SONICWALL®

Unmasking the Threats That Target
Global Enterprises, Governments & SMBs

2019 SONICWALL CYBER THREAT REPORT

sonicwall.com | @sonicwall

TABLE OF CONTENTS

A WORD FROM BILL

The cybersecurity industry is a unique community. Although we may offer different methods to achieve a secure outcome, we share similar values, objectives and an overall duty to protect others.

For SonicWall, that means offering powerful but cost-effective security solutions for small- and medium-sized businesses (SMBs), enterprises and government agencies.

But we also understand the power of shared knowledge. Collaboration is critical. Dialogue is vital. Awareness is our lifeblood.

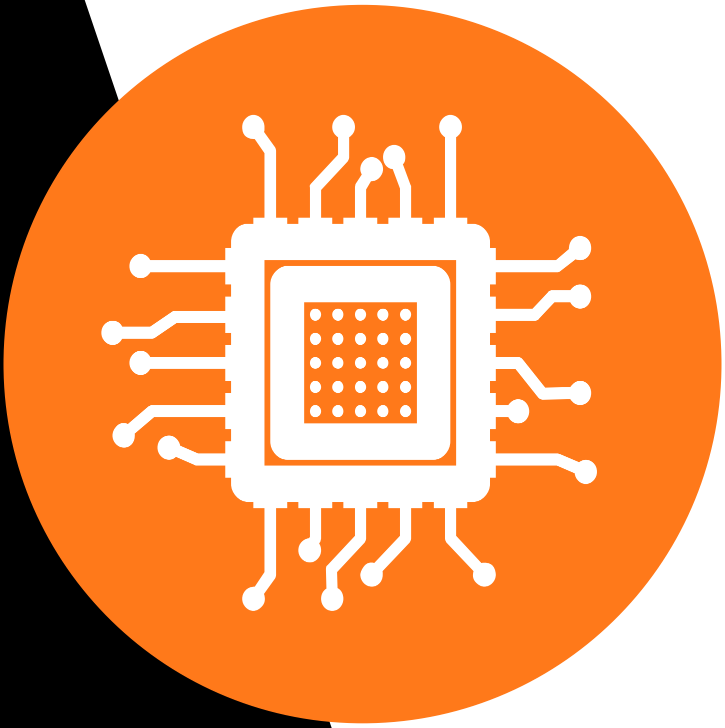
We publish the annual SonicWall Cyber Threat Report to promote this communal ideology. I'm confident you'll find this threat intelligence and research valuable in your pursuit to safeguard your own businesses, customers, networks and data.

Our team has been on the front lines of the cyber arms race for 27 years. We will never relent from that cause. We stand by your side with a common mission: a safer online landscape. That's our commitment to you.

More business. Less fear.

Bill

Bill Conner
President & CEO
SonicWall



DECODING THE CYBER ARMS RACE

Even for organizations, businesses and governments, a cyberattack is personal. At its very core, they strip these establishments and employees of their identities, intellectual property, privacy, reputation and monetary assets.

In the end, the victims are always human — whether they are the leadership at large enterprises, small-business owners who have been extorted, or just a single innocent contact in a massive data dump on the dark web.

As SonicWall has documented through the years, the cyber arms race does not discriminate or differentiate. If a network, identity, device or data is valuable — particularly information tied to intellectual property, financials, sensitive files, critical infrastructure or political leverage — cybercriminals will identify, target and ruthlessly attack.

To promote global awareness and facilitate important dialogues, SonicWall remains steadfast in its commitment to research, analyze and share threat intelligence via the **2019 SonicWall Cyber Threat Report**.

The unification, analysis and visualization of these threats will empower these groups to fight back with more authority, determination and veracity than ever before.

> To promote global awareness and facilitate important dialogues, SonicWall remains steadfast in its commitment to research, analyze and share threat intelligence.

Breaches steal the headlines

It was the "perfect" ending to a year headlined by breaches. In previous years, specific malware strands — Petya/NotPetya, Bad Rabbit and WannaCry — earned media attention. But 2018 was more about the result, not the cause. Breach after breach was reported, each seemingly eclipsing the size and scale of the last.

Then, either as a final cap to 2018 or a foreboding start to the new year, 2019 began with news of 'Collection No. 1.' But don't let the mega data dump's generic name mask its industry-rattling impact; more than 772.9 million unique email addresses and some 21 million unique passwords were posted on a hacking forum for sale to anyone willing to pay.

The dump was first flagged by 'Have I Been Pwned,' a free service that emails you if your name or email address is recorded in a data dump. To date, the service has recorded more than 6.4 trillion compromised accounts across 340 sites.

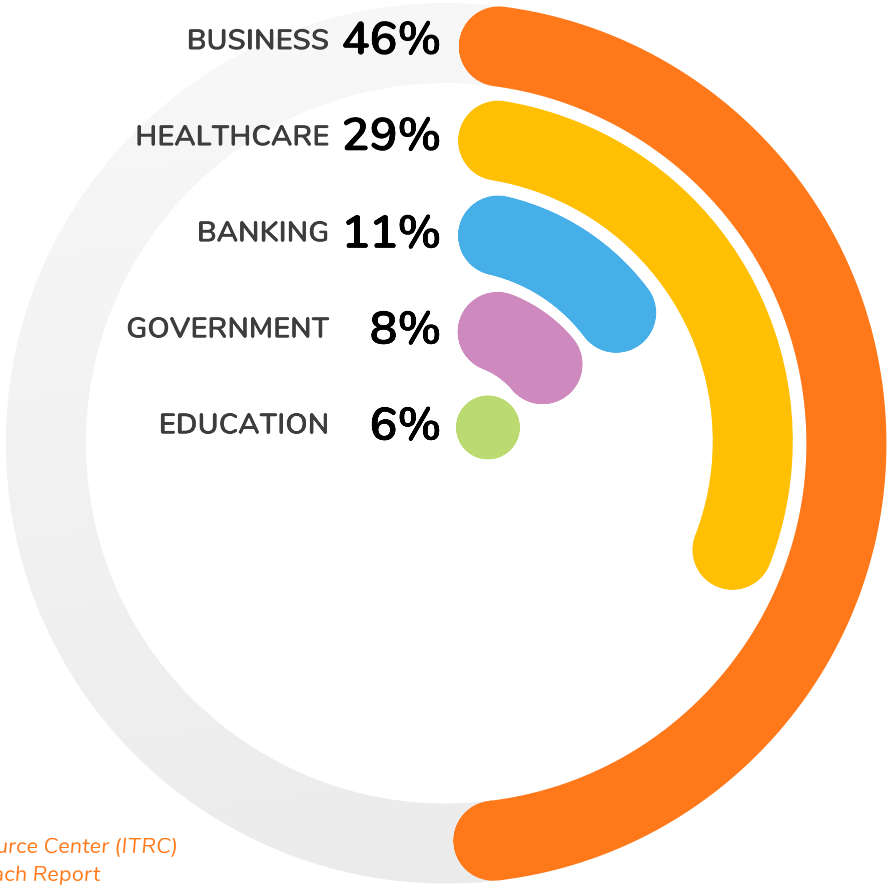
Weeks later, Collections 2-5 were discovered. These massive stolen data troves reportedly weigh in at some 845 gigabytes and include more than 25 billion records. According to the Hasso Plattner Institute in Potsdam, Germany, these four collections are triple the size of the original Collection No. 1.

The massive data thefts aside, 2018 was riddled with breaches at major companies, brands, services and government agencies. Breaches at Exactis (340 million records), Under Armour (150 million), Facebook (in April and September for 137 million total records), Quora (100 million), MyHeritage (92 million) and Panera (37 million) all grabbed headlines with data thefts that soared above 35 million records.

Processor attacks still an unknown, dangerous threat

New side-channel threats, including the much publicized Spectre, Meltdown, Foreshadow, PortSmash and Spoiler attacks, moved the cyber war to an entirely new theater in 2018 — one that is extremely difficult to monitor or defend. Alarmingly, these are only the processor vulnerabilities the public actually knows about to date.

2018 U.S. BREACH VOLUME BY INDUSTRY



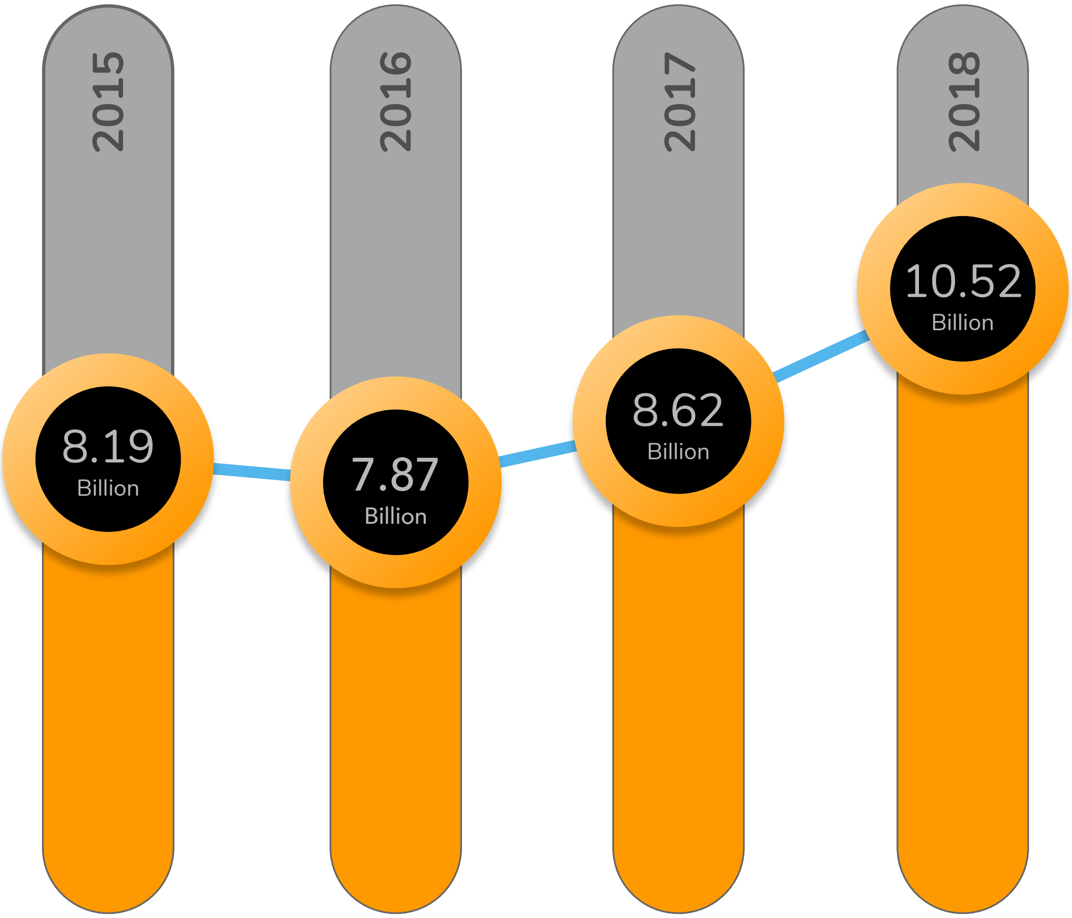
Source: *Identity Theft Resource Center (ITRC) 2018 End-of-Year Data Breach Report*

Global malware volume up for third straight year

In 2016, the industry witnessed a decline in malware volume, leading some to speculate that cybercrime was on the decline. Since then, **malware attacks have increased 33.4 percent**.

Globally, SonicWall logged 10.52 billion* malware attacks in 2018 — the most the company has ever recorded. Conversely, SonicWall logged **45 million unique malware samples in 2018** compared to 56 million in 2017, an 11 percent dip.

