Cyberwarfare: Ukraine - Russia (2022) Wipers and Encryptors

Reference: https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

**1-12-2022 – WhisperGate / Whisperkill**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: Government, ICT, and non-profits
* **Purpose:** Destruction
* **Impact**: WhisperGate wiper was found on some of the IT company's systems and had overwritten the master boot records on those machines. The company took the systems down to rebuild from scratch.
* **Confidence**: Probable
* **Threat** **Actor**: Dev-0586
* **References**: [Recorded Future](https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/), [Zero Day](https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r), [Microsoft](https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/)

**1-13-2022 – WhisperGate / Whisperkill**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Defacement
* **Targets**: ICT
* **Purpose:** Disruption
* **Impact**: On January 14, 2022, Orthodox New Year, over 70 Ukrainian government websites were defaced with political imagery and a statement in Russian, Ukrainian, and Polish before going down temporarily. Most sites were restored within hours. The attack crippled much of the government’s public-facing digital infrastructure, including the most widely used site for handling government services online, Diia. Diia also has a role in Ukraine’s coronavirus response and in encouraging vaccination. It also crippled the sites of the Cabinet of Ministers and the ministries of energy, sports, agriculture, veterans’ affairs, and ecology. The Ukrainian company Kitsoft also confirmed that it found the WhisperGate malware on some of its systems. At least 50 of the 70 sites targeted for defacement were developed and maintained by Kitsoft. Kitsoft was compromised, which allowed the hackers to gain access to Kitsoft’s administrator panel and use the company’s credentials to deface customer websites. The purpose of such attacks is reportedly: to destabilize the internal situation in the country. - to spread chaos and despair in society.
* **Confidence**: Confirmed
* **Threat** **Actor**: UNC1151
* **References**:[Ukraine Center for Strategic Communications](https://spravdi.gov.ua/ataka-na-uryadovi-sajty-novyj-rozdil-kibervijny-proty-ukrayiny/:), [New York Times](https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html), [BBC](https://www.bbc.com/news/world-europe-59992531), [Zero Day](https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r)

**2-22-2022 – HermeticWiper / FoxBlade**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: Government, ICT, Financial, and Energy
* **Purpose:** Destruction
* **Impact**: Hundreds of systems spanning multiple government, information technology, financial sector, and energy organizations were impacted.
* **Confidence**: Confirmed
* **Threat** **Actor**: Sandworm
* **References**:Wall Street Journal, SC Media, Microsoft(2), Broadcom, Microsoft(1), ESET WeLiveSecurity

**2-23-2022 – AcidRain**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: ICT
* **Purpose:** Destruction
* **Impact**: Internet access offline for more than 2 weeks. - Nearly 9,000 subscribers of a satellite internet service provider were deprived of the internet in France. - Around a third of 40,000 subscribers of another satellite internet service provider in Europe (Germany, France, Hungary, Greece, Italy, Poland) were affected. - A major German energy company has lost remote monitoring access to over 5,800 wind turbines. - Impacted several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe.
* **Confidence**: Confirmed
* **Threat** **Actor**: Nation State - Russian Federation
* **References**: [The Record](https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack/), [SecurityWeek](https://www.securityweek.com/cyberattack-knocks-thousands-offline-europe), [France24](https://www.france24.com/fr/info-en-continu/20220304-des-milliers-d-internautes-en-europe-priv%C3%A9s-d-internet-suite-%C3%A0-une-probable-cyber-attaque), [The Stack](https://thestack.technology/viasat-ka-sat-outage-cyber/), [REVERSEMODE](https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html), [Viasat](https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/), [SentinelLabs](https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/), [Council of the EU](https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/), [Reuters](https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/), [Washingtonpost](https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/)

**2-23-2022 – IsaacWiper**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: Government
* **Purpose:** Destruction
* **Impact**: ESET identified a further wiper in Ukrainian government networks, affecting organizations that had not been attacked by HermeticWiper and does not share any code similarity with it. On February 25, the attackers dropped a new version of IsaacWiper with debug logs, indicating that the attackers were unable to wipe some of the compromised machines. The malware was developed/employed at least since October 19, 2021.
* **Confidence**: Confirmed
* **Threat** **Actor**: Sandworm
* **References**: [ESET WeLiveSecurity](https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/)

**2-24-2022 – Official Invasion of Ukraine**

**2-28-2022 – DesertBlade**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: Media
* **Purpose:** Disruption
* **Impact**: Suspected Russian threat actor launched "DesertBlade" malware against a major broadcasting company on March 1, the same day that the Russian military announced its intention to destroy “disinformation” targets in Ukraine and directed a missile strike against a TV tower in Kyiv. The intent was the loss of access to a key source of information for the Ukrainian public.
* **Confidence**: Probable
* **Threat** **Actor**: Unknown
* **References**: [Microsoft](https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd)

