MALWARE/
TOOLS
PROFILE

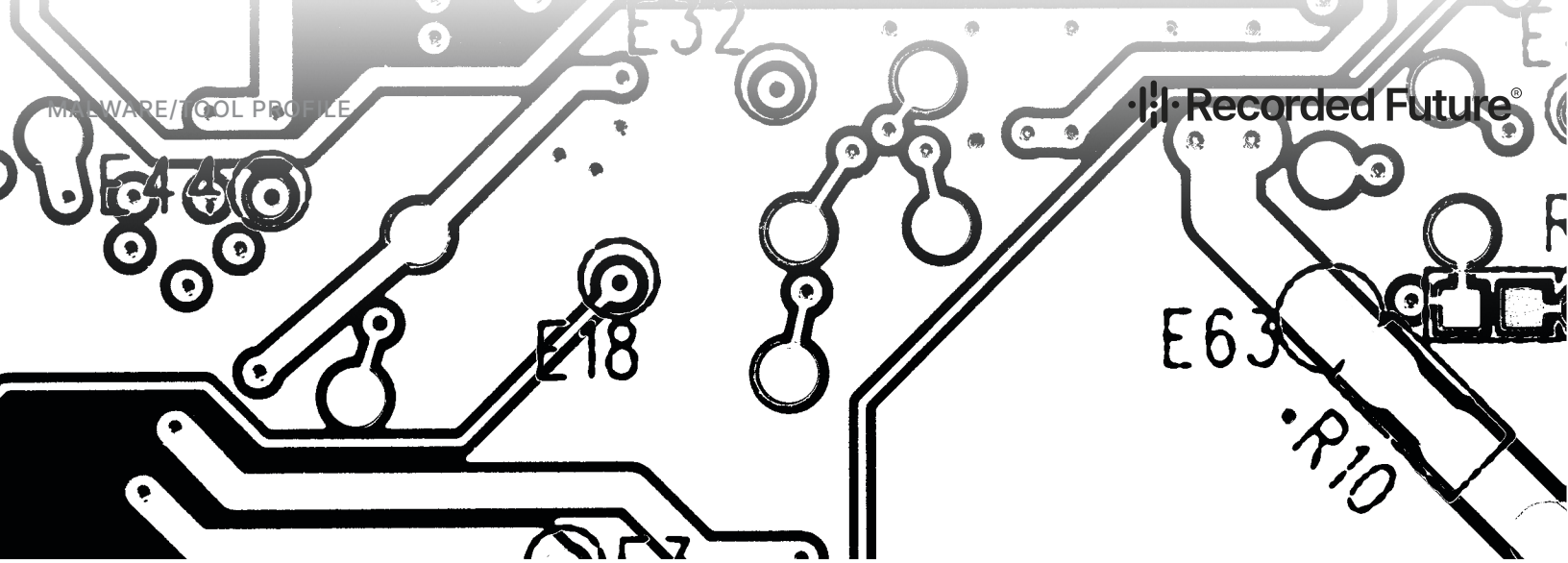
Recorded Future®

By Insikt Group®

May 12, 2022

Overview of the 9 Distinct Data Wipers Used in the Ukraine War

Recorded Future®



This report serves as a high-level comparative overview of the 9 wipers analyzed by Insikt Group in association with the ongoing Ukraine/Russia war. It is meant to provide insight into the similarities and differences between the tools and the geopolitical implications of their development and usage. The intended audience of this report is those looking for a high-level technical overview of the wipers. Sources used include reverse engineering tools, OSINT, the Recorded Future® Platform, and PolySwarm.

Executive Summary

While the Ukraine/Russia war is primarily a kinetic conflict, several destructive data wipers targeting Ukrainian entities emerged in the immediate lead-up to and during the first 2-plus months of the war, bringing the conflict to cyberspace. The 9 wipers analyzed by Insikt Group had the same high-level destructive goal but differed in technical implementation and the operating systems they targeted, suggesting that each was a distinct tool, possibly created by different authors. Over time, the wipers also became more simplistic at a technical level, including reductions in the number of stages, the existence of obfuscation, and attempts to masquerade as ransomware, though none were at the level of sophistication of some other known Russian state-sponsored malware.

