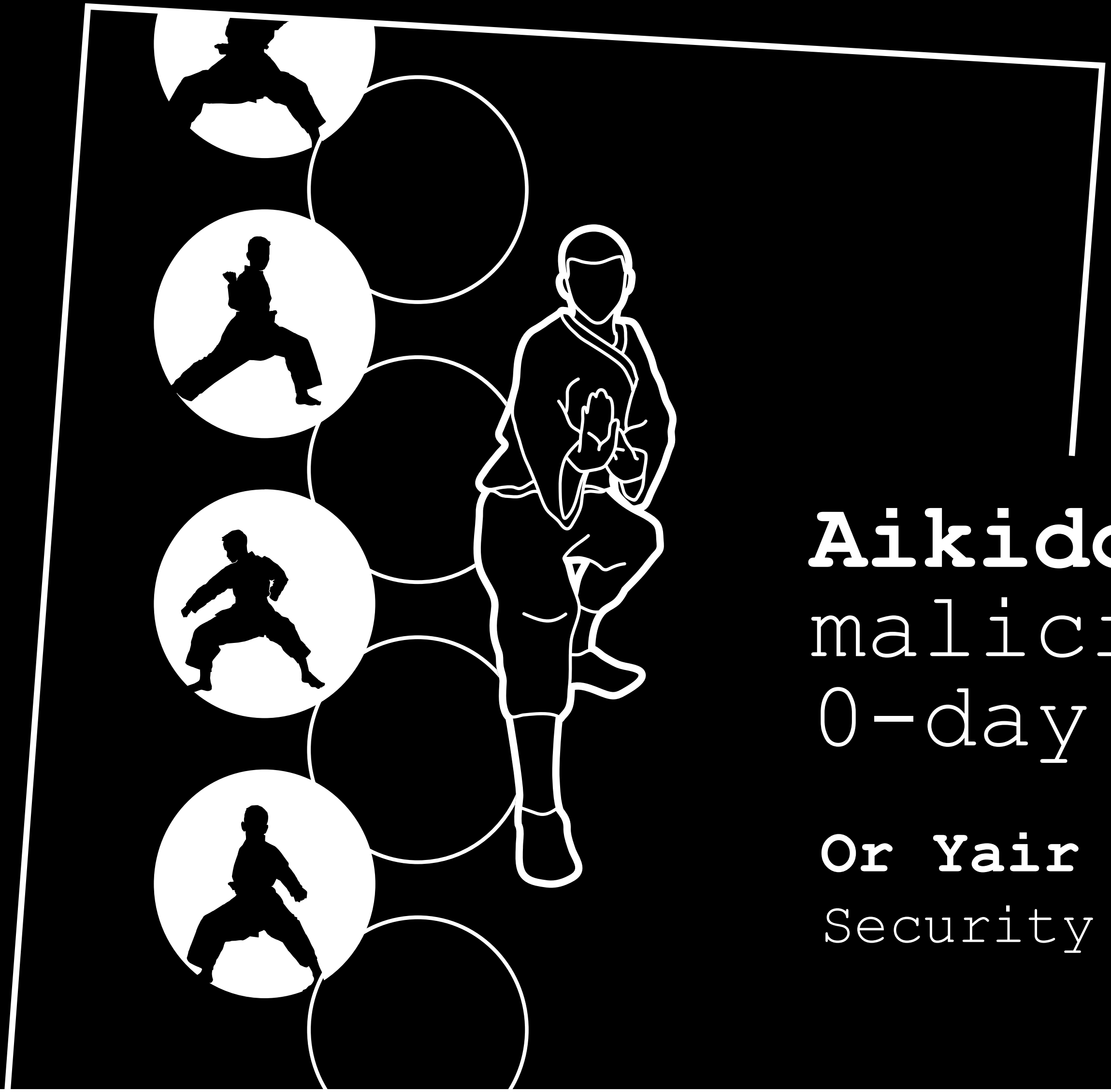


Aikido: Turning EDRs to malicious wipers using 0-day exploits

Or Yair

Security Research Team Lead, SafeBreach

Or Yair

Security Research Team Lead at SafeBreach

6+ years in security research

Linux, embedded and some Android research

3+ years Windows research

SafeBreach

Agenda

Research goal

Wipers background

Research process

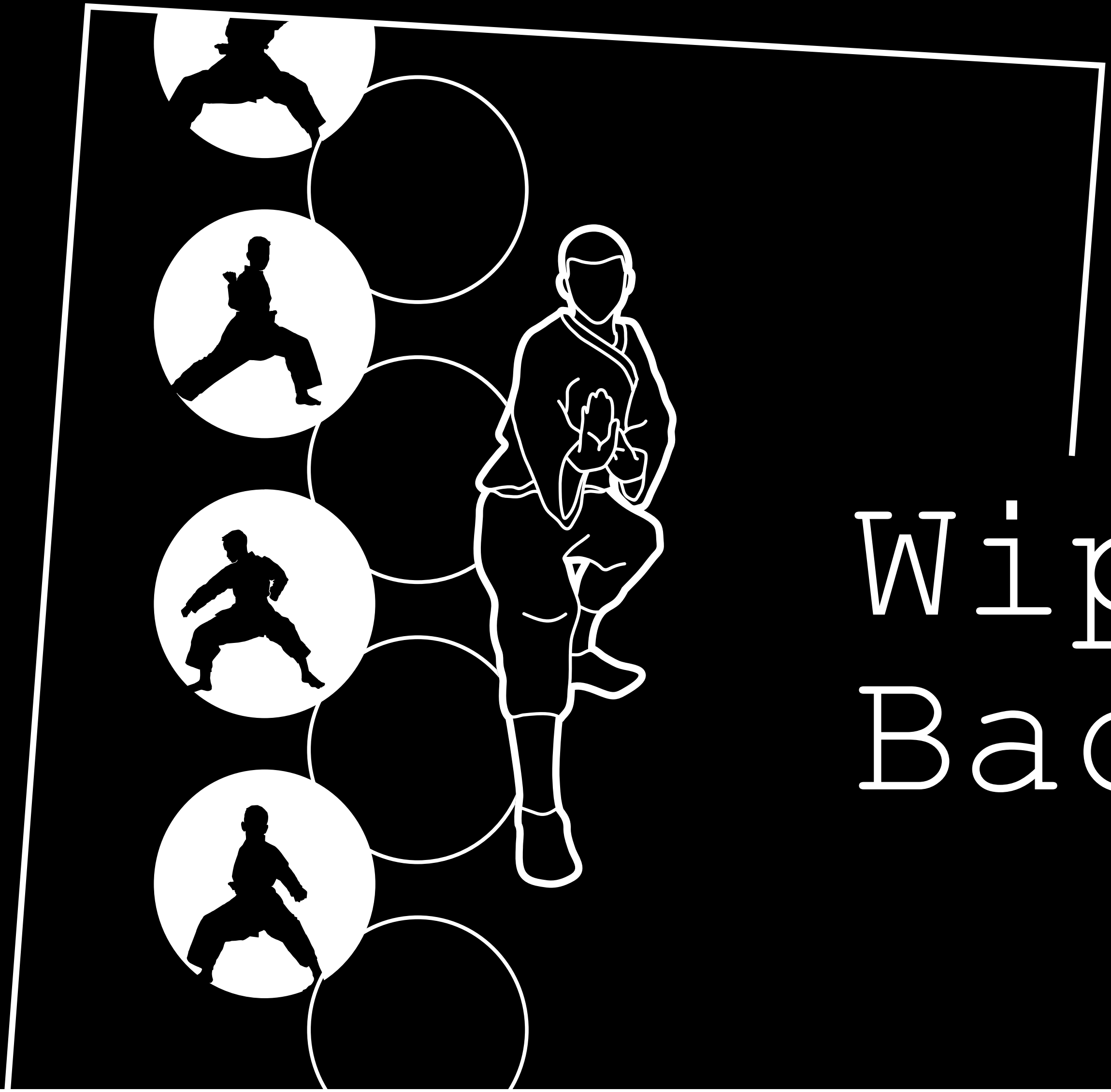
0-day vulnerabilities

Aikido Wiper

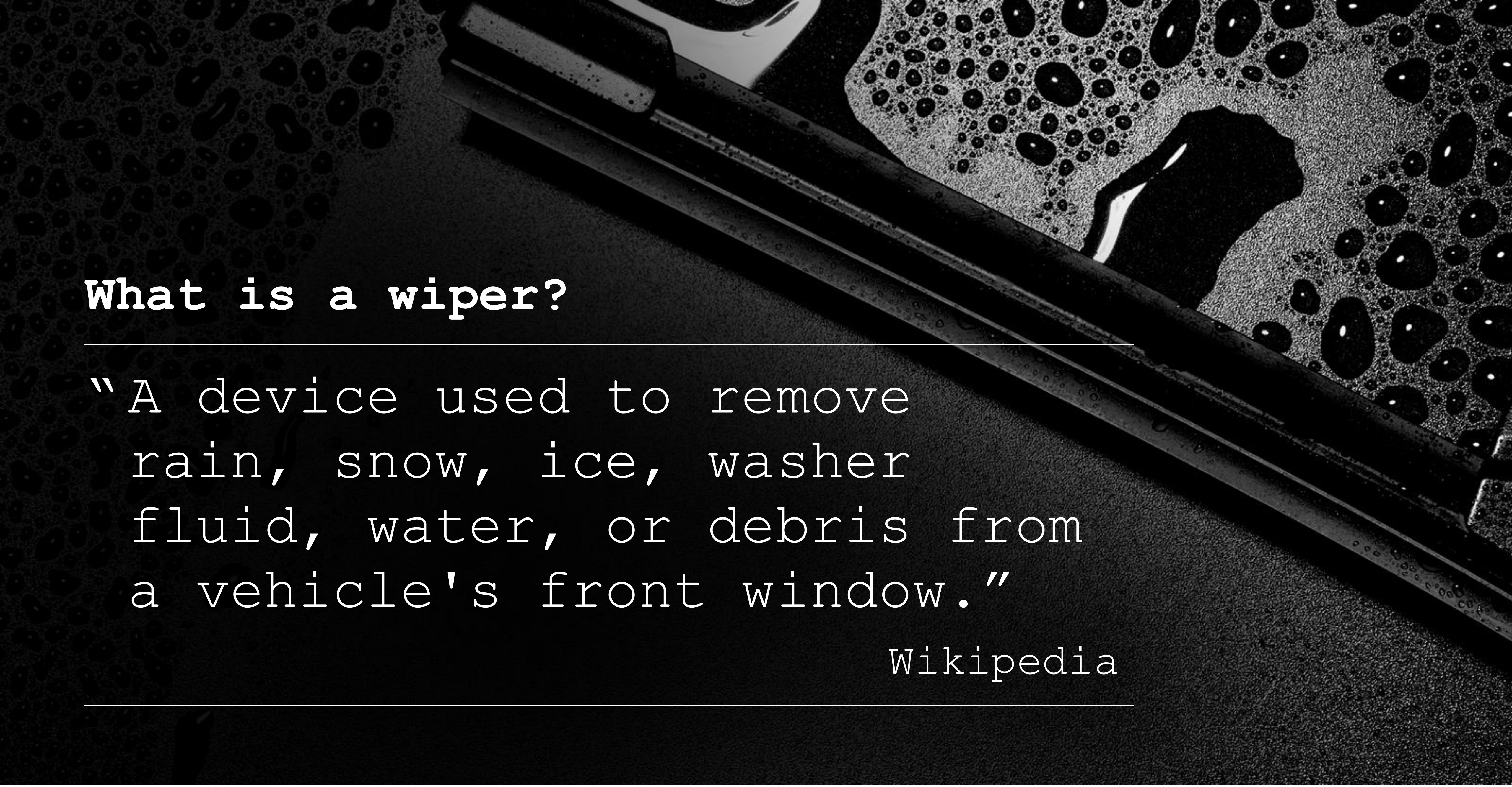
Summary

Research Goal

Creating the next-gen wiper

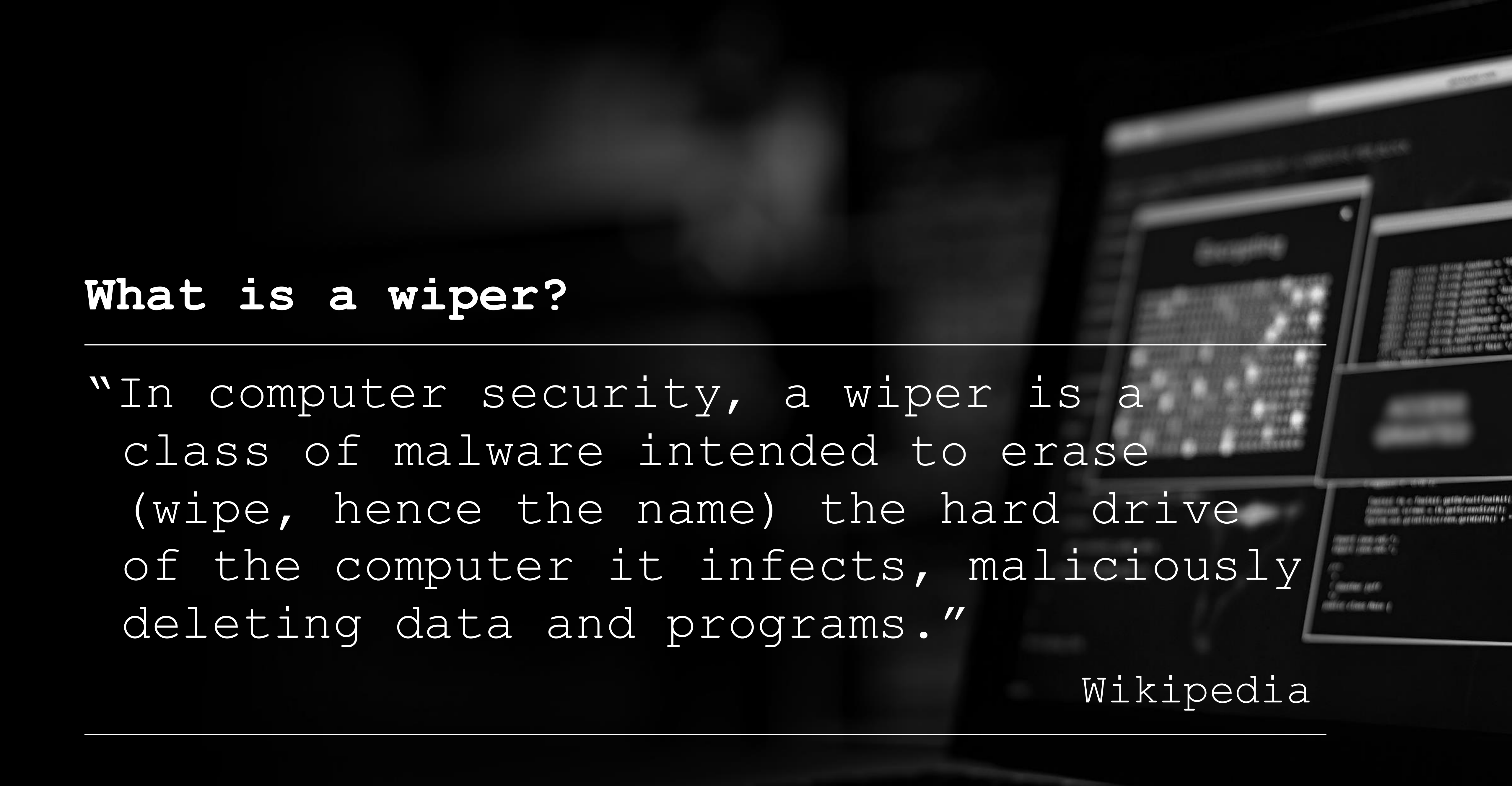


Wipers Background



What is a wiper?

> "A device used to remove rain, snow, ice, washer fluid, water, or debris from a vehicle's front window."
>
> Wikipedia



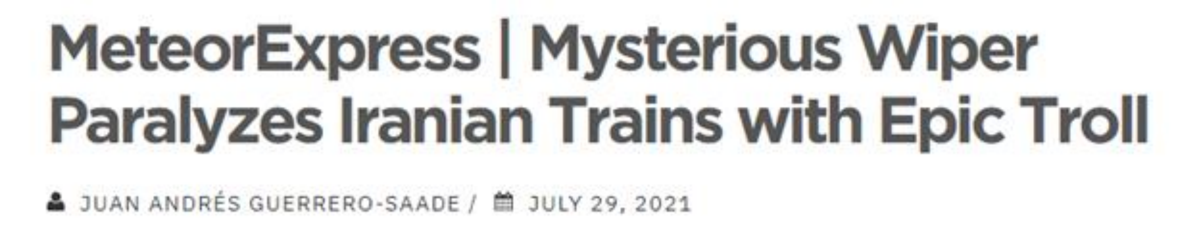
What is a wiper?

