Hades (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:37:18 UTC

According to PCrisk, Hades Locker is an updated version of WildFire Locker ransomware that infiltrates systems and encrypts a variety of data types using AES encryption. Hades Locker appends the names of encrypted files with the ".~HL[5_random_characters] (first 5 characters of encryption password)" extension.

2025-01-17 · Google Cloud Security · Office of the CISO
Threat Horizons - H1 2025 Threat Horizons Report
FAKEUPDATES Conti Hades LockBit Phoenix Locker RansomHub TRIPLESTRENGTH 2022-06-13 · Jorge Testa · Jorge Testa
Killing The Bear - Evil Corp
FAKEUPDATES Babuk Blister DoppelPaymer Dridex Entropy FriedEx Hades Macaw Phoenix Locker WastedLoader WastedLocker 2022-06-02 · Mandiant · Mandiant Intelligence
To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions
FAKEUPDATES Blister Cobalt Strike DoppelPaymer Dridex FriedEx Hades LockBit Macaw MimiKatz Phoenix Locker WastedLocker 2022-02-01 · Sentinel LABS · Antonio Pirozzi, Antonis Terefos, Idan Weizman
Sanctions be Damned | From Dridex To Macaw, The Evolution of Evil Corp
Dridex FriedEx Hades Phoenix Locker WastedLocker 2021-10-22 · HUNT & HACKETT · Krijn de Mik
Advanced IP Scanner: the preferred scanner in the A(P)T toolbox
Conti DarkSide Dharma Egregor Hades REvil Ryuk 2021-09-14 · CrowdStrike · CrowdStrike Intelligence Team
Big Game Hunting TTPs Continue to Shift After DarkSide Pipeline Attack
BlackMatter DarkSide REvil Avaddon BlackMatter Clop Conti CryptoLocker DarkSide DoppelPaymer Hades REvil 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 2021-06-30 · Advanced Intelligence · AdvIntel Security & Development Team, Brandon Rudisel, Yelisey Boguslavskiy
Ransomware-&-CVE: Industry Insights Into Exclusive High-Value Target Adversarial Datasets
BlackKingdom Ransomware Clop dearcry Hades REvil 2021-06-29 · Accenture · Accenture Security
HADES ransomware operators continue attacks
Cobalt Strike Hades MimiKatz 2021-06-15 · Secureworks · Counter Threat Unit ResearchTeam
Hades Ransomware Operators Use Distinctive Tactics and Infrastructure
Cobalt Strike Hades 2021-05-10 · DarkTracer · DarkTracer
Intelligence Report on Ransomware Gangs on the DarkWeb: List of victim organizations attacked by ransomware gangs released on the DarkWeb
RansomEXX Avaddon Babuk Clop Conti Cuba DarkSide DoppelPaymer Egregor Hades LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker Nefilim Nemty Pay2Key PwndLocker RagnarLocker Ragnarok

RansomEXX REvil Sekhmet SunCrypt ThunderX 2021-05-05 · TRUESEC · Mattias Wåhlén

Are The Notorious Cyber Criminals Evil Corp actually Russian Spies?

Cobalt Strike Hades WastedLocker 2021-04-12 · Twitter (@inversecos) · inversecos

Tweet on TTPs associated with Hades Ransomware

Hades 2021-03-26 · Accenture · Eric Welling, Jeff Beley, Ryan Leininger

It's getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims

Hades 2021-03-25 · Bleeping Computer · Sergiu Gatlan

Evil Corp switches to Hades ransomware to evade sanctions

Hades WastedLocker 2021-03-01 · AWAKE · Jason Bevis

The Unseen One: Hades Ransomware Gang or Hafnium

Hades 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD WINTER

Cobalt Strike Hades Meterpreter GOLD WINTER

There is no Yara-Signature yet.
