PowGoop (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:43:42 UTC

ps1.powgoop (Back to overview)

PowGoop

Actor(s): MuddyWater

DLL loader that decrypts and runs a powershell-based downloader.

References

2022-05-11 · NTT Security Holdings · NTT Security Holdings
Analysis of an Iranian APTs “E400” PowGoop Variant Reveals Dozens of Control Servers Dating Back to 2020
PowGoop

2022-02-25 · infoRisk TODAY · Prajeet Nair
MuddyWater Targets Critical Infrastructure in Asia, Europe
POWERSTATS PowGoop STARWHALE GRAMDOOR MoriAgent

2022-02-24 · CISA, CNMF, FBI, NCSC UK
Alert (AA22-055A) Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks
POWERSTATS PowGoop MoriAgent

2022-02-24 · CISA, CNMF, FBI, NCSC UK, NSA
Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks
POWERSTATS PowGoop GRAMDOOR MoriAgent

2022-01-12 · Sentinel LABS · Amitai Ben Shushan Ehrlich
Wading Through Muddy Waters | Recent Activity of an Iranian State-Sponsored Threat Actor
PowGoop

2022-01-12 · U.S. Cyber Command · U.S. Cyber Command
Iranian intel cyber suite of malware uses open source tools
PowGoop MoriAgent

2021-02-28 · PWC UK · PWC UK

Cyber Threats 2020: A Year in Retrospect

elf.wellmess FlowerPower PowGoop 8.t Dropper Agent.BTZ Agent Tesla Appleseed Ave Maria Bankshot BazarBackdoor BLINDINGCAN Chinoxy Conti Cotx RAT Crimson RAT DUSTMAN Emotet FriedEx FunnyDream Hakbit Mailto Maze METALJACK Nefilim Oblique RAT Pay2Key PlugX QakBot REvil Ryuk StoneDrill StrongPity SUNBURST SUPERNOVA TrickBot TurlaRPC Turla SilentMoon WastedLocker WellMess Winnti ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team

2020-10-21 · Symantec · Threat Hunter Team

Seedworm: Iran-Linked Group Continues to Target Organizations in the Middle East

PowGoop

2020-10-21 · CyberScoop · Sean Lyngaas

'MuddyWater' spies suspected in attacks against Middle East governments, telecoms

PowGoop

2020-10-15 · ClearSky · ClearSky

Operation Quicksand: MuddyWater’s Offensive Attack Against Israeli Organizations

PowGoop Covicli

2020-09-04 · Palo Alto Networks Unit 42 · Robert Falcone

Thanos Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa

PowGoop Hakbit

There is no Yara-Signature yet.

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