Homeland Security

17 April 2020

(U) Cyber Mission Center

(U//FOUO) Cyber Targeting of US Public Health and Healthcare Sector Likely to Increase During Pandemic

(U//FOUO) Scope. This *Article* informs the public health and healthcare sector and other federal, state, local, and critical infrastructure stakeholders of the likely increase in malicious cyber activity against the sector during the COVID-19 pandemic. The malicious cyber events described in this *Article* are examples of ongoing malicious cyber activity against the network and is not intended to be comprehensive. The information cutoff date for this *Article* is 25 March 2020.

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

(U//FOUO) DHS assesses the US public health and healthcare sector likely are at increased threat of cyber targeting during the COVID-19 pandemic due to heightened public fears related to the pandemic causing users to open documents and click links before investigating their legitimacy. We base this assessment on cybersecurity researchers' indication that COVID-19-themed lures represent the largest single-themed targeting seen in years, as well as deliberate targeting of US and foreign-based healthcare organizations by suspected advanced persistent threat (APT) and other actors during the pandemic.

» (U) Cybersecurity researchers in mid-March 2020 indicated the cumulative volume of coronavirus-related e-mail lures now represents the greatest collection of attack types united by a single theme seen in years, if not ever. Researchers have observed credential phishing, malicious attachments, malicious links, landing pages, downloaders, spam, and malware, among others, all leveraging coronavirus lures, according to a cybersecurity firm with a history of credible cyber threat reporting.[1] Multiple threat actors of varying motivations as of 19 March 2020 have leveraged coronavirus-themed lures in their operations, and this trend is expected to continue for the foreseeable future, according to a separate cybersecurity firm with a history of credible cyber threat reporting.[2]

» (U) Russian APT cyber actors in mid-February 2020 leveraged the COVID-19 pandemic to target Ukraine with spear-phishing e-mails containing malicious attachments and purporting to be from the Ministry of Health of Ukraine, according to a cybersecurity firm.[3] The spear-phishing e-mails appear to have been part of a more widespread disinformation campaign that hit Ukraine on several different fronts, including on social media, according to the cybersecurity firm.

» (U) Suspected advanced persistent threat actors 13 March 2020 targeted the network of the World Health Organization using the same infrastructure that has been used to target other healthcare and humanitarian organizations, according to a cybersecurity firm with a history of credible cyber threat reporting.[4]

» (U) Suspected APT actors in mid-March 2020 conducted a distributed denial-of- service (DDoS) attack against the network of the Department of Health and Human Services (HHS) that temporarily overloaded servers for several hours. An HHS spokeswoman reported that during this cyber attack systems were not significantly slowed and no penetration into HHS networks occurred, according to media reporting.[5]

(U) Unknown cyber actors on 5 March 2020 conducted an unidentified type of cyber attack against a group of Arkansas hospitals, causing the hospitals to shutdown and restart their systems, according to local media reporting.[6,7] The attack delayed some appointments and procedures, but all patient services remained open and there was no evidence of patient information being affected during the attack. Network administrators as of 10 March 2020 continued to refine online connections to external partners in an attempt to restore full network connectivity, according to the same reports.

» (U) Suspected cybercriminals between 15 and 17 March 2020 used COVID-19-themed phishing e-mails containing malware—which primarily targets financial institutions in the United States—and purporting to be from Department of Health and Human Services or the Centers for Disease Control and Prevention (CDC) to target predominately healthcare, biotechnology, and financial service industries within the United States, but also organizations in Germany, Switzerland, Australia, Japan, and the United Kingdom, according to a cybersecurity firm with a history of credible cyber threat reporting and a DHS report derived from a law enforcement official with direct and indirect access to the information.[8,9]

» (U) Cybercriminal groups in mid-March 2020 used malicious COVID-19-themed phishing e-mails—offering remedies in exchange for bitcoin—to target the US healthcare, manufacturing, and pharmaceutical industries, according to a cybersecurity firm with a history of credible cyber threat reporting.[10] These cybercriminals also targeted Canadian victims with e-mails impersonating public health officials providing information on the latest developments and news surrounding the virus to infect the victim with known financial malware, according to the same cybersecurity firm.

» (U) Unidentified cybercriminals on 11 March 2020 targeted the website of a Midwestern state's public health district with a new ransomware variant called NetWalker, preventing public health employees from accessing files, according to local media reporting.[11] Local administrators were able to affirm that sensitive environmental health and patient electronic medical records were safe and still available, according to the same reports.

(U) Outlook

(U//FOUO) Although some cybercriminal groups have publicly claimed that they will not directly target the healthcare sector or local government networks during the pandemic, the autonomous and wide-reaching nature of their cyber activities have continued to have impacts by those same actors as they continue to perform them internationally.[12,13] Malicious COVID-19-themed cyber activities continue to evolve, and DHS anticipates malicious cyber groups will continue to target the public health and healthcare sector exploiting the fear, urgency, and goodwill of audiences for their independently motivated benefits.

