Homeland Security

INTELLIGENCE NOTE

2 April 2020

(U) Cyber Mission Center

(U//FOUO) Cyber Actors Sending Coronavirus-Themed Phishing E-mails

(U//FOUO) Scope. This *Intelligence Note* informs federal civilian government and private sector network defenders of a Coronavirus-themed phishing campaign against state and local entities. The information cutoff date for this *Note* is 23 March 2020.

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) Cyber Mission Center (CYMC). Coordinated with Cybersecurity and Infrastructure Security Agency (CISA) and FBI.

(U//FOUO) Malicious cyber actors since at least 12 March 2020 have been sending coronavirus-themed phishing e-mails—purporting to be from official US Government agencies—to various state and local agencies in an identified US state, according to a US state law enforcement agent.[1]

(U) Support to Computer Network Defense

(U//FOUO) The phishing e-mails contained password-protected attachments with embedded malware. The body of the phishing e-mails were either Coronavirus/COVID-19 or invoice-themed. The below indicators are associated with this phishing campaign:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Description	Indicator
Phishing e-mail sent from actor-controlled domain	gmx[.]com
Subject line in the e-mails	Coronavirus today infected [XX] people in your state
Spoofed sender name	Department of Health US gov
Spoofed sender name	CDC US Government
Spoofed sender name	HHS Government
Spoofed sender name	HHS gov
MD5 hash	74AEB7771EB0762C39CCEB8C68F5FD58C9CE7119971022B0131251DF64FFDE56 B57A98C87F7AED39EAF87A832BB60E492F95CF803FB3EB8C6D1E221A21BA3FD6 85703997FDCDB1EF96F9FBF9E631160D4E06B7BFA529DD67435DDA99BB1CD14E F9DF4219B1D8EC228FDB4BE1BA1C94785BE0014869DC79BF8924E89CB71EC0F0

IA-43471-20

(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 US 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-1.2, HSEC-1.5, HSEC-1.8

[1] (U//FOUO); DHS; IIR 4 007 0604 20; 231819Z MAR 20; DOI 12-20 March 2020; (U//FOUO); IIR 4 007 0604 20/Unidentified Malicious Cyber Actors Sending Coronavirus/COVID-19-themed Phishing Emails Containing Danabot Malware to State and Local Agencies in an identified Northeastern US State during March 2020; Extracted information is U//FOUO; Overall document classification is U//FOUO. Source is a US state law enforcement official with direct and firsthand knowledge of the information obtained during the course of official duties.

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

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Cyber Actors Sending Coronavirus-Themed Phishing E-mails

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**

Product Serial Number: IA-43471-20 REV: 01 August 2017