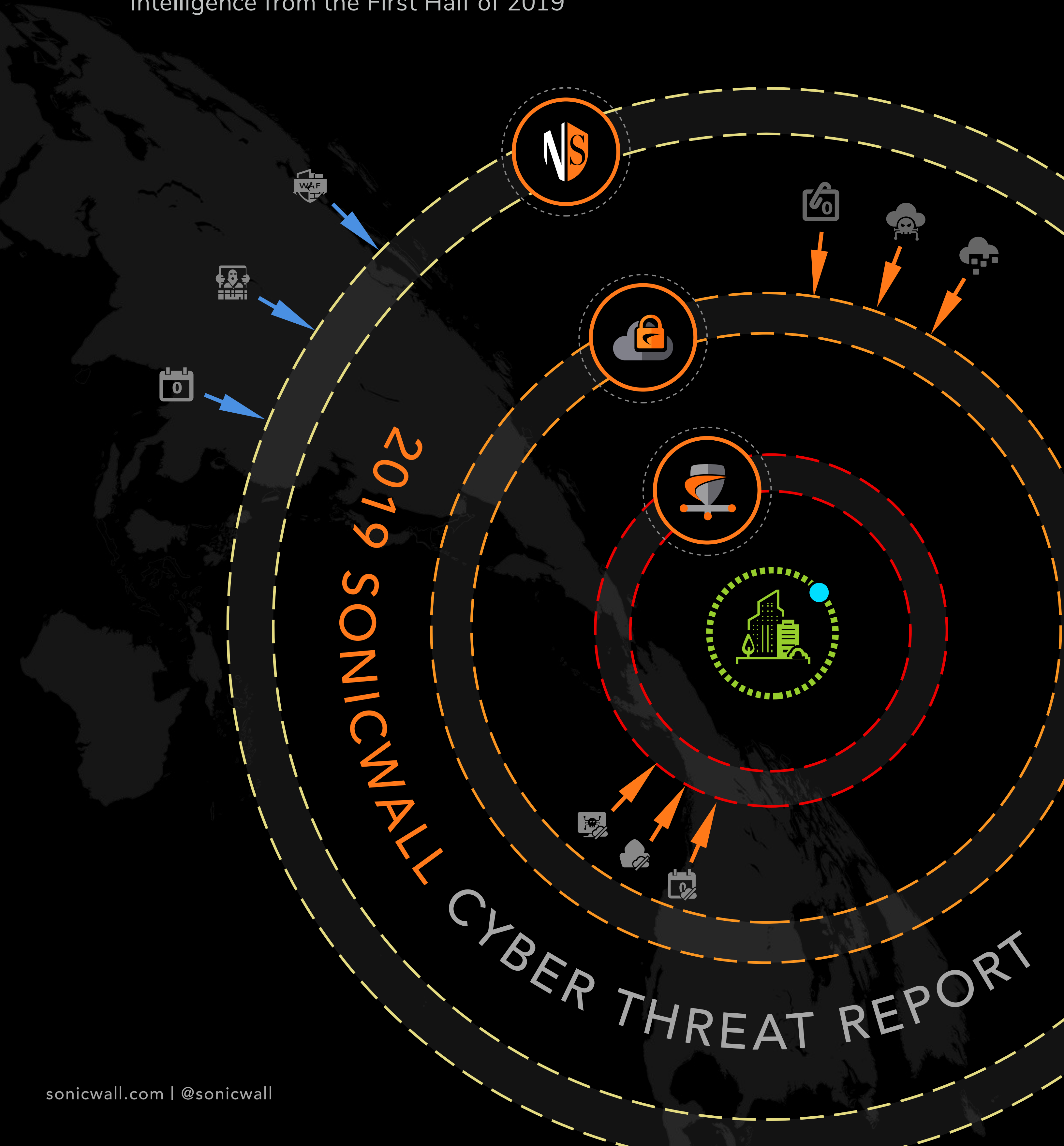
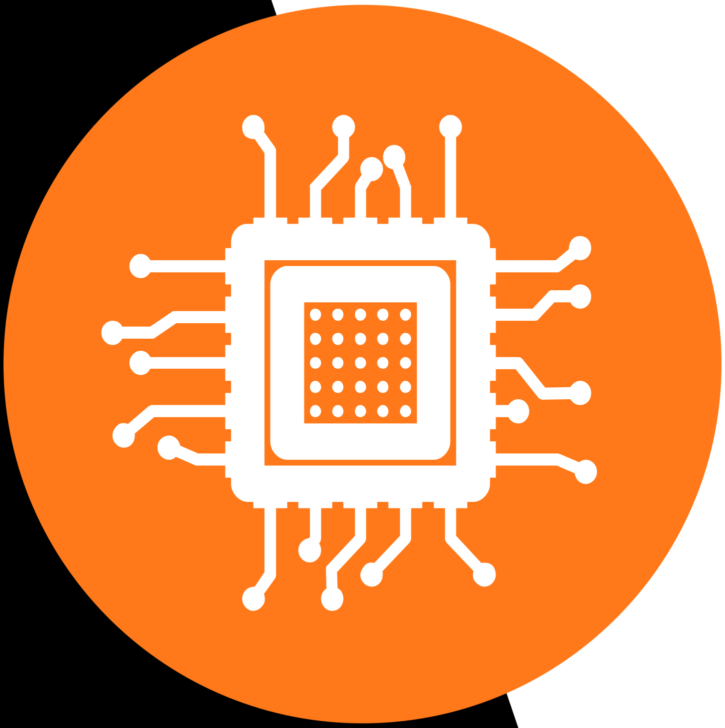
SONICWALL®

Arm Your Business with the Latest Threat Intelligence from the First Half of 2019



sonicwall.com | @sonicwall

TABLE OF CONTENTS



INTRODUCTION

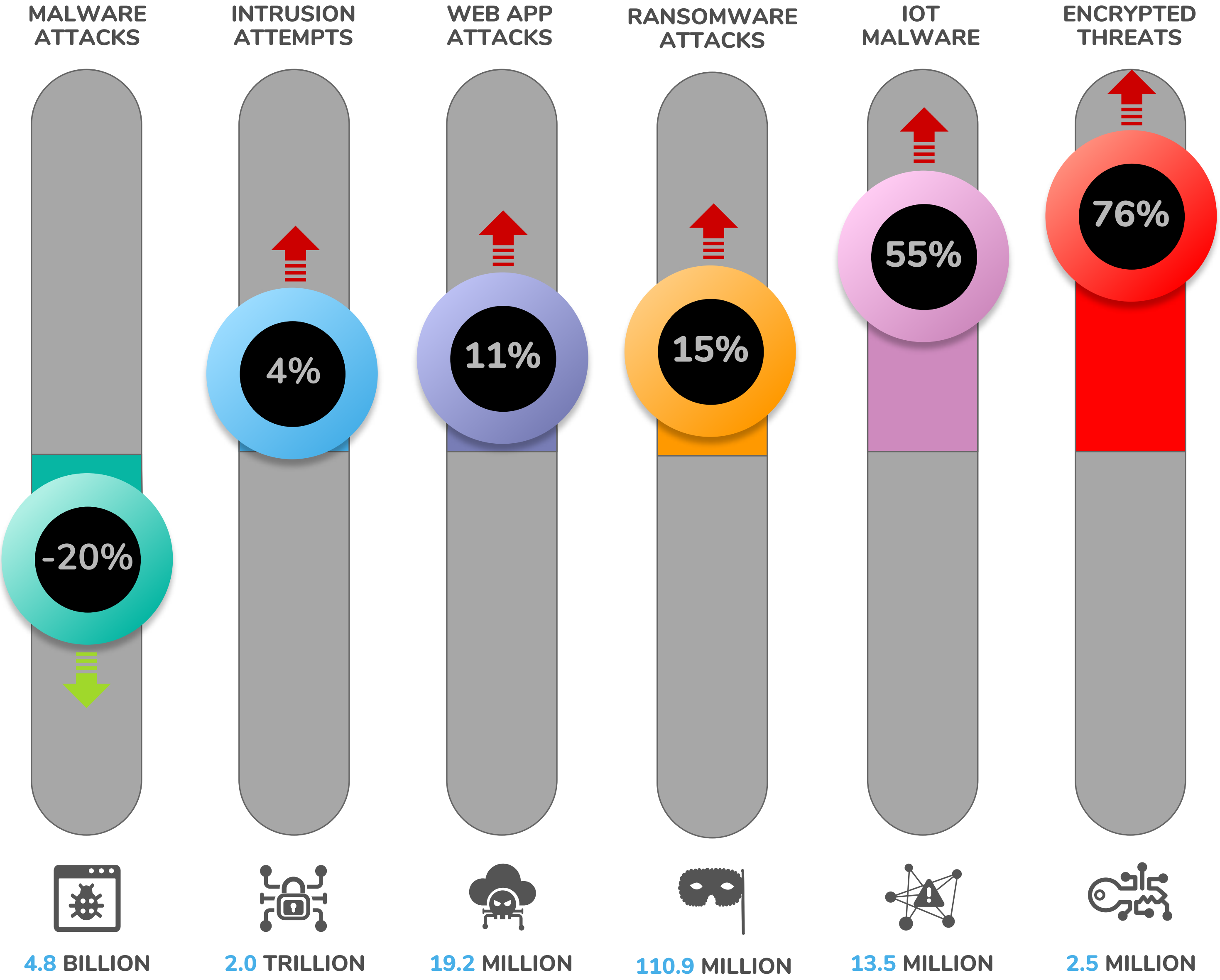
The speed and progression of the cyber arms race requires a constant, detailed and unwavering commitment to threat analysis.

