DRIFTPIN (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:31:43 UTC

win.driftpin (Back to overview)

DRIFTPIN

aka: Toshliph, Spy.Agent.ORM

Actor(s): Anunak

Driftpin is a small and simple backdoor that enables the attackers to assess the victim. When executed the trojan connects to a C&C server and receives commands to grab screenshots, enumerate running processes and get information about the system and campaign ID.

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

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

2017-06-12 · FireEye · Barry Vengerik, James T. Bennett
Behind the CARBANAK Backdoor
Carbanak DRIFTPIN

2015-09-08 · ESET Research · Anton Cherepanov

Carbanak gang is back and packing new guns

DRIFTPIN

There is no Yara-Signature yet.
