SEADADDY (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:38:53 UTC

win.seadaddy (Back to overview)

SEADADDY

aka: SeaDuke, Seadask

Actor(s): APT29

Backdoor written in Python 2, deployed with PyInstaller.

References

2020-07-14 · Cyborg Security · Austin Jackson
PYTHON MALWARE ON THE RISE
Poet RAT PyLocky SEADADDY

2017-02-20 · Contagio Dump · Mila Parkour
Part I. Russian APT - APT28 collection of samples including OSX XAgent
X-Agent Komplex Coreshell Downdelph HideDRV SEADADDY Sedreco Seduploader X-Agent XTunnel

2016-06-15 · CrowdStrike · Dmitri Alperovitch
Bears in the Midst: Intrusion into the Democratic National Committee
X-Agent ATI-Agent SEADADDY Seduploader X-Agent XTunnel APT28

2015-07-13 · Symantec · A L Johnson
“Forkmeiamfamous”: Seaduke, latest weapon in the Duke armory
SEADADDY

2014-07-15 · Palo Alto Networks Unit 42 · Josh Grunzweig
Unit 42 Technical Analysis: Seaduke
SEADADDY

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.seadaddy