Reason LABS

THREAT ANALYSIS REPORT

COVID-19

Info Stealer & the Map of Threats

By **Shai Alfasi**, Cybersecurity researcher at **Reason Labs**

Table of Contents

Summary

As global awareness of a Coronavirus pandemic gradually gives way to full out panic, and as governments begin ramping up their efforts to combat the virus and protect its citizens, global news agencies find themselves racing to answer the public's demand for accurate information about new Corona related infections, deaths, transmissions etc.

This demand creates a vulnerability that malicious actors have quickly taken advantage of by spreading malware disguised as a "Coronavirus map". Reason Labs' cybersecurity researcher, Shai Alfasi, found and analyzed this malware which had weaponized coronavirus map applications in order to steal credentials such as user names, passwords, credit card numbers and other sensitive information that is stored in the users' browser. Attackers can use this information for many other operations as well, such as selling it on the deep web or for gaining access to bank accounts or social media.

The new malware activates a strain of malware known as AZORult. AZORult is an information stealer and was first discovered in 2016. It is used to steal browsing history, cookies, ID/passwords, cryptocurrency and more. It can also download additional malware onto infected machines. AZORult is commonly sold on Russian underground forums for the purpose of collecting sensitive data from an infected computer. There is also a variant of the AZORult that creates a new, hidden administrator account on the infected machine in order to allow Remote Desktop Protocol (RDP) connections.

As the corona virus continues to spread and more apps and technologies are developed to monitor it, we will likely be seeing an increase in corona malware and corona malware variants well into the foreseeable future.

Sample Analyzed

VT: https://www.virustotal.com/gui/file/2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307/detection

File Name Corona-virus-Map.com.exe

MD5 73da2c02c6f8bfd4662dc84820dcd983

SHA-1 949b69bf87515ad8945ce9a79f68f8b788c0ae39

SHA-256 2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307

File Size 3.26 MB (3421696 bytes)

File Type Win32 EXE

First Submission 2020-03-02 16:50:25

Persistence & Installation

Short summary

The malware has a GUI that looks very good and convincing. When running the malware, the GUI window loads information, which it pools from the web.

The malware uses a few layers of packing as well as a multi-sub-process technique to make research more difficult. The malware also uses an information stealing technique, which was first seen in 2016 and related to the “AZORult” malware family. To make sure the malware can persist and keep operating, it uses the “Task Scheduler”.

Indicators of compromise

Created Files

Corona-virus-Map.com.exe	C:\Users\%username%\AppData\Local\Temp\aut9BDA.tmp
Corona-virus-Map.com.exe	C:\Users\%username%\AppData\Roaming\Z11062600\Corona[.]exe
Corona-virus-Map.com.exe	C:\Users\%username%\AppData\Local\Temp\aut9DFE.tmp
Corona-virus-Map.com.exe	C:\Users\%username%\AppData\Roaming\Z11062600\Corona-virus-Map.com[.]exe
Corona.exe	C:\Users\%username%\AppData\Local\Temp\RarSFX0\Corona[.]bat
Corona.exe	C:\Users\%username%\AppData\Local\Temp\RarSFX0\Corona.sfx[.]exe
Corona.exe	C:\Users\%username%\AppData\Local\Temp\autA83E.tmp
Corona.exe	C:\Users\%username%\AppData\Roaming\Z58538177\bin[.]exe
Corona.exe	C:\Users\%username%\AppData\Local\Temp\autAAB0.tmp
Corona.exe	C:\Users\%username%\AppData\Roaming\Z58538177\Build[.]exe
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-console-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-datetime-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-debug-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-errorhandling-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-2-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-file-l2-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-handle-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-heap-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-interlocked-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-libraryloader-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-localization-l1-2-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-memory-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-namedpipe-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-processenvironment-l1-1-0.dll

Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-processthreads-l1-1-0.dl
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-processthreads-l1-1-1.dl
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-profile-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-rtlsupport-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-string-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-console-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-2-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-sysinfo-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-timezone-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-util-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-conio-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-convert-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-environment-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-filesystem-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-heap-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-locale-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-math-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-multibyte-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-private-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-process-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-runtime-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-stdio-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-string-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-time-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-c
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-2-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-sysinfo-l1-1-0.dll

Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-timezone-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-util-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-conio-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-convert-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-environment-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-filesystem-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-heap-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-locale-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-math-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-multibyte-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-2-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-sysinfo-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-timezone-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-core-util-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-conio-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-convert-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-environment-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-filesystem-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-heap-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-locale-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-math-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-multibyte-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-private-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-process-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-runtime-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-stdio-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-string-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-time-l1-1-0.dll

Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\api-ms-win-crt-utility-l1-1-0.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\freebl3.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\mozglue.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\msvcp140.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\nss3.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\nssdbm3.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\softokn3.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\ucrtbase.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\vcruntime140.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\nss3.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\nss3.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\mozglue.dll
Bin.exe	C:\Users\%username%\AppData\Local\Temp\2fda\vcruntime140.dll
Build.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Local\Temp\autB628.tmp
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.sqlite3.module.dll.2
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.sqlite3.module.dll
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Local\Microsoft\Windows\INetCache\IE\2KY2PE8H\getMe[1].json
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_74167E25E5476CCA2A5946AAA61BF9E1
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Local\Microsoft\Windows\INetCache\IE\1OZ94YX5\json[1].json
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\1\Information.txt
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Local\Temp\autCC51.tmp
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.module.exe.2
Windows.Globalization.Fontgroups.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.module.exe

Windows.Globalization.Fontgroups.module.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z
Windows.Globalization.Fontgroups.module.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z
Windows.Globalization.Fontgroups.module.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z
Windows.Globalization.Fontgroups.module.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z
Windows.Globalization.Fontgroups.module.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z
Windows.Globalization.Fontgroups.module.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z
Windows.Globalization.Fontgroups.module.exe	C:\Users\%username%\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z

Modified registers

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntrane

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix

HKLM\System\CurrentControlSet\Services\bam\State\
UserSettings\S-1-5-21-3887374624-1885671809-3229943349-1001\\Device\HarddiskVoume4\Windows\SysWOW64\
cmd.exe

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475

HKCU\Software\Classes\Local Settings\MuiCache\56\52C64B7E\LanguageList

HKCU\Software\Classes\Local Settings\MuiCache\56\52C64B7E\LanguageList

HKCU\Software\Classes\Local Settings\MuiCache\56\52C64B7E\LanguageList

HKCU\Software\Classes\Local Settings\MuiCache\56\52C64B7E\LanguageList

Mutexes Created

\Sessions\1\BaseNamedObjects\A4B6CE24-E72D679B-BE9A182F-D7CE305A-FB62BB342

\Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208

\Sessions\1\BaseNamedObjects\417087542ENU_FE97A6DDE921C7562535

\Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex

\Sessions\1\BaseNamedObjects\GdiplusFontCacheFileV1

\Sessions\1\BaseNamedObjects\Global\CPFATE_2304_v4.0.30319

\Sessions\1\BaseNamedObjects\Local\c:!users!user!appdata!roaming!microsoft!windows!ietldcache!

\Sessions\1\BaseNamedObjects\Local_!MSFTHISTORY!_LOW!_

\Sessions\1\BaseNamedObjects\Local\c:!users!user!appdata!local!microsoft!windows!temporary internet
files!low!content.ie5!

\Sessions\1\BaseNamedObjects\Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!low!

\Sessions\1\BaseNamedObjects\Local\c:!users!user!appdata!local!microsoft!windows!history!low!history.ie5!

