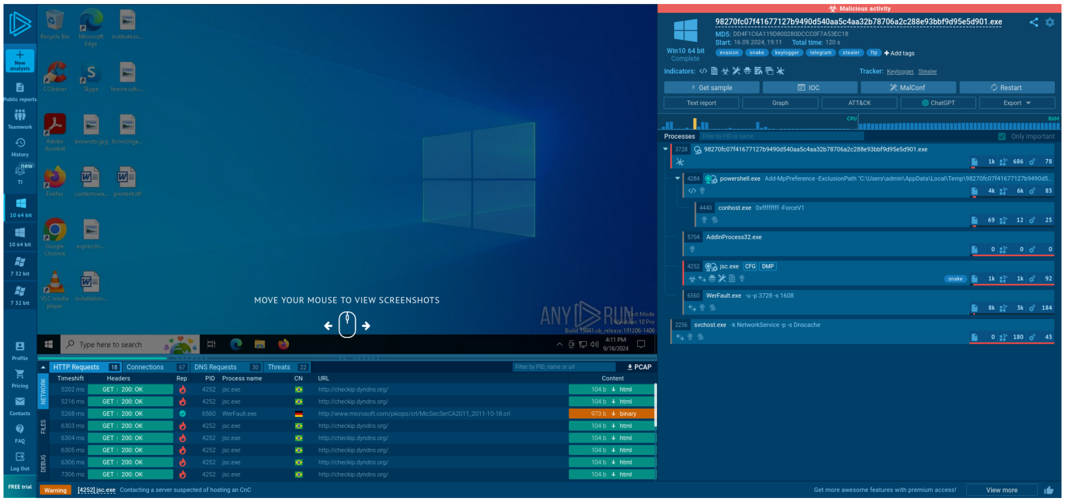
Lab 3: Malware analysis

Hayder Sarhan

Analysis:

After running the analysis on Any.run , using a Windows 10 (64-bit) I go the following:



Malicious activity

98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe

MD5: DD4F1C6A119D800280DCCC0F7A53EC18

Start: 16.09.2024, 19:11 Total time: 120 s

Win10 64 bit Complete

Tags: evasion, snake, keylogger, telegram, stealer, ftp

Tracker: Keylogger, Stealer

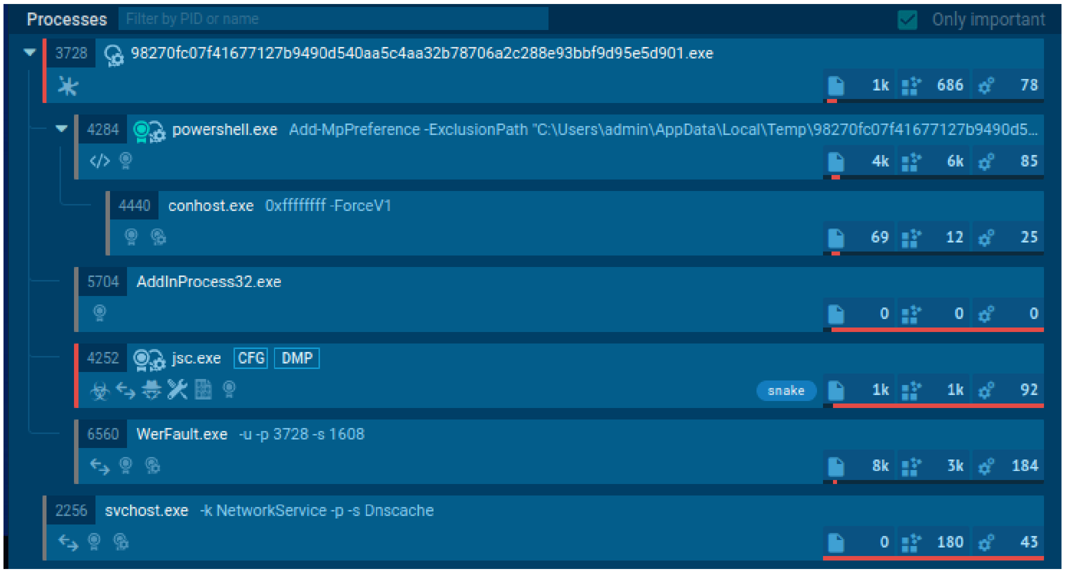
HTTP Requests 18 | Connections 67 | DNS Requests 30 | Threats 22

Timeshift	Headers	PID	Process name	URL	Content
5202 ms	GET 200: OK	4252	jsc.exe	http://checkip.dyndns.org/	104 b html
5216 ms	GET 200: OK	4252	jsc.exe	http://checkip.dyndns.org/	104 b html
5268 ms	GET 200: OK	6560	WerFault.exe	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
6303 ms	GET 200: OK	4252	jsc.exe	http://checkip.dyndns.org/	104 b html
6304 ms	GET 200: OK	4252	jsc.exe	http://checkip.dyndns.org/	104 b html
6305 ms	GET 200: OK	4252	jsc.exe	http://checkip.dyndns.org/	104 b html
6306 ms	GET 200: OK	4252	jsc.exe	http://checkip.dyndns.org/	104 b html
7306 ms	GET 200: OK	4252	jsc.exe	http://checkip.dyndns.org/	104 b html

