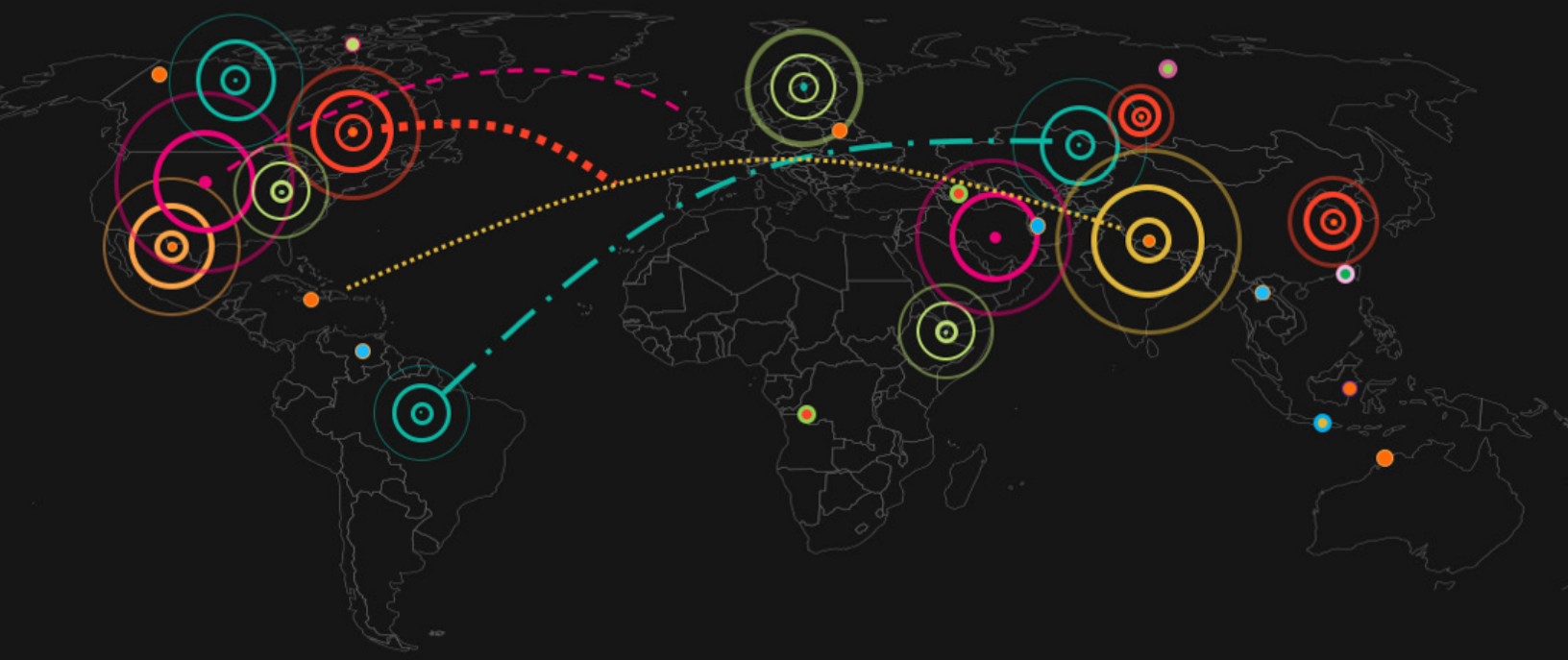
2018 SONICWALL CYBER THREAT REPORT

Threat Intelligence, Industry Analysis and Cybersecurity Guidance for the Global Cyber Arms Race



sonicwall.com | @sonicwall

SONICWALL®

TABLE OF CONTENTS

MALWARE ATTACKS BOUNCE BACK

Advance and retreat. Flank and charge. Ambush and assault.

The modern cyberwar — against governments, businesses and individuals alike — is comprised of a series of attacks, counterattacks and respective defensive countermeasures. Many are simple and effective. Others are targeted and complex. Yet they are all highly dynamic and require persistence, commitment and resources to mitigate. And they will not go away.

Unfortunately, organizations large and small are caught in the middle of a global cyber arms race with vastly different resources at their disposal. And while growing budgets do make a positive impact on the effectiveness against known exploits, the threat landscape evolves at such a rate that yesterday's investment in technology could already be insufficient to deal with tomorrow's cyber threats.

All told, there were more than 12,500 new Common Vulnerabilities and Exposures (CVE) reported in 2017 — 78 percent of which were related to network attacks.

No one has immunity.

Headline breaches — Last year was another record-breaker for data breaches. In 2017, the Equifax breach[i] leaked the personal information of approximately 143 million individuals (44 percent of the U.S. population); the NSA leak of multiple exploits was widely used by popular ransomware; and 57 million Uber accounts were released from a 2016 data breach.

Ransomware is retooling — With WannaCry, Petya and Bad Rabbit all becoming headline news, ransomware was a hot topic for the second year in a row. SonicWall Capture Labs threat researchers found that while attackers didn't push the same volume as they did in 2016, the number of variants jumped considerably.

SonicWall Capture Labs detected **184 million ransomware attacks** in 2017 compared to 638 million in 2016. However, there was also a corresponding **101.2 percent increase in new ransomware variants** — a key indicator that attack strategies are shifting.

Attack volumes on the rise — While ransomware volume took a substantial dip, other malware attacks jumped significantly in 2017. All told, SonicWall logged **9.32 billion** attacks — an 18.4 percent increase over 2016.

The battle within encrypted traffic — Encryption was leveraged more than previous years, for both legitimate traffic and malicious payload delivery. Based on data from a subset of SonicWall firewalls using DPI-SSL, an average of 4.2 percent of all file-based malware propagation attempts used SSL/TLS encryption.

SonicWall Capture Labs found, on average, 60 file-based malware propagation attempts per SonicWall firewall each day. Without the ability to inspect encrypted traffic, the average organization would have **missed over 900 attacks per year hidden by SSL/TLS encryption**.

> For the first time ever, SonicWall provides empirical data on the volume of attacks leveraging SSL/TLS encryption.

THIS IS A CHALLENGE WE FACE TOGETHER.

And it's the core reason we're committed to passing our findings, intelligence, analysis and research to the global public via the SonicWall 2018 Cyber Threat Report.

Memory attacks — While the Meltdown and Spectre vulnerabilities were first disclosed to the public in early 2018, the processor vulnerabilities were actually discovered last year.[ii] In fact, Intel notified Chinese technology companies of the vulnerability before alerting the U.S. government.[iii]

Threat actors and cybercriminals are already leveraging memory as an attack vector. Since these memory-based attacks are using proprietary encryption methods that can't be decrypted, organizations must quickly detect, capture and track these attacks once they're exposed in memory — usually in under 100 nanoseconds. Chip-based attacks will be at the forefront of the cyber arms race for some time to come.

IoT threats looming — The Internet of Things (IoT) was also a big target, demonstrated by the new IoT Reaper botnet that borrows code from 2016's first IoT open-source botnet, Mirai. IoT devices will be in the crosshairs in 2018, as "smart" hardware is not updated regularly and is often physically located in unknown or hard-to-reach places.

Cyberattacks the top business risk — Data breaches and cyberattacks are no longer back-of-mind concerns. To the modern executive, they represent the No. 1 risk to business, brand, operations and financials. So much so, Lloyd's of London, one of the world's oldest and premier specialty insurance markets, now considers cyberattacks an even bigger threat than catastrophic natural disasters.

"There are substantial insurance gaps, as a majority of cyber risks are not covered by any form of insurance," Lloyd's of London CEO Inga Beale said on a panel during the January 2018 Asian Financial Forum in Hong Kong. "Just like natural catastrophes, cyber events such as hacker attacks or internet failures can cause severe impact on businesses and economies." [iv]

SonicWall president and CEO Bill Conner expounded on the growing risk and how it's affecting the outlook and exposure for businesses.

"Governments, enterprises and individuals are in the crosshairs of a global cyber arms race," Conner said. "The risks to business, privacy and related data grow by the day — so much so that cybersecurity is outranking some of the more traditional business risks and concerns."

This position is supported by the World Economic Forum (WEF) Global Risks Report 2018,[v] which found that many of the unexpected costs from 2017 came from cyberattacks.

"The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64 percent of all malicious emails," noted the report.

See Real-Time Attack Data

What attacks are happening right now? Visit the SonicWall Security Center to see the latest attack trends, types and volume across the world.

