Mphasis
The Next Applied

Antivirus and EDR solutions tricked into acting as data wipers

Severity: Medium

Date: 12th Dec 2022

Description

A security researcher has found a way to exploit the data deletion capabilities of widely used endpoint detection and response (EDR) and antivirus (AV) software from Microsoft, Sentinel One, TrendMicro, Avast, and AVG to turn them into data wipers.

Wipers are a special type of destructive malware that purposely erases or corrupts data on compromised systems and attempts to make it so that victims cannot recover the data.

Safe Breach researcher Or Yair came up with the idea to exploit existing security tools on a targeted system to make the attacks stealthier and remove the need for a threat actor to be a privileged user to conduct destructive attacks.

Also, abusing EDRs and AVs for data wiping is a good way to bypass security defenses as the file deletion capabilities of security solutions are expected behavior and would likely be missed.

How It Works

Triggering the (wrong) deletion

Antivirus and EDR security software constantly scan a computer's filesystem for malicious files, and when malware is detected, attempt to quarantine, or delete them.

Furthermore, with real-time protection enabled, as a file is created, it is automatically scanned to determine if it is malicious and, if so, deleted/quarantined.

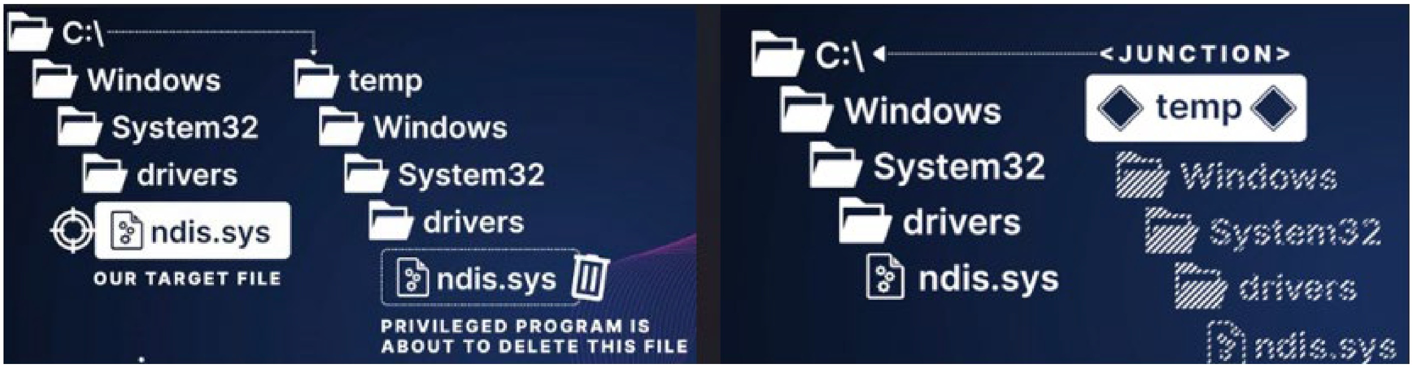
"There are two main events when an EDR deletes a malicious file. First, the EDR identifies a file as malicious and then it deletes the file," explained Yair in his report.

"If I could do something between these two events, using a junction, I might be able to point the EDR towards a different path. These are called time-of-check to time-of-use (TOCTOU) vulnerabilities.

Yair's idea was to create a C:\temp\Windows\System32\drivers folder and store the Mimi Katz program in the folder as ndis.sys.

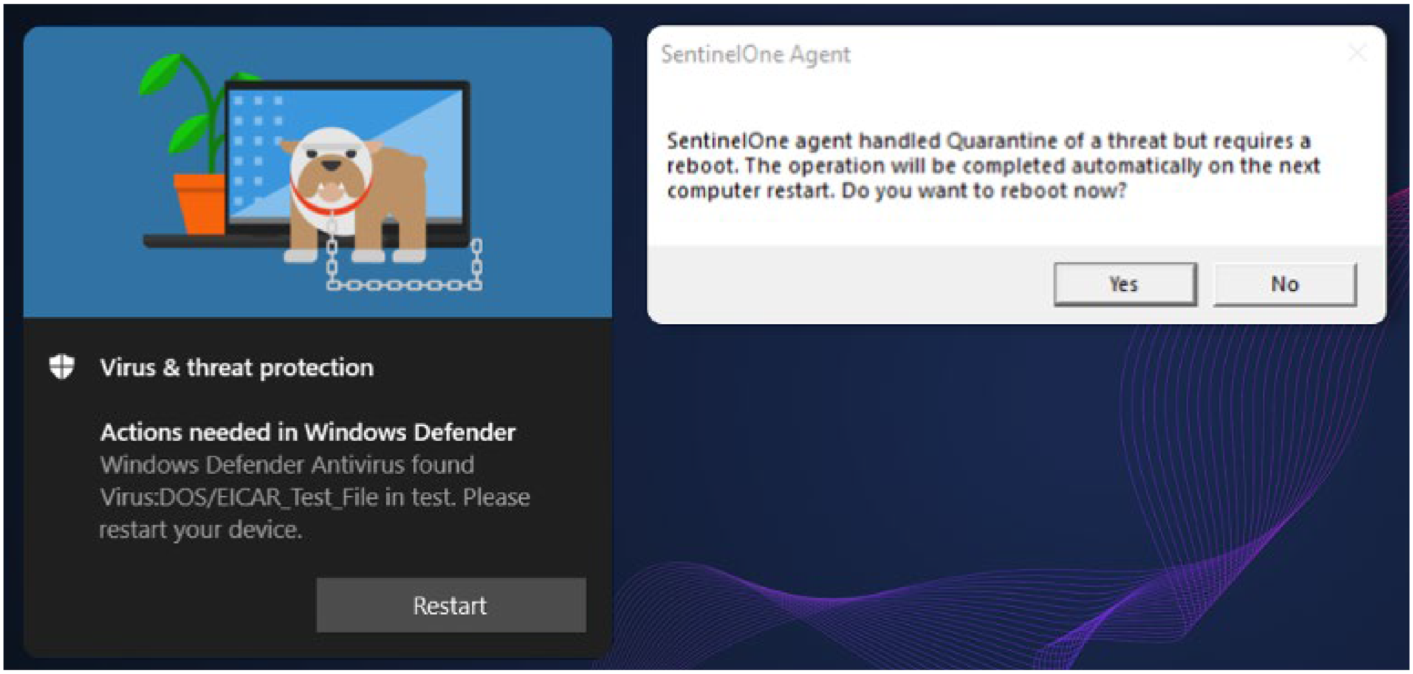
As Mimi Katz is detected by most EDR platforms, including Microsoft Defender, the plan was for it to be detected as malicious on creation. However, before the EDR could delete the file, the researcher would quickly delete the C:\Temp folder and create a Windows Junction from C:\Temp to C:\Windows.

