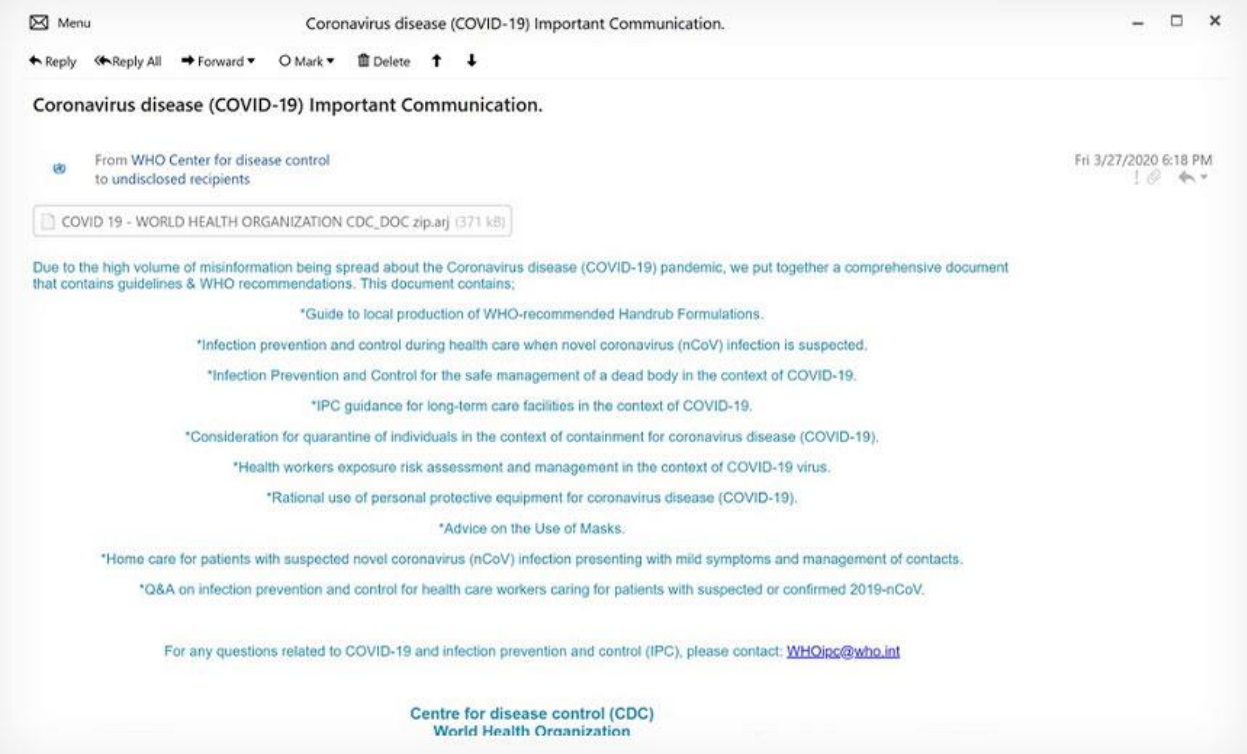
Spear-Phishing Campaign Uses COVID-19 to Spread LokiBot



Spear-phishing email using WHO images (Source: FortiGuard Labs)

A recently uncovered spear-phishing campaign is using fears of the COVID-19 pandemic to spread a specific information stealer called LokiBot, according to a report released by FortiGuard Labs, the research arm of security firm Fortinet.

Once again, researchers find that attackers are using official images and other trademarks of the **World Health Organization** as a lure to entice victims to open an attached message that contains the malware, according to the report. In a twist, the phishing email pretends to offer details about misinformation concerning the COVID-19 pandemic.

"The body of the email contains multiple points about infection control and other suggestions and recommendations, which is obviously a lure to further compel the recipient to continue reading," the report notes. "And in a twisted fashion, the messaging pretends to address misinformation related to COVID-19/Coronavirus."

The phishing campaign started around March 27, although it is not clear if it is still active. FortiGuard Labs researchers believe that these spear-phishing emails have targeted victims mainly in the U.S., Turkey, Portugal, Germany and Austria.

Phishing Emails

The spear-phishing emails, written in English, contain numerous grammar and spelling mistakes. For example, the researchers' note that the emails contain a reference to the U.S. "Centre for Disease Control," when the American version of the word should be spelled "Centers." The emails also claim the CDC is located in Switzerland, when the actual agency is headquartered in Atlanta.

The spear-phishing emails contain an attached compression file called "COVID_19-WORLD HEALTH ORGANIZATION CDC_DOC.zip.arj," which can be opened with 7-Zip. ARJ is actually a compression format for creating very efficient compressed files. The attackers appear to have used this format to present the file as legitimate, according to Val Saengphaibul, a FortiGuard Labs researcher who wrote the report.

"The attackers behind this latest attack likely hope that the ARJ format might allay the concerns of an unsuspecting victim about opening an unknown attachment, given that the populace has been trained to not open suspicious file extensions such as .exe," Saengphaibul notes.

If the attachment is opened and decompressed, another file called "DOC.pdf.exe" appears. If opened, this file attempts to plant the LokiBot within the infected device, according to the report.

Once installed, the LokiBot information stealer is able to capture a wide range of data, including FTP credentials, stored email passwords, passwords stored in the browser as well as other credentials. Once collected, the exfiltrated information is sent to a specific URL controlled by the attackers, the report notes.

Versions of LokiBot have been developed over the past several years, and the malware can be bought for as little as $300 on dark net market forums. Nigerian criminal gangs

have used this information stealer for a variety of schemes, including business email compromise scams (see: Nigerian BEC Scammers Increase Proficiency: Report).

A March report by Recorded Future noted that nation-state actors are also using phishing emails with a COVID-19 message to plant malware, including LokiBot, on victims' devices (see: Nation-State Hackers Using COVID-19 Fears to Spread Malware).

https://www.careersinfosecurity.com/spear-phishing-campaign-uses-covid-19-to-spread-lokibot-a-14058