BONDUPDATER (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:25:48 UTC

ps1.bondupdater (Back to overview)

BONDUPDATER

aka: Poison Frog, Glimpse

Actor(s): OilRig, APT34

There is no description at this point.

References

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

COBALT GYPSY

TwoFace MacDownloader BONDUPDATER pupy Helminth jason RGDoor TinyZbot OilRig

2019-11-09 · NSFOCUS · Mina Hao

APT34 Event Analysis Report

BONDUPDATER DNSpionage

2019-09-18 · IronNet · Jonathan Lepore

Chirp of the PoisonFrog

BONDUPDATER

2019-08-22 · Cyware · Cyware
APT34: The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations
TwoFace BONDUPDATER POWRUNER QUADAGENT Helminth ISMAgent Karkoff LONGWATCH OopsIE PICKPOCKET RGDoor VALUEVAULT

2019-05-02 · Marco Ramilli's Blog · Marco Ramilli
APT34: Glimpse project
BONDUPDATER

2019-04-30 · Palo Alto Networks Unit 42 · Bryan Lee, Robert Falcone
Behind the Scenes with OilRig
BONDUPDATER

2019-04-19 · Medium · x0rz
Hacking (Back) and Influence Operations
BONDUPDATER

2019-04-17 · Malware Reversing Blog · F-Secure Global
The Dukes: 7 Years Of Russian Cyber-Espionage
TwoFace BONDUPDATER DNSpionage

2019-04-16 · Robert Falcone
DNS Tunneling in the Wild: Overview of OilRig’s DNS Tunneling
BONDUPDATER QUADAGENT Alma Communicator Helminth ISMAgent

2018-09-14 · NetScout · ASERT Team
Tunneling Under the Sands
BONDUPDATER

2018-09-12 · Palo Alto Networks Unit 42 · Kyle Wilhoit, Robert Falcone
OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government
BONDUPDATER

2018-04-20 · Booz Allen Hamilton · Jay Novak, Matthew Pennington
Researchers Discover New variants of APT34 Malware
BONDUPDATER POWRUNER

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/ps1.bondupdater