VISIT THE SECURITY CENTER

KEY FINDINGS FROM 2017

Security Industry Advances

Total ransomware attack volume declines. Full-year data shows that ransomware attacks dropped from **638 million to 184 million** between 2016 and 2017.

SSL/TLS use increases again. Traffic encrypted by SSL/TLS standards increased 24 percent and represented 68 percent of total sessions in 2017.

Effectiveness of exploit kits impacted. With most browsers dropping support of Adobe Flash, no critical Flash vulnerabilities were discovered in 2017. Cybercriminals are having to work harder to find new vectors for leveraging exploit kits.

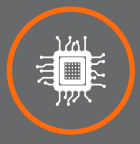
Law enforcement turns the tide. Key arrests of cybercriminals continued to help disrupt malware supply chains and impact the rise of new would-be hackers and authors.

Cybercriminal Advances

More unique types of ransomware found in the wild. While the total volume of ransomware attacks was down significantly year over year, the number of ransomware variants in play increased **101.2 percent** in 2017. SonicWall Capture Labs threat researchers created 2,855 new unique ransomware signatures for the year.

Encryption still cloaking cyberattacks. Without the ability to inspect encrypted traffic, the average organization would have missed over 900 file-based attacks per year hidden by SSL/TLS encryption.

Malware cocktails mixing things up. While no single exploit rose to the level of Angler or Neutrino in 2016, there were plenty of malware writers leveraging one another's code and mixing them to form new malware, thus putting a strain on signature-only security controls.



IoT and chip processors are emerging battlegrounds. Cybercriminals are pushing new attack techniques into advanced technology spaces, notably the Internet of Things (IoT) and chip processors.

About the SonicWall Capture Labs Threat Network

Data for the 2018 SonicWall Cyber Threat Report was gathered by the SonicWall Capture Labs Threat Network, which sources information from global devices and resources including:

- More than 1 million security sensors in nearly 200 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 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
- Intelligence from freelance security researchers

Capture Network

1 MILLION +
Sensors

200 +
Countries & Territories

24 x 7 x 365
Monitoring

<24 HOURS
Response to Zero-Day Vulnerabilities

200K +
Malware Samples Collected Daily

200K +
Malicious Events Analyzed Daily

SONICWALL®

TOTAL RANSOMWARE VOLUME DECLINES

If ransomware's global impact was the major headline in 2016, its sharp decline in 2017 is just as intriguing. Even with WannaCry, Petya, NotPetya and Bad Rabbit stealing the headlines, the expectations of more ransomware attacks in 2017 simply did not materialize as anticipated.

The SonicWall Capture Threat Network detected **183.6 million ransomware attacks in 2017.** This marked a **71.2 percent drop** from the 638 million ransomware attack events SonicWall recorded in 2016.

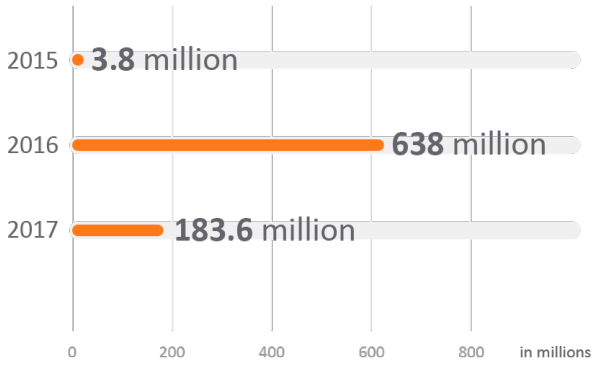
Regionally, the Americas were victimized the most, receiving 46 percent of all ransomware attack attempts in 2017. Europe saw 38 percent of ransomware attacks during that same time.

Even with a decline in volume, the multi-engine SonicWall Capture Advanced Threat Protection (ATP) sandbox was responsible for identifying one new malware variant for every 250 unknown hits.

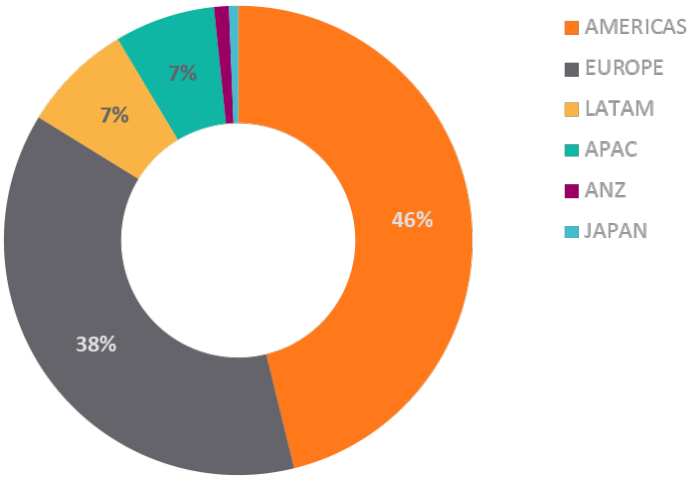
Capture ATP is currently deployed at more than 30,000 organizations around the world and identifies almost 500 new malicious files each day.

SonicWall Capture ATP is automatically identifying almost 500 new malicious files each day.

Ransomware Trend (total hits in millions)



Total Ransomware Hit Locations



SONICWALL®

By analyzing bitcoin data — the preferred currency of threat actors and cybercriminals — SonicWall researchers found that transactions via ransomware-related wallet addresses dropped in 2017.

Many organizations are also better informed and more prepared for ransomware attacks. Proactive organizations are not only building sound disaster recovery and business continuity strategies, they're also hoarding bitcoin stockpiles — ideally when prices are lowest — as a last resort to keep business running.[vi]

Top Ransomware in 2017

WannaCry

The ransomware attack hit over 150 countries across the world with an untold number of victims. WannaCry is a combination of a Trojan/ransomware and a worm. It leverages an SMB file-sharing protocol exploit named EternalBlue, which was part of the April 2017 Shadow Brokers leak of NSA-developed exploits.

Petya & NotPetya

SonicWall Capture Labs identified the original Petya variants in 2016. However, a new variant in 2017 called NotPetya drilled into networks with a worm exploiting the EternalBlue vulnerability, much like WannaCry. Systems infected with NotPetya displayed a flashing skull, followed by a lock screen, before seeking payment for encrypted data.

Bad Rabbit

First appearing in Russia and the Ukraine, Bad Rabbit ransomware was installed by masquerading as an Adobe Flash update for local execution. Interestingly, the malware contained a list of hard-coded Microsoft Windows credentials, most likely to enable brute-force entry into devices on the network.

Cerber

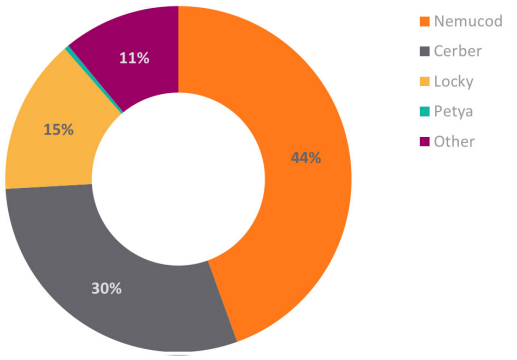
Like Petya, Cerber first appeared in 2016. It wasn't until 2017, however, when multiple variants of the ransomware were appearing daily. It was thought to be linked to Russian ransomware-as-a-service (RaaS) sources.

Nemucod

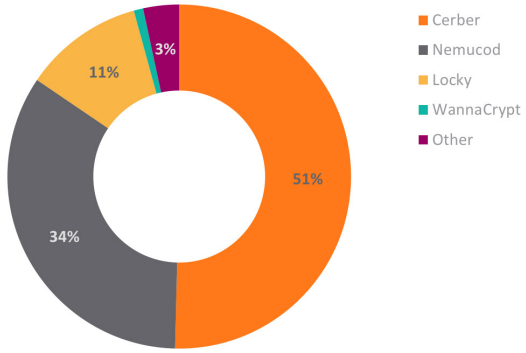
While this was another ransomware that gained notoriety in 2016, Nemucod increased its use of encryption to hide malicious content in 2017. According to SonicWall research, Nemucod had six of the top 10 variants that leveraged encryption to avoid detection.

