Latest SonicWall Intelligence Reveals Unstable Cyber Threat Landscape, Amplifying Concerns for Security Professionals

Submitted by: Positive Marketing
Tuesday, 25 October 2022

-Global malware volume tops 4 billion, flat through three quarters
-Malware attempts dipped 8% in U.S., rose 3% in EMEA
Despite 31% decline in global ransomware attempts from 2021, volume exceeds full-year totals when compared to four of the last five years (623.3 million)
-Customers saw an average 1,014 ransomware attempts through three quarters
-91% of IT leaders cited financially motivated attacks as biggest concern
-Capture ATP earns seventh consecutive 100% threat detection score in ICSA Labs Advanced Threat Defense (ATD) Q3 2022 testing

MILPITAS, Calif. — OCT. 25, 2022 — SonicWall, publisher of the world's most quoted ransomware threat intelligence, today released new threat data through the third quarter of 2022 (https://www.sonicwall.com/2022-cyber-threat-report/?elqCampaignId=15400&sfc=7015d000002k7FCAAY). SonicWall recorded more than 4 billion malware attempts globally while year-to-date ransomware attempts in 2022 have already exceeded full-year totals from four of the last five years. In the recent 2022 SonicWall Cyber Threat Mindset Survey (https://www.sonicwall.com/resources/white-papers/2022-sonicwall-threat-mindset-survey/), 91% of organizations reported that they are most concerned about ransomware attacks, indicating a rise of anxiety among security professionals.

"Being a security professional has never been more difficult," said SonicWall President and CEO Bob VanKirk. "The cyber warfare battlefront continues to shift, posing dangerous threats to organizations of all sizes. With expanding attack surfaces, growing numbers of threats and the current geo-political landscape, it should be no surprise that even the most seasoned IT professional can feel overwhelmed. Armed with the latest cybersecurity tools, SonicWall partners can play a vital role in helping customers stay secure in even the most dynamic threat environments."

Ransomware Attacks Shift, Tactics Intensify, Diversify

After a record-breaking 2021, overall ransomware attacks have trended down in the first three quarters of 2022 — especially in the United States (-51%). However, attack locations have continued to shift, as ransomware attempts jumped in the U.K. (20%), EMEA (38%) and APJ (56%) compared to the same time frame last year. Proprietary SonicWall threat intelligence also found that Q3 2022 was the lowest quarterly ransomware volume since Q3 2020. Even in decline, SonicWall recorded 338.4 million ransomware attempts since the beginning of the year.

It is easier than ever to perform ransomware attacks. With Ransomware-as-a-Service (RaaS) offerings, even less technical cybercriminals can purchase ransomware kits on the dark web and target organizations with minimal experience.

Ransomware actors also are diversifying their business models and broadening their networks as demand for their services continues to grow, leading to an explosion in the variety of different tools and resources

being offered via illicit marketplaces. According to SonicWall survey data (https://www.sonicwall.com/news/new-sonicwall-survey-data-reveals-91-of-organizations-fear-ransomware-attacks-in-2022/), organizations are concerned with how easily ransomware attacks can be launched and 89% cited concern of financially motivated threats.

“Ransomware has evolved at an alarming rate, particularly in the past five years — not only in volume but in attack vectors,” said SonicWall Emerging Threat Expert Immanuel Chavoya. “The latest Q3 data shows how bad actors are getting smarter in the development of evolutionary strains and more targeted in their assaults.”

Cryptojacking, IoT Malware Volume Continue Upward Trend

Hackers are increasingly targeting financial firms, such as banks and trading houses, with cyberattacks designed to maliciously use computer systems to illegally mine cryptocurrencies. Cryptojacking numbers jumped 35% globally through three quarters, including a 377% spike in EMEA and 160% increase in APJ.

With more smart devices entering the digital space every day there is a growing need for Internet of things (IoT) security. IoT devices have multiple ways to connect to a network, offering multiple attack vectors to exploit. IoT malware climbed 92% globally, with 82% and 200% jumps in APJ and North America, respectively.

“With over 1.4 million endpoints collecting data around the globe, SonicWall has more data to uncover emerging threat trends and provide a true depiction of what is happening in the cyber threat landscape,” said Solutions Granted (SGI) CEO Michael Crean. “They say knowledge is power and SonicWall’s proprietary data helps SGI stay informed, which in turn helps us educate our customer base. Leveraging SonicWall’s research helps SGI create actionable steps to help us keep our customers safer!”

Machine Learning Uncovering ‘Never-before-seen’ Malware Variants

SonicWall’s patented Real-Time Deep Memory InspectionTM (RTDMI) technology identified 373,756 never-before-seen malware variants during the first three quarters of 2022 — a 22% increase year-to-date.

One of these never-before-seen malware variants was Spyder Loader, which was observed targeting government organizations in Hong Kong in October 2022. SonicWall RTDMI proactively detected this malware strain and SonicWall Capture Labs threat researchers were the first to publish their analysis in a March 2021 SonicAlert (https://securitynews.sonicwall.com/xmlpost/chinas-winnti-spyder-module/) — a showcase of RTDMI’s machine learning-powered capabilities.

SonicWall Capture ATP Showcases ‘Perfect Threat Detection’

In October 2022, SonicWall Capture Advanced Threat Protection (ATP) with RTDMI earned its seventh consecutive 100% threat detection score in ICSA Labs Advanced Threat Defense (ATD) testing for Q3 2022, the solution’s 11th consecutive certification. ICSA Labs is an independent third party that tested

SonicWall's solutions using never-before-seen malware samples, many just hours old.

To learn more about SonicWall security efficacy and perfect threat detection scores from Capture ATP, please visit SonicWall.com/ICSA (https://www.sonicwall.com/ICSA).

About SonicWall Capture Labs
SonicWall Capture Labs threat researchers gather, analyze and vet cross-vector threat information from the SonicWall Capture Threat network, consisting of global devices and resources, including more than 1 million security sensors in nearly 215 countries and territories. SonicWall Capture Labs, which pioneered the use of artificial intelligence for threat research and protection over a decade ago, performs rigorous testing and evaluation on this data, establishes reputation scores for email senders and content, and identifies new threats in real-time.

About SonicWall
SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com (https://www.sonicwall.com/) or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall Press Contacts

UK
Positive
Inés Mitsou
imitsou@positivemarketing.com
+44 (0)770 388 4664