Vaporworms, Global Internet Disruption and Rogue AI Chatbots: WatchGuard Issues Security Predictions for 2019

Eight predictions from WatchGuard cover the next evolution of ransomware, escalating nation-state attacks, biometric hacking, Wi-Fi protocol security, and m

Sydney – 16 November 2018 – WatchGuard Technologies, a leader in advanced network security solutions, today issued a series of information security industry predictions for 2019. They include the emergence of “vaporworms,” a new breed of fileless malware with wormlike properties that allow it to self-propagate through vulnerable systems, a takedown of the internet itself and ransomware targeting utilities and industrial control systems. WatchGuard’s Threat Lab research team developed these predictions based on an analysis of major security and threat trends over the past year. “Cyber criminals are continuing to reshape the threat landscape as they update their tactics and escalate their attacks against businesses, governments, and even the infrastructure of the internet itself,” said Corey Nachreiner, chief technology officer at WatchGuard Technologies. “The Threat Lab’s 2019 predictions span from highly likely to audacious, but consistent across all eight is that there’s hope for preventing them. Organisations of all sizes need to look ahead at what new threats might be around the corner, prepare for evolving attacks and ensure they’re equipped with layered security defenses to meet them head-on." The WatchGuard Threat Lab’s 2019 Security Predictions are: 1. “Vaporworms” or Fileless Malware Worms Will Emerge. Fileless malware strains will exhibit wormlike properties in 2019, allowing them to self-propagate by exploiting software vulnerabilities. Fileless malware is more difficult for traditional endpoint detection to identify and block because it runs entirely in memory, without ever dropping a file onto the infected system. Combine that trend with the number of systems running unpatched software vulnerable to certain exploits, and 2019 will be the year of the vaporworm. 2. Attackers Hold the Internet Hostage. A hacktivist collective or nation-state will launch a coordinated attack against the infrastructure of the internet in 2019. The protocol that controls the internet (BGP) operates largely on the honour system, and a 2016 DDoS attack against hosting provider Dyn showed that a single attack against a hosting provider or registrar could take down major websites. The bottom line? The internet itself is ripe for the taking by someone with the resources to DDoS multiple critical points underpinning the internet or abuse the underlying protocols themselves. 3. Escalations in State-level Cyber Attacks Force a UN Cyber Security Treaty. The UN will more forcefully tackle the issue of state-sponsored cyber attacks by enacting a multinational Cyber Security Treaty in 2019. 4. AI-Driven Chatbots Go Rogue. In 2019, cyber criminals and black hat hackers will create malicious chatbots on legitimate sites to socially engineer unknowing victims into clicking malicious links, downloading files containing malware, or sharing private information. 5. A Major Biometric Hack Will be the Beginning of the End for Single-Factor Authentication. As biometric logins like Apple’s FaceID become more common, hackers will take advantage of the false sense of security they encourage and crack a biometric-only login method at scale to pull off a major attack. As a result, 2019 will see strong growth in the use of multi-factor authentication (MFA) for added protection among groups with more security knowledge, particularly push-based authentication and MFA for Cloud application defense. 6. A Nation-State to Take “Fire Sale” Attacks from Fiction to Reality. In the Die Hard movie series, a “fire sale” was a fictional three-pronged cyber-attack, targeting a city or state’s transportation operations, financial systems, public utilities and communication infrastructure. The fear and confusion caused during this attack was designed to allow the terrorists to siphon off huge sums of money undetected. Modern cyber security incidents suggest that nation-states and terrorists have developed these capabilities, so 2019 may be the first year one of these multi-pronged attacks is launched to cover up a hidden operation. 7. Hackers to Cause Real-World Blackouts as Targeted Ransomware Focuses on Utilities and Industrial Control Systems. Targeted ransomware campaigns will cause chaos in 2019 by targeting industrial control systems and public utilities for larger payoffs. The average payment demand will increase by over 6500 percent, from an average of $300 to $20,000 per attack. These assaults will result in real-world consequences like city-wide blackouts and the loss of access to public utilities. 8. A WPA3 Wi-Fi network will be hacked using one of the six Wi-Fi threat categories. Hackers will use rogue APs, Evil Twin APs, or any of the six known Wi-Fi threat categories (as defined by the Trusted Wireless Environment Framework (https://www.watchguard.com/wgrd-solutions/security-topics/trusted-wireless-environment) to compromise a WPA3 Wi-Fi network in 2019, despite enhancements to the new WPA3 encryption standard. Unless more comprehensive security is built into the Wi-Fi infrastructure across the entire industry, users can be fooled into feeling safe with WPA3 while still being susceptible to attacks like Evil Twin APs. To read WatchGuard’s complete 2019 Security Predictions visit: https://www.watchguard.com/2019Predictions Additional Materials · WatchGuard’s 2019 Security Predictions: https://www.watchguard.com/2019Predictions · WatchGuard’s 2019 Security Predictions Podcast: https://www.secplicity.org/category/the-443 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. 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 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. ENDS

Contacts

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