GLOBAL MALWARE ATTACK VOLUME

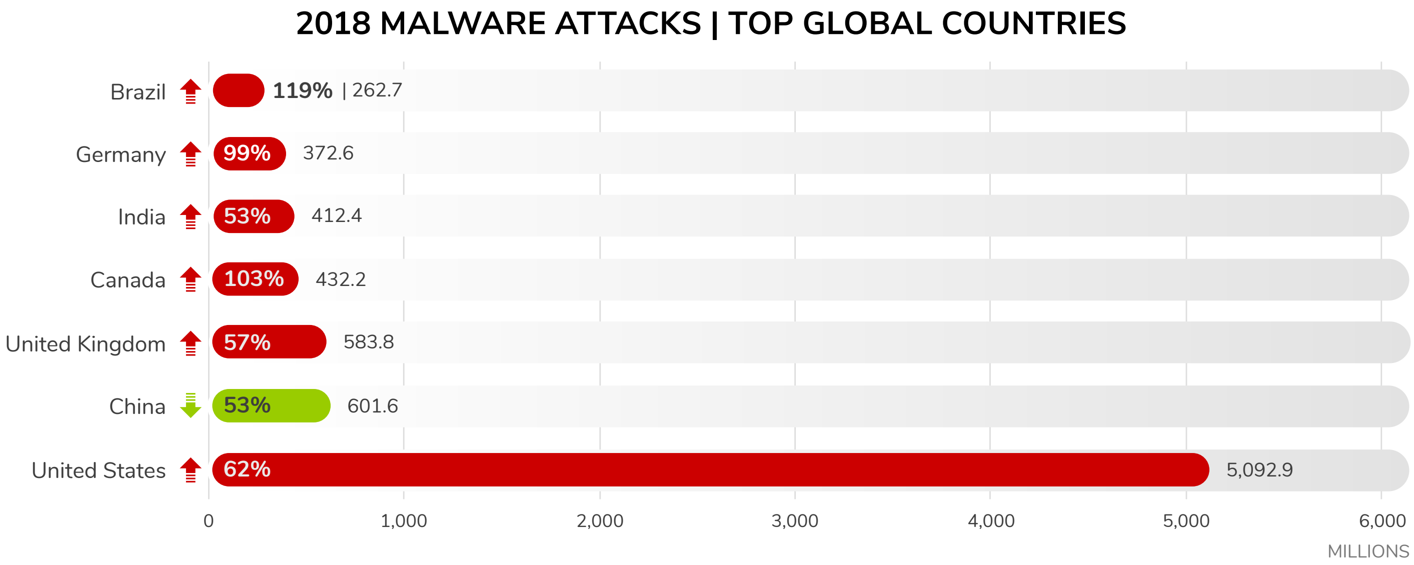


* *As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.*

U.S. most targeted country by malware — and it's not close

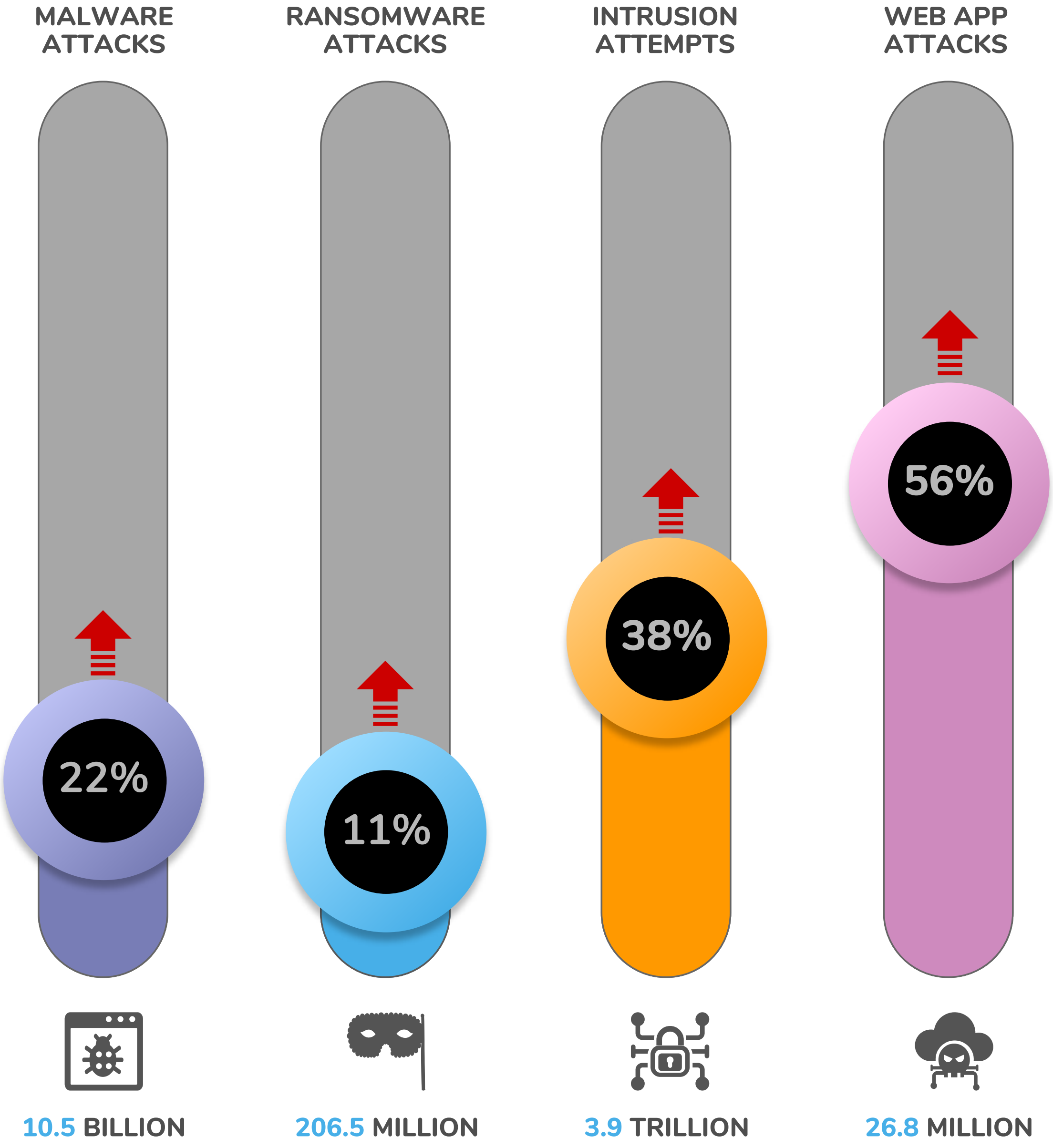
If U.S. citizens feel they're in the middle of a cyber war, it's because they are. The U.S. was the country most heavily targeted by malware in the world — and by a wide margin.

The country faced more than 5.1 billion malware attacks in 2018, which is nearly 50 percent of the 10.52 billion total malware attacks SonicWall recorded worldwide. Only China (601.6 million), the U.K. (583.8 million), Canada (432.2 million) and India (372.6 million) were even close in the volume of malware each faced.



Top 10 ranking for malware data based on number of SonicWall customers.

2018 GLOBAL CYBERATTACK TRENDS



Published CVEs more than doubled since 2016

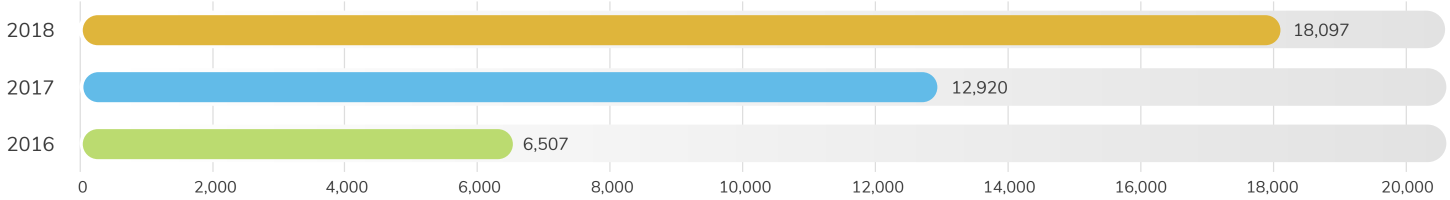
As a trusted Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA), SonicWall closely collaborates with the global cybersecurity industry to help identify vulnerabilities and quickly ensure greater security awareness.

In 2018, **18,097 new CVEs were collectively published**, a 178 percent increase since 2016. This trend signifies that the industry is working quicker and more efficiently together to identify critical vulnerabilities and ensure the greater public has guidance to correct any issues.

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.

CVE Numbering Authorities (CNAs) are organizations that operate under the auspices of the CVE program to assign new CVE IDs to emerging vulnerabilities that affect devices and products within their scope.

CVEs PUBLISHED BY YEAR



2018 Zero-Day Vulnerabilities

Of the more than 18,000 new CVEs published in 2018, 10 were published to immediately identify and correct zero-day vulnerabilities.

MONTH	CVE RECORD	VULNERABILITY
February	CVE-2018-4878	Adobe Flash Player Use-After-Free Vulnerability
June	CVE-2018-5002	Adobe Flash Player Stack-Based Buffer Overflow
July	CVE-2018-4990	Adobe Acrobat Reader ‘Double Free’ Vulnerability
July	CVE-2018-8120	Microsoft Win32k Elevation of Privilege Vulnerability
September	CVE-2018-8440	Microsoft Windows ALPC Elevation of Privilege Vulnerability
September	CVE-2018-8393	Microsoft JET Database Engine Buffer Overflow
October	CVE-2018-8453	Microsoft Win32k Elevation of Privilege Vulnerability
November	CVE-2018-8589	Windows Win32k Elevation of Privilege Vulnerability
December	CVE-2018-15982	Adobe Flash Player Use After Free vulnerability
December	CVE-2018-8653	Scripting Engine Memory Corruption Vulnerability

ABOUT THE SONICWALL CAPTURE LABS THREAT NETWORK

Intelligence for the 2019 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 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 MILLION+
Global Sensors

215+
Countries & Territories

24x7x365
Monitoring

<24 HOURS
Threat Response

140,000+
Malware Samples Collected Daily

28 MILLION+
Malware Attacks Blocked Daily

KEY FINDINGS FROM 2018

Security Advances

U.K., India Harden Against Ransomware

Globally, ransomware volume was up across the board in almost every geographic region but two: the U.K. and India.

Dangerous Memory Threats, Side-Channel Attacks Identified Early

In 2018, we saw the likes of Meltdown, Spectre, Foreshadow, PortSmash and, in March 2019, Spoiler shift the cyber war to an entirely new theater. Fortunately, SonicWall's patent-pending Real-Time Deep Memory Inspection™ (RTDMI™) is one of the few solutions able to identify and mitigate attacks against these processor vulnerabilities.

Machine Learning Maturing to Stop New Malware Variants

SonicWall RTDMI technology uses machine learning to identify 'never-before-seen' cyberattacks — variants so sophisticated they weren't identified or blocked by any other security technology at the time of discovery.

Rise & Fall of Cryptojacking

In 2018, cryptojacking dwindled nearly as fast is it appeared. Volume peaked in September, but has been on a steady decline since. Cryptocurrencies remain a valuable commodity to cybercriminals because of its anonymity — especially if they can mine for it with stolen processing power. But will it return in 2019?

Global Phishing Volume Down, Attacks More Targeted

As businesses get better at blocking email attacks and ensuring employees can spot and delete suspicious emails, attackers are shifting tactics. New data suggests they're reducing overall attack volume and launching more highly targeted phishing attacks.

TLS/SSL Encryption Maintains Steady Growth

The use of transport layer security (TLS) and secure sockets layer (SSL) protocols to encrypt and protect data in transit is a standard for modern internet security. Data again shows steady, but positive, growth in the use of HTTPS.

KEY FINDINGS FROM 2018

Criminal Advances

Ransomware Attacks Up Again Globally
Despite regional efforts to thwart ransomware attacks, ransomware volume jumped 11 percent year over year. Exclusive SonicWall data paints a detailed picture of which regions are being targeted.

