INTELLIGENCE ENTERPRISE

HOMELAND INTELLIGENCE ARTICLE

Homeland Security

8 April 2020

(U) Cyber Mission Center

(U//FOUO) Malicious Cyber Actors Likely See Opportunity to Target Virtual Private Network Vulnerabilities as More People Telework Due to COVID-19

(U//FOUO) Scope. This *Article* warns federal, state, local, and private sector network defenders of the likely targeting of virtual private network (VPN) vulnerabilities as more people turn to these networks as the COVID-19 pandemic forces more people to telework. This *Article* supplements IA-43325-20, "(U//FOUO) Cyber Actors Almost Certainly View Growing Telework During the Novel Coronavirus Pandemic as an Opportunity to Exploit Enterprise Networks," dated 30 March 2020, by examining the VPN threat during this period of heightened remote employment. The information cutoff for this *Article* is 17 March 2020.

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) Cyber Mission Center (CYMC). Coordinated with CBP, CISA, CWMD, FEMA, ICE, S&T, TSA, USCG, USSS, CIA, DIA, Department of Energy, Department of State, Department of the Treasury, FBI, NASIC, NGA, NIC, and NSA.

(U//FOUO) We assess the growth of VPN use resulting from increased telework during the COVID-19 pandemic likely presents an opportunity for malicious cyber actors—including advanced persistent threat (APT) actors—to exploit commonly known VPN vulnerabilities, increasing the chances for compromise or inadvertent connection disruption to occur. We base this assessment on US government cyber alerts in 2019 and 2020 warning of vulnerabilities within popular VPNs. We additionally base this assessment on previous malicious cyber campaigns that exploited VPN vulnerabilities, including the compromise of the US Postal Service (USPS). Furthermore, we base this assessment on recent statistical measurements predicting the increase in VPN users during the COVID-19 pandemic.

(U) Malicious cyber actors as of January 2020 continued to exploit unpatched Pulse Secure VPN remote code execution (RCE) vulnerabilities (CVE-2019-11510), according to a CISA Cyber Alert.[1] Cybercriminals on 31 December exploited this vulnerability on seven Pulse Secure VPNs belonging to the foreign exchange company Travelex to conduct a ransomware attack on the company's network, according to an online news site focused on cybersecurity and information technology.[2]

(U//FOUO) APT actors as of October 2019 were exploiting common vulnerabilities in popular US VPN products to gain access to unprotected networks, according to an NSA cybersecurity advisory.[3] The APT cyber actors often use newly released software patches to develop exploits and access networks which have not yet upgraded with vendor released patches, according to the same source.

(U) Suspected Iranian APT cyber actors from 2017 to late 2019 launched a large campaign by exploiting unpatched VPN and remote desktop protocol (RDP) servers to gain access to and steal information from dozens of companies worldwide, according to a report from a UK cybersecurity firm.[4] The targets included numerous companies and organizations worldwide involved in information technology, telecommunications, oil and gas, aviation, government, and security. This attack vector is not just used by Iranian APT groups, but also cybercrime, ransomware, and other state-sponsored offensive groups, according to the same source.

(U) Unknown malicious cyber actors in 2014 gained access to a USPS VPN server, allowing the actors to exfiltrate personal data on 800,000 employees, according to two cybersecurity firms that provided an initial timeline of the compromise and a follow-up on the VPN compromise vector.[5,6] USPS restricted network communications with the internet until VPN security upgrades could be made upon discovering the location of the compromise, according to the same sources.

*(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.*

(U) The spread of COVID-19 has increased the use of VPNs in the countries most affected by the virus, according to a reputable online cybersecurity magazine.[7] VPN use in the United States increased 53 percent in the first two weeks of March 2020, and s expected to jump to 150 percent by the end of the month, according to the same source.

(U) Mitigation

(U) CISA advises that organizations stay current with the most recent software updates. As more people telework during the COVID-19 pandemic, CISA also encourages organizations to implement multifactor authentication (MFA) on VPN servers.[8] For more information, please see https://www.us-cert.gov/ncas/alerts/aa20-073a.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form. The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every U.S. state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

(U) Tracked by: HSEC-1.1, HSEC-1.5, HSEC-1.6, HSEC-1.8, HSEC-1.10

(U) Source Summary Statement

(U//FOUO) This *Article* is based on a CISA cyber alert, a defense cybersecurity advisory, three cybersecurity firm bulletins, and two reports from online companies that focus on federal technology news.

