New Security Research Reveals Password Inadequacy a Top Threat, Need for Multi-Factor Authentication

WatchGuard's Q2 2018 Internet Security Report uncovers cybercriminals' heightened use of credential-focused attacks, the continued prevalence of malicious Office documents, and more

SEATTLE, WASH – September 12, 2018 – WatchGuard® Technologies, a leader in advanced network security solutions, today announced the findings of its Internet Security Report for Q2 2018, which explores the latest security threats affecting small to midsize businesses (SMBs) and distributed enterprises. The new research from the WatchGuard Threat Lab revealed that 50 percent of government and military employee LinkedIn passwords were weak enough to be cracked in less than two days. This finding, along with the emergence of the Mimikatz credential-stealing malware as a top threat and the popularity of brute force login attacks against web applications, underscores the reality that passwords alone can't offer sufficient protection, and emphasises the need for multi-factor authentication (MFA) solutions in every organisation. "Authentication is the cornerstone of security, and we're seeing overwhelming evidence of its critical importance in the common trend of password- and credential-focused threats throughout Q2 2018," said Corey Nachreiner, chief technology officer at WatchGuard Technologies. "Whether it's an evasive credential-stealing malware variant or a brute force login attack, cyber criminals are laser-focused on hacking passwords for easy access to restricted networks and sensitive data. At WatchGuard, these trends are driving new innovative defenses within our product portfolio, including AuthPoint, our Cloud-based multi-factor authentication solution and our IntelligentAV service, which leverages three malware detection engines to prevent malware strains that evade traditional signature-based antivirus products. Every organisation should seek out vendor and solution provider partners that offer layered protection against these ever-evolving attack techniques." The insights, research and security best practices included in WatchGuard's quarterly Internet Security Report are designed to help organisations of all sizes understand the current cyber security landscape and better protect themselves, their partners and customers from emerging security threats. The top takeaways from the Q2 2018 report include: - Roughly half of government and military employee passwords are weak. After conducting a thorough analysis of the 2012 LinkedIn data dump to identify trends in user password strength, WatchGuard's Threat Lab team found that half of all passwords associated with ".mil" and ".gov" email address domains within the database were objectively weak. Of the 355,023 government and military account passwords within the database, 178,580 were cracked in under two days. The most common passwords used by these accounts included "123456," "password," "linkedin," "sunshine," and "111111." Conversely, the team found that just over 50 percent of civilian passwords were weak. These findings further illustrate the need for stronger passwords for everyone, and a higher standard for security among public service employees that handle potentially sensitive information. In addition to better password training and processes, every organisation should deploy multi-factor authentication solutions to reduce the risk of a data breach. - Mimikatz was the most prevalent malware variant in Q2. Representing 27.2 percent of the top 10 malware variants listed last quarter, Mimikatz is a well-known password and credential stealer that has been popular in past quarters, but has never been the top strain. This surge in Mimikatz's dominance suggests that authentication attacks and credential theft are still major priorities for cyber criminals – another indicator that passwords alone are inadequate as a security control, and should be fortified with MFA services that make hackers' lives harder by requiring additional authentication factors in order to successfully login and access the network. - More than 75 percent of malware attacks are delivered over the web. A total of 76 percent of threats from Q2 were web-based, suggested that organisations need an HTTP and HTTPS inspection mechanism to prevent the vast majority of attacks. Ranked as the fourth most prevalent web attack in particular, "WEB Brute Force Login -1.1021" enables attackers to execute a massive deluge of login attempts against web applications, leveraging an endless series of random combinations to crack user passwords in a short period of time. This attack in particular is another example of cyber criminals' heightened focus on credential theft, and shows the importance of not only password security and complexity, but the need for MFA solutions as a more effective preventative measure. - Cryptocurrency miners earn spot as a top malware variant. As anticipated, malicious cryptominers are continuing to grow in popularity as a hacking tactic, making their way into WatchGuard's top 10 malware list for the first time in Q2. Last quarter, WatchGuard uncovered its first named cryptominer, Cryptominer.AY, which matches a JavaScript cryptominer called "Coinhive" and uses its victims' computer resources to mine the popular privacy-focused cryptocurrency, Monero (XRM). The data shows that victims in the United States were the top geographical target for this cryptominer, receiving approximately 75 percent of the total volume of attacks. Cyber criminals continue to rely on malicious Office documents. Threat actors continue to booby-trap Office documents, exploiting old vulnerabilities in the popular Microsoft product to fool unsuspecting victims. Interestingly, three new Office malware exploits made WatchGuard's top 10 list, and 75 percent of attacks from these attacks targeted EMEA victims, with a heavy focus on users in Germany specifically. The complete Internet Security Report features an in-depth analysis of the EFail encryption vulnerability, along with insights into the top attacks in Q2 and defensive strategies SMBs can use to improve their security posture. These finding are based on anonymised Firebox Feed data from nearly 40,000 active WatchGuard UTM appliances worldwide, which blocked nearly 14 million malware variants (449 per device) and more than 1 million network attacks (26 per device) in Q2 2018. For more information, download the full report here: https://www.watchguard.com/wgrd-resource-center/security-report-q2-2018. To access live, real-time threat insights by type, region and date, visit WatchGuard's Threat Landscape data visualisation

tool: https://www.secplicity.org/threat-landscape today. 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 favoruite podcasts. About WatchGuard Technologies, Inc. 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 distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit: https://www.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.

Contacts

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