2023 SonicWall Cyber Threat Report Casts New Light on Shifting Front Lines, Threat Actor Behavior

Submitted by: Positive Marketing
Tuesday, 28 February 2023

Overall malware up 2%, with surges in IoT malware (+87%) and cryptojacking (+43%)

Ransomware attacks dipped 21% globally, but 2022 still second-highest year on record for global ransomware attempts (493.3 million)

Education (+157%), finance (+86%) and retail (+50%) verticals hit hardest by malware

Ukraine saw record levels of malware (25.6 million) and ransomware (7.1 million)

SonicWall discovered 465,501 ‘never-before-seen’ malware variants in 2022

Intrusion attempts against Log4j vulnerabilities eclipsed 1 billion

MILPITAS, Calif. — February 28, 2023 — SonicWall, publisher of the world’s most quoted ransomware data and trusted cyberattack intelligence, today released the 2023 SonicWall Cyber Threat Report. The bi-annual report details an increasingly diversified cyberattack landscape amid shifting threat actor strategies. SonicWall recorded the second-highest year on record for global ransomware attempts, as well as an 87% increase in Internet of Things (IoT) malware and a record number of cryptojacking attacks (139.3 million) in 2022.

“The past year reinforced the need for cybersecurity in every industry and every facet of business, as threat actors targeted anything and everything, from education to retail to finance,” said SonicWall President and CEO Bob VanKirk. “While organizations face an increasing number of real-world obstacles with macroeconomic pressures and continued geopolitical strife, threat actors are shifting attack strategies at an alarming rate.”

Threat Actors Shift Strategies, Opt for Covert Cyberattack Methods

Global malware volume increased 2% year-over-year, but it was jumps in IoT malware (+87%) and cryptojacking (+43%) that offset the decline of overall global ransomware volume (-21%), signifying a strategic shift. Threat actors have embraced slower and more stealthy approaches to achieve financially-motivated cyberattacks.

“Cyberattacks are an ever-present danger for companies of all sizes, putting their operations and reputation on the line,” said SonicWall Threat Detection and Response Strategist Immanuel Chavoya. “It is crucial for organizations to understand attackers’ tactics, techniques and procedures (TTPs),

and commit to threat-informed cybersecurity strategies to defend and recover successfully from business-disrupting events. This includes stopping sophisticated ransomware attacks as well defending emerging threat vectors, including IoT and cryptojacking."

In addition to cyberattacks becoming more sophisticated and covert, threat actors are showing clear preferences for certain techniques, with notable shifts toward weak IoT devices, cryptojacking and potentially soft targets like schools and hospitals.

Prominent ransomware attacks impacted enterprises, governments, airlines, hospitals, hotels and even individuals causing widespread system downtime, economic loss and reputational damage. Following global trends, several industries faced large year-over-year increases of ransomware volume, including education (+275%), finance (+41%) and healthcare (+8%).

Diverse Attacks Offset Global Ransomware Decline

Cybercriminals are using increasingly advanced tools and tactics to exploit and extort victims, with state-sponsored activity growing as a concern. While ransomware continues to be a threat, SonicWall Capture Labs threat researchers expect more state-sponsored activity targeting a broader set of victims in 2023, including SMBs and enterprises.

The 2023 SonicWall Cyber Threat Report provides insight on a range of cyber threats, including:

Malware – Total volume was up 2% in 2022 after three straight years of decline — just as SonicWall predicted in the 2022 SonicWall Cyber Threat Report. Following that trend, Europe as a whole saw increased levels of malware (+10%) as did Ukraine, which had a record 25.6 million attempts, suggesting malware was used heavily in regions impacted by geopolitical strife. Interestingly, malware was down year-over-year in key countries like the U.S. (-9%), U.K. (-13%) and Germany (-28%).

Ransomware – Although overall ransomware numbers saw a 21% decline globally, the total volume in 2022 was higher than 2017, 2018, 2019 and 2020. In particular, total ransomware in Q4 (154.9 million) was the highest since Q3 2021.

IoT Malware – Global volume rose 87% in 2022, totaling 112 million hits by year's end. With no corresponding slowdown in the proliferation of connected devices, bad actors are likely probing soft targets to leverage as potential attack vectors into larger organizations.

Apache Log4j – Intrusion attempts against the industry's Apache Log4j 'Log4Shell' vulnerability

eclipsed 1 billion in 2022. The vulnerability was first discovered in December 2021 and has been actively exploited since.

Cryptojacking – Use of cryptojacking as a ‘low and slow’ approach continued to surge, rising 43% globally, which is the most SonicWall Capture Labs threat researchers have recorded in a single year. The retail and financial industry felt the sting of cryptojacking attacks, seeing 2810% and 352% increases, respectively, year-over-year.

"Cyberattacks of all varieties continue to hinder organizations worldwide," said Logically Chief Operating Officer Keith Johnson. "SonicWall's annual intelligence report gives us a deeper understanding of the current threat landscape and helps breakdown why cyberattacks continue to be successful, as well as the drivers and trends behind them. By making this report available to partners, SonicWall helps elevate us as trusted advisors and strengthens our ability to provide sound security measures to our customers.”

Patented RTDMI Discovered more than 465,000 ‘Never-Before-Seen’ Malware Variants in 2022

SonicWall’s patented Real-Time Deep Memory InspectionTM (RTDMITM) technology identified a total of 465,501 never-before-seen malware variants in 2022, a 5% year-over-year increase and an average of 1,279 per day. Dating to 2019, this is the fourth straight year RTDMI increased its total of malware discoveries.

To learn more about SonicWall and get the complete 2023 SonicWall Cyber Threat Report, please visit SonicWall.com/ThreatReport (https://www.sonicwall.com/2023-cyber-threat-report/).

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.

Press Contacts
Inés Mitsou
Account Director
SonicWall@positivemarketing.com
+44 (0)20 3637 0640