INTELLIGENCE ENTERPRISE

HOMELAND INTELLIGENCE ARTICLE

Homeland Security

15 April 2020

(U) Cyber Mission Center

(U//FOUO) COVID-19: Cybercriminals Almost Certainly Will Continue to Target US Public Using Economic Relief Themes and Scams

(U//FOUO) Scope. This *Article* informs federal, state, local, and private sector partners of the almost certain threat from cybercriminals exploiting COVID-19 financial and economic relief themes for financial gain. This *Article* is the latest in a series of COVID-19 cyber threat products.[a,b] The information cutoff date for this *Article* is 30 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 cybercriminals almost certainly will continue to target the US public using COVID-19 economic- and financial-relief themes and scams. We base this judgment on cybercriminals using COVID-19 government relief themes to lure individuals into downloading financial malware. Cybercriminals already are using COVID-19-themed scams, such as fraudulent websites offering vaccine kits. In addition, cybercriminals historically have used a variety of social engineering techniques to target government and charitable financial relief efforts in the wake of natural disasters, such as hurricanes, earthquakes, and pandemic illnesses and are currently exploiting the COVID-19 pandemic for financial gain.

» (U) Cybercriminals as of at least 30 March 2020 have been targeting individuals waiting for COVID-19 government relief payments with phishing e-mails containing malicious attachments, according to a US cybersecurity company.[1] The e-mails instruct victims to open and fill out the attached document to receive compensation for having to stay home due to COVID-19. The malware is a modular banking Trojan that was first observed in 2015 targeting major financial institutions in the United Kingdom, Brazil, Australia, and North America, according to the same source.

» (U) Cybercriminals since at least 2005 with hurricane Katrina and following subsequent natural disasters as recently as 2018 have set up illegitimate charitable websites to steal money and personal information from victims, according to the FBI and US media reports.[2,3,4] In addition, cybercriminals spoof the websites of legitimate charitable organizations and use e-mails embedded with malicious links and documents to target victims, according to the same FBI report.

» (U) The Department of Justice (DOJ) on 21 March 2020 filed its first enforcement action against COVID-19 fraud, according to a DOJ press release.[5] The fraud scheme involved a website claiming to offer access to World Health Organization vaccine kits for a shipping charge, which consumers would pay for by entering their

[a] (U//FOUO) *Homeland Intelligence Article* titled "Nation-State Cyber Actors Likely to Conduct COVID-19-Themed Spear-Phishing Against Homeland Targets", published on 27 March 2020, serial number IA-43452-20

[b] (U//FOUO) *Homeland Intelligence Article* titled "Cyber Actors Almost Certainly View Growing Telework During the Novel Coronavirus Pandemic as an Opportunity to Exploit Enterprise Networks", published on 30 March 2020, serial number IA-43325-20.

credit card information on the website, according to the same report. The press release also provided recommended steps for Americans to avoid being exploited by these types of scams.[c]

» (U) CISA in May 2019 released a notification ahead of the 2019 hurricane season alerting individuals and organizations to be aware of malicious cyber activity targeting victims and potential donors. Fraudulent e-mails commonly appear after major natural disasters and often contain links or attachments that direct users to malicious websites, according to the CISA notification.[6]

» (U) The US National Center for Disaster Fraud since 2005 has received over 95,000 complaints related to disaster fraud from all 50 states and 6 US territories involving over 100 natural and man-made disasters, according to the DOJ website.[7]

(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

[c] (U); DOJ; "Justice Department Files Its First Enforcement Action Against COVID-19 Fraud: Federal Court Issues Temporary Restraining Order Against Website Offering Fraudulent Coronavirus Vaccine"; 2020; https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud.

(U) Source Summary Statement

(U//FOUO) This *HIA* is based on three DOJ reports, a report from a US cybersecurity company, a CISA notification, and two US media reports.

(U//FOUO) CYMC assesses cybercriminals almost certainly will continue to target the US public using COVID-19 economic and financial relief themes and scams. We have **moderate confidence** in our assessment. Our confidence level is based on multiple reports from authoritative government sources and credible media entities. Our confidence level would increase with additional reporting showing cybercriminal actors' COVID-19 themed activity for financial gain. Our understanding of how cybercriminal actors' tactics, techniques, and procedures have changed or improved over time is a gap.

[1] (U); IBM; "Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy"; 2020; https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/; accessed on 31 MAR 2020.

[2] (U); FBI; "Beware Hurricane Katrina Relief Scams: FBI Cyber Exec Warns of Online Schemers Exploiting the Tragedy"; 2005; https://archives.fbi.gov/archives/news/stories/2005/september/katrina_scams091405; accessed 31 MAR 2020.

[3] (U); Krebs on Security; "Beware of Hurricane Florence Relief Scams"; 2018; https://krebsonsecurity.com/2018/09/beware-of-hurricane-florence-relief-scams/; accessed 31 MAR 2020.

[4] (U); Washington Post; "Fraud Inevitably Follows Disasters, so Authorities in Texas, Florida Prepare for Post-Storm Scams; 2017; https://www.washingtonpost.com/news/true-crime/wp/2017/09/08/fraud-inevitably-follows-disasters-so-authorities-in-texas-florida-prepare-for-post-storm-scams/; accessed 31 MAR 2020.

[5] (U); DOJ; "Justice Department Files Its First Enforcement Action Against COVID-19 Fraud: Federal Court Issues Temporary Restraining Order Against Website Offering Fraudulent Coronavirus Vaccine"; 2020; https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud; accessed on 11 APR 2020.

[6] (U); CISA; "Hurricane Related Scams"; 2019; https://www.us-cert.gov/ncas/current-activity/2019/05/30/Hurricane-Related-Scams; accessed on 30 MAR 2020.

[7] (U); DOJ; "National Center for Disaster Fraud"; 2020; https://www.justice.gov/disaster-fraud; accessed on 31 MAR 2020.

Homeland Security | *Office of Intelligence and Analysis*

Customer Feedback Form

Product Title: (U//FOUO) COVID-19: Cybercriminals Almost Certainly Will Continue to Target US Public Using Economic I

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