In March, findings from the 2019 SonicWall Cyber Threat Report were published globally to empower businesses, SMBs, enterprises and government agencies with timely and actionable data to better defend their networks, applications and sensitive information.

To supplement that invaluable threat intelligence, SonicWall offers a complimentary mid-year update to review the attack volume, trends and techniques that defined the narrative for the first half of 2019.

This update expands on SonicWall's yearly malware and ransomware data, 'never-before-seen' threats, dangerous PDF and Office attacks, growing attacks across non-standard ports, spikes in cryptojacking signatures and more.

2019 GLOBAL CYBERATTACK TRENDS



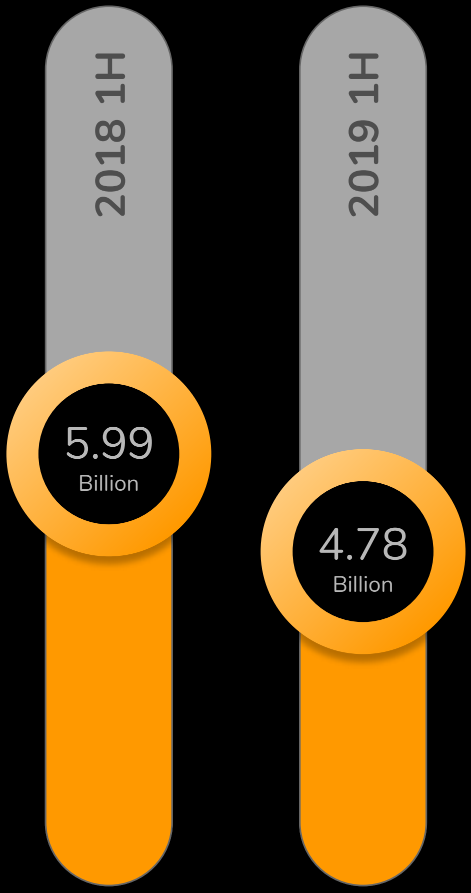
MALWARE DIPS AS OTHER ATTACK TYPES REBOUND

In 2018, global malware volume hit a record-breaking 10.52 billion attacks, the most ever recorded by SonicWall Capture Labs threat researchers.

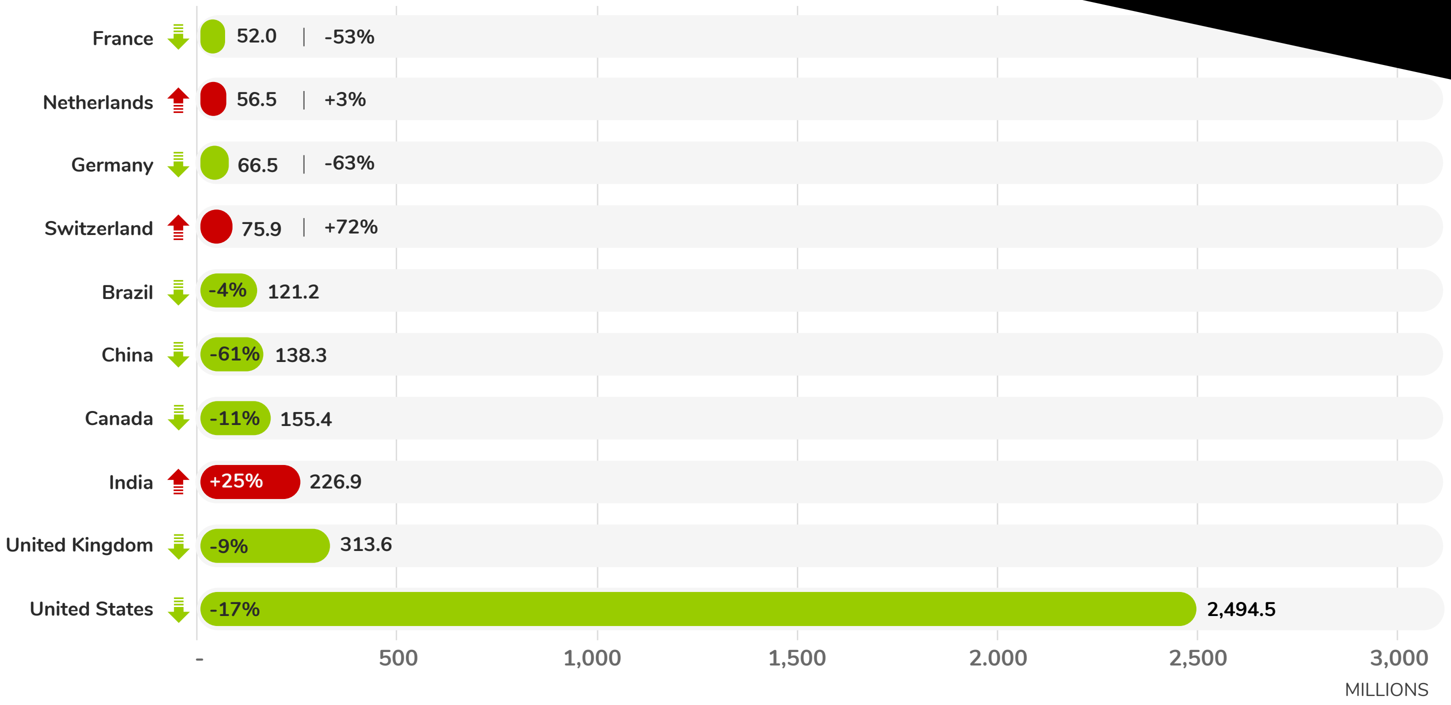
Fortunately, during the first six months of 2019, that trend slowed — at least somewhat. SonicWall recorded 4.8 billion* attacks, a 20% drop compared to the same time period last year.

These findings trended across major regions except a few countries: India (25%), Switzerland (72%) and the Netherlands (3%) were the top countries that suffered increased malware activity.

The United States (-17%) and United Kingdom (-9%) led the world in the amount of malware attacks faced, but total volume for both were down year to date compared to 2018.