Warning [4252] jsc.exe Contacting a server suspected of hosting an CnC

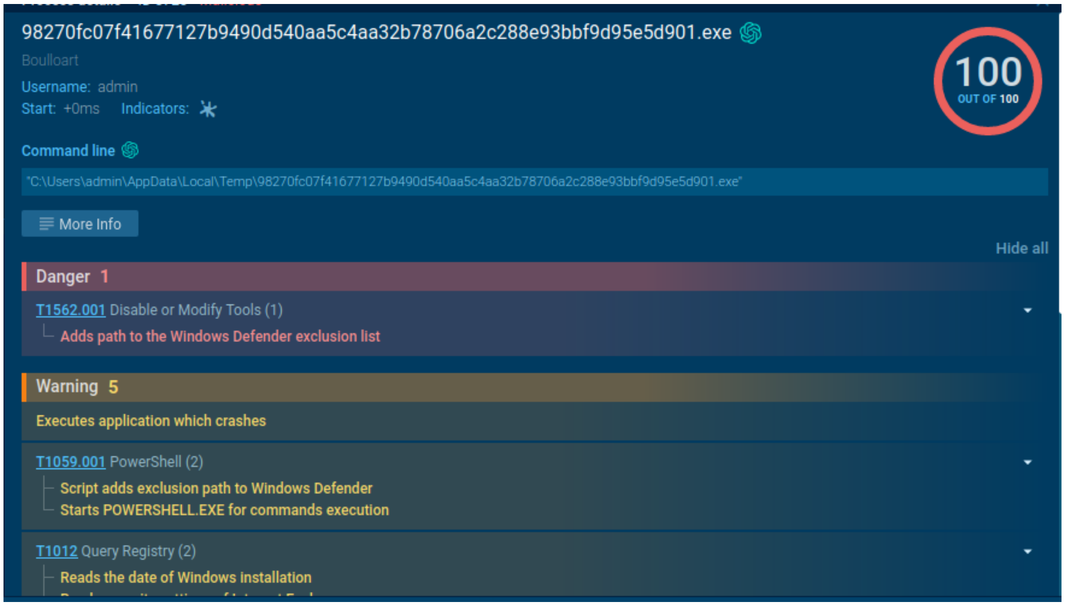
We first notice that the platform detected 2 possible malwares in this exe, the first is a **Keylogger** that spies and records the user's keyboard, the second one is a **Stealer** that is used to get access to users data and steal them.

We can see that once the exe is executed it fires up multiple processes:



```
3728 98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe    1k   686   78
  4284 powershell.exe Add-MpPreference -ExclusionPath "C:\Users\admin\AppData\Local\Temp\98270fc07f41677127b9490d5...    4k   6k   85
    4440 conhost.exe 0xffffffff -ForceV1    69   12   25
  5704 AddInProcess32.exe    0   0   0
  4252 jsc.exe CFG DMP    snake   1k   1k   92
  6560 WerFault.exe -u -p 3728 -s 1608    8k   3k   184
2256 svchost.exe -k NetworkService -p -s Dnscache    0   180   43
```

Let's examine the main exe:



98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe

Boulloart

Username: admin

Start: +0ms   Indicators:

100 OUT OF 100

Command line

"C:\Users\admin\AppData\Local\Temp\98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe"

Danger 1

T1562.001 Disable or Modify Tools (1)
- Adds path to the Windows Defender exclusion list

Warning 5

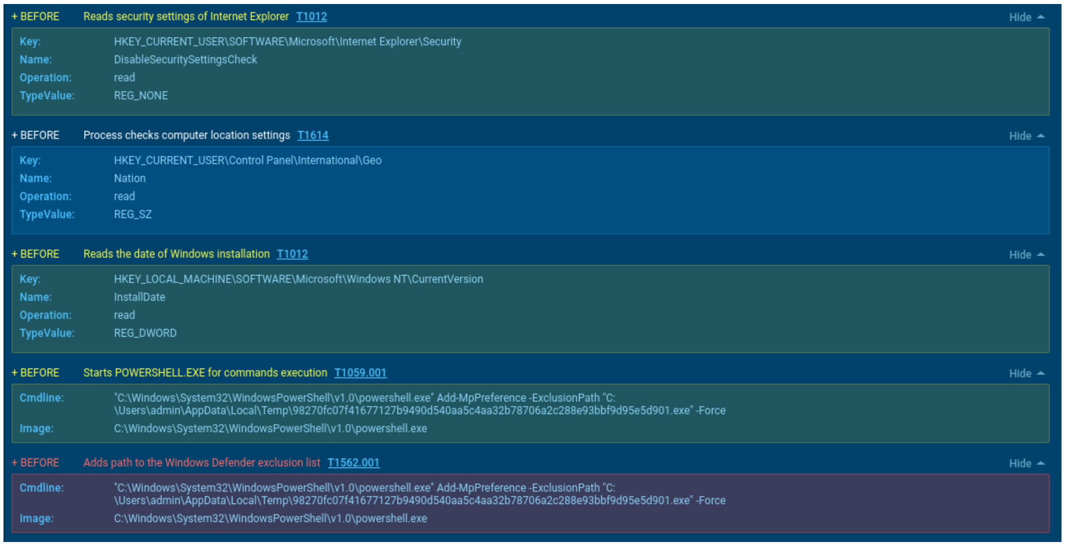
Executes application which crashes

T1059.001 PowerShell (2)
- Script adds exclusion path to Windows Defender
- Starts POWERSHELL.EXE for commands execution