"In computer security, a wiper is a class of malware intended to erase (wipe, hence the name) the hard drive of the computer it infects, maliciously deleting data and programs."

Wikipedia

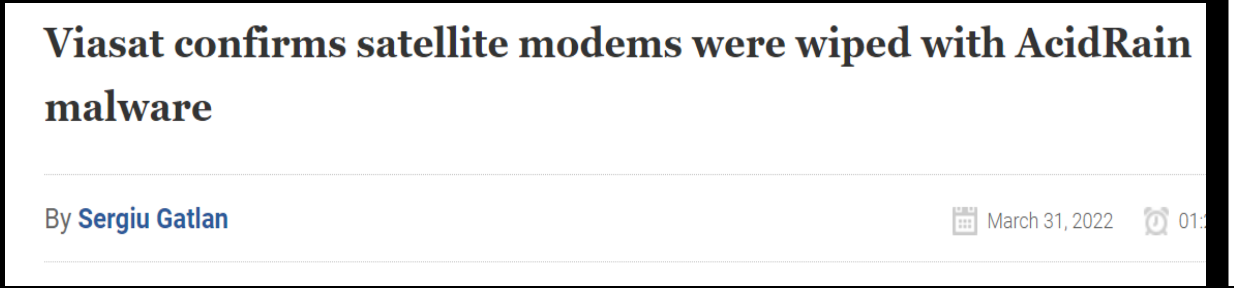
Why are wipers used?

Harm a certain entity (State, Company, etc…)



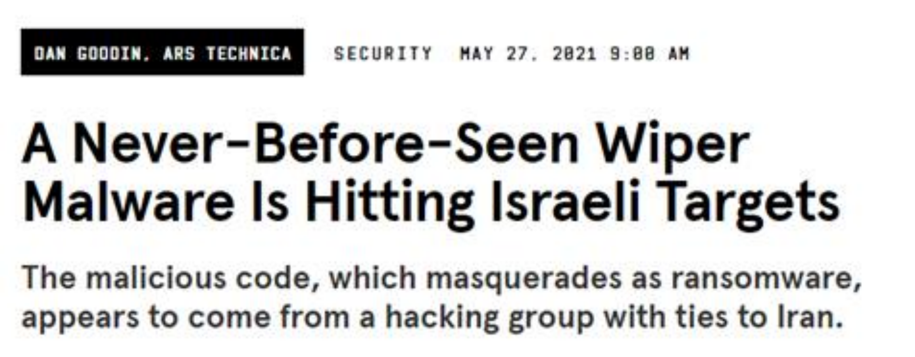
MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll

JUAN ANDRÉS GUERRERO-SAADE / JULY 29, 2021



Viasat confirms satellite modems were wiped with AcidRain malware

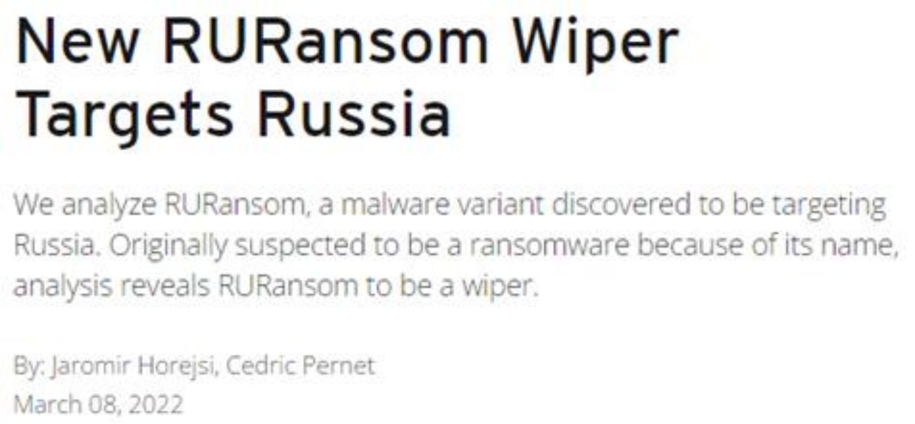
By Sergiu Gatlan March 31, 2022 01:



DAN GOODIN, ARS TECHNICA SECURITY MAY 27, 2021 9:00 AM

A Never-Before-Seen Wiper Malware Is Hitting Israeli Targets

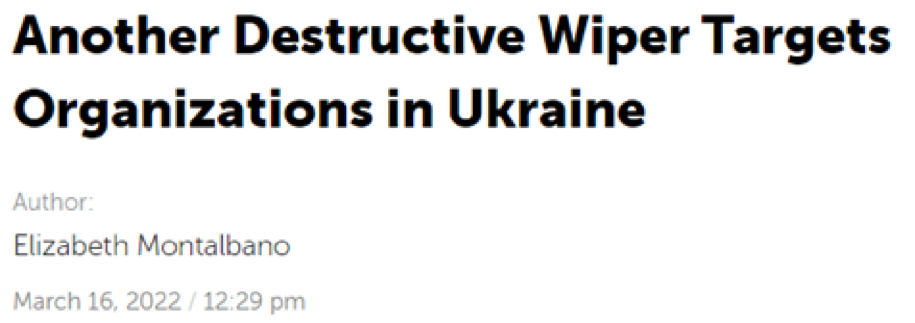
The malicious code, which masquerades as ransomware, appears to come from a hacking group with ties to Iran.