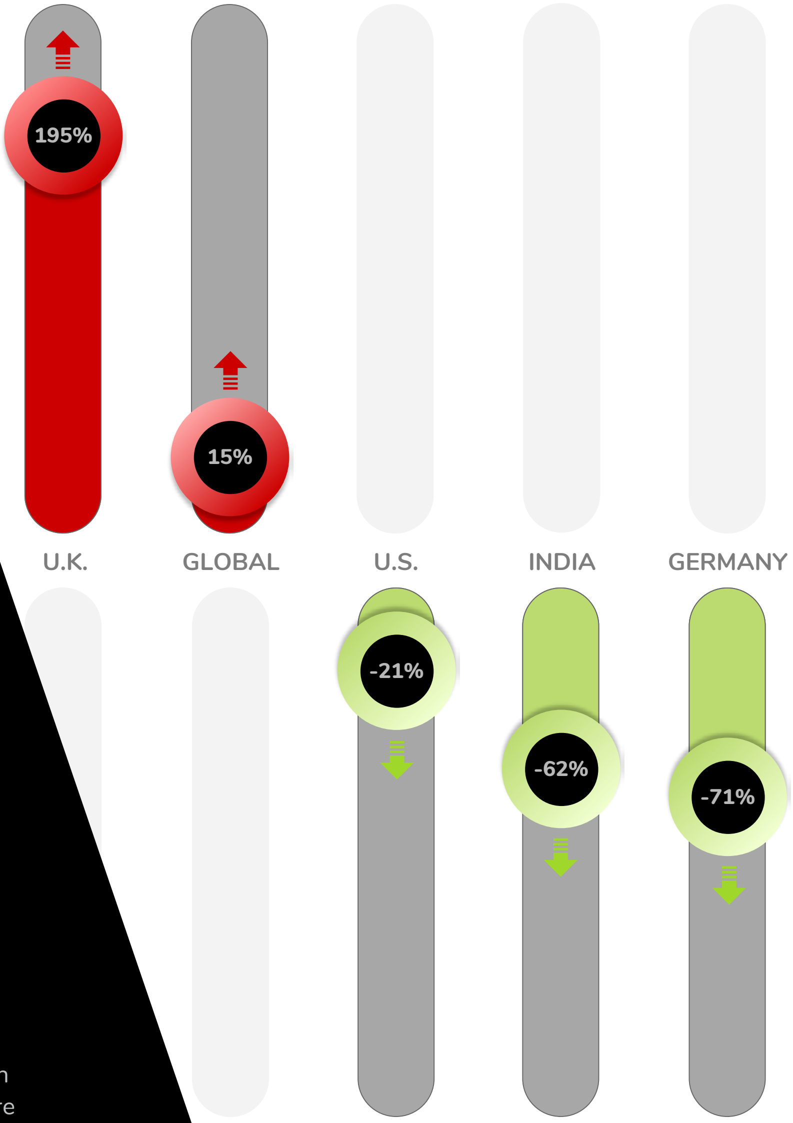
2019 MALWARE ATTACKS | TOP COUNTRIES



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

* 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.

2019 RANSOMWARE VOLUME



RaaS THE EXPLOIT KIT OF CHOICE IN 2019

Despite overall declines in malware volume, ransomware continues to pay dividends for cybercriminals. All told, global ransomware volume reached 110.9 million for the first half of 2019, a 15% year-to-date increase.

The most alarming ransomware data was sourced from the U.K. After enjoying a 59% decline in ransomware in 2018, the region saw ransomware volume jump 195% year-to-date for the first half of the year.

Globally, cybercriminals continue to pivot toward new tactics. Exclusive SonicWall data highlights an escalation in ransomware-as-a-service (RaaS) and open-source malware kits in the first half of 2019.

2018			2019		
FAMILY	VOLUME	TYPE	FAMILY	VOLUME	TYPE
Cerber	101.6 Million	RaaS	Cerber	39.5 Million	RaaS
BadRabbit	7.8 Million	Custom	Gandcrab	4.0 Million	RaaS
Dharma	7.3 Million	Custom	HiddenTear	4.0 Million	Open Source
LockyCrypt	6.1 Million	Custom	CryptoJoker	2.4 Million	Open Source
CryptoJoker	5.6 Million	Open Source	Locky	1.8 Million	Custom
Locky	2.4 Million	Custom	Dharma	1.5 Million	Custom
Petya	1.9 Million	Custom			

ATTACKS AGAINST NON-STANDARD PORTS STILL A CONCERN

Cybercriminals are seeing an unguarded entry point to your network. And they're lining up to get in.

As defined in the full **2019 SonicWall Cyber Threat Report**, 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.

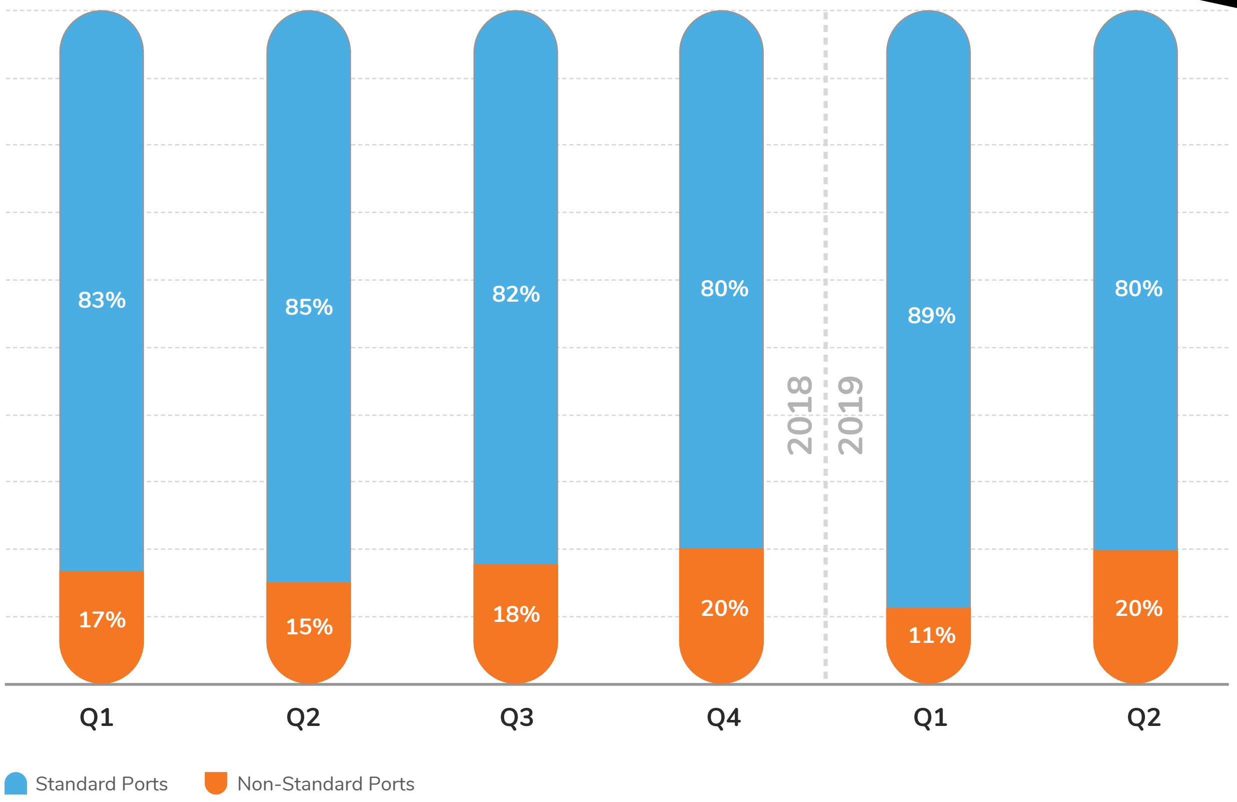
For example, Ports 80 and 443 are standard ports for web traffic, which is where most firewalls focus. But cybercriminals understand this too, so they are sending malware through non-standard port traffic to help deploy their payloads undetected in target environments.

At the close of 2018, more than 19.2% of all malware attacks (based off of a sampling of 700 million malware attacks) were coming across non-standard ports. For the first half of 2019, that share dipped to 13% globally due to below-normal volume in January (8%) and February (11%).

However, in May 2019, SonicWall monitored an alarming spike, when a quarter of all recorded malware attacks were coming across non-standard ports, the highest volume since Capture Labs has been tracking the attack vector.

SonicWall's non-standard port data is based on a sample size of more than 210 million malware attacks recorded worldwide through June 2019.

