WatchGuard Technologies Report Finds Two-Thirds of Malware is Encrypted, Invisible Without HTTPS Inspection

Q1 2020 Internet Security Report highlights the danger of encrypted malware, offers details about the security impact of the COVID-19 pandemic, as well as a surge in Monero cryptominers, Flawed-Ammyy and Cryxos malware, and more

SEATTLE – June 24, 2020 – WatchGuard® Technologies, a global leader in network security and intelligence, secure Wi-Fi, multi-factor authentication and advanced endpoint protection, today announced the release of its Internet Security Report for Q1 2020. For the first time ever, this report includes data on the percentage of malware in the wild delivered via encrypted HTTPS connections. WatchGuard's threat intelligence shows that 67% of all malware in Q1 was delivered via HTTPS, so organisations without security solutions capable of inspecting encrypted traffic will miss two-thirds of incoming threats.

Additionally, 72% of encrypted malware was classified as zero day (meaning no antivirus signature exists for it, and it will evade signature-based protections). These findings show that HTTPS inspection and advanced behavior-based threat detection and response solutions are now requirements for every security-conscious organization. The report also includes a special section detailing the impact of COVID-19 on the threat landscape.

"Some organisations are reluctant to set up HTTPS inspection due to the extra work involved, but our threat data clearly shows that a majority of malware is delivered through encrypted connections and that letting traffic go uninspected is simply no longer an option," said Corey Nachreiner, chief technology officer at WatchGuard. "As malware continues to become more advanced and evasive, the only reliable approach to defense is implementing a set of layered security services, including advanced threat detection methods and HTTPS inspection."

WatchGuard's Internet Security Report prepares midmarket businesses, the service providers that support them, and the end users that work for them with data on the trends, research and best practices they need to defend against modern security threats. Here are the key findings from the Q1 2020 report:

Monero cryptominers surge in popularity. Five of the top ten domains distributing malware in Q1 (identified by WatchGuard's DNS filtering service DNS Watch) either hosted or controlled Monero cryptominers. This sudden jump in cryptominer popularity could simply be due to its utility; adding a cryptomining module to malware is an easy way for online criminals to generate passive income.

Flawed-Ammyy and Cryxos malware variants join top lists. The Cryxos trojan was third on WatchGuard's top-five encrypted malware list and also third on its top-five most widespread malware detections list, primarily targeting Hong Kong. It is delivered as an email attachment disguised as an invoice and will ask the user to enter their email and password, which it then stores. Flawed-Ammyy is a support scam where the attacker uses the Ammyy Admin support software to gain remote access to the victim's computer.

Three-year-old Adobe vulnerability appears in top network attacks. An Adobe Acrobat Reader exploit that was patched in Aug. 2017 appeared in WatchGuard's top network attacks list for the first time in Q1. This vulnerability resurfacing several years after being discovered and resolved illustrates the importance of regularly patching and updating systems.

Mapp Engage, AT&T and Bet365 targeted with spear phishing campaigns. Three new domains hosting phishing campaigns appeared on WatchGuard top-ten list in Q1 2020. They impersonated digital marketing and analytics product Mapp Engage, online betting platform Bet365 (this campaign was in Chinese) and an AT&T login page (this campaign is no longer active at the time of the report's publication).

COVID-19 Impact. Q1 2020 was only the start of the massive changes to the cyber threat landscape brought on by the COVID-19 pandemic. Even in just these first three months of 2020, we still saw a massive rise in remote workers and attacks targeting individuals.

Malware hits and network attacks decline. Overall there were 6.9% fewer malware hits and 11.6% fewer network attacks in Q1, despite a 9% increase in the number of Fireboxes contributing data. This could be attributed to fewer potential targets operating within the traditional network perimeter with worldwide work-from-home policies in full force during the COVID-19 pandemic.

Great Britain and Germany heavily targeted by widespread malware threats. WatchGuard's most widespread malware list showed Germany and Great Britain were top targets for almost all of the most prevalent malware in Q1.
Third-party testing has found that WatchGuard products consistently maintain high throughput when inspecting HTTPS traffic. Many competitive products show a significant degradation in performance in this scenario. For example, an independent test performed by Miercom found that the Firebox M370 outperformed competitive products while inspecting HTTPS traffic with full security services enabled.

The findings in WatchGuard's Internet Security Reports are drawn from anonymised Firebox Feed data from active WatchGuard appliances whose owners have opted in to share data to support the Threat Lab's research efforts. Today, over 44,000 appliances worldwide contribute threat intelligence data to the report. In Q1 2020, they blocked over 32,148,519 malware variants in total (730 samples per device) and more than 1,660,000 network attacks (38 attacks per device).

The complete report includes key defensive best practices that organizations of all sizes can use to protect themselves in today's threat landscape and a detailed analysis of how the COVID-19 pandemic and associated shift to working from home affected the cyber security landscape.

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 midmarket businesses and distributed enterprises. 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 (https://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: http://www.secplicity.org. Subscribe to The 443 – Security Simplified podcast at: https://www.secplicity.org or wherever you find your favourite podcasts.

###

Contacts

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