Robert Gonzalez · Follow
11 min read · Mar 16, 2020

John Hopkins Covid-19 Map

Covid-19 Cyber Infection

or

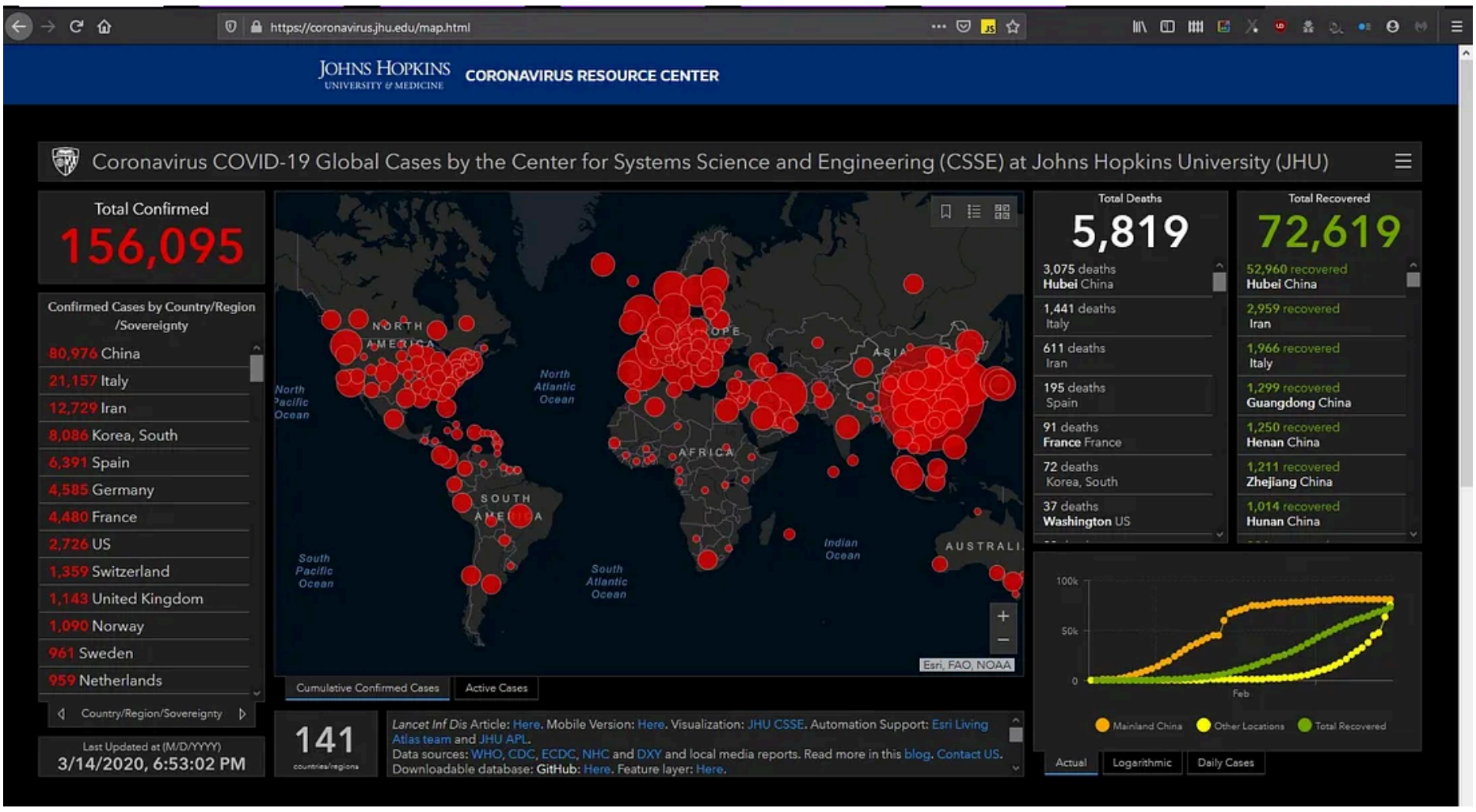
The Illness Dwells Inside You

We loathe to pander to sensationalism by riding on popular topics that everyone is discussing. This may make us less than popular in the realms of SEO or acting like a tabloid organization but as a company we attempt to always go where those of us are afraid to or publicize that which many people do not hear about. The amount of traffic that is nefarious that goes on in cybersecurity is voluminous, but it does take a bit for it to come to the surface. However, this one I could not resist simply because of the absurdity of it. However, currently when panic buying is going on and bathroom tissue is a premium, who am I to judge. Regardless of such, we should never download things without complete certainty of where they are coming from, even if it looks like a pretty map that is the wrapping for something, we are familiar with. Humble folk I give you — the Corona Virus — Covid-19 map.