The wiper deployment activity aligns with prior Russian state-sponsored cyber operations against Ukraine as well as other nations; these efforts often occur before and during active conflict and are likely intended to act as a "force multiplier" for Russian military operations. Ongoing efforts to deploy disruptive cyber operations against Ukrainian targets show that the Russian government almost certainly considers such operations to be valuable, and suggest that these efforts will likely continue.

Key Judgments

- 6 of the wipers associated with the Ukraine/Russia conflict analyzed by Insikt Group all serve the same high-level destructive purpose of rendering a Windows machine inoperable; the other wipers targeted Linux systems (including satellite modems).
- The wipers do not share obvious code similarities between them and are unlikely to be iterations on, or new versions of, each other.
- HermeticWiper was the only wiper found to be distributed by a worm component, known as HermeticWizard. HermeticWizard restricted its spread to local IP addresses within the victim's network, preventing the external distribution seen with other worm incidents like NotPetya.
- None of the wipers themselves contained any network connectivity functionality that would permit them to exfiltrate victim data further, suggesting that their purpose was targeted destruction of specific entities.

Background

There is an observable, historical pattern of entities, very likely acting in support of Russian government interests, engaging in cyber operations prior to and concurrent with Russian military operations. Such operations date back to at least August 2008 when reports describe pro-Russian hacktivists engaging in a series of sustained Distributed Denial of Service (DDoS) attacks and website defacements against a number of Georgian government, banking, media, communications, and transportation resources at approximately the same time the Russian military was launching an offensive in South Ossetia and engaging in a bombing campaign throughout Georgia. Since 2014, Russian state-sponsored advanced persistent threat (APT) groups affiliated with the Russian Main Intelligence Directorate (GRU), such as Sandworm, have consistently engaged in cyber operations against important domestic sectors in Ukraine, such as the electric power grid in both 2015 and 2016 (1, 2), as well as "utility companies, banks, airports, and government agencies" in 2017. Following the launch of Russia's full-scale invasion and subsequent war in Ukraine, Sandworm and other likely GRU-affiliated threat activity groups again engaged in attempts to deploy cyber attacks in concert with military operations against Ukrainian entities, most recently via the deployment of a series of unsuccessful data wiping attacks. This report explores the malware, its timing, and the tactics, techniques, and procedures (TTPs) involved with these wiper attacks, and what this means for the overall conflict.

Threat Analysis

Insikt Group analyzed 9 of the wipers associated with the Ukraine/Russia conflict - WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, AcidRain, AwfulShred, SoloShred, DoubleZero, and DesertBlade. The analysis showed that 8 of the 9 wipers differed significantly from each other in implementation, despite remaining fairly similar in their overall functionality and purpose, and do not appear to originate from the same author.

Table 1 below contains a brief, high-level summary of each wiper's functionality. The MBR (master boot record), GPT (GUID partition table), and Files columns indicate which components of the victim's machine were targeted by the wiper. For the purposes of this report, if the GPT was recoverable, then it is listed as not affected. In the instance of DesertBlade, public samples were not available and open-source reporting was limited; therefore, it is unknown at the time of this writing whether the wiper affected MBR or GPT-style partition tables. The Associated Ransomware column indicates whether a fake ransomware component was delivered as part of the wiper's attack. Finally, the Target OS and Languages columns describe the intended victim operating system (OS) and the programming language used to develop the wipers.

