Homeland Security

23 April 2020

(U) Cyber Mission Center and Counterintelligence Mission Center

(U//FOUO) Cyber Actors Develop Malicious COVID-19-Themed Mobile Applications That Likely Pose a Growing Threat to Third-Party App Store Users

(U//FOUO) Scope. This *Article* warns federal, state, local, and private sector stakeholders of a growing threat to their employees who use third-party app stores of malicious COVID-19-themed mobile applications.[a] Employees seeking information on COVID-19 should avoid downloading applications from untrusted sources and third-party market places, and further, should scrutinize applications from approved market places for trustworthiness and origin. This *Article* is the latest in a series of COVID-19 cyber threat products.[b,c,d,e,f] 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) and Counterintelligence Mission Center (CIMC). 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) Release of malicious COVID-19-themed mobile apps by suspected state-sponsored and unidentified cyber actors likely poses a growing threat to US users of third-party app stores. We base this judgment on reporting Iran and Libya-based cyber actors developing COVID-19-themed mobile applications with embedded spyware to target domestic users. We also base this judgment on unidentified cyber actors deploying ransomware against what appears to be a broader target group of Android users. In addition, we assume the threat of malicious COVID-19-themed mobile applications targeting the homeland is more widespread than the limited available reporting reflects due to potential underreporting during the current public health crisis.

(U) Cyber Actors Capitalize on Global Events

(U) Cyber actors often capitalize on events with global attention and exploit those seeking relevant information with malware. For example, during the 2018 FIFA World Cup, cyber actors created multiple malicious apps that were advertised as live match streaming apps or apps that predict the outcome of the game; however, once these apps were downloaded, they provided cyber actors with access to victims' devices.[1]

[a] (U) Third-party app stores are application marketplaces that are developed and managed by a company other than the manufacture of the device or operating system.
[b] (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 is IA-43452-20.
[c] (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 is IA-43325-20.
[d] (U//FOUO) *Homeland Intelligence Article* titled "Malicious Cyber Actors Likely See Opportunity to Target Virtual Private Network Vulnerabilities as More People Telework Due to COVID-19," published on 8 April 2020, serial number is IA-43472-20.
[e] (U//FOUO) *Homeland Intelligence Article* titled "COVID-19: Cybercriminals Almost Certainly Will Continue to Target US Public Using Economic Relief Themes and Scams," published on 15 April 2020; serial number is IA-43603-20
[f] (U//FOUO) *Homeland Intelligence Today Article* titled "(U//FOUO) Cyber Targeting of US Public Health and Healthcare Sector Likely to Increase During Pandemic," published on 15 April 2020; serial number is IA-43541-20.

IA-43540-20

» (U) Iran released an application named "AC19" in mid-March 2020, according to a credible American business technology news website.[2] The application allows users to register their phone numbers, and then asks users a series of questions related to coronavirus symptoms, according to the same report. Though the public-facing functionality of the application appears to be designed for domestic use, it was initially made available on Google's Android application store, contains real-time geolocation technology with a remote backend, and was developed by a company that is suspected of building applications for Iranian intelligence agencies, according to the same report and a separate USG media outlet that reported on previous Iranian state-sponsored applications.[3] Though Google has since removed the application from its store, it remains available on third-party sites. It is also worth noting Iran has historically designed its mobile applications to look similar to their Western equivalents, according to an American financial and business news website.[4]

» (U) Researchers in mid-March 2020 also discovered a malicious COVID-19-themed Android application, called "corona live 1.1." that has embedded spyware and appears to be part of a larger mobile surveillance campaign operating from Libya, according to a US-based information technology security company.[5] The application requests access to photos, media, files, and device location, as well as permission to take pictures and record video, according to the same source. The application is a trojanized version of the legitimate "corona live" application, which provides an interface to the data found on the Johns Hopkins coronavirus tracker, including infection rates and number of deaths over time per country. Though the malicious application is intended to target Libyan individuals, it is available on third-party sites.

» (U) A COVID-19 tracking mobile application, named "CovidLock," since at least mid-March 2020 has been infecting Android devices with ransomware, according a US-based cybersecurity firm and a Romanian-based technology news website.[6,7,8] The application reportedly deploys a screen lock attack that reconfigures the password used to protect the device, locks the device, and demands the owner pay a $100 ransom in Bitcoin to unlock the device, according to the same reports. The actors claim they will steal sensitive data—such as photos, videos, and social media—and leak it online, as well as, erase the phone's memory if the ransom is not paid in 48 hours, according to the same sources. The same cybersecurity firm has reportedly reverse engineered the ransomware and will make the decryption key publicly available.