Ransomware Variants by Region

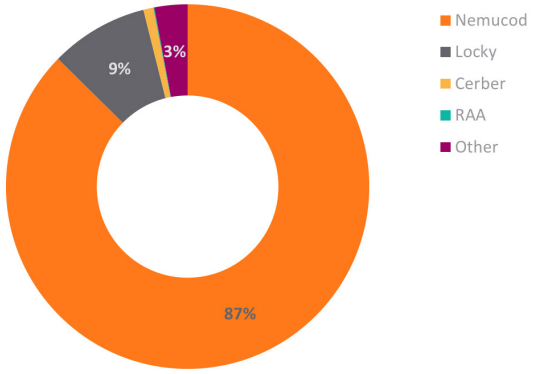
Americas



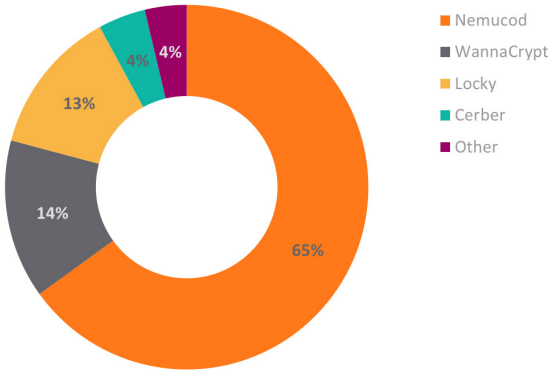
Europe



Latin America



Asia Pacific



SONICWALL®

SSL/TLS USE INCREASES YET AGAIN

The use of secure sockets layer (SSL) and transport layer security (TLS) protocols to encrypt and protect data in transit across the internet is nothing new. Until recently, encryption was typically reserved for the most sensitive web traffic (e.g., payment data, transactions, PII, etc.).

Each year, however, more and more everyday web traffic is encrypted. On March 5, 2012, Google announced[vii] it was switching to HTTPS by default. Since then, SonicWall has recorded a rapid increase of HTTPS sessions in comparison to unencrypted HTTP traffic.

For analysis, SonicWall monitors the use of HTTP and HTTPS to demonstrate the increase of encrypted sessions. The graphs to the right contrast the use of each across a three-year span. The split was nearly the same at the beginning of 2015. In 2017, the **use of encrypted sessions grew 24 percent over 2016 and accounted for 68 percent of overall sessions**.

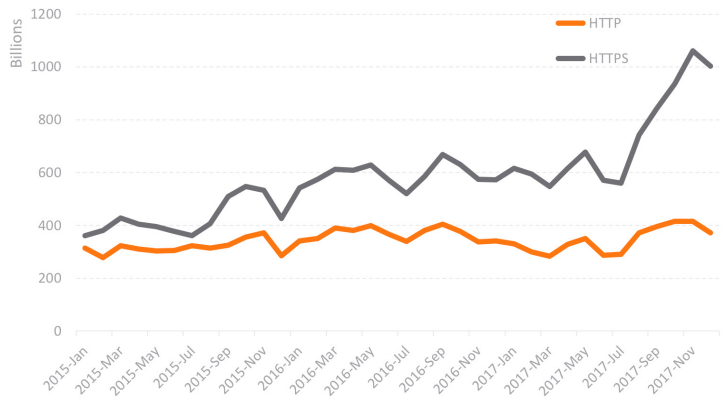
The acceptance of hybrid cloud environments, coupled with an explosive application-dependent society, will only accelerate the use of HTTPS in the coming years. This shift has already given more opportunity for cybercriminals and threat actors to hide malicious payloads in encrypted traffic.

In response, organizations are implementing security controls, such as deep packet inspection (DPI) of SSL/TLS traffic, to responsibly inspect, detect and mitigate encrypted attacks.

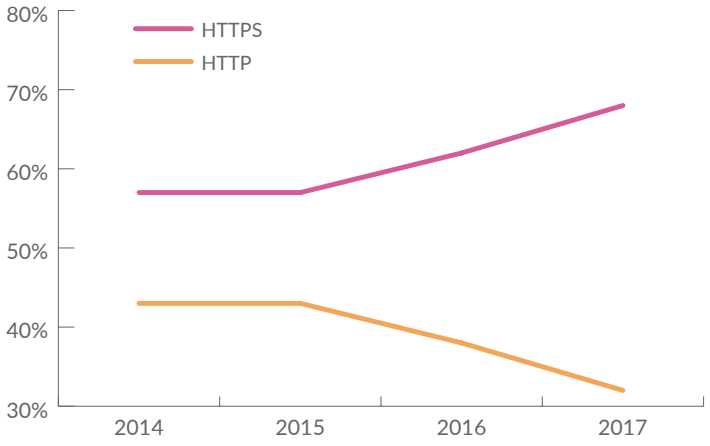
Do you have SSL/TLS inspection controls?

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. Contact your security or firewall provider to ensure you have this capability and that it is properly activated.

Global HTTPS vs. HTTP Web Connection (in billions)



HTTPS vs. HTTP Traffic



SONICWALL®

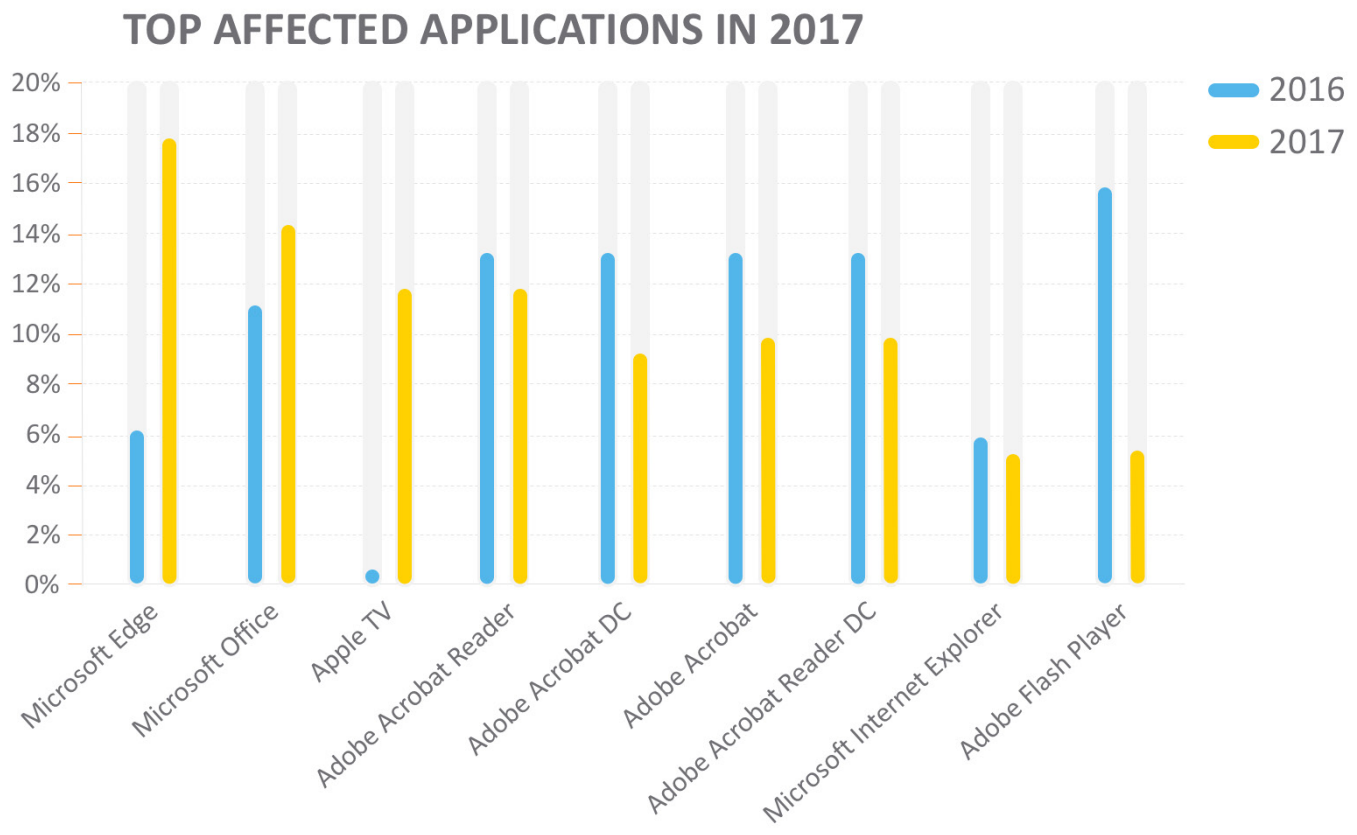
EFFECTIVENESS OF EXPLOIT KITS IMPACTED

In 2016, we saw three major zero-day vulnerabilities hit Adobe Flash, which were used in multiple attacks. But since browser vendors have largely phased out Flash — it's disabled in default browser settings — new Flash Player exploits are less attractive to attackers.

