PartyTicket (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:08:57 UTC

PartyTicket is a Go-written ransomware, which was described as a poorly designed one by Zscaler. According to Brett Stone-Gross this malware is likely intended to be a diversion from the Hermetic wiper (aka. KillDisk.NCV, DriveSlayer) attack.

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 ·
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 2023-02-15 · 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 2022-10-24 · Youtube (Virus Bulletin) · Alexander Adamov
Russian wipers in the cyberwar against Ukraine
AcidRain CaddyWiper DesertBlade DoubleZero EternalPetya HermeticWiper HermeticWizard INDUSTROYER2 IsaacWiper KillDisk PartyTicket WhisperGate 2022-08-18 · 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 2022-05-19 · Mandiant · Alden Wahlstrom, Alice Revelli, David Mainor, Ryan Serabian, Sam Riddell
The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine
HermeticWiper PartyTicket 2022-05-11 · Kaspersky · GReAT
New ransomware trends in 2022
BlackCat Conti DEADBOLT DoubleZero LockBit PartyTicket StealBit 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 2022-03-21 · eSentire · eSentire

eSentire Threat Intelligence Malware Analysis: HermeticWiper & PartyTicket

HermeticWiper PartyTicket 2022-03-14 · Kaspersky · GReAT

Webinar on cyberattacks in Ukraine – summary and Q&A

HermeticWiper HermeticWizard IsaacWiper PartyTicket WhisperGate 2022-03-10 · splunk · Splunk Threat Research Team

Detecting HermeticWiper

HermeticWiper PartyTicket 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 2022-03-04 · Threat Post · Lisa Vaas

Free HermeticRansom Ransomware Decryptor Released

PartyTicket 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 · Avast Decoded · Threat Research Team

Help for Ukraine: Free decryptor for HermeticRansom ransomware

PartyTicket 2022-03-03 · Bleeping Computer · Bill Toulas

Free decryptor released for HermeticRansom victims in Ukraine

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

IOC Resource for Russia-Ukraine Conflict-Related Cyberattacks

ClipBanker Conti HermeticWiper PartyTicket WhisperGate 2022-03-02 · Techtarget · Arielle Waldman

CrowdStrike cracks PartyTicket ransomware targeting Ukraine

PartyTicket 2022-03-02 · Recorded Future · Insikt Group

HermeticWiper and PartyTicket Targeting Computers in Ukraine

HermeticWiper PartyTicket 2022-03-01 · ESET Research · ESET Research

IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine

HermeticWiper IsaacWiper PartyTicket 2022-03-01 · Kaspersky Labs · Kaspersky

Ransomware as a distraction

HermeticWiper PartyTicket 2022-03-01 · Kaspersky · GReAT

Elections GoRansom – a smoke screen for the HermeticWiper attack

PartyTicket 2022-03-01 · CrowdStrike · CrowdStrike Intelligence Team

Decryptable PartyTicket Ransomware Reportedly Targeting Ukrainian Entities

PartyTicket 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 · Microsoft · MSRC Team

Cyber threat activity in Ukraine: analysis and resources

HermeticWiper IsaacWiper PartyTicket WhisperGate 2022-02-25 · Zscaler

Technical Analysis of PartyTicket Ransomware
PartyTicket

There is no Yara-Signature yet.
