Latest SonicWall Report Reveals Stealthier Threat Actor Behaviors: Cryptojacking Soars as Cyberattacks Increase, Intensify, Diversify

Submitted by: Positive Marketing
Wednesday, 26 July 2023

-Intrusion attempts climb (+21%), with a record surge in cryptojacking volume (+399%)
-Cryptojacking volume in North America and Europe jumps (+345%) and (+788%) respectively
-IoT malware (+37%) and encrypted threats (+22%) also on the rise
-Opportunistic threat actors target education and government verticals with digital barrage
-SonicWall discovered 172,146 ‘never-before-seen’ malware variants
-Lowest first half totals on ransomware attempts (-41%) since 2020, despite big Q2 jump – suggesting a likely rebound over the next 6 months

MILPITAS, Calif. — July 26, 2023 — SonicWall, publisher of trusted cyberattack intelligence and leader of ransomware data, today released the 2023 SonicWall Mid-Year Cyber Threat Report. The bi-annual report uncovers evolving tactical behaviors from digital threat actors as they opt for different types of malicious attacks compared to years past.

Overall intrusion attempts were up, led by the highest year on record for global cryptojacking volume recorded by SonicWall, as threat actors shifted away from traditional ransomware attacks in favor of a stealthier means of malicious activities. The data suggests increased law enforcement activity, heavy sanctions and victims’ refusal to pay ransom demands have altered criminal conduct, and threat actors are targeting other means of revenue.

“The seemingly endless digital assault on enterprises, governments and global citizens is intensifying, and the threat landscape continues to expand,” said SonicWall President and CEO Bob VanKirk. “Threat actors are relentless, and our data indicates they are more opportunistic than ever, targeting schools, state and local governments, and retail organizations at unprecedented rates. The 2023 SonicWall Mid-Year Cyber Threat Report helps us better understand the mindset and criminal behavior that will in turn help SonicWall create the right countermeasures, and help organizations protect themselves by being better prepared and build stronger defenses against malicious activities.”

Rise of Cryptojacking; Evolution of Ransomware
Cybercriminals are diversifying and expanding their skill sets to attack critical infrastructure, making the threat landscape even more complex and forcing organizations to reconsider their security needs. Despite the decline in global ransomware attempts (-41%), a variety of other attacks have trended up globally, including cryptojacking (+399%), IoT malware (+37%) and encrypted threats (+22%).

“SonicWall intelligence suggests that bad actors are pivoting to lower-cost, less risky attack methods with potentially high returns, like cryptojacking,” said SonicWall Vice President of Product Security Bobby Cornwell. “It also explains the reason we’re seeing higher levels of cybercrime in regions like Latin America and Asia. Hackers search for the weakest points of entry, with the lightest possible repercussions, limiting their risk and maximizing their potential profits.”

Financially motivated threat actors continue to be successful despite challenges. They have pivoted to

crimes with greater certainty of success but they will not abandon proven tactics like ransomware; they are simply shifting strategy by target rather than exiting altogether.

Prominent attacks continued to plague enterprises, cities, airlines, and even K-12 schools, causing widespread system downtime, economic loss and reputational damage. While several industries followed the global trend of ransomware volume decline, they saw a huge growth in cryptojacking attacks: education (+320X), government (+89X) and healthcare (+69X).

Threat Actors Diversify Cyberattack Strategies
Cybercriminals are using increasingly advanced tools and tactics to exploit and extort victims. 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, government entities and enterprises.

The 2023 Mid-Year SonicWall Cyber Threat Report provides insight on a range of cyber threats, including:
-Malware – Total global malware volume dipped slightly (-2%), in the first half of 2023, with the U.S. and U.K. logging the biggest dips – (-14%) and (-7%) respectively. Surprisingly, malware numbers climbed in every other tracked region. Europe saw an (+11%) increase, while Latin America malware jumped (+19%) – suggesting a geo-migration of threat actor behavior as they move from targeting traditional hotspots to more opportunistic locations.

-Ransomware – Although overall ransomware numbers saw a -41% decline globally, Q2 suggests a potential rebound, as it spiked 73.7% when compared to Q1. Some countries still felt the sting of ransomware attacks as Germany increased (+52%) and India spiked a whopping (+133%).

-IoT Malware – Global volume rose 37%, totaling almost 78 million hits by the end of June. 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 six months was encrypted threats, which climbed (+22%) globally.

“Every year we see cybercrime increase at a staggering and unprecedented rate, and our customers depend on us protect their most valuable digital assets,” said President and CEO of LAN Infotech Michael Goldstein. “That is why we have partnered with SonicWall for the past 15 years, knowing that they will always deliver cutting-edge products and timely research to provide us with the support we need to keep our customers safe. Reports like the 2023 SonicWall Mid-Year Cyber Threat Report arm the channel with the latest cyber trends and help us become trusted advisors to provide sound security measures to our customers.”

Patented RTDMI Discovered more than 172,000 ‘Never-Before-Seen’ Malware Variants

SonicWall’s patented Real-Time Deep Memory InspectionTM (RTDMITM) technology identified a total of 172,146 never-before-seen malware variants in the first half of 2023, which is down (-36%) year-over-year, suggesting bad actors are spending less time on research and development, and more time

on volume-based attacks – utilizing open-source tools that may be less likely to be intercepted. In addition, threat actors appear to be leverage existing tools – leaning on tools they know will help them be successful.

Despite the dip in never-before-seen malware variants, the threat landscape remains complex, with almost 1,000 strains of new variants discovered each day.

To learn more about SonicWall and get the complete 2023 SonicWall Mid-Year Cyber Threat Report, please visit www.sonicwall.com/threatreport.

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 or follow us on Twitter (https://twitter.com/SonicWall), LinkedIn (https://www.linkedin.com/company/SonicWall), Facebook (https://www.facebook.com/SonicWall) and Instagram. (https://www.instagram.com/sonicwall_inc)

UK Press Contacts:
Carl Escoffier
cescoffier@positivemarketing.com
020 3637 0640