New RURansom Wiper Targets Russia

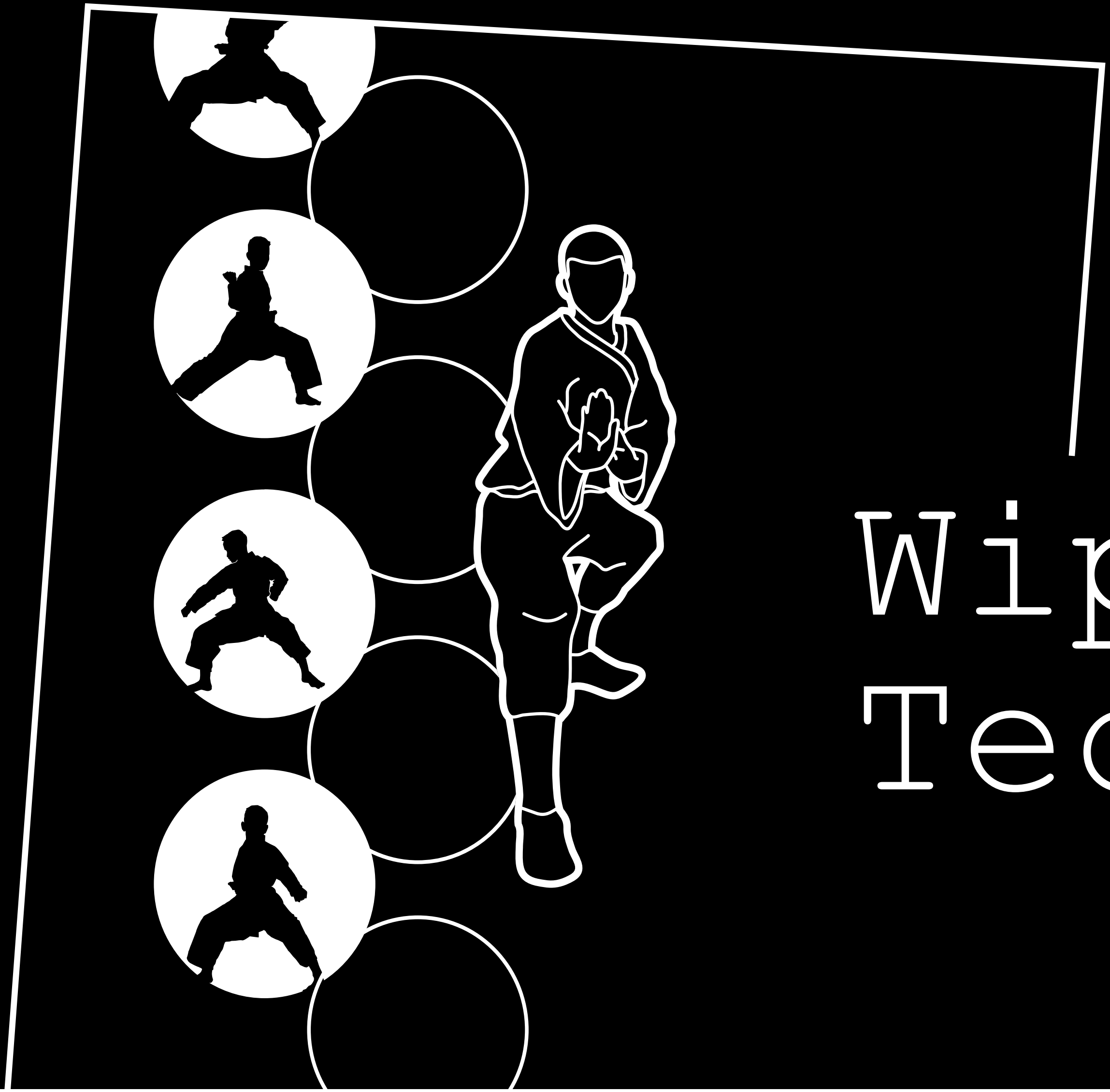
We analyze RURansom, a malware variant discovered to be targeting Russia. Originally suspected to be a ransomware because of its name, analysis reveals RURansom to be a wiper.

By: Jaromir Horejsi, Cedric Pernet
March 08, 2022



Another Destructive Wiper Targets Organizations in Ukraine

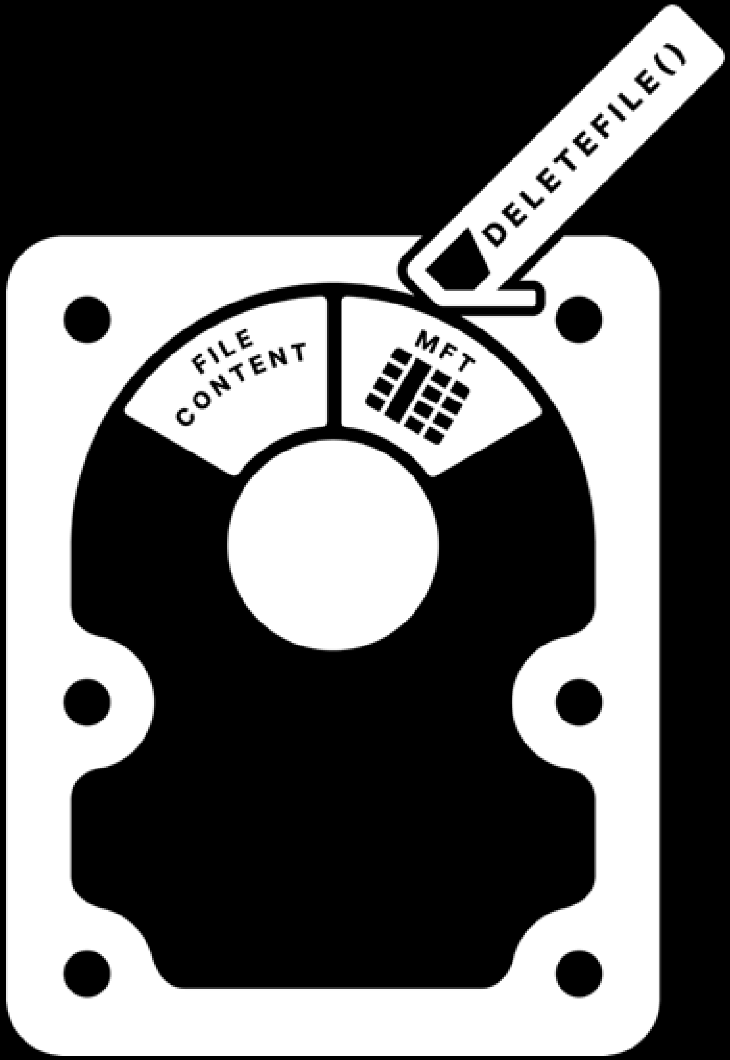
Author:
Elizabeth Montalbano
March 16, 2022 / 12:29 pm



Wipers Techniques

File Deletion

Not enough



Delete to Wipe

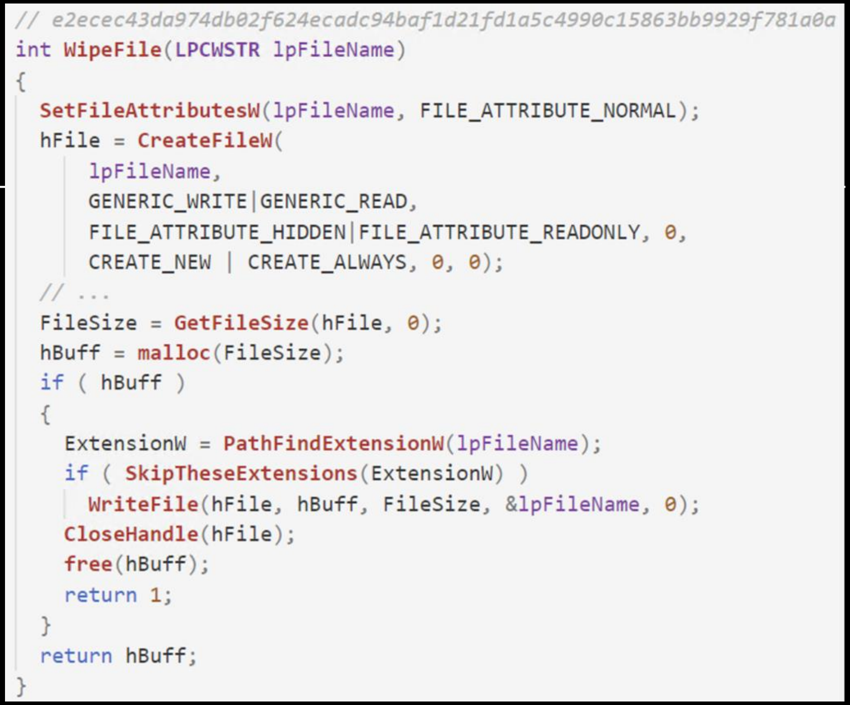
MSDN:

"When files are deleted from an NTFS file system volume, their MFT entries are marked as free and may be reused."

File Overwrite

Overwrites the actual content of files

- Admin’s files require Admin’s privileges

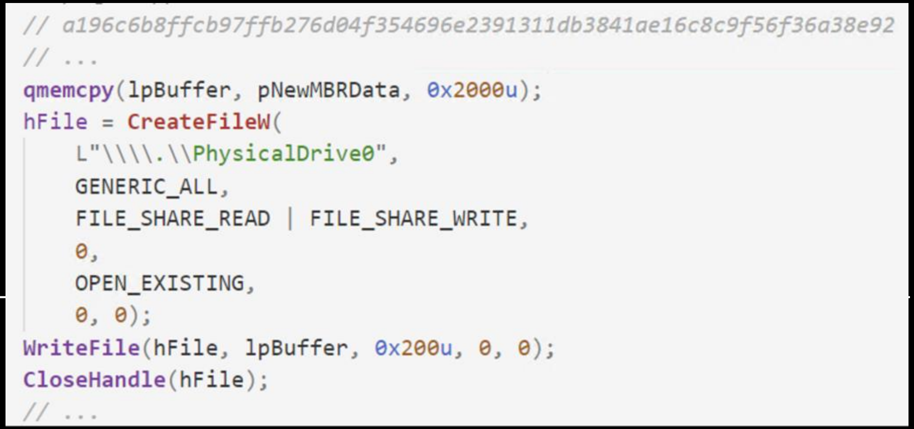


```
// e2ecec43da974db02f624ecadc94baf1d21fd1a5c4990c15863bb9929f781a0a
int WipeFile(LPCWSTR lpFileName)
{
  SetFileAttributesW(lpFileName, FILE_ATTRIBUTE_NORMAL);
  hFile = CreateFileW(
      lpFileName,
      GENERIC_WRITE|GENERIC_READ,
      FILE_ATTRIBUTE_HIDDEN|FILE_ATTRIBUTE_READONLY, 0,
      CREATE_NEW | CREATE_ALWAYS, 0, 0);
  // ...
  FileSize = GetFileSize(hFile, 0);
  hBuff = malloc(FileSize);
  if ( hBuff )
  {
    ExtensionW = PathFindExtensionW(lpFileName);
    if ( SkipTheseExtensions(ExtensionW) )
      WriteFile(hFile, hBuff, FileSize, &lpFileName, 0);
    CloseHandle(hFile);
    free(hBuff);
    return 1;
  }
  return hBuff;
}
```