T1012 Query Registry (2)
- Reads the date of Windows installation

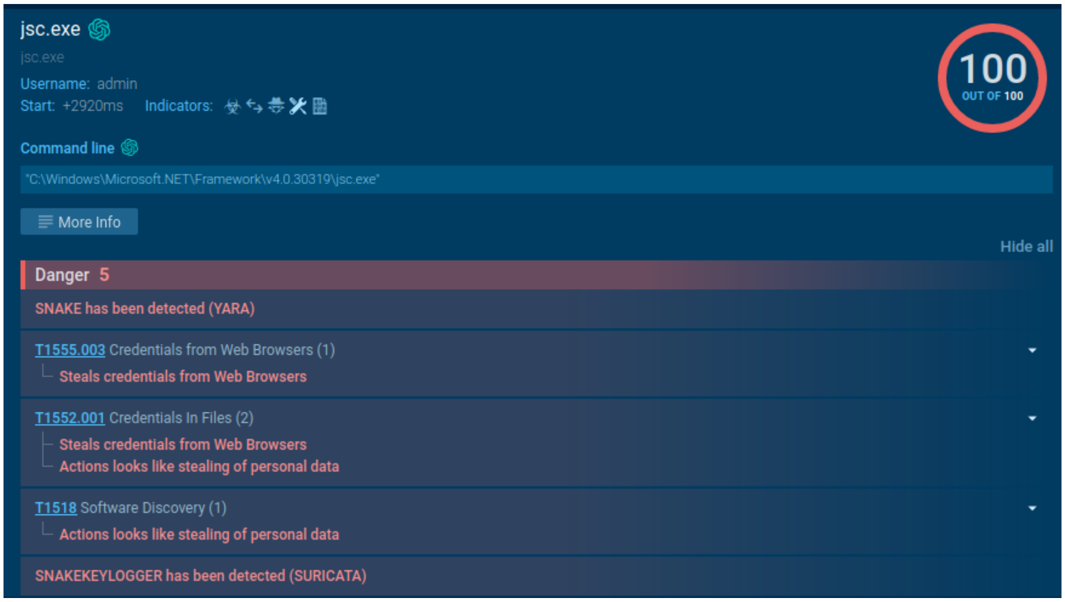
we see that the malware tries to edit the Windows Defender exclusion list

When we go to deep analysis we get the following:
For the first couple of seconds of starting the device the malware does do anything suspicious, but after sometime it starts trying to get access to user’s data and manipulate the system to hide itself using scripts.



```
+ BEFORE    Reads security settings of Internet Explorer  T1012                                   Hide
Key:        HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security
Name:       DisableSecuritySettingsCheck
Operation:  read
TypeValue:  REG_NONE

+ BEFORE    Process checks computer location settings  T1614                                      Hide
Key:        HKEY_CURRENT_USER\Control Panel\International\Geo
Name:       Nation
Operation:  read
TypeValue:  REG_SZ

+ BEFORE    Reads the date of Windows installation  T1012                                         Hide
Key:        HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Name:       InstallDate
Operation:  read
TypeValue:  REG_DWORD

+ BEFORE    Starts POWERSHELL.EXE for commands execution  T1059.001                               Hide
Cmdline:    "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:
            \Users\admin\AppData\Local\Temp\98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe" -Force
Image:      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

+ BEFORE    Adds path to the Windows Defender exclusion list  T1562.001                           Hide
Cmdline:    "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:
            \Users\admin\AppData\Local\Temp\98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe" -Force
Image:      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

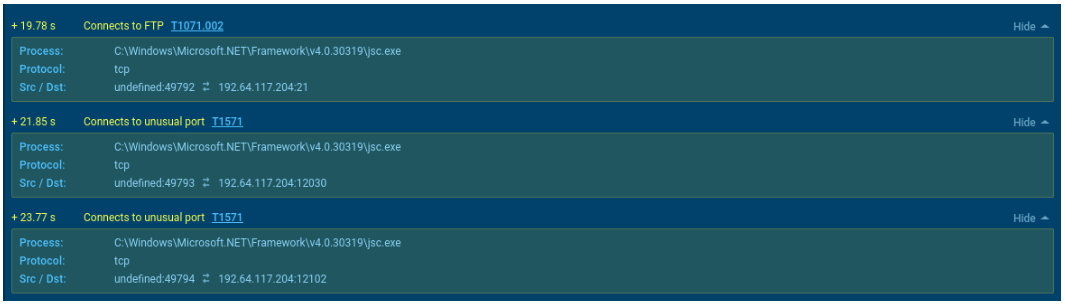
Going back to the process the malware tries to run, we can notice another threat:



