SonicWall Threat Data Exposes Depths of Cyberattacks; Propels the Need for Managed Service Providers (MSPs)

Submitted by: Positive Marketing
Wednesday, 21 February 2024

SonicWall Threat Data Exposes Depths of Cyberattacks; Propels the Need for Managed Service Providers (MSPs)

Overall intrusion attempts climb (+20%), as threat actors diversify tactics - increase in attacks around the globe
Ransomware intensifies through the year (+27% in 2H) peaking during the summer months (+37%)
Total cryptojacking volume – spikes +659% globally
IoT exploit (+15%) and encrypted threats (+117%) also on the rise
SonicWall discovered 293,989 ‘never-before-seen’ malware variants – 805 a day

MILPITAS, Calif. — February 21, 2024 — SonicWall today released the 2024 SonicWall Annual Cyber Threat Report, which exposes all types of cyber behaviors and trends from digital adversaries to help partners build data-driven solutions to keep customers safe. 2023 proved to be a year of volatile, adaptive and creative digital threats, as threat actors continue to be relentless in their assault, leaving organizations looking for another layer of defense.

Organizations are increasingly turning to Managed Service Providers (MSPs) to alleviate pressure on IT departments. Managed services have emerged as a game-changing solution, providing organizations with an additional human-layer of defense, addressing alert fatigue, and freeing up valuable resources and time for core business functions.

“The SonicWall 2024 Threat Report reveals that the threat landscape continues to grow in complexity and depth as threat actors adopt new tactics and platforms,” said SonicWall President and CEO Bob VanKirk. “It has become clear that conventional network security isn’t enough. Security professionals need assistance to cope with the overwhelming volume of cyberattacks and protect from the endpoint to the cloud. Especially as the cloud becomes an indispensable reality for businesses, the role of MSPs is shifting from technical maintenance to raising the bar on their customers security posture.”

Overall intrusions numbers climbed, totaling almost 1 billion more attempts compared to the same time as last year. Global cryptojacking volume rose 659% and encrypted threat jumped 117%, as threat actors opted for a stealthier, less risky means of malicious activities. The data illustrates the tenacious and evolving state of cyber threats, underscoring the need for businesses to continually adapt their security strategies, and serves as a call for organizations to lean on MSPs to help identify and remediate threats quickly.

Evolved, Diversified Attack Vector

“When it comes to protecting your most valuable assets, organizations must remain alert, and deploy proactive cybersecurity measures, and focus on the threats that actually matter,” said SonicWall Executive Vice President of Managed Security Services Michael Crean. “Today’s organizations demand an integrated approach for end-to-end managed threat protection enabling MSPs to help customers navigate the

cybersecurity landscape with confidence and resilience – giving them a distinct competitive edge."

Cybercriminals and nation states are adapting their abilities to gain access to critical infrastructure, making the threat landscape even more complex and forcing organizations to reconsider their security needs. The second half of the 2023 saw a barrage of ransomware activity (+27%) and a variety of other attacks have trended up globally annually, including IoT exploit (+15%), intrusion attempts (+20%) and encrypted threats (+117%).

"In an era where cyber threats are increasingly sophisticated, MSPs are the frontline defense protecting their customers and helping them spend more of their time managing their business' needs," said CTO of Compass MSP and longtime SonicWall partner Alex Tsukanov. "New threats are emerging every day, and MSPs use threat insights to build an actual plan with the necessary capabilities to keep our customers safe, like that found in the SonicWall's threat report."

SMB to the Enterprise – The Surge Continues

While ransomware continues to be a threat, SonicWall Capture Labs threat researchers expect a broader set of actions in 2024, specifically targeting SMBs, governments and the enterprise. SonicWall sensors identify and prevent more than 19,000 threats per day.

The 2024 SonicWall Cyber Threat Report provides insight on a range of threats, including:

Malware – Total global malware volume rose 11% in 2023, with Latin America and the U.S. logging the biggest jumps – (+30%) and (+15%) respectively. Surprisingly, Europe saw a (-2%) decrease, with the UK seeing the steepest decline of -28%.
Ransomware – Overall ransomware numbers saw a -36% decline annually, the summer months and second half of the year suggests a strong rebound, as it spiked +37% during the summer months when compared to the same time last year.
IoT Exploit – Global volume rose 15%, as connected devices continue to rapidly multiply, bad actors are targeting weak points of entry as potential attack vectors into organizations.
Encrypted Threats – Yet another quieter approach embraced by bad actors in the last year was encrypted threats, which spiked (+117%) globally.

Patented RTDMI Discovered more than 294,000 'Never-Before-Seen' Malware Variants

SonicWall's patented Real-Time Deep Memory InspectionTM (RTDMITM) technology identified a total of 293,989 never-before-seen malware variants in 2023. The threat landscape remains complex, with almost 800 strains of new variants discovered each day.

To learn more about SonicWall and get the complete 2024 SonicWall Cyber Threat Report, please visit www.sonicwall.com/threatreport (http://www.sonicwall.com/threatreport).

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 (https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.sonicwall.com%2F&data=05%7C01%7Cbfitzger is a cybersecurity forerunner with more than 30 years of expertise and is recognized as a leading partner-first company. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real-time, SonicWall provides seamless protection against the most evasive cyberattacks across endless exposure points for increasingly remote, mobile and cloud-enabled users. With its own threat research center, SonicWall can quickly and economically provide purpose-built security solutions to enable any organization—enterprise, government agencies and SMBs—around the world. For more information, visit www.sonicwall.com (https://nam04.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.sonicwall.com%2F&data=05%7C01%7Cbfitzgera or follow us on Twitter (https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FSonicWall&data=05%7C01%7Cbfitzge LinkedIn (https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.linkedin.com%2Fcompany%2Fsonicwall%2F&da Facebook (https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.facebook.com%2FSonicWall%2F&data=05%7C and Instagram (https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.instagram.com%2Fsonicwall_inc%2F%3Fhl%3D