Report: Macro-less Word Document Attacks on the Rise, Zero Day Malware Variants Jump 167 Percent

WatchGuard Launches Threat Landscape visualization tool for analysing Firebox Feed data to better understand security threats

SYDNEY – March 29, 2018 – WatchGuard® Technologies, a leader in advanced network security solutions, today announced new research findings from its Internet Security Report for Q4 2017. Among the report's most notable findings, threat intelligence from Firebox appliances protecting small and midsize businesses (SMBs) and distributed enterprises around the world showed that total malware attacks are up by 33 percent, and that cyber criminals are increasingly leveraging Microsoft Office documents to deliver malicious payloads. WatchGuard has also launched a new Threat Landscape data visualisation tool (https://www.secplicity.org/threat-landscape), available for the public to access to daily updates about the most prevalent computer and network security threats affecting SMBs and distributed enterprises. "After a full year of collecting and analysing Firebox Feed data, we can clearly see that cyber criminals are continuing to leverage sophisticated, evasive attacks and resourceful malware delivery schemes to steal valuable data," said Corey Nachreiner, chief technology officer at WatchGuard Technologies. "Although these criminal tactics may vary over time, we can be certain that this broad trend will persist, so the risks have never been greater for small and midsize organisations with less IT and security resources. We encourage businesses of all sizes to proactively mitigate these threats with layered security services, advanced malware protection, and employee education and training in security best practices." WatchGuard's Internet Security Report provides a quarterly update on the most ubiquitous security threats targeting businesses today, as well key strategies they can use to protect employees, customers and stakeholders from data theft. The top takeaways from the Q4 2017 report include: · Cyber criminals leveraged malicious Office documents to trick victims. Dynamic Data Exchange (DDE) attacks cracked WatchGuard's top ten malware list in Q4, as hackers increasingly exploited issues within this Microsoft Office standard to execute code. Also called "macro-less malware," these malicious documents often use PowerShell and obfuscated script to get past network defences. Additionally, two of the top-ten network attacks in Q4 involved Microsoft Office exploits, further emphasising the growing trend of malicious document attacks. · Overall malware attacks grew significantly, while zero day malware variants jumped 167 percent. WatchGuard Fireboxes blocked over 30 million total malware variants in Q4, which was a 33 percent increase over the previous quarter. Out of the total threats prevented in Q4, the subset of new or "zero day" malware instances rose steeply by 167 percent compared to Q3. These increases can likely be attributed to heightened criminal activity during the holiday season. · Nearly half of all malware eluded basic antivirus (AV) solutions. WatchGuard Fireboxes block malware using both legacy signature-based detection techniques and the modern, proactive behavioural detection solution – APT Blocker (https://www.watchguard.com/wgrd-products/security-services/apt-blocker). When APT Blocker catches a malware variant, it means the legacy AV signatures missed it. This zero day malware accounted for 46 percent of all malware in Q4. That level of growth suggests criminals are using more sophisticated evasion techniques capable of slipping attacks past traditional AV services, which further underscores the importance of behaviour-based defences. · Scripting attacks account for 48 percent of top malware. Script-based attacks caught by signatures for JavaScript and Visual Basic Script threats, such as downloaders and droppers, accounted for the majority of malware detected in Q4. Users should take note of the continued popularity of these attacks and watch out for malicious script in web pages and email attachments of any kind. The full Internet Security Report features evaluations of the quarter's most pervasive malware and network attacks, recommendations for useful defensive strategies in today's threat landscape, and a detailed breakdown of "the Krack Attack" – one of the top information security issues in 2017. Additionally, the report includes a new research project from the WatchGuard Threat Lab, which analyses a database of more than 1 billion stolen password records to stress just how often users choose weak passwords and re-use credentials across multiple accounts. This quarter's conclusions are based on anonymised Firebox Feed data from nearly 40,000 active WatchGuard Fireboxes worldwide, which blocked more than 30 million malware variants (783 per device) and 6.9 million network attacks (178 per device) in Q4 2017. New Threat Landscape Data Visualization Tool WatchGuard's new Threat Landscape data visualisation tool (https://www.secplicity.org/threat-landscape/) offers daily security insights regarding the top malware and network attacks around the globe. The Threat Landscape page enables users to search Firebox Feed data a by type of attack, region or country, and targeted date ranges, with interactive graphics that are updated instantly and easy to read. To access live, real-time threat insights by type, region and date, visit WatchGuard's Threat Landscape page: https://www.secplicity.org/threat-landscape About WatchGuard Technologies, Inc. WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 80,000 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 <http://www.watchguard.com/> . Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org <http://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