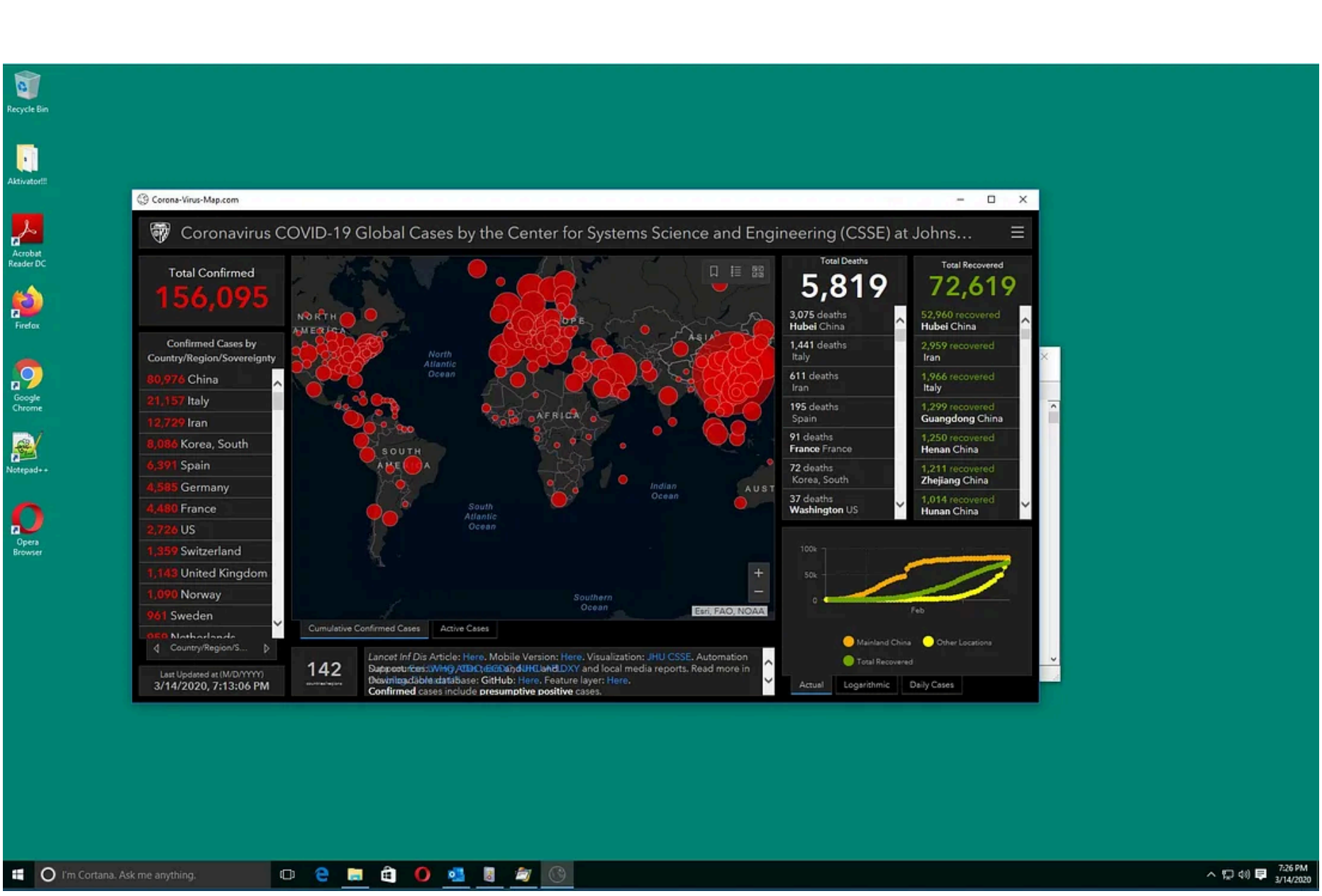
John Hopkins University of Medicine has a live Covid-19 map that can be found at https://coronavirus.jhu.edu/map.html. The binary in question is not that map but bears some similarities so if one is uninformed, they can get fooled, the delivery method from what we have witnessed has been both via email and website download.

Part One -
Cartography of the Wicked

The John Hopkins Covid-19 map looks like the below:



The rogue map looks like the below:



As you can see there are similarities except for obvious discrepancies. What is more important is what is happening underneath. Now before I continue let me preface this by saying that if you are running the most current version of windows, have Malwarebytes on top, Defender activated, and SmartScreen you should be fine and will be warned about this map as its blacklisted already. We ran it on Windows Enterprise on a fully updated system and Defender immediately detects this as malware and Malwarebytes has blacklisted it. Oddly though as of the writing of this article the server is still active.

. . .

Part Two:

The first occurrence is the launch/creation of the process. As the logs are our friend, we are alerted to new process being created, Syson makes creating alerts easier.

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:52.820

ProcessGuid: {80D90D24–6788–5E6D-0000–001050440307}

ProcessId: 1104

Image: C:\Users\bishop.PROJECTFARSCAPE\Downloads\Corona-virus-Map.com.exe

FileVersion: ?

