

MID-YEAR UPDATE

# 2023

# SONICWALL CYBER THREAT REPORT

TRACKING CYBERCRIMINALS  
INTO THE SHADOWS

## EXECUTIVE SUMMARY

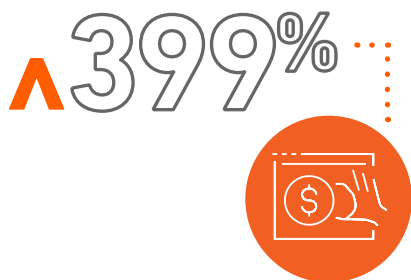


**THIS EXECUTIVE SUMMARY OFFERS A HIGH-LEVEL OVERVIEW OF THE YEAR'S MOST CRITICAL FINDINGS. FOR A MORE IN-DEPTH LOOK AT SONICWALL'S EXCLUSIVE THREAT DATA, [DOWNLOAD THE FULL UPDATE.](#)**

Cybercriminals showed a preference for quieter attacks in the first half of 2023, shifting from or augmenting ransomware with cryptojacking, IoT malware and encrypted threats. Feeling the heat from increased enforcement efforts, high-profile busts and heightened security in the U.S., threat actors are also moving their attacks to new shores, and are splitting their attention between large, high-profile targets potentially offering an outsized payday, and soft targets such as educational organizations. While the resulting threat landscape is one in a state of change, SonicWall has and will continue to track these threats and trends throughout the latter half of 2023 and beyond.

**GET THE FULL UPDATE**

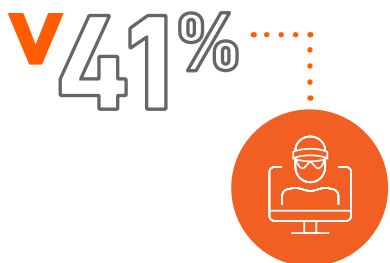
— [sonicwall.com/threatreport](https://sonicwall.com/threatreport)



### CRYPTOJACKING'S RECORD SURGE CONTINUES

In 2022, cryptojacking surpassed the 100 million mark for the first time. In the first six months of 2023, attack volumes have not only eclipsed that high water mark, they've nearly *tripled* it, rising 399% to more than 332 million. This number represents an unprecedented new record high, but that's not all. If this growth continues apace—or even if it slows dramatically—cryptojacking volumes in 2023 are poised to exceed all other years we've tracked this threat type *combined*.

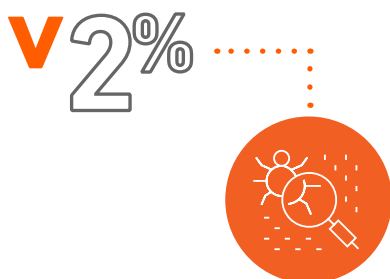
North American customers, European customers, and those working in government and education saw outsized spikes in cryptojacking volume in the first half.



### RANSOMWARE STILL FALLING, BUT POISED FOR A REBOUND

As threat actors pivoted to stealthier forms of attack, ransomware rates continued to drop in the first half of 2023, falling 41% to 140 million. However, even with this sustained decrease, ransomware still isn't back to pre-pandemic levels — and with a 74% increase from first-quarter attack volume to second quarter, it seems likely to rebound in the second half.

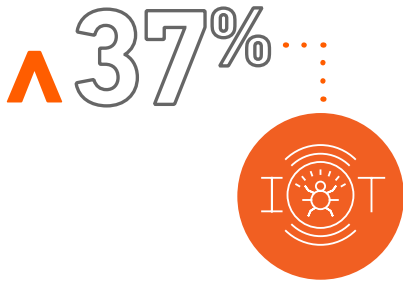
But while attack volumes are down overall, ransomware is still rising for some, including customers in Germany and India and those working in government.



### MALWARE CONTINUES ITS MIGRATION

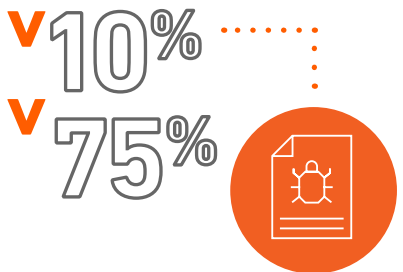
While malware *volumes* remain largely unchanged over the same time period in 2022, a look at who's being attacked shows a great deal of change. With 1.3 billion hits (out of a global total of 2.7 billion), the U.S. remains the world's malware epicenter, but this region was also the only one to show a decrease, falling 12% year to date. In contrast, Europe and LATAM recorded double-digit growth, suggesting that attackers are continuing to shift their attention to new shores.

Education and finance customers in particular saw large increases in malware, though none of the industries we examined showed a decrease.



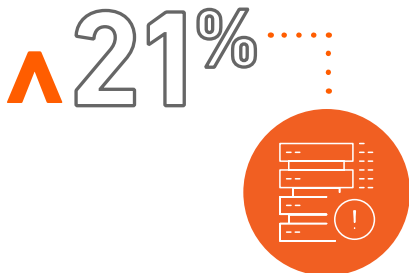
### *IoT MALWARE JUMPS BY MORE THAN A THIRD*

IoT malware continued to climb in the first half of 2023, jumping 37% to 77.9 million. This total represents a new record and puts 2023 on pace to easily eclipse last year's record high of 112.3 million. Following the trend seen in overall malware, IoT malware saw its only decrease in North America, where volumes fell 3% — a drop easily offset by triple-digit spikes in LATAM and Asia. India in particular was hard-hit by these attacks: IoT malware volume there skyrocketed 311%.



### *MALICIOUS PDF & OFFICE FILES FALL BY DOUBLE DIGITS*

Attacks involving malicious PDFs fell 10% in the first half of 2023, but malicious Office files fell far more: Compared with the same time period in 2022, these attacks are down a staggering 75%. Some of this decrease may be due to Microsoft's recent efforts to increase security: Time will tell whether this is a sustained downturn, or whether cybercriminals make inroads around these new restrictions.



### *OVERALL INTRUSION ATTEMPTS RISE*

In the first half of 2023, SonicWall logged 3.7 trillion overall intrusion attempts, an increase of 21% year to date. But while total volume was up, moderate- and high-severity intrusion attempts fell 7% globally. Education customers were targeted at rates far exceeding those seen in other industries: Roughly 39% of these customers saw an attempt each month, up from the same time period last year.

**GET THE FULL UPDATE** — [sonicwall.com/threatreport](https://sonicwall.com/threatreport)

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](https://www.sonicwall.com) or follow us on [Twitter](#), [LinkedIn](#), [Facebook](#) and [Instagram](#).



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

**SONICWALL**

© 2023 SonicWall Inc. ALL RIGHTS RESERVED.  
SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products.  
2023-MidYearThreatReport-ExecSum-JK-8743