Used by: Shamoon, CaddyWiper, DoubleZero, IsaacWiper, KillDisk, Meteor

Image Source: https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/

Drive Destruction



```
// a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
// ...
qmemcpy(lpBuffer, pNewMBRData, 0x2000u);
hFile = CreateFileW(
    L"\\\\.\\PhysicalDrive0",
    GENERIC_ALL,
    FILE_SHARE_READ | FILE_SHARE_WRITE,
    0,
    OPEN_EXISTING,
    0, 0);
WriteFile(hFile, lpBuffer, 0x200u, 0, 0);
CloseHandle(hFile);
// ...
```

Writing directly to `\\.\PhysicalDisk0` and/or `\\.\C:`

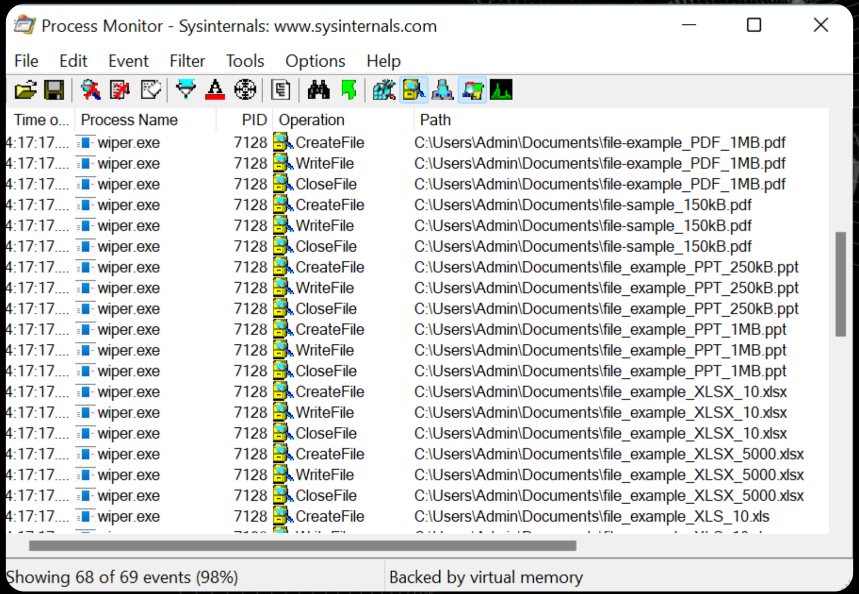
- Requires Administrator privileges

Used by: IsaacWiper, KillDisk, Petya wiper variant, SQLShred, StoneDrill, WhisperGate and DriveSlayer

Image Source: https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/

Wiper Techniques

Every technique is obviously initiated by the wiper itself



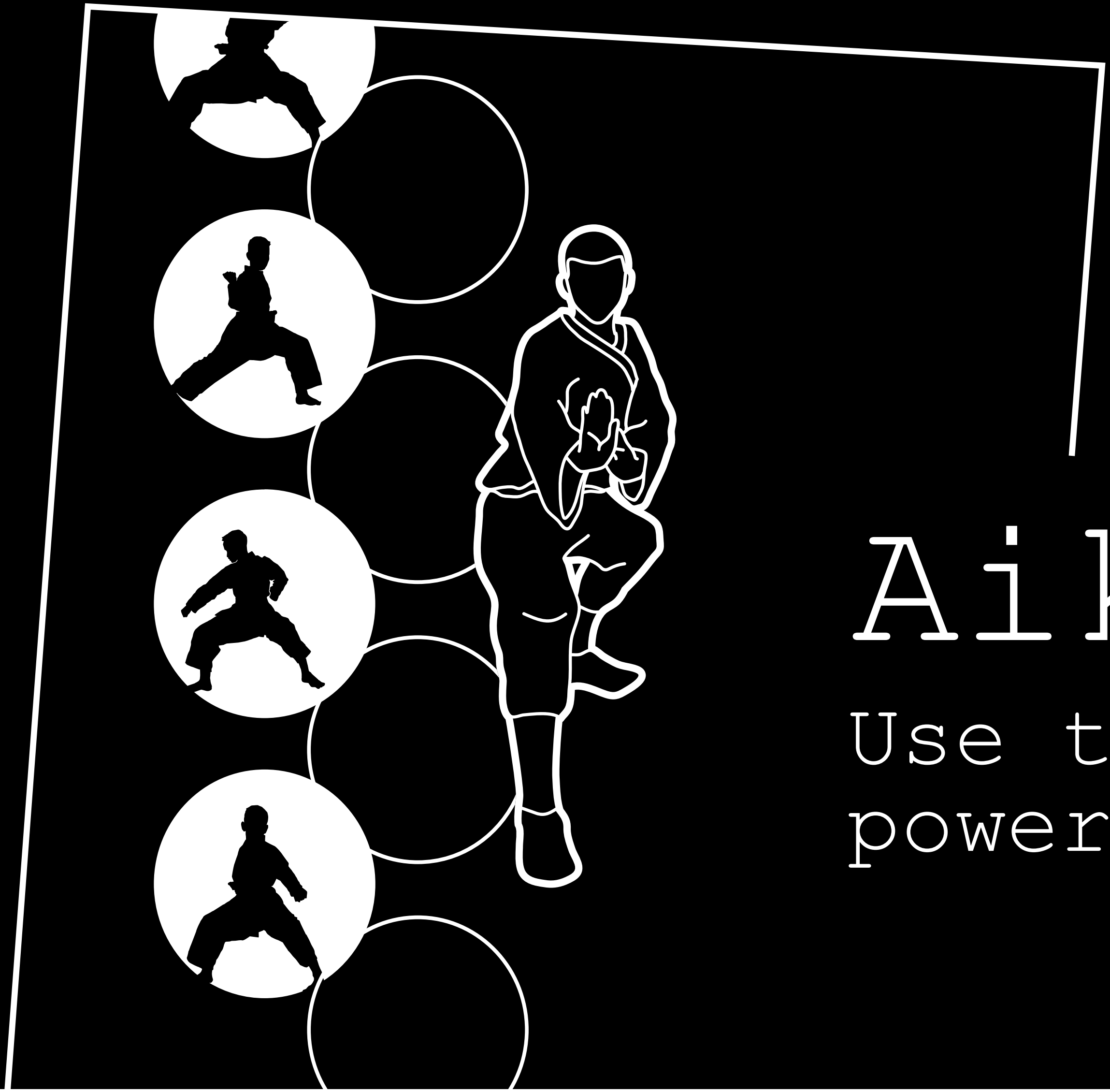
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path
4:17:17....	wiper.exe	7128	CreateFile	C:\Users\Admin\Documents\file-example_PDF_1MB.pdf
4:17:17....	wiper.exe	7128	WriteFile	C:\Users\Admin\Documents\file-example_PDF_1MB.pdf
4:17:17....	wiper.exe	7128	CloseFile	C:\Users\Admin\Documents\file-example_PDF_1MB.pdf
4:17:17....	wiper.exe	7128	CreateFile	C:\Users\Admin\Documents\file-sample_150kB.pdf
4:17:17....	wiper.exe	7128	WriteFile	C:\Users\Admin\Documents\file-sample_150kB.pdf
4:17:17....	wiper.exe	7128	CloseFile	C:\Users\Admin\Documents\file-sample_150kB.pdf
4:17:17....	wiper.exe	7128	CreateFile	C:\Users\Admin\Documents\file_example_PPT_250kB.ppt
4:17:17....	wiper.exe	7128	WriteFile	C:\Users\Admin\Documents\file_example_PPT_250kB.ppt
4:17:17....	wiper.exe	7128	CloseFile	C:\Users\Admin\Documents\file_example_PPT_250kB.ppt
4:17:17....	wiper.exe	7128	CreateFile	C:\Users\Admin\Documents\file_example_PPT_1MB.ppt
4:17:17....	wiper.exe	7128	WriteFile	C:\Users\Admin\Documents\file_example_PPT_1MB.ppt
4:17:17....	wiper.exe	7128	CloseFile	C:\Users\Admin\Documents\file_example_PPT_1MB.ppt
4:17:17....	wiper.exe	7128	CreateFile	C:\Users\Admin\Documents\file_example_XLSX_10.xlsx
4:17:17....	wiper.exe	7128	WriteFile	C:\Users\Admin\Documents\file_example_XLSX_10.xlsx
4:17:17....	wiper.exe	7128	CloseFile	C:\Users\Admin\Documents\file_example_XLSX_10.xlsx
4:17:17....	wiper.exe	7128	CreateFile	C:\Users\Admin\Documents\file_example_XLSX_5000.xlsx
4:17:17....	wiper.exe	7128	WriteFile	C:\Users\Admin\Documents\file_example_XLSX_5000.xlsx
4:17:17....	wiper.exe	7128	CloseFile	C:\Users\Admin\Documents\file_example_XLSX_5000.xlsx
4:17:17....	wiper.exe	7128	CreateFile	C:\Users\Admin\Documents\file_example_XLS_10.xls

Showing 68 of 69 events (98%)   Backed by virtual memory

What Ifs

- What if the next-gen wiper could wipe files without using these obvious API calls?
- What if the next-gen wiper could do all that as an unprivileged user?



Aikido

Use the opponent's power against them

The Super Power of EDR Products

Delete any file no matter the privileges

When are malicious files deleted or quarantined?

Depends on configuration

On open

On close after write

Scan

How can we exploit the power of the opponent (AV / EDR)?

