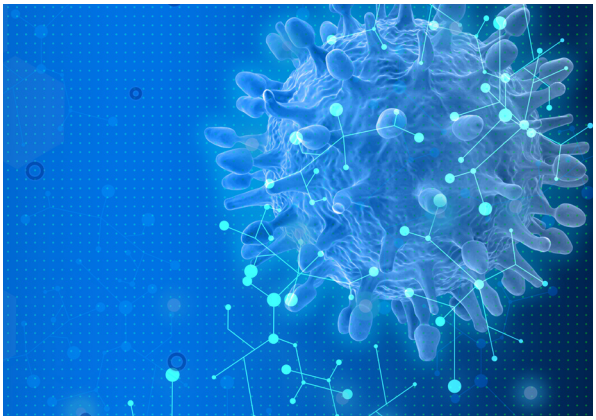
Spoofed Coronavirus Map Delivers AZORult Infostealer

Author: James Barnett



Overview

On 9 March, Reason Security reported on a malicious campaign that used a weaponized Coronavirus map to deliver the AZORult information stealer (infostealer).[1]

Infoblox has been monitoring Coronavirus-themed lures; this is our second Cyber Campaign Brief on the topic.[2] We are taking this opportunity to provide an expanded list of indicators from other malware campaigns using a Coronavirus lure (see Appendix).

Customer Impact

AZORult is an infostealer that can steal a victim's credentials, Bitcoin wallets, chat logs, and files. It can also take screenshots of the infected system and transmit them to the attacker.

Infoblox has previously published on AZORult,[3] including a detailed report on its characteristics.[4] While most of that analysis remains accurate, the AZORult sample from this campaign includes methods to achieve persistence, whereas the previous sample did not.

Campaign Analysis

The primary lure in this campaign was a Coronavirus map that was a repurposed version of the legitimate Coronavirus dashboard produced by Johns Hopkins University.[5]

While we found no information about the distribution method(s) for this campaign, the actors behind AZORult have previously distributed the infostealer via malicious advertisements that masquerade as legitimate services to lure users into downloading and installing the malware.[6]

Attack Chain

When the victim downloads and runs the malicious executable, it creates and runs two additional executables.

The first, Corona-virus-Map.com.exe, is a benign Coronavirus dashboard that the threat actors plagiarized from John Hopkins University. This file is essentially a decoy to convince the victim that the application is legitimate.

The second executable, Corona.exe, is an AZORult unpacker that contains an embedded Windows batch file and a password-protected archive. Upon execution, Corona.exe drops the batch and archive file onto the infected system and uses cmd.exe to run the batch file. The batch file then extracts and executes the malicious AZORult payload contained within the password-protected archive.

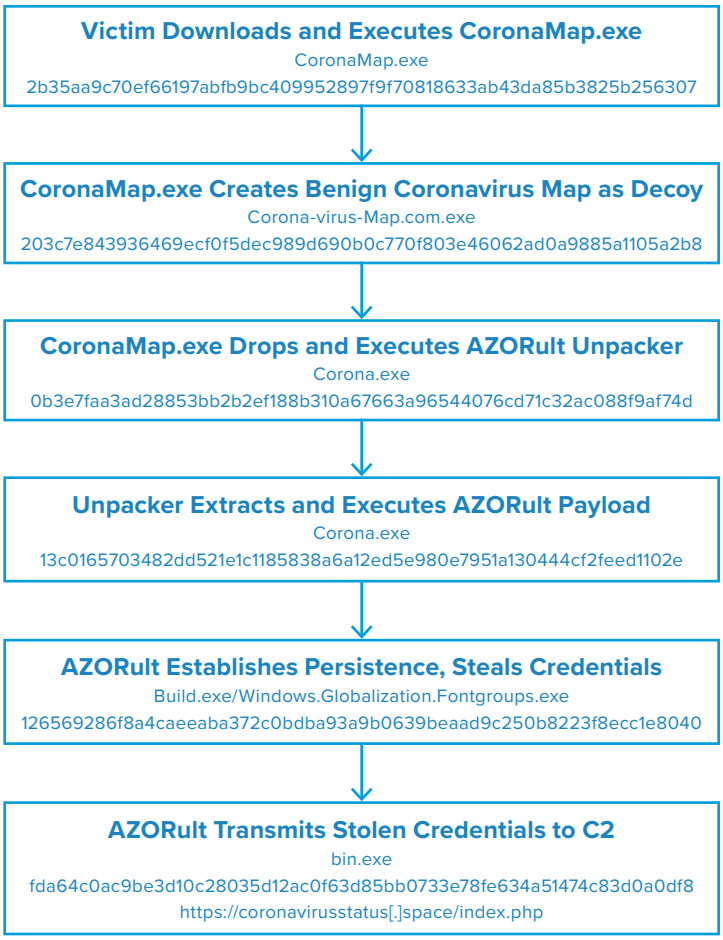
When the AZORult payload first runs, it uses a legitimate Windows dynamic link library (DLL) named taskschd.dll to create a scheduled task that runs every 60 seconds. This task checks to see if a copy of AZORult is still running, and if not, it creates and executes a new copy of the malware.

