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

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

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

. . .

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:

Company: ?

OriginalFileName: ?

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

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

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.

. . .

FileVersion: ?

Description: ?

Product: ?

Company: ?

OriginalFileName: ?

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”

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)

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=8948CBF2B798684CA93D2CB844B2254C382B0AB8

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

. . .

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:

OriginalFileName: CONHOST.EXE

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

CurrentDirectory: C:\Windows

User: PROJECTFARSCAPE\bishop

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

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.

. . .

FileVersion: ?

Description: ?

Product: ?

Company: ?

OriginalFileName: ?

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” “

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: ?

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Hashes: SHA1=B11EA20D95AAEA2FDE9BEE0D7AC5EAC0B81A839C

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

Part Eight:

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

Process Create:

RuleName:

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

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

User: PROJECTFARSCAPE\bishop

LogonGuid: {80D90D24-81E4-5E60-0000-002008E70200}

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:

SourceHostname: asylum.projectfarscape.net

SourcePort: 58366

SourcePortName:

DestinationIsIpv6: false

DestinationIp: 104.24.103.192

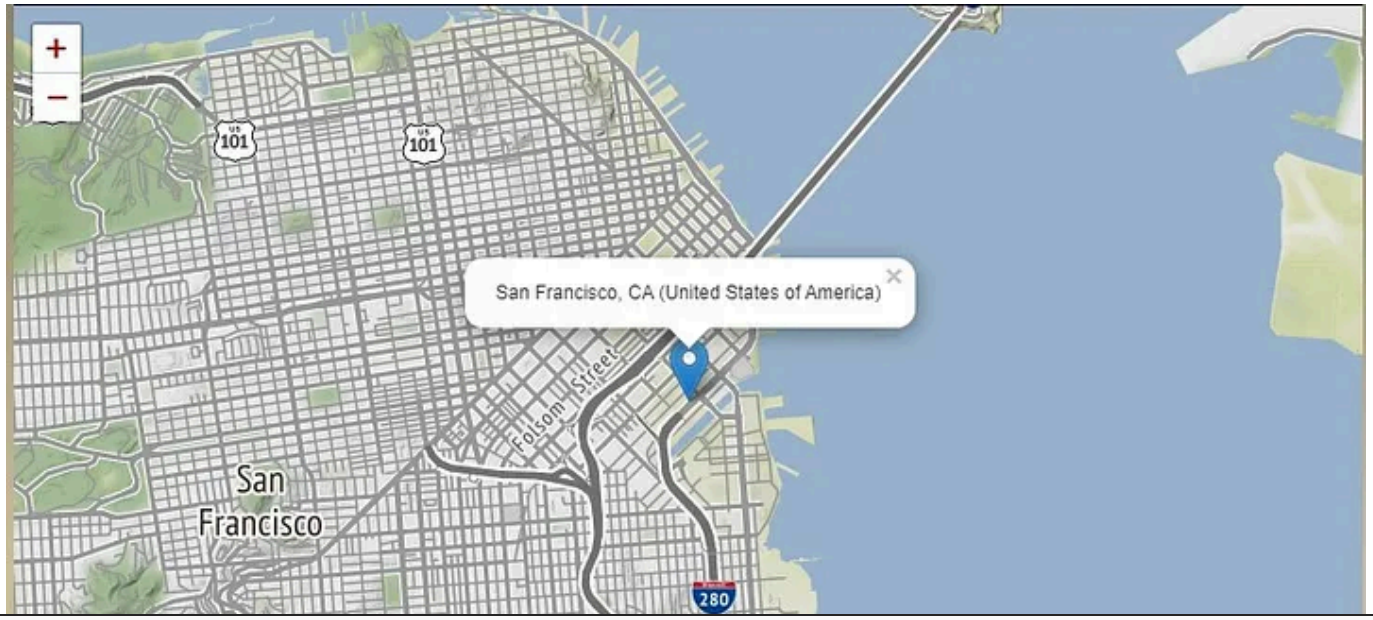
Address: 104.24.102.192

Name: coronavirusstatus.space

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

Name: coronavirusstatus.space

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



Medium

Sign up to discover human stories that deepen your understanding of the world.

