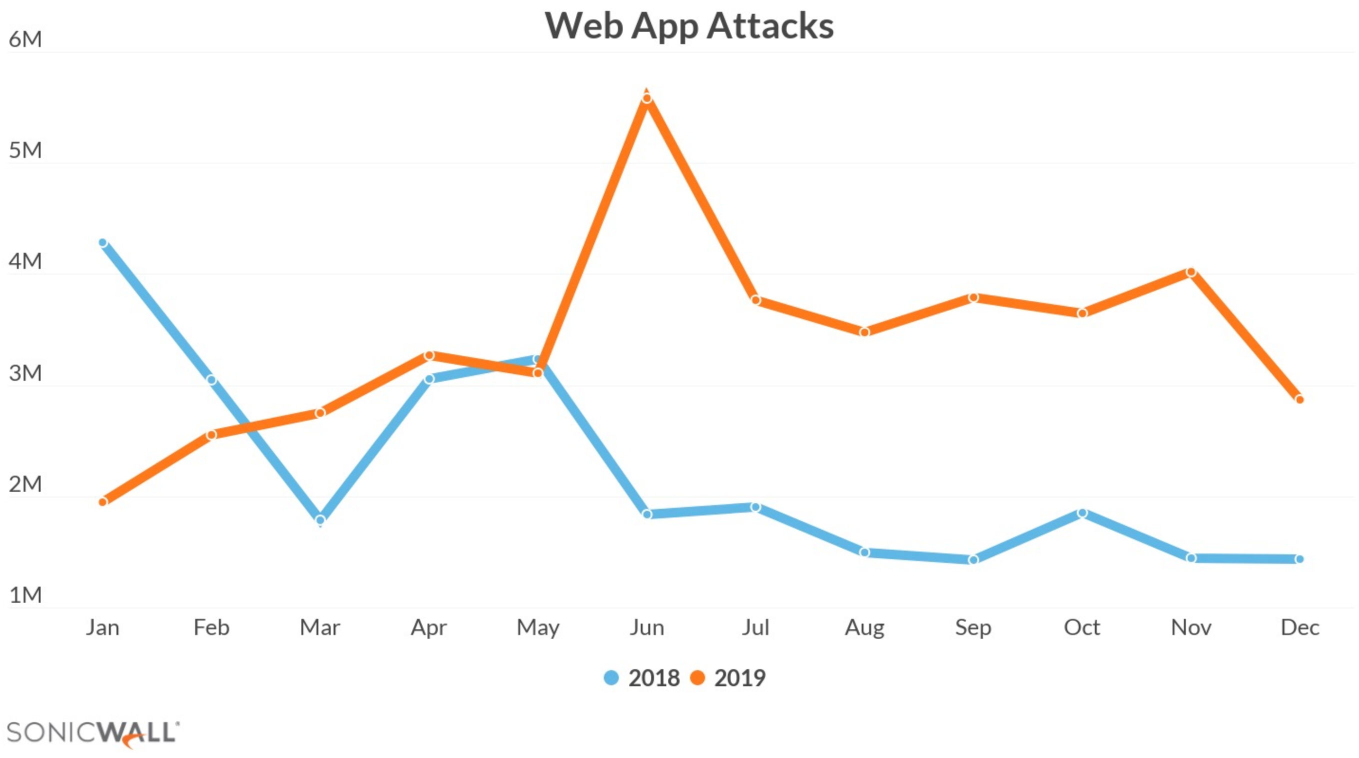
Every few years, the Open Web Application Security Project (OWASP) publishes detailed analysis, guidance and threat warnings across a range of networking, cloud and security topics.

One of their most popular is "The Ten Most Critical Web Application Security Risks," which identifies and categorizes potential risks against web applications.

And they are increasing their pace and sophistication.

For 2019, SonicWall Capture Labs threat researchers recorded a **52% year-over-year increase in web app attacks**.

Volume was largely flat until May, but SonicWall recorded spikes in across the final seven months of year to push total **web app attack volume past 40 million**.



# WEB APP ATTACKS DOUBLE IN 2019

This list is often leveraged by the greater security industry as a framework to protect against common web app attacks.

Unfortunately, this dynamic also provides cybercriminals with a better blueprint from designing attacks.

Currently, the top known web attacks include SQL injection, directory traversal, cross-site scripting (XSS), broken authentication and session management, cross-site request forgery (CSRF) security misconfigurations, sensitive data exposure and more.

For this, many organizations are complementing physical and virtual firewalls with web application firewalls (WAF) to eliminate security vulnerabilities and harden their overall security posture.

| 2019 Top WAF Attacks |
|---|
| SQL Injection Attack 1 |
| Web Application Directory Traversal Attack 5 |
| Unauthorized Remote File Access |
| Web Application Directory Traversal Attack 6 |
| SQL Injection Attack 11 |
| Cross-site Scripting (XSS) Attack |
| PHP NULL Poisoning |
| Blind SQL Injection Attack Variant 12 |
| Web Application Directory Traversal Attack 1 |
| Bash Code Injection |

# PREPARING FOR WHAT'S NEXT

The evasive and persistent cyberattacks outlined in this report create boundless points of exposure to your organization. These fast-moving dynamics affect even the wellfunded or intentioned organizations, damaging their ability to operate.

Risk escalates exponentially. Cost becomes prohibitive. The shortage of trained personnel becomes more acute. Constrained resources can't keep up.

SonicWall takes pride in not only collaborating with the global cybersecurity community, but also ensuring our teams and capabilities are finely tuned to exceed your business and security objectives.

With SonicWall you always know the unknown, see everything in real time, and act fast on what matters — preventing even the most evasive emerging threats.

To learn more, visit **sonicwall.com**

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

* 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

SonicWall has been fighting the cybercriminal industry for over 28 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award-winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.