(U) Appendix A: Cyber Protection and Mitigation

(U) Cyber Protection from COVID-19 Related Schemes

(U) The Department of Justice recommends that Americans take the following precautionary measures to protect themselves from known and emerging cyber frauds related to COVID-19.[14]

- (U) Independently verify the identity of any company, charity, or individual that contacts you regarding COVID-19.
- (U) Check the websites and e-mail addresses offering information, products, or services related to COVID-19. Be aware that scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use "cdc9[.]com" or "cdc[.]org" rather than "cdc[.]gov."
- (U) Be wary of unsolicited e-mails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the public in this manner.
- (U) Do not click on links or open e-mail attachments from unknown or unverified sources, doing so could download a virus onto your computer or device.
- (U) Make sure the anti-malware and antivirus software on your computer are operating and up to date.
- (U) Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if a vaccine becomes available, you will not hear about it for the first time through an e-mail solicitation, online ad, or unsolicited sales pitch.
- (U) Check online reviews of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.
- (U) Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving any donation. Remember, an organization may not be legitimate even if it uses words like "CDC" or "government" in its name or has reputable-looking seals or logos on its materials. For online resources on donating wisely, visit the Federal Trade Commission (FTC) website.

(U) Securing Information Technology Systems

(U) As organizations explore various alternate workplace options in response to COVID-19, CISA recommends examining the security of information technology systems by taking the following steps:

- (U) Secure systems that enable remote access.[15]
- (U) Ensure virtual private network and other remote access systems are fully patched.[16]
- (U) Enhance system monitoring to receive early detection and alerts on abnormal activity.
- (U) Implement multi-factor authentication.[17]
- (U) Ensure all machines have properly configured firewalls and anti-malware and intrusion prevention installed.[18]
- (U) Test the capacity of remote access solutions, and increase capacity as needed.
- (U) Ensure continuity of operations plans or business continuity plans are up to date.
- (U) Increase awareness of information technology support mechanisms for employees who work remotely.
- (U) Update incident response plans to consider workforce changes in a distributed environment.

(U) Protecting Against Phishing and Disinformation

(U) Malicious cyber actors could take advantage of public concern surrounding COVID-19 by conducting phishing attacks and disinformation campaigns. Phishing attacks often use a combination of e-mail and fraudulent websites to trick victims into revealing sensitive information.[19] Disinformation campaigns can spread discord, manipulate the public conversation, influence policy development, or disrupt markets.

(U) CISA encourages individuals to guard against COVID-19-related phishing attacks and disinformation campaigns by taking the following precautions.

» (U) Avoid clicking on links in unsolicited e-mails and be wary of e-mail attachments.
» (U) Do not reveal personal or financial information in e-mails, and do not respond to e-mail solicitations for this information.
» (U) Review CISA's "Tip on Avoiding Social Engineering and Phishing Scams" for more information on recognizing and protecting against phishing.
» (U) Review the Federal Trade Commission's blog post on coronavirus scams for information on avoiding COVID-19 related scams.[20]
» (U) Use trusted sources, such as legitimate government websites for up-to-date, fact-based information about COVID-19.

(U) For more information and additional detailed recommendations, see CISA's COVID-19 webpage at https://www.cisa.gov/coronavirus and the "CISA Insights on Risk Management for Novel Coronavirus" at https://cisa.gov/coronavirus/insights.

(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-1.2, HSEC-1.5, HSEC-1.8

(U) Source Summary Statement

(U//FOUO) This *Article* is based on a DHS report, five cybersecurity firm reports, four media reports from online companies focused on federal technology news, one domestic news media source, and one local news media source. The DHS report is from a state law enforcement source with direct and indirect access, the majority of media and cybersecurity firm reporting are from entities with a history of credible reporting, while the veracity of some media reporting cannot be established. We lack corroborating IC reporting, and granularity of the topology of the public health and healthcare sector to fully assess the varying levels of initial and sustained network impacts.

(U//FOUO) DHS assesses the US public health and healthcare sector likely are at increased threat of targeting during the COVID-19 pandemic due to heightened public fears related to the pandemic causing users to open documents and click links before investigating their legitimacy. We have **moderate confidence** in our assessment based on numerous observed cyber incidents against the public health and healthcare sector reported from February 2020 to 25 March 2020 from a variety of sources, including a diverse body of credible US media and cybersecurity firms with first and secondhand access, including official government sources with high levels of reliability. These sources were fundamental in highlighting the threat landscape. Multiple cyber incidents found in media reporting were corroborated by other media. Our confidence level would increase if additional information was obtained on the network topology of the public health and healthcare sector that have been affected by malicious cyber activities, which would assist to understand the full impact to other critical infrastructure networks.