Malicious PDF & Office Files Beating Legacy Security Controls
Cybercriminals are tooling trusted PDFs and Office files to circumvent traditional firewalls and even sandboxes. Proprietary threat data highlights this growing trend.

Non-Standard Ports Ripe for Exploitation
Ports 80 and 443 are standard ports for web traffic, so they are where most firewalls focus their protection. In response, cybercriminals are targeting a range of non-standard ports to ensure their payloads can be deployed undetected in a target environment. The problem? Organizations aren't safeguarding this vector, leaving attacks unchecked.

IoT Attacks Escalating
The speed at which Internet of Things (IoT) devices are blanketing homes, offices and public spaces is impacting cybersecurity and network defenses. Consumers are simply hungry for more and more connected devices. But this appetite has resulted in a deluge of IoT devices rushed to market without proper security controls.

Encrypted Attacks Growing Steady
The growth in encrypted traffic is coinciding with more attacks being cloaked by TLS/SSL encryption. More than 2.8 million cyberattacks were encrypted in 2018.

Building Global Trust

In April 2018, SonicWall was named the 85th Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA).

LEARN MORE

U.K., INDIA HARDEN AGAINST RANSOMWARE

SonicWall Capture Lab threat researchers analyzing full-year 2018 threat data found that ransomware was up in just about every geographic region but two: the U.K. and India.

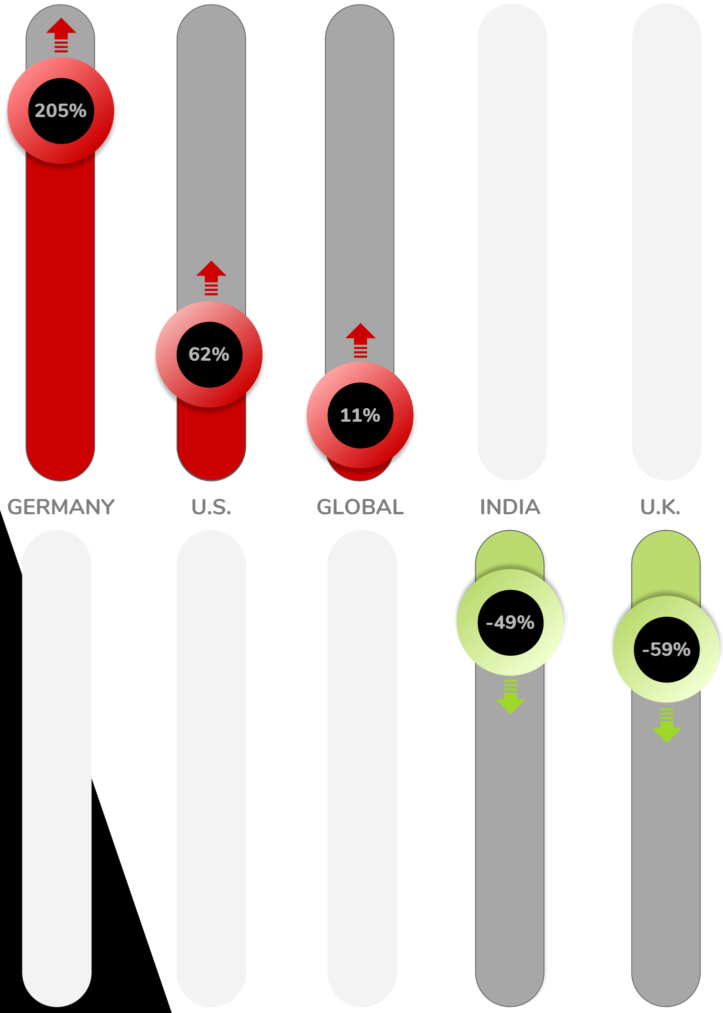
While many major countries across North America, Europe and Asia were all experiencing increases in ransomware attacks, the U.K. and India quietly faced 59 and 49 percent reductions, respectively, in ransomware volume.

In the U.K., one theory focuses on the fallout from one of 2017's most high-profile ransomware attacks. In May 2017, an estimated 40 National Health Service (NHS) entities in England and Scotland were victimized by ransomware that affected care or slowed access to patient data.

"Most of the vendors in the U.K. and their customers put solutions in place to protect against multiple family variants of ransomware," SonicWall President and CEO Bill Conner told Information Age. "Geographically, you see who has taken ransomware more seriously, just based on the numbers."

As seen in the NHS case, ransomware remains one of the most malicious cyberattacks that can cripple a business or organization. Cybercriminals are shifting attacks to larger corporations with weaker defenses and demanding greater sums of money, typically in the form of cryptocurrency. Attackers also will continue to target organizations with high-value data, such as financial and hospital records.

2018 RANSOMWARE VOLUME



DANGEROUS MEMORY THREATS, SIDE-CHANNEL ATTACKS IDENTIFIED EARLY

One of the key themes of 2018 was the growing number of processor vulnerabilities and related side-channel attacks.

While past years were dominated by large-scale malware attacks, the recent past has seen Foreshadow, Spoiler, PortSmash, Meltdown and Spectre drive the most cause for concern.

Unfortunately, current research declares 'Spectre is here to stay' and acknowledges various vulnerabilities in processors cannot be patched — either in software or hardware — and are a much deeper security concern. As such, side-channel attacks will be a continued risk to the computing landscape, which will make technology that can mitigate these attacks a necessary requirement.

"Relentless researchers are demonstrating that cybercriminals can use the very architecture of processor chips to gain access to sensitive and often highly valued information," said SonicWall President and CEO Bill Conner in an August 2018 story outlining the Foreshadow impact.

SonicWall RTDMI is a prime example of technology being ahead of the curve. A complement of the SonicWall Capture ATP cloud sandbox, RTDMI was one of the few solutions able to identify and mitigate these processor attacks.

SonicWall RTDMI™ vs. Side-Channel Attacks

SonicWall President and CEO Bill Conner hosts CTO John Gmuender as they explain how SonicWall RTDMI technology mitigates today's most dangerous chip-based and side-channel cyberattacks.

WATCH NOW

> **"Relentless researchers are demonstrating that cybercriminals can use the very architecture of processor chips to gain access to sensitive and often highly valued information."**
>
> — Bill Conner
> President & CEO
> SonicWall

Ahead of the Curve

Meltdown & Spectre
JANUARY 2018

These are a pair of complementary attacks that take advantage of speculative execution techniques used on modern processors. Meltdown, for example, leaks sensitive kernel data to other programs, which leads to serious security ramifications. Spectre, which was effective in tests against AMD, ARM and Intel processors, is very similar to Meltdown, but also leaks data to virtualized hypervisors, other systems or programs.

Foreshadow
AUGUST 2018

Foreshadow abuses the same processor vulnerability as the Meltdown exploit, in which an attacker can leverage results of unauthorized memory accessed in transient out-of-order instructions before they are rolled back.

PortSmash
NOVEMBER 2018

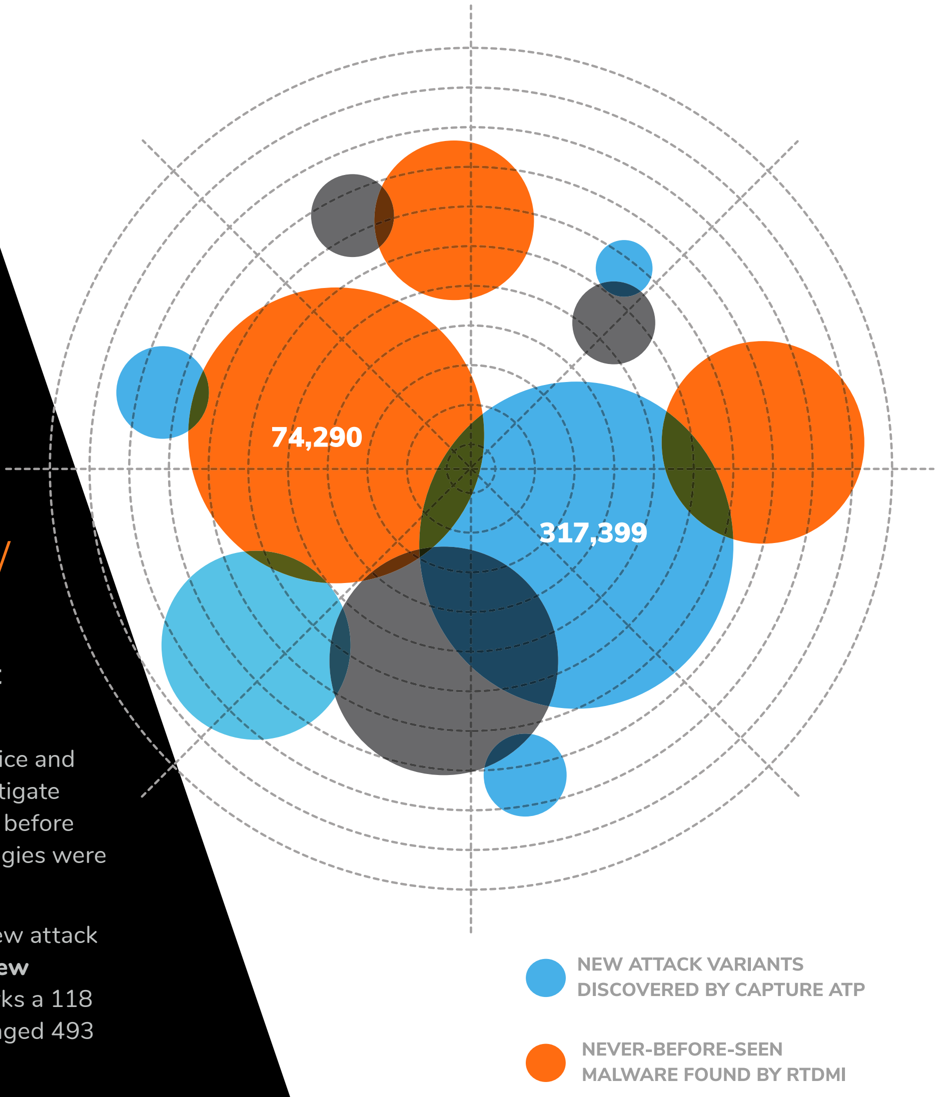
Discovered by researchers in Finland and Cuba, PortSmash is a side-channel attack that takes advantage of simultaneous multi-threading (SMT), which is used by modern processors to execute many parallel instructions on the same CPU. PortSmash is used to run malicious code next to legitimate code and potentially "eavesdrop" on the other simultaneous — and thought to be encrypted — instructions.

Spoiler
MARCH 2019

Research from the Worcester Polytechnic Institute in Worcester, Massachusetts, and the University of Lübeck in Germany, identified a new Spectre-like attack. The group's paper proposes the Spoiler attack, which could exploit a "previously unknown microarchitectural leakage stemming from the false dependency hazards during speculative load operations." The report notes that Spoiler only affects Intel Core processors and not current AMD and ARM processors.

> In a real-world use case, RTDMI is capable of detecting Foreshadow because the technology operates at the CPU-instruction level and has full visibility into the code as the attack is taking place. This allows RTDMI to detect specific instruction permutations that lead to an attack.
>
> To be successful, cache timing must be "measured" by the attack or it can't know what is or isn't cached. This required measurement is detected by RTDMI and the attack is mitigated. In addition, RTDMI can detect this attack via its 'Meltdown-style' exploit detection logic since user-level process will try to access privileged address space during attack execution.

NEW ATTACK VARIANTS DISCOVERED BY CAPTURE ATP



MACHINE LEARNING MATURING TO STOP NEW MALWARE VARIANTS

The more data available, the more efficient machine learning capabilities evolve.

