EXECUTIVE SUMMARY

2023 SONICWALL CYBER THREAT REPORT

CHARTING CYBERCRIME'S SHIFTING FRONTLINES

SONICWALL

sonicwall.com | @sonicwall

THIS EXECUTIVE SUMMARY OFFERS A HIGH-LEVEL OVERVIEW OF THE YEAR'S MOST CRITICAL FINDINGS. FOR A MORE IN-DEPTH LOOK AT SONICWALL'S EXCLUSIVE THREAT DATA, DOWNLOAD THE FULL REPORT.

Spurred by high-profile busts and continued geopolitical unrest, threat actors in 2022 showed a renewed interest in subtlety. But there was no hiding from SonicWall Capture Labs threat researchers, who were tracking the continued evolution of cybercrime in real time. We've compiled our research into the 2023 SonicWall Cyber Threat Report, which offers actionable threat intelligence to arm organizations against today's ever-changing threat environment.

GET THE FULL REPORT — sonicwall.com/threatreport

∨ 21%

RANSOMWARE DOWN, BUT NOT OUT

Ransomware continued to fall in 2022, with volumes dipping to 493.3 million — a 21% year-over-year decrease. But less ransomware does not equal low ransomware: 2022's total volume still easily eclipses 2018, 2019 and 2020 totals, and amounts to more ransomware attempts than 2019 and 2020 combined. Worryingly, ransomware began to rise again by the end of 2022, with Q4's attack volume reaching 154.9 million — the highest since Q3 2021.

Despite 2022's global decrease, not every region saw a drop: ransomware in Europe jumped 83%, including a 112% increase in the U.K. The education and finance industries were also heavily targeted, with increases of 275% and 41%, respectively.

∧ 2%

MALWARE UP FOR FIRST TIME SINCE 2018

In 2022, SonicWall threat researchers recorded 5.5 billion malware attacks, a 2% increase year over year. While modest, this represents the reversal of a longstanding trend: 2022 is the first year since 2018 to see a rise. This was largely fueled by a 43% rise in cryptojacking and an 87% spike in IoT malware, which together offset a 21% drop in global ransomware volume.

As attackers shift tactics, we're also seeing a shift in targets: malware volume dropped in countries that traditionally see more malware, such as the U.S. (-9%), the U.K. (-13%) and Germany (-28%). The biggest jumps in malware volume were in the Asia-Pacific region (38%) and Latin America (17%), the two regions that typically see the least malware.

∧ 87%

IOT MALWARE NEARLY DOUBLES

After a relatively stable 2021, IoT malware volume jumped dramatically in 2022, breaking the 100 million mark for the first time and setting a new yearly record. SonicWall Capture Labs threat researchers recorded 112.3 million attacks in 2022, an 87% year-over-year increase. Much of this spike was centered in North America, where attacks rose 145%, and the U.S., which saw volumes rise 169%.

^43%

CRYPTOJACKING CONTINUES RECORD-BREAKING RUN

Threat actors augmented ransomware with more steady and low-profile revenue streams in 2022, pushing cryptojacking past the 100 million mark for a new record high. SonicWall recorded 139.3 million cryptojacking attacks in 2022, representing a 43% increase over 2021 and a 142.3% increase since SonicWall began tracking this malware in 2018. With several new campaigns surfacing late in the year, we're likely to see this total continue to rise — particularly in Europe, where attack volume surged a staggering 549% year-over-year.

465K+

RTDMI™ DETECTIONS CONTINUE TO RISE

SonicWall Capture ATP and patented Real-Time Deep Memory Inspection™ (RTDMI) continued to raise the bar, with RTDMI discovering 465,501 never-before-seen malware variants last year — an average of 1,279 per day. SonicWall Capture Advanced Threat Protection (ATP), which includes RTDMI, logged a 35% year-over-year increase in the number of new PDF-based attacks. This surge pushed PDFs into the top three malicious filetypes discovered and blocked by Capture ATP.

^19%

OVERALL INTRUSION ATTEMPTS UP

In 2022, SonicWall logged 6.3 trillion overall intrusion attempts, an increase of 19% year over year. But while total volume was up, moderate- and high-severity intrusion attempts fell 10% globally. Researchers also noted a sizeable spike in the percentage of RCE (remote code execution) attempts — these attempts now make up 21.5% of total malicious intrusions, a larger share than any other attack type.

As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. 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.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035

SONICWALL