

# WhisperGate (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:16:41 UTC

## WhisperGate

aka: PAYWIPE

VTCollection

---

Destructive malware deployed against targets in Ukraine in January 2022.

### References

2025-07-18 · [The Record](#) ·

UK sanctions Russian cyber spies accused of facilitating murders

[WhisperGate](#)

2024-09-05 · [CISA](#) · [CISA](#)

AA24-249A: Russian Military Cyber Actors Target US and Global Critical Infrastructure

[WhisperGate](#)

2024-06-26 · [US Department of Justice](#) · [Office of Public Affairs](#)

Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data

[WhisperGate](#)

2023-06-14 · [Microsoft](#) · [Microsoft Threat Intelligence](#)

Cadet Blizzard emerges as a novel and distinct Russian threat actor

[p0wnyshell](#) [reGeorg](#) [WhisperGate](#) [DEV-0586](#) [SaintBear](#)

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](#)

2023-02-15 · [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](#)

2022-09-26 · [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](#)

2022-08-12 · [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](#)

2022-07-18 · [Palo Alto Networks Unit 42](#) · [Unit 42](#)

Ruinous Ursa

[WhisperGate](#) [DEV-0586](#)

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 · [Blackberry](#) · [The BlackBerry Research & Intelligence Team](#)

.NET Stubs: Sowing the Seeds of Discord (PureCrypter)

[Aberebot](#) [AbstractEmu](#) [AdoBot](#) [404](#) [Keylogger](#) [Agent Tesla](#) [Amadey](#) [AsyncRAT](#) [Ave Maria](#) [BitRAT](#) [BluStealer](#)  
[Formbook](#) [LimeRAT](#) [Loki](#) [Password Stealer \(PWS\)](#) [Nanocore](#) [RAT](#) [Orcus](#) [RAT](#) [Quasar](#) [RAT](#) [Raccoon](#) [RedLine](#)  
[Stealer](#) [WhisperGate](#)

2022-05-19 · [Blackberry](#) · [The BlackBerry Research & Intelligence Team](#)

.NET Stubs: Sowing the Seeds of Discord

[Agent Tesla](#) [Quasar](#) [RAT](#) [WhisperGate](#)

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](#)

2022-03-30 · [CrowdStrike](#) · [CrowdStrike Threat Intel Team](#)

Who is EMBER BEAR?

[WhisperGate](#)

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](#)

2022-03-10 · [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 · [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 · [Trend Micro](#) · [Trend Micro Research](#)

Cyberattacks are Prominent in the Russia-Ukraine Conflict

[BazarBackdoor](#) [Cobalt Strike](#) [Conti](#) [Emotet](#) [WhisperGate](#)

2022-03-03 · [LIFARS](#) · [LIFARS](#)

A Closer Look at the Russian Actors Targeting Organizations in Ukraine

[HermeticWiper](#) [IsaacWiper](#) [Saint Bot](#) [WhisperGate](#)

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](#)

2022-02-26 · [CISA](#) · [CISA](#), [FBI](#)

Destructive Malware Targeting Organizations in Ukraine

[HermeticWiper WhisperGate](#)

2022-02-26 · [CISA](#)

Alert (AA22-057A) 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 · [CyberPeace Institute](#)

UKRAINE: Timeline of Cyberattacks

[VPNFilter EternalPetya HermeticWiper WhisperGate](#)

2022-02-24 · [Tesorion](#) · [TESORION](#)

Report OSINT: Russia/ Ukraine Conflict Cyberaspect

[Mirai VPNFilter BlackEnergy EternalPetya HermeticWiper Industroyer WhisperGate](#)

2022-02-24 · [nviso](#) · [Michel Coene](#)

Threat Update – Ukraine & Russia conflict

[EternalPetya GreyEnergy HermeticWiper Industroyer KillDisk WhisperGate](#)

2022-02-23 · [The Record](#) · [Catalin Cimpanu](#)

Second data wiper attack hits Ukraine computer networks

[HermeticWiper WhisperGate](#)

2022-02-15 · [Intel 471](#) · [Intel 471](#)

How the Russia-Ukraine conflict is impacting cybercrime

[WhisperGate](#)

2022-02-10 · [InQuest](#) · [Josiah Smith](#)

