# WatchGuard's Q2 Internet Security Report Finds Malware Hiding on Popular Content Delivery Networks

## Data also shows Kali Linux modules cracking malware top ten list and a dramatic year-over-year increase in overall malware volume

Sydney – Sept 27, 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 Q2 2019. For the first time, the report reveals and ranks the most common domains attackers use to host malware and launch phishing attacks – including several subdomains of legitimate sites and Content Delivery Networks (CDNs) such as CloudFlare.net, SharePoint and Amazonaws.com. It also highlights that modules from the popular Kali Linux penetration testing tool made the top ten malware list for the first time, year-over-year malware volume increased by 64%, and more. "This edition of the Internet Security Report exposes the gritty details of the methods hackers use to sneak malware or phishing emails onto networks by hiding them on legitimate content-hosting domains," said Corey Nachreiner, chief technology officer at WatchGuard Technologies. "Luckily there are several ways to defend against this, including DNS-level filtering to block connections to known malicious websites, advanced anti-malware services, multi-factor authentication to prevent attacks leveraging compromised credentials, and training to help employees recognise phishing emails. No one defense will prevent every attack, so the best way for organisations to protect themselves is with a unified security platform that offers multiple layered security services." WatchGuard's Internet Security Report provides real-world data on top security threats, as well as detailed analysis of major security incidents and best practices to help organisations of all sizes protect their business and their customers' data. Key findings from the Q2 2019 report include: Malware and phishing attacks abusing legitimate domains – WatchGuard's DNS Watch service intercepts connections intended for known malicious domains at the DNS level and redirects them. By tracking the most common malicious domains blocked by DNSWatch, WatchGuard can identify the top domains hosting malware and phishing attacks. Of note, several of these domains are subdomains of legitimate CDNs like CloudFront.net (which belongs to Amazon) and legitimate file-sharing websites like my[.]mixtape[.]moe. While this attack method isn't new, WatchGuard's research sheds light on the specific domains used in these attacks. Kali Linux makes its debut on the top ten malware list – For the first time ever, two modules from the popular hacking operating system Kali Linux appear on WatchGuard's list of most common malware. Trojan.GenericKD, which covers a family of malware that creates a backdoor to a command-and-control server, and Backdoor.Small.DT, a web shell script used to create backdoors on web servers, were numbers six and seven on the list. This could indicate either growing adoption among malicious actors or more penetration testing by white hat hackers using Kali Linux. Significant year-over-year increase in overall malware volume – Across the board, the total volume of malware hitting WatchGuard Fireboxes is up significantly compared to last year. Two of WatchGuard's three malware detection services saw increased malware in Q2 2019 than Q2 2018; one blocked 58% more and the other blocked 68% more, for an overall year-over-year increase of 64%. Widespread phishing and Office exploit malware increases – Two pieces of malware (a phishing attack that threatens to release fake compromising information on the victim, and a Microsoft Office exploit) that appeared on the most widespread malware list in Q1 2019 and Q4 2018 have graduated to the top ten list by volume. This illustrates that these campaigns are on the rise and are sending a high volume of attacks at a wide range of targets. Users should update Office regularly and invest in anti-phishing and DNS filtering security solutions. SQL injection dominates network attacks – SQL injection attacks made up 34% of all network attacks detected in Q2 2019 and have increased significantly in volume year-over-year (one specific attack increased over 29,000% from Q2 2018 to Q2 2019). Anyone who maintains a SQL database, or a web server with access to one, should patch systems regularly and invest in a web application firewall. Malware increasingly targets Europe and APAC – In Q2 2019, nearly 37% of malware targeted the EMEA region, with several individual attacks focusing on the UK, Italy, Germany, and Mauritius. APAC came in second, targeted by 36% of overall malware attacks. The Razy and Trojan.Phishing.MH malware variants in particular primarily targeted the APAC region, with 11% of Trojan.Phishing.MH detections found in Japan. WatchGuard's Internet Security Report is based on anonymised Firebox Feed data from a subset of active WatchGuard UTM appliances whose owners have opted in to share data to support the Threat Lab's research efforts. Today, 41,229 appliances throughout the world contribute to the Internet Security Report data pool. In total, those appliances blocked more than 22,619,836 malware variants, at a rate of 549 samples per device. Additionally, those Firebox appliances prevented 2,265,425 network attacks (60 per device), a significant increase from Q1 2019 that runs counter to past trends in network attack volume. The complete report includes more detailed statistics on the most impactful malware and network attack trends from Q2 2019, an analysis of the RobbinHood ransomware attack that paralysed the city of Baltimore in May 2019 (and cost approximately $17 million in total damages), and advice and best practices that readers can use to better protect themselves and their organisations. Analysis of MSP Sodinokibi Ransomware Attacks The report also contains a detailed analysis of the actual malware used in the Sodinokibi MSP ransomware attacks. The WatchGuard Threat Lab's research shows that the attackers leveraged weak, stolen, or leaked credentials to gain administrative access to legitimate management tools that these MSPs used to monitor and manage their clients' networks, then used these tools to disable security controls and stage and deliver the Sodinokibi ransomware via PowerShell. For more information, download the full report here: https://www.watchguard.com/wgrd-resource-center/security-report-q2-2019 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 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 (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 favourite 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