2018-2019 MALWARE ATTACKS

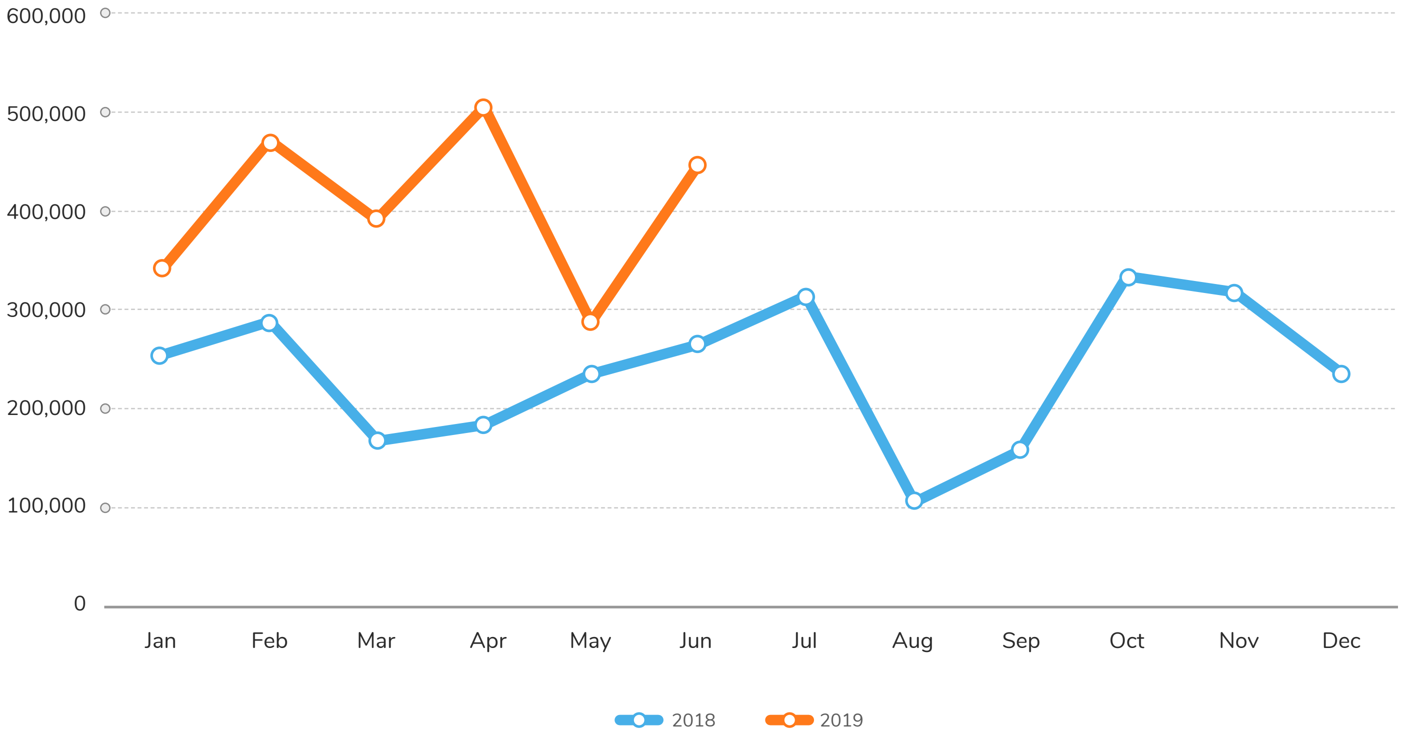


ENCRYPTED THREATS INTENSIFYING

In 2018, SonicWall logged more than 2.8 million encrypted malware attacks, which was already a 27% jump over the previous year. So far in 2019, that threat is only accelerating.

Through the first six months of 2019, SonicWall has registered 2.4 million encrypted attacks, almost eclipsing the 2018 full-year total in half the time. This marks a 76% year-to-date increase.

ENCRYPTED MALWARE ATTACKS



MACHINE LEARNING, MULTI-ENGINE SANDBOXES EVOLVING TO 'MUST-HAVE' SECURITY IN 2019

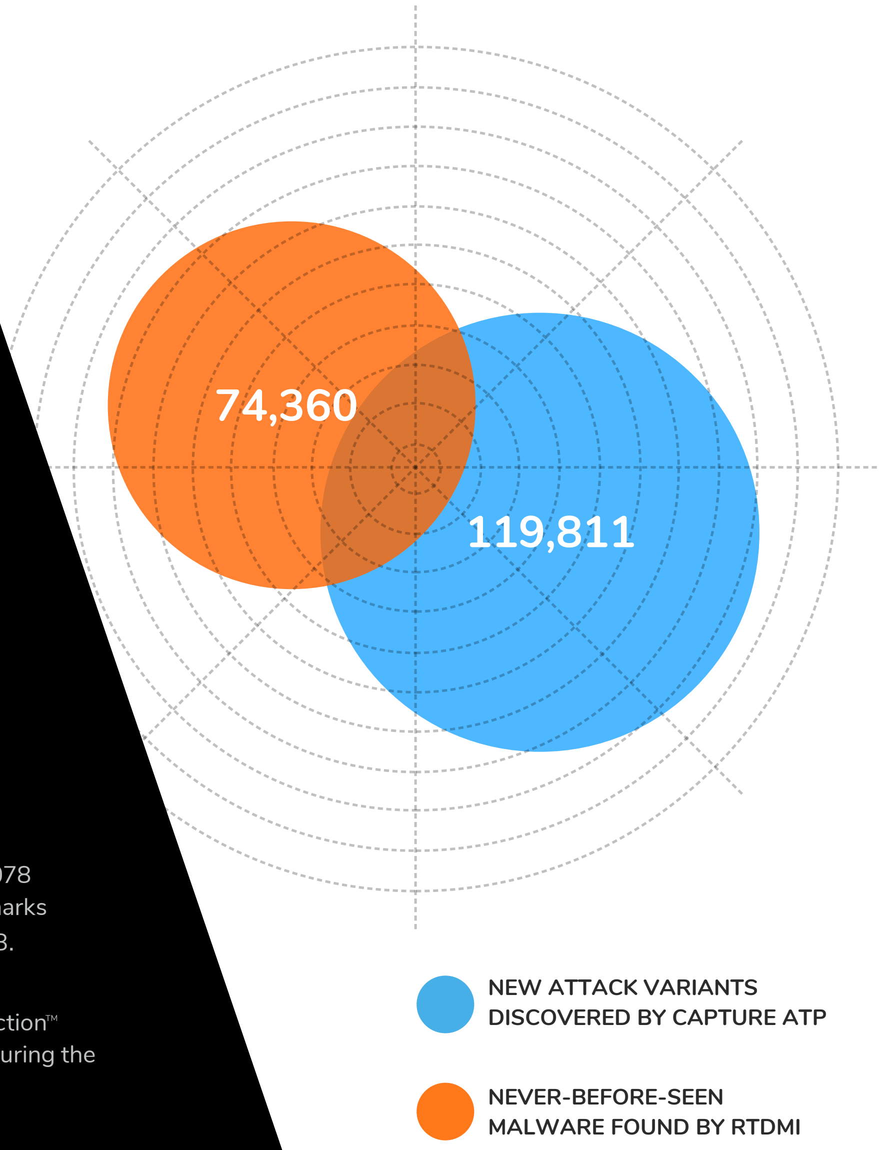
So far in 2019, the multi-engine SonicWall Capture Advanced Threat Protection (ATP) cloud sandbox has exposed 194,171 new malware variants — a pace of 1,078 new variant discoveries each day of the year. This also marks a rapid year-to-date increase of 45% compared to 2018.

But Capture ATP is only part of the story. Included with Capture ATP, SonicWall Real-Time Deep Memory Inspection™ unveiled 74,360 'never-before-seen' malware variants during the first half of the year.

74,360

Number of never-before-seen malware variants identified by SonicWall RTDMI™ so far in 2019.

