MID-YEAR UPDATE | JULY 2018

2018 SONICWALL CYBER THREAT REPORT

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

SONICWALL®

sonicwall.com | @sonicwall

TABLE OF CONTENTS

INTRODUCTION

Each year, SonicWall releases an in-depth cybersecurity industry report that analyzes threat intelligence and cyberattack behavior from the previous 12 months. Released in March 2018, the complete 2018 SonicWall Cyber Threat Report compared advances made by the cybersecurity industry and cybercriminals alike.

But the cyber arms race moves with great agility and purpose. So much so, SonicWall is publishing the first mid-year update to its annual report. It's critical that the greater public is armed with as much cyber threat intelligence as possible to help safeguard sensitive data, networks and applications.

Explore the mid-year update to discover cyberattack trends for the first six months of the year, including real-world threat intelligence on malware, ransomware, encrypted attacks, chip-based attacks and more.

SonicWall also publishes monthly cyber threat intelligence via public-facing threat meters within the company's **Capture Security Center**.

In addition to offering threat data and security alerts, the cloud-based tool offers the ultimate in visibility, agility and capacity to govern entire SonicWall security operations and services with greater clarity, precision and speed — all from a single pane of glass.

EXPLORE THE MID-YEAR UPDATE TO DISCOVER CYBERATTACK TRENDS FOR THE FIRST SIX MONTHS OF THE YEAR, INCLUDING REAL-WORLD THREAT INTELLIGENCE ON MALWARE, RANSOMWARE, ENCRYPTED ATTACKS, CHIP-BASED ATTACKS AND MORE.

See Real-Time Attack Data

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

VISIT THE SECURITY CENTER

MALWARE VOLUME SURGES IN 2018

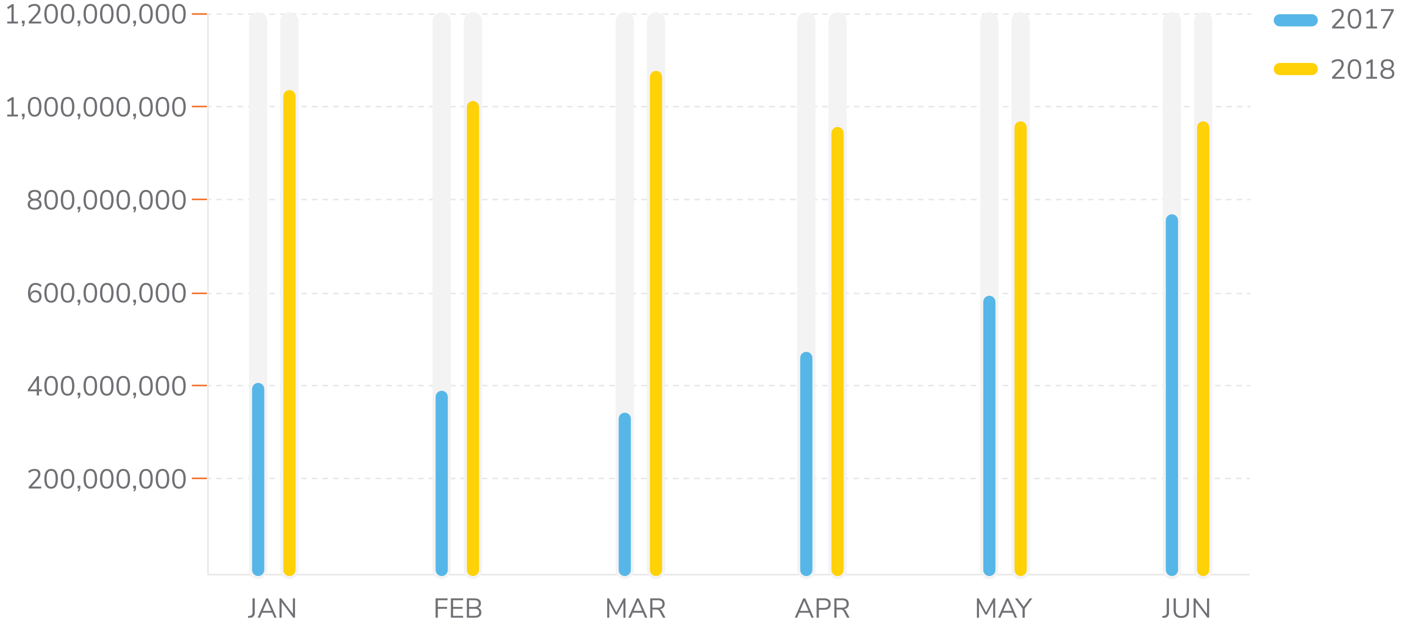
After a down 2016, malware volume in 2017 reached 9.32 billion. It was a staggering jump. Unfortunately, 2018 is already outpacing last year's record numbers.

