POWERSOURCE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:09:32 UTC

ps1.powersource (Back to overview)

POWERSOURCE

Actor(s): Anunak

POWERSOURCE is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. The backdoor uses DNS TXT requests for command and control and is installed in the registry or Alternate Data Streams.

References

2023-07-26 · cocomelonc · cocomelonc
Malware development trick - part 35: Store payload in alternate data streams. Simple C++ example.
Valak POWERSOURCE Gazer PowerDuke

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

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

2017-03-07 · FireEye · Barry Vengerik, Jordan Nuce, Steve Miller
FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings
POWERSOURCE FIN7

There is no Yara-Signature yet.