That's how the SonicWall Capture ATP sandbox service and RTDMI technology work in parallel to identify and mitigate new and advanced cyberattacks — some never seen before by a single security vendor or solution. Both technologies were dynamically self-learning in 2018.

In fact, SonicWall Capture ATP identified 391,689 new attack variants in 2018 — an average of more than **1,073 new attacks discovered and blocked each day**. This marks a 118 percent increase over 2017, when Capture ATP averaged 493 new variant discoveries a day.

Looking deeper into the solution, **RTDMI identified 74,290 never-before-seen attacks in 2018**. These are malware variants so new, unique or complex that no other vendor in the world had been able to track or create signatures for them at the time SonicWall discovered them.

Using proprietary machine learning capabilities, RTDMI has become more and more efficient at identifying and mitigating cyberattacks never seen by anyone in the cybersecurity industry.

Since July 2018, the technology's machine learning capabilities caught more undetectable cyberattacks in every month except one. In January 2019, this figure eclipsed 17,000.

74,290

Number of never-before-seen cyberattacks identified by SonicWall RTDMI™ in 2018.

How RTDMI works

Traditional sandbox engines execute files in a virtual environment, log the resulting activity and, after execution, look for and attempt to correlate malicious behavior. The correlation and scoring of these activities and behaviors are prone to both false positives and false negatives.

Modern malware writers implement advanced techniques, including custom encryption, obfuscation and packing, as well as acting benign within sandbox environments, to allow malicious behavior to remain hidden. These techniques often hide the most sophisticated weaponry, which is only exposed when run dynamically and, in most cases, is impossible to analyze in real-time using static detection techniques.

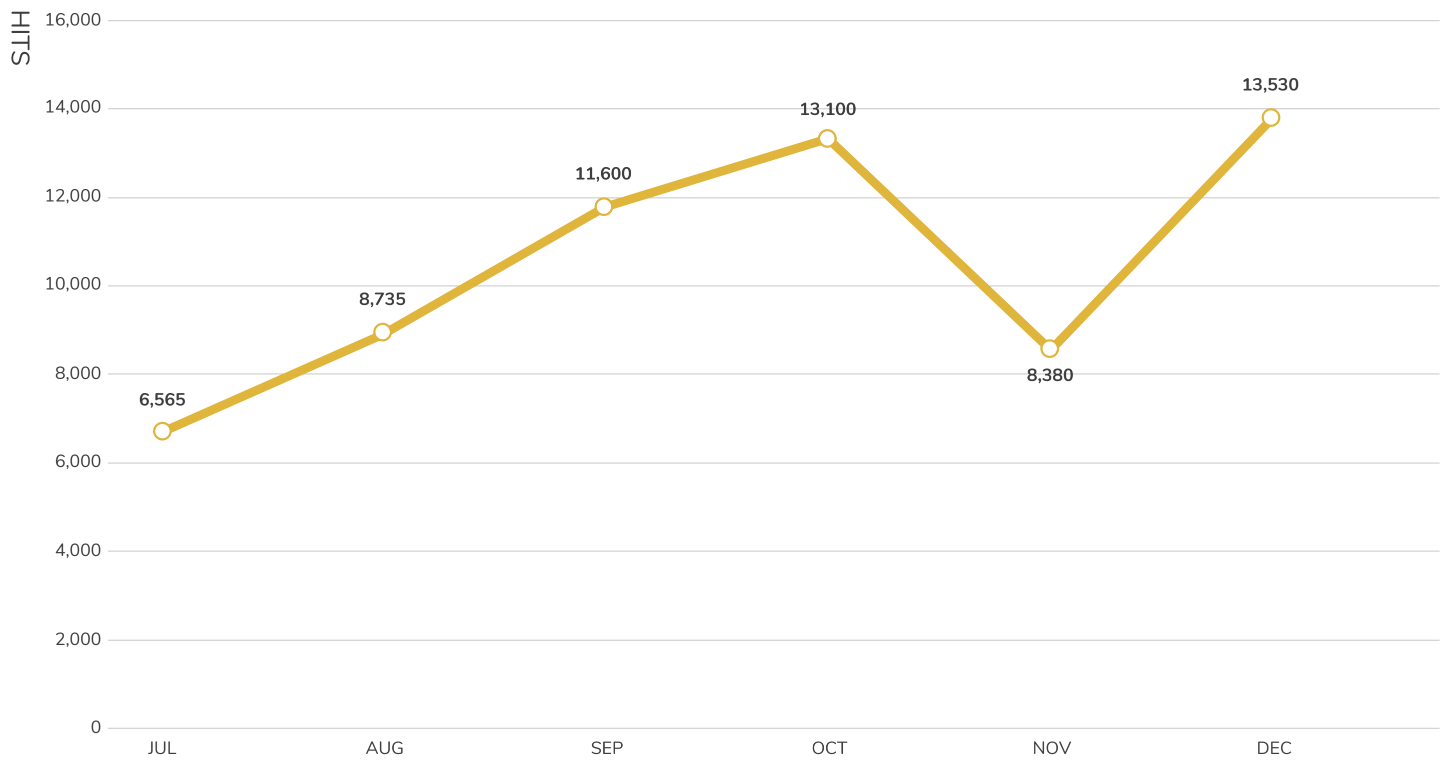
SonicWall Capture Labs threat researchers engineered an advanced method for identifying and mitigating threats through deep memory inspection — all in real time.

SonicWall RTDMI technology detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. 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.

Besides being highly accurate, RTDMI also improves sample analysis time. Since it can detect malicious code or data in memory in real-time during execution, no malicious system behavior is necessary for detection. The presence of malicious code can be identified prior to any malicious behavior taking place, thereby rendering a quicker verdict.

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.

'NEVER-BEFORE-SEEN' ATTACKS DISCOVERED BY RTDMI



RISE & FALL OF CRYPTOJACKING

Cryptomining is a legitimate practice of sourcing cryptocurrency. Comparatively, cryptojacking is the practice of leveraging malware to illegally steal compute power to mine for cryptocurrency.

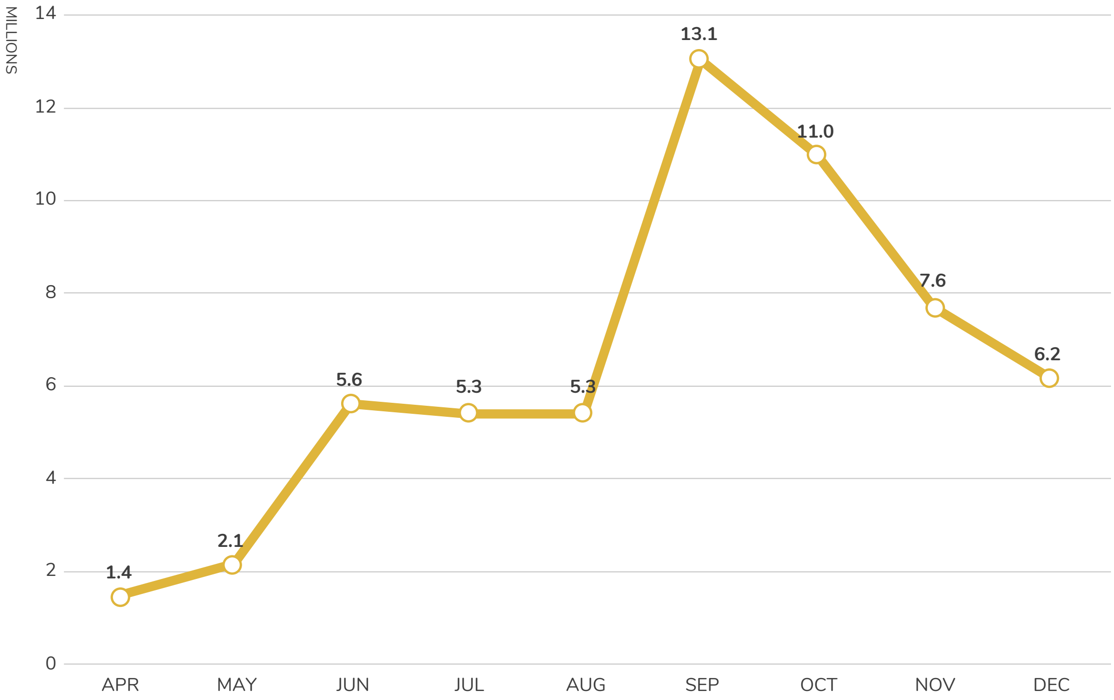
In comparison to more traditional malware, cryptomining attack variants are still in their infancy. While there have been improvements in the cryptomining strains found by SonicWall, security firms are working to create better heuristic defenses against them.

The value of cryptojacking to cybercriminals is, however, dictated by capital expenditures, operating costs and the potential total return on investment — a formula that is directly tied to the price of cryptocurrency. As the price of coins fall, criminals get less return for more work.

That said, in 2018, cryptojacking faded nearly as fast as it appeared. SonicWall recorded **57.5 million cryptojacking attacks** globally between April and December.

> Cryptojacking could soon 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.

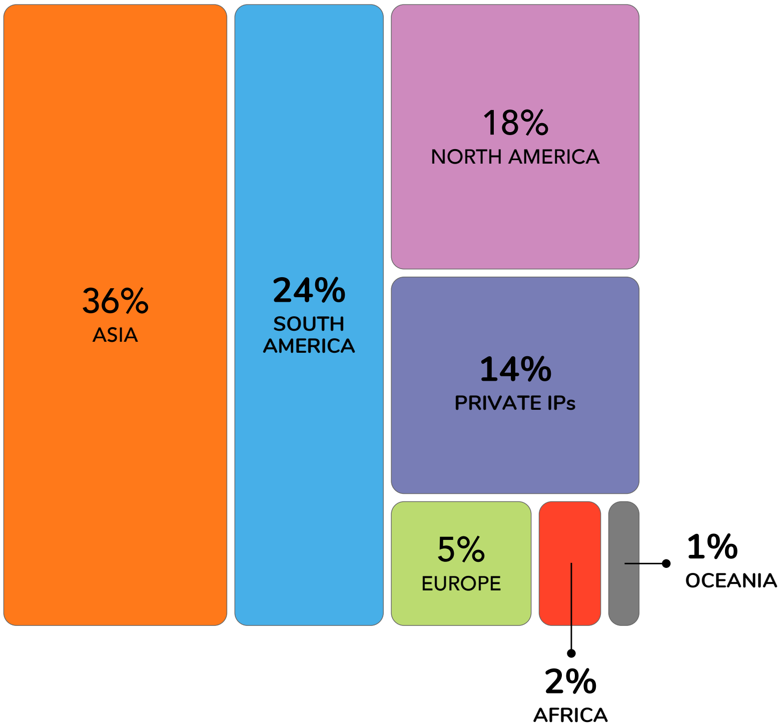
CRYPTOJACKING HITS | APRIL-DECEMBER 2018



Mining for Millions

Cryptojacking attempts peaked at 13.1 million in September 2018 before dropping to close the year. SonicWall believes 2019 will see a sizable surge in new cryptojacking variants and techniques.

2018 CRYPTOJACKING BY REGION



The volume peaked in September, with 13.1 million recorded attacks, but have been on a steady decline since. Despite falling prices, cryptocurrencies remain a valuable commodity to cybercriminals because of their anonymity.

Globally, the signature *Coinhive.JS_2* was the payload of choice for 70 percent of all cryptojacking attempts between April and December. Only *XMRig.XMR_3* (15 percent) was close in total volume.

TOP 10 CRYPTOMINING SIGNATURES

Signature	Hits
Coinhive.JS_2	40,253,927
XMRig.XMR_3	8,600,592
Stak.XMR	3,426,232
XMRig.XMR_5	1,064,258
CoinHive.JS	1,026,108
BitMiner.KJ_2	950,639
Minerd.LC	730,009
XMRig.XMR_4	674,913
Firelce.XMR_2	353,582
XMRig.XMR_6	146,365

The geographic breakdown was relatively balanced. Asia (36 percent), South America (24 percent) and North America (18 percent) saw the most cryptojacking volume during the eight-month span. Another 14 percent of cryptojacking attacks were against unknown or private IP addresses.