To date, SonicWall has recorded 5.99 billion malware attacks in 2018, which represents a 102 percent increase over the same six-month window in 2017.

102%

Year-to-Date Increase in Malware Volume Over 2017

GLOBAL MALWARE VOLUME



RANSOMWARE BACK IN FORCE

SonicWall cyber threat intelligence from 2017 presented an interesting case study in cybercriminal behavior. Until that time, the use of ransomware had grown at an aggressive rate each year.

However, the full-year data released with the original 2018 SonicWall Cyber Threat Report showed that ransomware attacks actually dropped from 645 million to 184 million between 2016 and 2017. It was a surprising downturn that went against all behavior SonicWall recorded to that point.

The first six months of 2018 have normalized — and then some. All told, SonicWall recorded 181.5 million ransomware attacks year to date. This marks a 229 percent increase over this same time frame in 2017.

During the first six months of 2018, SonicWall Capture Labs threat researchers identified and analyzed more than a dozen new ransomware variants, which leveraged a variety of clever tactics to help compromise target machines.

One of the most high-profile cases so far in 2018 was the **SamSam ransomware attack on the City of Atlanta**. The SamSam ransomware variant affected five out of 13 city departments and shut down systems for 10 days. Fortunately, the $51,000 ransom went unpaid but the damages to systems, lost files and productivity far outweigh the demand.

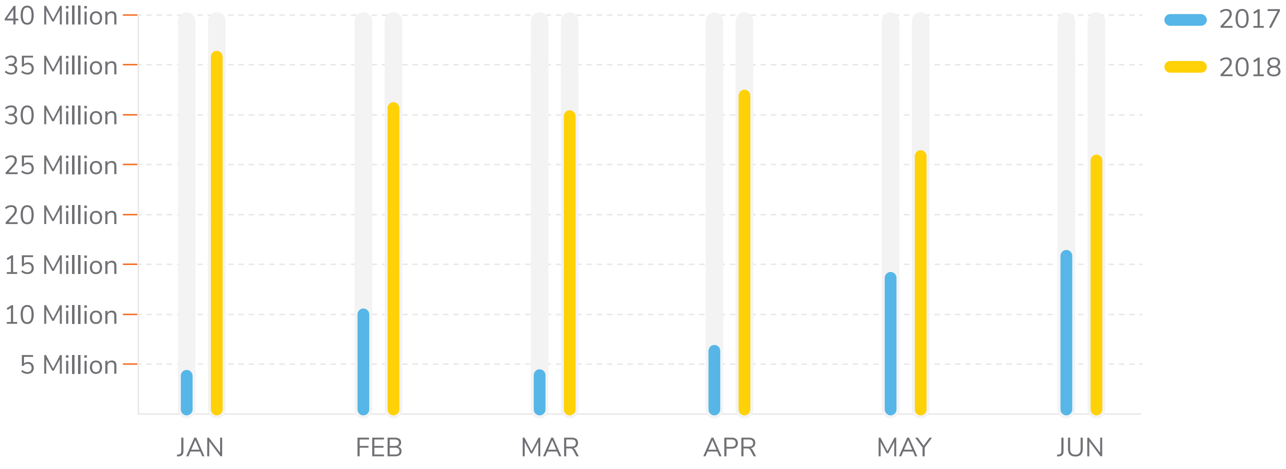
Because of the naming differences between security vendors, SonicWall customers were protected by SamSam ransomware via the Hidden Tear gateway antivirus (GAV) signature.

Inside 2018's Newest Ransomware Variants

SonicWall Capture Labs threat researchers analyzed the year's newest ransomware types. Click on the ransomware below for a detailed breakdown.