NEW ATTACK VARIANTS DISCOVERED BY CAPTURE ATP



Interestingly, RTDMI also found numerous cases of unique variants that leveraged different forms of PDF file types to launch their exploits. Some examples include:

- **Scams & Frauds:** These PDF-based fraud campaigns include links to scam sites. These are not malware by definition, but very malicious and encourage users to visit seemingly "safe" websites. SonicWall Capture ATP with RTDMI detected and mitigated these new variants in real time.
- **Malicious URLs:** Attacks contained standard PDF files that include malicious links that download the next stage of a malicious Office file (or another level of misdirection). The final payload in this example is Emotet, a true malware.
- **Phishing:** These "phishing style" attacks offer a PDF with direct links to either malware downloads or phishing sites.

'ZERO-DAY' VS. 'NEVER-BEFORE-SEEN' ATTACKS

The 'zero-day attack' is one of the more mainstream security terms because of its connections to high-profile breaches. This type of attack is a completely new and unknown attack that targets a zero-day vulnerability that doesn't have any existing protections (e.g., patches, updates, etc.), usually from the target vendor or company.

Conversely, SonicWall tracks detection and mitigation of 'never-before-seen' attacks. These attacks mark the first time SonicWall Capture ATP identifies a signature/SHA256 as malicious. These discoveries often closely align with zero-day attack patterns due to the volume of attacks analyzed by SonicWall.

VIEW ATTACK DATA

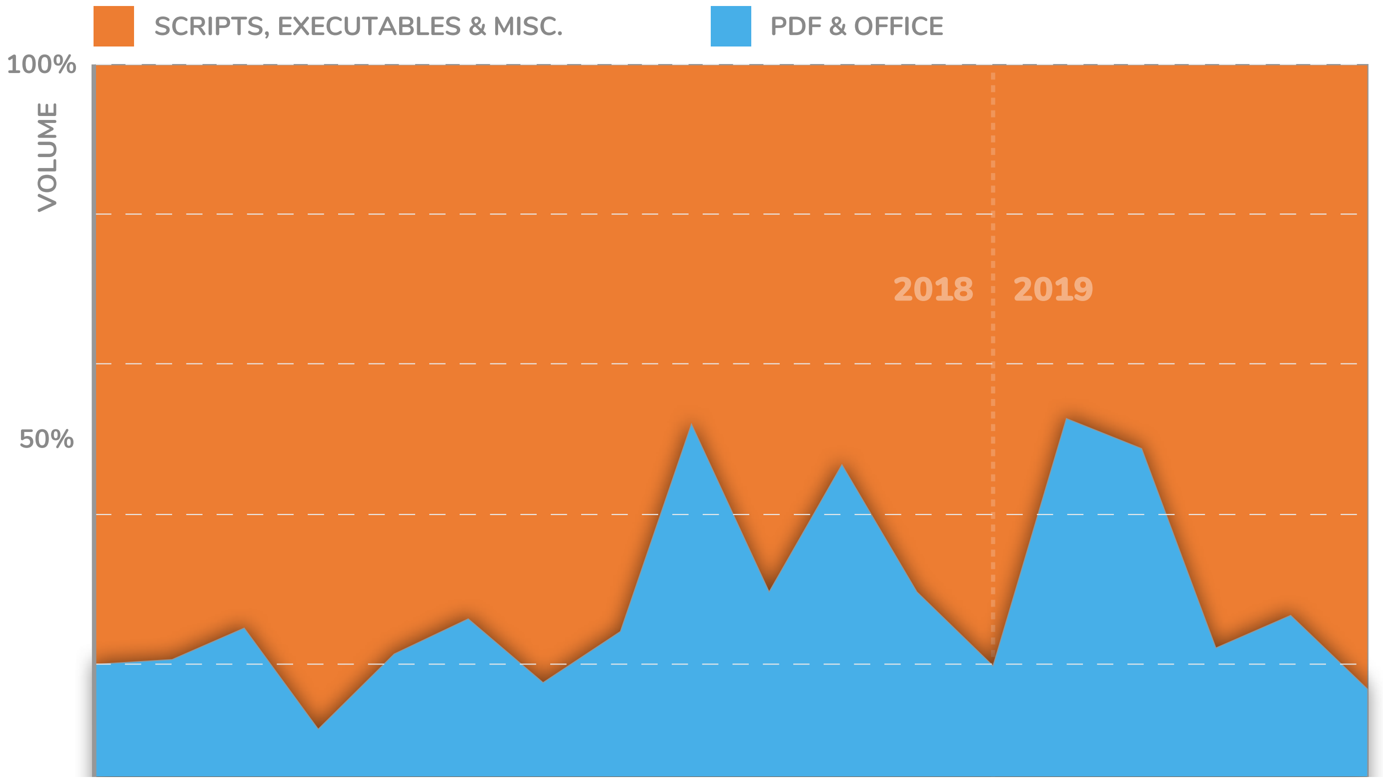
MALICIOUS PDFs, OFFICE FILES REMAIN DANGEROUS TO BUSINESSES

Traditional PDFs and Office files continue to be routinely leveraged to exploit users' trust and experience — particularly in office settings — to deliver malicious payloads.

While overall volume is relatively low, this sophisticated tactic is used to surgically defeat traditional firewalls and single-engine sandboxes.

The attack trends do, however, ebb and flow. In February and March 2019, SonicWall Capture Labs threat researchers found that 51% and 47% of 'never-before-seen' attacks, respectively, came via PDFs or Office files. Other months saw less volume, particularly compared to the spikes witnessed during the latter part of 2018.

PDF & OFFICE THREATS FOUND BY CAPTURE ATP IN 2019



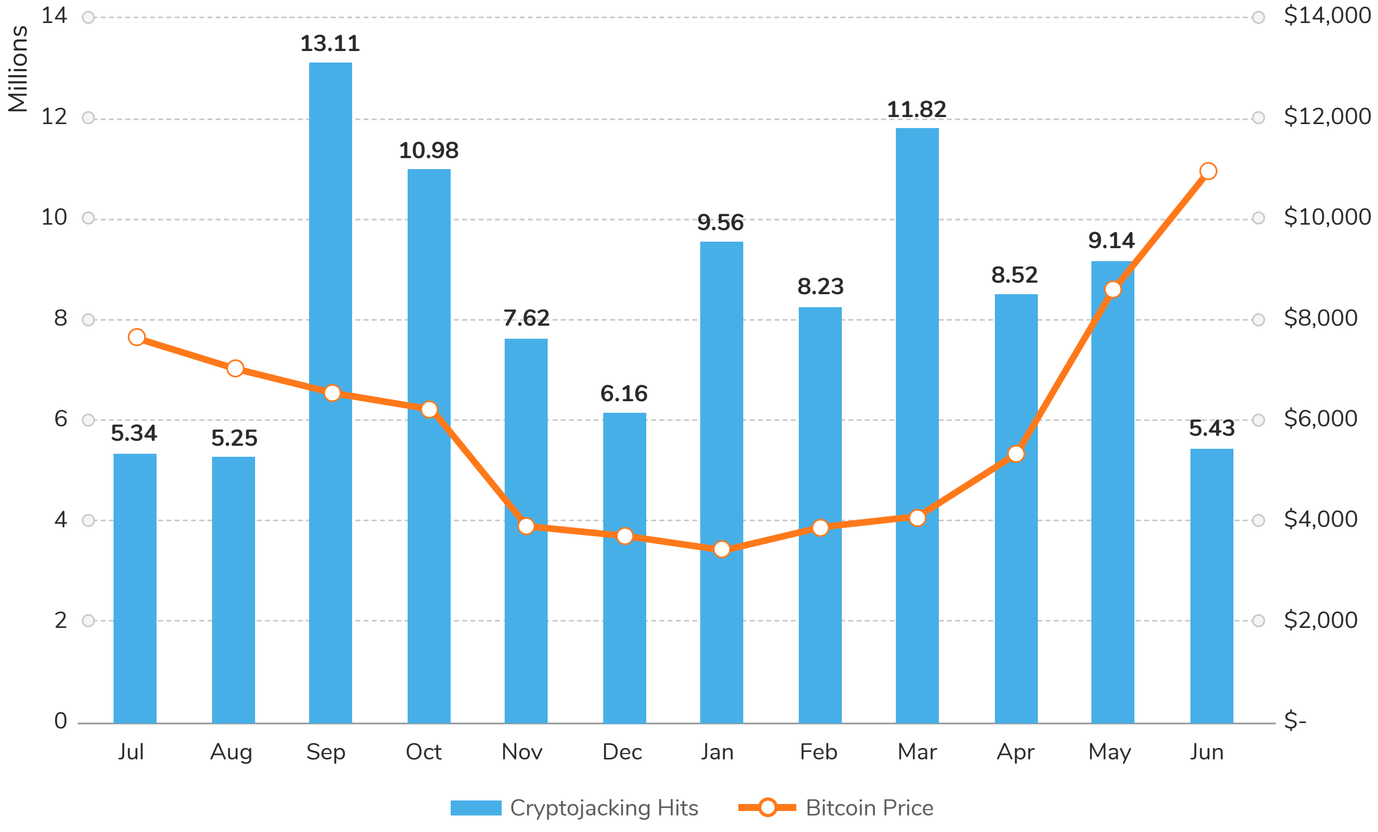
BITCOIN RUN KEEPING CRYPTOJACKING IN PLAY

