PowerRatankba (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:28:33 UTC

win.power_ratankba (Back to overview)

PowerRatankba

aka: QUICKRIDE.POWER

Actor(s): Lazarus Group

QUICKRIDE.POWER is a PowerShell variant of the QUICKRIDE backdoor. Its payloads are often saved to C:\windows\temp\

References

2020-02-19 · Lexfo · Lexfo
The Lazarus Constellation A study on North Korean malware
FastCash AppleJeus BADCALL Bankshot Brambul Dtrack Duuzer DYEPACK ELECTRICFISH HARDRAIN Hermes HOPLIGHT Joanap KEYMARBLE Kimsuky MimiKatz MyDoom NACHOCHEESE NavRAT PowerRatankba RokRAT Sierra(Alfa,Bravo, ...) Volgmer WannaCryptor

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

2019-01-15 · Flashpoint · Vitali Kremez
Disclosure of Chilean Redbanc Intrusion Leads to Lazarus Ties
PowerRatankba

2018-01-24 · Trend Micro · CH Lei, Fyodor Yarochkin, Lenart Bermejo, Philippe Z Lin, Razor Huang
Lazarus Campaign Targeting Cryptocurrencies Reveals Remote Controller Tool, an Evolved RATANKBA,

and More
PowerRatankba

2018-01-01 · FireEye · FireEye
APT38
Bitsran BLINDTOAD BOOTWRECK Contopee DarkComet DYEPACK HOTWAX NESTEGG PowerRatankba REDSHAWL WORMHOLE Lazarus Group

2017-12-20 · RiskIQ · Yonathan Klijnsma
Mining Insights: Infrastructure Analysis of Lazarus Group Cyber Attacks on the Cryptocurrency Industry
PowerRatankba

2017-12-19 · Proofpoint · Darien Huss
North Korea Bitten by Bitcoin Bug
QUICKCAFE PowerSpritz Ghost RAT PowerRatankba

There is no Yara-Signature yet.
