HermeticWiper (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:38:51 UTC

HermeticWiper

aka: DriveSlayer, FoxBlade, KillDisk.NCV, NEARMISS

VTCollection

According to SentinelLabs, HermeticWiper is a custom-written application with very few standard functions. It abuses a signed driver called "empntdrv.sys" which is associated with the legitimate Software "EaseUS Partition Master Software" to enumerate the MBR and all partitions of all Physical Drives connected to the victims Windows Device and overwrite the first 512 Bytes of every MBR and Partition it can find, rendering them useless. This malware is associated to the malware attacks against Ukraine during Russians Invasion in February 2022.

References

2024-04-16 · Mandiant · Alden Wahlstrom, Anton Prokopenkov, Dan Black, Dan Perez, Gabby Roncone, John Wolfram, Lexie Aytes, Nick Simonian, Ryan Hall, Tyler McLellan
APT44: Unearthing Sandworm
VPNFilter BlackEnergy CaddyWiper EternalPetya HermeticWiper Industroyer INDUSTROYER2 Olympic Destroyer PartyTicket RoarBAT Sandworm

2023-04-18 · Mandiant · Mandiant
M-Trends 2023
QUIETEXIT AppleJeus Black Basta BlackCat CaddyWiper Cobalt Strike Dharma HermeticWiper Hive INDUSTROYER2 Ladon LockBit Meterpreter PartyTicket PlugX QakBot REvil Royal Ransom SystemBC WhisperGate

2023-03-15 · Microsoft · Microsoft Threat Intelligence
A year of Russian hybrid warfare in Ukraine
CaddyWiper DesertBlade DoubleZero HermeticWiper INDUSTROYER2 IsaacWiper PartyTicket SwiftSlicer WhisperGate

2023-02-24 · Twitter (@Sebdraven) · Sébastien Larinier
Tweet on IOCTL manipulation in TDL4 and HermeticWiper
Alureon HermeticWiper

2023-02-15 · Google · Google Threat Analysis Group, Mandiant
Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape

CaddyWiper Dharma HermeticWiper INDUSTROYER2 PartyTicket WhisperGate Callisto Curious Gorge MUSTANG PANDA Turla

2022-12-03 · Microsoft · Cliff Watts

Preparing for a Russian cyber offensive against Ukraine this winter

CaddyWiper HermeticWiper Prestige

2022-10-24 · Youtube (Virus Bulletin) · Alexander Adamov

Russian wipers in the cyberwar against Ukraine

AcidRain CaddyWiper DesertBlade DoubleZero EternalPetya HermeticWiper HermeticWizard INDUSTROYER2 IsaacWiper KillDisk PartyTicket WhisperGate

2022-09-26 · CrowdStrike · Ioan Iacob, Iulian Madalin Ionita

The Anatomy of Wiper Malware, Part 3: Input/Output Controls

CaddyWiper DEADWOOD DistTrack DoubleZero DUSTMAN HermeticWiper IsaacWiper Meteor Petya Sierra(Alfa,Bravo, ...) StoneDrill WhisperGate ZeroCleare

2022-08-18 · Trustwave · Pawel Knapczyk

Overview of the Cyber Weapons Used in the Ukraine - Russia War

AcidRain CaddyWiper Cobalt Strike CredoMap DCRat DoubleZero GraphSteel GrimPlant HermeticWiper INDUSTROYER2 InvisiMole IsaacWiper PartyTicket

2022-08-18 · Trustwave · Pawel Knapczyk

Overview of the Cyber Weapons Used in the Ukraine - Russia War

AcidRain CaddyWiper Cobalt Strike CredoMap DCRat DoubleZero GraphSteel GrimPlant HermeticWiper INDUSTROYER2 InvisiMole IsaacWiper PartyTicket

2022-08-12 · CrowdStrike · Ioan Iacob, Iulian Madalin Ionita

The Anatomy of Wiper Malware, Part 1: Common Techniques

Apostle CaddyWiper DEADWOOD DistTrack DoubleZero DUSTMAN HermeticWiper IsaacWiper IsraBye KillDisk Meteor Olympic Destroyer Ordinypt Petya Sierra(Alfa,Bravo, ...) StoneDrill WhisperGate ZeroCleare