---

[1] (U); Proofpoint; "TA505 and Others Launch New Coronavirus Campaigns; Now the Largest Collection of Attack Types in Years"; 16 MAR 2020; https://www.proofpoint.com/us/threat-insight/post/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack; Accessed on 24 MAR 2020.

[2] (U); FireEye; "Coronavirus-Themed Phishing Lures and Malicious JNLP Files Used to Distribute a DanaBot; Highlights Increasing Use of Coronavirus Lures"; 19 MAR 2020; https://intelligence.fireeye.com/news_analysis/20-00004826; Accessed on 24 MAR 2020.

[3] (U); FireEye; "State-Sponsored hackers are now using coronavirus lures to infect their targets"; 14 MAR 2020; https://intelligence.fireeye.com/news_analysis/20-00004502; Accessed on 24 MAR 2020.

[4] (U); Reuters; "Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike"; 23 MAR 2020; https://www.reuters.com/article/health-coronavirus-who-hack/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSL8N2BF160; Accessed on24 MAR 2020.

[5] (U); Bloomberg; "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak"; 16 MAR 2020; https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response; Date of Accessed on 24 MAR 2020.

[6] (U); Beckers; "Arkansas Children's Hospital reboots IT system after cyberattack"; 06 MAR 2020; https://www.beckershospitalreview.com/cybersecurity/arkansas-children-s-hospital-reboots-it-system-after-cyberattack.html; Date of Accessed on 24 MAR 2020.

[7] (U); FoxNews; "Update: After cybersecurity threat, Arkansas Children's Hospital systems getting back online"; 10 MAR 2020; https://www.fox16.com/news/local-news/fbi-investigating-cybersecurity-threat-at-arkansas-childrens-hospital; Accessed on 24 MAR 2020.

[8] (U); FireEye; "Coronavirus-Themed Phishing Lures and Malicious JNLP Files Used to Distribute a DanaBot; Highlights Increasing Use of Coronavirus Lures"; 19 MAR 2020; https://intelligence.fireeye.com/reports/20-00004826; Accessed on 24 MAR 2020;

[9] (U//FOUO); DHS; IIR 4 007 0604 20; DOP: 23 MAR 2020; DOI: 23 MAR 2020; (U//FOUO); Unidentified Malicious Cyber Actors Sending Coronavirus/COVID-19-themed Phishing Emails Containing Danabot Malware to State and Local Agencies in an identified Northeastern U.S. State during March 2020; Extracted information is U//FOUO; Overall source classification is U//FOUO.

[10] (U); Proofpoint; "TA505 and Others Launch New Coronavirus Campaigns; Now the Largest Collections of Attack Types in Years"; 16 MAR 2020; https://www.proofpoint.com/us/corporate-blog/post/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack; Accessed on 24 MAR 2020.

[11] (U); News-Gazette; "C-U Public Health District's website held hostage by ransomware attack"; 11 MAR 2020; https://www.news-gazette.com/news/local/health-care/c-u-public-health-district-s-website-held-hostage-by/article_2dadedcd-aadb-5cb1-8740-8bd9e8800e27.html; Accessed on 24 MAR 2020.

[12] (U); BleepingComputer; "Ransomware Gangs to Stop Attacking Health Orgs During Pandemic"; 18 MAR 2020; https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/; Accessed on 24 MAR 2020.

[13] (U); ComputerWeekly; "Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack"; 22 MAR 2020; https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus; Date of Access 24 MAR 2020.

[14] (U//FOUO); STAC & WSIC; 2020-4453; DOP: 24 MAR 2020; (U); Actors leverage COVID-19 to Defraud Consumers; Extracted information is UNCLASSIFIED; Overall source classification is U//FOUO).
[15] (U); DHS; "Be Cyber Smart"; 31 MAR 2020; https://www.dhs.gov/be-cyber-smart; Accessed on 31 MAR 2020.
[16] (U); CISA; "AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability"; 10 JAN 2020; https://www.us-cert.gov/ncas/alerts/aa20-010a; Accessed on 31 MAR 2020.
[17] (U); CISA; "NIST Publishes Multifactor Authentication Practice Guide"; 1 AUG 2019; https://www.us-cert.gov/ncas/current-activity/2019/08/01/nist-publishes-multifactor-authentication-practice-guide; Accessed on 31 MAR 2020.
[18] (U); CISA; "Understanding Firewalls for Home and Small Office Use"; 14 NOV 2019; https://www.us-cert.gov/ncas/tips/ST04-004; Accessed on 31 MAR 2020.
[19] (U); CISA; "Avoiding Social Engineering and Phishing Attacks"; 11 MAR 2019; https://www.us-cert.gov/ncas/tips/ST04-014; Accessed on 31 MAR 2020.
[20] (U); FTC; "Coronavirus: Scammers follow the headlines"; 10 FEB 2020; https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines; Accessed on 31 MAR 2020.

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

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Cyber Targeting of US Public Health and Healthcare Sector Likely to Increase During Pandemic

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**