SONICWALL

SonicWall Cyber Threat Report Illustrates Intense Cyber Arms Race; Cyber Attacks Becoming No. 1 Business Risk

- *9.32 billion total malware attacks in 2017, an 18.4 percent year-over-year increase*
- *Ransomware attacks dropped from 638 million to 184 million between 2016 and 2017*
- *Ransomware variants, however, increased 101.2 percent*
- *Average organization will see almost 900 file-based attacks per year hidden by SSL/TLS encryption*

PRESS RELEASE – March 6, 2018

MILPITAS, Calif. – SonicWall, the trusted security partner protecting more than 1 million networks worldwide, announces research and intelligence from its 2018 Cyber Threat Report. In sum, the company recorded 9.32 billion malware attacks in 2017 and saw more than 12,500 new Common Vulnerabilities and Exposures (CVE) reported for the year.

“The cyber arms race affects every government, business, organization and individual. It cannot be won by any one of us,” said SonicWall CEO Bill Conner. “Our latest proprietary data and findings show a series of strategic attacks and countermeasures as the cyber arms race continues to escalate. By sharing actionable intelligence, we collectively improve our business and security postures against today’s most malicious threats and criminals.”

The annual threat report frames, compares and contrasts advances made by both cybersecurity professionals and global cybercriminals.

- Cyber attacks are becoming the No. 1 risk to business, brands, operations and financials
- 9.32 billion total malware attacks in 2017, an 18.4 percent year-over-year increase from 2016
- Ransomware attacks dropped from 638 million to 184 million between 2016 and 2017
- Ransomware variants, however, increased 101.2 percent
- Traffic encrypted by SSL/TLS standards increased 24 percent, representing 68 percent of total traffic
- Without SSL decryption capabilities in place, the average organization will see almost 900 attacks per year hidden by SSL/TLS encryption
- SonicWall identifies almost 500 new previously unknown malicious files each day

“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,” said Conner.

Security Industry Advances

Total ransomware attack volume declines.
Even with WannaCry, Petya, NotPetya and Bad Rabbit ransomware attacks stealing the headlines, the expectations of more ransomware attacks simply did not materialize as anticipated in 2017. Full-year data shows that ransomware attacks dropped from 638 million to 184 million between 2016 and 2017.

- Volume 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 37 percent of ransomware attacks in 2017
- SonicWall Capture Advanced Threat Protection (ATP), a cloud-based, multi-engine sandbox, identified one new malware variant for every 250 unknown hits

SSL/TLS use increases again.
Web traffic encrypted by SSL/TLS standards made yet another significant jump in 2017. This shift has already given more opportunity for cybercriminals and threat actors to hide malicious payloads in encrypted traffic.

- Encrypted SSL/TLS traffic increased 24 percent
- SSL/TLS traffic made up 68 percent of total traffic in 2017
- Organizations are beginning to implement security controls, such as deep packet inspection (DPI) of SSL/TLS traffic, to responsibly inspect, detect and mitigate attacks in encrypted traffic

Effectiveness of exploit kits impacted.
With most browsers dropping support of Adobe Flash, no critical flash vulnerabilities were discovered in 2017. That, however, hasn't deterred threat actors from attempting new strategies.

- SonicWall provided protection against Microsoft Edge attacks, which we observed grew 13 percent in 2017 over 2016
- SonicWall also protects the most popular Adobe products — Acrobat, Acrobat DC, Reader DC and Reader — and we observed attacks against these applications were down across the board
- New targeted applications (e.g., Apple TV, Microsoft Office) cracked SonicWall's top 10 for the first time

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.

- Law enforcement agencies are making an impact by arresting and convicting malware authors and disruptors

- Cybercriminals are being more careful with how they conduct business, including dynamic cryptocurrency wallets and using different transaction currencies

- Cooperation between national and international law enforcement agencies is strengthening the disruption of global cyber threats

“Stabilizing the cyber arms race requires the responsible, transparent and agile collaboration between governments, law enforcement and the private sector,” said the Honorable Michael Chertoff, Chairman of the Chertoff Group, and former U.S. Secretary of Homeland Security. “Like we witnessed in 2017, joint efforts deliver a hard-hitting impact to cybercriminals and threat actors. This diligence helps disrupt the development and deployment of advanced exploits and payloads, and also deters future criminals from engaging in malicious activity against well-meaning organizations, governments, businesses and individuals.”

