TONESHELL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:39:54 UTC

win.toneshell (Back to overview)

TONESHELL

Actor(s): MUSTANG PANDA

There is no description at this point.

References

2025-09-11 · IBM X-Force · Golo Mühr, Joshua Chung
Hive0154, aka Mustang Panda, drops updated Toneshell backdoor and novel SnakeDisk USB worm
PUBLOAD SnakeDisk TONESHELL Yokai

2024-10-02 · ESET Research · Romain Dumont
Separating the bee from the panda: CeranaKeeper making a beeline for Thailand
PUBLOAD TONESHELL WavyExfiller CeranaKeeper

2024-09-03 · Hunt.io · Hunt.io
ToneShell Backdoor Used to Target Attendees of the IISS Defence Summit
TONESHELL

2024-08-23 · TEAMT5 · Still Hsu
Sailing the Seven SEAs: Deep Dive into Polaris' Arsenal and Intelligence Insights
Cobalt Strike Hodur PlugX TONESHELL

2024-01-23 · CSIRT-CTI · CSIRT-CTI
Stately Taurus Targets Myanmar Amidst Concerns over Military Junta’s Handling of Rebel Attacks
PlugX PUBLOAD TONESHELL

2023-09-22 · Palo Alto Networks Unit 42 · Lior Rochberger, Robert Falcone, Tom Fakterman
Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda
Cobalt Strike MimiKatz RemCom ShadowPad TONESHELL

2023-09-07 · Sekoia · Jamila B.
My Tea’s not cold. An overview of China’s cyber threat
Melofee PingPull SoWaT Sword2033 MgBot MQsTTang PlugX TONESHELL Dalbit MirrorFace

2022-11-18 · Trend Micro · Nick Dai, Sunny Lu, Vickie Su

Earth Preta Spear-Phishing Governments Worldwide

PUBLOAD TONESHELL MUSTANG PANDA

There is no Yara-Signature yet.
