New Research Shows Cybersecurity Battleground Shifting to Linux and Web Servers

WatchGuard's Internet Security Report evaluates the quarter's top threats, provides an analysis of the CIA Vault 7 leak, and features new research on IoT cameras

WatchGuard® Technologies, a leader in advanced network security solutions, today announced the findings of its quarterly Internet Security Report, which explores the latest computer and network security threats affecting small to midsize businesses (SMBs) and distributed enterprises. Among its most notable findings, the report revealed that despite an overall drop in general malware detection for the quarter, Linux malware made up more than 36 percent of the top threats identified in Q1 2017. This attack pattern demonstrates the urgent need for heightened security measures to protect Linux servers and Linux-dependent IoT devices.

"This new Firebox Feed data allows us to feel the pulse of the latest network attacks and malware trends in order to identify patterns that influence the constantly evolving threat landscape," said Corey Nachreiner, chief technology officer at WatchGuard Technologies. "The Q1 report findings continue to reinforce the importance and effectiveness of basic security policies, layered defenses and advanced malware prevention. We urge readers to examine the report's key takeways and best practices, and bring them to the forefront of information security efforts within their organisations."

WatchGuard's Internet Security Report is designed to offer educational insights, research and security recommendations to help readers better protect themselves and their organisations against modern threat actors. Key findings from the Q1 2017 report include:

- Linux malware is on the rise, making up 36 percent of the top malware detected in Q1. The increased presence of Linux/Exploit, Linux/Downloader and Linux/Flooder combined to illustrate attackers' increased focus on Linux servers and IoT devices. Users should protect IoT products and Linux servers from the internet with layered defenses.

- Legacy antivirus (AV) continues to miss new malware – at a higher rate. In fact, AV solutions missed 38 percent of the total threats WatchGuard caught in Q1, compared to 30 percent in Q4 2016. The growing number of new or zero day malware now evading traditional AV highlights the weaknesses of signature-based detection solutions and the need for services that can detect and deter advanced persistent threats.

- The cybersecurity battleground is shifting toward web servers. Last quarter, drive-by downloads and browser-based attacks were predominant. In Q1, 82 percent of the top network attacks targeted web servers (or other web-based services). Users should strengthen web server defenses by hardening permissions, limiting resource exposure, and patching server software.

- Attackers still exploit the Android StageFright flaw. This exploit first gained notoriety in 2015, and is proving its longevity as the first mobile-specific threat to hit WatchGuard Threat Lab's top 10 attacks list this year. At a minimum, Android users should regularly upgrade their operating systems to prevent mobile attacks like StageFright.

- Threat actors take a break from hacking the holidays. Overall, threat volume decreased 52% in Q1 2017 compared to Q4 2016. We believe the drop in malware detections can be attributed to the absence of seasonal malware campaigns associated with various Q4 holidays, which increased overall malware instances during that period.

WatchGuard's Internet Security Report is based on anonymised Firebox Feed data from more than 26,500 active WatchGuard UTM appliances worldwide, representing a small portion of our overall install base. These appliances blocked more than 7 million malware variants in Q1, representing an average of 266 samples blocked by each individual device. WatchGuard appliances also blocked more than 2.5 million network attacks in Q1, which equates to 156 attacks blocked per device. The complete report includes a breakdown of the quarter's top malware and attack trends, an analysis of the CIA Vault 7 leaks and key defensive learnings for readers. The report also features a new research project from the WatchGuard Threat Lab, which focuses on a new vulnerability in a popular IoT camera.

For more information, download the full report here: www.watchguard.com/security-report

About WatchGuard Technologies, Inc.

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 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, or on the LinkedIn Company 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.

###