malpedia

Fraunhofer
FKIE

Inventory   Statistics   Usage   ApiVector   Login

Quicksearch...

ANTHROPOID SPIDER   (Back to overview)

aka: CobaltGoblin, Empire Monkey

Publicly known as 'EmpireMonkey', ANTHROPOID SPIDER conducted phishing campaigns in February and March 2019, spoofing French, Norwegian and Belizean financial regulators and institutions. These campaigns used macro-enabled Microsoft documents to deliver the PowerShell Empire post-exploitation framework. ANTHROPOID SPIDER likely enabled a breach that allegedly involved fraudulent transfers over the SWIFT network.

Associated Families

There are currently no families associated with this actor.

References

2020-03-04 · CrowdStrike · CrowdStrike

📖 2020 CrowdStrike Global Threat Report

MESSAGETAP   More_eggs   8.t Dropper   Anchor   BabyShark   BadNews   Clop   Cobalt Strike   CobInt   Cobra Carbon System   Cutwail   DanaBot   Dharma   DoppelDridex   DoppelPaymer   Dridex   Emotet   FlawedAmmyy   FriedEx   Gandcrab   Get2   IcedID   ISFB   KerrDown   LightNeuron   LockerGoga   Maze   MECHANICAL   Necurs   Nokki   Outlook Backdoor   Phobos   Predator The Thief   QakBot   REvil   RobinHood   Ryuk   SDBbot   Skipper   SmokeLoader   TerraRecon   TerraStealer   TerraTV   TinyLoader   TrickBot   Vidar   Winnti   ANTHROPOID SPIDER   APT23   APT31   APT39   APT40   BlackTech   BuhTrap   Charming Kitten   CLOCKWORK SPIDER   DOPPEL SPIDER   FIN7   Gamaredon Group   GOBLIN PANDA   MONTY SPIDER   MUSTANG PANDA   NARWHAL SPIDER   NOCTURNAL SPIDER   PINCHY SPIDER   SALTY SPIDER   SCULLY SPIDER   SMOKY SPIDER   Thrip   VENOM SPIDER   VICEROY TIGER

2019-05-08 · Kaspersky Labs · Kaspersky Labs

📖 Fin7 hacking group targets more than 130 companies after leaders' arrest

Ave Maria   ANTHROPOID SPIDER

2019-02-28 · Fortiguard · FortiGuard

📖 EmpireMonkey malware distribution

ANTHROPOID SPIDER

Credits: MISP Project

Impressum   Datenschutzerklärung