3 March 2020

THREAT AWARENESS MESSAGE

(U) Malicious Cyber Actors Conduct Coronavirus-Themed Scams

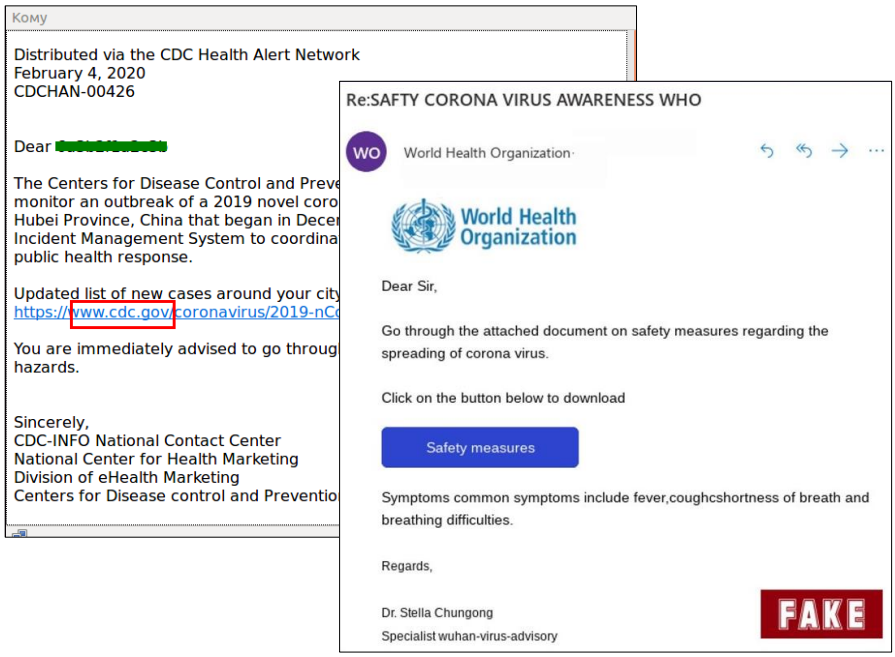
(U) **The Coronavirus outbreak, which has gained international attention, presents an opportunity for malicious actors to take advantage of the worldwide concern and use it to conduct various online scams.** Recently observed activity includes multiple spearphishing campaigns, financial scams, and disinformation campaigns spread via social media websites. Malicious actors are tailoring campaigns to target specific countries or groups in order to collect sensitive information, steal money via fake donation websites, spread false information, and deliver malware to victims.

- (U) Between January and February 2020, several spearphishing campaigns impersonated various healthcare organizations, to include the U.S. Centers for Disease Control (CDC), and the World Health Organization (WHO). In many cases, victims received Coronavirus-themed emails in which the actors requested the victim to open an attachment or click on a link provided via the email in order to obtain details about the Coronavirus. Once a victim clicks on the attachment or link, they are directed to a malicious website controlled by the actors or given a false login pop-up, requesting the victim to enter his/her login credentials. Malicious actors can use the login credentials to access the victim's accounts or to conduct further cyber operations. In a separate campaign, victims received emails that also appeared to originate from the CDC; however, malicious actors requested a donation via Bitcoin to fund a false "incident management system," in relation to the Coronavirus.[1,2]

- (U) In early February 2020, unidentified cyber actors targeted Japan-based users with malicious Coronavirus-themed spearphishing emails. The emails appeared to provide information relating to Coronavirus prevention; however, instead, they contained malicious Microsoft Office files, that when opened, would initiate the download of the notorious Emotet malware. Emotet is a sophisticated Trojan that is continuously evolving and used by various cyber actors in high-profile attacks against targets around the world, to include U.S. military and government targets. (For more reporting on Emotet malware, please see MTAC-TAM-CYBR-033-FY20.)[3,4]

- (U) U.S. officials have recently released statements claiming Russia is likely behind Coronavirus disinformation campaigns that are being spread via social media. Reports indicate thousands of Twitter, Facebook, and Instagram accounts have been discovered, that have been used to spread false information about Coronavirus and blame the U.S. for the outbreak. The posts were created in various languages to reach targets worldwide.[5]

THREAT AWARENESS MESSAGE



(U) Coronavirus-Themed Phishing Emails

(U) **How to identify and prevent becoming a victim of Coronavirus-themed online scams:**

- (U) Go directly to a trustworthy website for information rather than clicking on email attachments, links, or pop-ups
- (U) Double check a website address prior to typing it in as scammers typically slightly alter URLs so they closely resemble a legitimate URL
- (U) Do not enter sensitive data such as username and password into websites that do not typically ask for it
- (U) Use multi-factor authentication whenever possible (something you have and something you know)
- (U) Use complex passwords and use different passwords for different services
- (U) Change passwords often
- (U) Check for spelling and grammatical errors within the contents of emails or suspicious websites
- (U) Keep systems updated and running antivirus software

(U//FOUO) **NCIS assesses with MODERATE confidence that the wide range of Coronavirus scams have the potential to impact DON personnel via a possible compromise of personal and financial information or the download of malware to a vulnerable device.** Malicious actors continually take advantage of worldwide events and breaking news, to easily gain the interest of potential victims. Coronavirus-themed operations will likely increase against United States based users in

THREAT AWARENESS MESSAGE

the near future as the outbreak becomes more widespread. Personnel should stay on the lookout for phishing emails and other scams related to Coronavirus, and follow the steps necessary to prevent the download of malware to their device, or a possible compromise of sensitive information.

(U) Prepared by: MTAC Cyber Threat Division, MTAC_Cyber@ncis.navy.mil

MTAC-TAM-CYBR-042-FY20

(U) SOURCES

[1] (U) Business Insider. 19 February 2020. (U) Email Scammers are Taking Advantage of Coronavirus Fears to Impersonate Health Officials and Trick People into Giving up Personal Information. Cited portion is U. Overall classification is U. (U) Business Insider is an online platform that offers the latest business, celebrity, and technology news across America. https://www.businessinsider.com/coronavirus-email-scam-covid-19-phishing-false-information-who-cdc-2020-2

[2] (U) NBC News. 18 February 2020. (U) How to avoid falling victim to a coronavirus phishing email attack. Cited portion is U. Overall classification is U. (U) NBC News is the news division of the American broadcast television network NBC. https://www.nbcnews.com/better/lifestyle/how-avoid-falling-victim-coronavirus-phishing-email-attack-ncna1137941

[3] (U) Malwarebytes. 10 February 2020. (U) Battling Online Coronavirus Scams with Facts. Cited portion is U. Overall classification is U. (U) Malwarebytes is an American Internet security company that specializes in protecting home computers, smartphones, and companies. https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/

[4] (U) Security Intelligence. 05 February 2020. (U) Emotet Activity Rises as it Uses Coronavirus Scare to Infect Targets in Japan. Cited portion is U. Overall classification is U. (U) Security Intelligence is an online platform that provides analysis and insight for information security professionals. https://securityintelligence.com/posts/emotet-activity-rises-as-it-uses-coronavirus-scare-to-infect-targets-in-japan/

[5] (U) Business Insider. 24 February 2020. (U) U.S. Accuses Russia of Spreading Conspiracies about the Wuhan Coronavirus, Including that it's a CIA Biological Weapon. Cited portion is U. Overall classification is U. (U) Business Insider is an online platform that offers the latest business, celebrity, and technology news across America. https://www.businessinsider.com/us-officials-claim-russian-coronavirus-disinformation-campaign-2020-2