```
jsc.exe
jsc.exe
Username: admin
Start: +2920ms    Indicators:
                                                        100
                                                        OUT OF 100
Command line
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe"
More Info
                                                        Hide all
Danger 5
SNAKE has been detected (YARA)
T1555.003 Credentials from Web Browsers (1)
  └ Steals credentials from Web Browsers
T1552.001 Credentials In Files (2)
  ├ Steals credentials from Web Browsers
  └ Actions looks like stealing of personal data
T1518 Software Discovery (1)
  └ Actions looks like stealing of personal data
SNAKEKEYLOGGER has been detected (SURICATA)
```

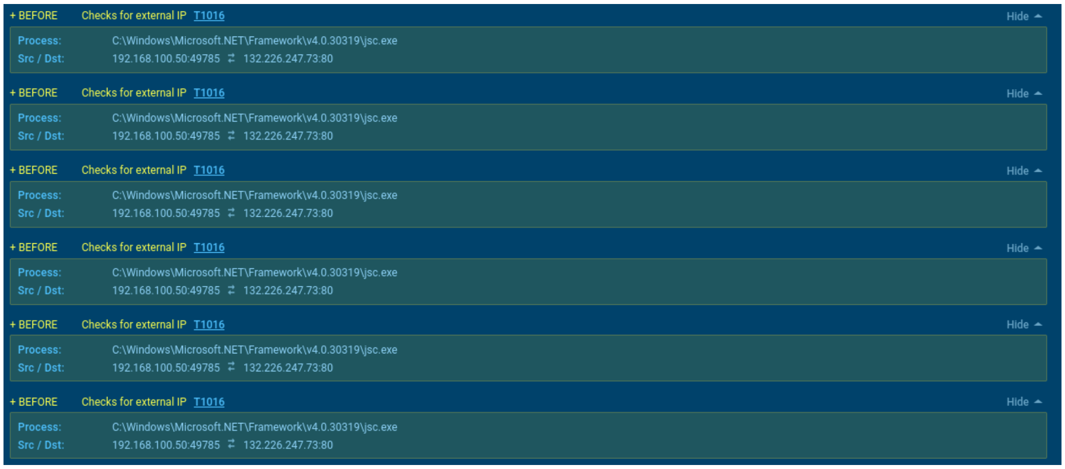
Here we see a lot of things that we need to uncover.
When we go to deep analysis we get the following:

First the exe tries to make suspicious connections to an IP with different port with each connection:



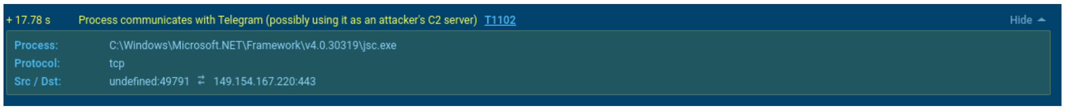
```
+ 19.78 s     Connects to FTP  T1071.002                                    Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Protocol:   tcp
  Src / Dst:  undefined:49792 ⇄ 192.64.117.204:21
+ 21.85 s     Connects to unusual port  T1571                               Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Protocol:   tcp
  Src / Dst:  undefined:49793 ⇄ 192.64.117.204:12030
+ 23.77 s     Connects to unusual port  T1571                               Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Protocol:   tcp
  Src / Dst:  undefined:49794 ⇄ 192.64.117.204:12102
```

It then starts checking for a certain IP, this process happens multiple times through the execution of the malware:



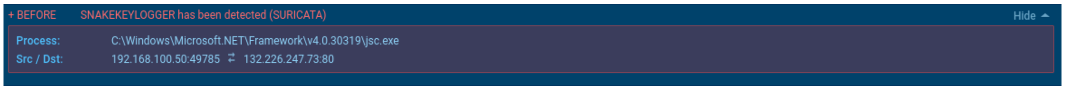
```
+ BEFORE     Checks for external IP  T1016                                  Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Src / Dst:  192.168.100.50:49785 ⇄ 132.226.247.73:80
+ BEFORE     Checks for external IP  T1016                                  Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Src / Dst:  192.168.100.50:49785 ⇄ 132.226.247.73:80
