Metastealer

Published: 2023-05-11 · Archived: 2026-04-05 19:45:14 UTC

Analysis

This sample has many strings related to the build process that have not been stripped. We can use these for our yara rule.

```
 "powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionExtension
```

```
 C:\Workspace\Projects\rat\client\stealer\third_party

C:\Workspace\Projects\rat\client\stealer\out\build\x86-Releaseird_party\cryptopp\_deps\cryptopp\rijndael_simd.cp

stealertest.dll

IBrowserBase@stealer
ChromeBrowser@stealer
EdgeBrowser@stealer
FirefoxBrowser@stealer
```

This sample looks similar maybe an earlier version
`5e5cc4f42c7d5481db280b28d1227568c17ed8cc4208970b7a963a4f30c7cc83`

```
 C:\3001_1\notbotnet\client\stealer\out\third_party\cryptopp
C:\3001_1\notbotnet\client\stealer\third_party
stealertest.dll
```

Yara Rule

```
 rule metastealer_dga {
strings:
    $libs = "rat\\client\\stealer" ascii wide
    $rtti_1 = "IBrowserBase@stealer"
    $rtti_2 = "ChromeBrowser@stealer"
    $rtti_3 = "EdgeBrowser@stealer"
    $rtti_4 = "FirefoxBrowser@stealer"
    $name = "stealertest.dll"
condition:
    $name or
    all of ($rtti_*) or
```

```
    $libs

}
```

String Decryption

This is a modified version of Jason Reeves' script from his blog

DGA

We want to statically extract the DGA seed.

```
 68 EF 06 00 00                          push    1775
89 85 84 FD FF FF                       mov     [ebp-27Ch], eax
8D 85 F0 FD FF FF                       lea     eax, [ebp-210h]
68 34 12 00 00                          push    1234h
```
