A year of wiper attacks in Ukraine

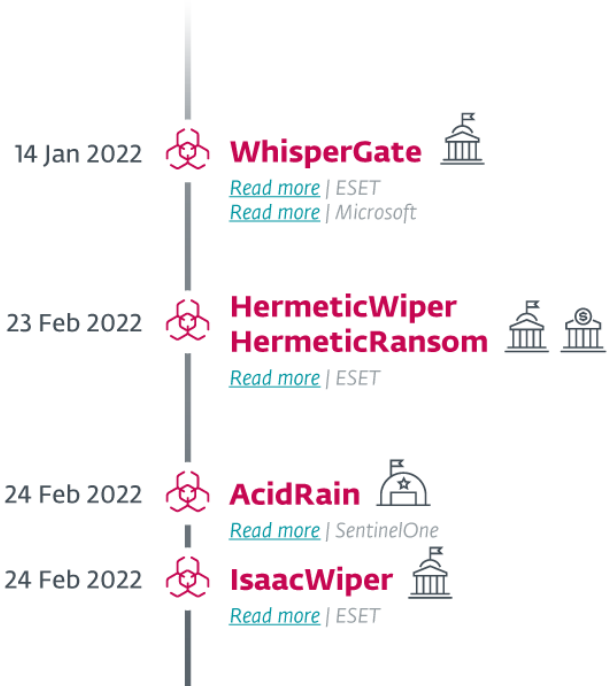
: 2/24/2023

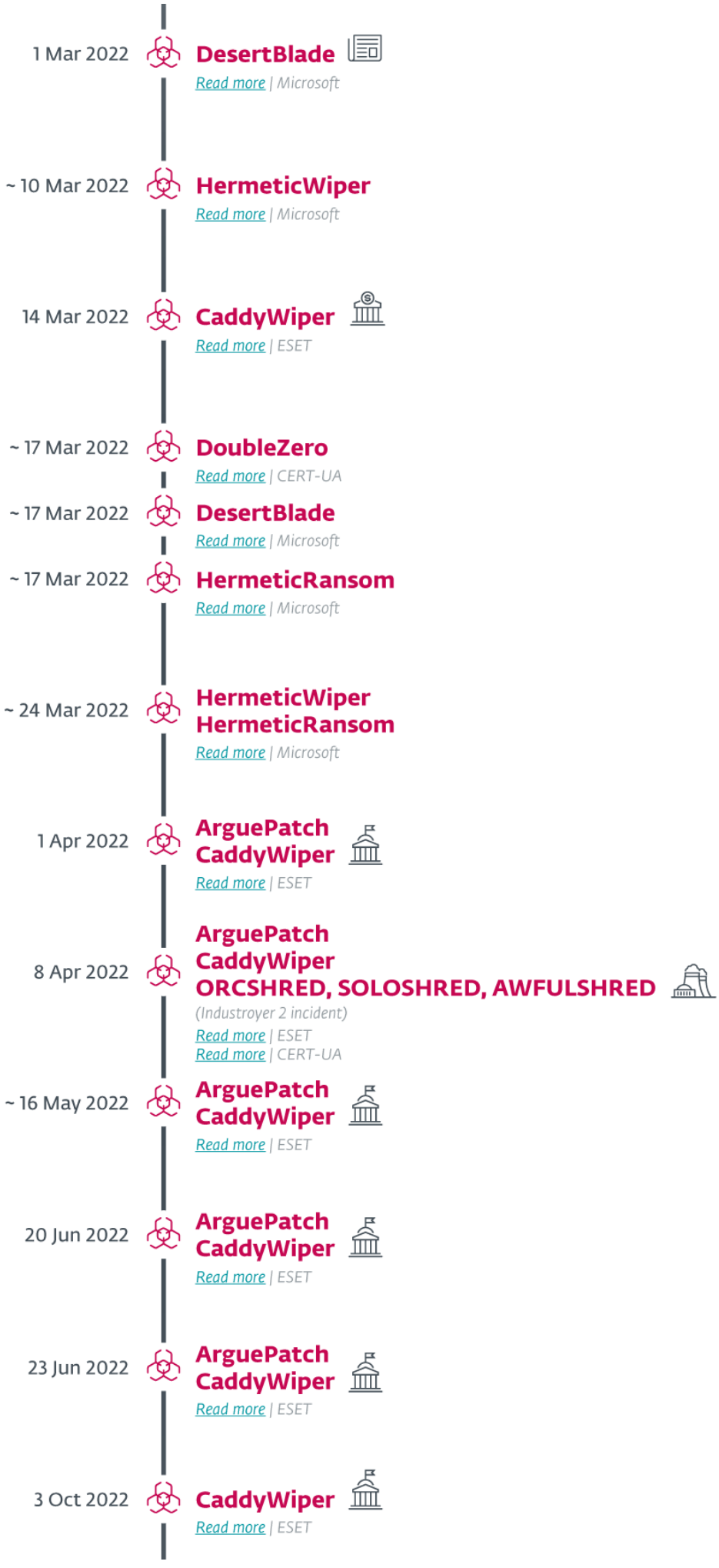
(e):r

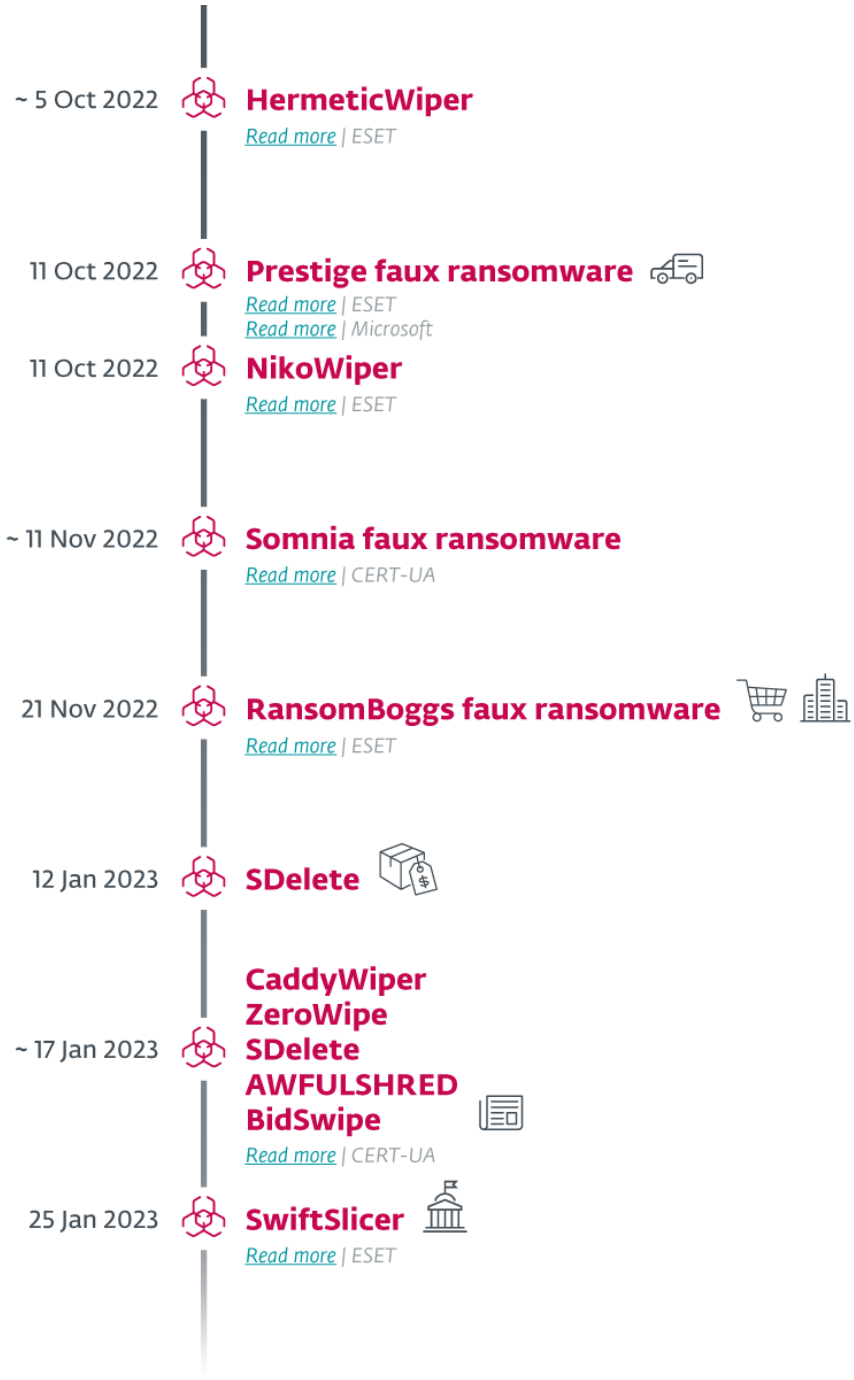
ESET Research
24 Feb 2023 - 11:30AM

ESET Research has compiled a timeline of cyberattacks that used wiper malware and have occurred since Russia's invasion of Ukraine in 2022