+ BEFORE     Checks for external IP  T1016                                  Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Src / Dst:  192.168.100.50:49785 ⇄ 132.226.247.73:80
+ BEFORE     Checks for external IP  T1016                                  Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Src / Dst:  192.168.100.50:49785 ⇄ 132.226.247.73:80
+ BEFORE     Checks for external IP  T1016                                  Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Src / Dst:  192.168.100.50:49785 ⇄ 132.226.247.73:80
+ BEFORE     Checks for external IP  T1016                                  Hide
  Process:    C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Src / Dst:  192.168.100.50:49785 ⇄ 132.226.247.73:80
```

Then it starts communicating with Telegram:



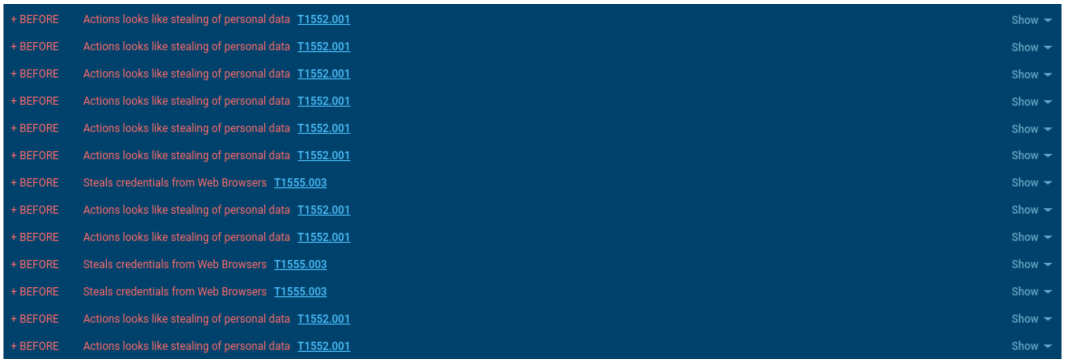
```
+ 17.78 s    Process communicates with Telegram (possibly using it as an attacker's C2 server)  T1102      Hide ▲
  Process:      C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Protocol:     tcp
  Src / Dst:    undefined:49791 ⇄ 149.154.167.220:443
```

After that we see the following:



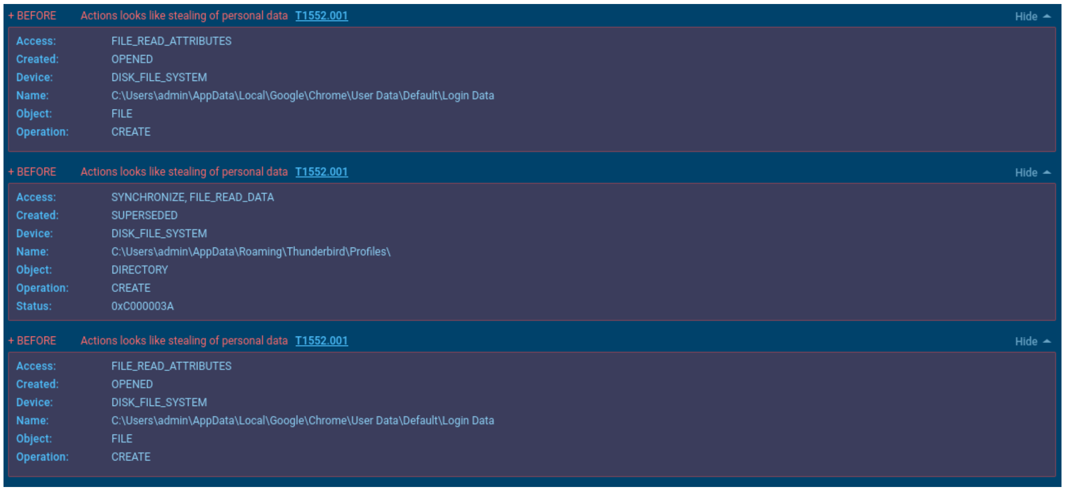
```
+ BEFORE     SNAKEKEYLOGGER has been detected (SURICATA)                                          Hide ▲
  Process:      C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
  Src / Dst:    192.168.100.50:49785 ⇄ 132.226.247.73:80
```

The malware is initializing a keylogger.
After it the malware starts stealing data for the user’s device:



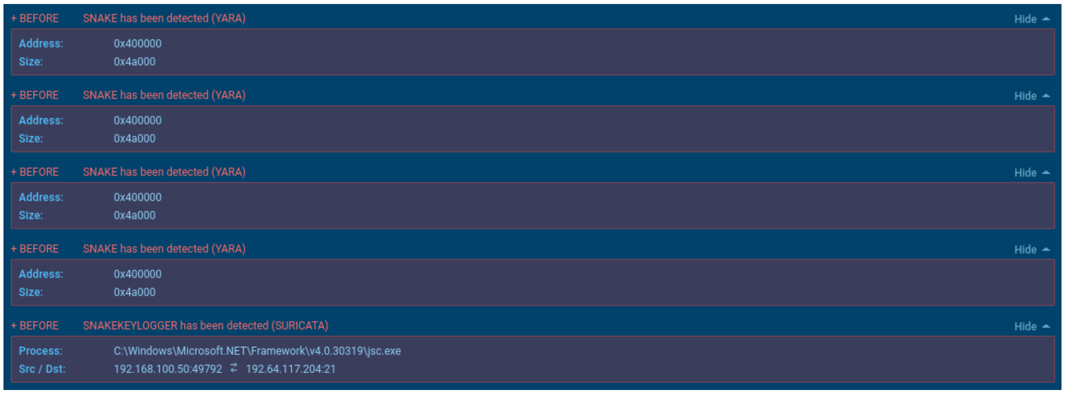
```
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Steals credentials from Web Browsers  T1555.003                Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Steals credentials from Web Browsers  T1555.003                Show ▼
+ BEFORE     Steals credentials from Web Browsers  T1555.003                Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Show ▼
```

more details on the first 3:



```
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Hide ▲
  Access:       FILE_READ_ATTRIBUTES
  Created:      OPENED
  Device:       DISK_FILE_SYSTEM
  Name:         C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Login Data
  Object:       FILE
  Operation:    CREATE
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Hide ▲
  Access:       SYNCHRONIZE, FILE_READ_DATA
  Created:      SUPERSEDED
  Device:       DISK_FILE_SYSTEM
  Name:         C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\
  Object:       DIRECTORY
  Operation:    CREATE
  Status:       0xC000003A
+ BEFORE     Actions looks like stealing of personal data  T1552.001        Hide ▲
  Access:       FILE_READ_ATTRIBUTES
  Created:      OPENED
  Device:       DISK_FILE_SYSTEM
  Name:         C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Login Data
  Object:       FILE
  Operation:    CREATE
```

Then a Snake get detected:



+ BEFORE SNAKE has been detected (YARA)

Address: 0x400000
Size: 0x4a000

+ BEFORE SNAKE has been detected (YARA)

Address: 0x400000
Size: 0x4a000

+ BEFORE SNAKE has been detected (YARA)

Address: 0x400000
Size: 0x4a000

+ BEFORE SNAKE has been detected (YARA)

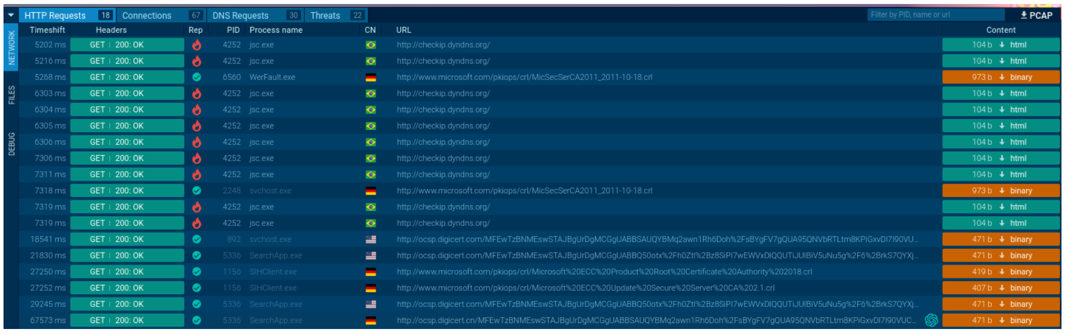
Address: 0x400000
Size: 0x4a000

+ BEFORE SNAKEKEYLOGGER has been detected (SURICATA)

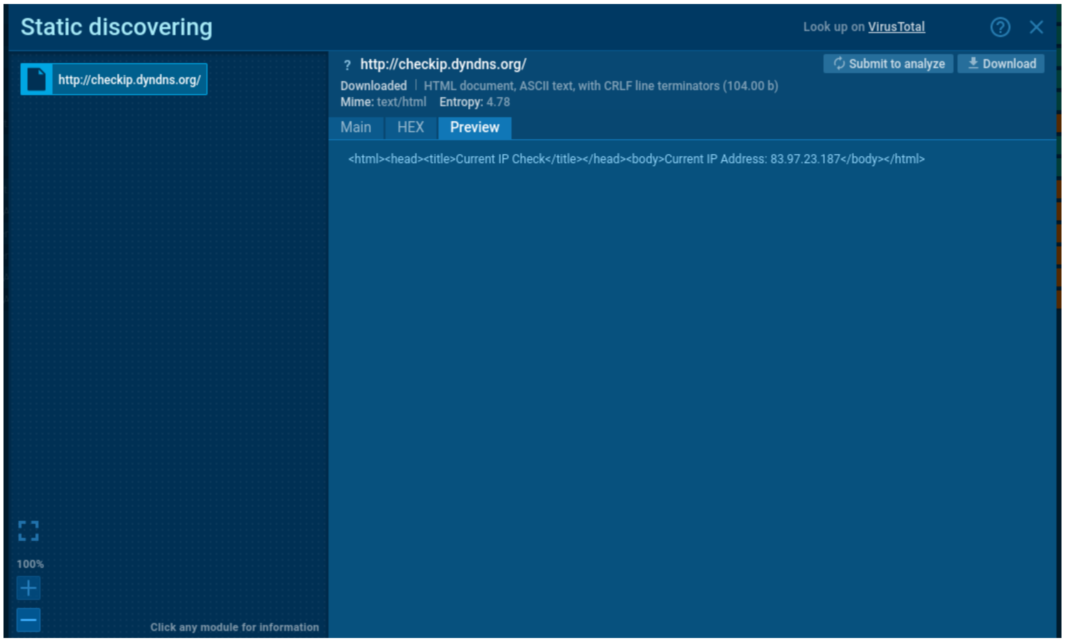
Process: C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe
Src / Dst: 192.168.100.50:49792 ⇄ 192.64.117.204:21

If we go back to the main page we can check on the connections made by the malware and the files that has been modified:

We can see that there are multiple malicious HTTP requests sent to a certain URL in Brazil:



Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5202 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
5216 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
5268 ms	GET | 200: OK	✓	6560	WerFault.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary
6303 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
6304 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
6305 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
6306 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
7306 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
7311 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
7318 ms	GET | 200: OK	✓	2248	svchost.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary
7319 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
7319 ms	GET | 200: OK	🔥	4252	jsc.exe	🇧🇷	http://checkip.dyndns.org/	104 b ↓ html
18541 ms	GET | 200: OK	✓	892	svchost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VU...	471 b ↓ binary
21830 ms	GET | 200: OK	✓	5336	SearchApp.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXj...	471 b ↓ binary
27250 ms	GET | 200: OK	✓	1156	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	419 b ↓ binary
27252 ms	GET | 200: OK	✓	1156	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	407 b ↓ binary
29245 ms	GET | 200: OK	✓	5336	SearchApp.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXj...	471 b ↓ binary
67573 ms	GET | 200: OK	✓	5336	SearchApp.exe	🇩🇪	http://ocsp.digicert.cn/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUC...	471 b ↓ binary

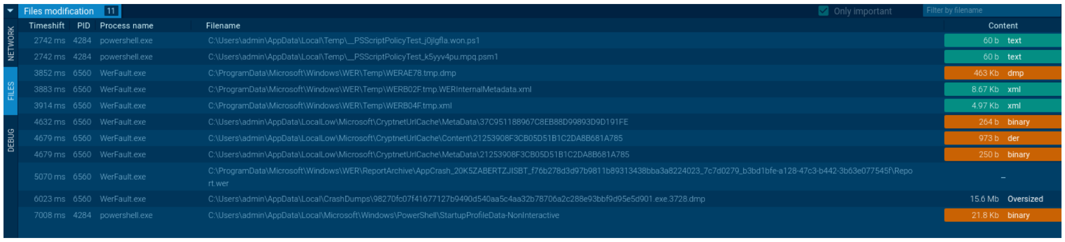


? http://checkip.dyndns.org/

Downloaded | HTML document, ASCII text, with CRLF line terminators (104.00 b)
Mime: text/html Entropy: 4.78

