SonicWall’s Mid-Year Cyber Threat Report Finds Malicious Microsoft Office Files On Rise, Ransomware Up in US, Globally

Submitted by: Positive Marketing
Thursday, 23 July 2020

20% jump in ransomware globally, 109% spike in United States
24% drop in malware attacks worldwide
7% of phishing attacks capitalized on COVID-19 pandemic
176% increase in malicious Microsoft Office file types
23% of malware attacks leveraged non-standards ports
50% rise of IoT malware attacks
Report analyzes threat intelligence data gathered from 1.1 million sensors in over 215 countries and territories

MILPITAS, Calif. — July 23, 2020 — The SonicWall Capture Labs threat research team today published the mid-year update to the 2020 SonicWall Cyber Threat Report, highlighting increases in ransomware, opportunistic use of COVID-19 pandemic, systemic weaknesses and growing reliance on Microsoft Office files by cybercriminals.

“Cybercriminals can be resourceful, often setting traps to take advantage of people’s kindness during a natural disaster, panic throughout a crisis and trust in systems used in everyday life,” said SonicWall President and CEO Bill Conner. “This latest cyber threat data shows that cybercriminals continue to morph their tactics to sway the odds in their favor during uncertain times. With everyone more remote and mobile than ever before, businesses are highly exposed and the cybercriminal industry is very aware of that. It’s imperative that organizations move away from makeshift or traditional security strategies and realize this new business normal is no longer new.”

Changing Landscape Leads to Waning Malware Volume

During the first half of 2020, global malware attacks fell from 4.8 billion to 3.2 billion (-24%) over 2019’s mid-year total. This drop is the continuation of a downward trend that began last November.

There are regional differences in both the amount of malware and the percentage change year over year, highlighting shifting cybercriminal focus. For example, the United States (-24%), United Kingdom (-27%), Germany (-60%) and India (-64%) all experienced reduced malware volume. Less malware doesn’t necessarily mean a safer world; ransomware has seen a corresponding jump over the same time period.

Ransomware Attackers Raise Stakes Again

Despite the global decline of malware volume, ransomware continues to be the most concerning threat to corporations and the preferred tool for cybercriminals, increasing a staggering 20% (121.4 million) globally in the first half of 2020.

“Remote and mobile workforces are at a turning point on the subject of security,” said Chad Sweet, Founder and CEO The Chertoff Group. “It has never been more prevalent for enterprises and organizations to prioritize online security and make what used to be a luxury, a secured and protected necessity.”

Comparatively, the U.S. and U.K. are facing different odds. SonicWall Capture Labs threat researchers logged 79.9 million ransomware attacks (+109%) in the U.S. and 5.9 million ransomware attacks (-6%) in the U.K. — trends that continue to ebb and flow based on the behaviors of agile cybercriminal networks.

Malware-laden COVID-19 Emails

The combination of the global pandemic and social-engineered cyberattacks has proven to be an effective mix for cybercriminals utilizing phishing and other email scams. Dating as far back as Feb. 4, SonicWall researchers detected a flurry of increased attacks, scams and exploits specifically based around COVID-19 and noted a 7% increase in COVID-related phishing attempts during the first two quarters.

As expected, COVID-19 phishing began rising in March, and saw its most significant peaks on March 24, April 3 and June 19. This contrasts with phishing as a whole, which started strong in January and was down slightly globally (-15%) by the time the pandemic phishing attempts began to pick up steam.

Office Lures Remain a Staple

Microsoft Office is a necessity with millions of employees now more remote and dependent on the business productivity suite of applications. Cybercriminals were quick to leverage this shift, as SonicWall threat researchers found a 176% increase in new malware attacks disguised as trusted Microsoft Office file types.

Leveraging SonicWall Capture Advanced Threat Protection (ATP) with Real-Time Deep Memory Inspection™ (RTDMI) technology, SonicWall discovered that 22% of Microsoft Office files and 11% of PDF files made up 33% of all newly identified malware in 2020. The patent-pending RTDMI™ technology identified a record 120,910 ‘never-before-seen’ malware variants during that time — a 63% increase over the first six months of 2019.

“Cybercriminals are too sophisticated to use known malware variants, so they’re re-imagining and re-writing malware to defeat security controls like traditional sandboxing techniques — and it’s working,” said Conner.

Attacks Using Non-standard Ports Make Comeback

Overall, an average of 23% of attacks took place over non-standard ports so far in 2020 — the highest mark since SonicWall began tracking the attack vector in 2018.

By sending malware across non-standard ports, assailants can bypass traditional firewall technologies, ensuring increased success for payloads. A ‘non-standard’ port is leveraged by services running on a port other than its default assignment (e.g., Ports 80 and 443 are standard ports for web traffic).

Two new monthly records were set during the first two quarters of 2020. In February, non-standard port attacks reached 26% before climbing to an unprecedented 30% in May. During that month, there was a surge

in many specific attacks, such as VBA Trojan Downloader, that may have contributed to the spike.

IoT Continues to Serve Threats

Work-from-home (WFH) employees or remote workforces can introduce many new risks, including Internet of Things (IoT) devices like refrigerators, baby cameras, doorbells or gaming consoles. IT departments are besieged with countless devices swarming networks and endpoints as the footprint of their corporate expands beyond the traditional perimeter.

Researchers at SonicWall found a 50% increase in IoT malware attacks, a number that mirrors the number of additional devices that are connected online as individuals and enterprise alike function from home. Unchecked IoT devices can provide cybercriminals an open door into what may otherwise be a well-secured organization.

To download the full mid-year update, please visit www.sonicwall.com/ThreatReport (https://www.sonicwall.com/2020-cyber-threat-report/#threat-report-form).

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
0770 388 4664|020 3637 0640

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