New SonicWall Research Finds Aggressive Growth in Ransomware, Rise in IoT Attacks

Submitted by: Positive Marketing
Thursday, 29 October 2020

Ryuk Ransomware Responsible for One Third of All Ransomware Attacks in 2020

MILPITAS, Calif. — OCT. 29, 2020 — SonicWall Capture Labs threat researchers today unveiled third-quarter threat intelligence collected by the company's more than 1 million global security sensors. Year-to-date findings through September 2020 highlight cyber criminals' growing use of ransomware, encrypted threats and attacks leveraging non-standard ports, while overall malware volume declined for the third consecutive quarter.

"For most of us, 2020 has been the year where we've seen economies almost stop, morning commutes end and traditional offices disappear," said SonicWall President and CEO Bill Conner. "However, the overnight emergence of remote workforces and virtual offices has given cybercriminals new and attractive vectors to exploit. These findings show their relentless pursuit to obtain what is not rightfully theirs for monetary gain, economic dominance and global recognition."

SonicWall Capture Labs key findings include:

39% decline in malware (4.4 billion YTD); volume down for third consecutive quarter
40% surge in global ransomware (199.7 million)
19% increase in intrusion attempts (3.5 trillion)
30% rise in IoT malware (32.4 million)
3% growth of encrypted threats (3.2 million)
2% increase in cryptojacking (57.9 million)

Malware Volume Dipping as Attacks More Targeted, Diversified
While malware authors and cybercriminals are still busy working to launch sophisticated cyberattacks, SonicWall research concludes that overall global malware volume continues steadily decline in 2020. In a year-over-year comparison through the third quarter, SonicWall researchers recorded 4.4 billion malware attacks — a 39% drop worldwide.

Regional comparisons show India (-68%) and Germany (-64%) have once again seen a considerable drop-rate percentage, as well as the United States (-33%) and the United Kingdom (-44%). Lower numbers of malware do not mean it is going away entirely. Rather, this is part of a cyclical downturn that can very easily right itself in a short amount of time.

Ransomware Erupts, Ryuk Responsible for Third of All Attacks
Ransomware attacks are making daily headlines as they wreak havoc on enterprises, municipalities, healthcare organizations and educational institutions. SonicWall researchers tracked aggressive growth during each month of Q3, including a massive spike in September. While sensors in India (-29%), the U.K. (-32%) and Germany (-86%) recorded decreases, the U.S. saw a staggering 145.2 million ransomware hits — a 139% YoY increase.

Notably, SonicWall researchers observed a significant increase in Ryuk ransomware detections in 2020. Through Q3 2019, SonicWall detected just 5,123 Ryuk attacks. Through Q3 2020, SonicWall detected 67.3 million Ryuk attacks — a third (33.7%) of all ransomware attacks this year.

“What’s interesting is that Ryuk is a relatively young ransomware family that was discovered in August 2018 and has made significant gains in popularity in 2020,” said SonicWall Vice President, Platform Architecture, Dmitriy Ayrapetov. “The increase of remote and mobile workforces appears to have increased its prevalence, resulting not only in financial losses, but also impacting healthcare services with attacks on hospitals.

“Ryuk is especially dangerous because it is targeted, manual and often leveraged via a multi-stage attack preceded by Emotet and TrickBot malware. Therefore, if an organization has Ryuk, it’s a pretty good indication that its infested with several types of malware.”

SonicWall Capture Advanced Threat Protection (ATP), with patent-pending Real-Time Deep Memory InspectionTM (RTDMI), protects against all Emotet, TrickBot and Ryuk ransomware variants — in real time.

IoT Dependency Grows Along with Threats

COVID-19 led to an unexpected flood of devices on networks, resulting in an increase of potential threats to companies fighting to remain operational during the pandemic. SonicWall Capture Labs found a 30% increase in IoT malware attacks, a total of 32.4 million world-wide.

Most IoT devices — including voice-activated smart devices, door chimes, TV cameras and appliances — were not designed with security as a top priority, making them susceptible to attack and supplying perpetrators with numerous entry points.

“Employees used to rely upon the safety office networks provided, but the growth of remote and mobile workforces has extended distributed networks that serve both the house and home office,” said Conner. “Consumers need to stop and think if devices such as AC controls, home alarm systems or baby monitors are safely deployed. For optimum protection, professionals using virtual home offices, especially those operating in the C-suite, should consider segmenting home networks.”

SonicWall threat intelligence data also concluded that while cryptojacking (57.9 million), intrusion attempts (3.5 trillion) and IoT malware threats (32.4 million) are trending with first-half volume reports, they continue to pose a threat and remain a source of opportunity for cybercriminals.

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 (http://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 Media Contacts:

Ines Mitsou
Positive
imitsou@positivemarketing.com
020 3637 0640

Max Bailey
Positive
mbailey@positivemarketing.com
020 3637 0640|07933318525