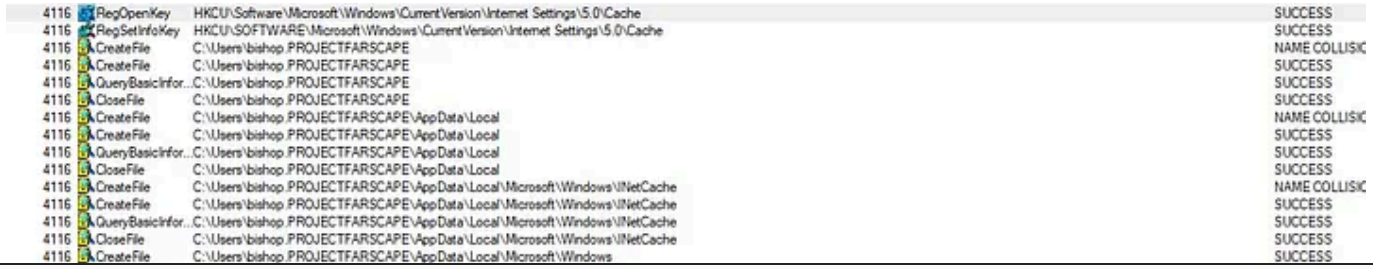
Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

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

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

Description: Журналы и оповещения производительности

Product: ?

Company: DLL помощника сетевой оболочки для winHttp

OriginalFileName: DisplaySwitch.exe

CommandLine:

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

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

User: PROJECTFARSCAPE\bishop

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

LogonId: 0x2F708

TerminalSessionId: 1

IntegrityLevel: High

Network connection detected:

RuleName:

UtcTime: 2020–03–14 23:23:10.013

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

ProcessId: 6268

SourcePortName:

DestinationIsIpv6: false

DestinationIp: 104.26.9.44

DestinationHostname:

DestinationPort: 443

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

DestinationPortName: http

The next one is one my favorites –

Network connection detected:

RuleName:

UtcTime: 2020–03–14 23:23:11.223

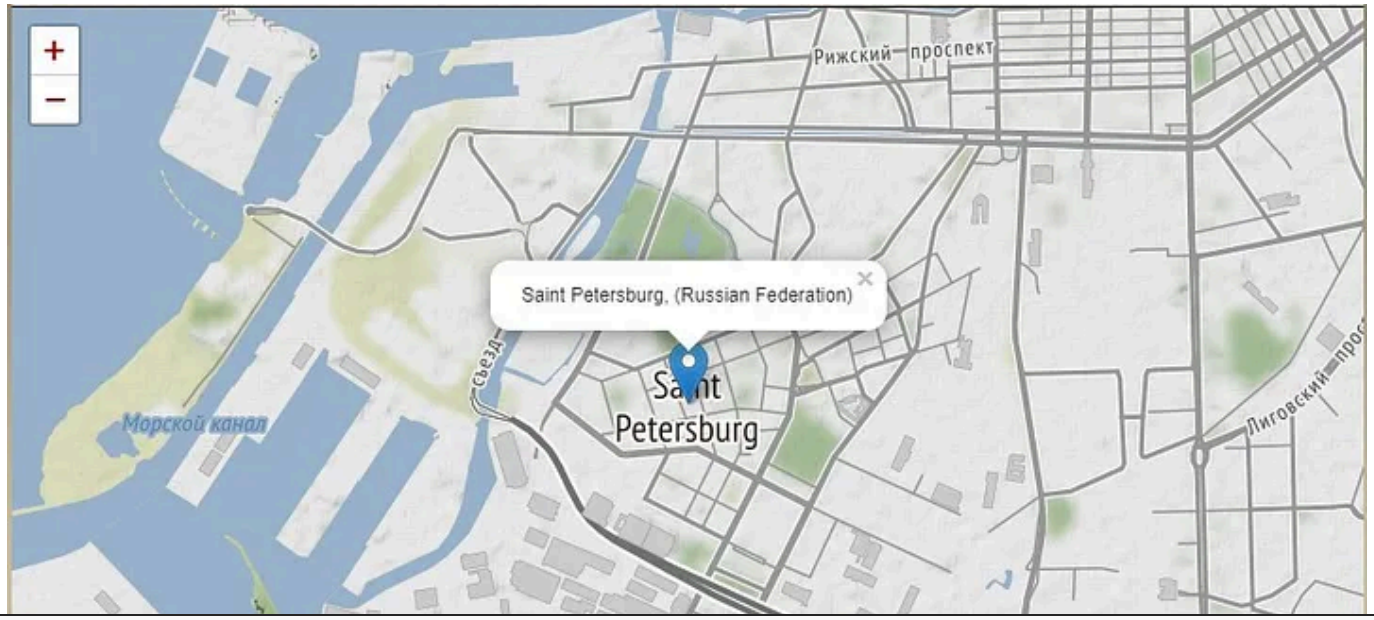
SourceHostname: asylum.projectfarscape.net

SourcePort: 58373

SourcePortName:

DestinationIsIpv6: false

DestinationIp: 149.154.167.220



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

RuleName:

UtcTime: 2020–03–14 23:24:00.845

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

ProcessId: 940

Image:

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

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.

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

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

Written by Robert Gonzalez

51 Followers

https://www.cybercrypto.net

Follow