Description: ?

Product: ?

Company: ?

OriginalFileName: ?

CommandLine: “C:\Users\bishop.PROJECTFARSCAPE\Downloads\Corona-virus-Map.com.exe”

CurrentDirectory: C:\Users\bishop.PROJECTFARSCAPE\Downloads\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=949B69BF87515AD8945CE9A79F68F8B788C0AE39

ParentProcessGuid: {80D90D24–81F5–5E69–0000–0010A11F0300}

ParentProcessId: 576

ParentImage: C:\Windows\explorer.exe

ParentCommandLine: C:\Windows\Explorer.EXE

There is nothing of incredible significance here except for the process being created, but we need to look for these things and be alerted to them otherwise you cannot stop what has happened nor explain the genesis of a malady, that way it does not happen again.

. . .

Part Three:

The map has spawned a process, this would indicate our patient zero.

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:53.336

ProcessGuid: {80D90D24–6789–5E6D-0000–001058560307}

ProcessId: 7008

Image: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z11062600\Corona.

exe

FileVersion: ?

Description: ?

Product: ?

Company: ?

OriginalFileName: ?

CommandLine:
“C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z11062600\Corona
.exe”

CurrentDirectory:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z11062600\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=6878E9825FAD4696E48ACA151E656A4581E3DC16

ParentProcessGuid: {80D90D24–6788–5E6D-0000–001050440307}

ParentProcessId: 1104

ParentImage: C:\Users\bishop.PROJECTFARSCAPE\Downloads\Corona-virus-Map.com.exe

ParentCommandLine:
“C:\Users\bishop.PROJECTFARSCAPE\Downloads\Corona-virus-Map.com.exe”

Note that as with most malware the child process created is another executable. Mind you this is going on while the user is looking at the map.

. . .

Part Four:

The child process goes straight to work by launching a headless cmd process. This means that a command shell is launched without a graphical interface, unbeknownst to the user while he/she is looking at infection rates of Covid-19.

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:53.765

ProcessGuid: {80D90D24–6789–5E6D-0000–0010B26B0307}

ProcessId: 4536

Image: C:\Windows\SysWOW64\cmd.exe

FileVersion: 10.0.10586.0 (th2_release.151029–1700)

Description: Windows Command Processor

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: Cmd.Exe

CommandLine: C:\Windows\system32\cmd.exe /c “”C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX0\Corona.bat” “

CurrentDirectory: C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX0

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=8948CBF2B798684CA93D2CB844B2254C382B0AB8

ParentProcessGuid: {80D90D24–6789–5E6D-0000–001058560307}

ParentProcessId: 7008

ParentImage: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z11062600\Corona.exe

ParentCommandLine: “C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z11062600\Corona.exe”

The command shell is running a batch file by the name Corona.bat. If you restrict permissions in your user’s home directory where the user cannot run a batch file even under the worse of circumstances that should help you. The user directory is a place where only known apps should be allowed to run and for your users this should be a set of apps that is known to you. If you are set to receive alerts when these things go on in your user’s home directory, then you will be able to catch this. Applocker and Windows Defender Application Control are your friends.

. . .

Part Five:

The next issue that shows up is something a lot of people ignore. I disagree with this, as it is important even out of the context of the malware. That batch process that the headless cmd.exe ran has spawned a new process.

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:53.805

ProcessGuid: {80D90D24–6789–5E6D-0000–00102D6E0307}

ProcessId: 6244

Image: C:\Windows\System32\conhost.exe

FileVersion: 10.0.10586.0 (th2_release.151029–1700)

Description: Console Window Host

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: CONHOST.EXE

CommandLine: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

CurrentDirectory: C:\Windows

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=F8204EE42D6AFD9A1B0A09F858C588387C07B22F

ParentProcessGuid: {80D90D24–6789–5E6D-0000–0010B26B0307}

ParentProcessId: 4536

ParentImage: C:\Windows\SysWOW64\cmd.exe

ParentCommandLine: C:\Windows\system32\cmd.exe /c “”C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX0\Corona.bat” “

The command line conhost.exe 0xffffffff -ForceV1 is significant, ForceV1 asks for information directly from the kernel space, conhost connects to the console application. It is important to look for these things. As they are flashing by the security operator’s screen it may look like nothing, but when you see it, you need to ask yourself, what spawned that and why? An alert for this will always keep you informed of something that is not right.

. . .

Part Six:

We then see the batch file create a new process. Notice the naming convention is similar as it adheres to the “Corona” theme.

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:53.983

ProcessGuid: {80D90D24–6789–5E6D-0000–001018760307}

ProcessId: 6636

Image:
C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX0\Corona.sfx.exe

FileVersion: ?

Description: ?

Product: ?

Company: ?

OriginalFileName: ?

