Griffon (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:30:57 UTC

Griffon

aka: Harpy

Actor(s): FIN7

GRIFFON is a lightweight JavaScript validator-style implant without any persistence mechanism. The malware is designed for receiving modules to be executed in-memory and sending the results to C2s. The first module downloaded by the GRIFFON malware to the victim’s computer is an information-gathering JavaScript, which allows the cybercriminals to understand the context of the infected workstation.

References

2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT

2022-05-09 · Microsoft Security · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
Griffon BazarBackdoor BlackCat BlackMatter Blister Gozi LockBit Pandora Rook SystemBC TrickBot

2022-04-27 · · 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

2022-04-04 · Mandiant · Brendan McKeague, Bryce Abdo, Ioana Teaca, Zander Work
FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7
Griffon BABYMETAL Carbanak Cobalt Strike JSSLoader Termite

2021-11-04 · CrowdStrike · Eric Loui, Josh Reynolds
CARBON SPIDER Embraces Big Game Hunting, Part 2
BlackMatter Griffon BlackMatter DarkSide HiddenTear JSSLoader

2021-11-04 · Deep instinct · Shaul Vilkomir-Preisman
Understanding the Windows JavaScript Threat Landscape
STRRAT Griffon BlackByte Houdini Vjw0rm FIN7

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

2021-02-26 · CrowdStrike · Eric Loui, Sergei Frankoff
Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact
DarkSide RansomEXX Griffon Carbanak Cobalt Strike DarkSide IcedID MimiKatz PyXie RansomEXX REvil

2020-03-26 · SpiderLabs Blog · Alejandro Baca, Rodel Mendrez
Would You Exchange Your Security for a Gift Card?
Griffon

2020-02-13 · Qianxin · Qi Anxin Threat Intelligence Center
APT Report 2019
Chrysaor Exodus Dacls VPNFilter DNSRat Griffon KopiLuwak More_eggs SQLRat AppleJeus BONDUPDATER Agent.BTZ Anchor AndroMut AppleJeus BOOSTWRITE Brambul Carbanak Cobalt Strike Dacls DistTrack DNSpionage Dtrack ELECTRICFISH FlawedAmmyy FlawedGrace Get2 Grateful POS HOPLIGHT Imminent Monitor RAT jason Joanap KerrDown KEYMARBLE Lambert LightNeuron LoJax MiniDuke PolyglotDuke PowerRatankba Rising Sun SDBbot ServHelper Snatch Stuxnet TinyMet tRat TrickBot Volgmer X-Agent Zebrocy

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

2019-05-08 · Kaspersky Labs · Félix Aime, Yury Namestnikov
FIN7.5: the infamous cybercrime rig “FIN7” continues its activities
Griffon Ave Maria FIN7

2018-11-06 · Twitter (@ItsReallyNick) · Nick Carr
Tweet on a GRIFFON sample
Griffon

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

There is no Yara-Signature yet.

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