New Research Shows Surge in Mac Malware, Malicious Office Documents and Web Application Exploits in Q1 2019

WatchGuard's Q1 2019 Internet Security Report highlights the increasingly dire need for a layered approach to security

SEATTLE – June 25, 2019 – WatchGuard® Technologies, a global leader in network security and intelligence, secure Wi-Fi and multi-factor authentication, today announced the release of its quarterly Internet Security Report for Q1 2019 (https://www.watchguard.com/wgrd-resource-center/security-report-q1-2019). Amid a massive 62% increase in overall malware detections compared to Q4 2018, the report found that cyber criminals are leveraging a wide array of varied attack techniques, including malicious Microsoft Office documents, Mac malware and web application exploits. Overall, these results illustrate that in 2019, hackers are doubling down on well-known tactics like credential theft and ransomware by utilising fake Office documents and other attack avenues that require organisations to deploy advanced defenses to combat a wider variety of threat vectors. "The key findings from this latest report illustrate the importance of layered security protections in today's advanced threat landscape," said Corey Nachreiner, chief technology officer at WatchGuard Technologies. "Whether it be DNS-level filtering to block connections to malicious websites and phishing attempts, intrusion prevention services to ward off web application attacks, or multi-factor authentication to prevent attacks leveraging compromised credentials – it's clear that modern cyber criminals are leveraging a bevy of diverse attack methods and the best way for organisations to protect themselves is with a unified security platform that offers a comprehensive range of security services." WatchGuard's Internet Security Report is designed to provide the threat intelligence, research and security best practices organisations need to defend against online adversaries and better protect their data. Key findings from the Q1 2019 report include: WatchGuard's Internet Security Report is designed to provide the threat intelligence, research and security best practices organisations need to defend against online adversaries and better protect their data. Key findings from the Q1 2019 report include: Attackers continue to favor malicious Office documents – In Q1 2019, more than 17% of Fireboxes blocked malicious Office documents, with two threats in this category making it into WatchGuard's most widespread malware list, and one in the top 10 malware attacks by volume. Over half of these malicious documents were blocked in EMEA, largely in Eastern European countries. Users should avoid interacting with unsolicited Office documents and consider any attachments that seek to enable macros as a threat.

Mac OS malware on the rise – Mac malware first appeared on WatchGuard's top 10 malware list in Q3 2018, and now two variants have become prevalent enough to make the list in Q1 2019. This increase in Mac-based malware further debunks the myth that Macs are immune to viruses and malware, and reinforces the importance of advanced threat protection for all devices and systems. Web application exploits soar – Despite a decrease in the overall volume of network attacks in Q1, web application attacks grew significantly. WatchGuard's IPS service caught attackers exploiting many cross-site scripting (XSS) and SQL injection (SQLi) vulnerabilities – both popular methods for credential theft. Two SQIi attacks made it onto WatchGuard's top 10 network attacks list, while one web XSS attack accounted for more than 10% of network attacks on the top 10 list overall. DNS filtering blocks more than 5 million malicious sites – WatchGuard's DNSWatch service successfully prevented 5,192,883 attempted visits to nefarious destinations, blocking over half a million connections to known malware-hosting domains, 187,101 connections to compromised websites and 61,096 connections to known phishing sites. Compromised websites can be difficult to identify and block, so DNS-level filtering is critical to prevent users from unknowingly falling victim to malware infections, credential theft or botnet command and control systems. Fileless malware stakes its claim – Fileless threats appeared in both WatchGuard's top 10 malware and top 10 network attack lists. On the malware side, a PowerShell-based code injection attack showed up in the top 10 list for the first time in Q1, while the popular fileless backdoor tool, Meterpreter, made its first appearance in the top 10 list of network attacks too. This trend further demonstrates cyber criminals' continued focus on utilizing this evasive threat category. Mimikatz malware skyrockets by 73%, remains the #1 threat – Accounting for 20.6% of all malware found in Q1, this popular open source tool is often used for password theft, and represents a major driver behind many network infiltrations. Mimikatz is a mainstay on WatchGuard's top 10 malware list, which highlights the importance of using lengthy, complex passwords unique to each individual account. Furthermore, with cyber criminals' persistent focus on credential theft, organisations of all sizes should consider adopting multi-factor authentication solutions in order to prevent bad actors from compromising legitimate user accounts. WatchGuard's Internet Security Report is based on anonymized Firebox Feed data from a subset of active WatchGuard UTM appliances whose owners have opted in to data-sharing to support the Threat Lab's research efforts. Today, 42,372 appliances throughout the world contribute to the Internet Security Report data pool. In total, those appliances blocked more than 23,884,979 malware variants, at a rate of 564 samples blocked per device. Additionally, those Firebox appliances prevented 989,759 network attacks (23 per device). The complete report explores the most impactful malware and attack trends from Q1 2019, a detailed analysis of the historic "51% attack" against the cryptocurrency Ethereum Classic (ETC) that resulted in $1.1 million in loses, and cyber security advice readers can use to better protect themselves and their organizations. For more information, download the full report

here: https://www.watchguard.com/wgrd-resource-center/security-report-q1-2019 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. 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 page: http://www.linkedin.com/company/watchguard-technologies. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at: www.secplicity.org. 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. WatchGuard is a registered trademark of WatchGuard Technologies, Inc. All other marks are property of their respective owners. ###

Contacts

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