- **Gandcrab**
- **BitPaymer**
- **Sigrun**
- **PUBG**
- **Satan**
- **Lockcrypt**
- **UselessDisk**
- **Godra**
- **InsaneCrypt**
- **Genasom**
- **Xorist**

GLOBAL RANSOMWARE VOLUME

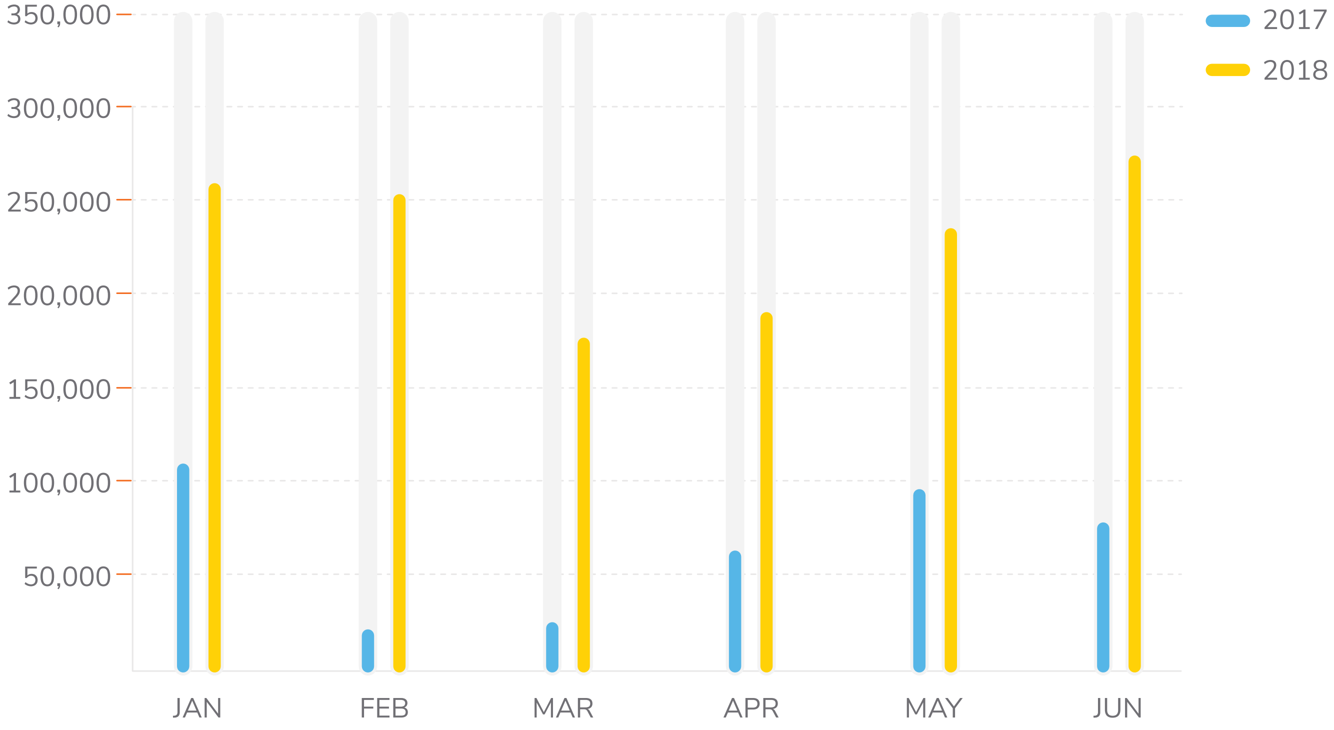


ENCRYPTED ATTACKS ASCEND TO RECORD HIGHS

In 2017, sessions encrypted by SSL/TLS standards represented 68 percent of total traffic. Without the ability to inspect encrypted traffic during this 12-month span, the average organization would have missed more than 900 file-based attacks per year hidden by TLS/SSL encryption.

Through six months of 2018, 69.7 percent of sessions are leveraging encryption. Logically, the use of encrypted cyberattacks also is increasing dramatically. SonicWall recorded 1.4 million encrypted attacks globally in 2018, a 275 percent year-to-date increase over 2017.

