HelloKitty (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 03:24:49 UTC

Unit42 states that HelloKitty is a ransomware family that first surfaced at the end of 2020, primarily targeting Windows systems. The malware family got its name due to its use of a Mutex with the same name: HelloKittyMutex. The ransomware samples seem to evolve quickly and frequently, with different versions making use of the .crypted or .kitty file extensions for encrypted files. Some newer samples make use of a Golang packer that ensures the final ransomware code is only loaded in memory, most likely to evade detection by security solutions.

2023-12-13 · cocomelonc · cocomelonc
Malware in the wild book
AsyncRAT Babuk BlackCat BlackLotus Carbanak HelloKitty Paradise Stealc WinDealer 2023-02-14 · Intrinsec · CTI Intrinsec, Intrinsec
Vice-Society spreads its own ransomware
HelloKitty PolyVice Zeppelin 2023-01-04 · cocomelonc
Malware development tricks: part 26. Mutex. C++ example.
AsyncRAT Conti HelloKitty 2022-09-20 · vmware · Dana Behling
Threat Report: Illuminating Volume Shadow Deletion
Conti HelloKitty 2022-09-06 · CISA · CISA, FBI, MS-ISAC, US-CERT
Alert (AA22-249A) #StopRansomware: Vice Society
Cobalt Strike Empire Downloader FiveHands HelloKitty SystemBC Zeppelin 2022-05-20 · AdvIntel · Marley Smith, Vitali Kremez, Yelisey Boguslavskiy
DisCONTInued: The End of Conti’s Brand Marks New Chapter For Cybercrime Landscape
AvosLocker Black Basta BlackByte BlackCat Conti HelloKitty Hive 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 2022-05-01 · BushidoToken · BushidoToken
Gamer Cheater Hacker Spy
Egregor HelloKitty NetfilterRootkit RagnarLocker Winnti 2022-04-25 · Medium proferosec-osm · Brenton Morris
Static unpacker and decoder for Hello Kitty Packer
HelloKitty 2022-04-18 · AdvIntel · Vitali Kremez, Yelisey Boguslavskiy
Enter KaraKurt: Data Extortion Arm of Prolific Ransomware Group
AvosLocker BazarBackdoor BlackByte BlackCat Cobalt Strike HelloKitty Hive Karakurt 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 2021-11-02 · SpearTip · Chris Swagler

FBI Warning: HelloKitty Ransomware Add DDoS to Extortion Arsenal

HelloKitty 2021-10-28 · FBI · FBI

CU-000154-MW: Tactics, Techniques, and Indicators of Compromise Associated with Hello Kitty/FiveHands Ransomware

HelloKitty 2021-08-24 · Palo Alto Networks Unit 42 · Doel Santos, Ruchna Nigam

Ransomware Groups to Watch: Emerging Threats

HelloKitty AvosLocker HelloKitty Hive LockBit 2021-07-17 · Bleeping Computer · Sergiu Gatlan

HelloKitty ransomware is targeting vulnerable SonicWall devices

HelloKitty 2021-06-28 · CrowdStrike · Alexandru Ghita

New Ransomware Variant Uses Golang Packer

FiveHands HelloKitty 2021-05-31 · DataBreaches.net · Dissent

Babuk re-organizes as Payload Bin, offers its first leak

Babuk HelloKitty 2021-04-29 · FireEye · Justin Moore, Raymond Leong, Tyler McLellan

UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat

Cobalt Strike FiveHands HelloKitty 2021-03-18 · Malwarebytes · Jovi Umawing

HelloKitty: When Cyberpunk met cy-purr-crime

HelloKitty 2021-03-08 · Sentinel LABS · Jim Walter

HelloKitty Ransomware Lacks Stealth, But Still Strikes Home

HelloKitty 2021-02-10 · Cado Security · Christopher Doman

Punk Kitty Ransom - Analysing HelloKitty Ransomware Attacks

HelloKitty 2021-02-09 · Twitter (@fwosar) · Fabian Wosar

Tweet on CD PROJEKT RED targeted by HelloKitty ransomware group

HelloKitty 2020-11-13 · ID Ransomware · Andrew Ivanov

HelloKitty Ransomware

HelloKitty

▶ [TLP:WHITE] win_hellokitty_auto (20251219 | Detects win.hellokitty.)
