Mac Malware Appears on the WatchGuard 'Top Ten Malware List' for First Time

WatchGuard Internet Security Report for Q3 2018 also finds that 6.8 percent of major websites still use an insecure SSL protocol.

SYDNEY – December 12, 2018 – WatchGuard® Technologies, a leader in advanced network security solutions, today issued its quarterly Internet Security Report for Q3 2018: https://www.watchguard.com/wgrd-resource-center/security-report-q3-2018> . For the first time ever, Mac-based malware appeared on WatchGuard's list of the top ten most common types of malware. The report also found that 6.8 percent of the world's top 100,000 websites still accept old, insecure versions of the SSL encryption protocol. Also, WatchGuard saw more malware hits in the Asia Pacific region than in any other geographical region, indicating a significant increase in malware targeting that region throughout 2018. This report is based on data from tens of thousands of active WatchGuard Firebox appliances around the world and covers the major malware campaigns, network attacks and security threats targeting midmarket businesses and distributed enterprises today. "Outside of a few surprising finds, like Mac scareware in our top ten malware list, we saw attackers stick to what they know in Q3 by reusing and modifying old attacks like cross-site scripting, Mimikatz and cryptominers. It's a good reminder that the vast majority of attacks aren't ultra-advanced zero days and can be prevented by using a layered security approach with advanced malware detection capabilities and investing in secure Wi-Fi and MFA solutions," said Corey Nachreiner, CTO at WatchGuard Technologies. "However, we are quite concerned at how many major websites are still using the insecure SSL protocol. This is a basic security best practices that should be implemented across 99.9 percent of the internet by now – it puts hundreds of thousands of users at risk." The insights, research and security best practices included in WatchGuard's quarterly Internet Security Report help organisations of all sizes understand the current cyber security landscape and better protect themselves, their partners and customers from emerging security threats. The top takeaways from the Q3 2018 report include: - 6.8 percent of the top 100,000 websites still support old, insecure versions of the SSL protocol. Despite it being deprecated by the Internet Engineering Task Force (SSL 2.0 was deprecated in 2011 and SSL 3.0 in 2015), 5,383 websites in the top 100,000 via Alexa still accept SSL 2.0 and SSL 3.0 encryption. Also, 20.9 percent of the top 100,000 websites still do not use web encryption at all. - Mac malware cracks the top ten for the first time ever. A piece of Mac scareware appeared in sixth place in WatchGuard's top ten malware list. It is primarily delivered by email and tries to trick victims into installing fake cleaning software. - Hackers target APAC. For the second time ever, APAC reported more total malware hits than EMEA or the USA. Top variants included Razy, which targeted APAC almost exclusively, Win32/Heur and MAC.OSX.AMCleanerCA. - Cryptominers remain popular. Razy, the second most common piece of malware detected by WatchGuard, evolved into a cryptominer in Q3 and made up 4 percent of all malware blocked by WatchGuard antivirus service worldwide. - Mimikatz remains the most popular malware in Q3. This popular password theft kit has dominated WatchGuard's top ten malware list for multiple quarters and shows no sign of slowing down. - Attackers go after web applications with cross-site scripting. Cross-site scripting accounted for 39.3 percent of the top ten exploits in Q3, primarily targeting web applications. The complete Q3 ISR also includes an analysis of the Facebook "View As" data breach. It explains how chaining vulnerabilities together allowed hackers to steal personal information from 50 million Facebook accounts, as well as best practices for security professionals based on the malware and network attack trends explained in this report. s These finding are based on anonymised Firebox Feed data from over 40,000 active WatchGuard UTM appliances worldwide, a substantial increase from the number of Fireboxes reporting in last year. In total, these Fireboxes blocked almost 18 million malware variants (445 per device) and approximately 850,000 network attacks (21 per device) in Q3 2018. For more information, download the full report here: https://www.watchguard.com/wgrd-resource-center/security-report-q3-2018> . To access live, real-time threat insights by type, region and date, visit WatchGuard's Threat Landscape data visualiation tool today: https://www.secplicity.org/threat-landscape/. Subscribe to The 443 – Security Simplified podcast (https://www.secplicity.org/category/the-443/) at Secplicity.org (http://www.secplicity.org/), or wherever you find your favorite podcasts. About WatchGuard Technologies, Inc. WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

##

Contacts

David Bass
+61 2 9922 6820
mailto: david@basspr.com.au
Patricia Gibson
02 9922 6820
mailto: patricia@basspr.com.au