POOLRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:06:47 UTC

osx.poolrat (Back to overview)

POOLRAT

aka: SIMPLESEA, SIMPLETEA

Actor(s): Lazarus Group

There is no description at this point.

References

2025-12-18 · Acronis · Acronis Security
Acronis TRU Alliance {Hunt.io}: Hunting DPRK threats - New Global Lazarus & Kimsuky campaigns
BADCALL POOLRAT Quasar RAT

2023-10-04 · Virus Bulletin · Peter Kálnai
Lazarus Campaigns and Backdoors in 2022-23
SimpleTea POOLRAT 3CX Backdoor BLINDINGCAN CLOUDBURST DRATzarus ForestTiger ImprudentCook LambLoad LightlessCan miniBlindingCan PostNapTea SecondHandTea SnatchCrypto wAgentTea WebbyTea WinInetLoader

2023-04-20 · Mandiant · ADRIAN SANCHEZ, DANIEL SCOTT, Dimiter Andonov, Fred Plan, Jake Nicastro, JEFF JOHNSON, Marius Fodoreanu, RENATO FONTANA
3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible
POOLRAT IconicStealer UNC4736

2023-04-20 · 3CX · Agathocles Prodromou
Security Update Thursday 20 April 2023 – Initial Intrusion Vector Found
POOLRAT

2023-04-20 · ESET Research · Marc-Etienne M.Léveillé, Peter Kálnai
Linux malware strengthens links between Lazarus and the 3CX supply-chain attack

BADCALL SimpleTea POOLRAT 3CX Backdoor BADCALL IconicStealer

2021-02-18 · Symantec · Threat Hunter Team

Lazarus: Three North Koreans Charged for Financially Motivated Attacks

AppleJeus POOLRAT Unidentified macOS 001 (UnionCryptoTrader) AppleJeus Unidentified 077 (Lazarus Downloader)

2021-02-17 · US-CERT · CISA

Malware Analysis Report (AR21-048E): AppleJeus: CoinGoTrade

AppleJeus POOLRAT AppleJeus

There is no Yara-Signature yet.