That, however, hasn't deterred threat actors from attempting new strategies. For example, between 2016 and 2017, SonicWall found that attacks on Microsoft Edge grew 13 percent. This signifies that attacks on the vulnerable Microsoft Internet Explorer browser are in rapid decline and cybercriminals are looking for all avenues to deploy traditional exploits.

Attacks against the most popular Adobe products — Acrobat, Acrobat DC, Reader and Reader DC — were down across the board. Attacks against Microsoft Office and related applications (e.g., Word, Excel) were up nearly 4 percent.

With new applications cracking the top 10 in 2017 (e.g., Apple TV, Microsoft Office), organizations should continually redefine and broaden the scope of applications and related files that could present a risk. In analyzing application volume, machine-learning technology helps protect against newer attack vectors like Microsoft Office files, PDFs and other email-based threats.



SONICWALL®

LAW ENFORCEMENT A DISRUPTIVE FORCE

Arrests of key malware and exploit kit authors in 2017 are now making a significant dent in the scale, volume and success of cyberattacks. While arrests in 2017 weren't as directly tied to reducing malware attacks as in the year before, they may end up being more strategic in the long term. These efforts are helping disrupt malware supply chains and are impacting the rise of new would-be hackers and authors.

For example, in December 2017, law enforcement officials from the United States, Romania, Britain and the Netherlands collaborated to arrest five Romanian hackers[viii] accused of operating CTB-Locker/Critroini ransomware.

In another high-profile case, Marcus Hutchins, the British cybersecurity researcher responsible for "accidentally stopping" the notorious WannaCry ransomware attack by unknowingly activating a *kill switch*, was later arrested for allegedly authoring banking Trojan Kronos. If convicted, Hutchins faces six counts of hacking charges that date back to 2014 and could hold a maximum 40-year prison term.[ix]

Are arrests like these truly making an impact in the cyber arms race? Or are these simply anecdotal wins that won't change the threat landscape? Reactive threat actor behavior in 2017 suggests law enforcement is closing in.

Top Cyber Crime Arrests of 2017

NAME	NATIONALITY	ARREST LOCATION	STATUS	GOVERNMENT/ AGENCIES	REASON
Pyotr Levashov[x, xi]	Russian	Spain	Seeking Extradition	Spain	Kelihos Botnet
Marcus Hutchins[xii]	British	U.S.	Trial Pending	U.S.	Kronos Banking Trojan
Ruslan Stoyanov[xiii]	Russian	Russia	Trial Pending	Russia	Treason (Kaspersky Executive)
Mark Vartanyan[xiv]	Russian	Norway	5 Years Prison	U.S., Norway	Citadel Malware Toolkit
Ytu Pingan[xv]	Chinese	U.S.	Trial Pending	U.S.	Sakula Malware; OPM Breach
Kamyar Jahanrakhshan[xvi]	American	U.S.	Sentence Pending	U.S.	Extortion; Attempted DDoS Attack
Alexandre Cazes[xvii]	Canadian	Thailand	Deceased	Europol, FBI, DEA, Dutch National Police	AlphaBay & Hansa Darkweb Market Operations
Yarden Bidani[xviii]	Israeli	Israel	Trial Pending	Israel	vDOS Service
Itay Huri[xix]	Israeli	Israel	Trial Pending	Israel	vDOS Service
Alexander Vinnik[xx]	Russian	Greece	Trial Pending	U.S., Greece, Russia	BTC-e exchange; Mt. Gox Theft
Identity Withheld[xxi]	Ukrainian	Ukraine	Trial Pending	Ukraine Cyber Police	NotPetya/ExPetr Ransomware Distribution

FOLLOWING THE BITCOIN TRAIL

Because of the inroads law enforcement agencies are making into arresting and convicting malware authors and disruptors, cybercriminals are being more careful with how they conduct business. This change is most clear in their processes for collecting data ransom payouts.

Unlike NotPetya or WannaCry ransomware, which were linked to only a handful of bitcoin wallets, most ransomware attacks in 2017 generated a unique bitcoin wallet per infection. Although still anonymous, this simple change made it more difficult to track payments received that might correlate how widespread an infection may have been.

While bitcoin and other cryptocurrencies are largely anonymous, law enforcement agencies are also cracking down on the proprietors and operators of different exchanges.

In 2017, for example, law enforcement arrested Russian Alexander Vinnik, operator of bitcoin exchange BTC-e, on more than 21 charges of money laundering, fraud and other financial crimes.

"As some suspected, Vinnik's alleged crimes go beyond just operating the exchange. [Federal agents] believe he played a role in the theft of more 800,000 bitcoin — about $400 million at the time — from Mt. Gox, a staggering loss that ultimately shuttered the exchange," wrote Russell Brandom and Sarah Jeong for The Verge. "According to the indictment, 530,000 of those bitcoin ended up passing through wallets controlled by or associated with Vinnik, although his role in the larger scheme remains unclear." [xxii]

Because of this change in behavior — whether caused by law enforcement or not — it is harder to track the bitcoin earnings of specific ransomware. The majority of SonicWall ransomware analysis completed in 2017 found wallet addresses with few or no transactions at all.

Despite these findings, comparing this year's ransomware attacks that were tied to a single bitcoin wallet (or a handful, like WannaCry's three known wallet addresses), SonicWall has seen fewer transactions than that of the previous year's attacks.

MORE RANSOMWARE VARIANTS IN THE WILD

This may mark a pivot point for threat actors. They've exhausted the capabilities of standard ransomware and need a new approach, as payouts are seemingly in decline. Despite the plunge in effectiveness, SonicWall Capture Labs recorded many more new ransomware variants, including WannaCry, NotPetya, Locky, Nemucod, Cerber, GlobeImposter,[xxiii] Bad Rabbit, SyncCrypt,[xxiv] etc.

As noted earlier in the report, the total volume of ransomware was down significantly year over year. However, the number of **unique ransomware variants in play increased 101.2 percent** in 2017. SonicWall Capture Labs threat researchers created 2,855 new unique ransomware signatures in 2017, which was up from the 1,419 published a year before.

Ransomware draws the media lens because of its ability to successfully and simultaneously target large organizations, small businesses and even individuals. But this high profile comes with a price: awareness and understanding.

While it is just a category of malware, ransomware is about as close as it comes to a household name. So much so, organizations and individuals are educated on the matter. While apathy does still exist, some organizations are more proactive and more prepared.

Victims are less inclined to pay ransoms once infected due to the uncertainty of retrieving their files. The most malicious cybercriminals will even use ransomware like GlobeImposter, which can render a system unbootable without even requesting payment.[xxv]

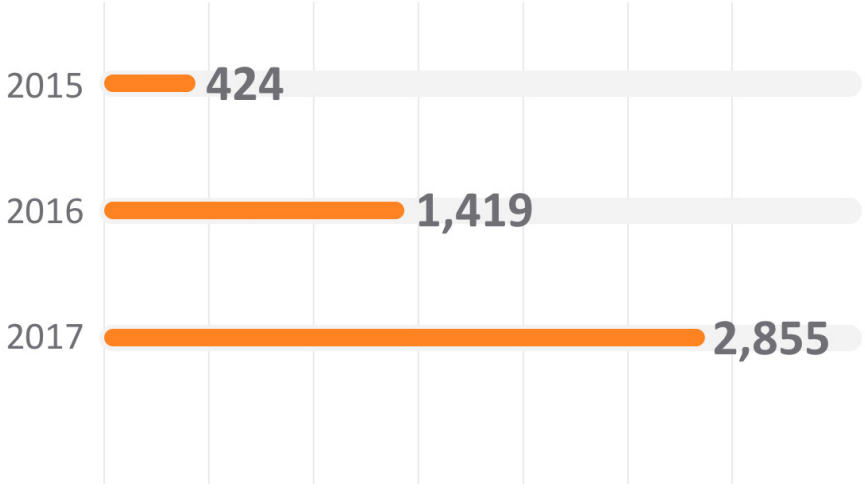
The supposed decline in revenue is not discouraging malware authors from creating new ransomware variants, which is proven by the increasing number of ransomware signatures SonicWall created and deployed in 2017.

In addition to the new jump in variants, cybercriminals are also relying on new propagation methods (e.g., EternalBlue, Remote Desktop) in attempt to slow the decline in usefulness.

