WatchGuard report uncovers massive increases in endpoint attacks, rising encrypted malware rates, new exploits targeting IoT devices, and more

SEATTLE – March 30, 2021 – WatchGuard® Technologies, a global leader in network security and intelligence, multi-factor authentication (MFA), advanced endpoint protection, and secure Wi-Fi, today released its Internet Security Report for Q4 2020. The report includes exciting new insights based on endpoint threat intelligence following WatchGuard's acquisition of Panda Security in June 2020. Among its most notable findings, the report reveals that fileless malware and cryptominer attack rates grew by nearly 900% and 25% respectively, while unique ransomware payloads plummeted by 48% in 2020 compared to 2019. Additionally, the WatchGuard Threat Lab found that Q4 2020 brought a 41% increase in encrypted malware detections over the previous quarter and network attacks hit their highest levels since 2018.

"The rise in sophisticated, evasive threat tactics last quarter and throughout 2020 showcases how vital it is to implement layered, end-to-end security protections," said Corey Nachreiner, chief technology officer at WatchGuard. "The attacks are coming on all fronts, as cyber criminals increasingly leverage fileless malware, cryptominers, encrypted attacks and more, and target users both at remote locations as well as corporate assets behind the traditional network perimeter. Effective security today means prioritising endpoint detection and response, network defenses and foundational precautions such as security awareness training and strict patch management."

WatchGuard's quarterly Internet Security Reports inform businesses, their partners and end customers about the latest malware, endpoint and network attack trends as they emerge. Key findings from the Q4 2020 report include:

Fileless malware attacks skyrocket – Fileless malware rates in 2020 increased by 888% over 2019. These threats can be particularly dangerous due to their ability to evade detection by traditional endpoint protection clients and because they can succeed without victims doing anything beyond clicking a malicious link or unknowingly visiting a compromised website. Toolkits like PowerSploit and CobaltStrike allow threat actors to easily inject malicious code into other running processes and remain operational even if the victim's defenses identify and remove the original script. Deploying endpoint detection and response solutions alongside preventative anti-malware can help identify these threats.

Cryptominers on the rise following 2019 lull – After virtually all cryptocurrency prices crashed in early 2018, cryptominer infections became far less prevalent and reached a low of 633 unique variant detections in 2019. That said, attackers continued adding cryptominer modules to existing botnet infections and extract passive income from victims while abusing their networks for other cyber crime. As a result, and with prices trending upward again in Q4 2020, the volume of cryptominer malware detections climbed more than 25% over 2019 levels to reach 850 unique variants last year.
Ransomware attack volumes continue to shrink – For the second year in a row, the number of unique ransomware payloads trended downward in 2020, falling to 2,152 unique payloads from 4,131 in 2019 and the all-time-high of 5,489 in 2018. These figures represent individual variants of ransomware that may have infected hundreds or thousands of endpoints worldwide. The majority of these detections resulted from signatures originally implemented in 2017 to detect WannaCry and its related variants, showing that ransomworm tactics are still thriving over three years after WannaCry burst onto the scene. The steady decline in ransomware volume indicates the attackers' continued shift away from the unfocused, widespread campaigns of the past toward highly targeted attacks against healthcare organizations, manufacturing firms and other victims for which downtime is unacceptable.
Encrypted, evasive malware attacks see double-digit growth – Despite being the fourth consecutive quarter of decreasing malware volumes overall, nearly half (47%) of all attacks WatchGuard detected at the network perimeter in Q4 were encrypted. Additionally, malware delivered via HTTPS connections increased by 41%, while encrypted zero day malware (variants that circumvent antivirus signatures) grew by 22% over Q3.
Botnet malware targeting IoT devices and routers becomes a top strain – In Q4, the Linux.Generic virus (also known as "The Moon") made its debut on WatchGuard's list of top 10 malware detections. This malware is part of a network of servers that directly targets IoT devices and consumer-grade network devices like routers to exploit any open vulnerabilities. WatchGuard's investigation uncovered Linux-specific malware designed for ARM processors and another payload designed for MIPS processors within the attacker's infrastructure, indicating a clear focus on evasive attacks against IoT devices.
SolarWinds breach illustrates the perils of supply chain attacks – The sophisticated, allegedly state-sponsored SolarWinds supply chain breach will have wide implications throughout the security industry for years to come. Its effects spread far beyond SolarWinds to almost 100 companies, including some major Fortune 500s, big security companies, and even the US government. WatchGuard's detailed incident breakdown showcases the

importance of defending against supply chain attacks in today's interconnected digital ecosystem.
New trojan dupes email scanners with multi-payload approach – Trojan.Script.1026663 made its way onto WatchGuard's top five most-widespread malware detections list in Q4. The attack begins with an email asking victims to review an order list attachment. The document triggers a series of payloads and malicious code that ultimately lead the victim machine to load the final attack: the Agent Tesla remote access trojan (RAT) and keylogger.
Network attack volume approaches 2018 peak – Total network attack detections grew by 5% in Q4, reaching their highest level in over two years. Additionally, total unique network attack signatures showed steady growth as well with a 4% increase over Q3. This shows that even as the world continues to operate remotely, the corporate network perimeter is still very much in play as threat actors continue to target on-premises assets.
In Q4, WatchGuard appliances blocked a total of more than 20.6 million malware variants (456 per device) and nearly 3.5 million network threats (77 detections per appliance). WatchGuard Fireboxes collectively blocked 455 unique attack signatures in Q4 – a 4% increase over Q3 and the most since Q4 2018. WatchGuard's quarterly research reports are based on anonymised Firebox Feed data from active WatchGuard appliances whose owners have opted in to share data to support the Threat Lab's research efforts. Additionally, the report's new endpoint threat intelligence provides deeper insight into specific malware attacks and trends throughout the year 2020 based on over 2.5 million unique payload alerts gathered from 1.7 million endpoints across 92 countries.

The full report includes details on additional malware and attack trends from Q4 2020, a detailed analysis of the infamous SolarWinds supply chain attack, and key security best practices for readers. Read WatchGuard's complete Q4 2020 Internet Security Report here: https://www.watchguard.com/wgrd-resource-center/security-report-q4-2020

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 18,000 security resellers and service providers to protect more than 250,000 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 or on the LinkedIn Company page. 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 at Secplicity.org, or wherever you find your favorite podcasts.

ENDS

Contacts

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