# New SonicWall 2020 Research Shows Cyber Arms Race at Tipping Point

Submitted by: SonicWall
Tuesday, 16 March 2021

---

Threat actors weaponizing cloud storage, advanced cloud-based tools to create record ransomware attack effectiveness, volume

- Ransomware soars with 62% increase since 2019
- Office files preferred by cybercriminals, surpass PDFs, roughly 1 in 4 malicious
- Never-before-seen' malware variants up 74% year-over-year
- Cryptojacking shows three-year high with 28% year-over-year increase
- IoT malware rises 66% as criminals continue to leverage COVID-19 pandemic
- Retail, healthcare and government face mounting ransomware volume

MILPITAS, Calif. — MARCH 16, 2021 — The pandemic's work-from-home reality resulted in an unprecedented change for organizations as they fought to defend exponentially greater attack surfaces from cybercriminals armed with powerful cloud-based tools, cloud storage and endless targets. As working environments evolved, so did the methods of threat actors and other motivated perpetrators, as detailed in the latest 2021 SonicWall Cyber Threat Report.

"2020 offered a perfect storm for cybercriminals and a critical tipping point for the cyber arms race," said SonicWall President and CEO Bill Conner. "The pandemic — along with remote work, a charged political climate, record prices of cryptocurrency, and threat actors weaponizing cloud storage and tools — drove the effectiveness and volume of cyberattacks to new highs. This latest threat intelligence offers a look at how cybercriminals shifted and refined their tactics, painting a picture of what they are doing amid the uncertain future that lies ahead."

The 2021 SonicWall Cyber Threat Report highlights how COVID-19 provided threat actors with ample opportunity for more powerful, aggressive and numerous attacks, thriving on the fear and uncertainty of remote and mobile workforces navigating corporate networks from home.

"There is no code of conduct when it comes to cybercriminals, their methods of attacks and the selection of their targets," said Conner. "Technology is moving at an unprecedented rate. Threats that were once thought to be two or three years away are now a reality, with do-it-yourself, cloud-based tools creating an army of cybercriminals armed with the same devastating force and impact of a nation-state or larger criminal enterprise. Organizations must remain vigilant and proactive in hardening their cybersecurity posture."

The 2021 SonicWall Cyber Threat Report goes inside the stories that headlined 2020, and takes a closer look at new and disruptive cyber threats to provide insight into the evolving cyber threat landscape. Major findings of the new in-depth SonicWall report include:

- Ransomware reaches new heights with increasingly targeted attacks: A 62% increase in ransomware globally, and 158% spike in North America, points to cybercriminals using more sophisticated tactics and more dangerous variants, like Ryuk, to earn an easy payday.

- Ryuk ransomware rises from obscurity, sees astronomical increase: First identified in August 2018, Ryuk did not appear outside of North America, Europe or Asia as late as January 2020. The following month, Ryuk began climbing the charts, eventually overtaking top-ranking Cerber ransomware. With 109.9 million cases detected worldwide, Ryuk was logged nearly every eight seconds in September alone.

- More ‘never-before-seen’ malware variants identified: SonicWall’s newly patented Real-Time Deep Memory Inspection™ (RTDMI), a component of the company’s Capture Advanced Threat Protection (ATP) sandbox service, discovered 268,362 ‘never-before-seen’ malware variants in 2020, a 74% year-over-year increase. RTDMI™ is proven to proactively detect and block unknown mass-market malware, including malicious Office, and PDF file types.

- Malicious Office files surpass last year’s preferred PDFs: SonicWall research shows the shift to employees working from home full-time could be directly linked to the increased utilization of Office files and PDFs as malicious vehicles armed with phishing URLs, embedded malicious files and other dangerous exploits. New SonicWall data indicates a 67% increase in malicious Office files in 2020, while malicious PDFs dropped 22%.

- Cryptojacking returns as cryptocurrency breaks records: Once thought to be a dying attack vector after the industry’s major mining operation boarded its online service, cryptojacking is back thanks to rising cryptocurrency values and its appeal of concealed payouts. Total cryptojacking for 2020 set records with 81.9 million hits, a 28% increase from last year’s 64.1 million total.

- IoT malware increases as pandemic creates potential network of disruption: In March 2020, masses of employees packed their personal office belongings and equipment to work from home for months on end, simultaneously creating an explosion of new attack vectors. In 2020, SonicWall Capture Labs threat researchers recorded 56.9 million IoT malware attempts, a 66% increase that showed shifting tactics for lurking cybercriminals.

- Intrusion attempts up as attack patterns change: The distribution of intrusion attacks took on an entirely new character as a result of the changes brought on by the pandemic. In 2020, Directory Traversal tactics (34%) took over the top spot after a tie with remote code execution (21% for both) in 2019.

- Retail, healthcare and government face mounting ransomware volume: Industry-specific ransomware data reflects the impact cybercriminals had on retail (365%), healthcare (123%) and government (21%) sectors over the course of the pandemic.

The annual 2021 SonicWall Cyber Threat Report arms enterprises, small- and medium-sized business, government agencies and other organizations with actionable threat intelligence collected by the SonicWall Capture Labs threat research team. In-house researchers work collectively with other industry experts, over 50 industry collaboration groups, research teams and freelance security researchers.

Data for the report is gathered from over 1.1 million sensors strategically placed in over 215 countries and territories around the world as well as cross-vector, threat related information shared among

SonicWall security systems, including firewalls, email security devices, endpoint security solutions, honeypots, content filtering systems and the SonicWall Capture Advanced Threat Protection (ATP) multi-engine sandbox.

To download the complete 2021 SonicWall 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, LinkedIn, Facebook and Instagram.