The increased popularity of ransomware as a service (RaaS) also affected the increase in variants recorded.[xxvi] It's another channel strategy for authors and cybercriminals to get their "product" in the market, particularly those who want to modify someone else's code to make a quick — albeit illegal — dollar.

Thankfully, the security industry has had several years to implement countermeasures to mitigate ransomware attacks. The period between 2013-2016 was lucrative for cybercriminals. Their sophistication and innovation paid off. It's too soon to know if 2017 was an outlier or if 2018 will continue this downward trend, signifying a true shift in the threat landscape.

Unique Ransomware Signatures



SONICWALL®

THE RISE OF IOT RANSOMWARE

IoT ransomware is a type of attack against an IoT device to gain control of the device's functionality. While many smart devices do not hold any valuable data, there is still a potential for holding an owner, business or organization ransom.[xxvii]

This type of attack largely depends on timing. For example, if an attacker can gain control of a business HVAC during work hours, there is a higher likelihood that they will pay the ransom.

Unfortunately, there will be more insidious cases (e.g., controlling connected cars, baby monitors, medical equipment) where victims may have no choice but to pay ransoms to regain control of critical devices or equipment.

DDoS attacks still remain the major threat to IoT devices and networks. Each compromised device could send up to 30 million packets per second to the target, creating an IoT-powered botnet that could easily launch a terabit-level DDoS attack in the future. The security of IoT devices will remain a critical topic in 2018.

Is Mobile Ransomware Next?

The mobile device is ubiquitous across all cultures, ages, regions and even incomes. It's estimated that 6 billion mobile devices will be in circulation by 2020.[xxviii] With such a footprint, there's little surprise that it would make the perfect target for a ransomware attack.

Following reports from WikiLeaks, Israeli researcher Amihai Neiderman uncovered 40 zero-day vulnerabilities of Samsung's open-source operating system Tizen, which works on a wide range of Samsung devices.

These vulnerabilities would allow attackers to remotely control Samsung devices already on the market, such as smart TVs, smart watches and the company's popular line of Android smartphones.[xxix] Because Android is the most targeted operating system, smartphones that run Android are the most targeted device.

The mechanisms used by ransomware to render victim devices useless has also shifted. Earlier attacks simply covered the entire screen with a custom message, but exploits in 2017 began to completely encrypt the device. One such attack encrypted the device and reset the lock screen security PIN. From that point, it's easy to make the jump to holding the device for ransom.

SSL ENCRYPTION HIDING CYBERATTACKS

While encrypting traffic is a necessary practice, it does leave opportunity for threat actors. The same great protections SSL and TLS encryption afford well-meaning organizations may be leveraged to cloak illegal or malicious traffic as well.

Over time, the malware industry has improved their skillsets and are applying new and sophisticated technologies into their campaigns, including the use of encryption to hide payloads transferred over the internet.

Encryption was leveraged more than previous years, for both legitimate traffic and malicious payload delivery. However, for the first time ever, SonicWall has real-world data that unmasks the volume of malware and other exploits hidden in encrypted traffic.

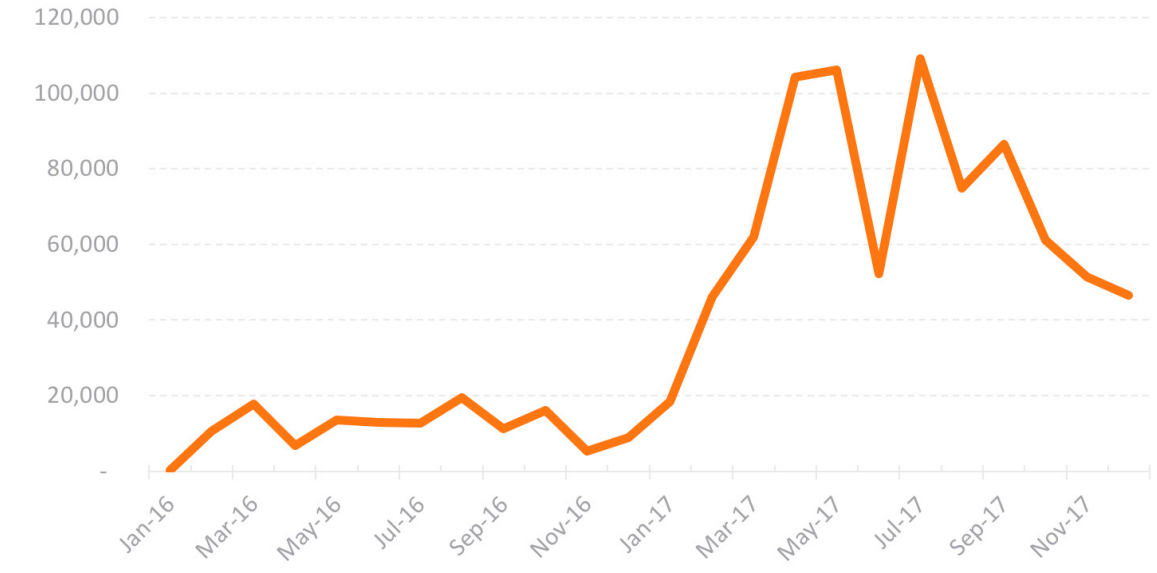
Based on data from the subset of SonicWall firewalls using DPI-SSL, an average of 4.2 percent of all file-based malware propagation attempts used SSL/TLS encryption in 2017.

SonicWall Capture Labs found, on average, 60 file-based malware propagation attempts per SonicWall firewall each day. Without the ability to inspect encrypted traffic, the typical organization would have missed over 900 file-based attacks per year hidden by SSL/TLS encryption.

Top Encrypted Ransomware

NAME	HITS
JScript.Nemucod.BZN	204,519
JScript.Nemucod.XJ_2	30,972
Cerber.G_17	5,651
JScript.Nemucod.CI_3	906
JScript.Nemucod.HM	641
Cerber.RSM	533
Locky.VBS_2	523
JScript.Nemucod.RJ_12	306
JScript.Nemucod.J	257

IPS Attacks Over SSL by Month



SONICWALL®

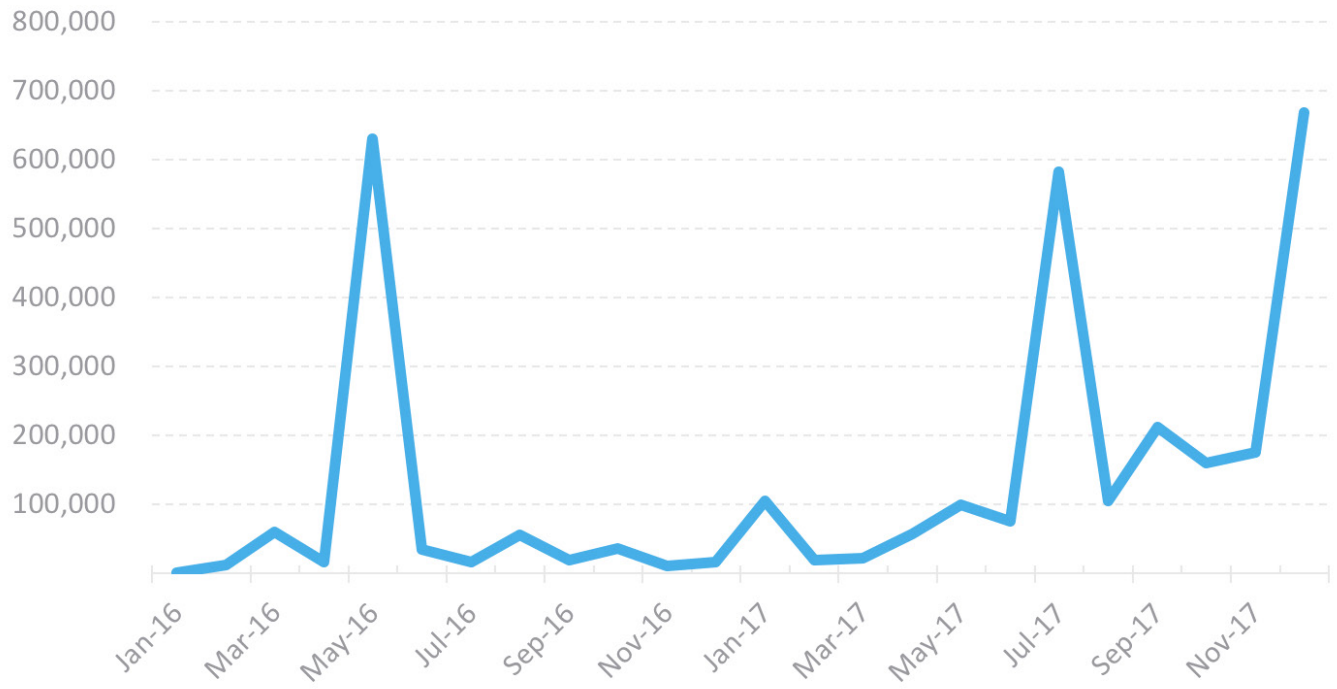
As outlined, the use of encryption to protect web traffic was up 24 percent in 2017. With this growth, each year provides cybercriminals more and more avenues for obscuring their malicious actions. For example, the use of SSL to download Nemucod content increased in 2017.