We can trigger a deletion

Trigger a deletion for the wrong file

Target Confusion

FIRST IDEA

Add malicious content to an innocent file

- Requires write permissions to the file
- Looks like file overwrite

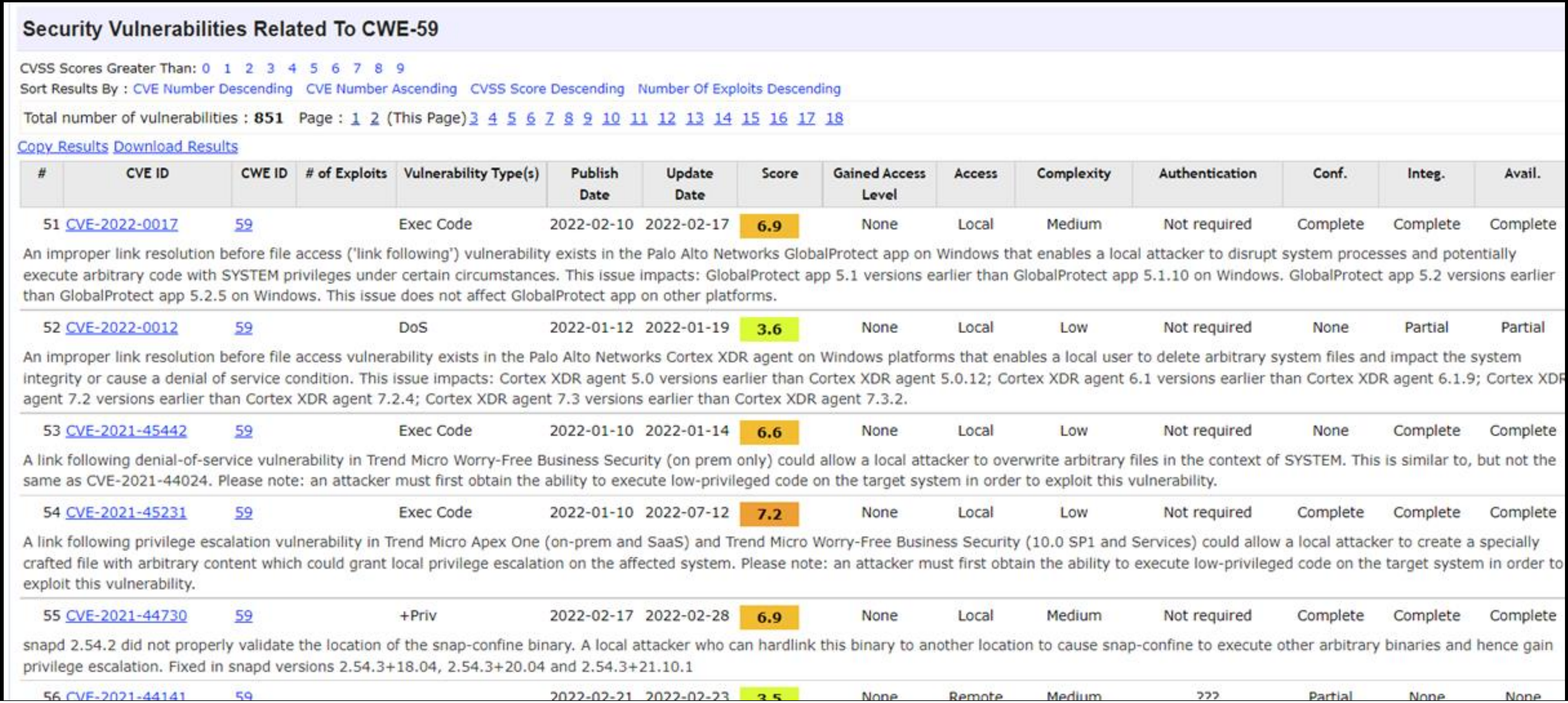
Target Confusion

SECOND IDEA

Somehow point the security control to a different path

- Links

Symlinks and Junctions Vulnerabilities - CWE-59



Security Vulnerabilities Related To CWE-59

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **851** Page : 1 2 (This Page) 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

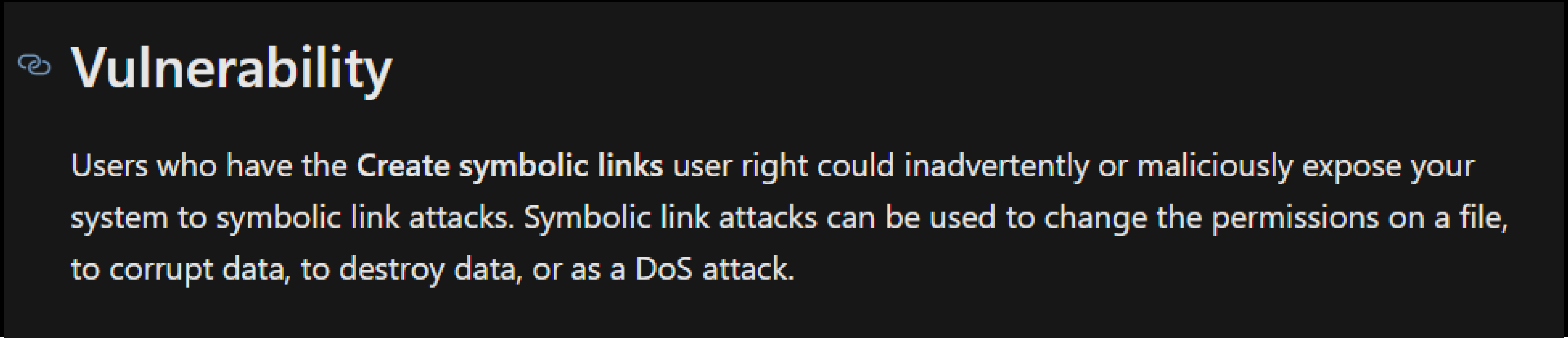
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
51	CVE-2022-0017	59		Exec Code	2022-02-10	2022-02-17	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
An improper link resolution before file access ('link following') vulnerability exists in the Palo Alto Networks GlobalProtect app on Windows that enables a local attacker to disrupt system processes and potentially execute arbitrary code with SYSTEM privileges under certain circumstances. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.10 on Windows. GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.5 on Windows. This issue does not affect GlobalProtect app on other platforms.														
52	CVE-2022-0012	59		DoS	2022-01-12	2022-01-19	3.6	None	Local	Low	Not required	None	Partial	Partial
An improper link resolution before file access vulnerability exists in the Palo Alto Networks Cortex XDR agent on Windows platforms that enables a local user to delete arbitrary system files and impact the system integrity or cause a denial of service condition. This issue impacts: Cortex XDR agent 5.0 versions earlier than Cortex XDR agent 5.0.12; Cortex XDR agent 6.1 versions earlier than Cortex XDR agent 6.1.9; Cortex XDR agent 7.2 versions earlier than Cortex XDR agent 7.2.4; Cortex XDR agent 7.3 versions earlier than Cortex XDR agent 7.3.2.														
53	CVE-2021-45442	59		Exec Code	2022-01-10	2022-01-14	6.6	None	Local	Low	Not required	None	Complete	Complete
A link following denial-of-service vulnerability in Trend Micro Worry-Free Business Security (on prem only) could allow a local attacker to overwrite arbitrary files in the context of SYSTEM. This is similar to, but not the same as CVE-2021-44024. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.														
54	CVE-2021-45231	59		Exec Code	2022-01-10	2022-07-12	7.2	None	Local	Low	Not required	Complete	Complete	Complete
A link following privilege escalation vulnerability in Trend Micro Apex One (on-prem and SaaS) and Trend Micro Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to create a specially crafted file with arbitrary content which could grant local privilege escalation on the affected system. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.														
55	CVE-2021-44730	59		+Priv	2022-02-17	2022-02-28	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
snapd 2.54.2 did not properly validate the location of the snap-confine binary. A local attacker who can hardlink this binary to another location to cause snap-confine to execute other arbitrary binaries and hence gain privilege escalation. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1														
56	CVE-2021-44141	59			2022-02-21	2022-02-23	3.5	None	Remote	Medium	???	Partial	None	None

JUNCTIONS VS SYMLINKS

Junctions	Symlinks
No special permissions are required	“Create symbolic link” user right is required

MICROSOFT

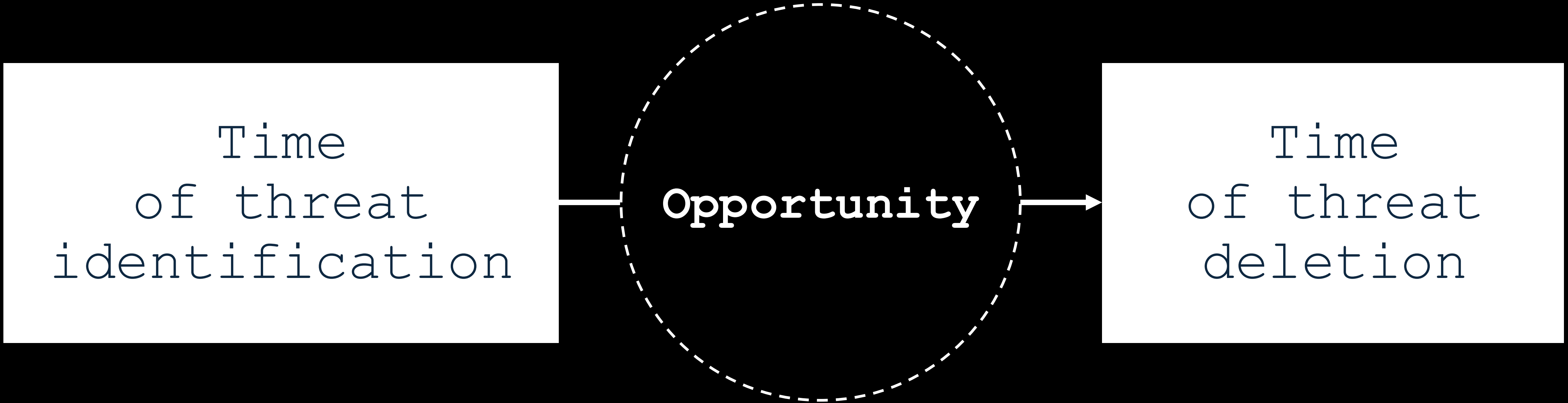


Vulnerability

Users who have the **Create symbolic links** user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a DoS attack.