\Sessions\1\BaseNamedObjects\A4B6CE24-E72D679B-BE9A182F-DACC8B0F-7324685F3

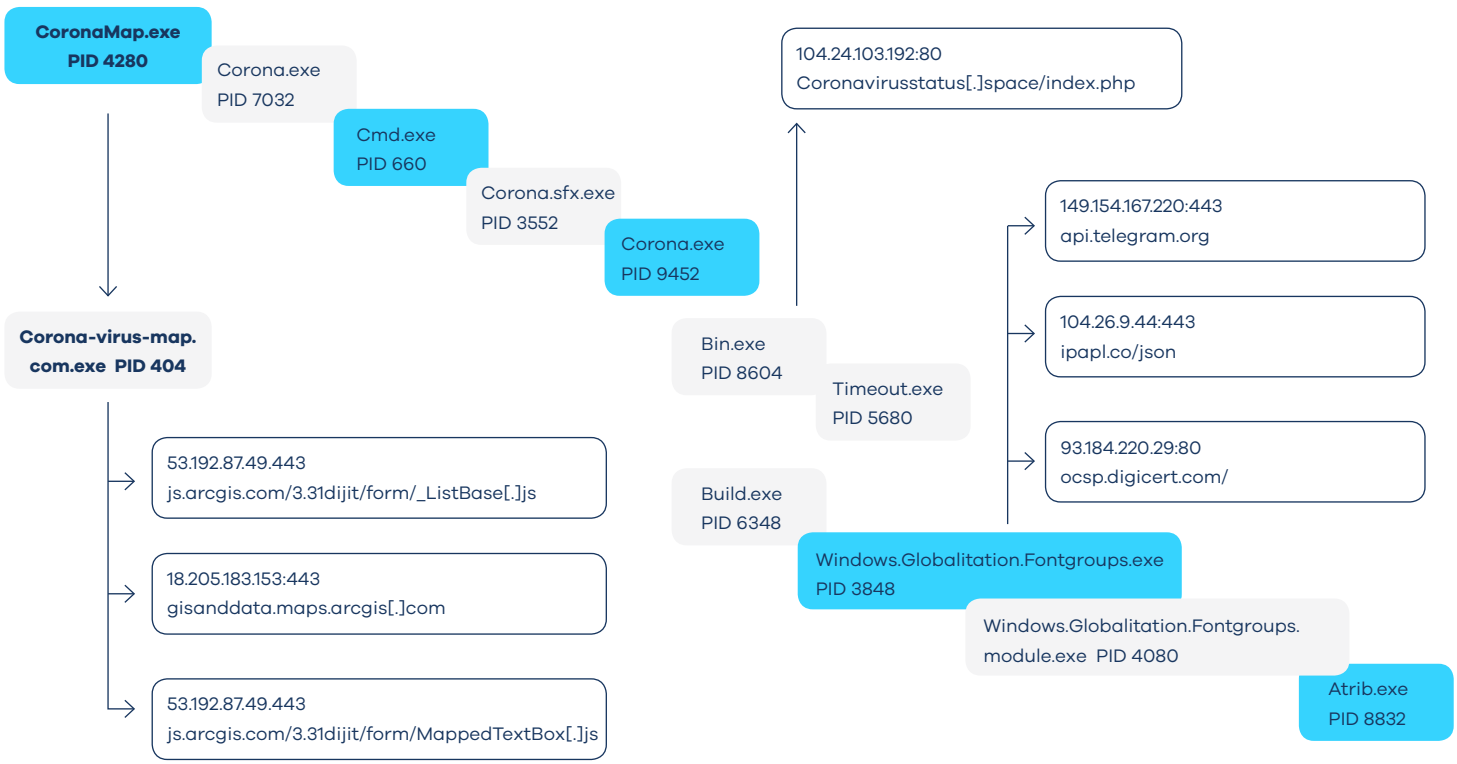
\Sessions\1\BaseNamedObjects\417087542ENU_687FE9797AC054582535