More cryptojacking on the way?

The ebb and flow of cryptojacking events in 2018 is curious. While the damage caused by cryptojacking so far is relatively minor, the war has not been won. There's far too much profit to be made with stolen computing power, particularly if cryptocurrency prices rise again.

But the industry is still young and very much in flux. In February 2019, Coinhive publicly announced it was ceasing operations March 8. The service stated that it wasn't "economically viable anymore" and that the "crash" impacted the business severely.

Despite this news, SonicWall predicts there will still be a surge in new cryptojacking variants and techniques to fill the void. Cryptojacking 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.

GLOBAL PHISHING VOLUME DOWN, ATTACKS MORE TARGETED

It’s the attack vector that won’t relent.

Phishing emails were one of the first cybersecurity terms to earn “household” status. And for two good reasons: email is everywhere, and cybercriminals are easily able to fool distracted recipients with even the most rudimentary phishing attempts.

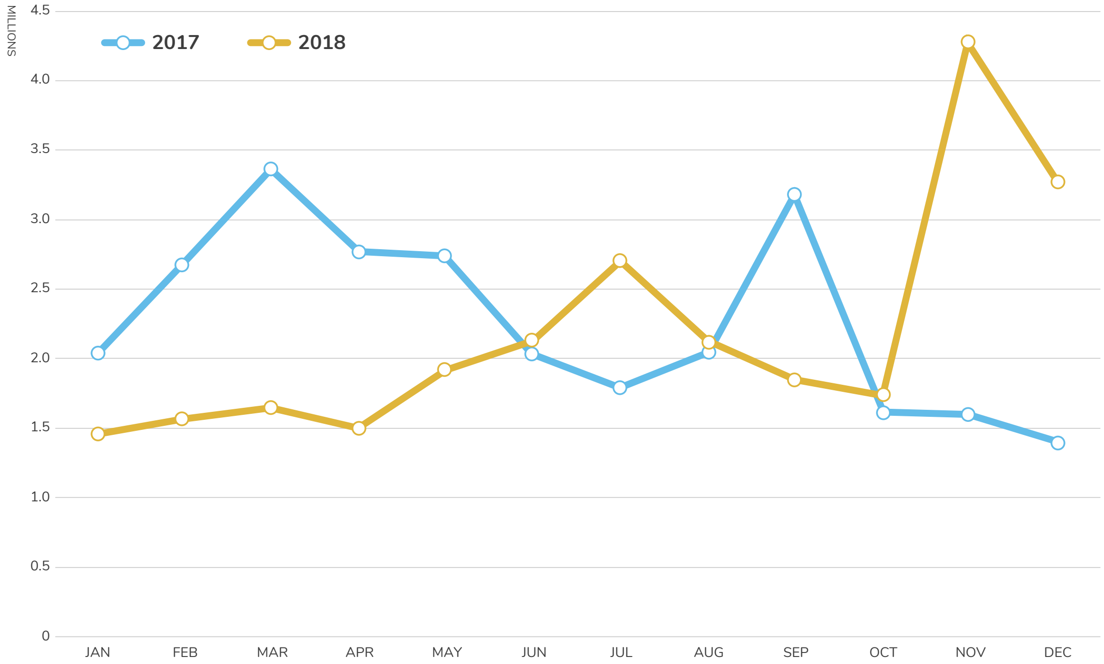
But even as awareness about phishing increased over the years, so did the sophistication of the email attacks themselves. Instead of large, aimless campaigns, cybercriminals launch highly targeted attacks, such as Business Email Compromise (BEC).

Despite these advances, businesses are getting better at blocking phishing attacks and ensuring employees can spot and delete suspicious emails. According to internet security company Cofense (formerly Phishme), organizational susceptibility dropped to 10 percent in 2017 — a 3.3 percent decrease since 2015.

In 2018, SonicWall recorded **26 million phishing attacks worldwide**, a 4.1 percent drop from 2017. During that time, the average SonicWall customer faced 5,488 phishing attacks.

Tactically, cybercriminals shifted behavior in 2018 by selecting how and when they attacked. SonicWall Capture Labs threat researchers observed major email phishing campaigns in June and July, and a spike during the holiday season through November and December 2018. Monthly attack volume differed greatly when compared to 2017.

GLOBAL PHISHING ATTACKS BY MONTH



Holiday Rush

SonicWall’s phishing email data shows major attack campaigns in July, and again during the holiday shopping season starting in November.

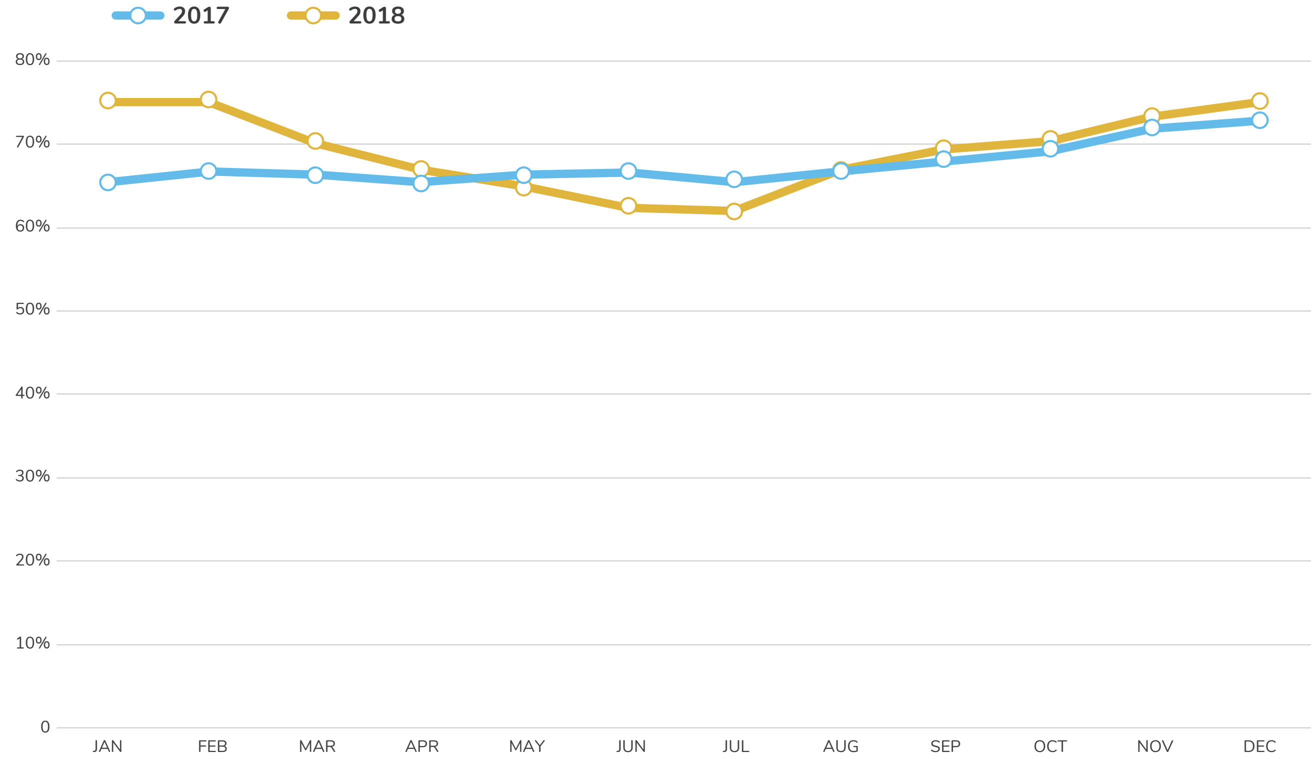
TLS/SSL ENCRYPTION MAINTAINS STEADY GROWTH

The use of transport layer security (TLS) and secure sockets layer (SSL) protocols to encrypt and protect data in transit is a standard for modern internet security.

Once reserved for the most sensitive data (e.g., payment data, transactions, PII, etc.), the encryption standard is mostly commonplace, but some sessions are still unencrypted.

Thankfully, the volume of unencrypted sessions continues to dwindle each year. In 2018, SonicWall found that **69.7 percent of all web sessions used TLS or SSL encryption**, a 2.6 percent bump over 2017.

GROWTH OF HTTPS SESSIONS



RANSOMWARE ATTACKS UP AGAIN GLOBALLY

The up-and-down ransomware story took another turn in 2018.

Despite regional efforts to thwart ransomware attacks, overall global ransomware volume still eclipsed **206.4 million in 2018** — an 11 percent year-over-year increase.

The usual suspects — WannaCry, Cerber and Nemucod — attracted the most attention. The jump can be attributed to the creativity of malware authors, who are yet again mixing and matching components to create new variants, which are harder for traditional, single-layer security controls to identify and block.

According to one report, victims who chose to pay the ransom to receive the decryption keys spent an average of $6,733 per incident during the fourth quarter of 2018.

Linking ransomware to financial impact is difficult, however. Many organizations, particularly larger enterprises, fear damage to their business relationships, reputation or brand. Savvy attackers will demand higher ransoms from larger organizations, further skewing public figures.

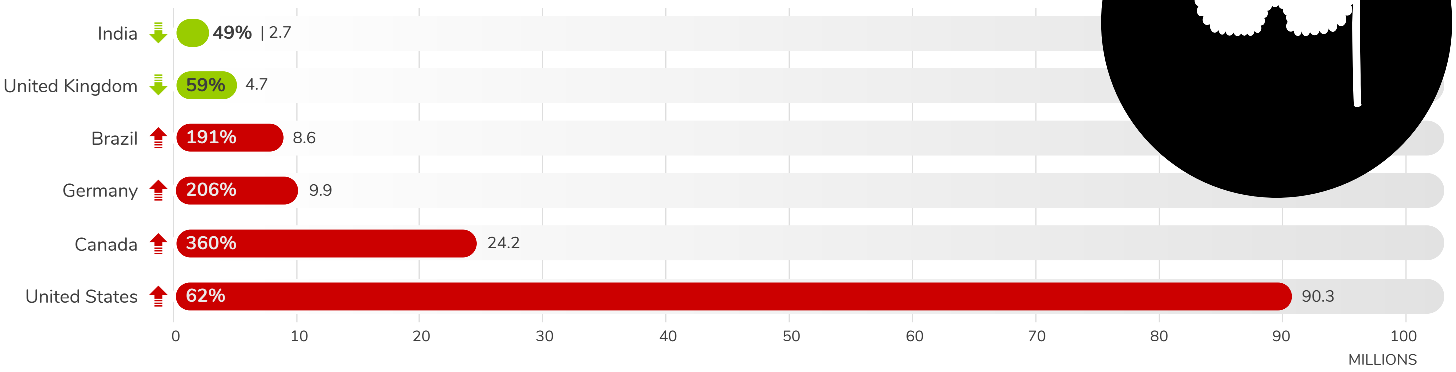
Cloaked for Cash

Like traditional malware, cybercriminals are also cloaking more ransomware. The infamous Cerber and Nemucod topped SonicWall's list of most-encrypted ransomware.

ENCRYPTED RANSOMWARE

Name	Hits
JScript.Nemucod.BZN	8,927
Cerber.FLFJ	5,698
JScript.Nemucod.RJ_2	315
Locky.VBS_2	310
JScript.Nemucod.AW_10	241
Nemucod.KM	239
PDFDropper.RSM_7	178
Cerber.RSM	160
Cerber.G_5	142
JScript.Nemucod.J	142

2018 RANSOMWARE ATTACKS | TOP GLOBAL COUNTRIES



Top 10 ranking for ransomware data based on number of SonicWall customers globally.