Leveraging intrusion prevention systems (IPS), SonicWall recorded and analyzed similar trends for attempted network intrusions. The top IPS attacks focus on HTTP Header, Directory Traversal and SQL Injection.

Encrypted traffic will continue to grow, but unencrypted traffic will remain for most public services. However, threat actors will continue to use encryption to hide attacks in 2018 and beyond.

In response, more organizations and enterprises are implementing SSL decryption, inspection and mitigation capabilities into their security strategy.

Malware Attacks Over SSL by Month



SONICWALL®

MALWARE COCKTAILS STILL MIXING THINGS UP

The data presented to this point highlights changes in cybercriminal behavior. Cybercriminals are mainly relying on existing code — with a few minor changes — to build malware variants that can spread quickly and more dangerously. All with the purpose of avoiding detection. This is the malware cocktail.

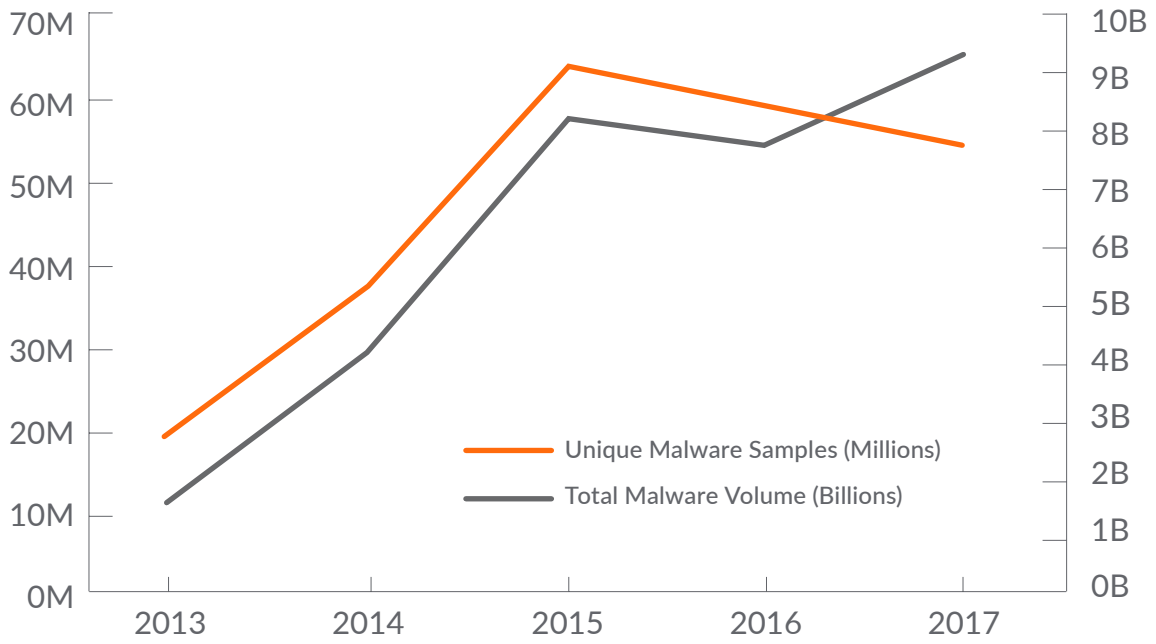
As an example, while the total volume of malware attacks was up, the number of unique malware signatures declined. In 2017, SonicWall collected **56 million unique malware samples** in contrast to the 60 million samples discovered in 2016.

For the year, unique malware signatures dipped 6.7 percent from 2016 and 12.5 percent from 2015. However, 2017 levels remain 51.4 percent higher than the 2014 mark.

SonicWall Capture Labs uses machine learning to examine individual artifacts of malware signatures to categorize each as unique or something that already exists. This helps reduce the number of new signatures needed to effectively mitigate known and unknown malware attacks.

The reason? Malicious groups are still using the same malware — with slight tweaks and modifications — as seen in years past. But threat actors aren't just re-tooling old malware code and launching it haphazardly. While some of that still occurs from 'script kiddies' and other less-skilled hackers, innovative authors are refining how they target their victims.

Rise of the Malware Cocktail



SONICWALL®

Evolving malware tactics

Take Cerber, for example. It's a Trojan that mainly spreads via email spam, but also leverages exploit kits (EK), such as Magnitude EK in September 2017. It also was one of the top attacks that used encryption to avoid detection.

What's noteworthy about Cerber is its ability to evolve in a short period of time. SonicWall Capture Labs threat researchers were identifying updated versions of Cerber being caught in the wild — as many as two versions a day.

These were **malware cocktails** created by cybercriminals to elude signature-based security solutions. Even more interesting, the new Cerber variants were utilizing seven different tactics to evade detection.[xxx]

Hits vs. Detection

Signature Detection
The number of attacks, by the malware type and its variants, caught by the signature.

Malware Hit
The recognition of a malware attack. Once detected, the attack is blocked.

New exploit kits, old code

SonicWall Capture Labs threat researchers aren't discovering many new exploit kits. What they are finding, however, are EKs that repurpose old code for new gains.

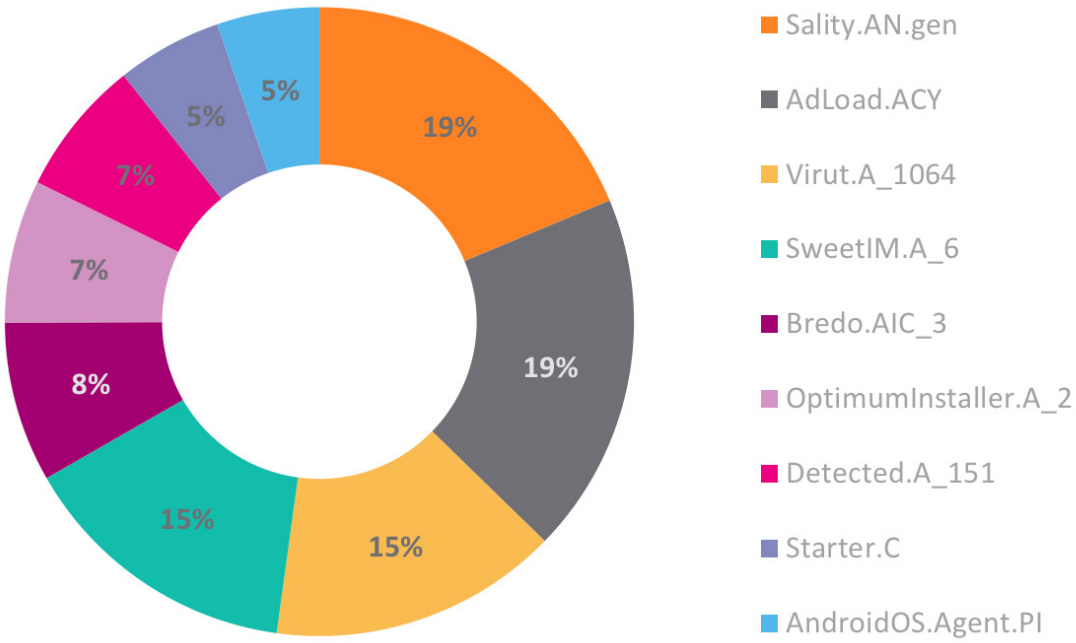
Terror, for example, was an exploit kit first noticed in early 2017. Then a new version of the Terror exploit kit appeared, which seemed to be based on code stolen from both the RIG and Sundown exploit kits.[xxxi]

The Terror landing page consisted of a JavaScript that appeared to be taken from RIG, followed by another script stolen from Sundown. This stolen JavaScript was followed by embedded Flash exploits. There is no obfuscation seen in this exploit kit, and both the landing page and payload are unencrypted.