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 created continues an upward trend since 2015. The variant increase, coupled with the associated volume of 184 million attacks, leaves ransomware a prevelant threat.

- Ransomware variants increased 101.2 percent in 2017

- SonicWall Capture Labs threat researchers created 2,855 new unique ransomware signatures in 2017, up from the 1,419 published in 2016

- Ransomware against IoT and mobile devices is expected to increase in 2018

SSL encryption still hiding cyber attacks.
Hackers and cybercriminals continued to encrypt their malware payloads to circumvent traditional security controls. For the first time ever, SonicWall has real-world data that unmasks the volume of malware and other exploits hidden in encrypted traffic.

- Encryption was leveraged more than previous years, for both legitimate traffic and malicious payload delivery

- SonicWall Capture Labs found, on average, 60 file-based malware propagation attempts per SonicWall firewall each day

- Without SSL decryption capabilities in place, the average organization will see almost 900 file-based attacks per year hidden by TLS/SSL encryption

“Industry reports indicate as high as 41% of attack or malicious traffic now leverages encryption for obfuscation, which means that traffic analysis solutions and web transaction solutions such as secure web gateways each must support the ability to decrypt SSL traffic to be effective,” wrote Ruggero Contu and Lawrence Pingree of Gartner.*

Malware cocktails mixing things up.

While no single exploit in 2017 rose to the level of darknet hacker tools 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. SonicWall Capture Labs uses machine-learning technology to examine individual malware artifacts and categorizes each as unique or as a malware that already exists.

- SonicWall collected 56 million unique malware samples in 2017, a slight 6.7 percent decrease from 2016

- Total volume of unique malware samples in 2017 was 51.4 percent higher than 2014

Chip processors, IoT are emerging battlegrounds.
Cybercriminals are pushing new attack techniques into advanced technology spaces, notably chip processors.

- Memory regions are the next key battleground that organizations will battle over with cybercriminals

- 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

- 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

"Sandbox techniques are often ineffective when analyzing the most modern malware," said SonicWall CTO John Gmuender. "Real-time deep memory inspection is very fast and very precise, and can mitigate sophisticated attacks where the malware's most protected weaponry is exposed for less than 100 nanoseconds."

In addition to these findings, the 2018 SonicWall Annual Threat Report also identified best practices and security predictions for 2018, which are discussed in detail in the full report. To download the complete report, please visit **www.sonicwall.com/ThreatReport.**

For current cyber attack data, visit the **SonicWall Security Center** to see latest attack trends, types and volume across the world.

*Gartner, "Competitive Landscape: Secure Web Gateways," Ruggero Contu, Lawrence Pingree, 12 September 2017.

About the SonicWall Capture Threat Network
Data for the 2018 SonicWall Cyber Threat Report was 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, endpoint security, honeypots, content-filtering systems; SonicWall Capture Advanced Threat Protection multi-engine sandbox; and SonicWall's internal malware analysis automation framework.

For More Information
To learn more about opportunities to partner with SonicWall, please visit:

- **SonicWall on Twitter**
- **SonicWall on Facebook**
- **SonicWall on LinkedIn**

About SonicWall
SonicWall has been fighting the cyber-criminal industry for over 26 years defending small, medium-size businesses and enterprises worldwide. Backed by research from SonicWall Capture Labs, our award-winning real-time breach detection and prevention solutions coupled with the formidable resources of over 21,000 loyal channel partners around the globe, are the backbone securing more than a million business and mobile networks and their emails, applications, and data. This combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 150 countries. These businesses can run more effectively and fear less about security. For more information, visit www.sonicwall.com.