BABYMETAL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 11:21:47 UTC

win.babymetal (Back to overview)

BABYMETAL

Actor(s): Anunak

BABYMETAL is a command line network tunnel utility based on the TinyMet Meterpreter tool, primarily used to execute Meterpreter reverse shell payloads.

References

2022-04-27 · · ANSSI · ANSSI
LE GROUPE CYBERCRIMINEL FIN7
Bateleur BELLHOP Griffon SQLRat POWERSOURCE Andromeda BABYMETAL BlackCat BlackMatter BOOSTWRITE Carbanak Cobalt Strike DNSMessenger Dridex DRIFTPIN Gameover P2P MimiKatz Murofet Qadars Ranbyus SocksBot

2022-04-04 · Mandiant · Brendan McKeague, Bryce Abdo, Ioana Teaca, Zander Work
FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7
Griffon BABYMETAL Carbanak Cobalt Strike JSSLoader Termite

2018-10-01 · FireEye · Katie Nickels, Regina Elwell
ATT&CKing FIN7
Bateleur BELLHOP Griffon ANTAK POWERPIPE POWERSOURCE HALFBAKED BABYMETAL Carbanak Cobalt Strike DNSMessenger DRIFTPIN PILLOWMINT SocksBot

2018-08-01 · FireEye · Barry Vengerik, Kimberly Goody, Nick Carr, Steve Miller
On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation
BELLHOP POWERPIPE BABYMETAL SocksBot FIN7

2016-01-12 · FireEye · Barry Vengerik, John Miller
The Magnificent FIN7: Revealing a Cybercriminal Threat Group
BABYMETAL

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.babymetal