This blogpost presents a compiled overview of the disruptive wiper attacks that we have observed in Ukraine since the beginning of 2022, shortly before the Russian military invasion started. We were able to attribute the majority of these attacks to Sandworm, with varying degrees of confidence. The compilation includes attacks seen by ESET, as well as some reported by other reputable sources like CERT-UA, Microsoft, and SentinelOne.




1 Mar 2022
DesertBlade
Read more | Microsoft
~ 10 Mar 2022
HermeticWiper
Read more | Microsoft
14 Mar 2022
CaddyWiper
Read more | ESET
~ 17 Mar 2022
DoubleZero
Read more | CERT-UA
~ 17 Mar 2022
DesertBlade
Read more | Microsoft
~ 17 Mar 2022
HermeticRansom
Read more | Microsoft
~ 24 Mar 2022
HermeticWiper
HermeticRansom
Read more | Microsoft
1 Apr 2022
ArguePatch
CaddyWiper
Read more | ESET
8 Apr 2022
ArguePatch
CaddyWiper
ORCSHRED, SOLOSHRED, AWFULSHRED
(Industroyer 2 incident)
Read more | ESET
Read more | CERT-UA
~ 16 May 2022
ArguePatch
CaddyWiper
Read more | ESET
20 Jun 2022
ArguePatch
CaddyWiper
Read more | ESET
23 Jun 2022
ArguePatch
CaddyWiper
Read more | ESET
3 Oct 2022
CaddyWiper
Read more | ESET



Note: Approximate dates (~) are used when the exact date of deployment in uncertain or unknown. In some cases, the date of discovery or (in the case of non-ESET discoveries) the date of publication of the attack is used.

Pre-invasion

Among numerous waves of DDoS attacks that had been targeting Ukrainian institutions at the time, the WhisperGate malware struck on January 14th, 2022. The wiper masqueraded as ransomware, echoing NotPetya from June 2017 – a tactic that would also be seen in later attacks.

On February 23rd, 2022, a destructive campaign using HermeticWiper targeted hundreds of systems in at least five Ukrainian organizations. This data wiper was first spotted just before 17:00 local time (15:00 UTC): the cyberattack preceded, by only a few hours, the invasion of Ukraine by Russian Federation forces. Alongside HermeticWiper, the HermeticWizard worm and HermeticRansom faux ransomware were also deployed in the campaign.

Invasion and spring wave

On February 24th, 2022, with the Ukrainian winter thawing away, a second destructive attack against a Ukrainian governmental network started, using a wiper we have named IsaacWiper.

Also on the day of the invasion, the AcidRain wiper campaign targeted Viasat KA-SAT modems, with spillover outside of Ukraine as well.

Another wiper, initially disclosed by Microsoft, is DesertBlade, reportedly deployed on March 1st, 2022 and again around March 17th, 2022. The same report also mentions attacks using wipers from the Hermetic campaign, namely HermeticWiper (Microsoft calls it FoxBlade) around March 10th, 2022, HermeticRansom (Microsoft calls it SonicVote) around March 17th, 2022, and an attack around March 24th, 2022 using both HermeticWiper and HermeticRansom.

CERT-UA reported on its discovery of the DoubleZero wiper on March 17th, 2022.

On March 14th, 2022, ESET researchers detected an attack using CaddyWiper, which targeted a Ukrainian bank.

On April 1st, 2022, we detected CaddyWiper again, this time being loaded by the ArguePatch loader, which is typically a modified, legitimate binary that is used to load shellcode from an external file. We detected a similar scenario on May 16th, 2022, where ArguePatch took the form of a modified ESET binary.