Malware	MBR	GPT	Files	Associated Ransomware	Target OS	Languages
WhisperGate	Y	N	Y	Y	Windows	C++ (Stage 1) .NET (Stage 2, 3)
HermeticWiper	N**	N**	Y	Y	Windows	C, Assembly
IsaacWiper	Y	N**	N	N	Windows	C, C++, Assembly
DesertBlade	?	?	Y	N	Windows	Golang
ACIDRAIN*	N/A	N/A	Y	N	Linux (MIPS)	C
CaddyWiper	Y	N	Y	N	Windows	C
DoubleZero	N**	N**	Y	N	Windows	.NET
AwfulShred	Y	Y	Y	N	Linux	Bash
SoloShred	Y	Y	Y	N	Solaris	Bash

Table 1: High-level overview of each wiper's functionality (Source: Recorded Future)
** ACIDRAIN targets satellite modems, not desktop operating systems, so some fields may not be relevant.*
*** Although the MBR/GPT may be recoverable (or not affected at all), the wiper destroys the filesystem or critical files that prevent the system from successfully booting.*

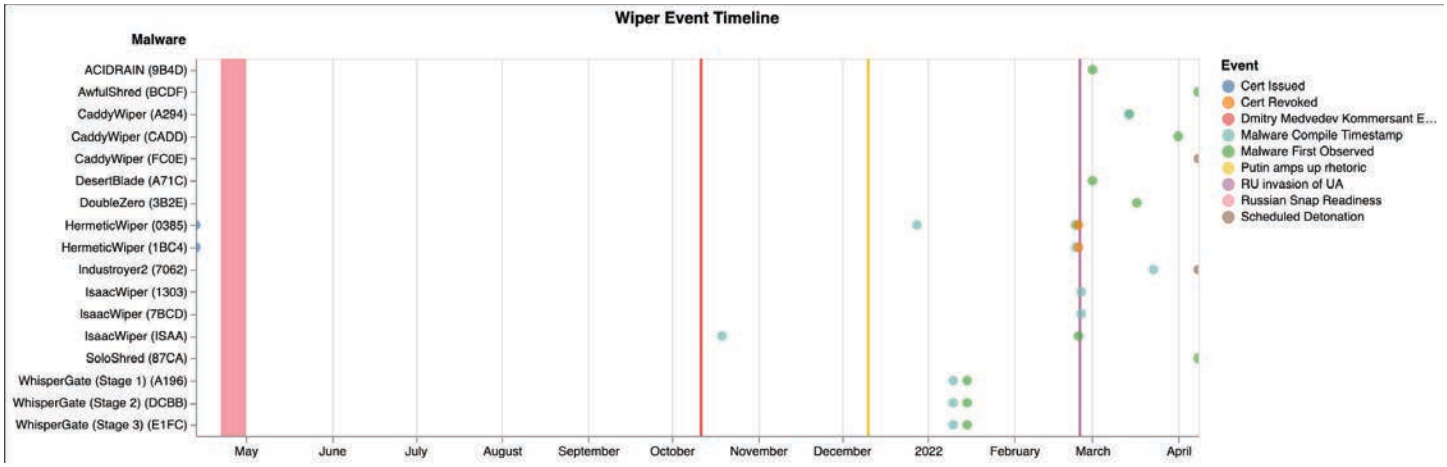


Figure 1: Timeline of when wipers were first identified in the wild, compilation date of the binaries, and certificate issue/revoke dates overlaid with key dates in the Ukraine/Russia conflict (Source: Recorded Future)

Overall Assessment

The wipers did not share code between them and were written in various programming languages, suggesting they were distinct tools, possibly written by different developers. Over time, the Windows wipers, as a whole, became less complex. The earliest wiper, WhisperGate, was the most sophisticated; it employed obfuscation, contained the most number of stages, masqueraded as ransomware, and downloaded its final stage from a remote server. Subsequent wipers, like HermeticWiper and DoubleZero, present elements of these techniques, but not all of them. However, these malicious tools do not approach the level of sophistication of suspected Russian state-sponsored tools like Zebrocy, PowerDuke, or Havex.

None of the wipers displayed network connectivity capabilities that would allow them to spread to other machines outside of the network (with only HermeticWizard having worm behavior) or exfiltrate data, suggesting that the wipers had a singular purpose: to perform targeted destruction of particular systems (rather than espionage).