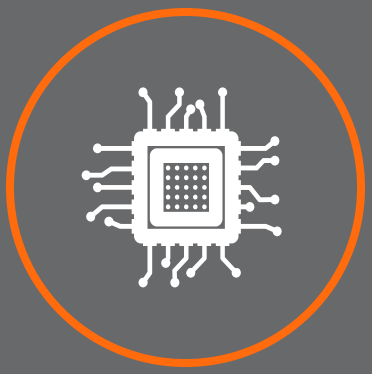
Similarly, the exploit kit Nebula was discovered in February 2017. It was likely a variant of Sundown and spread the DiamondFox and Ramnit malware, among others.[xxxii]

Agile malware cocktails, coupled with new propagation methods (e.g., NSA exploits, remote desktop protocols, toast overlays), show that some cybercriminals are still at work mixing and matching malware attacks to circumvent defenses, particularly legacy signature-based security approaches.

Top Malware Detection



SONICWALL®



IOT, PROCESSOR THREATS SIGNAL WHAT'S TO COME

Cybercriminals are pushing new attack techniques into advanced technology spaces, notably the Internet of Things (IoT) and chip processors. These areas are grossly overlooked and unsecured, and present a window of opportunity for successful cyberattacks.

Mitigating Meltdown

In January 2018, a processor vulnerability, known as Meltdown, was published by Google's Project Zero security team.[xxxiii] Variants of this issue are known to affect many modern processors. A successful exploit of this vulnerability could allow an attacker to access sensitive information (e.g., passwords, emails, documents) inside protected memory regions on modern processors.

"Threat actors have been so far ahead of the game they've been able to create highly evasive malware without the greater industry even knowing," said Conner.

These memory regions are the next key battlegrounds where organizations will combat cybercriminals. To mitigate these chip-based threats, organizations will soon need to implement advanced techniques that can detect and block malware that does not exhibit any malicious behavior and hides its weaponry via custom encryption. This weaponry is exposed in memory for less than 100 nanoseconds, so real-time identification and mitigation is critical.

"This is a revolution in engineering, execution and innovation," said General Michael Hayden, Principal at the Chertoff Group, a global advisory firm focused on security and risk management. "To introduce this technology in the relatively early stages of these advanced attacks is a huge win for the security industry, as well as the public and private sectors."[xxxvi]

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 in memory. 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.

IoT Reaper looming

Since the unwelcomed and unexpected appearance of Mirai and related DDoS attacks in September 2016, the IoT space has been highly active.

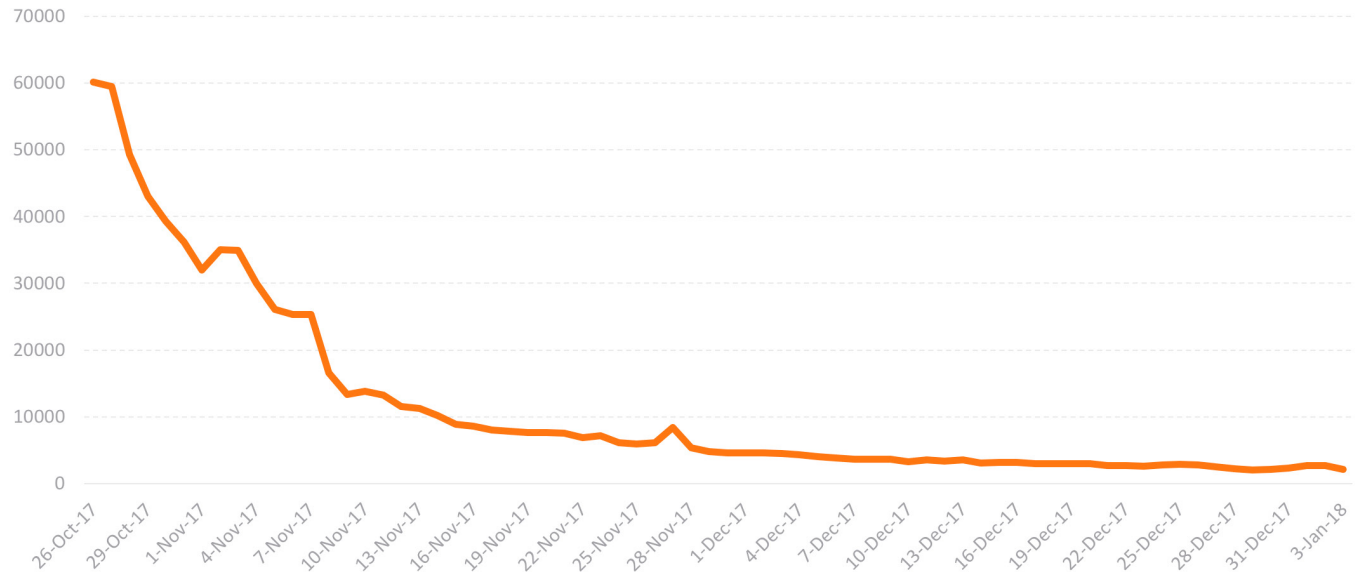
The most high-profile evolution of Mirai is IoT Reaper. This variant doesn't leverage weak password policies like Mirai, but rather exploits nine vulnerabilities in various IoT devices. As an example, IoT Reaper, a type of Trojan, integrated LUA execution environments for more complex attacks.

At one point in 2017, SonicWall Capture Labs was recording more than 62,000 IoT Reaper hits each day. Unmitigated, it slowly faded away without being leveraged to launch a wide-scale attack.

Inspect Deep Memory

A patent-pending technology, the SonicWall Real-Time Deep Memory Inspection (RTDMI™) engine proactively detects and blocks unknown mass-market malware via deep memory inspection. In real time, the engine identifies and mitigates even the most insidious modern threats, including future Meltdown exploits.

IoT Reaper IPS Hits



At one point in 2017, SonicWall was recording more than 62,000 IoT Reaper hits each day. SonicWall created and automatically applied nine unique IPS signatures and five GAV signatures to mitigate IoT Reaper.

The Mirai Legacy

First discovered in late 2016, Mirai is an IoT malware that can be used to launch gigabit-plus DDoS attacks via a zombie botnet created with compromised internet-connected devices (e.g., DVRs, IP cameras, etc.). Until that point, the majority of DDoS prevention solutions couldn't handle traffic that surpassed 1 Gbps, so many public services and domain name systems (DNS) were knocked offline.

Mirai used common factory default usernames and passwords to gain access to connected devices and infect them with malicious code. SonicWall discovered several variants of Mirai that were re-tooled to add new vulnerabilities or target specific devices.

2018 PREDICTIONS

Meltdown & Spectre Exploits

The appearance of Meltdown and Spectre in early 2018 were strong indicators of what the year may hold. It's likely these are just two of many processor vulnerabilities already in play. We predict the emergence of password-stealers and infostealers to take advantage of Meltdown and Spectre vulnerabilities.

PDF & Microsoft Office Threats

Cybercriminals will leverage users' trust in PDFs and Microsoft Office applications as a new attack vector. Because of obfuscation techniques, many legacy firewalls and anti-virus solutions are an unable to effectively identify and mitigate PDFs or Microsoft Office file types that contain malicious content.

More Infostealers

Many of the critical threats identified in 2017 were based on malware that attempted to steal sensitive information from a device. In some cases, highly targeted attacks had political motivation and targeted defense personnel of a particular region. As user-related data is extremely valuable to attackers, it should be no surprise that most of the attacks focused on gaining this valuable commodity.

New Ransomware Tricks

With a decline in ransomware attacks in 2017, we will see new tricks from ransomware authors. The mechanism used by ransomware to render a victim's device useless has shifted. Earlier threats simply covered the entire screen with a custom message. In 2017, more and more threats completely encrypted the device. We expect to see even newer techniques used in 2018.

Surge in Encrypted Attacks

This is only the beginning of encrypted attacks. In 2018, we will likely witness more sophisticated malware that rely on encrypted traffic to covertly infiltrate organizations.

Proactive IoT Malware

Advanced IoT malware will leverage automated active attacks to spread easier and faster (e.g., actively exploiting the vulnerabilities and spreading like a worm).

Malicious Cryptocurrency Mining

With the rise of cryptocurrency, malware will force a victim's device resources — from mobile devices and desktops alike — to mine currency for attackers. Such malware and websites are more prevalent for Microsoft Windows, but recent SonicWall analysis shows increased threats against Android as well. In fact, some of this activity is already occurring in 2018. [xxxv]

Consumer IoT Attacks

Home-based IoT attacks will lead headlines as they begin to threaten average citizens' privacy, information and identities.

