INTELLIGENCE ENTERPRISE

HOMELAND INTELLIGENCE ARTICLE

Homeland Security

27 March 2020

(U) Cyber Mission Center

(U//FOUO) Nation-State Cyber Actors Likely to Conduct COVID-19-Themed Spear-Phishing Against Homeland Targets

(U//FOUO) Scope. This *Article* informs federal, state, local, and private sector partners of the likely threat from nation-state actors' continued COVID-19-themed spear-phishing campaigns. The FBI on 20 March released a Public Service Announcement (PSA) warning individuals to research links purporting to provide information on COVID-19 before clicking on them.[a] The PSA warns against fake Centers for Disease Control and Prevention (CDC) phishing e-mails. The information cutoff date for this *Article* is 20 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) CYMC assesses nation-state cyber actors likely will exploit the spread of COVID-19 to target homeland victims with COVID-19-themed spear-phishing e-mails. Nation-state actors since at least February 2020 have targeted foreign victims with COVID-19-themed e-mails intended to appear to be from legitimate government sources, including US Government entities such as the CDC and the Department of State. We assume because more Americans during this pandemic will seek COVID-19 information from US Government sources they will be more apt to open messages appearing to be from government entities.

» (U) Chinese cyber actors in February and early March 2020 conducted COVID-19-themed spear-phishing campaigns targeting Vietnam, Taiwan, the Philippines, and Mongolia, according to multiple cybersecurity firms.[1,2,3] Many of the e-mails were tailored to appear as though they were from legitimate government sources. For example, suspected Chinese Government cyber actors sent spear-phishing e-mails to targets in Vietnam that contained a statement purportedly from the Vietnamese Prime Minister, according to the same cybersecurity firm.

» (U) A Russian state-sponsored cyber actor with ties to the same group that compromised the Democratic National Committee[USPER] in 2016 deployed backdoor malware in mid-February 2020 through spear-phishing e-mails containing the latest news regarding COVID-19, according to a US cybersecurity firm.[4] The documents were sent to targets in Ukraine, disguised as e-mails coming from the Center for Public Health of the Ministry of Health of Ukraine. The e-mails appear to have been part of a larger misinformation campaign against Ukraine containing false information about Ukrainian COVID-19 cases and government countermeasures, according to the same report.

[a] (U); FBI; "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic"; 2020; https://www.ic3.gov/media/2020/200320.aspx; accessed 20 MAR 2020.

IA-03272020-T-4

» (U) Likely North Korean Government-affiliated cyber actors in late February 2020 directed a spear-phishing campaign against South Korean officials, according to a media report.[5] The actors sent documents detailing South Korea's response to COVID-19 that contained malware previously associated with a North Korean cyber group, according to the same report.

» (U) Although nation-state activity has been identified, COVID-19 spear-phishing as of early March 2020 has primarily been used by cybercriminals, according to a second US cybersecurity firm.[6] Cybercriminals are similarly using e-mails purporting to contain legitimate information on COVID-19, according to the same cybersecurity firm.

(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-1.2, HSEC-1.5, HSEC-1.8

(U) Source Summary Statement

(U//FOUO) This assessment is based on two reports from US cybersecurity firms, two US media reports, and a Public Service Announcement from the FBI.

(U//FOUO) CYMC assesses nation-state cyber actors likely will exploit the spread of COVID-19 to target homeland victims with COVID-19-themed spear-phishing e-mails. We have **moderate confidence** in our assessment. Our confidence level is based on observable activity reported by credible cybersecurity firms and media sources. Reporting indicating nation-state cyber actors are losing interest in COVID-19 spear-phishing would probably cause us to change our confidence level. We would have higher confidence in our judgment if we have indications of nation-state intent to use this social engineering theme against homeland targets.

[1] (U); FireEye; "Coronavirus (COVID-19) Exploited Globally to Enhance Spear-Phishing and Disinformation Campaigns"; 2020; https://intelligence.fireeye.com/reports/20-00004349; accessed 19 MAR 2020.
[2] (U); Recorded Future; "Capitalizing on Coronavirus, Threat Actors Target Victims Worldwide"; 2020; https://www.recordedfuture.com/coronavirus-panic-exploit/; accessed 19 MAR 2020.
[3] (U); Cyberscoop; "Cybercriminals, nation-states increasingly tailoring coronavirus spearphishing campaigns"; 2020; https://www.cyberscoop.com/coronavirus-phishing-scams-iran-china/; accessed 19 MAR 2020.
[4] (U); ZDNet; "State-sponsored hackers are now using coronavirus lures to infect their targets"; 2020; https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/; accessed on 19 MAR 2020.
[5] (U); ZDNet; "State-sponsored hackers are now using coronavirus lures to infect their targets"; 2020; https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/; accessed on 19 MAR 2020.
[6] (U); Recorded Future; "Capitalizing on Coronavirus, Threat Actors Target Victims Worldwide"; 2020; https://www.recordedfuture.com/coronavirus-panic-exploit/; accessed 19 MAR 2020.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Nation-State Cyber Actors Likely to Conduct COVID-19-Themed Spear- Phishing Against Home

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:		*Position:*	
Organization:		*State:*	
Contact Number:		*Email:*	

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**