We also detected the ArguePatch-CaddyWiper tandem on April 8th, 2022, in perhaps the most ambitious Sandworm attacks since the beginning of the invasion: their unsuccessful attempt to disrupt the flow of electricity using Industroyer2. In addition to ArguePatch and CaddyWiper, in this incident, we also discovered wipers for non-Windows platforms: ORCSHRED, SOLOSHRED, and AWFULSHRED. For details, see the notification by CERT-UA, and our WeLiveSecurity blogpost.

A quieter summer

The summer months saw fewer discoveries of new wiper campaigns in Ukraine as compared to the previous months, yet several notable attacks did occur.

We have worked together with CERT-UA on cases of ArguePatch (and CaddyWiper) deployments against Ukrainian institutions. The first incident took place in the week starting June 20th, 2022, and another on June 23rd, 2022.

Autumn wave

With temperatures dropping in preparation for the northern winter, on October 3rd, 2022 we detected a new version of CaddyWiper deployed in Ukraine. Unlike the previously used variants, this time CaddyWiper was compiled as an x64 Windows binary.

On October 5th, 2022, we identified a new version of HermeticWiper that had been uploaded to VirusTotal. The functionality of this HermeticWiper sample was the same as in the previous instances, with a few minor changes.

On October 11th, 2022, we detected Prestige ransomware being deployed against logistics companies in Ukraine and Poland. This campaign was also reported by Microsoft.

On the same day, we also identified a previously unknown wiper, which we named NikoWiper. This wiper was used against a company in the energy sector in Ukraine. NikoWiper is based on the SDelete Microsoft command line utility for securely deleting files.

On November 11th, 2022, CERT-UA published a blogpost about an attack using the Somnia faux ransomware.

On November 21st, 2022, we detected in Ukraine new ransomware written in .NET that we named RansomBoggs. The ransomware has multiple references to the movie Monsters, Inc. We observed that the malware operators used POWERGAP scripts to deploy this filecoder.

January 2023

In 2023 the disruptive attacks against Ukrainian institutions continue.

On January 1st, 2023, we detected execution of the SDelete utility at a Ukrainian software reseller.

Another attack using multiple wipers, this time against a Ukrainian news agency, took place on January 17th, 2023, according to CERT-UA. The following wipers were detected in this attack: CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe. BidSwipe is noteworthy, as it is a FreeBSD OS wiper.

On January 25th, 2023, we detected a new wiper, written in Go and that we named SwiftSlicer, being deployed against Ukrainian local government entities.

In almost all the above-mentioned cases, Sandworm used Active Directory Group Policy (T1484.001) to deploy its wipers and ransomware, specifically using the POWERGAP script.

Conclusion

The use of disruptive wipers – and even wipers masquerading as ransomware – by Russian APT groups, especially Sandworm, against Ukrainian organizations is hardly new. Since around 2014, BlackEnergy employed disruptive plugins; the KillDisk wiper was a common denominator in Sandworm attacks in the past; and the Telebots subgroup has launched numerous wiper attacks, most infamously NotPetya.

Yet the intensification of wiper campaigns since the military invasion in February 2022 has been unprecedented. On a positive note, many of the attacks have been detected and thwarted. However, we continue to monitor the situation vigilantly, as we expect the attacks to continue.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.

