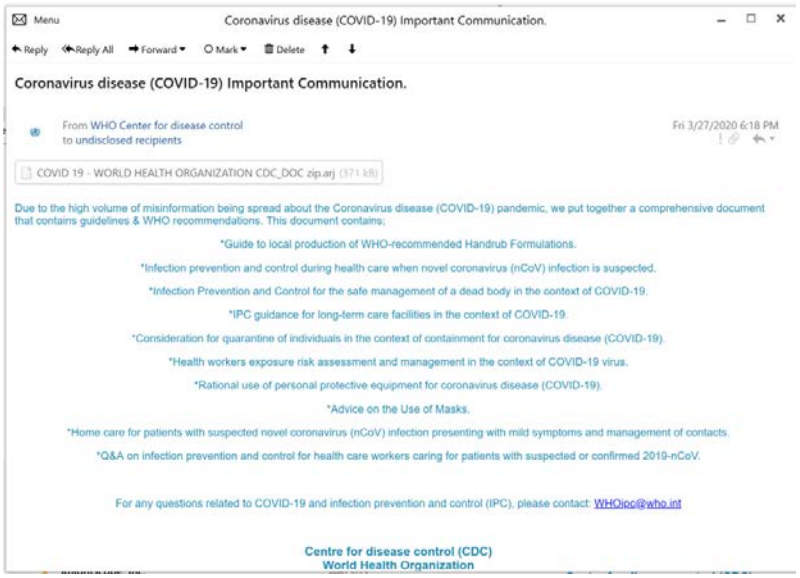
Health Sector Cybersecurity Coordination Center (HC3)
Sector Note
June 16, 2020 **TLP: WHITE** **Report: 202006161030**

LokiBot Malware Threat to Healthcare

Executive Summary

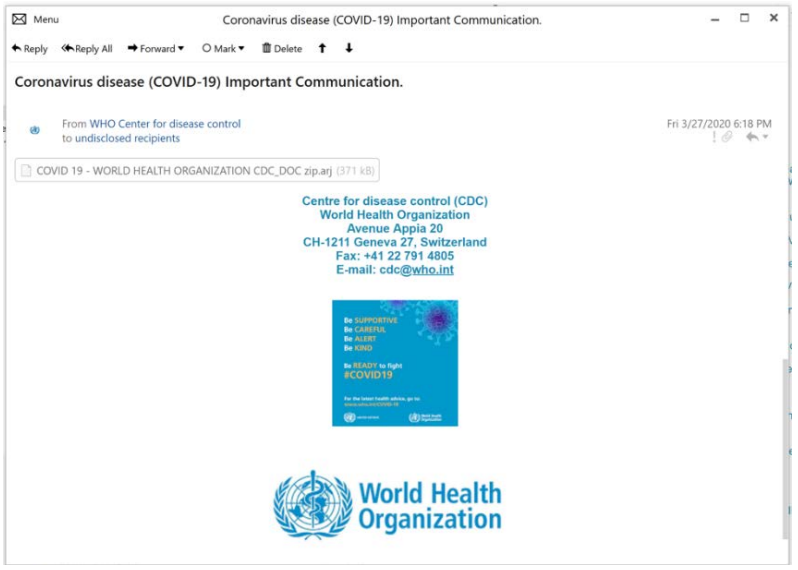
Researchers have discovered threat actors are capitalizing on attention towards the COVID-19 pandemic and the World Health Organization (WHO) with a new spearphishing email designed to spread the LokiBot trojan that uses the WHO trademark as a lure.

Lokibot is an information stealer; the main functionality of its binary is to collect system and application credentials and user information to send back to the attacker.



Report

In late March, FortiGuard Labs discovered a new COVID-19/Coronavirus-themed spearphishing email that uses the World Health Organization (WHO) trademark in an attempt to convince recipients of its authenticity. The email contains the subject line "Coronavirus disease (COVID-19) Important Communication." It also includes an attachment entitled "COVID_19- WORLD HEALTH ORGANIZATION CDC_DOC.zip.arj" that appears to contain additional information, but is in fact a decoy. Since it was first detected, the spearphishing campaign has gone global, with Turkey, Portugal, Germany, Austria and the United States showing the highest incidents.



Lokibot is a malware designed to collect credentials and security tokens from an infected machine running on a Windows Operating System (OS). Lokibot was first observed in 2015, when it targeted cryptocoin wallets, though there is evidence that the widely-spread version was a hijacked version (also referred to as patched or cracked version) of the earlier one. One of the key differences is that the patched version allows the attacker to change the command and control (C2) URL.

Once executed, Lokibot unpacks the main binary into memory using hollow process injection2 to insert itself into a legitimate Microsoft Windows application to hide its activities. Lokibot also uses an infected system machine global unique identifier (GUID) value to generate a mutex (an MD5 hash) that acts as a flag to prevent itself from infecting the same machine again. Lokibot collects information and credentials from multiple applications, including but not limited to Mozilla Firefox, Google Chrome, Thunderbird, FTP and SFTP applications.

To prevent infection, HC3 recommends that all Antivirus and Intrusion Prevention System definitions are kept up to date on a continual basis. Healthcare Organizations are also urged to maintain a proactive patching routine whenever vendor updates are made available. If it is deemed that patching a device is not feasible, it is recommended that a risk assessment is conducted to determine additional mitigation safeguards.

Healthcare Organizations are encouraged to conduct ongoing training sessions to educate and inform personnel about the latest phishing/spearphishing attacks. Employees should also be reminded to never open attachments from someone they don't know, and to always treat emails from unrecognized/untrusted senders with caution.

References

Montalbano, Elizabeth. "Spearphishing Campaign Exploits COVID-19 To Spread Lokibot Infostealer," April 3, 2020. https://threatpost.com/spearphishing-campaign-exploits-covid-19-to-spread-lokibot-infostealer/154432/.

Saengphaibul, Val. "Latest Global COVID-19/Coronavirus Spearphishing Campaign Drops Infostealer." Fortinet Blog, April 2, 2020. https://www.fortinet.com/blog/threat-research/latest-global-covid-19-coronavirus-spearphishing-campaign-drops-infostealer.html.

"LokiBot Impersonates Popular Game Launcher and Drops Compiled C# Code File." TrendLabs Security Intelligence Blog, February 14, 2020. https://blog.trendmicro.com/trendlabs-security-intelligence/lokibot-impersonates-popular-game-launcher-and-drops-compiled-c-code-file/.

"Most LokiBot Samples in the Wild Are 'Hijacked' Versions of the Original Malware." The Hacker News, July 6, 2018. https://thehackernews.com/2018/07/lokibot-infostealer-malware.html.

"LokiBot Malware Profile." FireEye Threat Intelligence, July 21, 2017. https://intelligence.fireeye.com/reports/17-00006560.