**3-13-2022 – CaddyWiper**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: Unknown
* **Purpose:** Destruction
* **Impact**: ESET researchers have uncovered yet another destructive data wiper that was used in attacks against a limited number of organizations in Ukraine. No code similarities to either HermeticWiper or IsaacWiper were identified. There’s evidence to suggest that the threat actors behind CaddyWiper infiltrated the target’s network before executing the wiper.
* **Confidence**: Confirmed
* **Threat** **Actor**: Sandworm
* **References**: [ESET](https://twitter.com/ESETresearch/status/1503436423818534915), [Bleeping Computer](https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/https:/cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya)

**3-14-2022 – CaddyWiper**

* Deployment of CaddyWiper against a Ukrainian bank

**3-16-2022 – DoubleZero**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: Unknown
* **Purpose:** Destruction
* **Impact**: On March 17, CERT-UA discovered several ZIP archives of a destructive malware dubbed “DoubleZero.” The activity is tracked by the UAC-0088 identifier and is directly related to attempts to violate the regular mode of operation of information systems of Ukrainian enterprises.
* **Confidence**: Confirmed
* **Threat** **Actor**: UAC-0088
* **References**:[CERT-UA](https://cert.gov.ua/article/38088), [SOC Prime](https://socprime.com/blog/doublezero-destructive-malware-used-in-cyber-attacks-at-ukrainian-companies-cert-ua-alert/)

**4-1-2022 – CaddyWiper**

* Deployment of CaddyWiper against a Ukrainian governmental entity

**4-8-2022 – CaddyWiper**

* Deployment of CaddyWiper on some Windows machines and of Linux and Solaris destructive malware at the energy provider

**All malware below was part of a single attack by Sandworm (Russian APT) on a Ukrainian energy system.**

*https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/*

-------------------------------------------------------------------------------------------------------------------------------

**4-8-2022 – Industroyer2**

* The second iteration of Industroyer malware used to destroy and disrupt energy ICS systems

**4-8-2022 – ORCSHRED**

* Linux and Solaris wiper used with Industroyer2

**4-8-2022 – AWFULSHRED**

* Linux and Solaris wiper used with Industroyer2

**4-8-2022 – SOLOSHRED**

* Linux and Solaris wiper used with Industroyer2

**4-8-2022 – CaddyWiper**

* Deployment of CaddyWiper on some Windows machines and of Linux and Solaris destructive malware at the energy provider

-------------------------------------------------------------------------------------------------------------------------------

**10-11-2022 – Prestige Ransomware**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Ransomware
* **Targets**: Polish and Ukrainian logistics companies.
* **Purpose:** Destruction
* **Impact**: Unknown
* **Confidence**: Very Likely
* **Threat** **Actor**: IRIDIUM (Sandworm)
* **References**:[Microsoft](https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/)

**10-27-2022 – Azov Ransomware**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Wiper
* **Targets**: Unknown
* **Purpose:** Destruction
* **Impact**: Unknown
* **Confidence**: Probable
* **Threat** **Actor**: Unknown
* **References**:[Bleeping Computer](https://www.bleepingcomputer.com/news/security/new-azov-data-wiper-tries-to-frame-researchers-and-bleepingcomputer/)

Azov Ransomware samples VirusTotal Query:

(behaviour:'Local\\\\Kasimir\_\*' OR behaviour:'Local\\\\azov') AND (behaviour\_files:'RESTORE\_FILES' OR behaviour\_registry:'rdpclient.exe')

Over 17k samples of Azov submitted to VT since late October.

**11-11-2022 – Somnia Ransomware**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Pseudo-Ransomware (Wiper)
* **Targets**: Unknown
* **Purpose:** Destruction
* **Impact**: Disruption of some systems.
* **Confidence**: Confirmed
* **Threat** **Actor**: FRwL
* **References**:[CERT-UA](https://cert.gov.ua/article/2724253)

**11-25-2022 – RansomBoggs**

* **By**: Russia
* **Victim**: Ukraine
* **Type**: Ransomware
* **Targets**: Unknown
* **Purpose:** Destruction
* **Impact**: Unknown
* **Confidence**: Probable
* **Threat** **Actor**: Sandworm
* **References**:[ESET WeLiveSecurity](https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/), [Twitter](https://twitter.com/ESETresearch/status/1596181925663760386)

**Estonia is helping Ukraine combat and establish a cybersecurity posture. This may explain the reduction in cyber-attacks recently as seen by the monthly incident graph:**

*https://www.politico.com/news/2022/12/07/estonia-ukraine-cybersecurity-russian-hackers-00072925*