KEYPLUG (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:23:00 UTC

KEYPLUG

aka: ELFSHELF

Actor(s): APT41

There is no description at this point.

References

2025-01-23 · Hunt.io ·
Mapping Suspected KEYPLUG Infrastructure: TLS Certificates, GhostWolf, and RedGolf/APT41 Activity
KEYPLUG

2024-09-24 · Virus Bulletin · Aragorn Tseng, Chi-Yu You, Cristiana Brafman Kittner, Steve Su
Down the GRAYRABBIT HOle - Exposing UNC3569 and its Modus Operandi
KEYPLUG Cobalt Strike CROSSWALK GRAYRABBIT HelloBot HUI Loader PlugX SiestaGraph

2024-05-21 · Yoroi · Carmelo Ragusa, Luigi Martire
Uncovering an undetected KeyPlug implant attacking industries in Italy
KEYPLUG

2023-12-11 · Sentinel LABS · Aleksandar Milenkoski, Bendik Hagen
Sandman APT | China-Based Adversaries Embrace Lua
KEYPLUG LuaDream

2023-03-30 · Recorded Future · Insikt Group
With KEYPLUG, China’s RedGolf Spies On, Steals From Wide Field of Targets
KEYPLUG Cobalt Strike PlugX RedGolf

2022-05-12 · TEAMT5 · Leon Chang, Silvia Yeh
The Next Gen PlugX/ShadowPad? A Dive into the Emerging China-Nexus Modular Trojan, Pangolin8RAT (slides)
KEYPLUG Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad Winnti SLIME29 TianWu

2022-03-28 · Mandiant · Brandon Wilbur, Dallin Warne, Geoff Ackerman, James Maclachlan, John Wolfram, Tufail Ahmed
Forged in Fire: A Survey of MobileIron Log4Shell Exploitation
KEYPLUG

2022-03-08 · Mandiant · Douglas Bienstock, Geoff Ackerman, John Wolfram, Rufus Brown, Van Ta
Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments
KEYPLUG Cobalt Strike LOWKEY

2022-03-08 · Twitter (@CyberJack42) · CyberJack
Tweet on ELFSHELF alias for KEYPLUG
KEYPLUG

2022-02-26 · Mandiant · Mandiant
TRENDING EVIL Q1 2022
KEYPLUG FAKEUPDATES GootLoader BazarBackdoor QakBot

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/elf.keyplug