Raccoon Infostealer Malware Returns with New TTPS – Detection & Response

socinvestigation.com/raccoon-infostealer-malware-returns-with-new-ttps-detection-response/

August 18, 2022

IOC

By

BalaGanesh

-

August 18, 2022

0

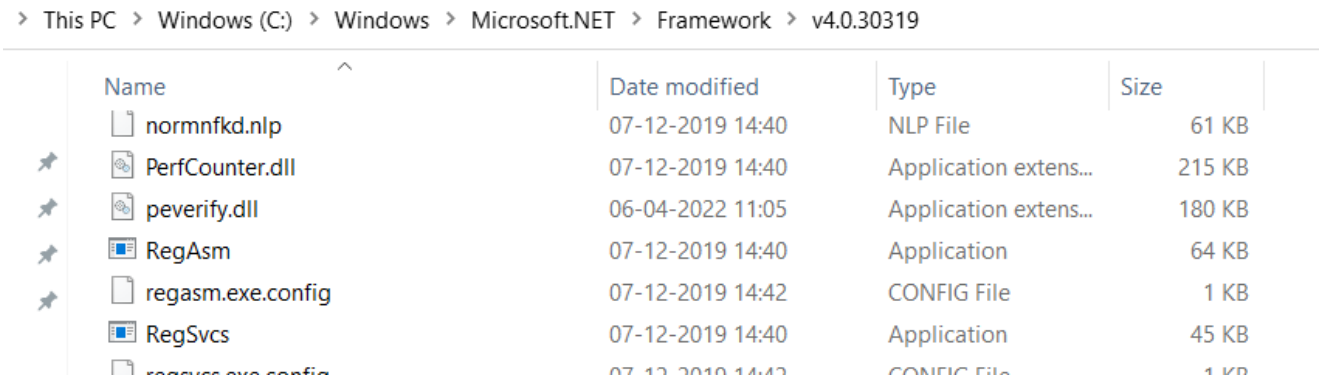
Raccoon is an info stealer type malware available as **malware-as-a-service** on underground forums since early 2019. It can be obtained for a subscription and costs $200 per month. Raccoon malware has already infected over 100,000 devices and became one of the most mentioned viruses on the underground forums.

Also Read: Latest IOCs – Threat Actor URLs , IP's & Malware Hashes

The Raccoon Malware is a robust stealer that allows the stealing of data such as passwords, cookies, and autofill data from browsers. Raccoon stealers also support theft from all cryptocurrency wallets. Raccoons are often infected through phishing campaigns or exploit kits.

Malware Spread:

Firstly malware binary drops into the temp directory in any random name "\AppData\Local\Temp\ecc322f22da7cee63fb2ee0bfd5df59c.exe" and later it leverages RegSvcs.exe genuine software component of Microsoft**. NET Framework by Microsoft** which is located at C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe



Malicious File name ecc322f22da7cee63fb2ee0bfd5df59c.exe running as a background process and executes the RegSvcs.exe.

Regsvcs.exe connects to CnC and downloads another malicious DLL **http://85[.]192.63.46/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll** and file downloaded to temp directory "C:\Users\Balaganesh\AppData\LocalLow\nss3.dll"

Also Read: Latest Cyber Security News – Hacker News !

Downloaded Dropper "nss3.dll" allows stealing of data such as passwords, cookies, and autofill data from browsers.

Some other DLLs also dropped on the same AppData folder containing Bitcoin addresses "C:\Users\Balaganesh\AppData\LocalLow\mozglue.dll" Dropper "mozglue.dll" object may contain Bitcoin addresses and supports cryptocurrency wallets thefts.

Data Exfiltration

HTTP post method is used and stolen data is sent to attackers' IP addresses.**http://85[.]192.63.46/** ASN (Informacines sistemos ir technologijos, UAB) & **http://85[.]192.63.46/** ASN (JSC Digital Network)

Indicators of Compromise

IPs:

http://85[.]192.63.46/
http://88[.]119.170.241/

File hashes:

51c33c00a3823180a7b39ab838542d9d

7a1618c1616dae2aa4402b2f9f0febc7

1de2a5e94f070e9d6e8d70fe63e87175

c8f9b86af75c8cb9f973683dbee27f93

704cb6b7d8863165857bca2c33283fa0

e490eacd7d52073891790cd3411a1221

52b4394897b2ddd3c47ec410ea1ff869

52b4394897b2ddd3c47ec410ea1ff869

2eb2d4dc60b185e1961746b120d45f97

ecc322f22da7cee63fb2ee0bfd5df59c

Detection & Response

Splunk:

```
source="WinEventLog:*" AND ((Image="*\*.exe") AND Image="*\\RegSvcs.exe" AND
TargetFilename="*\\AppData\\Local\\Temp\*.exe*" AND
(TargetFilename="*AppData\\LocalLow\*.dll*"))
```

Qradar:

```
SELECT UTF8(payload) from events where LOGSOURCETYPENAME(devicetype)='Microsoft
Windows Security Event Log' and ("Image" ilike '%\%.exe') and "Image" ilike
'%\RegSvcs.exe' and "Filename" ilike '%\AppData\Local\Temp\%.exe%' and ("Filename"
ilike '%AppData\LocalLow\%.dll%')
```

Elastic Query:

```
(process.executable.text:*\*.exe AND process.executable.text:*\\RegSvcs.exe AND
file.path.text:*\\AppData\\Local\\Temp\*.exe* AND
file.path.text:*AppData\\LocalLow\*.dll*)
```

CarbonBlack:

```
(process_name:*\*.exe AND process_name:*\\RegSvcs.exe AND
filemod_name:*\\AppData\\Local\\Temp\*.exe* AND
filemod_name:*AppData\\LocalLow\*.dll*)
```

Crowdstike:

```
(((ImageFileName="*\*.exe") AND ImageFileName="*\\RegSvcs.exe") AND
(TemporaryFileName="*\\AppData\\Local\\Temp\*.exe*" OR
TargetFileName="*\\AppData\\Local\\Temp\*.exe*") AND
((TemporaryFileName="*AppData\\LocalLow\*.dll*") OR
(TargetFileName="*AppData\\LocalLow\*.dll*")))
```

Graylog:

```
(Image.keyword:*\*.exe AND Image.keyword:*\\RegSvcs.exe AND
TargetFilename.keyword:*\\AppData\\Local\\Temp\*.exe* AND
TargetFilename.keyword:*AppData\\LocalLow\*.dll*)
```

Logpoint:

```
(Image IN "*\*.exe" Image="*\\RegSvcs.exe"
TargetFilename="*\\AppData\\Local\\Temp\*.exe*" TargetFilename IN
"*AppData\\LocalLow\*.dll*")
```

Microsoft Defender:

```
DeviceProcessEvents | where ((FolderPath matches regex @".*\.*\.exe") and FolderPath
endswith @"\RegSvcs.exe" and FolderPath matches regex
@".*\\AppData\\Local\\Temp\.*\.exe.*" and (FolderPath matches regex
@".*AppData\\LocalLow\.*\.dll.*"))
```

Microsoft Sentinel:

```
SecurityEvent |  where EventID == 1 | where ((NewProcessName matches regex '(?
i).*\.*.exe') and NewProcessName endswith @'\RegSvcs.exe' and TargetFilename matches
regex '(?i).*\AppData\Local\Temp\.*.exe.*' and (TargetFilename matches regex '(?
i).*AppData\LocalLow\.*.dll.*'))
```

SumoLogic:

```
(_sourceCategory=*windows* AND (Image = "*\*.exe") AND Image="*\RegSvcs.exe" AND
("\AppData\Local\Temp\" AND ".exe") AND (("AppData\LocalLow\" AND ".dll")))
```

Google Chronicle:

```
target.process.file.full_path = /.*\\.*\.exe$/ and target.process.file.full_path =
/.*\\RegSvcs\.exe$/ and target.file.full_path = /.*\\AppData\\Local\\Temp\\.*\.exe.*/
and target.file.full_path = /.*AppData\\LocalLow\\.*\.dll.*/
```

Securonix:

```
index = archive AND (rg_functionality = "Microsoft Windows" AND ((@customstring54 =
"**.exe") OR (@destinationprocessname = "**.exe")) AND (@customstring54 ENDS WITH
"\RegSvcs.exe" OR @destinationprocessname ENDS WITH "\RegSvcs.exe") AND rawevent =
"*\AppData\Local\Temp*.exe*" AND (rawevent = "*AppData\LocalLow*.dll*"))
```

LEAVE A REPLY

Please enter your comment!

Please enter your name here

You have entered an incorrect email address!

Please enter your email address here