In the closing months of 2018, cryptojacking volume began fading as prices for bitcoin and other cryptocurrencies fell. Cryptocurrency markets are fast-moving, where quick bull runs can cause dramatic price spikes. Bitcoin (BTC) prices also drive the value of Monero (XMR), which is the alt coin of choice for many cybercriminals.

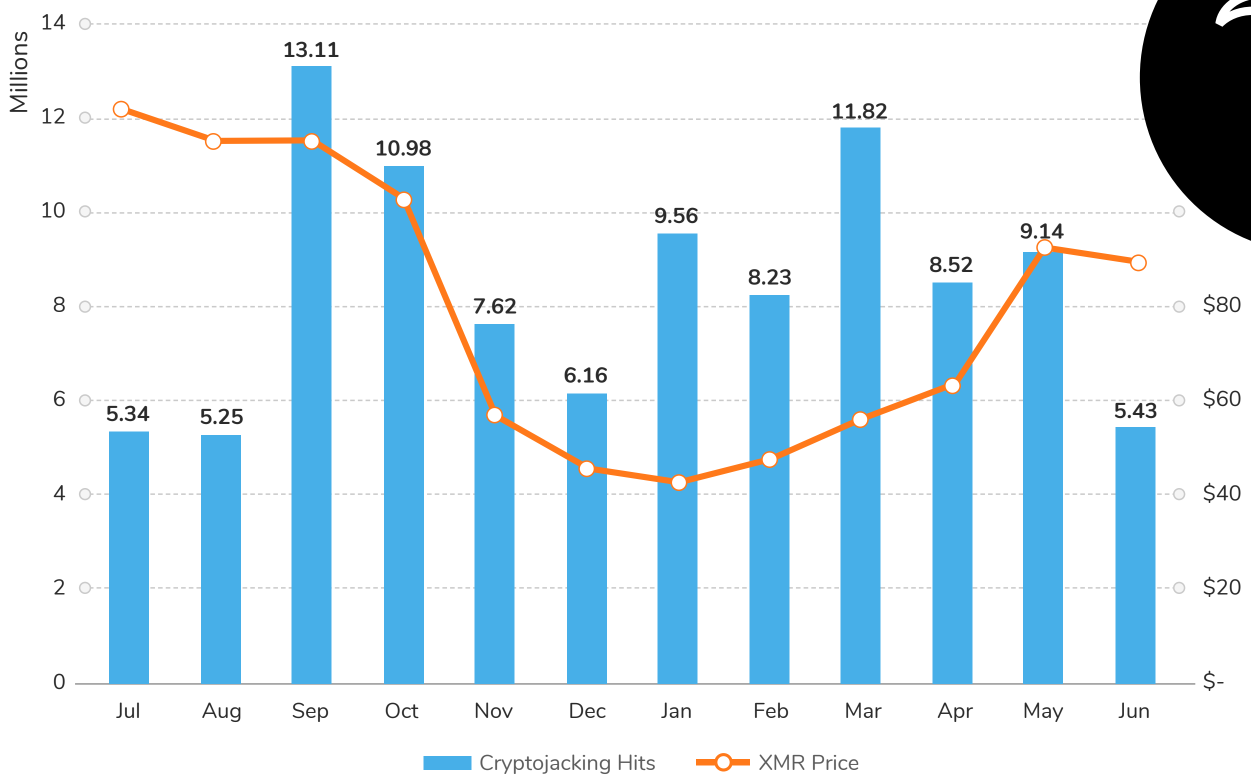
Halfway through 2019, bitcoin is surging again and is helping cryptojacking stay relevant as a lucrative option for cybercriminals. Cryptojacking volume hit 52.7 million for the first six months of the year, a 9% increase over the last six months of 2018.

Volume aside, it remains difficult to align cryptojacking attacks — and criminal intentions — with cryptocurrency value. For example, despite year-to-date highs for bitcoin prices in June, the month showed the lowest cryptojacking volume of the year.

CRYPTOJACKING VOLUME VS. BTC PRICE



CRYPTOJACKING VOLUME VS. XMR PRICE



Interestingly, Coinhive remains the top cryptojacking signature despite the service closing in March 2019. One reason for the high detection is that compromised websites have not been cleaned since the infection, even though the Coinhive service is non-existent and the URL has been abandoned.

This foundation, however, could potentially be used by malicious authors in the future. For example, they could conceivably register the Coinhive domain and reuse the URL left in the compromised websites. Another possibility is that cybercriminals are hoping Coinhive returns to reclaim the URL, making their Coinhive investments useable once again.

Facebook Libra Won’t Be Mined, But Caution Still Required

In June, Facebook announced its own cryptocurrency, Libra. Governed by the Libra Association, an independent, non-profit organization, Libra will theoretically give millions of global users instant access to cryptocurrency-based digital payments with almost no transaction fees and without the need for a traditional, centralized bank. This “easy access,” however, should come with caution, particularly with regards to security and privacy.

Because Libra will only be “minted” and released by the Libra Reserve, it can’t be mined like bitcoin or Monero. This likely means that Libra won’t be used in traditional cryptojacking attacks. That said, if there’s money to be made, cybercriminals will find a way. Once Libra launches in 2020, SonicWall expects many of the early exploits to focus on social engineering and other online scams that will attempt to manipulate users into sending Libra (via the complementary Calibra digital wallet) on a number of supported applications, including Facebook, Facebook Messenger, WhatsApp, etc.

