WatchGuard Report Details COVID-19 Impact on Security Threat Landscape

Q3 2020 Internet Security Report sheds light on COVID-19 threat trends, growing network attacks, malware targeting U.S. SCADA systems, and more

SEATTLE – December 9, 2020 – WatchGuard® Technologies, a global leader in network security and intelligence, advanced endpoint protection, multi-factor authentication and secure Wi-Fi, today announced the release of its Internet Security Report for Q3 2020. Top findings from the research reveal how COVID-19 has impacted the security threat landscape, with evidence that attackers continue to target corporate networks despite the shift to remote work, and a rise in pandemic-related malicious domains and phishing campaigns.

“As the impact of COVID-19 continues to unfold, our threat intelligence provides key insight into how attackers are adjusting their tactics,” said Corey Nachreiner, chief technology officer at WatchGuard. “While there’s no such thing as ‘the new normal’ when it comes to security, businesses can be sure that increasing protection for both the endpoint and the network will be a priority in 2021 and beyond. It will also be important to establish a layered approach to information security, with services that can mitigate evasive and encrypted attacks, sophisticated phishing campaigns and more.”

WatchGuard’s Internet Security Reports inform businesses, their partners and end customers with hard data, expert analysis and actionable insights on the latest malware and network attack trends as they emerge and influence the ever-evolving threat landscape. Key findings from the Q3 2020 report include:

Network attacks and unique detections both hit two-year highs – Network attacks swelled to more than 3.3 million in Q3, representing a 90% increase over the previous quarter and the highest level in two years. Unique network attack signatures also continued on an upward trajectory, reaching a two-year high in Q3 as well. These findings highlight the fact that businesses must prioritise maintaining and strengthening protections for network-based assets and services, even as workforces become increasingly remote.COVID-19 scams grow in prevalence – In Q3, a COVID-19 adware campaign running on websites used for legitimate pandemic support purposes made WatchGuard’s list of the top 10 compromised websites. WatchGuard also uncovered a phishing attack that leverages Microsoft SharePoint to host a pseudo-login page impersonating the United Nations (UN), and the email hook contained messaging around small business relief from the UN due to COVID-19. These findings further emphasise that attackers will continue to leverage the fear, uncertainty, and doubt surrounding the global health crisis to entice and fool their victims.Businesses click on hundreds of phishing attacks and bad links – In Q3, WatchGuard’s DNSWatch service blocked a combined 2,764,736 malicious domain connections, which translates to 499 blocked connections per organisation in total. Breaking it down further, each organization would have reached 262 malware domains, 71 compromised websites, and 52 phishing campaigns. Combined with the aforementioned rise in convincing COVID-19 scams, these findings illustrate the importance of deploying DNS filtering services and user security awareness training.Attackers probe for vulnerable SCADA systems in the U.S. – The one new addition to WatchGuard’s most-widespread network attacks list in Q3 exploits a previously-patched authentication bypass vulnerability in a popular supervisory control and data acquisition (SCADA) control system. While this class of vulnerability isn’t as serious as a remote code execution flaw, it could still allow an attacker to take control of the SCADA software running on the server. Attackers targeted nearly 50% of U.S. networks with this threat in Q3, highlighting that industrial control systems could be a major focus area for bad actors in the coming year.LokiBot look-a-like debuts as a top widespread malware variant – FareIt, a password stealer that resembles LokiBot, made its way into WatchGuard’s top five most-widespread malware detections list in Q3. Though it is unclear if the FareIt botnet uses the same command and control structure as LokiBot, there’s a high probability the same group, SilverTerrier, created both malware variants. This botnet takes many steps to bypass antivirus controls and fool users into installing the malware. While researching the threat, WatchGuard found strong evidence indicating the malware has likely targeted many more victims than the data suggests.Emotet persists – Emotet, a prolific banking trojan and known password stealer, made its debut on WatchGuard’s top ten malware list for the first time in Q3 and narrowly missed the top ten list of domains distributing malware (by only a few connections). Despite coming in at #11 for the latter list, this appearance is particularly notable, as the WatchGuard Threat Lab and other research teams have seen current Emotet infections dropping additional payloads like Trickbot and even the Ryuk ransomware with no signs of slowing down.

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. In Q3, nearly 48,000 WatchGuard appliances contributed data to the report (the most ever), blocking a total of more than 21.5 million malware variants (450 per device) and more than 3.3 million network threats (or roughly 70 detections per appliance). Firebox appliances continued their upward trend of unique signature detections as well, collectively identifying and blocking 438 unique attack signatures – a 6.8% increase over Q2 and the most since Q4 2018.

The complete report includes in-depth research and key defensive best practices that businesses of all sizes can use to protect themselves against modern security threats. The report also features a detailed analysis of the historic Twitter hack that compromised 130 high-profile accounts to promote a Bitcoin scam in July 2020.

Read WatchGuard's full Q3 2020 Internet Security Report here today: https://www.watchguard.com/wgrd-resource-center/security-report-q3-2020.

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.

###

Contacts

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