Device Control

More and more devices (e.g., cars, refrigerators, thermostats, light bulbs) are being hyper-connected without much oversight. This increases the scope of locking these devices for ransom. The threat of a botnet based on consumer IoT devices also looms.

BEST PRACTICES & FINAL TAKEAWAYS

Each year presents new and interesting developments that define the state of the cyber arms race and cybersecurity industry. These advances drive the actions of each organization, business, government and individual. Unsurprisingly, 2017 was no different.

While threat actors and cybercriminals are sophisticated, agile and well-funded, the public and private sectors are turning the tide in the cyberwar. But it is a war, not just a battle.

To survive the cyberwar, organizations must ensure they're leveraging the proper security tools, services and solutions that will appropriately protect their brand, data and customers.

What was once a must-have capability two or three years ago could be outdated today. It's imperative that security solutions, appliances and strategies are continually optimized or evaluated to ensure that they are layered, integrated, intelligent and versatile.

Layered

The best cybersecurity strategies are layered, automatic and dynamic. Security-conscious organizations will deploy a cohesive mix of devices and controls to serve as the fabric of their security posture. This includes next-generation firewalls, email security solutions, real-time cloud sandboxing, secure mobile access controls and wireless access points.

- Layer security across wired, wireless, cloud and mobile networks
- Regularly patch all operating systems, software, network devices and security appliances
- Evaluate the use of cybersecurity insurance to help mitigate risk exposure

Integrated & Automated

Still, it takes more than buying siloed point solutions. They should be integrated as the foundation of an automated, real-time breach detection and protection platform, which will link security, intelligence, analytics, management and reporting.

- Deploy next-generation firewalls that leverage shared intelligence and real-time mitigation to protect against advanced cyberattacks
- Implement responsible SSL/TLS decryption and inspection capabilities
- Properly configure gateway anti-virus and intrusion prevention on next-generation firewalls
- Use email security solutions to block email-borne threats

Intelligent

Once deployed, this strategy should be dynamic enough — using machine-learning and artificial intelligence — to make real-time decisions against the most advanced and savvy cyberattacks. Intelligence must also extend past technology to include employees, contractors and vendors.

- Use automated cloud sandboxes to identify and analyze unknown cyberattacks (e.g., ransomware, zero-day threat) in real time
- Bolster security via shared intelligence by subscribing to relevant security services from your vendor or solution provider
- Educate employees about cyberattack risks (e.g., phishing, malware) and routinely test awareness
- Investigate the use of real-time deep memory inspection

Versatile

To protect their business, brand and data, organizations require critical security capabilities — deployed in an integrated, cohesive manner — across their environments. They should have the power and flexibility to deploy what they want, when they want and where they want to eliminate complexity and potential network vulnerabilities.

- Procure security solutions that match the deployment capabilities and form factors that makes sense for your business
- Build agility through hybrid infrastructures via powerful virtualized cybersecurity controls

ABOUT SONICWALL

The modern organization exists in an increasingly complex and globally connected world. Cybersecurity technology is both an enabler and inhibitor as organizations adapt to this rapidly changing environment.

As security teams and the cyber landscape evolve, a new cyber arms race has emerged, which places organizations and their cybersecurity solutions in the crosshairs of a growing global cybercriminal industry.

Cybercriminals are turning to highly effective weapons like ransomware, infostealers, IoT malware, mobile threats and SSL/TLS-encrypted malware to target all organizations around the world. Now is the time to add new cyber defenses to your security arsenal to stay proactive against both known and unknown threats.

SonicWall developed its Automated Real-Time Breach Detection and Prevention Platform to provide cutting-edge defenses in this cyber arms race. SonicWall Capture Labs researchers pioneered the use of artificial intelligence for threat research and protection over a decade ago.

Today, SonicWall machine-learning algorithms are used to analyze data and classify and block known malware before it can infect the network. Unknown files are sent to the Capture Cloud Platform for analysis using a variety of techniques, including hypervisor analysis, emulation, virtualization and the newly introduced patent-pending Real-Time Deep Memory Inspection.™ Decisions are rendered in nanoseconds, blocking zero-day malware in near real time.

SonicWall has been fighting the cybercriminal industry for over 26 years, defending small- and medium-sized businesses and enterprises worldwide. The award-winning Capture Cloud Platform, coupled with the power of tens of thousands of global channel partners, protects your network, email data, cloud environments, applications and files. This combination of products and partners enables a real-time cyber defense solution tuned to the specific needs of the business.

More business and less fear.

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

RESOURCES

[i] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

[ii] https://www.wsj.com/articles/intel-warned-chinese-companies-of-chip-flaws-before-u-s-government-1517157430

[iii] https://www.theregister.co.uk/2018/01/29/intel_disclosure_controversy/

[iv] http://www.scmp.com/business/banking-finance/article/2128492/lloyds-london-chief-executive-warns-cyberattack-now

[v] https://www.weforum.org/reports/the-global-risks-report-2018

[vi] http://www.zdnet.com/article/uk-firms-stockpile-bitcoin-to-pay-off-ransomware-hackers/

[vii] https://search.googleblog.com/2012/03/bringing-more-secure-search-around.html

[viii] https://www.washingtonpost.com/local/public-safety/romanian-hackers-arrested-in-international-ransomware-investigation/2017/12/20/44a380b6-e5bc-11e7-833f-155031558ff4_story.html

[ix] https://www.theguardian.com/technology/2017/may/15/accidental-hero-who-halted-cyber-attack-is-22-year-old-english-blogger

[x] https://www.nytimes.com/2017/04/09/world/europe/peter-severa-levahsov-russia-arrest.html

[xi] https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/

[xii] https://www.theguardian.com/technology/2017/aug/14/marcus-hutchins-malware-wannacry-kronos

[xiii] https://arstechnica.com/information-technology/2017/01/kaspersky-labs-top-investigator-reportedly-arrested-in-treason-probe/

[xiv] https://www.justice.gov/usao-ndga/pr/russian-citizen-who-helped-develop-citadel-malware-toolkit-sentenced-0

[xv] https://www.cbsnews.com/news/yu-pingan-chinese-national-arrested-hacking-conspiracy-sakura/

[xvi] https://www.justice.gov/usao-ndtx/pr/seattle-man-arrested-attempted-extortion-leaglecom-and-several-other-media-companies

[xvii] https://www.forbes.com/sites/thomasbrewster/2017/07/20/dark-web-drugs-to-suicide-accused-alexandre-cazes/

[xviii] https://krebsonsecurity.com/2017/08/alleged-vdos-operators-arrested-charged/

[xix] https://krebsonsecurity.com/2017/08/alleged-vdos-operators-arrested-charged/

[xx] https://www.cbsnews.com/news/russian-bitcoin-fraud-alexander-vinnik-extradition-us-greece-supreme-court/

[xxi] https://threatpost.com/ukrainian-man-arrested-charged-in-notpetya-distribution/127391/

[xxii] https://www.theverge.com/2017/7/29/16060344/btce-bitcoin-exchange-takedown-mt-gox-theft-law-enforcement

[xxiii] https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=1098

[xxiv] https://www.mysonicwall.com/SonicAlert/searchresults.aspx?ev=article&id=1072

[xxv] https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=1098

[xxvi] https://blog.sonicwall.com/2017/05/ransomware-as-a-service-raas-is-the-new-normal/

[xxvii] https://www.techrepublic.com/article/ransomware-attacks-will-target-more-iot-devices-in-2018/

[xxviii] https://www.cnbc.com/2017/01/17/6-billion-smartphones-will-be-in-circulation-in-2020-ihs-report.html

[xxix] https://motherboard.vice.com/en_us/article/xy9p7n/samsung-tizen-operating-system-bugs-vulnerabilities

[xxx] https://blog.sonicwall.com/2017/03/catching-cerber-ransomware/

[xxxi] https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=1017

[xxxii] https://blog.threatstop.com/nebula-ek-the-rising-exploit-kit-variant

[xxxiii] https://googleprojectzero.blogspot.co.at/2018/01/reading-privileged-memory-with-side.html

[xxxiv] https://www.sonicwall.com/en-us/about-sonicwall/news/press-releases/pr-articles/sonicwall-invents-real-time-deep-memory-inspection

[xxxv] https://www.mysonicwall.com/SonicAlert/searchresults.aspx?ev=article&id=1114

[xxxvi] https://www.sonicwall.com/en-us/about-sonicwall/news/press-releases/pr-articles/sonicwall-invents-real-time-deep-memory-inspection

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

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