Report: Malicious Cryptocurrency Miners Gaining Momentum, Poised for Continued Growth

WatchGuard's Q1 2018 Internet Security Report reveals a rise in crypto-miner attacks and several geographically targeted malware campaigns

SEATTLE, WASH – June 28, 2018 – WatchGuard® Technologies, a leader in advanced network security solutions, today published its latest Internet Security Report (https://www.watchguard.com/wgrd-resource-center/security-report-q1-2018). Threat intelligence from Q1 2018 revealed that 98.8 percent of seemingly common Linux/Downloader malware variants were actually designed to deliver a popular Linux-based cryptocurrency miner. This is just one of several signs that malicious crypto-mining malware is becoming a top tactic among cyber criminals. The complete report details delivery mechanisms for these crypto-miner attacks, and explores other prevalent security threats targeting small to midsize businesses (SMBs) and distributed enterprises today. "Our Threat Lab team has uncovered multiple indicators that suggest malicious crypto miners are becoming a mainstay in cyber criminals' arsenals, and will continue to grow more dominant in Q2," said Corey Nachreiner, chief technology officer at WatchGuard Technologies. "While ransomware and other advanced threats are still a major concern, these new crypto-miner attacks illustrate that bad actors are constantly adjusting their tactics to find new ways to take advantage of their victims. In fact, once again in Q1, we saw nearly half of all malware slip past basic signature-based antivirus solutions due to various obfuscation methods. One way every organisation can become more secure against these sophisticated, evasive threats is to deploy defences enabled with advanced malware prevention like our APT Blocker service." WatchGuard's Internet Security Report offers in-depth insights on the top cyber threats each quarter, along with defense recommendations SMBs can use to protect themselves. The findings are based on data from tens of thousands of active Firebox UTM appliances around the world. The top takeaways from the Q1 2018 report include:

Cryptocurrency miners are on the rise. Several cryptocurrency miners appeared for the first time in WatchGuard's list of the top 25 malware variants. Firebox appliances have a rule called Linux/Downloader, which catches a variety of Linux "dropper" or "downloader" programs that download and run malware payloads. Usually these droppers download a wide range of malware, but in Q1 2018, 98.8 percent of Linux/Downloader instances were trying to download the same popular Linux-based crypto miner. Evidence from Q2 so far indicates that crypto-mining malware will stay on WatchGuard's top 25 list and may even crack the top 10 by the end of the quarter. The Ramnit trojan makes a comeback in Italy. The only malware sample on WatchGuard's top 10 list that hadn't appeared in a past report was Ramnit, a trojan that first emerged in 2010 and had a brief resurgence in 2016. Nearly all (98.9 percent) of WatchGuard's Ramnit detections came from Italy, indicating a targeted attack campaign. Since past versions of Ramnit have targeted banking credentials, WatchGuard advises Italians to take extra precautions with their banking information and enable multi-factor authentication for any financial accounts. For the first time, APAC reports the highest malware volume. In past reports, APAC has trailed EMEA and AMER in the number of reported malware hits by a wide margin. In Q1 2018, APAC received the most malware overall. The vast majority of these attacks were Windows-based malware and 98 percent were aimed at India and Singapore. Nearly half of all malware eludes basic antivirus (AV) solutions. WatchGuard UTM appliances block malware using both legacy signature-based detection techniques and a modern, proactive behavioural detection solution - APT Blocker. When APT Blocker catches a malware variant, it means the legacy AV signatures missed it. This zero day malware (a term for malware that is able to evade traditional signature-based AV) accounted for 46 percent of all malware in Q1. This level of zero day malware suggests that criminals are continuing to use obfuscation techniques to beat traditional AV services, emphasising the importance of behaviour-based defences. Mimikatz targets the US, skips Asia Pacific. The Mimikatz Windows credential-stealing malware reappeared on WatchGuard's top 10 malware list after several quarters of absence. Two thirds of the detection of this malware was in the United States and under 0.1 percent of detections were in APAC, possibly due to the complexity of double-byte characters in countries like Japan that use a symbol-based language for passwords. The complete Internet Security Report features a detailed breakdown of the record-breaking GitHub 1.35 Tbps DDoS attack, as well as analysis of the quarter's top malware and network attacks, and key defence tactics for SMBs. This quarter's conclusions are based on anonymised Firebox Feed data from nearly 40,000 active WatchGuard UTM appliances worldwide, which blocked more than 23 million malware variants (628 per device) and over 10 million network attacks (278 per device) in Q1 2018. Don't miss the new podcast, The 443 – Security Simplified (https://www.secplicity.org/category/the-443), from the team behind the Internet Security Report and Secplicity.org. Each week, they will analyse the methods and techniques behind the latest hacks, attacks, and breaches. They'll detail what happened, how the bad guys did it, and provide actionable insights businesses can use to protect themselves. For more information, download the full report here: https://www.watchguard.com/wgrd-resource-center/security-report-q1-2018. To access live, real-time threat insights by type, region and date, visit WatchGuard's Threat Landscape data visualisation tool (https://www.secplicity.org/threat-landscape) today. 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 favourite podcasts. About WatchGuard Technologies, Inc. WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 80,000 customers worldwide. The company'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. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook: https://www.facebook.com/watchguardtechnologies, or on the LinkedIn Company (http://www.linkedin.com/company/watchguard-technologies) page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Contacts

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