The earliest compilation date for these wipers was in mid-October 2021 (IsaacWiper), 4 months before the first observation of IsaacWiper's use in the wild, and the certificates associated with HermeticWiper were created in mid-April 2021, nearly 10 months before the first observation of HermeticWiper's use in the wild. This suggests that while the wipers were largely compiled close to the time when they were first used against Ukrainian entities, some preparation occurred prior to the onset of the conflict. Overall, the use of the wipers escalated as the physical conflict did, suggesting that these attacks were likely intended to act as a force multiplier for ongoing kinetic operations.

Finally, the destructive capabilities of these wipers designed to target Windows and Unix-like systems, including Surfbeam2 and Surfbeam2+ satellite modems, combined with the discriminant targeting of largely Ukrainian entities, further suggests that these efforts are almost certainly aligned with Russian state-sponsored threat activity groups, likely in affiliation with the Main Intelligence Directorate (GRU). Historical attacks by GRU-attributed threat activity groups have heavily targeted Ukrainian entities (1, 2), have included the use of false ransomware, such as the 2017 NotPetya and Bad Rabbit (1, 2) attacks, and have conducted known attacks that employed malware targeting Windows (1, 2) and Unix-like OSes (1, 2, 3, 4).

WhisperGate

WhisperGate, the first wiper to be associated with the Ukraine/Russia conflict, is a 3-stage destructive malware that overwrites the MBR of a Windows machine. The first stage overwrites the MBR (but is ineffective on GPT-style devices) and displays a ransom note alleging that the victim's hard drive has been corrupted and providing a Bitcoin wallet address to which they should send payment. Subsequently, the malware deploys stage 2, which downloads the final stage of the malware that is hosted on Discord's content delivery network (CDN) as a JPG attachment and executes it. Stage 3 is a file corrupter that looks for files matching a list of 191 file extensions(such as .xlsx, .pdf, and .zip) and overwrites the first 1MB of each with "0xCC" bytes.

HermeticWiper

HermeticWiper and its purported ransomware component, PartyTicket, are destructive malware that renders a victim's Windows machine inoperable. The wiper is distributed by a worm component known as HermeticWizard. HermeticWizard uses various means to identify IP addresses on the victim's local network, and then spreads itself to new victims via the Windows Server Message Block (SMB) and Windows Management Instrumentation (WMI) protocols, before finally executing HermeticWiper. HermeticWiper corrupts NTFS and FAT file systems. Unlike WhisperGate, HermeticWiper does not corrupt the MBR or the GPT; it merely overwrites the filesystem. This allows HermeticWiper to succeed in its destructive capabilities against both types of file systems. The PartyTicket "ransomware" component, like that of WhisperGate, is not true ransomware. Unlike actual ransomware, PartyTicket does not display "branding" of any specific group and encrypts files that include executables such as .exe and .dll files that are critical to the computer's ability to operate. This suggests that both components serve a destructive purpose, and are not likely to be the work of a criminal threat actor.

IsaacWiper

IsaacWiper attempts to overwrite all physical disks and logical volumes of the victim machine, including the MBR. The wiper overwrites these disks and volumes with random data. Unlike the previously released wipers, HermeticWiper and Whispergate, IsaacWiper does not have a component that masquerades as ransomware.

DesertBlade

On March 1, 2022, suspected Russian threat actors used DesertBlade in an attack on a major broadcasting company. Microsoft reports that DesertBlade was used again during the week of March 17-23, but at the time of this report has not provided any additional details. In the initial incident, the malware was reportedly deployed via an Active Directory Group Policy Object (GPO), indicating that the attacker had first gained control of the Active Directory for the network. DesertBlade overwrites files on the victim machine and then deletes them. The extra step of overwriting the files is likely performed in an attempt to ensure that the files cannot be recovered.

ACIDRAIN

ACIDRAIN is a wiper malware targeting satellite modems used for internet access. On March 1, 2022, an American telecommunications company that provides high-speed satellite broadband services and secure networking systems covering residential, commercial, and military markets, announced that the disruption of its satellite internet services in Ukraine and Europe, was caused by a cyberattack. This disruption coincided with the Russian invasion of Ukraine.