\Sessions\1\BaseNamedObjects\Global\CPFATE_1308_v4.0.30319

Network communication

PROCESS	IP ADDRESS	URL
Bin.exe	104.24.103.192:80	Coronavirusstatus[.]space/index.php
Windows.Globalization. Fontgroups.exe	149.154.167.220:443	api.telegram.org
Windows.Globalization. Fontgroups.exe	104.26.9.44:443	ipapi.co/json
Windows.Globalization. Fontgroups.exe	93.184.220.29:80	ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCG-gUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMI-JHWMys%2BghUNoZ7OrUETfACEA%2Fz5hY5qj0aEmX-0H4s05bY%3D
Corona-virus-Map.com.exe	18.205.183.153:443	gisanddata.maps.arcgis[.]
Corona-virus-Map.com.exe	54.192.87.49:443	https://js.arcgis.com/3.31/dijit/form/_ListBase[.]js
Corona-virus-Map.com.exe	54.192.87.49:443	https://js.arcgis.com/3.31/dijit/form/MappedTextBox[.]js

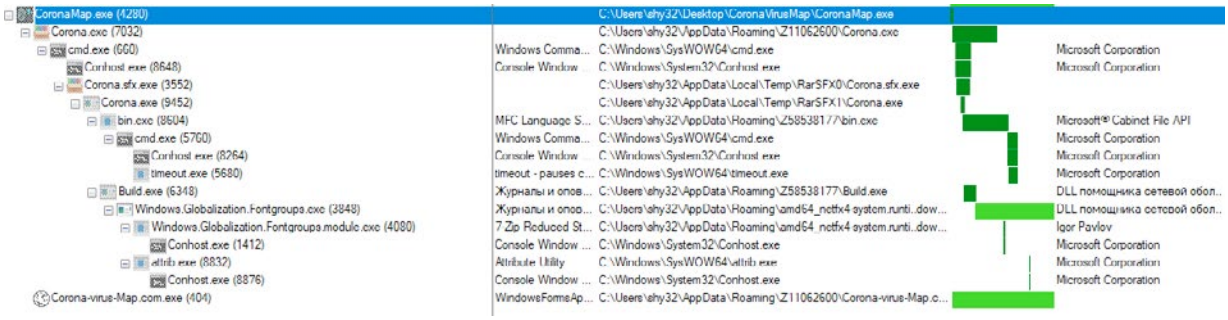
Execution Flow Summary



Full analysis

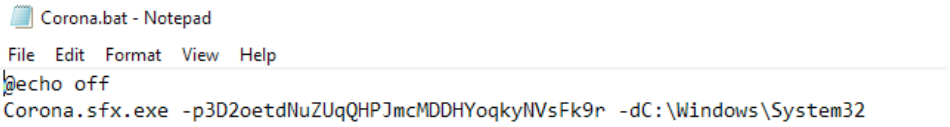
After receiving the sample, I started first with a dynamic analysis, executed the file “CoronaMap.exe”[PID 4280] and opened up a window that showed the following “CoronaVirus” statistics:

Running procmon at the same time revealed a multi-sub process that was created by “CoronaMap.exe”[PID 4280] which is the root process.



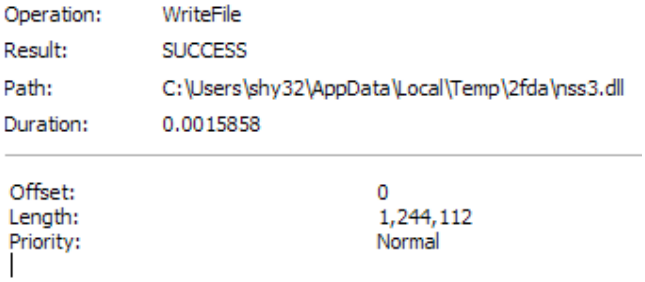
“CoronaMap.exe”[PID 4280] starts by creating another binary called “Corona.exe”[PID 7032]. When analyzing this file, it was easy to see that it was an archive, which means that it probably contains execution commands that can execute it.