2022-06-06 · Trellix · Trelix

Growling Bears Make Thunderous Noise

Cobalt Strike HermeticWiper WhisperGate NB65

2022-06-02 · Eclypsium · Eclypsium

Conti Targets Critical Firmware

Conti HermeticWiper TrickBot WhisperGate

2022-05-19 · Mandiant · Alden Wahlstrom, Alice Revelli, David Mainor, Ryan Serabian, Sam Riddell

The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine

HermeticWiper PartyTicket

2022-05-02 · AT&T · Fernando Martinez
Analysis on recent wiper attacks: examples and how wiper malware works
AcidRain CaddyWiper DoubleZero HermeticWiper INDUSTROYER2 IsaacWiper

2022-04-28 · Fortinet · Gergely Revay
An Overview of the Increasing Wiper Malware Threat
AcidRain CaddyWiper DistTrack DoubleZero EternalPetya HermeticWiper IsaacWiper Olympic Destroyer Ordinypt WhisperGate ZeroCleare

2022-04-27 · Microsoft · Microsoft Digital Security Unit (DSU)
Special Report: Ukraine An overview of Russia’s cyberattack activity in Ukraine
CaddyWiper DoubleZero HermeticWiper INDUSTROYER2 IsaacWiper PartyTicket WhisperGate

2022-04-07 · InQuest · Nick Chalard, Will MacArthur
Ukraine CyberWar Overview
CyclopsBlink Cobalt Strike GraphSteel GrimPlant HermeticWiper HermeticWizard MicroBackdoor PartyTicket Saint Bot Scieron WhisperGate

2022-03-25 · GOV.UA · State Service of Special Communication and Information Protection of Ukraine (CIP)
Who is behind the Cyberattacks on Ukraine's Critical Information Infrastructure: Statistics for March 15-22
Xloader Agent Tesla CaddyWiper Cobalt Strike DoubleZero GraphSteel GrimPlant HeaderTip HermeticWiper IsaacWiper MicroBackdoor Pandora RAT

2022-03-24 · NextGov · Brandi Vincent
Ukrainian Cyber Lead Says ‘At Least 4 Types of Malware’ in Use to Target Critical Infrastructure and Humanitarian Aid
CaddyWiper DoubleZero HermeticWiper IsaacWiper

2022-03-21 · eSentire · eSentire
eSentire Threat Intelligence Malware Analysis: HermeticWiper & PartyTicket
HermeticWiper PartyTicket

2022-03-17 · Blackberry · BlackBerry Research & Intelligence Team
Threat Thursday: HermeticWiper Targets Defense Sectors in Ukraine
HermeticWiper

2022-03-14 · Kaspersky · GReAT
Webinar on cyberattacks in Ukraine – summary and Q&A
HermeticWiper HermeticWizard IsaacWiper PartyTicket WhisperGate

2022-03-11 · Bitdefender · Radu Crahmaliuc
Five Things You Need to Know About the Cyberwar in Ukraine
HermeticWiper WhisperGate

2022-03-11 · Security Boulevard · Teri Robinson
IsaacWiper Followed HermeticWiper Attack on Ukraine Orgs

HermeticWiper IsaacWiper

2022-03-10 · BrightTALK (Kaspersky GReAT) · Costin Raiu, Dan Demeter, Ivan Kwiatkowski, Kurt Baumgartner, Marco Preuss

BrightTALK: A look at current cyberattacks in Ukraine

HermeticWiper HermeticWizard IsaacWiper PartyTicket WhisperGate

2022-03-10 · splunk · Splunk Threat Research Team

Detecting HermeticWiper

HermeticWiper PartyTicket

2022-03-10 · Brandefense · Brandefense

HermeticWiper - Technical Analysis Report

HermeticWiper

2022-03-04 · Github (eln0ty) · Abdallah Elnoty

HermeticWiper/FoxBlade Analysis (in-depth)