The company self-reported the incident, in which a modem wiper was employed to disrupt SurfBeam2 and SurfBeam2+ modems and associated equipment used in KA-SAT deployments. The wiper is tracked as ACIDRAIN (aka SKYFALL) and uses multiple methods to overwrite the flash memory of the targeted device. When executed as root, ACIDRAIN performs an initial recursive overwrite and deletion of files located outside of standard system directories before destroying the data in storage devices.

CaddyWiper

CaddyWiper is a wiper malware targeting Windows systems. The malware checks to see if it is running on the primary domain controller and, if so, it simply exits. ESET speculated in a social media post that this is to ensure that the threat actor does not lose their access to the victim's network. If the victim machine is not a primary domain controller then the wiper begins to recursively erase files located under the "C:\Users" directory, followed by the contents of drives lettered D to Z. Each file is overwritten with zeros to ensure that the data is destroyed and not recoverable. Finally, the MBRs of the first 10 physical drives connected to the system (\\.\PhysicalDrive[0-9]) are overwritten with zeros via an input/output control (IOCTL) call for IOCTL_DISK_SET_DRIVE_LAYOUT_EX.

DoubleZero

In mid-March 2022, DoubleZero emerged, targeting Windows systems. DoubleZero was discovered by CERT-UA (Ukraine's cyber security intelligence agency) inside a zipped file named "Virus ... extremely dangerous !!!. Zip". The malware was written in .NET and progressively destroys data on a victim system, starting with non-system files and then shifting to system files and registry entries. Files are destroyed either via an IOCTL call for FSCTL_SET_ZERO_DATA or by overwriting the file's first 4096 bytes with zeros. Once the wiping process is complete, the victim machine is rebooted. Microsoft reports that they have observed DoubleZero used in attacks against Ukrainian broadcast and media organizations.

AwfulShred

AwfulShred is one of the Linux wipers associated with the thwarted Industroyer2 attack on a Ukrainian energy provider in early April 2022. It is a Bash script distributed by OrcShred, a worm component used in the attack to spread the Linux wiper to other systems. In the early April attack, the OrcShred malware created a cron job (scheduled task) to execute AwfulShred on April 8, 2022, at 2:58 PM UTC. Upon execution, the task first stops and disables HTTP and SSH services, then deletes the contents of the /boot, /home, and /var/log directories. It then erases all attached disks using the "shred" or "dd" (copy and convert) utility. When more than 1 disk is present, the disks are wiped simultaneously. Upon completion, a system reboot is issued.

SoloShred

SoloShred is a Bash script that is similar to AwfulShred and was intended to target Solaris operating systems in the failed Industroyer2 attack in early April 2022. It begins by stopping and disabling any services that start with "ssh", "http", "apache", "ora_", or "oracle". Next, databases on the system are deleted, and then /boot, /home, and /var/log along with any file paths present in environment variables starting with "ORA" are destroyed using the shred and "rm" (remove files) utilities. All disks on the system are wiped simultaneously using the shred utility, in a similar manner to AwfulShred.

Outlook

Destructive data wipers against Ukrainian targets, coincident with kinetic operations by Russia, were frequently deployed between the end of February through late March of 2022; the cadence of new wiper attacks appeared to slow down in April. While it is certainly possible that the Ukraine/Russia conflict continues to have a cyber component and other malware is being used at this time, actions in the conflict appear to be largely kinetic for now. On April 27, Microsoft indicated that the wiper attacks were primarily conducted by the GRU; Microsoft attributed the FoxBlade and CaddyWiper attacks to Sandworm/Unit 74455, and WhisperGate to DEV-0586 (also a suspected GRU-affiliated entity). While no attribution for the other wipers has been made at this time, based on the victimology and objectives achieved it is likely that Russian-aligned threat activity groups are behind these wipers as well. Based on historical precedent and the activity described in this report, Russian-aligned groups will almost certainly continue to view destructive cyber operations as useful force multipliers in their war against Ukraine and more destructive malware attacks are likely as the conflict persists.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.