WatchGuard Finds Attacks Targeting Leading Web Conference Solution Exploding in Popularity in Q4 2018

WatchGuard's Internet Security Report for Q4 2018 also finds growing use of a new sextortion phishing malware customised to individual victims

SEATTLE, WASH – March 21, 2019 – WatchGuard® Technologies, a leader in advanced network security solutions, today issued its quarterly Internet Security Report for Q4 2018. It found that network attacks targeting a vulnerability in the Cisco Webex Chrome extension increased in popularity dramatically, rising to be the second-most common network attack after being almost non-existent in early 2018. Phishing campaigns showed a dangerous increase in sophistication in Q4, with new attacks utilising advanced methods such as threatening to release recordings of users visiting adult content online, customising emails for specific targets and creating fake banking login web pages. Based on data from tens of thousands of active WatchGuard Firebox appliances around the world, the complete report examines the top malware and network attacks targeting mid-market businesses and distributed enterprises today. "There was a noticeable increase in advanced phishing attacks targeting high-value information this quarter," said Corey Nachreiner, CTO at WatchGuard Technologies. "Now more than ever, it's vital for businesses to take the layered approach to security, and deploy solutions like WatchGuard's DNSWatch that offer DNS-level filtering designed to detect and block potentially dangerous connections and automatically refer employees to resources that bolster phishing awareness and prevention. A combination of security controls and human training will help businesses avoid becoming hooked by phishing attacks." 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 Q4 2018 report include: New network attack targets Cisco Webex Chrome extension – A new network attack targeting a remote code execution vulnerability in the Chrome extension for Cisco Webex exploded in popularity last quarter. This vulnerability was disclosed and patched in 2017, but WatchGuard detected almost no network attacks targeting it until now. Detections grew by 7,016 percent from Q3 to Q4. This spike shows just how important it is to install security patches as soon as they are available. New customised "sextortion" phishing campaign on the rise – A new "sextortion" phishing attack was the second-most common attack that our malware engines detected in Q4 2018, mainly targeting APAC. It accounts for almost half of all of the unique malware hashes detected in Q4 because the email phishing message is tailored to each recipient. The message claims the sender has infected the victim's computer with a trojan and recorded them visiting adult websites. It threatens to send these compromising images to their email contacts unless they pay a ransom. WatchGuard saw a significant amount of this malware in Q4 and all users should be on the lookout for these fake emails. 16.5 percent of all Fireboxes were targeted by CoinHive cryptominer – The most widespread malware variant in Q4 came from the popular CoinHive cryptominer family, showing that cryptomining remains a popular attack type. Two of the top ten most common pieces of malware detected in Q4 were also cryptominers, carrying over from past quarters. A major phishing attack leverages a fake bank page – Another widespread piece of malware in Q4 sent a phishing email with a fake, but highly realistic Wells Fargo login page to capture victim emails and passwords. Overall, WatchGuard saw a rise in sophisticated phishing attacks targeting banking credentials in Q4. One ISP's filtering error routed Google traffic through Russia and China for 74 minutes – The report includes a technical analysis of a Border Gateway Protocol (BGP) hijack in November 2018 that inadvertently sent most of Google's traffic through Russia and China for a short time. WatchGuard found that a Nigerian ISP called MainOne made a mistake in their routing filters, which then spread to Russian and Chinese ISPs and caused much of Google's traffic to be routed through these ISPs unnecessarily. This accidental hijack highlights how insecure many of the underlying standards that the internet is based on are. A sophisticated attack targeting these flaws could have potentially catastrophic consequences. Network attacks rise after historic lows in mid-2018 – Network attacks rose 46 percent by volume and 167 percent in terms of unique signature hits in Q4 compared to Q3. This follows a trend seen in previous years with attacks ramping up during the holiday season. The Q4 ISR also includes a granular analysis of source code for the Exobot banking trojan. This highly sophisticated malware attempts to steal banking and financial information from Android devices. The WatchGuard Threat Lab's analysis includes a list of the 150 sites such as Amazon, Facebook Paypal and Western Union that Exobot can automatically target, as well as a detailed look at the UI an attacker using Exobot would use to push commands to infected devices. These finding are based on anonymised Firebox Feed data from over 42,000 active WatchGuard UTM appliances worldwide. In total, these Fireboxes blocked over 16 million malware variants (382 per device) and approximately 1,244,000 network attacks (29 per device) in Q4 2018. For more information, download the full report here: https://www.watchguard.com/wgrd-resource-center/security-report-q4-2018 To access live, real-time threat insights by type, region and date, visit WatchGuard's Threat Landscape data visualization tool (https://www.secplicity.org/threat-landscape/) today. Subscribe to The 443 – Security Simplified podcast at www.secplicity.orgwherever you find your favourite 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. To learn more, visit: www.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 (https://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