The hope was that the EDR would attempt to delete the ndis.sys file, which due to the junction, is now pointing to the legitimate C:\Windows\system32\drivers\ndis.sys file.



Deleting the malicious directory and using junction to point to the target *(SafeBreach)*

The solution was to create the malicious file, hold its handle by keeping it open, and not define what other processes are allowed to write/delete it so that EDRs and AVs detecting it can’t wipe it.After the detection was triggered and having no rights to delete the file, the security tools prompted the researcher to approve a system reboot that would release the handle, freeing the malicious fil for deletion.



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

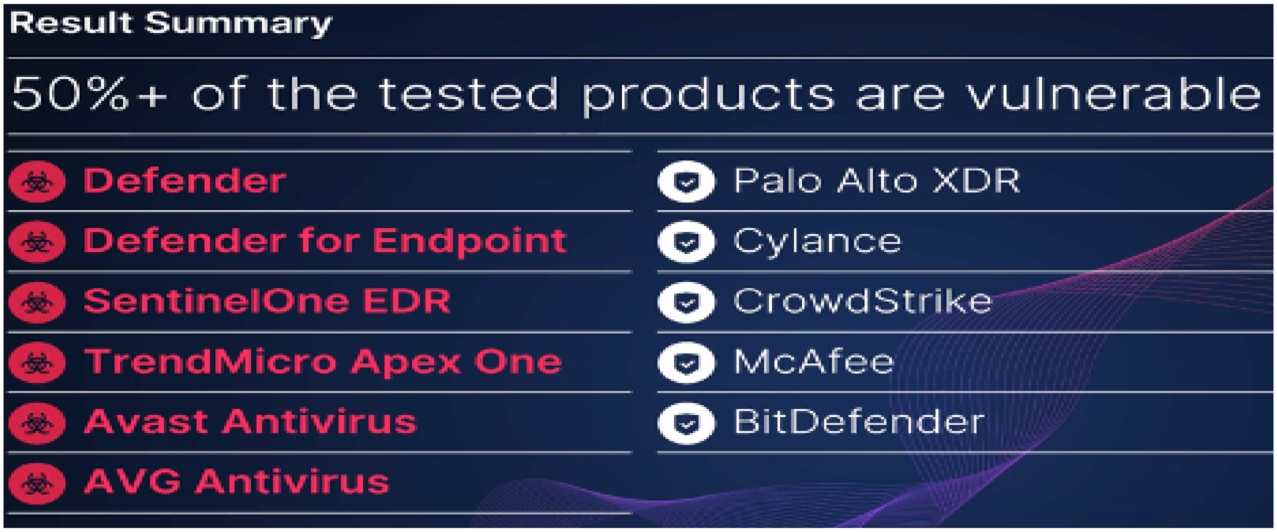
SentinelOne agent handled Quarantine of a threat but requires a reboot. The operation will be completed automatically on the next computer restart. Do you want to reboot now?

Security tools prompting a reboot *(SafeBreach)*

Impact and response

Yair tested the exploit against 11 security tools and found that Microsoft Defender, Defender for Endpoint, Sentinel One EDR, TrendMicro Apex One, Avast Antivirus, and AVG Antivirus were all vulnerable.

Security solutions that were not exploitable include Palo Alto, Cylance, CrowdStrike, McAfee, and Bitdefender, which the analyst also tested.



Result Summary

50%+ of the tested products are vulnerable

Defender

Defender for Endpoint

SentinelOne EDR

TrendMicro Apex One

Avast Antivirus

AVG Antivirus

Palo Alto XDR

Cylance

CrowdStrike

McAfee

BitDefender

Tested security product *(SafeBreach)*

Aikido features exploits for vulnerabilities found in Microsoft Defender, Defender for Endpoint, and Sentinel One EDR because they were the easiest to implement on the wiper tool.

Yair reported the flaws to all vulnerable vendors between July and August 2022, and they have all released fixes by now.

The vulnerability IDs assigned by the vendors for this issue are CVE-2022-37971 (Microsoft), “CVE-2022-45797 (Trend Micro), and CVE-2022-4173 (Avast and AVG).

The fixed versions are:

- Microsoft Malware Protection Engine: 1.1.19700.2 or later
- TrendMicro Apex One: Hotfix 23573 & Patch_b11136 or later
- Avast & AVG Antivirus: 22.10 or later

All users of the above products are recommended to apply the security updates as soon as possible to mitigate the severe risk of having their files wiped by malware mimicking the Aikido wiper functionality.

Reference Links

https://www.bleepingcomputer.com/news/security/antivirus-and-edr-solutions-tricked-into-acting-as-data-wipers/