DNSMessenger (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:58:10 UTC

win.dnsmessenger (Back to overview)

DNSMessenger

aka: TEXTMATE

Actor(s): Anunak

DNSMessenger makes use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker.

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

2022-03-31 · APNIC · Debashis Pal
How to: Detect and prevent common data exfiltration attacks
Agent Tesla DNSMessenger PingBack Rising Sun

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

2017-10-11 · Wraith Hacker Blog · Wraith Hacker
More info on 'Evolved DNSMessenger'
DNSMessenger

2017-10-11 · Cisco Talos · @Simpo13, Colin Grady, Dave Maynor, Edmund Brumaghin

Spoofed SEC Emails Distribute Evolved DNSMessenger

DNSMessenger

2017-03-02 · Cisco · Colin Grady, Edmund Brumaghin

Covert Channels and Poor Decisions: The Tale of DNSMessenger

DNSMessenger

There is no Yara-Signature yet.