(U) Outlook: Counterintelligence Concern

(U//FOUO) Foreign-developed COVID-19 apps also present a growing counterintelligence concern. In addition to the app Iran released, Israel in mid-March 2020 also released an app named "Hamagen" or "The Shield," according to a UK-based broadcast news organization.[9] The app allows users to allow access to their cellphone location data, which is then compared to data on confirmed COVID-19 patients held by the Ministry of Health, according to the same report. Although the app appears to be developed for legitimate use and there is no evidence of malicious activity, there is the potential for its misuse given its availability to the public and its vague policy terms regarding information sharing with authorities.

(U//FOUO) Israel's Shin Bet internal security service since at least mid-March 2020 was authorized to use undisclosed collection techniques and cellphone data to track the movements of people who have contracted COVID-19 and identify others who should be quarantined if their paths cross, according to a US-based newspaper with worldwide readership.[10] Shin Bet has previously used similar authorities for counterterrorism in Israel. While this COVID-19 application could provide Shin Bet with additional user data, they are already capable of tracking cellphones of individuals in Israel, regardless if the app has been downloaded.

(U//FOUO) Although these apps are designed for use in Israel, their potential availability to US persons could enable Shin Bet collection efforts against homeland targets during and after the COVID-19 public health crisis.

(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

(U) Source Summary Statement

(U//FOUO) This assessment is based on nine articles from credible sources that specialize in technology, cybersecurity, financial and business, and other media reporting.

(U//FOUO) Release of malicious COVID-19-themed mobile applications by suspected state-sponsored and unidentified cyber actors likely poses a growing threat to US users of third-party app stores. We have **low confidence** in this assessment. Our confidence is derived entirely from a limited body of open-source reporting, which includes a mixture of news, media, cybersecurity and information technology security sources covering this topic. We would have higher confidence in this assessment if we had data on the scale and scope of these campaigns and others exploiting the COVID-19 public health crisis with malicious mobile applications, and data on US compromises from these and other similarly malicious applications. Having that additional data would provide for a clearer threat picture and enable us to further assess adversary intent and identify those most at risk. We are submitting additional collection requirements to help fill some of these gaps and also are leveraging private sector cybersecurity partner detection capabilities.

[1] (U); TrendMicro; "Sporting Event Threats: Lessons from the 2018 FIFA World Cup"; 7 November 2018; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/sporting-event-threats-lessons-from-the-2018-fifa-world-cup; accessed on 25 March 2020.

[2] (U); ZDNET; "Coronavirus: Business and technology in a pandemic": 09 MAR 2020; https://www.zdnet.com/article/spying-concerns-raised-over-irans-official-covid-19-detection-app/; accessed on 20 MAR 2020.

[3] (U); Radio Farda; "Lawmaker Says Iran Behind Bogus Messaging Apps, Banned By Google": 06 May 2019; https://en.radiofarda.com/a/lawmaker-says-iran-behind-bogus-messaging-apps-banned-by-google/29924990.html; accessed on 20 MAR 2020.

[4] (U); Business Insider; "From an app store named after the Persian word for 'apple,' to a payments platform called ZarinPal, Iran's most popular apps are strikingly similar to their Western equivalents"; 24 OCT 2019; https://www.businessinsider.com/iranian-apps-that-mimic-western-counterparts-netflix-uber-app-store-2019-10; accessed on 20 MAR 2020.

[5] (U); Lookout; "New Threat Discovery Shows Commercial Surveillanceware Operators Latest to Exploit COVID-19"; 18 MAR 2020; https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19; accessed on 20 MAR 2020.

[6] (U); DOMAINTOOLS; "CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware"; 13 March 2020; https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#; accessed on 20 March 2020.

[7] (U); DOMAINTOOLS; "CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware; 16 March 2020; https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware; accessed on 24 MAR 2020

[8] (U); Softpedia; "Virus-tracking app coming with a virus of its own"; 16 March 2020; https://news.softpedia.com/news/coronavirus-tracker-infects-smartphone-with-ransomware-529464.shtml; accessed on 20 MAR 2020.

[9] (U); BBC; "Israel launches apps to help fight virus"; 25 MARCH 2020; https://www.bbc.com/news/topics/c302m85q5ljt/israel; accessed on 30 MAR 2020.

[10] (U); The New York Times; "To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data"; 16 MARCH 2020; https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html; accessed on 30 MAR 2020.

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

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Cyber Actors Develop Malicious COVID-19-Themed Mobile Applications That Likely Pose a Gro

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-43540-20 REV: 01 August 2017