CommandLine: Corona.sfx.exe -p3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r -dC:\Windows\System32

CurrentDirectory: C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX0\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=401431F0781B416F3E237E993B1A283B3A37613E

ParentProcessGuid: {80D90D24–6789–5E6D-0000–0010B26B0307}

ParentProcessId: 4536

ParentImage: C:\Windows\SysWOW64\cmd.exe

ParentCommandLine: C:\Windows\system32\cmd.exe /c “”C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX0\Corona.bat” “

The tail of the executable in the command line that is spawned by that batch file is -p3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r -d. I am unclear as to what it does but there are registry changes going on with write permissions. The key being affected specifically is

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

We then see the batch file which is in RarSFX0 create a new file in RarSFX1

. . .

Part Seven:

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:54.624

ProcessGuid: {80D90D24–678A-5E6D-0000–0010578C0307}

ProcessId: 5248

Image: C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX1\Corona.exe

FileVersion: ?

Description: ?

Product: ?

Company: ?

OriginalFileName: ?

CommandLine:
“C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX1\Corona.exe”

CurrentDirectory: C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX1\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=B11EA20D95AAEA2FDE9BEE0D7AC5EAC0B81A839C

ParentProcessGuid: {80D90D24–6789–5E6D-0000–001018760307}

ParentProcessId: 6636

ParentImage:
C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX0\Corona.sfx.exe

ParentCommandLine: Corona.sfx.exe -
p3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r -dC:\Windows\System32

This is the second time we see a Corona.exe executable spawned. What occurs next is when the malady truly begins its work. As with most malware, multiple processes are spawned, and each process has its own task. Keep in mind always when looking at your logs that while malware is nefarious, it is still software, which uses the operating system resources to achieve its end goal.

. . .

Part Eight:

A new process called **bin.exe** has come forth.

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:55.042

ProcessGuid: {80D90D24–678B-5E6D-0000–00101EA40307}

ProcessId: 4116

Image:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\bin.exe

FileVersion: 5.7.2.8

Description: MFC Language Specific Resources

Product:

Company: Microsoft® Cabinet File API

OriginalFileName: ?

CommandLine:
“C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\bin.exe”

CurrentDirectory:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=4C8A7C3DABF12748201C496525A37EC65577CBBB

ParentProcessGuid: {80D90D24–678A-5E6D-0000–0010578C0307}

ParentProcessId: 5248

ParentImage:
C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX1\Corona.exe

ParentCommandLine:
“C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX1\Corona.exe”

Notice that the process created is a file with a Microsoft description.

This process does something no process should do. Process 4116 is bin.exe.
A connection is made to a command and control server.

Network connection detected:

RuleName:

UtcTime: 2020–03–14 23:23:08.438

ProcessGuid: {80D90D24–6752–5E6D-0000–0010CFA80007}

ProcessId: 4116

Image: C:\Windows\System32\dllhost.exe

User: NT AUTHORITY\SYSTEM

Protocol: tcp

Initiated: true

SourceIsIpv6: false

SourceIp: 192.168.50.51

SourceHostname: asylum.projectfarscape.net

SourcePort: 58366

SourcePortName:

DestinationIsIpv6: false

DestinationIp: 104.24.103.192

DestinationHostname:

DestinationPort: 80

DestinationPortName: http

An http connection is made to the highlighted address. That address resolves to the following:

Non-authoritative answer:

Name: coronavirusstatus.space

Address: 104.24.103.192

Name: coronavirusstatus.space

Address: 104.24.102.192

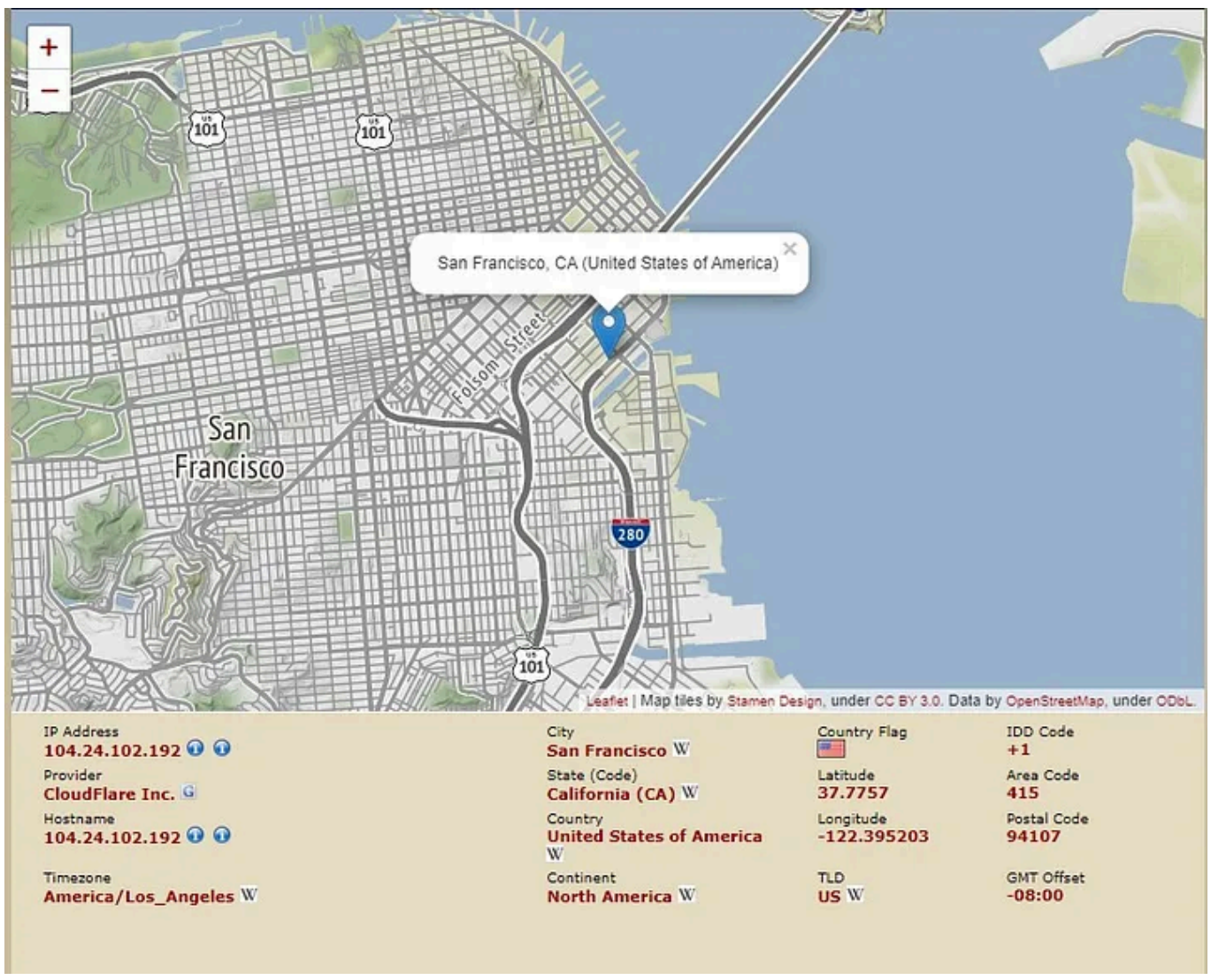
Name: coronavirusstatus.space

Address: 2606:4700:3031::6818:66c0

Name: coronavirusstatus.space

Address: 2606:4700:3030::6818:67c0

This is Cloudflare -



If your going to host a covid-19 map that has malware on it do it on good cloud provider. We are going to return to this as initial research gives us an idea of who this is but, in the meanwhile, lets follow that psychotic horse to that burning stable.

. . .

Part Nine:

As mentioned previously the process is doing a lot and not only is it making connections to external entities but it is exhibiting odd behavior, bin.exe as process ID 4116 goes on a registry tour. The number of queries is voluminous but the below stand out –

4116	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	SUCCESS
4116	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	SUCCESS
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE	NAME COLLISIC
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE	SUCCESS
4116	QueryBasicInfor...	C:\Users\bishop.PROJECTFARSCAPE	SUCCESS
4116	CloseFile	C:\Users\bishop.PROJECTFARSCAPE	SUCCESS
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local	NAME COLLISIC
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local	SUCCESS
4116	QueryBasicInfor...	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local	SUCCESS
4116	CloseFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local	SUCCESS
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache	NAME COLLISIC
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache	SUCCESS
4116	QueryBasicInfor...	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache	SUCCESS
4116	CloseFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache	SUCCESS
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows	SUCCESS
4116	QueryBasicInfor...	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows	SUCCESS
4116	CloseFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows	SUCCESS
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	SUCCESS
4116	QueryBasicInfor...	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	SUCCESS
4116	CloseFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	SUCCESS
4116	CreateFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache\IE	SUCCESS
4116	QueryBasicInfor...	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache\IE	SUCCESS
4116	CloseFile	C:\Users\bishop.PROJECTFARSCAPE\AppData\Local\Microsoft\Windows\INetCache\IE	SUCCESS
4116	RegQueryKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	SUCCESS
4116	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	SUCCESS
4116	RegQueryKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	SUCCESS
4116	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix	SUCCESS
4116	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CacheLimit	SUCCESS
4116	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	SUCCESS
4116	RegQueryKey	HKLM	SUCCESS
4116	RegQueryKey	HKLM	SUCCESS
4116	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions	SUCCESS
4116	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions	SUCCESS
4116	RegQueryKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions	SUCCESS
4116	RegOpenKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{2B0F765D-C0E9-4171-908E-08A611B84FF6}	SUCCESS
4116	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions	SUCCESS
4116	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{2B0F765D-C0E9-4171-908E-08A611B84FF6}\Category	SUCCESS
4116	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{2B0F765D-C0E9-4171-908E-08A611B84FF6}\Name	SUCCESS
4116	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{2B0F765D-C0E9-4171-908E-08A611B84FF6}\ParentFolder	SUCCESS

