PRESS RELEASE

SonicWall Annual Threat Report Highlights Advances Made by Both Security Professionals and Cyber Criminals

- *The volume of unique malware samples declined to 60 million, a 6.25 percent decrease.*
- *Point-of-sale malware creation declined by 93 percent since 2014.*
- *Secure Sockets Layer/Transport Layer Security encrypted traffic increased by 38 percent year-over-year.*
- *Cyber criminals shifted their focus to new threats, including ransomware attacks which grew by 167x year-over-year.*
- *Internet of Things devices created a new attack vector, opening the door for large scale distributed denial-of-service attacks.*

SANTA CLARA, Calif. — SonicWall, the trusted security partner protecting more than a million business networks worldwide, today announced findings from its Annual Threat Report, which highlights the most notable advancements made by security professionals and cyber criminals in 2016. The report was compiled from data collected throughout 2016 by the SonicWall Global Response Intelligence Defense (GRID) Threat Network with daily feeds from more than 1 million security sensors in nearly 200 countries and territories.

According to the 2017 SonicWall Annual Threat Report, 2016 could be considered a highly successful year from the perspective of both security professionals and cyber criminals. Unlike in years past, SonicWall saw the volume of unique malware samples collected fall to 60 million compared with 64 million in 2015, a 6.25 percent decrease. Total malware attack attempts dropped for the first time in years to 7.87 billion from 8.19 billion in 2015. However, cyber criminals garnered quick payoffs from ransomware, fueled partly by the rise in ransomware-as-a-service (RaaS).

“It would be inaccurate to say the threat landscape either diminished or expanded in 2016 — rather, it appears to have evolved and shifted,” said Bill Conner, president and CEO of SonicWall. “Cybersecurity is not a battle of attrition; it’s an arms race, and both sides are proving exceptionally capable and innovative.”

Security Industry Advances

Point-of-sale malware attacks declined by 93 percent from 2014 to 2016.

High-profile retail breaches in 2014 led to companies adopting more proactive security measures. Since then, the industry has seen the implementation of chip-based POS systems, usage of the Payment Card Industry Data Security Standard (PCI-DDS) checklist and other ongoing security measures.

- Back in 2014, the SonicWall GRID Threat Network observed a 333 percent increase in the number of new POS malware countermeasures developed and deployed compared with the year prior.

- The SonicWall GRID Threat Network saw the number of new POS malware variants decrease by 88 percent year-over-year and 93 percent since 2014. This implies that cyber criminals are becoming less interested in devoting time to POS malware innovation.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) encrypted traffic grew by 38 percent, partly in response to growing cloud application adoption.

The trend toward SSL/TLS encryption has been on the rise for several years. As web traffic grew throughout 2016, so did SSL/TLS encryption, from 5.3 trillion web connections in 2015 to 7.3 trillion in 2016 according to the SonicWall GRID Threat Network.

- The majority of web sessions that the SonicWall GRID Threat Network detected throughout the year were SSL/TLS-encrypted, comprising 62 percent of web traffic.

- One reason for the increase in SSL/TLS encryption is the growing enterprise appetite for cloud applications. The SonicWall GRID Threat Network has seen cloud application total usage grow from 88 trillion in 2014 and 118 trillion in 2015 to 126 trillion in 2016.

While this trend toward SSL/TLS encryption is overall a positive one, it also merits a word of caution. SSL/TLS encryption makes it more difficult for cyber thieves to intercept payment information from consumers, but it also provides an uninspected and trusted backdoor into the network that cyber criminals can exploit to sneak in malware. The reason this security measure can become an attack vector is that most companies still do not have the right infrastructure in place to perform deep packet inspection (DPI) in order to detect malware hidden inside of SSL/TLS-encrypted web sessions.

Dominant exploit kits Angler, Nuclear and Neutrino disappeared in mid-2016.
As 2016 began, the malware market was dominated by a handful of exploit kits, particularly Angler, Nuclear and Neutrino. Following the arrest of more than 50 Russian hackers for leveraging the Lurk Trojan to commit bank fraud, the SonicWall GRID Threat Network saw the Angler exploit kit suddenly stop appearing, leading many to believe Angler’s creators were among those arrested.[i] For a while following Angler’s disappearance, Nuclear and Neutrino saw a surge in usage, before quickly fading out as well.

- The SonicWall GRID Threat Network noticed the remaining exploit kits began to fragment into multiple, smaller versions to fill this void. By the third quarter of 2016, Rig had evolved into three versions leveraging different URL patterns, landing page encryption and payload delivery encryption.

