POISONPLUG (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:57:46 UTC

win.poisonplug (Back to overview)

POISONPLUG

aka: Barlaiy

Actor(s): APT41

According to FireEye, POISONPLUG is a highly obfuscated modular backdoor with plug-in capabilities. The malware is capable of registry or service persistence, self-removal, plug-in execution, and network connection forwarding. POISONPLUG has been observed using social platforms to host encoded C&C commands.

References

2025-01-29 · Google · Conor Quigley, Luke Jenkins, Nino Isakovic
ScatterBrain: Unmasking the Shadow of PoisonPlug's Obfuscator
POISONPLUG ShadowPad SNAPPYBEE

2020-11-03 · Kaspersky Labs · GReAT
APT trends report Q3 2020
WellMail EVILNUM Janicab Poet RAT AsyncRAT Ave Maria Cobalt Strike Crimson RAT CROSSWALK Dtrack LODEINFO MoriAgent Okrum PlugX POISONPLUG Rover ShadowPad SoreFang Winnti

2020-09-18 · Symantec · Threat Hunter Team
APT41: Indictments Put Chinese Espionage Group in the Spotlight
CROSSWALK PlugX POISONPLUG ShadowPad Winnti

2019-12-12 · FireEye · Chi-en Shen, Oleg Bondarenko
Cyber Threat Landscape in Japan – Revealing Threat in the Shadow
Cerberus TSCookie Cobalt Strike Dtrack Emotet Formbook IcedID Icefog IRONHALO Loki Password Stealer (PWS) PandaBanker PLEAD POISONPLUG TrickBot BlackTech

2019-11-19 · FireEye · Kelli Vanderlee, Nalani Fraser
Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions

MESSAGETAP TSCookie ACEHASH CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT HIGHNOON HTran MimiKatz NetWire RC POISONPLUG Poison Ivy pupy Quasar RAT ZXShell

2019-10-15 · FireEye · Tobias Krueger

LOWKEY: Hunting for the Missing Volume Serial ID

LOWKEY POISONPLUG

2019-08-09 · FireEye · FireEye

Double Dragon APT41, a dual espionage and cyber crime operation

CLASSFON crackshot CROSSWALK GEARSHIFT HIGHNOON HIGHNOON.BIN JUMPALL POISONPLUG Winnti

There is no Yara-Signature yet.

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