After achieving persistence via its scheduled task, AZORult proceeds to harvest sensitive user credentials and valuable files from the victim's system. It then compresses this stolen data into an encrypted archive and transmits it to its command and control (C2) server.

Vulnerabilities & Mitigation

Threat actors often use current events to lure victims into downloading and executing malware. Infoblox recommends the following actions to reduce the risk of this type of infection:

- Use only credible sources to download essential installers.
- Verify that necessary installers only download the desired software.
- Scan downloaded files with antivirus software.
- Do not allow web browsers such as Mozilla Firefox or Google Chrome to save credentials or other sensitive information.



Appendix

Representative Indicators of Compromise	Description
CoronaMap.exe 2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307	Coronavirus map with AZORult unpacker
Corona-virus-Map.com.exe 203c7e843936469ecf0f5dec989d690b0c770f803e46062ad0a9885a1105a2b8	Decoy Coronavirus map
Corona.exe 0b3e7faa3ad28853bb2b2ef188b310a67663a96544076cd71c32ac088f9af74d	AZORult unpacker
Corona.exe 13c0165703482dd521e1c1185838a6a12ed5e980e7951a130444cf2feed1102e	AZORult payload
Build.exe 126569286f8a4caeeaba372c0bdba93a9b0639beaad9c250b8223f8ecc1e8040	AZORult persistence / infostealer module
bin.exe fda64c0ac9be3d10c28035d12ac0f63d85bb0733e78fe634a51474c83d0a0df8	AZORult C2 communication module
https://coronavirusstatus[.]space/index.php coronavirusstatus[.]space	AZORult C2

Representative IOCs from Other Coronavirus-Themed Campaigns	Description
FW: Sensient Food Colors _ Supply Chain Update in the Context of Coronavirus (Covid-19)] Payment Slip - Transferred 19/02/2020 FW: Corona Virus (Covid-19 / 2019-nCoV) Impact to Sea freight Supply Chains	LokiBot malspam subject lines
GEE CustomerUpdate English Corona 27022020..rar CoVid19_BAH.PDF.tar	LokiBot malspam attachment file names
d63b218af57f1c9c80bb394695fd51174fe580d6d46843e9e236d74ea6e83460 a98fc7162c77d34068fd270dd762ea98557b8743aad2165f311c6d92a9f84fa0	LokiBot file SHA256
http://tailuong[.]com[.]vn/[.]xxx/playbook/onelove/fre[.]php site-inspection[.]com	LokiBot C2s
2020 Coronavirus Updates Coronavirus Updates	Spoofed WHO Formbook campaign subject lines
HealthCare.pdf.zip	Spoofed WHO Formbook campaign file name
77adf962cb6e58d91aba3893c335e106d1e1a3ce458614dd7a74b58f2d28d003	Spoofed WHO Formbook campaign attachment SHA256
moleaves[.]ml	Spoofed WHO Formbook campaign sender host
Coronavirus: Informazioni importanti su precauzioni	Ostap/Trickbot campaign subject line
F\d{11}.doc	Regex for Ostap/Tricbot campaign file name
dmg[.]ncyes[.]ncyu[.]edu[.]tw	Ostap/Trickbot campaign sender host
a496abe5caf5e37c7621b4e162c297f6f2a598e703940155d83b740462281aed de93bb4ac611385c59539ab193ad246f7db10f2175264cbf0cb2a7a9f960ae2f 85aa463c30c04be31a544fd2bf7b498a8aec658c7f0df42aed1732b68d32b4d5	Ostap/Trickbot campaign campaign attachment SHA256s
45[.]128[.]134[.]14 185[.]234[.]73[.]125 https://45[.]128[.]134[.]14/C821al/vc2Tmy[.]php https://185[.]234[.]73[.]125/wMB03o/Wx9u79[.]php	Ostap C2s

Endnotes

1. https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--62
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--17
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--29
5. https://coronavirus.jhu.edu/map.html
6. https://securityintelligence.com/news/azorult-trojan-uses-fake-protonvpn-installer-to-disguise-attacks/

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com