WatchGuard Research Finds 12% Spike in Evasive Threats Despite Decrease in Overall Malware Volume

New report underscores the importance of layered security as zero day malware variants, JavaScript malware attacks and Microsoft Excel-based threats rise

SEATTLE – 24 September , 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 Q2 2020 (https://www.watchguard.com/wgrd-resource-center/security-report-q2-2020). Among its most notable findings the report showed that despite an 8% decrease in overall malware detections in Q2, 70% of all attacks involved zero day malware (variants that circumvent antivirus signatures), which represents a 12% increase over the previous quarter.

“Businesses aren’t the only ones that have adjusted operations due to the global COVID-19 pandemic – cyber criminals have too,” said Corey Nachreiner, CTO of WatchGuard. “The rise in sophisticated attacks, despite the fact that overall malware detections declined in Q2 (likely due to the shift to remote work), shows that attackers are turning to more evasive tactics that traditional signature-based anti-malware defenses simply can’t catch. Every organization should be prioritising behaviour-based threat detection, cloud-based sandboxing, and a layered set of security services to protect both the core network, as well as remote workforces.”

WatchGuard’s Internet Security Report provides a detailed look at the latest malware and network attack trends, in-depth threat research and recommended security best practices organisations can leverage to better protect themselves, their partners and customers. Key findings from the Q2 2020 report include:

Attackers Continue to Leverage Evasive and Encrypted Threats – Zero day malware made up more than two-thirds of the total detections in Q2, while attacks sent over encrypted HTTPS connections accounted for 34%. Organisations that aren’t able to inspect encrypted traffic will miss a massive one-third of incoming threats. Even though the percentage of threats using encryption decreased from 64% in Q1, the volume of HTTPS-encrypted malware increased dramatically. It appears that more administrators are taking the necessary steps to enable HTTPS inspection on Firebox security appliances, but there’s still more work to be done.

JavaScript-based Attacks Are on the Rise – The scam script Trojan.Gnaeus made its debut at the top of WatchGuard’s top 10 malware list for Q2, making up nearly one in five malware detections. Gnaeus malware allows threat actors to hijack control of the victim’s browser with obfuscated code, and forcefully redirect away from their intended web destinations to domains under the attacker’s control. Another popup-style JavaScript attack, J.S. PopUnder, was one of the most widespread malware variants last quarter. In this case, an obfuscated script scans a victim’s system properties and blocks debugging attempts as an anti-detection tactic. To combat these threats, organisations should prevent users from loading a browser extension from an unknown source, keep browsers up to date with the latest patches, use reputable adblockers and maintain an updated anti-malware engine.

Attackers Increasingly Use Encrypted Excel Files to Hide Malware – XML-Trojan.Abracadabra is a new addition to WatchGuard’s top 10 malware detections list, showing a rapid growth in popularity since the technique emerged in April. Abracadabrais a malware variant delivered as an encrypted Excel file with the password “VelvetSweatshop” (the default password for Excel documents). Once opened, Excel automatically decrypts the file and a macro VBA script inside the spreadsheet downloads and runs an executable. The use of a default password allows this malware to bypass many basic antivirus solutions since the file is encrypted and then decrypted by Excel. Organisations should never allow macros from an untrusted source, and leverage cloud-based sandboxing to safely verify the true intent of potentially dangerous files before they can cause an infection.

An Old, Highly Exploitable DoS Attack Makes a Comeback – A six-year-old denial of service (DoS) vulnerability affecting WordPress and Drupal made an appearance on WatchGuard’s list of top 10 network attacks by volume in Q2. This vulnerability is particularly severe because it affects every unpatched Drupal and WordPress installation and creates DoS scenarios in which bad actors can cause CPU and memory exhaustion on underlying hardware. Despite the high volume of these attacks, they were hyper-focused on a few dozen networks primarily in Germany. Since DoS scenarios require sustained traffic to victim networks, this means there’s a strong likelihood that attackers were selecting their targets intentionally.

Malware Domains Leverage Command and Control Servers to Wreak Havoc – Two new destinations made WatchGuard’s top malware domains list in Q2. The most common was findresults[.]site, which uses a C&C server for a Dadobra trojan variant that creates an obfuscated file and associated registry to ensure the attack runs and can exfiltrate sensitive data and download additional malware when users start up Windows systems. One user alerted the WatchGuard team to Cioco-froll[.]com, which uses another C&C server to support an Asprox botnet variant (often delivered via PDF

document) and provides a C&C beacon to let the attacker know it has gained persistence and is ready to participate in the botnet. DNS firewalling can help organisations detect and block these kinds of threats independent of the application protocol for the connection.
WatchGuard's quarterly research reports are based on anonymized Firebox Feed data from active WatchGuard appliances whose owners have opted in to share data to support the Threat Lab's research efforts. In Q2, nearly 42,000 WatchGuard appliances contributed data to the report, blocking a total of more than 28.5 million malware variants (684 per device) and more than 1.75 million network threats (42 per device). Firebox appliances collectively detected and blocked 410 unique attack signatures in Q2, a 15% increase over Q1 and the most since Q4 2018.

The complete report includes more insights on the top malware and network trends affecting midmarket businesses today, as well as recommended security strategies and best practices to defend against them. The report also includes a detailed analysis of the recent data breach spree brought on by hacking group ShinyHunters.

Read WatchGuard's full Q2 2020 Internet Security Report here today: https://www.watchguard.com/wgrd-resource-center/security-report-q2-2020.

About WatchGuard Technologies, Inc.

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, advanced endpoint protection, 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: https://www.secplicity.org/category/the-443. Subscribe to The 443 – Security Simplified podcast at Secplicity.org (https://www.secplicity.org/category/the-443/) or wherever you find your favourite podcasts.

ENDS

Contacts

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