Hancitor (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:42:00 UTC

Hancitor(aka Chanitor) emerged in 2013 which spread via social engineering techniques mainly through phishing mails embedded with malicious link and weaponized Microsoft office document contains malicious macro in it.

2022-08-17 · Group-IB ·
Switching side jobs Links between ATMZOW JS-sniffer and Hancitor
Hancitor 2022-02-12 · muha2xmad · Muhammad Hasan Ali
Full Hancitor malware analysis
Hancitor 2022-01-08 · muha2xmad · Muhammad Hasan Ali
Unpacking Hancitor malware
Hancitor 2021-12-31 · 0ffset Blog · Chuong Dong
HANCITOR: Analysing The Main Loader
Hancitor 2021-12-28 · Medium Crovax · Crovax
Extracting Hancitor's Configuration with Ghidra part 1
Hancitor 2021-11-23 · 0ffset Blog · Chuong Dong
HANCITOR: Analysing The Malicious Document
Hancitor 2021-11-01 · The DFIR Report · @iiamaleks, @samaritan_o
From Zero to Domain Admin
Cobalt Strike Hancitor 2021-10-04 · Github (OALabs) · OALabs
Reverse engineered the Hancitor DLL and built a static config extractor
Hancitor 2021-10-04 · pid4.io · James Hovious
How to Write a Hancitor Extractor in Go
Hancitor 2021-09-29 · Malware Traffic Analysis · Brad Duncan
2021-09-29 (Wednesday) - Hancitor with Cobalt Strike
Cobalt Strike Hancitor 2021-09-29 · Malware Traffic Analysis · Brad Duncan
Hancitor with Cobalt Strike
Cobalt Strike Hancitor 2021-09-09 · Cyber-Anubis · Nidal Fikri
Hancitor Loader | RE & Config Extraction
Hancitor 2021-08-05 · Group-IB · Nikita Rostovcev, Viktor Okorokov
Prometheus TDS The key to success for Campo Loader, Hancitor, IcedID, and QBot
Prometheus Backdoor Buer campoloader Hancitor IcedID QakBot 2021-07-20 · VMRay · Mateusz Lukaszewski
Hancitor's Multi-Step Delivery Process
Hancitor 2021-07-09 · InfoSec Handlers Diary Blog · Brad Duncan
Hancitor tries XLL as initial malware file
Cobalt Strike Hancitor 2021-07-08 · McAfee · McAfee Labs
Hancitor Making Use of Cookies to Prevent URL Scraping
Hancitor 2021-06-28 · The DFIR Report · The DFIR Report

Hancitor Continues to Push Cobalt Strike

Cobalt Strike Hancitor 2021-06-21 · Medium elis531989 · Eli Salem

Dissecting and automating Hancitor’s config extraction

Hancitor 2021-06-17 · Binary Defense · Brandon George

Analysis of Hancitor – When Boring Begets Beacon

Cobalt Strike Ficker Stealer Hancitor 2021-05-19 · Intel 471 · Intel 471

Look how many cybercriminals love Cobalt Strike

BazarBackdoor Cobalt Strike Hancitor QakBot SmokeLoader SystemBC TrickBot 2021-05-07 · Group-IB · Oleg Skulkin, Semyon Rogachev

Connecting the Bots Hancitor fuels Cuba Ransomware Operations

Cuba Hancitor 2021-04-16 · InQuest · Dmitry Melikov

Unearthing Hancitor Infrastructure

Hancitor 2021-04-07 · Palo Alto Networks Unit 42 · Brad Duncan

Wireshark Tutorial: Examining Traffic from Hancitor Infections

Hancitor 2021-04-01 · Palo Alto Networks Unit 42 · Brad Duncan

Hancitor’s Use of Cobalt Strike and a Noisy Network Ping Tool

Cobalt Strike Hancitor Moskalvzapoe 2021-02-11 · Twitter (@TheDFIRReport) · The DFIR Report

Tweet on Hancitor Activity followed by cobaltsrike beacon

Cobalt Strike Hancitor 2021-02-01 · Silent Push · Martijn Grooten

Pivoting: finding malware domains without seeing malicious activity

Hancitor 2021-01-13 · InfoSec Handlers Diary Blog · Brad Duncan

Hancitor activity resumes after a hoilday break

Hancitor 2021-01-10 · Medium walmartglobaltech · Jason Reaves

MAN1, Moskal, Hancitor and a side of Ransomware

Cobalt Strike Hancitor SendSafe VegaLocker Moskalvzapoe 2019-11-01 · Dodge This Security · Dodge This Security

Hancitor. Evasive new waves, and how COM objects can use Cached Credentials for Proxy Authentication

Hancitor 2019-05-01 · Felix Weyne

Hancitor's Packer Damystified

Hancitor 2018-11-05 · Vitali Kremez

Let's Learn: In-Depth Reversing of Hancitor Dropper/Loader: 2016 vs 2018 Malware Progression

Hancitor 2018-02-27 · Palo Alto Networks Unit 42 · Jeff White

Dissecting Hancitor’s Latest 2018 Packer

Hancitor 2018-02-07 · Palo Alto Networks Unit 42 · Brad Duncan, Vicky Ray

Compromised Servers & Fraud Accounts: Recent Hancitor Attacks

Hancitor 2016-09-23 · FireEye · Ankit Anubhav, Dileep Kumar Jallepalli

Hancitor (AKA Chanitor) observed using multiple attack approaches

Hancitor 2016-08-22 · Palo Alto Networks Unit 42 · Jeff White

VB Dropper and Shellcode for Hancitor Reveal New Techniques Behind Uptick

Hancitor 2016-08-19 · Minerva Labs · Minerva Labs Research Team

New Hancitor Malware: Pimp my Downloaded

Hancitor 2016-07-12 · Fidelis Cybersecurity · Threat Research Team

Me and Mr. Robot: Tracking the Actor Behind the MAN1 Crypter

Hancitor Vawtrak 2016-05-12 · Proofpoint · Axel F, Matthew Mesa

Hancitor and Ruckguv Reappear, Updated and With Vawtrak On Deck

Hancitor Ruckguv 2015-01-09 · Zscaler · Zscaler

Chanitor Downloader Actively Installing Vawtrak

Hancitor

▶ [TLP:WHITE] win_hancitor_auto (20251219 | Detects win.hancitor.)
