POWERSTATS (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:45:31 UTC

POWERSTATS

aka: Valyria

Actor(s): MuddyWater

POWERSTATS is a backdoor written in powershell.
It has the ability to disable Microsoft Office Protected View, fingerprint the victim and receive commands.

References

2023-06-29 · DeepInstinct ·
PhonyC2: Revealing a New Malicious Command & Control Framework by MuddyWater
PhonyC2 POWERSTATS

2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Boggy Serpens
POWERSTATS MuddyWater

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, NSA
Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks
POWERSTATS PowGoop 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

2021-01-13 · Shells.System blog · Ahmed Khlief
Reviving MuddyC3 Used by MuddyWater (IRAN) APT
POWERSTATS

2020-01-15 · Marco Ramilli's Blog · Marco Ramilli
Iranian Threat Actors: Preliminary Analysis
POWERSTATS

2020-01-07 · Prevailion · Danny Adamitis
Summer Mirage
POWERSTATS

2020-01-01 · Secureworks · SecureWorks
COBALT ULSTER
POWERSTATS Koadic MuddyWater

2019-08-01 · Kaspersky Labs · GReAT
APT trends report Q2 2019
ZooPark magecart POWERSTATS Chaperone COMpfun EternalPetya FinFisher RAT HawkEye Keylogger HOPLIGHT Microcin NjRAT Olympic Destroyer PLEAD RokRAT Triton Zebrocy

2019-06-10 · Trend Micro · Daniel Lunghi, Jaromír Hořejší
MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools
POWERSTATS

2019-05-29 · Group-IB · Group-IB
Catching fish in muddy waters
POWERSTATS

2019-04-15 · ClearSky · ClearSky Research Team
Iranian APT MuddyWater Attack Infrastructure Targeting Kurdish Political Groups and Organizations in Turkey
POWERSTATS MuddyWater

2019-04-10 · Check Point · Check Point Research
The Muddy Waters of APT Attacks
POWERSTATS

2019-03-21 · · Qianxin · Qi Anxin
Analysis of the latest attack activities of the suspected MuddyWater APT group against the Iraqi mobile operator Korek Telecom
POWERSTATS

2018-11-28 · ClearSky · ClearSky Research Team
MuddyWater Operations in Lebanon and Oman
POWERSTATS

2018-06-06 · ClearSky · ClearSky Cyber Security
Iranian APT group ‘MuddyWater’ Adds Exploits to Their Arsenal
POWERSTATS

2018-05-08 · Security 0wnage · Mo Bustami
Clearing the MuddyWater - Analysis of new MuddyWater Samples
POWERSTATS

2018-03-22 · Sekoia · sekoia
Falling on MuddyWater
POWERSTATS

2018-03-13 · FireEye · Ben Read, Dileep Kumar Jallepalli, Sudeep Singh, Yogesh Londhe
Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign
POWERSTATS MuddyWater

2018-03-12 · Trend Micro · Jaromír Hořejší
Campaign Possibly Connected to “MuddyWater” Surfaces in the Middle East and Central Asia
POWERSTATS MuddyWater

2018-03-01 · Security 0wnage · Mo Bustami
A Quick Dip into MuddyWater's Recent Activity
POWERSTATS

2018-01-02 · Security 0wnage · Mo Bustami
Burping on MuddyWater
POWERSTATS

2017-11-22 · Reaqta · Reaqta
A dive into MuddyWater APT targeting Middle-East
POWERSTATS

2017-11-14 · Palo Alto Networks Unit 42 · Tom Lancaster
Muddying the Water: Targeted Attacks in the Middle East
POWERSTATS MuddyWater

2017-10-04 · Security 0wnage · Mo Bustami
Continued Activity targeting the Middle East
POWERSTATS

2017-09-26 · Malwarebytes · Malwarebytes Labs
Elaborate scripting-fu used in espionage attack against Saudi Arabia Government entity
POWERSTATS

There is no Yara-Signature yet.