+380-GlowSpark

[GlowSpark WhisperGate](#)

2022-02-03 · [YouTube \(Malfind Labs\)](#) · [Lasq](#)

Analyzing WhisperGate - destructive malware targeting Ukraine - part 1

[WhisperGate](#)

2022-02-03 · [Blackberry](#) · [The BlackBerry Research & Intelligence Team](#)

Threat Spotlight: WhisperGate Wiper Wreaks Havoc in Ukraine

[WhisperGate](#)

2022-02-01 · [Cyborg Security](#) · [Brandon Denker](#)

WhisperGate Malware - Update

[WhisperGate](#)

2022-02-01 · [Max Kersten's Blog](#) · [Max Kersten](#)

Dumping WhisperGate's wiper from an Eazfuscator obfuscated loader

[WhisperGate](#)

2022-01-31 · [CrowdStrike](#) · [Liviu Arsene](#), [Sarang Sonawane](#)

CrowdStrike Falcon Proactively Protects Against Wiper Malware as CISA Warns U.S. Companies of Potential Attacks

[WhisperGate](#)

2022-01-28 · [CrowdStrike](#) · [CrowdStrike Intelligence Team](#)

Lessons Learned From Successive Use of Offensive Cyber Operations Against Ukraine and What May Be Next

[WhisperGate](#)

2022-01-28 · [Recorded Future](#) · [Insikt Group®](#)

WhisperGate Malware Corrupts Computers in Ukraine

[WhisperGate](#)

2022-01-27 · [Recorded Future](#) · [John Wetzel](#)

Russia's Biggest Threat Is Its Instability

[WhisperGate](#)

2022-01-27 · [splunk](#) · [Splunk Threat Research Team](#)

Threat Advisory: STRT-TA02 - Destructive Software

[WhisperGate](#)

2022-01-27 · [Gigamon](#) · [Joe Slowik](#)

Focusing on "Left of Boom"

[WhisperGate](#)

2022-01-27 · [Blackberry](#) · [The BlackBerry Research & Intelligence Team](#)

Threat Thursday: WhisperGate Wiper Targets Government, Non-profit, and IT Organizations in Ukraine

[WhisperGate](#)

2022-01-27 · [splunk](#) · [Splunk Threat Research Team](#)

Threat Advisory: STRT-TA02 - Destructive Software

[WhisperGate](#)

2022-01-26 · [Netskope](#) · [Gustavo Palazolo](#)

Netskope Threat Coverage: WhisperGate

[WhisperGate](#)

2022-01-26 · [Cert-UA](#) · [Cert-UA](#)

Fragment of cyberattack research 14.01.2022

[WhisperGate](#)

2022-01-22 · [csirt-mon](#) · [csirt-mon](#)

Analysis of the Cyberattack on Ukrainian Government Resources

[WhisperGate](#)

2022-01-21 · [Secureworks](#) · [Counter Threat Unit ResearchTeam](#)

WhisperGate: Not NotPetya

[WhisperGate](#)

2022-01-21 · [Github \(OALabs\)](#) · [OALabs](#)

WhisperGate Malware

[WhisperGate](#)

2022-01-21 · [Zero Day](#) · [Kim Zetter](#)

Hackers Were in Ukraine Systems Months Before Deploying Wiper

[WhisperGate](#)

2022-01-21 · [Secureworks](#) · [Counter Threat Unit ResearchTeam](#)

Disruptive Attacks in Ukraine Likely Linked to Escalating Tensions

[WhisperGate](#)

2022-01-21 · [Talos Intelligence](#) · [Chris Neal](#), [Dmytro Korzhevin](#), [Matt Olney](#), [Michael Chen](#), [Nick Biasini](#)

Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation

[WhisperGate](#)

2022-01-20 · [Trellix](#) · [Mo Cashman](#), [Raj Samani](#), [Taylor Mullins](#)

Update on WhisperGate, Destructive Malware Targeting Ukraine – Threat Intelligence & Protections Update

[WhisperGate](#)

2022-01-20 · [Palo Alto Networks Unit 42](#) · [Josh Grunzweig](#), [Mike Harbison](#), [Robert Falcone](#)

Threat Brief: Ongoing Russia and Ukraine Cyber Conflict

[WhisperGate](#)