Shifting strategies focusing on regional targets

As outlined in an earlier section, ransomware dropped in some specific regions (e.g., U.K. and India), but overall volume was up slightly globally. The U.S. (90.3 million) and Canada (24.2 million) were victimized the most by ransomware in 2018, followed only by Germany (9.9 million), which suffered a 206 percent year-over-year increase.

Dollars over coins

In the fall of 2017, cryptocurrency prices were at an all-time high. This surge — and media attention — drew the eyes of many cybercriminals who wanted in on digital coins, specifically *bitcoin*. And they chose ransomware as their means to a payday.

A year later, bitcoin prices are down 80-90 percent. In response, cybercriminals began asking for specific dollar amounts of bitcoin, rather than a static number (i.e., '$6,000 of bitcoin' versus 'two bitcoins'). Despite drastic price fluctuations, criminal groups still prefer the anonymity of cryptocurrency.

Increase in ransomware kits, service offerings

Ransomware authors and criminal networks are diversifying their go-to-market tactics, too. Ransomware-as-a-Service (RaaS) offerings continue to make it easier for any ill-meaning person to compromise devices or networks for money.

RaaS packages can usually be purchased for less than $500 — making the malware lucrative for both operators and attackers. Even a single ransom payout can offer more than 100 percent return on investment for an attacker. The service operators can maintain a low-risk position and, in some models, receive a portion of the ransom payout.

Construction kits removing technical entry barriers

Don't want to pay for a ransomware service? Do-it-yourself construction kits are empowering novice "hackers" and criminals to build ransomware variants with little to no programing experience.

One such example is Xorist, a creative ransomware construction kit that helps criminals configure various features such as message text, file extension of encrypted files, encryption algorithm and unlock passwords.

In June 2018, attackers were charging around 0.8 bitcoin for file recovery — but as Capture Labs threat researchers discovered, everything is negotiable.

Make It Yours

Xorist Customization Options

- File extensions to target for encryption
- File extension text to append to encrypted files
- Decryption password
- Wallpaper to show on desktop background
- Icon for the malware executable file
- Autorun at startup
- Encryption algorithm to use (XOR/TEA)
- Ransom note text
- File recovery password attempts
- UPX file packing

Fake ransomware preying on novice victims

Ransomware often hits the desktop of a random user with an unknown skillset. In many cases, the person isn't technically savvy enough to understand encryption or how their files are "locked."

To reduce operating costs, cybercriminals decided it was easier to simply fake a ransomware attack and demand files that were "encrypted" even though they weren't. Attackers are banking on the victim not knowing the difference — and in many cases, they're right.

SonicWall has been monitoring, analyzing and blocking a number of fake ransomware variants. In one case, the "ransomware" simply overwrites the Master Boot Record (MBR) and demands payment. No files are actually encrypted and there is no encryption functionality present in the malware.

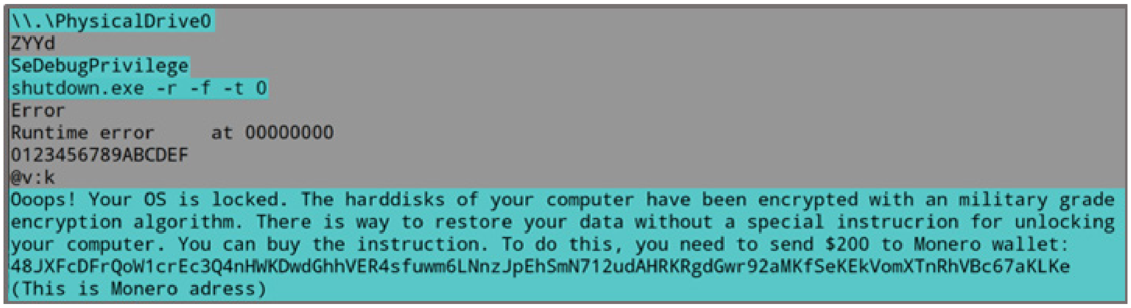
Although files can easily be restored by mounting the filesystem using a live operating system booted via a memory stick, most users will likely consider their files gone and perform a full reinstall. Interestingly, no contact information was provided to "restore" the files and there was no way of verifying if paying the $200 in Monero cryptocurrency would resolve the issue.

SonicWall Capture Labs threat researchers also caught and studied a fake ransomware Trojan that functions as a bootlocker. It is named Uselessdisk because of the debugging symbols and project name strings that the developer left in the executable file.

The attacker's three-part plan is simple. First, render the system unbootable. Second, pretend that files on the system have been encrypted. Finally, ask for bitcoin for file recovery. Fortunately, this particularly variant wasn't successful. The bitcoin address received no transactions almost a year after first analyzed.

Fake Ransomware

In this example, the attacker made no effort to hide the functionality of the fake ransomware. The malware was written in Delphi and is so straightforward that even a simple listing of strings in the binary instantly revealed its motive.



```
\\.\PhysicalDrive0
ZYYd
SeDebugPrivilege
shutdown.exe -r -f -t 0
Error
Runtime error     at 00000000
0123456789ABCDEF
@v:k
Ooops! Your OS is locked. The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is way to restore your data without a special instrucrion for unlocking
your computer. You can buy the instruction. To do this, you need to send $200 to Monero wallet:
48JXFcDFrQoW1crEc3Q4nHWKDwdGhhVER4sfuwm6LNnzJpEhSmN712udAHRKRgdGwr92aMKfSeKEkVomXTnRhVBc67aKLKe
(This is Monero adress)
```

MALICIOUS PDF & OFFICE FILES BEATING LEGACY SECURITY CONTROLS

Everyday files are being weaponized. And more are on the way.

You've always trusted '*Confidential_Payroll_Salary_Adjustments.xlxs.*' It's a file type from an application that has your full, unwavering confidence. It presents itself as official and important business. And, in many cases, it was sent as an attachment by someone you trust.

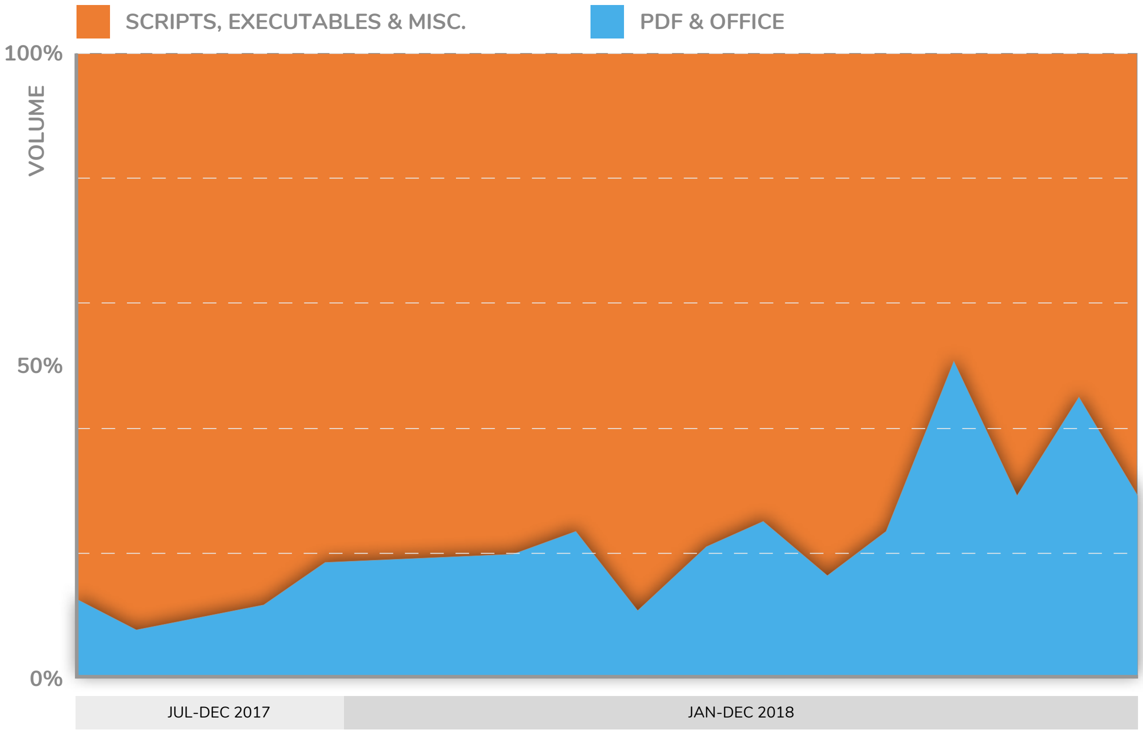
The modern cybercriminal is banking on your past experiences that one of the above reasons will coerce you into opening a seemingly benign file. And if those tricks aren't effective, human curiosity is always a handy catch-all.

But these file types — typically PDFs and Office files (e.g., Word, Excel, PowerPoint, etc.) — are now used as effective delivery mechanisms to circumvent traditional firewalls and single-engine sandboxes to deliver malware payloads.

Of the 391,689 new attack variants Capture ATP discovered in 2018, 47,073 were new PDF attacks and another 50,817 were new Office file attacks. While volume appears low, most security controls cannot identify and mitigate malware hidden in these file types, greatly increasing the success of the malware.

As the below graphic illustrates, the use of PDFs and Office files to hide malware is gradually taking over traditional delivery options like scripts, executables and other miscellaneous files types.

INCREASE IN MALICIOUS PDFS & OFFICE FILES



In the last half of 2017, **PDFs and Office files were used in 13 percent of new attack variants** discovered by Capture ATP. In the last half of 2018, that average jumped to 34 percent and continues to climb.

Like the ever-present ‘malware cocktail,’ cybercriminals continue to test new and innovative methods for delivering payloads. Leveraging users’ trust in PDF and Office files is further exploiting human behavior toward specific types of files.

Threatening Office & PDF vulnerabilities investigated

In late 2017 and through 2018, the Microsoft Equation Editor vulnerability (CVE-2017-11882) exploited Office documents (e.g., *.xls*, *.doc*, *.rtf*) to deliver malicious payloads, such as Lokibot, Formbook, Pony and Zeus. The exploit also leveraged advanced obfuscation techniques adapted in Microsoft VB macros to evade signature-based detection.

Using Visual Basic for Applications (VBA), macros are also embedded in Word or Excel documents to deliver fileless malware (PowerShell script). Once inside the environment, these scripts then covertly download the malicious payload to execute a given attack.

NEW OFFICE VULNERABILITIES

Description	CVE ID
Microsoft Office OLE Interface	CVE-2017-0199, CVE-2017-8570
Microsoft Equation Editor	CVE-2017-11882, CVE-2018-0802
Microsoft VB Script Engine	CVE-2018-8174
Microsoft .NET Framework Process	CVE-2017-8759
Microsoft Win32k Privilege Elevation	CVE-2018-8120
Microsoft Windows Shell Remote Code Execution	CVE-2018-8414

NEW PDF VULNERABILITIES

Description	CVE ID
Remote-Code Execution	CVE-2018-4990
New Technology LAN Manager (NTLM) Theft	CVE-2018-4993
Adobe Flash Player 31.0.0.153 & Earlier; 31.0.0.108 & Earlier	CVE-2018-15982
Adobe Flash Player 28.0.0.161 & Earlier	CVE-2018-4878

NON-STANDARD PORTS RIPE FOR EXPLOITATION

In networking, a port helps complete the destination or origination network address of a message.

It is always associated with a host IP address and the protocol type of the communication, for example TCP and UDP.

The lowest numbered 1024 port numbers are called the 'well-known' port numbers. The Internet Assigned Numbers Authority (IANA) is responsible for maintaining the official assignments of port numbers for specific uses.

A 'non-standard' port means a service 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, so they are where most firewalls focus their protection. In response, cybercriminals are targeting non-standard ports to help ensure their payloads can be deployed undetected in a target environment.

SonicWall Capture Labs threat researchers observed high volumes of non-standard port traffic used by malware. SonicWall recorded an increase in both HTTP and HTTPS traffic through ports other than 80 and 443, as well as FTP traffic on ports other than 20, 21 and 22.