Its reading the cache, which also means it is looking at the stored cookies. This means this is an information stealer because whatever it reads its going to send to its command and control server which it has already made a connection to using the above process ID. For the most parts we do not alert for registry querying, however I am certain that there are certain scenarios where we would, those scenarios are not under our privy though. We focus on the process because if you can't catch a process making an unauthorized call to an external entity then pretty much your lost. Terminate the disease before it spreads is what we believe. Still the registry queries and the handles being attached to are fascinating.

This in conjunction with the characteristics of the command and control server are Azorult. A well-known information stealer that is constantly getting upgraded.

. . .

Part Ten:

While all the above is going on the previously spawned Corona.exe with a Process ID of 5248 is not done causing havoc. It has created a new process, observe:

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:55.325

ProcessGuid: {80D90D24–678B-5E6D-0000–001061B00307}

ProcessId: 5148

Image: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\Build.exe

FileVersion: 4.8.9.9

Description: Журналы и оповещения производительности

Product: ?

Company: DLL помощника сетевой оболочки для winHttp

OriginalFileName: DisplaySwitch.exe

CommandLine: “C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\Build.exe”

CurrentDirectory: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=D64FF51020046FB13AEC3ED608BA499295CAF80D

ParentProcessGuid: {80D90D24–678A-5E6D-0000–0010578C0307}

ParentProcessId: 5248

ParentImage:
C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX1\Corona.exe

ParentCommandLine:
“C:\Users\BISHOP~1.PRO\AppData\Local\Temp\RarSFX1\Corona.exe”

A process called Build.exe has been spawned, the frightening fields here are obvious. The OriginalFileName is listed as DisplaySwitch.exe. Furthermore, the description is Cyrillic. In Windows 7 there exists a DisplaySwitch.exe for use for the monitor. The description here translates to

Performance Logs and Alerts. The translation in the company field says

Network Shell Helper DLL for winHttp.

. . .

Part Eleven:

The next process is spawned as a result of Build.exe.

Process Create:

RuleName:

UtcTime: 2020–03–14 23:23:56.191

ProcessGuid: {80D90D24–678C-5E6D-0000–0010D5C50307}

ProcessId: 6268

Image:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.exe

FileVersion: 4.8.9.9

Description: Журналы и оповещения производительности

Product: ?

Company: DLL помощника сетевой оболочки для winHttp

OriginalFileName: DisplaySwitch.exe

CommandLine:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.exe

CurrentDirectory:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=D64FF51020046FB13AEC3ED608BA499295CAF80D

ParentProcessGuid: {80D90D24–678B-5E6D-0000–001061B00307}

ParentProcessId: 5148

ParentImage:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\Build.exe

ParentCommandLine:
“C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\Z58538177\Build.exe”

This process is the fontmapping API which is unremarkable (save for the fact that no foreign process should be calling it and the description is very wrong). What is not unremarkable is this API communicating with an external entity.

Network connection detected:

RuleName:

UtcTime: 2020–03–14 23:23:10.013

ProcessGuid: {80D90D24–678C-5E6D-0000–0010D5C50307}

ProcessId: 6268

Image: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.exe

User: PROJECTFARSCAPE\bishop

Protocol: tcp

Initiated: true

SourceIsIpv6: false

SourceIp: 192.168.50.51

SourceHostname: asylum.projectfarscape.net

SourcePort: 58371

SourcePortName:

DestinationIsIpv6: false

DestinationIp: 104.26.9.44

DestinationHostname:

DestinationPort: 443

DestinationPortName: https

That is the command and control server being hosted on Cloudflare.

Here is another one that goes to Verizon

Network connection detected:

RuleName:

UtcTime: 2020–03–14 23:23:10.196

ProcessGuid: {80D90D24–678C-5E6D-0000–0010D5C50307}

ProcessId: 6268

Image: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.exe

User: PROJECTFARSCAPE\bishop

Protocol: tcp

Initiated: true

SourceIsIpv6: false

SourceIp: 192.168.50.51

SourceHostname: asylum.projectfarscape.net

SourcePort: 58372

SourcePortName:

DestinationIsIpv6: false

DestinationIp: 72.21.91.29

DestinationHostname:

DestinationPort: 80

DestinationPortName: http

The next one is one my favorites –

Network connection detected:

RuleName:

UtcTime: 2020–03–14 23:23:11.223

ProcessGuid: {80D90D24–678C-5E6D-0000–0010D5C50307}

ProcessId: 6268

Image: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.exe

User: PROJECTFARSCAPE\bishop

Protocol: tcp

Initiated: true

SourceIsIpv6: false

SourceIp: 192.168.50.51

SourceHostname: asylum.projectfarscape.net

SourcePort: 58373

SourcePortName:

DestinationIsIpv6: false

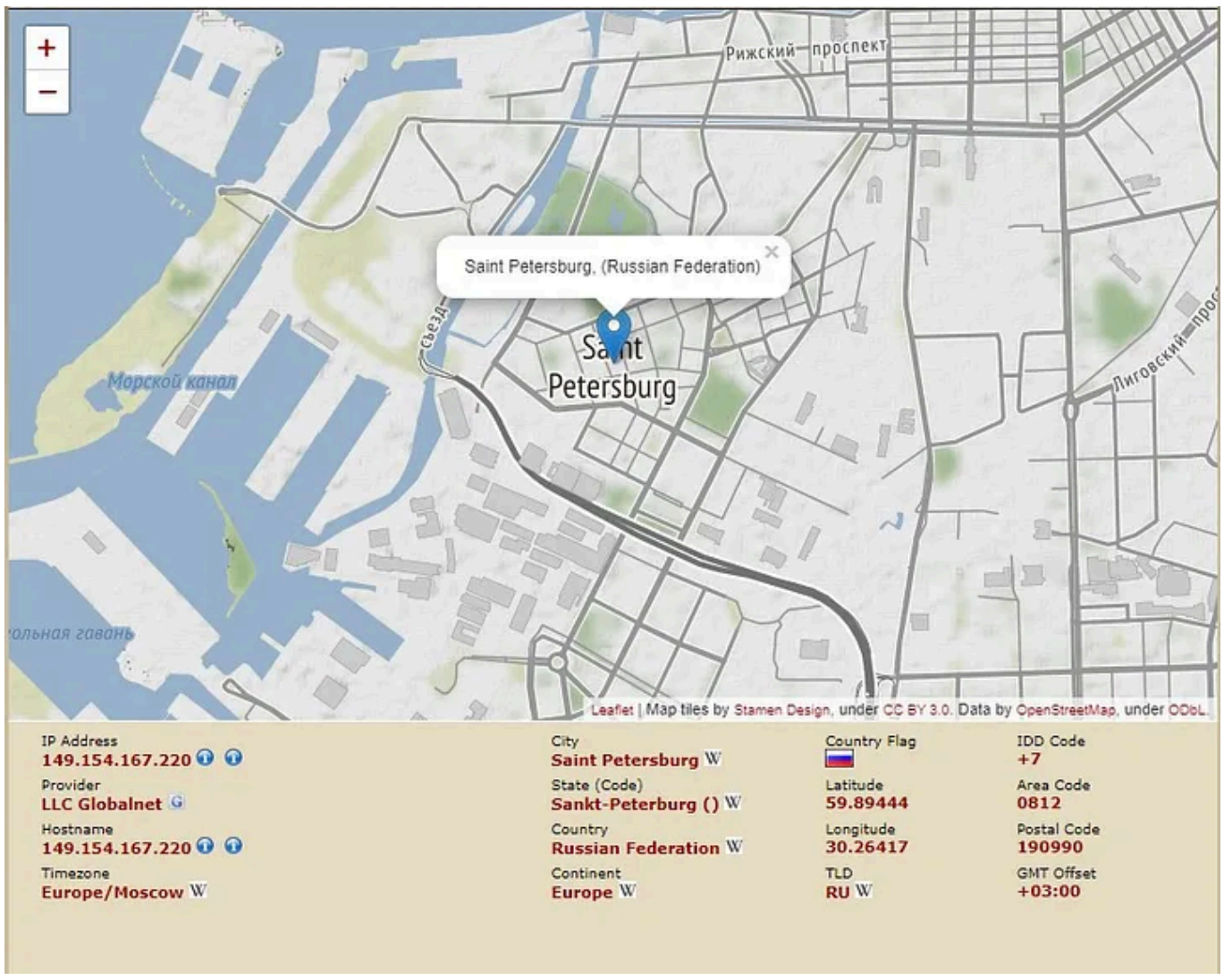
DestinationIp: 149.154.167.220

DestinationHostname:

DestinationPort: 443

DestinationPortName: https

Welcome to St. Petersburg -



. . .