```
<html><head><title>Current IP Check</title></head><body>Current IP Address: 83.97.23.187</body></html>
```

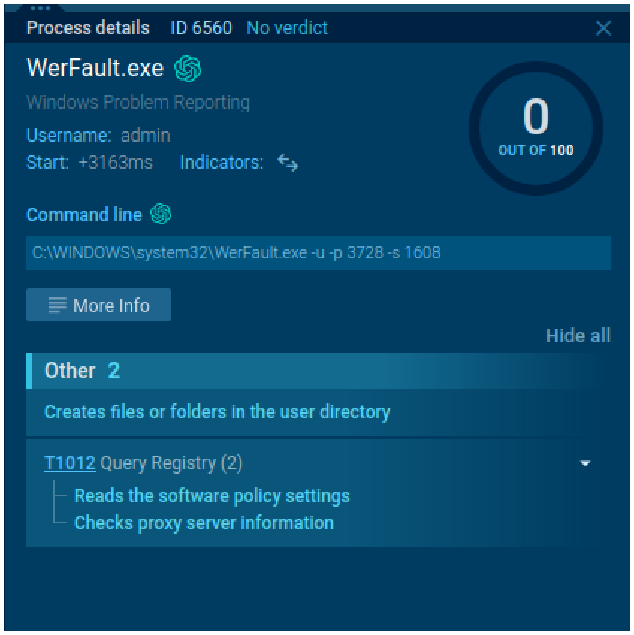
Now when we go to the files modification section we see the following:



Timeshift	PID	Process name	Filename	Content
2742 ms	4284	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_j0jlgfla.won.ps1	60 b text
2742 ms	4284	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_k5yyv4pu.mpq.psm1	60 b text
3852 ms	6560	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE78.tmp.dmp	463 Kb dmp
3883 ms	6560	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERB02F.tmp.WERInternalMetadata.xml	8.67 Kb xml
3914 ms	6560	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04F.tmp.xml	4.97 Kb xml
4632 ms	6560	WerFault.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE	264 b binary
4679 ms	6560	WerFault.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\21253908F3CB05D51B1C2DA8B681A785	973 b der
4679 ms	6560	WerFault.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\21253908F3CB05D51B1C2DA8B681A785	250 b binary
5070 ms	6560	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_20K5ZABERTZJISBT_f76b278d3d97b9811b89313438bba3a8224023_7c7d0279_b3bd1bfe-a128-47c3-b442-3b63e077545f\Report.wer	–
6023 ms	6560	WerFault.exe	C:\Users\admin\AppData\Local\CrashDumps\98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe.3728.dmp	15.6 Mb Oversized
7008 ms	4284	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	21.8 Kb binary

we notice that one of the process that the malware fired up is modifying xml and binary files.

more info about the process:



WerFault.exe

Windows Problem Reporting

Username: admin

Start: +3163ms Indicators:

Command line

C:\WINDOWS\system32\WerFault.exe -u -p 3728 -s 1608

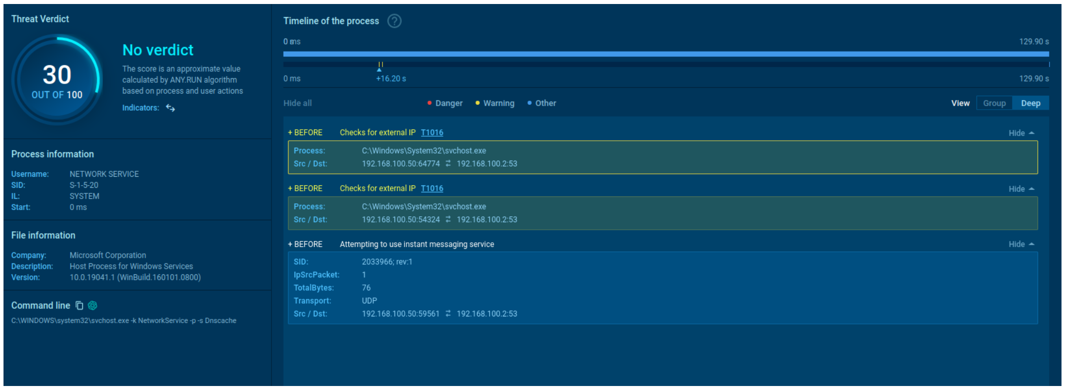
Other 2

Creates files or folders in the user directory

T1012 Query Registry (2)

- Reads the software policy settings
- Checks proxy server information

Finally, we may notice that the malware tried to use svchost.exe



No verdict

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username: NETWORK SERVICE
SID: S-1-5-20
IL: SYSTEM
