FiveHands (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:51:50 UTC

FiveHands

aka: Thieflock

Actor(s): [Unnamed group]

There is no description at this point.

References

2022-09-06 · CISA · CISA, FBI, MS-ISAC, US-CERT
Alert (AA22-249A) #StopRansomware: Vice Society
Cobalt Strike Empire Downloader FiveHands HelloKitty SystemBC Zeppelin

2022-08-30 · eSentire · eSentire Threat Response Unit (TRU)
Hacker Infrastructure Used in Cisco Breach Discovered Attacking a Top Workforce Management Corporation & an Affiliate of Russia's Evil Corp Gang Suspected, Reports eSentire
Cobalt Strike FiveHands UNC2447

2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT

2022-03-21 · eSentire · eSentire Threat Response Unit (TRU)
Conti Affiliate Exposed: New Domain Names, IP Addresses and Email Addresses Uncovered
HelloKitty BazarBackdoor Cobalt Strike Conti FiveHands HelloKitty IcedID

2021-11-30 · Bleeping Computer · Ionut Ilascu
Yanluowang ransomware operation matures with experienced affiliates
FiveHands

2021-11-30 · Symantec · Symantec Threat Hunter Team
Yanluowang: Further Insights on New Ransomware Threat
BazarBackdoor Cobalt Strike FiveHands

2021-08-15 · Symantec · Threat Hunter Team
The Ransomware Threat
Babuk BlackMatter DarkSide Avaddon Babuk BADHATCH BazarBackdoor BlackMatter Clop Cobalt Strike Conti DarkSide DoppelPaymer Egregor Emotet FiveHands FriedEx Hades IcedID LockBit Maze MegaCortex MimiKatz QakBot RagnarLocker REvil Ryuk TrickBot WastedLocker

2021-06-28 · CrowdStrike · Alexandru Ghita
New Ransomware Variant Uses Golang Packer
FiveHands HelloKitty

2021-06-15 · NCC Group · Michael Matthews, NCC RIFT, William Backhouse
Handy guide to a new Fivehands ransomware variant
FiveHands

2021-05-06 · CISA · CISA
Analysis Report: FiveHands Ransomware
FiveHands

2021-05-06 · CISA · CISA
MAR-10324784-1.v1: FiveHands Ransomware
FiveHands

2021-05-03 · Rewterz Information Security · Rewterz Information Security
Rewterz Threat Alert – Financially Motivated Aggressive Group Carrying Out Ransomware Campaigns – Active IOCs
FiveHands SombRAT UNC2447

2021-04-29 · FireEye · Justin Moore, Raymond Leong, Tyler McLellan
UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat
Cobalt Strike FiveHands HelloKitty

There is no Yara-Signature yet.
