Bateleur (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:33:13 UTC

js.bateleur (Back to overview)

Bateleur

Actor(s): Anunak

There is no description at this point.

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

2021-08-30 · CrowdStrike · Eric Loui, Josh Reynolds
CARBON SPIDER Embraces Big Game Hunting, Part 1
Bateleur Griffon Carbanak DarkSide JSSLoader PILLOWMINT REvil

2020-01-01 · Secureworks · SecureWorks
GOLD NIAGARA
Bateleur Griffon Carbanak Cobalt Strike DRIFTPIN TinyMet FIN7

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

2017-07-31 · Proofpoint · Darien Huss, Matthew Mesa
FIN7/Carbanak threat actor unleashes Bateleur JScript backdoor
Bateleur FIN7

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/js.bateleur