HermeticWiper

2022-03-04 · Malwarebytes · Malwarebytes Threat Intelligence

HermeticWiper: A detailed analysis of the destructive malware that targeted Ukraine

HermeticWiper

2022-03-04 · vmware · Giovanni Vigna, Oleg Boyarchuk, Stefano Ortolani, Threat Analysis Unit

Hermetic Malware: Multi-component Threat Targeting Ukraine Organizations

HermeticWiper

2022-03-04 · Mandiant · James Sadowski, Ryan Hall

Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation

HermeticWiper PartyTicket WhisperGate

2022-03-03 · Trend Micro · Trend Micro Research

IOC Resource for Russia-Ukraine Conflict-Related Cyberattacks

ClipBanker Conti HermeticWiper PartyTicket WhisperGate

2022-03-03 · LIFARS · LIFARS

A Closer Look at the Russian Actors Targeting Organizations in Ukraine

HermeticWiper IsaacWiper Saint Bot WhisperGate

2022-03-03 · Cloudsek · Anandeshwar Unnikrishnan, Deepanjli Paulraj

Technical Analysis of The Hermetic Wiper Malware Used to Target Ukraine

HermeticWiper

2022-03-03 · · YouTube (MBSD) · MBSD

Infection and explanation of "Hermetic Wiper", a destructive malware targeting Ukraine

HermeticWiper

2022-03-02 · Recorded Future · Insikt Group
HermeticWiper and PartyTicket Targeting Computers in Ukraine
HermeticWiper PartyTicket

2022-03-02 · Trellix · Max Kersten
Digging into HermeticWiper
HermeticWiper

2022-03-01 · Kaspersky Labs · Kaspersky
Ransomware as a distraction
HermeticWiper PartyTicket

2022-03-01 · Elastic · Andrew Pease, Cyril François, Daniel Stepanic, Github (@1337-42), Github (@ayfaouzi), Github (@jtnk), Mark Mager, Samir Bousseaden
Elastic protects against data wiper malware targeting Ukraine: HERMETICWIPER
HermeticWiper

2022-03-01 · Threat Post · Lisa Vaas
Ukraine Hit with Novel ‘FoxBlade’ Trojan Hours Before Invasion
HermeticWiper

2022-03-01 · DeepInstinct · Ido Kringel
What is HermeticWiper – An Analysis of the Malware and Larger Threat Landscape in the Russian Ukrainian War
HermeticWiper

2022-03-01 · ESET Research · ESET Research
IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine
HermeticWiper IsaacWiper PartyTicket

2022-03-01 · Qualys · Mayuresh Dani
Ukrainian Targets Hit by HermeticWiper, New Datawiper Malware
HermeticWiper

2022-03-01 · Marco Ramilli's Blog · Marco Ramilli
DiskKill/HermeticWiper and NotPetya (Dis)similarities
EternalPetya HermeticWiper

2022-02-28 · Microsoft · MSRC Team
Cyber threat activity in Ukraine: analysis and resources
CaddyWiper DesertBlade DoubleZero HermeticWiper INDUSTROYER2 IsaacWiper PartyTicket WhisperGate DEV-0586

2022-02-28 · Trellix · Taylor Mullins
Trellix Global Defenders: Cyberattacks Targeting Ukraine and HermeticWiper Protections
HermeticWiper

2022-02-28 · ZDNet · Jonathan Greig
Microsoft finds FoxBlade malware on Ukrainian systems, removes RT from Windows app store
HermeticWiper

2022-02-28 · Microsoft · MSRC Team
Cyber threat activity in Ukraine: analysis and resources
HermeticWiper IsaacWiper PartyTicket WhisperGate

2022-02-28 · Microsoft Sentinel 101 · mzorich
Detecting malware kill chains with Defender and Microsoft Sentinel
HermeticWiper

2022-02-26 · Yoroi · Carmelo Ragusa, Luca Mella, Luigi Martire
DiskKill/HermeticWiper, a disruptive cyber-weapon targeting Ukraine’s critical infrastructures
HermeticWiper

2022-02-26 · CISA
Alert (AA22-057A) Destructive Malware Targeting Organizations in Ukraine
HermeticWiper WhisperGate