Start: 0 ms

File information

Company: Microsoft Corporation
Description: Host Process for Windows Services
Version: 10.0.19041.1 (WinBuild.160101.0800)

Command line

C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache

+ BEFORE Checks for external IP T1016

Process: C:\Windows\System32\svchost.exe
Src / Dst: 192.168.100.50:64774 ⇄ 192.168.100.2:53

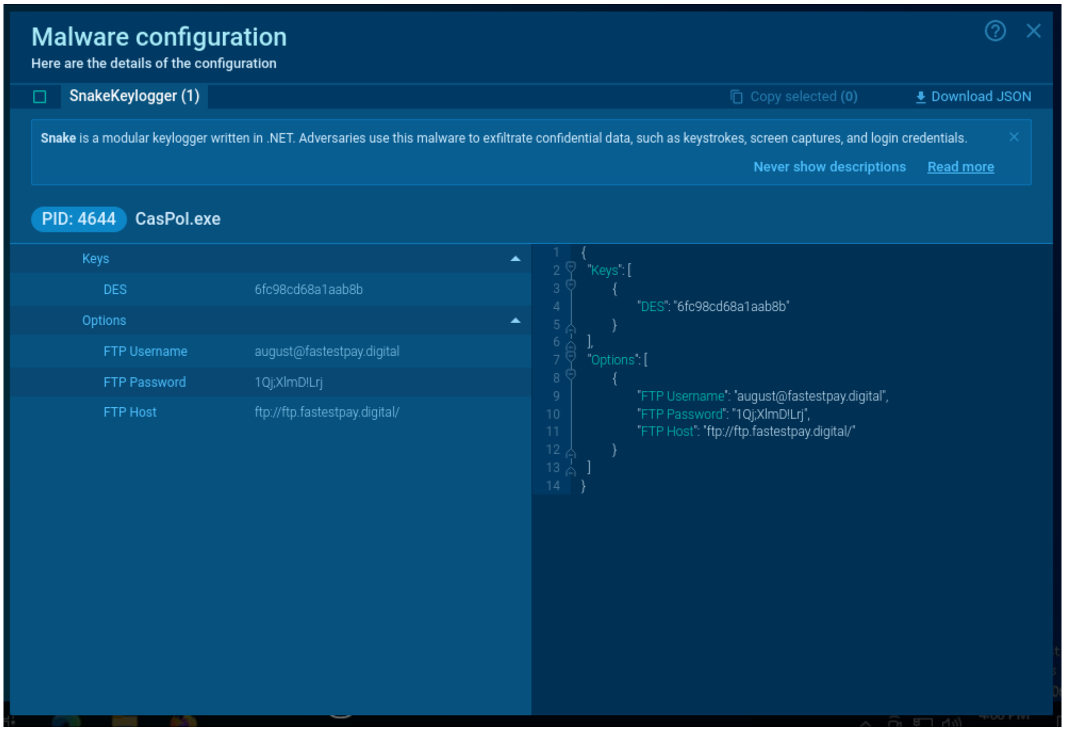
+ BEFORE Checks for external IP T1016

Process: C:\Windows\System32\svchost.exe
Src / Dst: 192.168.100.50:54324 ⇄ 192.168.100.2:53

+ BEFORE Attempting to use instant messaging service

SID: 2033966; rev:1
IpSrcPacket: 1
TotalBytes: 76
Transport: UDP
Src / Dst: 192.168.100.50:59561 ⇄ 192.168.100.2:53

Malware Config:



Malware configuration

Here are the details of the configuration

□ SnakeKeylogger (1)

Snake is a modular keylogger written in .NET. Adversaries use this malware to exfiltrate confidential data, such as keystrokes, screen captures, and login credentials.

PID: 4644 CasPol.exe

Keys	
DES	6fc98cd68a1aab8b
Options	
FTP Username	august@fastestpay.digital
FTP Password	1Qj;XlmD!Lrj
FTP Host	ftp://ftp.fastestpay.digital/

```
{
 "Keys": [
     {
         "DES": "6fc98cd68a1aab8b"
     }
 ],
 "Options": [
     {
         "FTP Username": "august@fastestpay.digital",
         "FTP Password": "1Qj;XlmD!Lrj",
         "FTP Host": "ftp://ftp.fastestpay.digital/"
     }
 ]
}
```

Remediation:

Multiple steps must be made:

- For a start the user should check on all of his online accounts and change their passwords. especially the ones saved on browsers like chrome and other apps that store their cache on the device. The apps that were targeted by this malware are: (Chrome, Thunderbird, CocCoc, Amigo, Orbitum, Kometa, Tencent)
- Deleting the malwares and any files created by it:
    - `C\Users\admin\AppData\Local\Temp\98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe`
    - `C:\Windows\` `Microsoft.NET` `\Framework\v4.0.30319\jsc.exe`
    - `C\Users\admin\AppData\Local\CrashDumps\98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe.3728.dmp`
- Download a reliable antivirus to make sure that the system is clean.