Simply by using Winrar to view the archive content, I found two files inside it and they were in self-extracted mode (SFX). The two files were “Corona.bat” and “Corona.sfx.exe”, which we can also see in the process tree in procmon. Upon opening the “Corona.bat” file, we could see that “Corona.sfx.exe” was extracted with a hard coded password (3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r) to the “C:\windows\system32” directory:

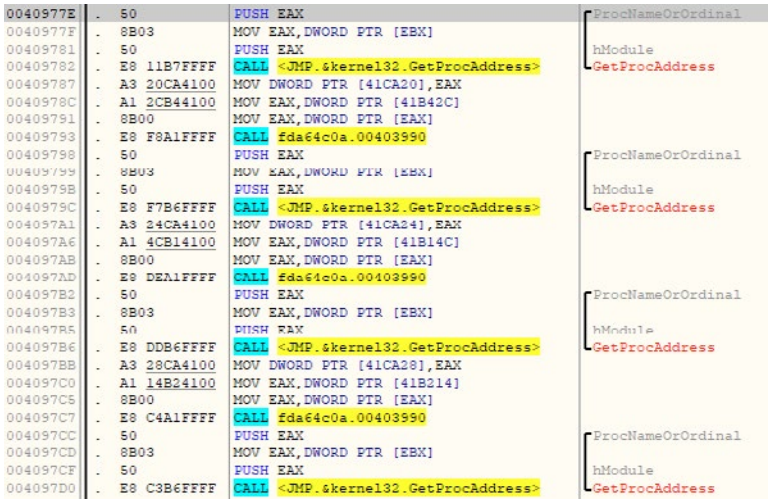


The “Corona.sfx.exe”[PID 3552] is an extracting process called “Corona.exe”[PID 9452]. This process creates more processes, but we will be focusing on only three of them: “bin.exe”[PID 8604], “timeout.exe”[PID 5680] And “Build.exe”[PID 6348]

As I started to analyze the“bin.exe”[PID 8604] with Ollydbg, I was able to see that it was writing some Dll’s, one of which was known to me from different actors: the “nss3.dll” :



Going deeper inside with Ollydbg, I saw static loading of APIs related to “nss3.dll”. The code utilized the API functions within the “nss3.dll” to decrypt saved passwords and create output data.



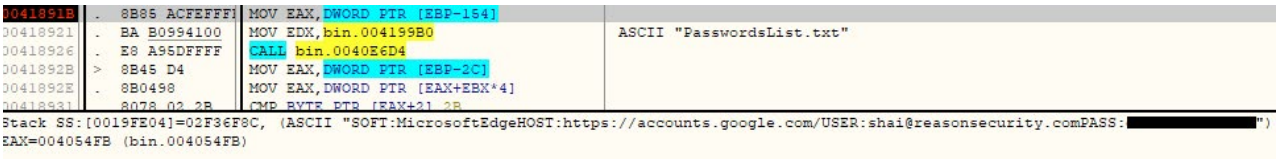
This technique is pretty common. I came across it once before, and after doing some digging around, discovered that this information-stealing tactic came from a malware family called "AZORult", which was first seen in the wild in 2016. Its behavior is as follows: When the victim gets infected, the malware extracts data and creates a unique ID of the victim's workstation. It then applies XOR encryption using the generated ID. This ID is used to tag the workstation in order to start the C2 communication. The C2 server responds with configuration data, which contains target web browser names, web browser path information, API names, sqlite3 queries, and legitimate DLLs.

Using Ollydbg and keeping a trace on the API calls from the loaded "nss3.dll", I was able to see the following calls:

- Sqlite3_open
- Sqlite3_close
- Sqlite3_prepare_v2
- Sqlite3_step
- sqlite3_column_text
- Sqlite3_column_bytes
- Sqlite3_finalize
- NSS_Init
- PK11_GetInternalKeySlot
- PK11_Authenticate
- PK11SDR_Decrypt
- NSS_Shutdown
- PK11_FreeSlot