2022-02-26 · CISA · CISA, FBI
Destructive Malware Targeting Organizations in Ukraine
HermeticWiper WhisperGate

2022-02-25 · The Hacker News · Ravie Lakshmanan
Putin Warns Russian Critical Infrastructure to Brace for Potential Cyber Attacks
HermeticWiper WhisperGate

2022-02-25 · Twitter (@fr0gger) · Thomas Roccia
Tweets with an overview of HermeticWiper
HermeticWiper

2022-02-25 · SOCRadar · SOCRadar
What You Need to Know About Russian Cyber Escalation in Ukraine
Mirai HermeticWiper

2022-02-25 · CyberPeace Institute
UKRAINE: Timeline of Cyberattacks
VPNFilter EternalPetya HermeticWiper WhisperGate

2022-02-25 · Secureworks · Counter Threat Unit ResearchTeam
Disruptive HermeticWiper Attacks Targeting Ukrainian Organizations
HermeticWiper

2022-02-25 · Deutsche Gesellschaft für Cybersicherheit · Deutsche Gesellschaft für Cybersicherheit (DGC)
Breaking news! Warning about “HermeticWiper Malware” by Russian APT Groups
HermeticWiper

2022-02-25 · EnglertOne · Thomas Englert
Reverse Engineering | Hermetic Wiper
HermeticWiper

2022-02-25 · CrowdStrike · Adrian Liviu Arsene, Farid Hendi, william thomas
CrowdStrike Falcon Protects from New Wiper Malware Used in Ukraine Cyberattacks
HermeticWiper

2022-02-24 · RiskIQ · RiskIQ
RiskIQ: HermeticWiper Compromised Server Used in Attack Chain
HermeticWiper

2022-02-24 · IBM · Anne Jobmann, Christopher Del Fierro, Claire Zaboeva, John Dwyer, Richard Emerson
IBM Security X-Force Research Advisory: New Destructive Malware Used In Cyber Attacks on Ukraine
HermeticWiper

2022-02-24 · Zscaler · Deepen Desai
HermeticWiper & resurgence of targeted attacks on Ukraine
HermeticWiper

2022-02-24 · ESET Research · welivesecurity
HermeticWiper: New data-wiping malware hits Ukraine
HermeticWiper

2022-02-24 · · t3n · Elisabeth Urban
Cyber-Attacken auf die Ukraine: Wiper-Malware befällt „Hunderte Computer“
HermeticWiper

2022-02-24 · Tesorion · TESORION
Report OSINT: Russia/ Ukraine Conflict Cyberaspect
Mirai VPNFilter BlackEnergy EternalPetya HermeticWiper Industroyer WhisperGate

2022-02-24 · Cluster25
Ukraine: Analysis Of The New Disk-Wiping Malware (HermeticWiper)
HermeticWiper

2022-02-24 · nviso · Michel Coene
Threat Update – Ukraine & Russia conflict
EternalPetya GreyEnergy HermeticWiper Industroyer KillDisk WhisperGate

2022-02-24 · Symantec · Symantec Threat Hunter Team
Ukraine: Disk-wiping Attacks Precede Russian Invasion
HermeticWiper

2022-02-23 · Sentinel LABS · Juan Andrés Guerrero-Saade
HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine
HermeticWiper

2022-02-23 · The Hacker News · Ravie Lakshmanan
New Wiper Malware Targeting Ukraine Amid Russia's Military Operation
HermeticWiper

2022-02-23 · Twitter (@threatintel) · Symantec Threat Intelligence
Tweet on new wiper malware being used in attacks on Ukraine
HermeticWiper

2022-02-23 · The Record · Catalin Cimpanu
Second data wiper attack hits Ukraine computer networks
HermeticWiper WhisperGate

2022-02-22 · Palo Alto Networks Unit 42 · Unit 42
Russia-Ukraine Crisis: How to Protect Against the Cyber Impact
HermeticWiper

Yara Rules

▶ [TLP:WHITE] win_hermeticwiper_auto (20251219 | Detects win.hermeticwiper.)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.hermeticwiper