Windows of Opportunity

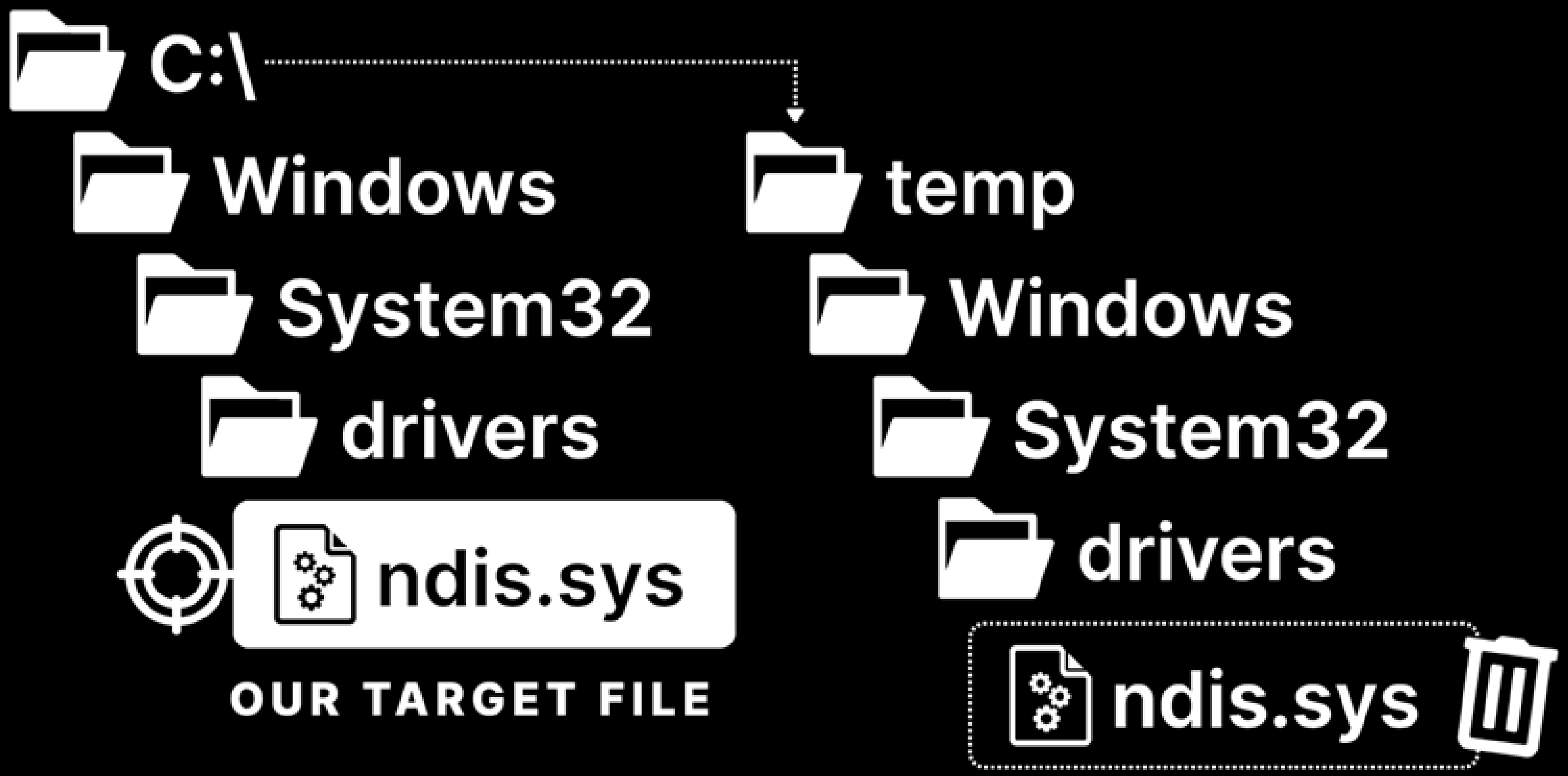
Windows of Opportunity - TOCTOU



Time of threat identification

Opportunity

Time of threat deletion



C:\
Windows
System32
drivers
ndis.sys

OUR TARGET FILE

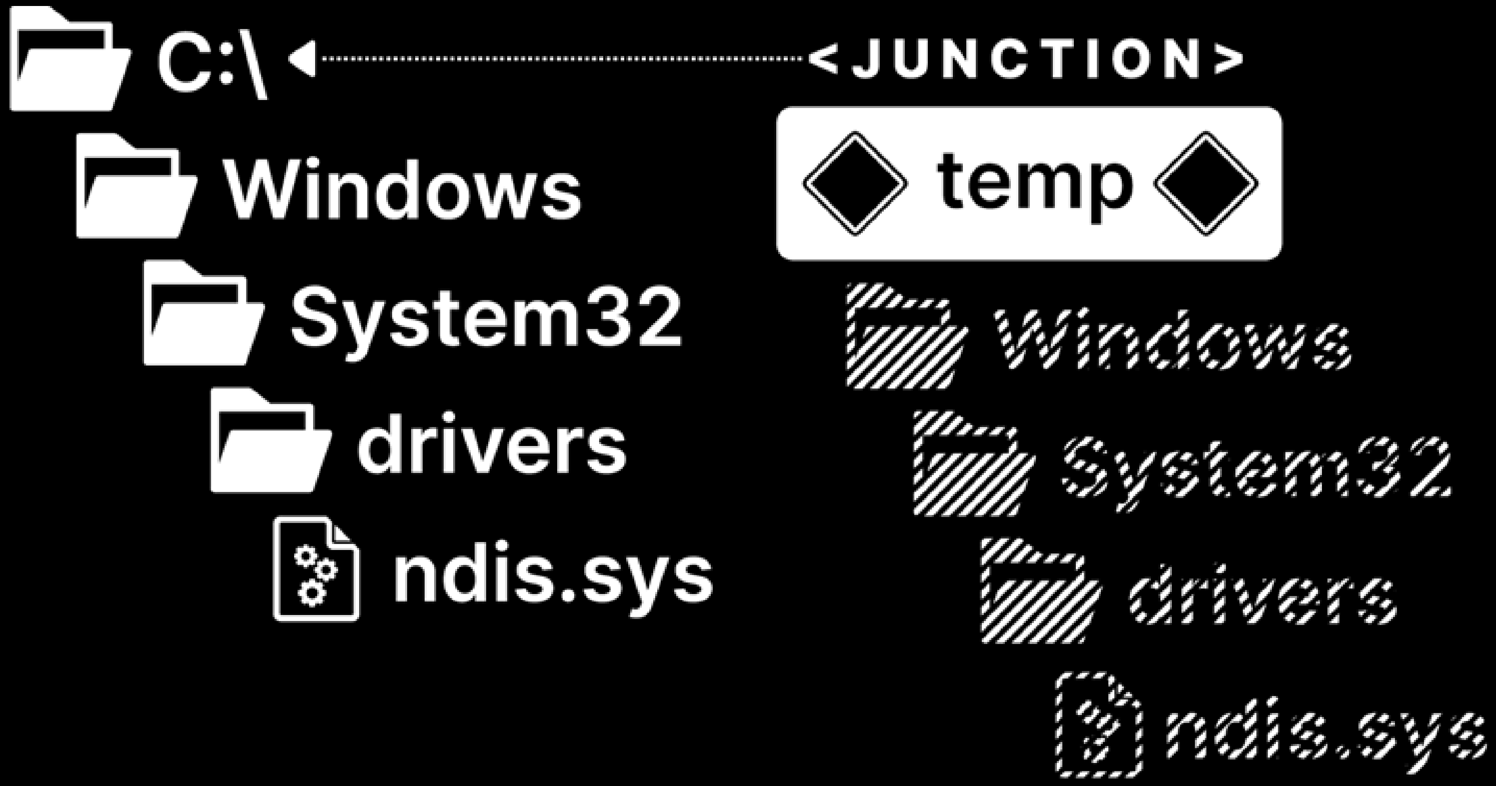
temp
Windows
System32
drivers
ndis.sys

PRIVILEGED PROGRAM IS ABOUT TO DELETE THIS FILE

```
C:\temp\Windows\System32\drivers\ndis.sys
```

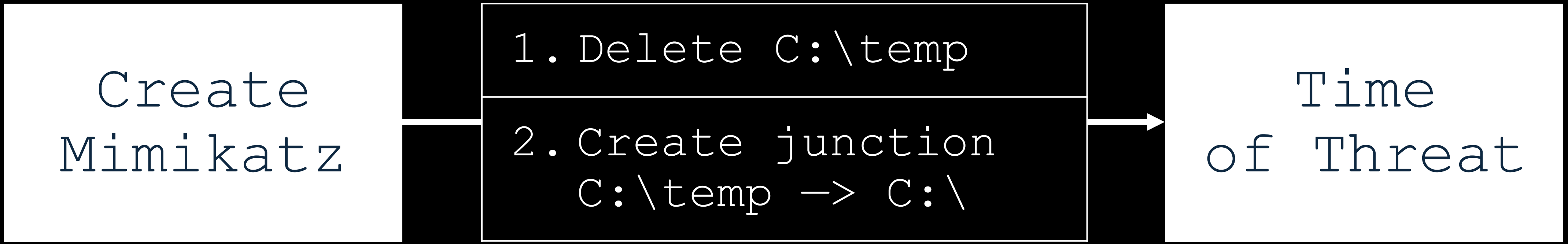
`C:\`**temp**`\Windows\System32\drivers\ndis.sys`

Same path leads to the original ndis.sys file



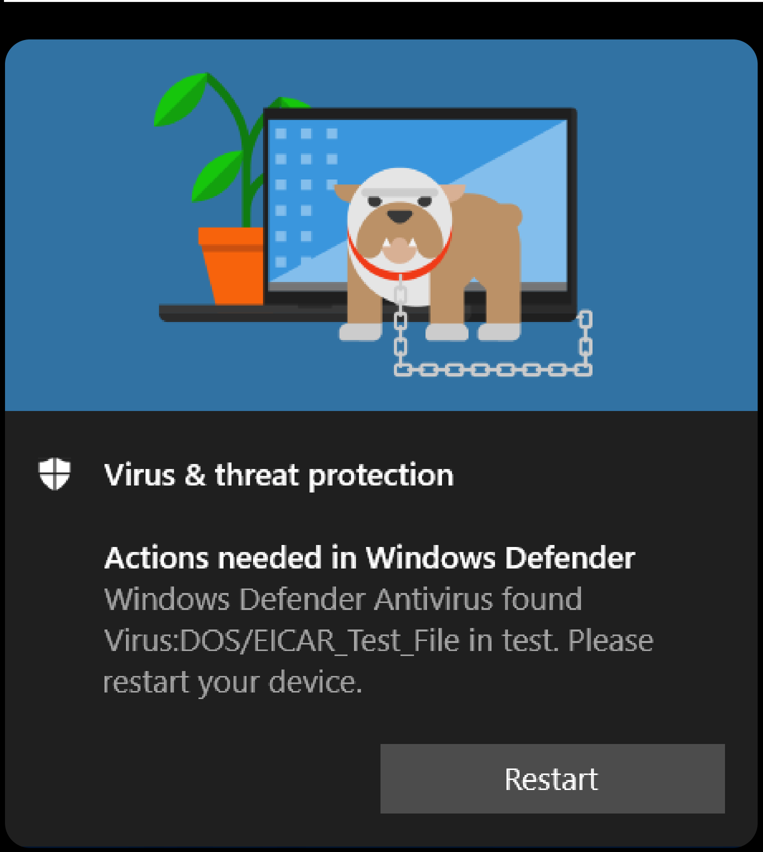
Failed Attempts

Target	C:\Windows\System32\drivers\ndis.sys
Mimikatz	C:\temp\Windows\System32\drivers\ndis.sys



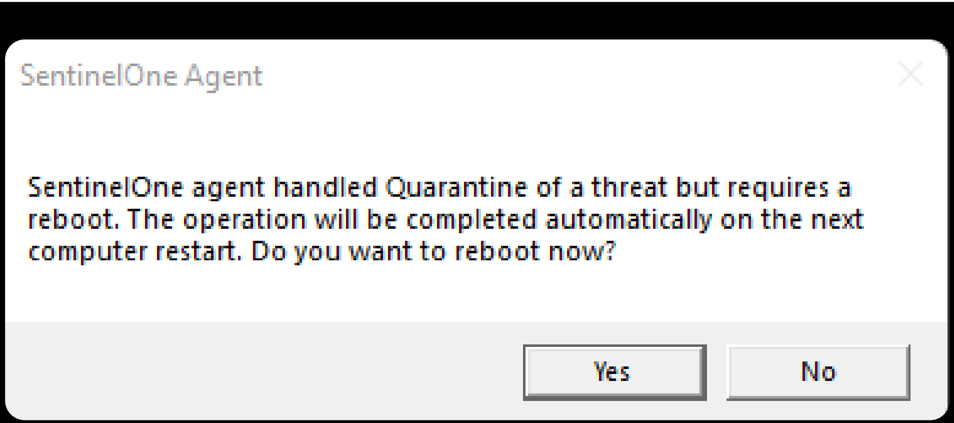
Creating a New Window of Opportunity

Handle catching - Forcing a reboot


Virus & threat protection

Actions needed in Windows Defender

Windows Defender Antivirus found Virus:DOS/EICAR_Test_File in test. Please restart your device.