ESET Research also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page

IoCs

Files

SHA-1	Filename	ESET detection name	
189166D382C73C242BA45889D57980548D4BA37E	stage1.exe	Win32/KillMBR.NGI	Wi sta ov
A67205DC84EC29EB71BB259B19C1A1783865C0FC	N/A	Win32/KillFiles.NKU	Wi sta pa
912342F1C840A42F6B74132F8A7C4FFE7D40FB77	com.exe	Win32/KillDisk.NCV	He
61B25D11392172E587D8DA3045812A66C3385451	conhosts.exe	Win32/KillDisk.NCV	He
F32D791EC9E6385A91B45942C230F52AFF1626DF	cc2.exe	WinGo/Filecoder.BK	He
86906B140B019FDEDAABA73948D0C8F96A6B1B42	ukrop	Linux/AcidRain.A	Ac
AD602039C6F0237D4A997D5640E92CE5E2B3BBA3	cl64.dll	Win32/KillMBR.NHP	Isa
736A4CFAD1ED83A6A0B75B0474D5E01A3A36F950	cld.dll	Win32/KillMBR.NHQ	Isa
E9B96E9B86FAD28D950CA428879168E0894D854F	clean.exe	Win32/KillMBR.NHP	Isa
5C01947A49280CE98FB39D0B72311B47C47BC5CC	clean.exe	Win32/KillMBR.NHP	Isa
59F5B9AECE751E58BE16E7F7A7A6D8C044F583BE	cll.exe	Win32/KillMBR.NHQ	Isa
172FBE91867C1D6B7F3E2899CEA69113BB1F21A0	notes.exe	WinGo/KillFiles.A	De wi
46671348C1A61B3A8BFBA025E64E5549B7FDFA98	N/A	Win32/KillDisk.NCV	He
DB0DA0D92D90657EA91C02336E0605E96DB92C05	clrs.exe	Win32/KillDisk.NCV	He
98B3FB74B3E8B3F9B05A82473551C5A77B576D54	caddy.exe	Win32/KillDisk.NCX	Ca
320116162D78AFB8E00FD972591479A899D3DFEE	cpcrs.exe	MSIL/KillFiles.CK	Dc wi
43B3D5FFAE55116C68C504339C5D953CA25C0E3F	csrss.exe	MSIL/KillFiles.CK	Dc wi
48F54A1D93C912ADF36C79BB56018DEFF190A35C	ukcphone.exe	Win32/Agent.AECG	Ar sh
6FA04992C0624C7AA3CA80DA6A30E6DE91226A16	peremoga.exe	Win32/Agent.AECG	Ar sh
9CE1491CE69809F92AE1FE8D4C0783BD1D11FBE7	pa1.pay	Win32/KillDisk.NDA	En Ca sh
3CDBC19BC4F12D8D00B81380F7A2504D08074C15	wobf.sh	Linux/KillFiles.C	Aw wi
8FC7646FA14667D07E3110FE754F61A78CFDE6BC	wsol.sh	Linux/KillFiles.B	So wi
796362BD0304E305AD120576B6A8FB6721108752	eset_ssl_filtered_cert_importer.exe	Win32/Agent.AEGY	Ar sh
8F3830CB2B93C21818FDBFCF526A027601277F9B	spn.exe	Win32/Agent.AEKA	Ar sh
3D5C2E1B792F690FBCF05441DF179A3A48888618	mslrss.exe	Win32/Agent.AEKA	Ar sh
EB437FF79E639742EE36E89F30C6A21072B86CBC	caclcly.exe	Win64/Agent.BQZ	Ca
57E3D0108636F6EE56C801F128306AD43AF60EE6	cmrss.exe	Win32/KillDisk.NCV	He
986BA7A5714AD5B0DE0D040D1C066389BCB81A67	open.exe	Win32/Filecoder.Prestige.A	Pr
C7186DEF5E9C3E1B01BF506F538F5D6185377A9C	sysate32.exe	Win32/Filecoder.Prestige.A	Pr

SHA-1	Filename	ESET detection name	
59621F5EFC311FDFE66683266CE9CB17F8227B23	mstc_niko.exe	Win32/DelAll.NAH	Nil
84E6A010B372D845C723A8B8D7DDD8D79675DCE5	Sullivan.1.v2.0.exe	MSIL/Filecoder.RansomBoggs.A	Ra file
F4D1C047923B9D10031BB709AABF1A250AB0AAA2	Sullivan.1.v4.5.exe	MSIL/Filecoder.RansomBoggs.A	Ra file
9A3D63C6E127243B3036BC0E242789EC1D2AB171	Sullivan.2.v2.exe	MSIL/Filecoder.RansomBoggs.A	Ra file
BB187EB125070176BD7EC6C57CFF166708DD60E1	Sullivan.2.v4.exe	MSIL/Filecoder.RansomBoggs.A	Ra file
3D593A39FA20FED851B9BEFB4FF2D391B43BDF08	Sullivan.v2.5.exe	MSIL/Filecoder.RansomBoggs.A	Ra file
021308C361C8DE7C38EF135BC3B53439EB4DA0B4	Sullivan.v4.5.exe	MSIL/Filecoder.RansomBoggs.A	Ra file
7346E2E29FADDD63AE5C610C07ACAB46B2B1B176	help.exe	WinGo/KillFiles.C	Sw

24 Feb 2023 - 11:30AM