Based on a sampling of more than 700 million malware attacks, SonicWall found that an average of **19.2 percent of all malware attacks came across non-standard ports** in 2018, an 8.7 percent year-over-year increase.

Organizations aren't protecting this attack vector with the same diligence as standard ports. Because there are so many to monitor, traditional proxy-based firewalls can't mitigate attacks over non-standard ports (for both encrypted and non-encrypted traffic).

ATTACKS AGAINST TOP 15 NON-STANDARD PORTS

Port	Hits
8014	9,467,542
8020	6,040,242
8080	5,386,333
81	1,867,724
8059	485,150
8220	480,561
9080	412,734
8081	301,631
9909	262,350
10083	246,783
3060	207,489
443	168,457
3128	143,941
16450	142,142
182	113,666

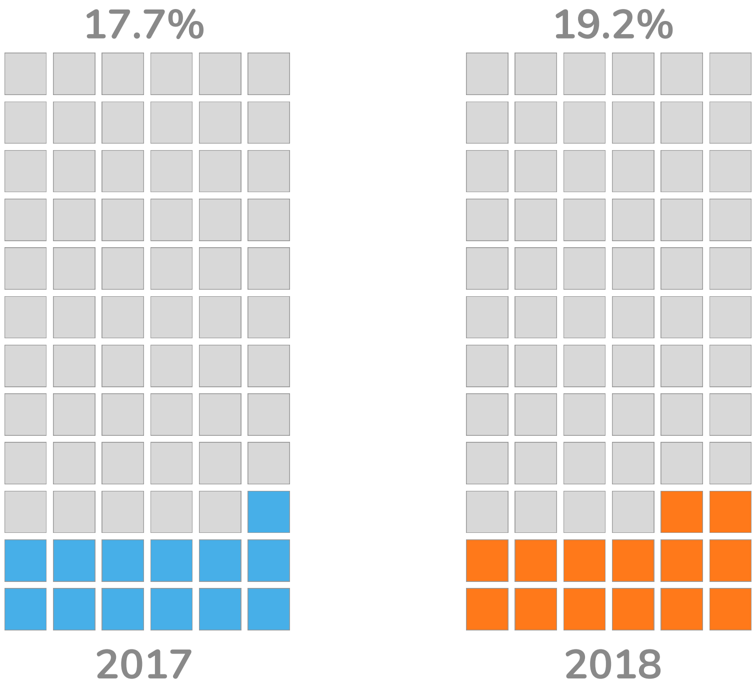
In January 2017, 6 percent of malware was coming across non-standard ports. By December 2018, that average rapidly jumped to 23 percent.

Security-conscious organizations should implement layered security solutions that identify and block attacks on all ports, not just 80, 443 and other common entry points.

The best way to monitor this many ports is by deploying firewalls that can analyze specific artifacts instead of all traffic (i.e., proxy-based approach). This helps ensure attacks over non-standard ports are mitigated quickly without affecting performance.

TOP 10 ATTACK SIGNATURES ON NON-STANDARD PORTS

Signature	Hits
Suspicious#polycrypt.13	3,295,326
KingSoft.D_10	312,592
EncPk.ACO_48	270,092
Downloader.Banload-1789	246,043
Cerber.EA	200,069
Suspicious#polycrypt.1_2	183,378
KeyLogger.OCI_2	165,445
Skeeyah.AN_4	153,124
Virlock.A_677	152,880
Generic.Shellcode.7	94,655



Unguarded Doors

19.2 percent of all malware attacks came across non-standard ports in 2018, an 8.7 percent year-over-year increase.

IOT ATTACKS ESCALATING

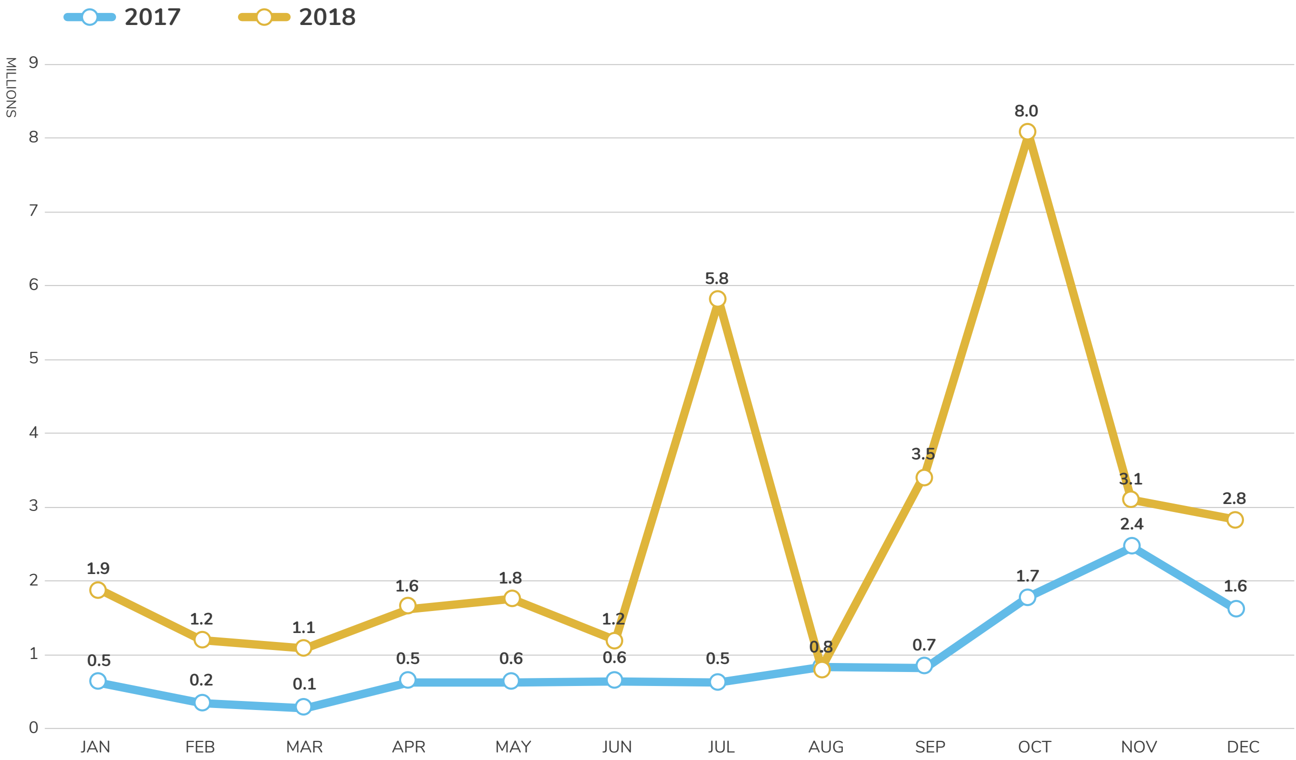
The speed at which Internet of Things (IoT) devices are blanketing homes, offices and public spaces is impacting cybersecurity and network defenses.

Consumers are hungry for connected devices. It's estimated that more than 31 billion IoT devices will be installed by 2020. But this appetite has resulted in a deluge of IoT devices rushed to market without proper security controls. In many cases, IoT devices are set up with out-of-the-box security settings, making them easy to compromise via default credentials or powerful botnets.

During the last 18 months, cybercriminals have capitalized on this apathy. The IoT landscape is so encompassing — everything from cars, routers, appliances, baby monitors, vacuums and medical equipment are connected — that it's far too late to level-set without standardized guidance or policy

All told, SonicWall recorded **32.7 million IoT attacks in 2018**, a 217.5 percent increase over the 10.3 million IoT attacks the company logged in 2017.

IoT ATTACK VOLUME | YEAR-OVER-YEAR COMPARISON



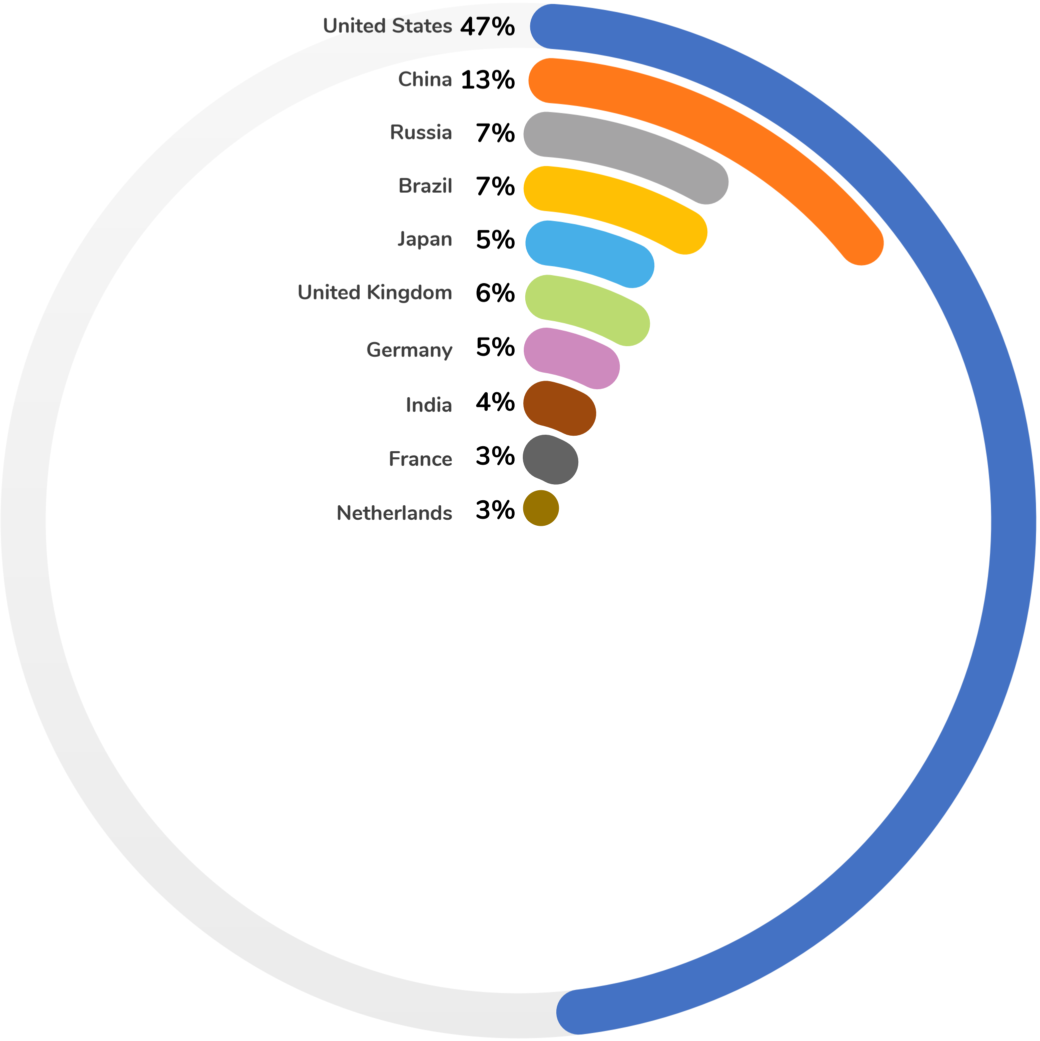
Majority of botnets hosted in the U.S.

In many cases, IoT devices are compromised via carefully crafted botnets. A botnet is a collection of internet-connected devices or computers, each of which is running one or more “bots” that execute a given task.

Botnets can be used to perform distributed denial-of-service (DDoS) attacks, steal data, send spam, or allow an attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. More than 46 percent of global botnets originated from U.S.-based IP addresses. The next closest was China at 13 percent.

To combat unwanted traffic, proactive organizations employ content filter controls to block unwanted or malicious traffic from certain IPs, origin countries or domains about certain topics.