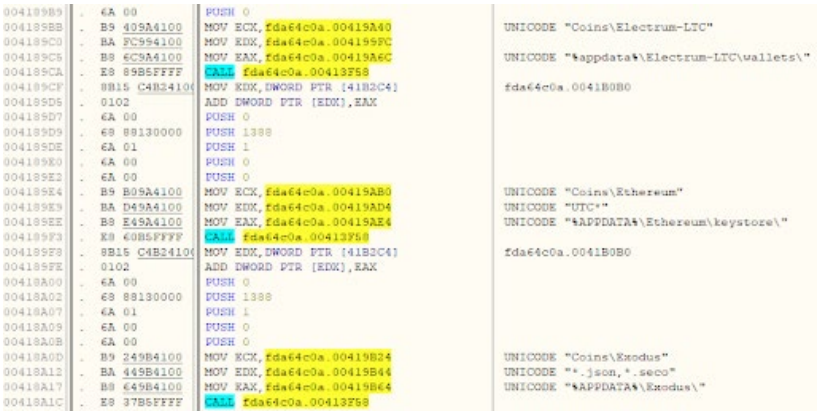
The password stealing operation process is simple because the malware steals the "login data" from the installed browser and moves it to "C:\Windows\Temp". The "login data" is based on Sqlite3 DB structure.

To read the date the malware queries the SQLite data in order to extract the information. Once the extraction is over, the malware creates a file called “PasswordList.txt”, which holds all the information.



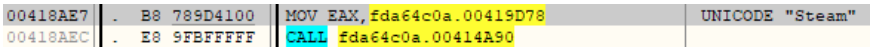
SOFT: MicrosoftEdge
HOST: https://accounts.google.com/
USER: shai@reasonsecurity.com
PASS: [redacted]

As I kept on digging in the code of “bin.exe”[PID 8604], I could see that the malware is also looking for different cryptocurrency wallets such as “Electrum” and “Ethereum”:



Also looking for “Telegram Desktop”:

Searches for “Steam” account:



Takes a screenshot and saves it as “scr.jpg”:

```
00418B09  .  50              PUSH EAX
00418B0A  .  6A 01           PUSH 1                                  [Index = SM_CYSCREEN
00418B0C  .  E8 1FC4FEFF     CALL <JMP.&user32.GetSystemMetrics>     [GetSystemMetrics
00418B11  .  50              PUSH EAX
00418B12  .  6A 00           PUSH 0                                  [Index = SM_CXSCREEN
00418B14  .  E8 17C4FEFF     CALL <JMP.&user32.GetSystemMetrics>     [GetSystemMetrics
00418B19  .  33C9            XOR ECX,ECX
00418B1B  .  5A              POP EDX
00418B1C  .  E8 8FE4FFFF     CALL fda64c0a.00416FB0
00418B21  .  BA A49D4100     MOV EDX,fda64c0a.00419DA4               ASCII "scr.jpg"
```

Resolve the public IP address of the victim machine and save it as “ip.txt”:

```
00418F33  .  B9 2C9E4100     MOV ECX,fda64c0a.00419E2C               ASCII "GET"
00418F38  .  33D2            XOR EDX,EDX
00418F3A  .  B8 389E4100     MOV EAX,fda64c0a.00419E38               ASCII "http://ip-api.com/json"
00418F3F  .  E8 40EEFFFF     CALL fda64c0a.00417D84
```

```
00418F8B  .  8B85 40FEFFFF   MOV EAX,DWORD PTR [EBP-1C0]
00418F91  .  BA 9C9E4100     MOV EDX,fda64c0a.00419E9C               ASCII "ip.txt"
00418F96  .  E8 3957FFFF     CALL fda64c0a.0040E6D4
00418F9B  .v EB 10           JMP SHORT fda64c0a.00418FAD
```

Collecting information about the system such as the OS system, the architecture,the host name,the username, etc:

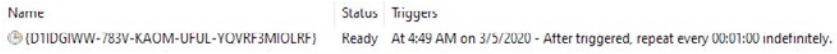
```
00418FE4  .  BA AC9E4100     MOV EDX,fda64c0a.00419EAC               ASCII "System.txt"
00418FE9  .  E8 E656FFFF     CALL fda64c0a.0040E6D4
00418FEE  .  8D85 30FEFFFF   LEA EAX,DWORD PTR [EBP-1D0]
00418FF4     E8 EFDCFEFF     CALL fda64c0a.00406CE8
00418FF9  .  8B85 30FEFFFF   MOV EAX,DWORD PTR [EBP-1D0]
00418FFF  .  8D95 34FEFFFF   LEA EDX,DWORD PTR [EBP-1CC]
00419005  .  E8 2AD8FEFF     CALL fda64c0a.00406834
0041900A  .  FFB5 34FEFFFF   PUSH DWORD PTR [EBP-1CC]
00419010  .  68 C09E4100     PUSH fda64c0a.00419EC0
00419015  .  8D85 28FEFFFF   LEA EAX,DWORD PTR [EBP-1D8]
0041901B  .  E8 E8EAFEFF     CALL fda64c0a.00407B08
00419020  .  0D05 20FEFFFF   MOV EAX,DWORD PTR [EDP 1D0]
00419026  .  8D95 2CFEFFFF   LEA EDX,DWORD PTR [EBP-1D41
0041902C  .  E8 03D8FEFF     CALL fda64c0a.00406834
00419031  .  FFB5 2CFEFFFF   PUSH DWORD PTR [EBP-1D4]
00419037  .  68 C09E4100     PUSH fda64c0a.00419EC0
0041903C  .  8D85 1CFEFFFF   LEA EAX,DWORD PTR [EBP-1E4]
00419042  .  E8 91DBFEFF     CALL fda64c0a.00406BD8
00419047  .  8B95 1CFEFFFF   MOV EDX,DWORD PTR [EBP-1E4]
0041904D  .  8D85 20FEFFFF   LEA EAX,DWORD PTR [EBP-1E0]
00419053  .  E0 24A7FEFF     CALL fda64c0a.0040377C
00419058  .  8B85 20FEFFFF   MOV EAX,DWORD PTR [EBP-1E01
0041905E  .  8D95 24FEFFFF   LEA EDX,DWORD PTR [EBP-1DC]
00419064  .  E8 CBD7FEFF     CALL fda64c0a.00406834
00419069  .  FFB5 24FEFFFF   PUSH DWORD PTR [EBP-1DC]
0041906F     68 C09E4100     PUSH fda64c0a.00419EC0
00419074  .  8D85 10FEFFFF   LEA EAX,DWORD PTR [EBP-1F0]
```

As I continued with “bin.exe”[PID 8604], I found that the malware communicates with it’s C2 server using the address of 104.24.103.192:80, which we can resolve to http://coronavirusstatus[.]space/. By analyzing the traffic, I found that the “bin.exe”[PID 8604] uses “chunked” transfer encoding, which is also something we see in the wild. When the Content-Length value is smaller than the chunked payload size, the origin server will check the Content-Length header to determine the length of the request, but there will be some leftover payload that will be concatenated to the next incoming request. This is how the malware sends out the information it steals:

```
15 9.768803     192.168.61.130     104.24.103.192     HTTP     337 POST /index.php HTTP/1.1

5961 19.902259     192.168.61.130     104.24.103.192     HTTP     9438 POST /index.php HTTP/1.1
```

Moving on to the “timeout.exe”[PID 5680], it was easy to understand that the malware author used it in order to create a delay execution. This is also a pretty common technique that is used to trick AVs. As I started analyzing the “Build.exe”[PID 6348], I could see a “Loadlibrary” of “taskschd.dll”, which I was already familiar with this in case of persistence:

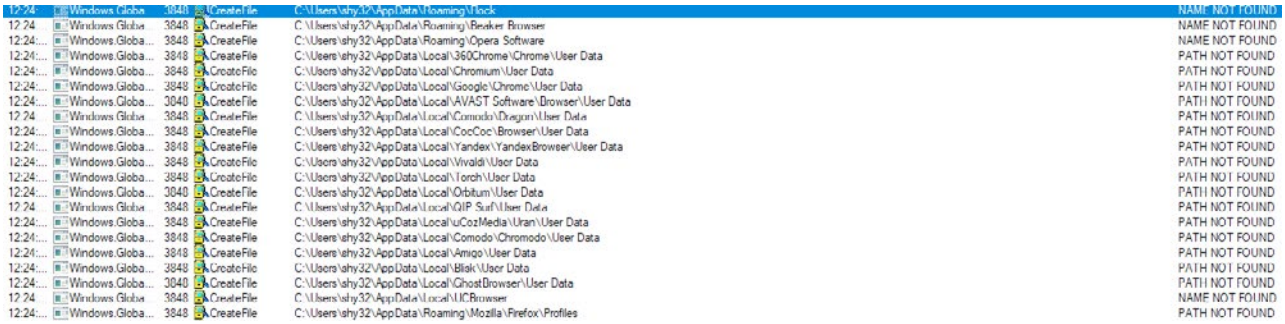


The “Build.exe”[PID 6348] creats a sub process “Windows.Globalization.Fontgroups.exe”[PID 3848] which the persistence runs.

When analyzing the “Windows.Globalization.Fontgroups.exe”[PID 3848], I could see that it was packed with UPX, which is pretty easy to unpack.

Property	Value
File Name	C:\Users\shy32\AppData\Roaming\amd64_netfx4-system.runti..dows...
File Type	Portable Executable 32
File Info	UPX v3.0
File Size	1.34 MB (1409536 bytes)
PE Size	1.34 MB (1409536 bytes)
Created	Monday 02 March 2020, 08.08.29
Modified	Monday 02 March 2020, 08.02.22
Accessed	Thursday 05 March 2020, 05.53.02
MD5	F6A5E02F46D761D3890DEBD8F2084D37
SHA-1	D64FF51020046FB13AEC3ED608BA499295CAF80D

After unpacking, I noticed that there was another layer of packing. This time, it was with AutoIT. Moving forward with the analysis, I found that this binary is responsible for enumerating the OS in order to find new browsers and resources that it can steal information from:



The “Windows.Globalization.Fontgroups.exe”[PID 3848] creates a process called “Windows.Globalization.Fontgroups.module.exe”[PID 3848] which is responsible for creating the zip file with all the information “bin.exe”[PID 8604] sends out: C:\Users\shy32\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_64B5614D0F4B35423983.7z

The “Windows.Globalization.Fontgroups.exe”[PID 3848] uses “Attrib.exe”[PID 8832] in order to hide this directory:

```
Command:    attrib +s +h "C:\Users\shy32\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml"
User:       DESKTOP-TA65K46\shy32
```

Prevention and Remediation

Remediation

Download the Reason Antivirus software.
Doubleclick on the installed executable and follow the prompts to complete the installation.
Once the installation is complete, click 'Finish'.
Definitions and security patches will automatically be updated.
Once the process is complete, select the 'Scan Now' button to start your scan.
When the scan is finished, select all the threats that were detected and then click on 'Remove selected threats'. When prompted, restart your computer.

MetaData

Hashes

- 2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307
- 0b3e7faa3ad28853bb2b2ef188b310a67663a96544076cd71c32ac088f9af74d
- 13c0165703482dd521e1c1185838a6a12ed5e980e7951a130444cf2feed1102e
- Fda64c0ac9be3d10c28035d12ac0f63d85bb0733e78fe634a51474c83d0a0df8
- 126569286f8a4caeeaba372c0bdba93a9b0639beaad9c250b8223f8ecc1e8040
- 203c7e843936469ecf0f5dec989d690b0c770f803e46062ad0a9885a1105a2b8

About Reason Labs

Reason Labs is the threat research arm of Reason Cybersecurity. We play a leading role in researching and exploring cyber threats and advancing the state of cybersecurity intelligence. Reason Labs collects raw data about existing and emerging threats and analyzes that data to deliver actionable insights in real-time.
We leverage the threat intelligence we gather from always-on active sensors, in order to continuously analyze, organize, and add context to evolving cyber activities, attacks and threats. This powerful intelligence network leaves Reason prepared to meet threats head-on.

For more information reach out at shai@reasonsecurity.com

Reason LABS