Part Twelve:

There are quite a few connections made but you understand the point. Another process comes after this and it is created by the rogue fontmapping API –

Process Create:

RuleName:

UtcTime: 2020–03–14 23:24:00.845

ProcessGuid: {80D90D24–6790–5E6D-0000–0010271C0407}

ProcessId: 940

Image: C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.module.exe

FileVersion: 16.04

Description: 7-Zip Reduced Standalone Console

Product: 7-Zip

Company: Igor Pavlov

OriginalFileName: 7zr.exe

CommandLine:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.module.exe a -y -mx9 -ssw
“C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\ENU_6801FE97D5C9310F8392.7z”
“C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\1*”

CurrentDirectory:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24–81F4–5E69–0000–002008F70200}

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=668661955BF3C20B9DC8CDAA7EC6E8DBBBD63285

ParentProcessGuid: {80D90D24–678C-5E6D-0000–0010D5C50307}

ParentProcessId: 6268

ParentImage:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.exe

ParentCommandLine:
C:\Users\bishop.PROJECTFARSCAPE\AppData\Roaming\amd64_netfx4-system.runti..dowsruntime.ui.xaml\Windows.Globalization.Fontgroups.exe

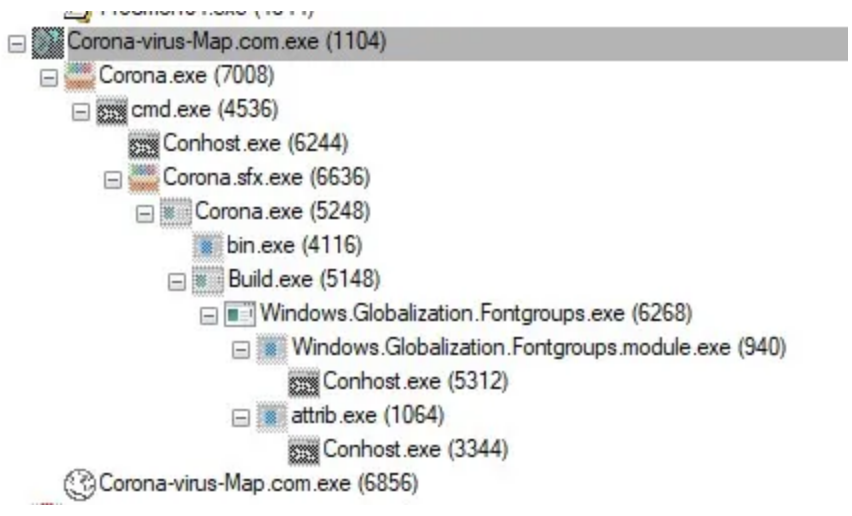
Here we see again another process being created where the original file names are revealed to us. In this case we see it’s the 7-Zip Reduced

Standalone Console. Following this we see attrib.exe used to modify amd64_netfx4-system.runti..dowsruntime.ui.xaml. All in all — a very busy map.

Conclusion:

A process is the command that sets the course of action, and by monitoring processes we are able to stop that which can hurt us. This map specifically is interesting because not only do we the processes the map engages but we see so much going on beneath.

Observe the process tree below:



As mentioned earlier the command and control server is still online. The information gathered from the domain hints at the origin of this malware.

A) Trackers

B) DNS

Value	First	Last	Type
dns.cloudflare.com	2020-03-15	2020-03-15	SOA
2606:4700:3031::6818:66c0	2020-02-01	2020-03-15	AAAA
2606:4700:3030::6818:67c0	2020-02-01	2020-03-15	AAAA
dns@cloudflare.com	2020-02-01	2020-03-15	SOA
coby.ns.cloudflare.com	2020-02-01	2020-03-15	NS
tara.ns.cloudflare.com	2020-02-01	2020-03-15	NS
coby.ns.cloudflare.com.	2020-02-01	2020-03-15	SOA
ns1.reg.ru	2020-02-01	2020-02-01	NS
ns2.reg.ru	2020-02-01	2020-02-01	NS

Note the last two — ns1.reg.ru and ns2.reg.ru

C) Server components

Hostname	First	Last	Category	Value
coronavirusstatus.space	2020-02-01	2020-03-13	Server	CloudFlare
coronavirusstatus.space	2020-02-01	2020-03-13	DDOS Protection	CloudFlare
coronavirusstatus.space	2020-02-01	2020-03-13	CDN	CloudFlare
coronavirusstatus.space	2020-03-12	2020-03-13	JavaScript Library	zepto (v1.1.4)
coronavirusstatus.space	2020-03-04	2020-03-12	Framework	PHP (v7.0.26)
coronavirusstatus.space	2020-03-04	2020-03-04	Server	cloudflare
coronavirusstatus.space	2020-02-01	2020-02-01	Analytics Service	Yandex Metrika

Again, we see the Yandex Analytic service

D) Host Pairs

Parent Hostname	Child Hostname	First	Last	Cause
coronavirusstatus.space	coronavirusstatus.space	2020-02-01	2020-02-01	parentPage
coronavirusstatus.space	mc.yandex.ru	2020-02-01	2020-02-01	parentPage

Child, hostname mc.yandex.ru

I will let you conclude the obvious.

Cybersecurity Cybercrime Malware Analysis Malware Virus

--

Written by Robert Gonzalez

51 Followers

https://www.cybercrypto.net

Follow