GLOBAL ENCRYPTED CYBERATTACKS



RTDMI™ DISCOVERING NEW MALWARE VARIANTS

In January 2018, SonicWall announced its patent-pending Real-Time Deep Memory Inspection™ (RTDMI) technology. Since then, RTDMI has identified and blocked more than 12,300 never-before-seen cyberattacks and malware variants.

SonicWall Capture ATP with RTDMI is one of the only cybersecurity engines that can **effectively mitigate Meltdown processor attacks**. And as of July 2018, RTDMI is also able to stop Spectre chip-based attacks.

Included in the SonicWall Capture Advanced Threat Protection (ATP) sandbox service, RTDMI identifies and mitigates even the most insidious cyber threats where weaponry is exposed for less than 100 nanoseconds.

RTDMI proactively detects and blocks unknown mass-market malware, including malicious PDFs and attacks leveraging Microsoft Office documents.

In addition, SonicWall Capture Labs threat researchers recently analyzed RTDMI stopping two advanced cyberattacks using Microsoft Office files to **hide a malicious VBA macro code** and a **Remote Access Trojan (RAT)**.

12,300 +

New Malware Variants Discovered by SonicWall RTDMI™ Since January 2018

COINHIVE LEADING CRYPTOJACKING GROWTH

With the popularity of cryptocurrency going mainstream the last 12 months, cybercriminals didn't hesitate to take full advantage. Instead of investing in cryptomining hardware and infrastructure like other hopeful billionaires, online criminals opted to employ a technique called cryptojacking.

One of the featured predictions in the 2018 SonicWall Cyber Threat Report, cryptojacking is the act of compromising a network of random machines — typically by commandeering websites to deliver malware exploits — and then using the compute power of that botnet to illegally "mine" for cryptocurrency.

SonicWall Capture Labs threat researchers have been **tracking large spikes in the use of Coinhive**, a JavaScript tool for mining Monero cryptocurrency. In most cases, Coinhive is used as cryptojacking malware that spreads via compromised websites and steals processing power of victims' devices (e.g., laptop, desktop, smartphone).

This processing power is leveraged to illegally mine for Monero, a blockchain-based cryptocurrency. Monero transactions, sources and identities aren't public, making the coin highly attractive to cybercriminals.

Since January 2018, SonicWall has recorded more than 5.6 million hits of Coinhive in use. In one case, there were more than 336,000 Coinhive attempts in a single day.

One such **exploit attempts to mine Monero cryptocurrency** by compromising Android smartphones via a set of six administrator privileges: Internet, Read Phone State, Access Network State, Receive Boot Completed, Wake Lock and Write External Storage.

If the privileges are not granted, the malware uses pop-up windows to repeatedly request admin access until granted. This malware is difficult to get rid of if administrator rights are granted upon infection.

Another technique **hides the Monero cryptominer malware** within an image file. At first glance, the image appears harmless. Upon more thorough inspection, the PNG image file format hides an executable file (ELF). Extracting this executable file, SonicWall threat researchers uncovered the XMRig Monero cryptocurrency miner.

In late June 2018, **SonicWall Capture Labs observed an adware dubbed PBot**. This version has the added functionality of stealing cryptocurrency from its victim.

5.6 MILLION

SonicWall has recorded more than 5.6 million hits of Coinhive in use since January 2018

PBot adware not only serves ads and redirects browser sessions (a common behavior of adware), it also looks for cues that the victim might be executing cryptocurrency transactions online. Once it identifies the website the victim is on, it overlays a gif image that makes it appear that the website is still loading content.

In the background, however, PBot adware will attempt to steal and send virtual currencies to hardcoded addresses. This version of adware appeared to target bitcoin (BTC), Bitcoin cash (BCH) and Ethereum (ETH). SonicWall Capture Labs provides protection against this threat via five unique signatures.

SONICWALL CAPTURE SECURITY CENTER

For organizations that require even more accurate cyber threat intelligence, the SonicWall Capture Security Center empowers stakeholders with single-pane visibility and situational awareness of their network security environment.