(U//FOUO) We assess the growth of VPN use resulting from increased telework during the COVID-19 pandemic likely presents an opportunity for malicious cyber actors—including advanced persistent threat (APT) actors—to exploit commonly known VPN vulnerabilities, increasing the chances for compromise or inadvertent connection disruption to occur. We have **high confidence** in this assessment, as the reporting overall depicts numerous, persisting cyber vulnerabilities and actors who have demonstrated a continued interest in them after previously exploiting the vulnerabilities. Additionally, the sourcing is considered very reliable, as the US government alerts are used as the foundation for the analysis by demonstrating the threat environment, while the cybersecurity firms report on examples of compromise. Each case can be corroborated by other sources, proving the information is factual. An NSA cyber alert brings attention to already known VPN vulnerabilities that are being targeted by APT and other malicious cyber actors, while the CISA alert indicates that some VPN servers have continued to not be patched even after the vulnerabilities were made public, which shows that these vulnerabilities are an ongoing issue. The NSA and CISA alerts provide credible reporting from cyber technical experts. The two reports from cybersecurity firms, as well as the NextGov federal technology report, provide examples of how previous malicious actors have exploited VPN servers in order to exfiltrate sensitive data on individuals and corporations. The reports reflect credible sourcing by depicting different types of targets, as well as different types of malicious cyber actors, which underscores how broad the threat to VPNs can be. Finally, the cybersecurity firm's bulletin on an increase VPN usage in the United States shows that the threat is only likely to increase, regardless of the preciseness of the source's statistics.

[1] (U); CISA; "Alert (AA20-010A) Continued Exploitation of Pulse Secure VPN Vulnerability"; 10 January 2020. https://www.us-cert.gov/ncas/alerts/aa20-010a

[2] (U); SC Media; " Travelex recovering from ransomware, but more firms at risk of VPN exploit;" 19 JAN 2020; https://www.scmagazine.com/home/security-news/ransomware/travelex-recovering-from-ransomware-but-more-firms-at-risk-of-vpn-exploit/.

[3] (U); NSA; "NSA Cybersecurity Advisory: Malicious Cyber Actors Leveraging VPN Vulnerabilities for Attack; Check VPN Products for Upgrade;" 7 October 2019; https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1982939/nsa-cybersecurity-advisory-malicious-cyber-actors-leveraging-vpn-vulnerabilitie/

[4] (U); ClearSky Security; "Fox Kitten – Widespread Iranian Espionage-Offensive Campaign;" 16 February 2020; Fox Kitten – Widespread Iranian Espionage-Offensive Campaign

[5] (U); NextGov; "Timeline: How the Postal Service Data Breach Went Down;" 19 November 2014; https://www.nextgov.com/cybersecurity/2014/11/timeline-how-postal-service-data-breach-went-down/99494/

[6] (U); Security Intelligence; "Malicious actors compromised a U.S. Postal Service VPN service and stole personally identifiable information (PII) of employees and customers;" 21 February 2020; https://securityintelligence.com/ibm_timeline/malicious-actors-compromised-a-u-s-postal-service-vpn-service-and-stole-personally-identifiable-information-pii-related-to-800000-active-and-previous-employees-and-2-9-million-customers/.

[7] (U); Info-Security; "US VPN Use Could Soar 150% as Covid-19 Spreads"; 17 March 2020. https://www.infosecurity-magazine.com/news/vpn-use-could-soar-150-us-covid19/

[8] (U); CISA; "Enterprise VPN Security"; 13 March 2020; https://www.us-cert.gov/ncas/alerts/aa20-073a.

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Malicious Cyber Actors Likely See Opportunity to Target Virtual Private Network Vulnerabilities

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

□ Drive planning and preparedness efforts, training, and/or emergency response operations
□ Observe, identify, and/or disrupt threats
□ Share with partners
□ Allocate resources (e.g. equipment and personnel)
□ Reprioritize organizational focus
□ Author or adjust policies and guidelines
□ Initiate a law enforcement investigation
□ Intiate your own regional-specific analysis
□ Intiate your own topic-specific analysis
□ Develop long-term homeland security strategies
□ Do not plan to use
□ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:
Position:
State:
Email:

Submit Feedback

Privacy Act Statement