TOP 10 CRYPTOJACKING SIGNATURES

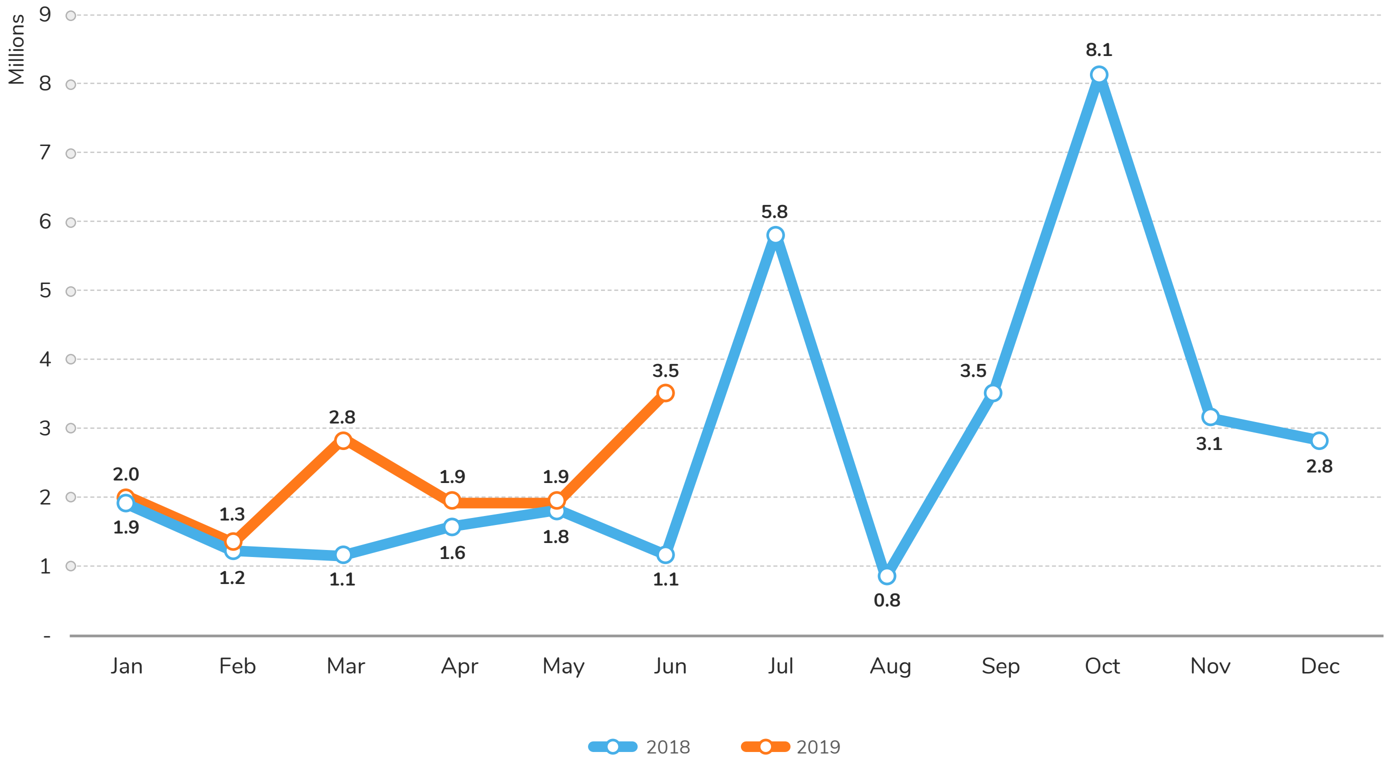
Signature	Hits
Coinhive.JS_2	33,711,537
XMRig.XMR_11	5,403,673
CoinHive.JS	3,916,250
XMRig.XMR_3	3,911,034
XMRig.XMR_4	1,723,487
Minerd.LC	947,773
BitMiner.KJ_2	843,222
XmrMiner.A	174,438
CoinMiner.A_30	128,117
BitCoinMiner.IY	46,640

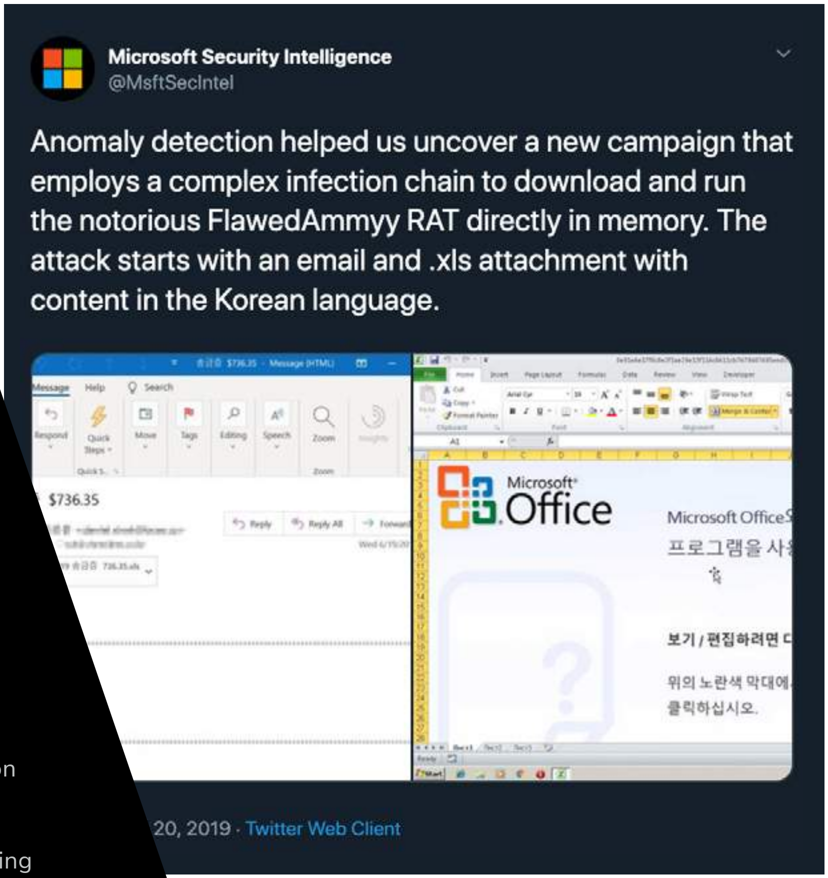
IoT MALWARE SURGING PAST RECORD 2018 VOLUME

The speed and ferocity in which IoT devices are being compromised to deliver malware payloads is alarming. In 2017, SonicWall logged just 10.3 million IoT attacks. Last year, that number skyrocketed 215.7% to 32.7 million.

In the first half of 2019, SonicWall Capture Labs threat researchers have already recorded 13.5 million IoT attacks, which outpaces the first two quarters of last year by 55%. If the final six months of 2019 match the surge of 2018, it will be another record year for cybercriminals' use of IoT malware.

GLOBAL IoT MALWARE





Microsoft Security Intelligence
@MsftSecIntel

Anomaly detection helped us uncover a new campaign that employs a complex infection chain to download and run the notorious FlawedAmmyy RAT directly in memory. The attack starts with an email and .xls attachment with content in the Korean language.

20, 2019 · Twitter Web Client

NEW PHISHING CAMPAIGN, MALWARE EXPLOIT OFFICE MACROS

In late June, Microsoft Security Intelligence announced that anomaly detection capabilities identified a new and complex attack that leverages various layers of deception to deploy an infamous remote access trojan (RAT).

The complex infection chain begins with a Korean phishing email that includes an *.xls* attachment and concludes with an MSI archive file extracting a series of executables before the *FlawedAmmyy RAT* malware is deployed.

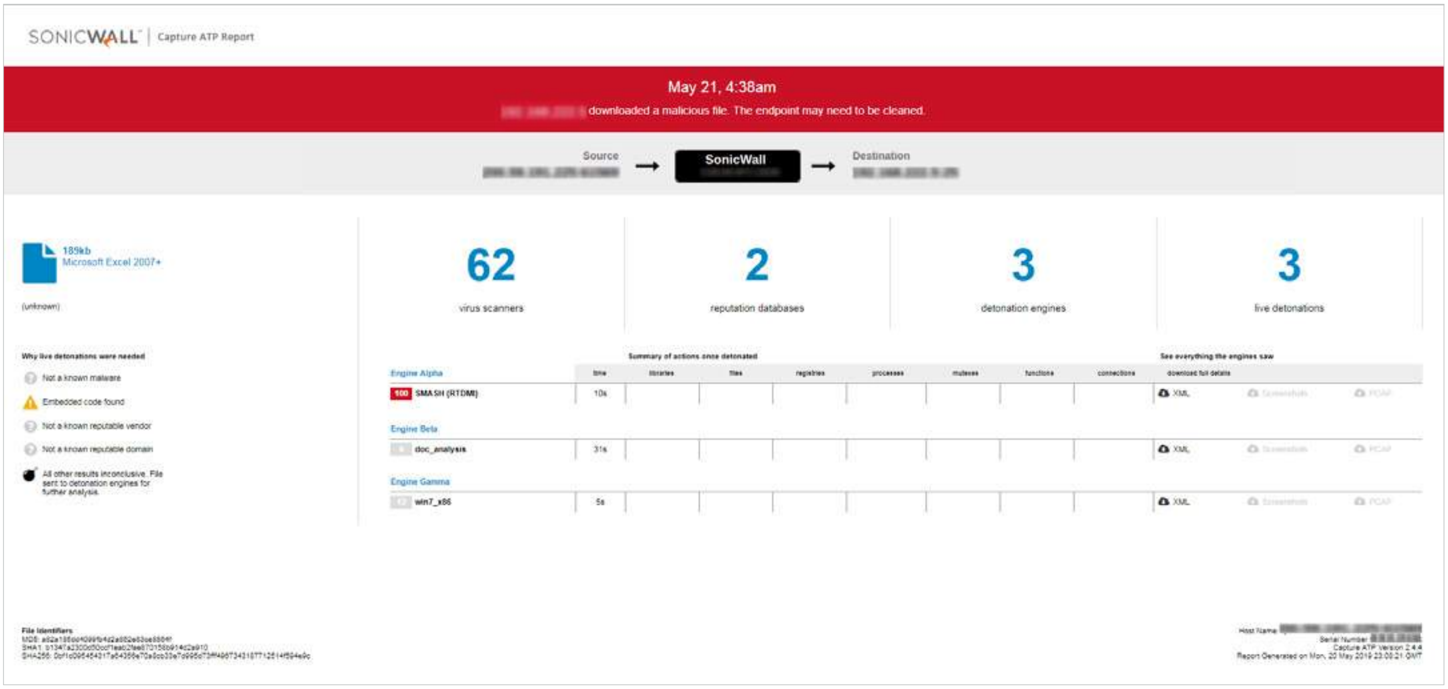
“When opened, the *.xls* file automatically runs a macro function that runs *msiexec.exe*, which in turn downloads an MSI archive,” Microsoft Security Intelligence stated on Twitter. “The MSI archive contains a digitally signed executable that is extracted and run, and that decrypts and runs another executable in memory.”

