Apostle (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:43:49 UTC

win.apostle (Back to overview)

Apostle

Actor(s): Pink Sandstorm

Malware used by suspected Iranian threat actor Agrius, turned from wiper into ransomware.

References

2023-11-06 · Palo Alto Networks Unit 42 · Assaf Dahan, Daniel Frank, Or Chechik, Tom Fakterman
Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors
Apostle Pink Sandstorm

2022-12-07 · ESET Research · Adam Burgher
Fantasy – a new Agrius wiper deployed through a supply-chain attack
Apostle DEADWOOD

2022-08-12 · CrowdStrike · Ioan Iacob, Iulian Madalin Ionita
The Anatomy of Wiper Malware, Part 1: Common Techniques
Apostle CaddyWiper DEADWOOD DistTrack DoubleZero DUSTMAN HermeticWiper IsaacWiper IsraBye KillDisk Meteor Olympic Destroyer Ordinypt Petya Sierra(Alfa,Bravo, ...) StoneDrill WhisperGate ZeroCleare

2021-09-30 · SentinelOne · Amitai Ben Shushan Ehrlich
New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education
Apostle

2021-05-27 · cyberpunkleigh · cyberpunkleigh
Apostle Ransomware Analysis
Apostle

2021-05-25 · SentinelOne · Amitai Ben Shushan Ehrlich

From Wiper to Ransomware: The Evolution of Agrius

Apostle DEADWOOD

There is no Yara-Signature yet.