TOP 10 COUNTRIES HOSTING BOTNETS



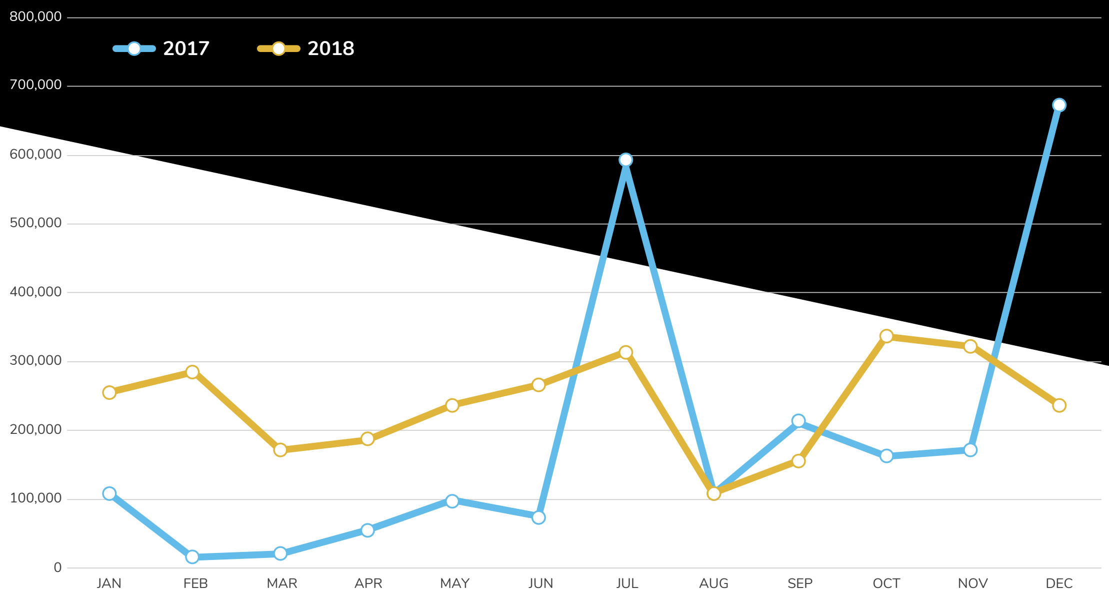
ENCRYPTED ATTACKS GROWING STEADY

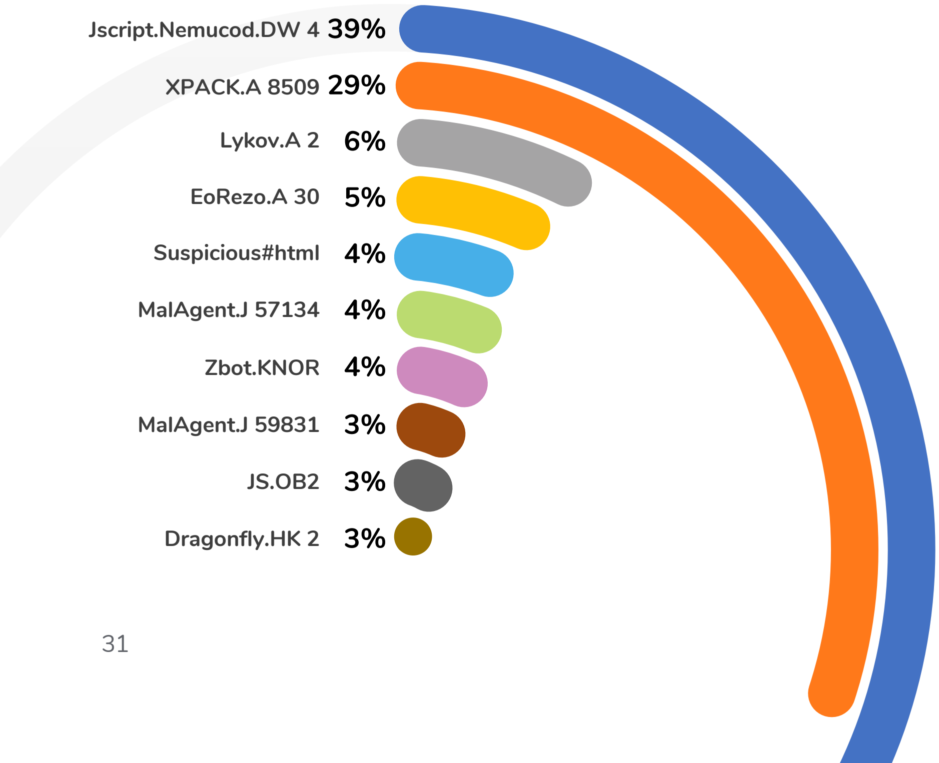
For all the benefits that transport layer security (TLS) and secure sockets layer (SSL) provide to help secure web sessions and internet communication, the same encryption can be used for malicious activity, too.

In March 2012, Google announced its intention to switch to HTTPS by default. Since then, SonicWall has recorded consistent increases of HTTPS sessions. It was the right decision. However, cybercriminals are following this trend to protect their payloads.

In fact, the growth in encrypted traffic is coinciding with more attacks being cloaked by TLS/SSL encryption. More than **2.8 million attacks were encrypted in 2018** — a 27 percent increase from the previous year.

ENCRYPTED MALWARE ATTACKS





TOP 10 ENCRYPTED MALWARE

With 471,415 total signature hits, the infamous Nemucod topped SonicWall's list of encrypted malware in 2018. It and XPACK.A 8509 (353,544 hits) made up 68 percent of all encrypted malware for the year.

SONICWALL'S 2019 CYBERSECURITY PREDICTIONS

Ransomware Back for More
Attackers will continue to accelerate the use of ransomware throughout 2019. Attacks will become even more targeted, especially against large organizations or regions not as quick to adopt security protections. More ransomware-as-a-service (RaaS) offerings and ransomware construction kits will contribute to this increase, particularly as an easy tool for novice or low-skilled criminals.

Cybercriminals Double-Down on Attacks Using PDFs & Office Files
This is just the beginning. Cybercriminals are weaponizing PDFs and Office files to hide their malware payloads. Since SonicWall began monitoring this attack strategy, volume has consistently shifted away from traditional scripts and executables. Expect more attacks to defeat network defenses in this manner.

First Malware Weaponized Against Processor Vulnerability
Based on how fast nation-states weaponized malware via Eternal Blue vulnerabilities in the last 12-18 months, it is likely we will see the first cyberattack against a known — or worse, unknown — processor vulnerability like Spectre, Meltdown, PortSmash, Foreshadow or Spoiler.

Hackers Turn AI Against Industry
Machine learning and artificial intelligence (AI) are helping the security industry automate cyber defenses that react and evolve with more agility. This year, malware writers will do the same. These technologies will be leveraged by cybercriminals to better understand detection techniques and, in response, create advanced malware strains that defeat security mechanisms by persistently changing malware's static and dynamic components.

More Attacks Against Wearables & "Smart" Devices
Due to the high penetration of wearables and "smart" devices like televisions and appliances, expect to see an uptick in malicious attacks against this vector in 2019. The fact that so many devices connect with one another in a single home or office highlights the extent to which malicious actors can infiltrate personal or businesses spaces and cause unimaginable damage.

Malware Traffic Shifts to Non-Standard Ports
More malware via non-standard port traffic will be seen in the coming year. Proactive organizations will begin implementing stricter parameters to monitor and mitigate attacks that come across non-standard ports.

Another Rise in Cryptojacking Attacks
Despite decreasing volume in late 2018, cryptojacking will continue to be popular in 2019. More malware authors will focus their efforts on money-making opportunities where cryptocurrency is prevalent. This may include extortion, such as with ransomware, or creatively bundling nefarious cryptomining programs (i.e., mixing old with new) to stay ahead of the security industry. More connected devices, including smartphones, provide fertile processing power to harvest for malicious gain.

PAIRING ACTIONABLE THREAT INTELLIGENCE WITH LAYERED SECURITY

Threat intelligence is only a single tool in your kit. Cyber threat data must be used to shape and define the security decisions your organization makes at micro and macro levels.

To be useful, actionable cyber intelligence must be paired with real-world technology and tactfully applied to decide which security layers to focus on based on your organization's budget, expertise, security objectives and business goals.

The following best practices help organizations understand which security layer is appropriate to solve a specific challenge. In many cases, they are complementary and overlapping by design.

Perimeter Security

Next-generation firewalls (NGFW) are extremely effective at stopping the majority of known cyberattacks and should be one of the cornerstones of any sound security strategy. Proven firewalls offer a range of security services, including cloud sandboxing, gateway antivirus (GAV), intrusion prevention services (IPS), content filtering, application controls, anti-spam features, protection for non-standard ports and TLS/SSL inspection options.

TLS/SSL Decryption & Inspection

As data in this report has shown, cybercriminals hide their attacks within encrypted TLS/SSL sessions. This makes it easier to sneak malware by traditional network defenses to infiltrate networks and damage your business. SonicWall provides solutions to responsibly decrypt, inspect and re-encrypt TLS and SSL traffic. The solution that's right for your business will depend on specific performance, deployment, budget and security objectives.

Email Security

The omnipresence of spam and phishing attacks makes email security a necessity. Secure email solutions help businesses defend against email-based threats, including malware, ransomware, zero-day threats, spear-phishing and BEC. Regardless if deployed on-premise or in the cloud, email security is a critical component to proactive layered security.

Multi-Engine Sandboxing

Cloud or networking sandboxing services offer real-time inspection of suspicious files that firewalls can't check against a known signature, particularly for mitigating never-before-seen threats that are able to circumvent standard security controls. The multi-engine SonicWall Capture ATP sandbox can quarantine suspicious files until a decision is determined, greatly reducing the chance of breach or infection.

Cloud Application Security & Management

Monitor, manage and protect the sanctioned and unsanctioned use of cloud-based resources and SaaS applications, including Microsoft Office 365 and G Suite. Sometimes known as Cloud Application Security Broker (CASB), these solutions help protect email, data and user credentials from advanced threats while ensuring compliance in the cloud. Advanced offerings will empower IT departments to roll out SaaS applications without compromising security or compliance. Administrators should be able to set consistent policies across all the SaaS applications deployed within the organization from a unified console or management dashboard.

Advanced Memory & Side-Channel Inspection

New side-channel threats, like Spectre, Meltdown, Foreshadow, PortSmash and Spoiler, are moving the cyber war to an entirely new theater. SonicWall RTDMI identifies and stops malicious PDFs and Office files, but also defends against advanced processor-based attacks. Working in parallel of the Capture ATP sandbox, RTDMI detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via custom encryption.

Endpoint Protection

Actively defend your endpoint footprint (e.g., laptops, mobile devices, etc.) with next-generation antivirus (NGAV) solutions or an endpoint protection platform (EPP). Endpoint protection solutions help organizations mitigate successful cyberattacks that compromise an endpoint, ensuring malware or ransomware can't systemically infect your entire organization.

Two-Factor Authentication

A common best practice among most organizations, multifactor authentication provides safeguards to protect against the misuse of credentials to illegally access networks, systems or software services. Strong authentication checks the validity of a user's credential by challenging them with something they are (e.g., biometrics), something they know (e.g., password) or something they have (e.g., one-time passcode, mobile tokens/approvals).

Policy, Compliance & Enforcement

Technology controls aren't effective without the consistent use of policy and the means to enforce them. Users remain the weakest link in an organization's security posture, so building a culture of awareness — underpinned and supported by policies and compliance standards — unifies the security fabric of your organization.

The Cyber Arms Race Doesn’t End Here

For more exclusive cyber threat intelligence, visit SonicWall.com/ThreatReport.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products.

EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

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.

ABOUT SONICWALL

SonicWall has been fighting the cybercriminal industry for over 27 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.

www.SonicWall.com

SONICWALL®