2022-01-20 · [Trellix](#) · [Christiaan Beek](#), [Max Kersten](#), [Raj Samani](#)

Return of Pseudo Ransomware

[WhisperGate](#)

2022-01-20 · [Twitter \(@nunohaien\)](#) · [Tillmann Werner](#)

Tweet on key points of Whispergate wiper

[WhisperGate](#)

2022-01-20 · [LIFARS](#) · [Vlad Pasca](#)

A Detailed Analysis of WhisperGate Targeting Ukrainian Organizations

[WhisperGate](#)

2022-01-19 · [CrowdStrike](#) · [CrowdStrike Intelligence Team](#)

Technical Analysis of the WhisperGate Malicious Bootloader

[WhisperGate](#)

2022-01-19 · [Elastic](#) · [Andrew Pease](#), [Daniel Stepanic](#), [James Spiteri](#), [Joe Desimone](#), [Mark Mager](#), [Samir Bousseaden](#)

Operation Bleeding Bear

[WhisperGate](#)

2022-01-19 · [Youtube \(HEXORCIST\)](#) · [Nicolas Brulez](#)

WhisperGate: MBR Wiper Malware Analysis. Ukraine Cyber Attack 2022

[WhisperGate](#)

2022-01-19 · [rxOred's blog](#) · [rxored](#)

WhisperGate

[WhisperGate](#)

2022-01-19 · [Elastic](#) · [Andrew Pease](#), [Daniel Stepanic](#), [James Spiteri](#), [Joe Desimone](#), [Mark Mager](#)

Operation Bleeding Bear

[WhisperGate](#)

2022-01-18 · [Stairwell](#) · [Silas Cutler](#)

Whispers in the noise

[WhisperGate](#)

2022-01-18 · [S2W Inc.](#) · [BLKSMTH](#)

Analysis of Destructive Malware (WhisperGate) targeting Ukraine

[WhisperGate](#)

2022-01-18 · [zetter substack](#) · [Kim Zetter](#)

Dozens of Computers in Ukraine Wiped with Destructive Malware in Coordinated Attack

[WhisperGate](#)

2022-01-18 · [Microsoft](#) · [Microsoft 365 Defender Threat Intelligence Team](#)

Evolved phishing: Device registration trick adds to phishers' toolbox for victims without MFA

[WhisperGate](#)

2022-01-18 · <a href="#">Twitter (@knight0x07)</a> · <a href="#">neeraj</a> Thread on yet another comprehensive analysis of WHISPERGATE <a href="#">WhisperGate</a>
2022-01-17 · <a href="#">Cado Security</a> · <a href="#">Cado Security</a> Resources for DFIR Professionals Responding to WhisperGate Malware <a href="#">WhisperGate</a>
2022-01-17 · <a href="#">Github (Dump-GUY)</a> · <a href="#">Jiří Vinopal</a> Debugging MBR - IDA + Bochs Emulator (CTF example) <a href="#">WhisperGate</a>
2022-01-17 · <a href="#">Twitter (@HuskyHacksMK)</a> · <a href="#">Matt   HuskyHacks</a> WhisperGate Wiper Malware Analysis Live Thread <a href="#">WhisperGate</a>
2022-01-17 · <a href="#">Twitter (@Libranalysis)</a> · <a href="#">Max Kersten</a> Tweet on short analysis of WHISPERGATE stage 3 malware <a href="#">WhisperGate</a>
2022-01-15 · <a href="#">Microsoft</a> · <a href="#">Microsoft</a> , <a href="#">Microsoft 365 Defender Threat Intelligence Team</a> , <a href="#">Microsoft Detection and Response Team (DART)</a> , <a href="#">Microsoft Digital Security Unit (DSU)</a> , <a href="#">Microsoft Security Intelligence</a> Destructive malware targeting Ukrainian organizations (DEV-0586) <a href="#">WhisperGate DEV-0586</a>
2022-01-15 · <a href="#">Microsoft</a> · <a href="#">Tom Burt</a> Malware attacks targeting Ukraine government (DEV-0586) <a href="#">WhisperGate</a>

#### Yara Rules

▶ [TLP:WHITE] win_whispergate_auto (20251219   Detects win.whispergate.)	
--	--

[Download all Yara Rules](#)

---

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.whispergate>