Analysing “Retefe” with Sysmon and Splunk

Published: 2019-05-23 · Archived: 2026-04-05 20:36:20 UTC

I recently took a closer look at Retefe because they seem to have abandon the short-lived “SmokeLoader”-phase and moved back to “socat.exe” and the TOR-network.

The original delivery method is by mail spam, sending an Office document (either a docx or xlsx attachment) with an embedded OLE object (the malicious .exe file). If the victim double clicks the embedded object (hidden behind an image), the Retefe infection chain is launched. In general Retefe consists of several PowerShell scripts, which download “7-Zip”, “tor.exe”, “socat.exe”, change the proxy settings on the system, install a new Root certificate and use scheduled tasks for persistence.

For details on the malware I recommend you read the following blog posts:

- https://www.govcert.admin.ch/blog/35/reversing-retefe
- https://www.govcert.admin.ch/blog/33/the-retefe-saga
- https://www.proofpoint.com/us/threat-insight/post/2019-return-retefe

A very easy way to detect Retefe is to look for “tor.exe” and “socat.exe” processes in the folder “ProgramData”:

```
`sysmon` ("tor.exe" OR "socat.exe") "\\ProgramData\\" EventCode=1
```

Alternatively you can look for active network connections from files “tor.exe” or “socat.exe” in “ProgramData”:

```
`sysmon` ("tor.exe" OR "socat.exe") "\\ProgramData\\" EventCode=3
```

With “*EventCode=11*” you can also look for the creation of the file (*Rule: FileCreate*).

Another way to detect unexpected behaviour could be to look for an “exe” file which creates “.ps1” files in the “Temp” folder:

```
`sysmon` Image="*.exe" EventCode=11 TargetFilename="*\\AppData\\Local\\Temp\\*.ps1" NOT "__PSScriptPolicyTest*.ps1"
```

Next is the “mshta” execution that Retefe uses for persistence. The call runs “socat.exe” with the configuration included in the call:

```
`sysmon` "socat tcp4-LISTEN:5588,reuseaddr,fork,keepalive,bind=127.0.0.1 SOCKS4A:127.0.0.1:*.onion:5588,socksport=9050"
```

A pretty new way (not a long history of observation) would be to hunt for executions of PowerShell with an “-ep” policy, running a “ps1” file, piping to “find” and storing the output in a log file:

```
`sysmon` "cmd.exe" "/c powershell -ep" ("bypass" OR "Unrestricted") -f "*\\Temp\\*.ps1" "| find /v \"\" >> \"*\\Temp\\*.log"
```

For a general detection of Tor or “socat.exe” on a system, this query can be helpful:

```
`sysmon` EventCode=3 "ProgramData" DestinationPort=9050 DestinationIp=127.0.0.1
```

Finally, with this query you can find the shortcuts (".lnk" files) that Retefe uses for persistence:

```
`sysmon` EventCode=11 Image="*\\powershell.exe" "\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\*.lnk"
```

Summary

From the few Splunk queries I have shared, you can see that Retefe is not a highly complex malware, it is in fact pretty noisy and offers several ways to identify potentially infected clients. Even without Sysmon and Splunk, you can look for signs of an infection in these places:

- Proxy settings of the browser ("http://127.0.0.1" string)
- tor.exe and socat.exe in a "ProgramData" sub-folder
- fake Root certificate
- various ".lnk" files in the startup folder

Any other detections rule that are useful? Let me know and I will add them here.