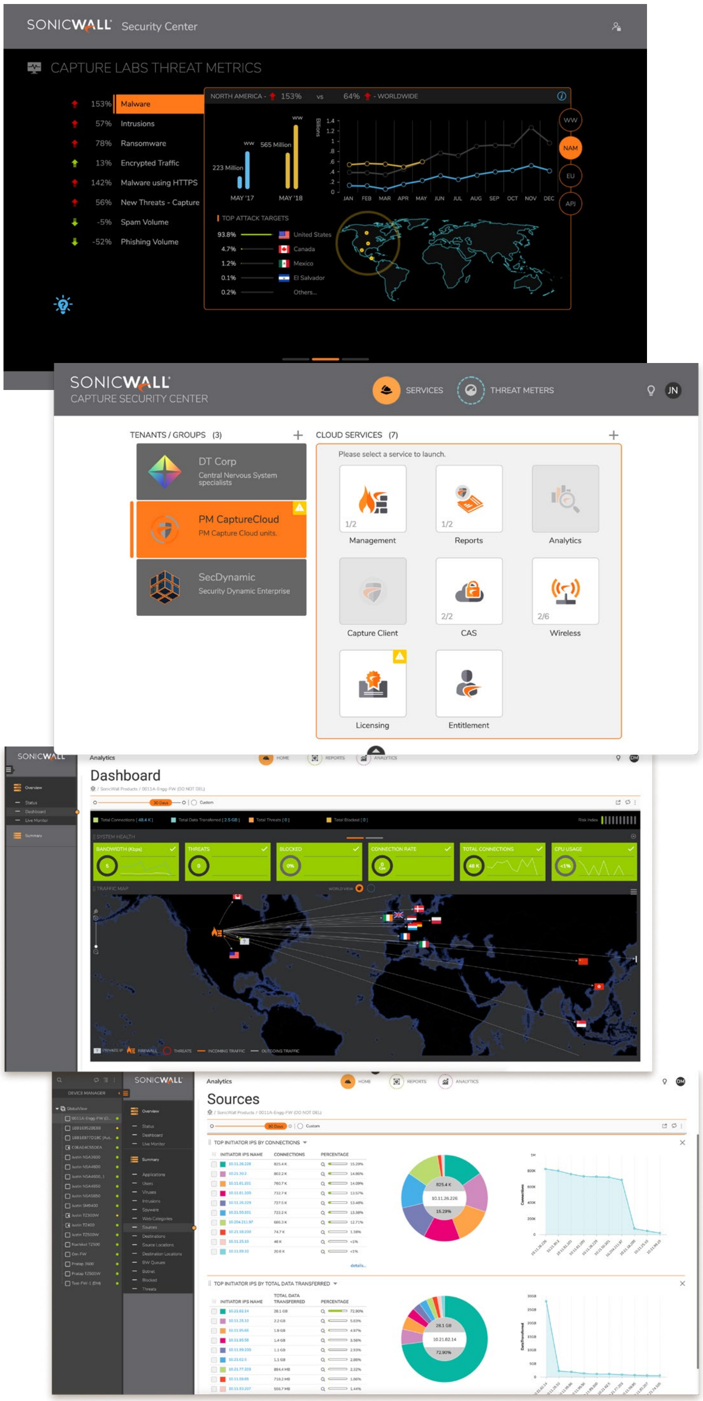
But SonicWall also wants organizations to know what they're up against. Even if they're not customers.

The **SonicWall Security Center threat meters** offer a graphical view of the worldwide attacks over the last 24 hours, countries being attacked and geographic attack origins. This complimentary tool helps illustrate the pace and speed of the cyber arms race, including attack data for:

- Malware
- Intrusions
- Ransomware
- Encrypted Threats
- Spam
- Phishing
- Zero-day threats

Guided by business processes and service level requirements, Capture Security Center helps form the foundation for a unified security governance, compliance and risk management strategy to position the company for success.

By establishing a holistic, connected approach to security orchestration, Capture Security Center can federate all operational aspects of the SonicWall security ecosystem.



SonicWall Capture Labs Threat Network

Data for the mid-year update of the SonicWall Cyber Threat Report is gathered by the SonicWall Capture 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 +

● Sensors per region

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 TLS/SSL-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.**

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

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 200 countries and territories, 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