SonicWall Capture Labs threat researchers confirmed that variants of the attack download a fraudulent file called wsus.exe, which masquerades as a legitimate Microsoft Windows Service Update Service (WSUS).

Beginning May 20, SonicWall Real-Time Deep Memory Inspection™ — a component of the Capture ATP sandbox service — detected multiple variants of the threat in the wild.

These examples used Korean and English phishing attacks and malicious Excel and Word attachments. (SonicWall Capture ATP customers were protected automatically from all variants of this threat.)

Microsoft confirmed that Microsoft Defender ATP blocked the attack, including the *FlawedAmmyy RAT* malware, and Microsoft Office 365 ATP detected the dangerous phishing campaign.



SONICWALL | Capture ATP Report

May 21, 4:38am

[redacted] downloaded a malicious file. The endpoint may need to be cleaned.

Source [redacted] → SonicWall [redacted] → Destination [redacted]

189kb
Microsoft Excel 2007+

(unknown)

62	2	3	3
virus scanners	reputation databases	detonation engines	live detonations

Why live detonations were needed

- Not a known malware
- ⚠ Embedded code found
- Not a known reputable vendor
- Not a known reputable domain
- All other results inconclusive. File sent to detonation engines for further analysis.

	Summary of actions once detonated								See everything the engines saw		
	time	libraries	files	registries	processes	mutexes	functions	connections	download full details		
Engine Alpha											
100 SMASH (RTDMI)	10s								XML	Screenshots	PCAP
Engine Beta											
[illegible] doc_analysis	31s								XML	Screenshots	PCAP
Engine Gamma											
[illegible] win7_x86	5s								XML	Screenshots	PCAP

File Identifiers
MD5: a92a185dd4099fb4d2a882e83ce8864f
SHA1: 61347a2300d50ccf1eab2fee87015bb914d2a910
SHA256: 0cf1c095454317a64356e70a8cb33e7d995c73ff4967343187712514f594e9c

Host Name [redacted]
Serial Number [redacted]
Capture ATP Version 2.4.4
Report Generated on Mon, 20 May 2019 23:09:21 GMT

SonicWall Capture ATP with RTDMI™ detected multiple variants of the complex threat that exploits macros in Microsoft Office files, notably Excel and Word.

‘WIPER’ ATTACKS HEADLINE NATION-STATE PHISHING CAMPAIGNS

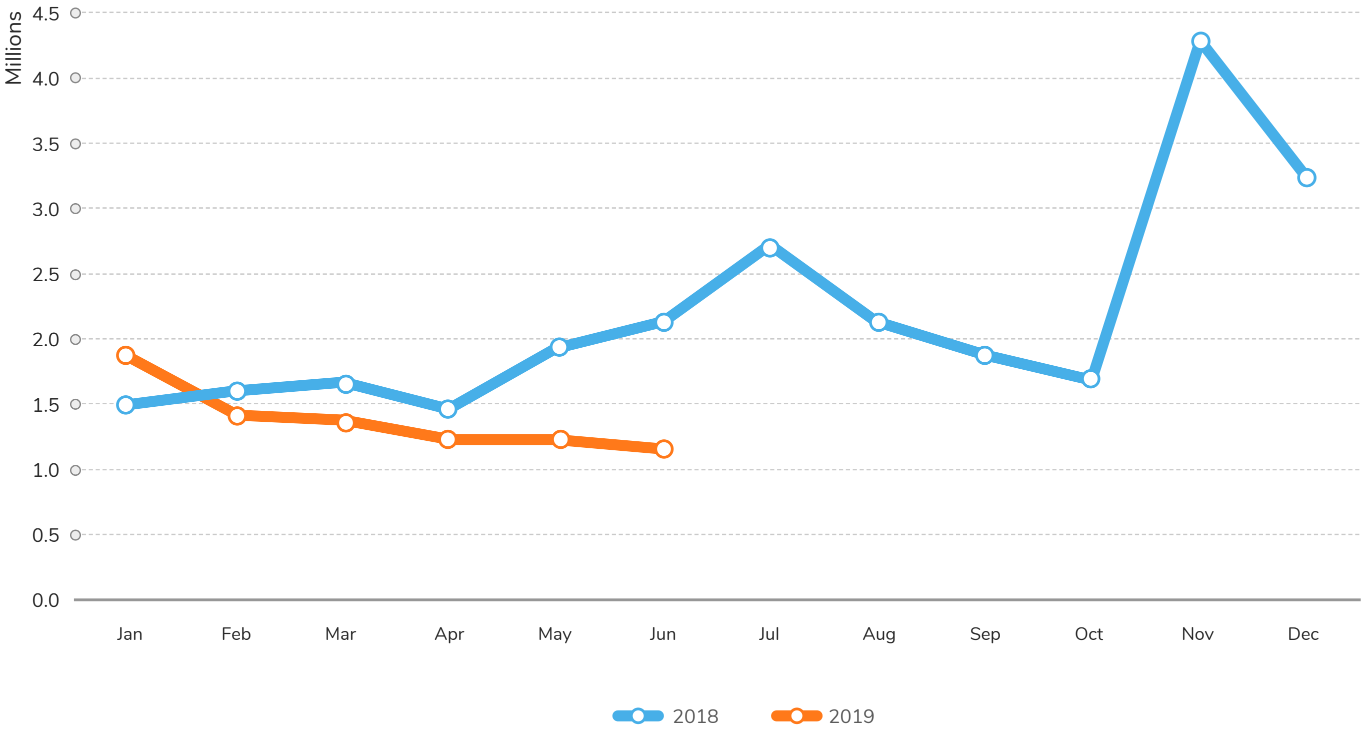
Overall, global phishing attacks are down to start 2019. But that isn’t a strong indicator that the attack vector is any less risky.

Through June 2019, overall phishing volume is down 19% year-to-date compared to 2018. There is time for the threat to rebound, unfortunately. Seasonal spikes last July, November and December accounted for 39% of the yearly attacks, further signifying that cybercriminals are systematically launching phishing campaigns to align with high-traffic months, particularly in North America.

But hard data only tells part of the story. On June 22, the U.S. Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued a public warning about ‘Wiper’ attacks coming from Iran.

“Iranian regime actors and proxies are increasingly using destructive ‘wiper’ attacks, looking to do much more than just steal data and money,” said CISA Director Christopher C. Krebs in the official statement. “These efforts are often enabled through common tactics like spear phishing, password spraying, and credential stuffing. What might start as an account compromise, where you think you might just lose data, can quickly become a situation where you’ve lost your whole network.”

GLOBAL PHISHING VOLUME



ABOUT THE SONICWALL CAPTURE LABS THREAT NETWORK

Intelligence for the mid-year update to 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

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.

2019ThreatReport-MidYearUpdate-KJ-447

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®