SentinelOne Agent

SentinelOne agent handled Quarantine of a threat but requires a reboot. The operation will be completed automatically on the next computer restart. Do you want to reboot now?

```
HANDLE CreateFileW(
…
…
  [in]           DWORD             dwShareMode,
…
…
);
```

Deleting a File After Reboot

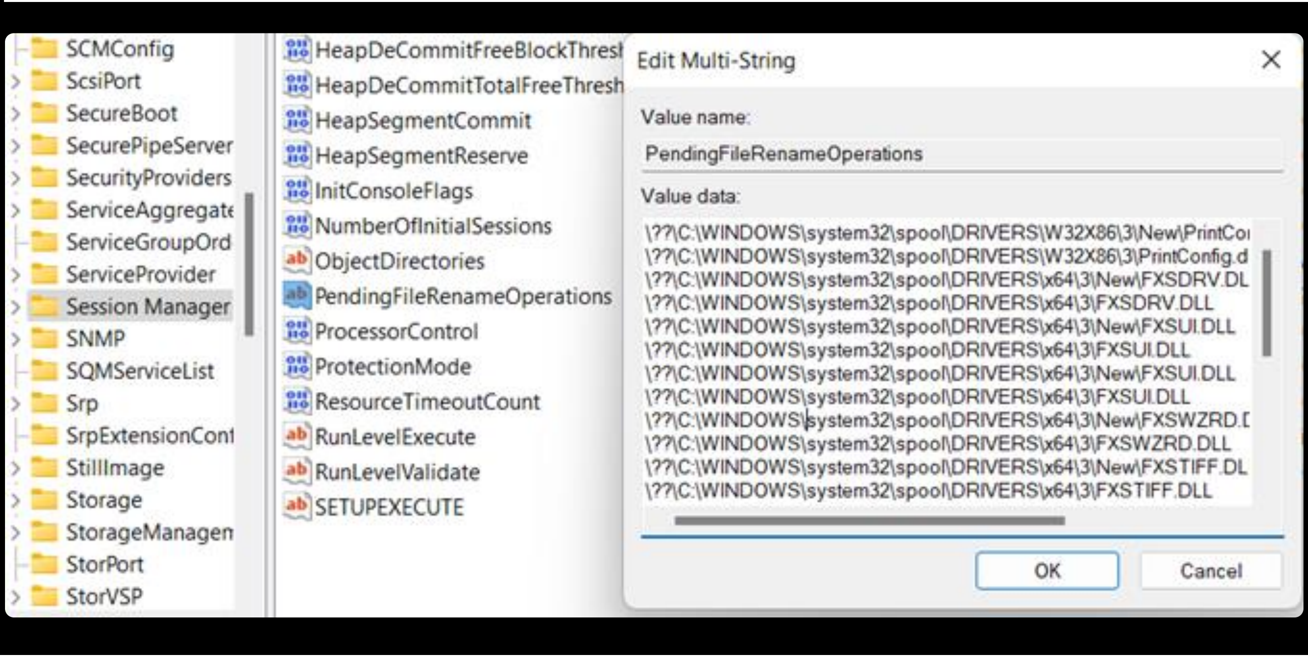
2 methods:

Using Windows API - MoveFileEx()	**Self implementation**
Example: SentinelOne	Example: Windows Defender

Windows API Mark for Deletion Mechanism

MoveFileEx() + MOVEFILE_DELAY_UNTIL_REBOOT

PendingFileRenameOperations



Value name:

PendingFileRenameOperations

Value data:

```
\??\C:\WINDOWS\system32\spool\DRIVERS\W32X86\3\New\PrintCo
\??\C:\WINDOWS\system32\spool\DRIVERS\W32X86\3\PrintConfig.d
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\New\FXSDRV.DL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\FXSDRV.DLL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\New\FXSUI.DLL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\FXSUI.DLL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\New\FXSUI.DLL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\FXSUI.DLL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\New\FXSWZRD.
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\FXSWZRD.DLL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\New\FXSTIFF.DL
\??\C:\WINDOWS\system32\spool\DRIVERS\x64\3\FXSTIFF.DLL
```

Mark For Deletion Mechanism

PendingFileRenameOperations follows junctions!

Self Implementation Post Reboot Deletion

Some self implementations follow junctions too !

The Complete Process

1. Create a malicious file in `C:\temp\Windows\System32\drivers\ndis.sys`

2. Hold its handle with a read-only file sharing mode and force the AV/EDR to postpone the deletion to after the next reboot

3. Delete the `C:\temp` directory

4. Create a junction `C:\temp` --> `C:\`

5. Reboot

Done ✅

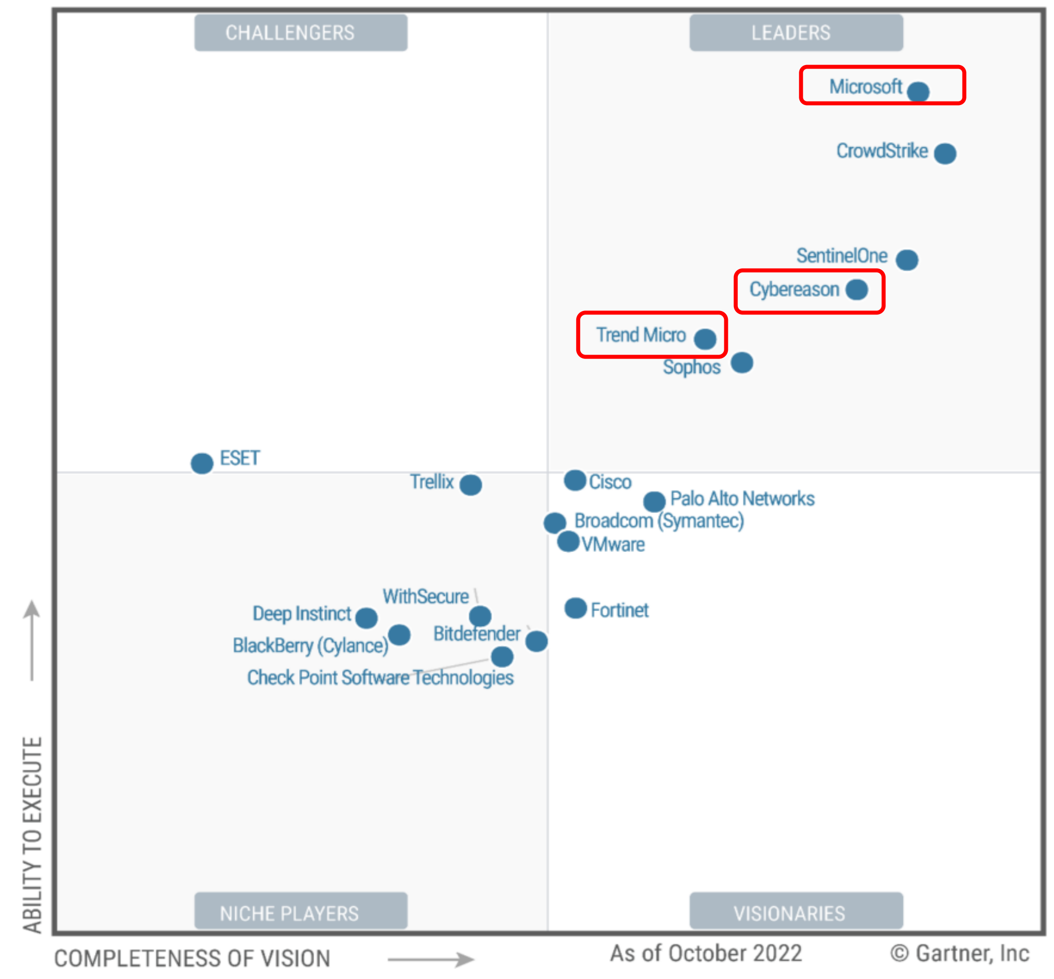
- ✅ What if the next-gen wiper could wipe files without using these obvious API calls?
- ✅ What if the next-gen wiper could do all that as an unprivileged user?

0-Day Vulnerabilities

Arbitrary Deletion
6 Vulnerable Products:

- Microsoft Defender
- Microsoft Defender for Endpoint
- SentinelOne XDR
- TrendMicro Apex One
- Avast Antivirus
- AVG Antivirus

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2022)

6 Products
3 CVEs

Microsoft	CVE-2022-37971 ▹ CVSS 3.1: 7.1
SentinelOne	No CVE
TrendMicro	CVE-2022-45797 ▹ CVSS 3.0: 5.6
Avast & AVG	CVE-2022-4173 ▹ CVSS 3.0: 7.3

Windows Defender VS the Rest

Arbitrary directory deletion only

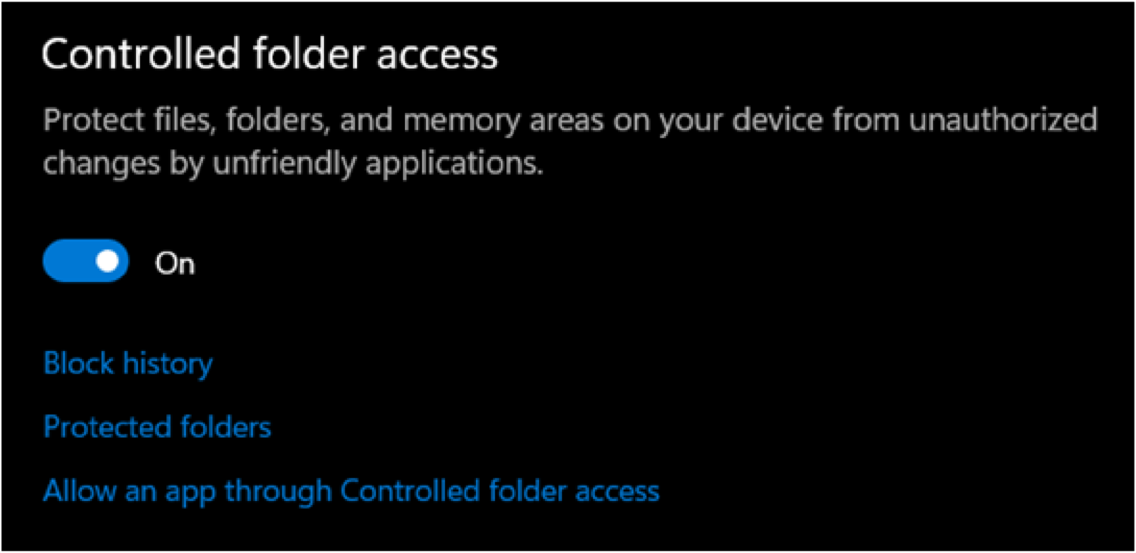
But – a wiper does not care about deleting a few extra files on the way😈

Windows Defender

Drivers Deletion Demo

Ransomware Protection Feature Bypass

Using the same exploit. It is also possible to bypass the controlled folder access security feature.



Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

Protected folders

Windows system folders are protected by default. You can also add additional protected folders.

Result Summary

50%+ of the tested products are vulnerable

- ☣ Defender
- ☣ Defender for Endpoint
- ☣ SentinelOne XDR
- ☣ TrendMicro Apex One
- ☣ Avast Antivirus
- ☣ AVG Antivirus

- 🛡 Palo Alto XDR
- 🛡 Cylance
- 🛡 CrowdStrike
- 🛡 McAfee
- 🛡 BitDefender

Most chances there are more

I was just unable to force other products to mark for deletion after reboot

If you find a way they will probably be vulnerable

Aikido Wiper Tool

Aikido Wiper

The next gen wiper

Implemented for SentinelOne XDR, Defender and Defender for endpoint

Makes the system unbootable

Able to delete system files such as drivers

Fully Undetectable

Deletes files using the most trusted entity on the system

An EDR / AV trusts itself

Uses EICAR not Mimikatz

Runs with unpriveleged user permissions

Able to delete files as an unprivileged user

Wipes important data

Able to delete the entire content of an admin user directory

Wipes important data

Fill free disk space a few times after the deletion

2 popular recovery products were not able to recover the files:

- Cleverfiles Disk Drill
- CCleaner Recuva

Wipes important data

Delete the quarantine directory

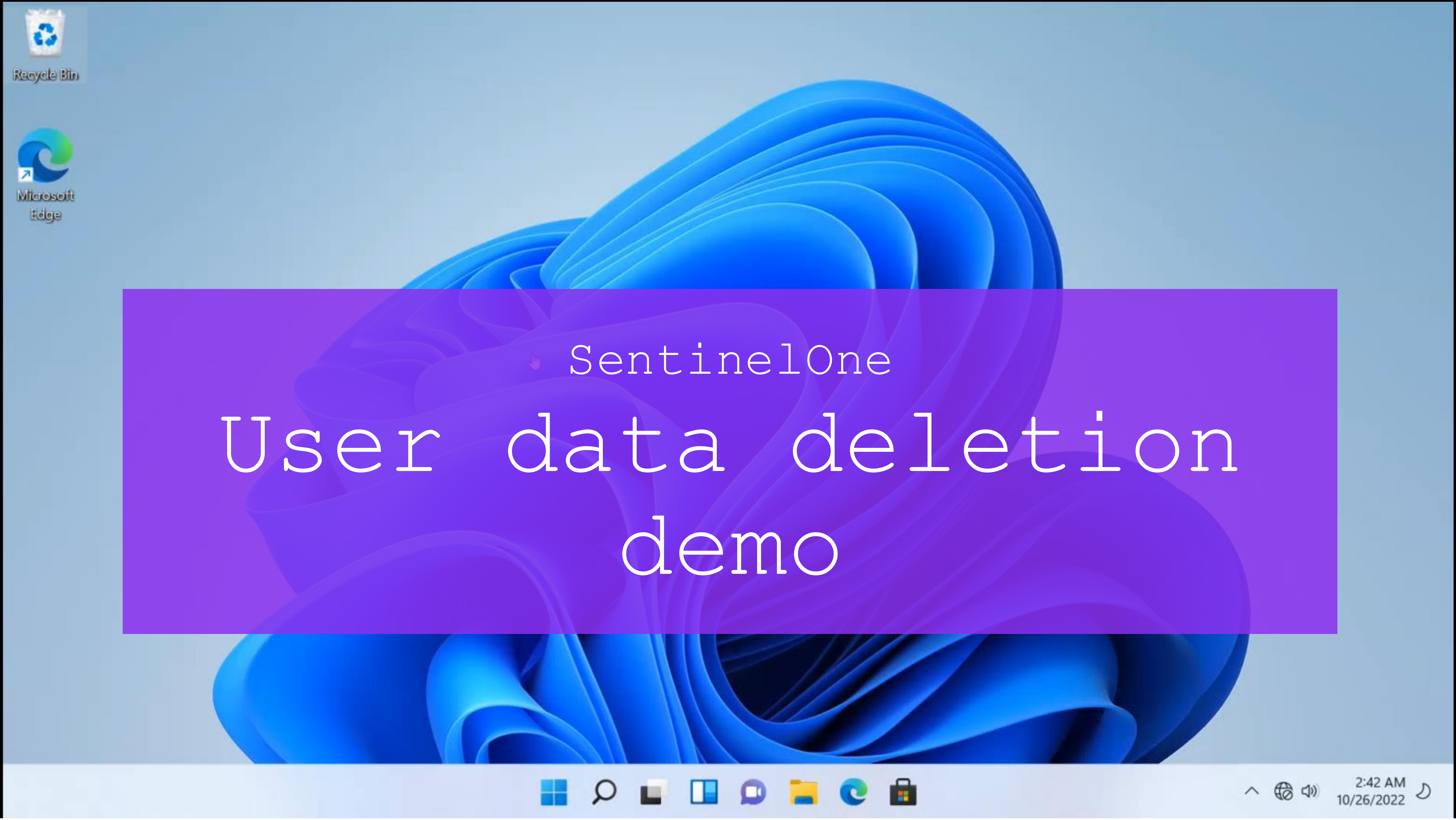
Repo Code

Well documented

Expandable

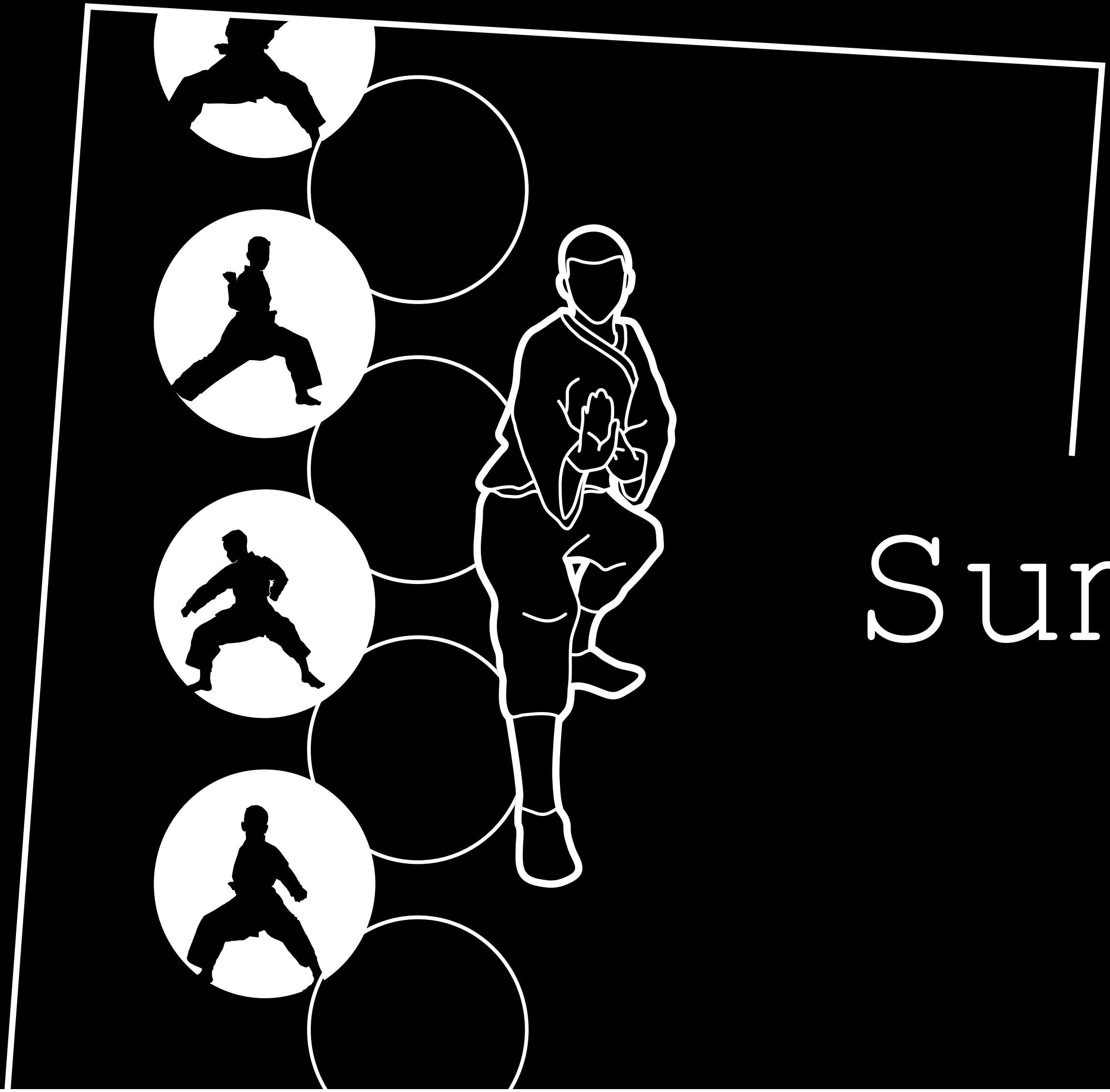
Aikido Wiper GitHub

https://github.com/SafeBreach-Labs/aikido_wiper



SentinelOne

User data deletion demo



Summary

Lessons Learned

A wiper is more dangerous if it uses a trusted entity on the system for deletion, especially a security control

Having security controls does not mean you are secure

Security controls might be a preferred target for attackers due to their very high privileges and are most trust level

Assume permissions can always be escalated

Vendors' Response

Microsoft Response

“Hello Or,

The fix in development for your report has completed testing and is tentatively scheduled to be released in the upcoming Defender Release later this month. We propose to disclose that fix on the October 11th patch Tuesday with the other security releases under CVE-2022-37971.

I hope that will meet your expectations.”

Gen

"Dear Or Yair,

Thanks for bringing this vulnerability to our attention.

On October 20th, 2022, Avast released an update (to version 22.10) to address an issue that was discovered in the malware removal functionality of Avast and AVG Antivirus versions 20.5 up to 22.9

Users of the affected versions have received an automatic update. We ask users to restart Windows once Avast and AVG prompts them to do so, in order to complete the update.

Good luck with the presentation, and enjoy Black Hat!

Best Regards,
Gen™

Gen™ is a global company with a family of consumer brands including Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner"

Update to be safe

Microsoft Malware Protection Engine	1.1.19700.2
SentinelOne Agent	22.3 EA
TrendMicro Apex One	Hotfix 23573 Patch_b11136
Avast & AVG Antivirus	22.10

PendingFileRenameOperations Risks

MoveFileEx()

+

MOVEFILE_DELAY_UNTIL_REBOOT

+

Unprivileged user controllable target path

=

Vulnerability

Credits

Shmuel Cohen

Security Researcher @ SafeBreach

Assistance with testing different products

Q&A

@oryair1999

https://www.linkedin.com/in/or-yair/

or.yair@safebreach.com