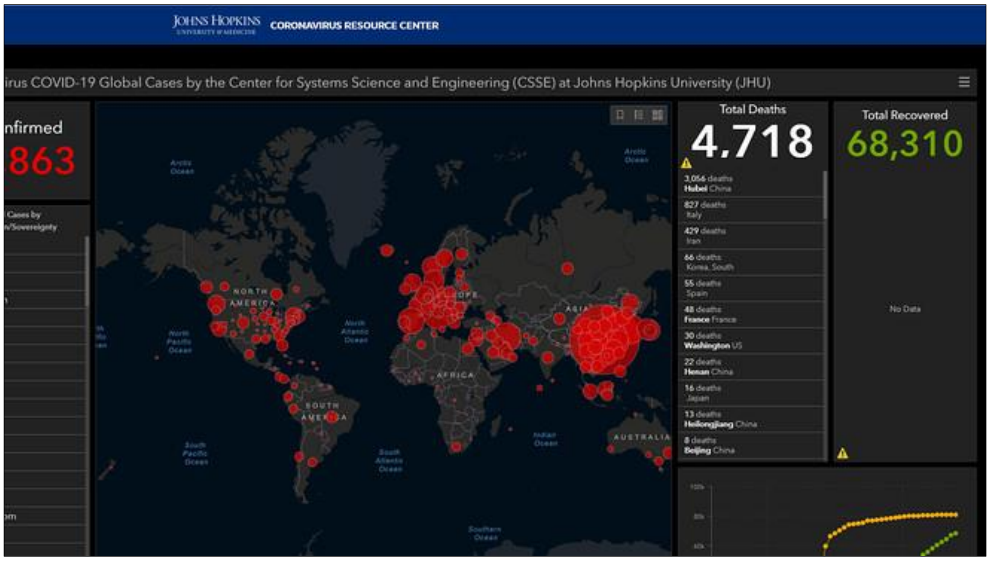
19 March 2020

# THREAT AWARENESS MESSAGE

## (U) Malicious Actors Hide Info-Stealing Trojan in Fake Coronavirus (COVID-19) Maps

(U) **Recently published NCIS Threat Advisory Messages MTAC-TAM-CYBR-042-FY20 and MTAC-TAM-CRIM-003-FY20 discussed various scams capitalizing on fears relating to the COVID-19 pandemic, including a recent report of a malicious website link that directs users to a false live map for tracking global COVID-19 cases.** While the map appears to be a legitimate reference from John Hopkins University, it is being used by unidentified cyber actors to spread malware to victims around the world. The malicious link is likely delivered to victims via phishing emails or online advertisements, some of which may show up during an online search for COVID-19. Once a victim clicks the link to view the map, a sophisticated information-stealing Trojan known as AZOrult is downloaded to the victim's device. AZOrult has the ability to download additional malware and exfiltrate sensitive data such as financial information, chat sessions, login credentials, browsing history, and more. The Trojan is currently available to malicious actors on underground forums.[1,2,3,4]



JOHNS HOPKINS UNIVERSITY & MEDICINE CORONAVIRUS RESOURCE CENTER

irus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)

nfirmed
863

Total Deaths
4,718

3,056 deaths
Hubei China

827 deaths
Italy

429 deaths
Iran

66 deaths
Korea, South

55 deaths
Spain

48 deaths
France France

30 deaths
Washington US

22 deaths
Henan China

16 deaths
Japan

13 deaths
Heilongjiang China

8 deaths
Beijing China

Total Recovered
68,310

No Data

(U) Fake Coronavirus Map

(U) AZOrult has been used against victims around the world since at least 2016 and malicious actors continuously improve the malware to enhance its information-stealing and downloading capabilities. Several samples of the malware recently discovered by security researchers revealed advanced obfuscation techniques, and the ability to go beyond basic information-stealing  to steal more cryptocurrency wallets, chat history and files from popular communication apps (e.g. Skype, Telegram, and Steam), and credentials, cookies, and histories from more browsers than it was previously capable of targeting. As actors continue to advance the capabilities of AZOrult, the number of possible targets the malware can be used against continues to expand.[5,6]

# THREAT AWARENESS MESSAGE

(U//FOUO) **NCIS assesses with MODERATE confidence that malicious actors will continue to use the COVID-19 outbreak as an opportunity to victimize users for financial gain or data theft.** Activities associated with AZOrult are likely widespread and not tailored to a specific set of targets; however, DON personnel could unwittingly fall victim to a compromise of personally identifiable information (PII), financial information, or other sensitive information if a device becomes infected with AZOrult malware. To help mitigate the download or spread of malware, users should refrain from opening or forwarding emails from unknown or suspicious senders, go directly to a trustworthy website for information rather than clicking on a link provided through search engines or pop-ups, and download a reputable antivirus software program that runs security scans often.

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

MTAC-TAM-CYBR-049-FY20

## (U) SOURCES

[1] (U) KHON2. 13 March 2020. (U) Fake Online Coronavirus Map Infects Computers with Malware. Cited portion is U. Overall classification is U. (U) KHON2 is a Hawaii news and weather website. https://www.khon2.com/coronavirus-2/fake-online-coronavirus-map-infects-computers-with-malware/

[2] (U) Malpedia. (U) AZOrult. Cited portion is U. Overall classification is U. (U) Malpedia is an independent resource for identifying and investigating malware. https://malpedia.caad.fkie.fraunhofer.de/details/win.azorult

[3] (U) Threat Vector. 04 June 2019. (U) Threat Spotlight: Analyzing AZOrult Infostealer Malware. Cited portion is U. Overall classification is U. (U) Threat Vector provides daily cyber related videos and research articles. https://threatvector.cylance.com/en_us/home.html

[4] (U) Trustwave. 15 October 2019. (U) Messing with AZOrult Part 1: Malware Breakdown. Cited portion is U. Overall classification is U. (U) Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data and reduce security risk. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/messing-with-azorult-part-1-malware-breakdown/

[5] (U) Proofpoint. 30 July 2018. (U) New Version of AZOrult Stealer Improves Loading Features, Spreads Alongside Ransomware in New Campaign. Cited portion is U. Overall classification is U. (U) Proofpoint is an enterprise security company that provides software as a service and products for inbound email security, outbound data loss prevention, social media, mobile devices, digital risk, email encryption, electronic discovery, and email archiving. https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

[6] (U) Palo Alto Networks Unit 42. 21 November 2018. (U) New Wine in Old Bottle: New AZOrult Variant Found in FindMyName Campaign Using Fallout Exploit Kit. Cited portion is U. overall classification is U. (U) Palo Alto Networks is a multinational cybersecurity company headquartered in the United States. https://unit42.paloaltonetworks.com/unit42-new-wine-old-bottle-new-azorult-variant-found-findmyname-campaign-using-fallout-exploit-kit/