- As with spam and other distribution methods in 2016, SonicWall saw exploit kits become part of the ransomware delivery machine, making variants of Cerber, Locky, CrypMIC, BandarChor, TeslaCrypt and others their primary payloads throughout the year. However, exploit kits never recovered from the massive blow they received early in the year with the takedown of their dominant families.

Cyber Criminal Advances

Ransomware usage grew by 167x year-over-year and was the payload of choice for malicious email campaigns and exploit kits.
The SonicWall GRID Threat Network detected an increase from 3.8 million ransomware attacks in 2015 to an astounding 638 million in 2016. The rise of RaaS made ransomware significantly easier to obtain and deploy. The unprecedented growth of the malware was likely driven as well by easier access in the underground market, the low cost of conducting a ransomware attack, the ease of distributing it and the low risk of being caught or punished.

- Ransomware remained on an upward climb throughout the year, beginning in March 2016 when ransomware attack attempts shot up from 282,000 to 30 million over the course of the month, and continuing through the fourth quarter, which closed at 266.5 million ransomware attack attempts for the quarter.

- The most popular payload for malicious email campaigns in 2016 was ransomware, typically Locky, which was deployed in about 90 percent of Nemucod attacks and more than 500 million total attacks throughout the year.

- No industry was spared from ransomware attack attempts. Industry verticals were targeted almost equally, with the mechanical and industrial engineering industry reaping 15 percent of average ransomware hits, followed by a tie between pharmaceuticals (13 percent) and financial services (13 percent), and real estate (12 percent) in third place.

Internet of Things devices were compromised on a massive scale due to poorly designed security features, opening the door for distributed denial-of-service attacks.
With their integration into the core components of our businesses and lives, IoT devices provided an enticing attack vector for cyber criminals in 2016. Gaps in IoT security enabled cyber thieves to launch the largest

distributed denial-of-service (DDoS) attacks in history in 2016, leveraging hundreds of thousands of IoT devices with weak telnet passwords to launch DDoS attacks using the Mirai botnet management framework.

- The SonicWall GRID Threat Network observed vulnerabilities on all categories of IoT devices, including smart cameras, smart wearables, smart homes, smart vehicles, smart entertainment, and smart terminals.

- During the height of the Mirai surge in November 2016, the SonicWall GRID Threat Network observed that the United States was by far the most targeted, with 70 percent of DDoS attacks directed towards the region, followed by Brazil (14 percent) and India (10 percent).[ii]

Android^{TM} devices saw increased security protections but remained vulnerable to overlay attacks. Google worked hard in 2016 to patch the vulnerabilities and exploits that cyber criminals have used against Android in the past, but attackers used novel techniques to beat these security improvements.[iii,iv]

- The SonicWall GRID Threat Network observed cyber criminals leveraging screen overlays to mimic legitimate app screens and trick users into entering login info and other data. When Android responded with new security features to combat overlays, SonicWall observed attackers circumventing these measures by coaxing users into providing permissions that allowed overlays to still be used.[v]

- Compromised adult-centric apps declined on Google Play but cybercriminals continued to find victims on third-party app stores. Ransomware was a common payload as were self-installing apps. The SonicWall GRID Threat Network observed more than 4,000 distinct apps with self-installing payloads in a matter of two weeks.[vi,vii]

This 2017 SonicWall Annual Threat Report also identified best practices and security predictions for 2017, which are discussed in detail in the report. To learn more, please visit:

- 2017 SonicWall Annual Threat Report
- Threat Report Blog by SonicWall President and CEO Bill Conner

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

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

About SonicWall
Over a 25-year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall customers can confidently say yes to the future.

HK Distributor
Data World Computer & Communication Ltd
Hotline: 2565 8733
Enquiry email: marketing@dataworld.com.hk
Website: http://dwcc.dataworld.com.hk/

[i] Kevin Townsend, "Did Angler Exploit Kit Die with Russian Lurk Arrests?" Security Week, June 13, 2016, http://www.securityweek.com/did-angler-exploit-kit-die-russian-lurk-arrests

[ii] Nicky Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, October 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[iii] John E Dunn, "Android Marshmallow's 10 most important security features," Techworld, September 30, 2015, http://www.techworld.com/picture-gallery/security/android-marshmallows-10-most-important-security-features-3626468/

[iv] Al Sacco, "Google details security features in Android 7.0 'Nougat,'" CIO, August 16, 2016, http://www.cio.com/article/3108382/android/google-details-security-features-in-android-7-0-nougat.html

[v] "Malicious banker tries to bypass Android Marshmallow security barriers," SonicWall Security Center, September 16, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=967

[vi] "New Android Lockscreen campaign spotted in the wild," SonicWall Security Center, May 12, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=929

[vii] "Self-installing porn apps rampage the Android ecosystem," SonicWall Security Center, June 17, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=940