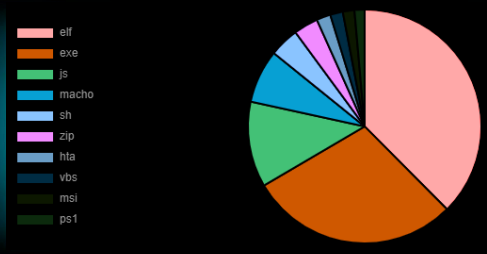

SORINT SEC
THREAT HUNTING
LAB
WEEK 22/09/2025 – 26/09/2025
PUBLIC

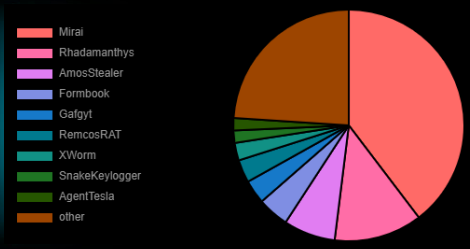
Index

Global Weekly Threat Overview

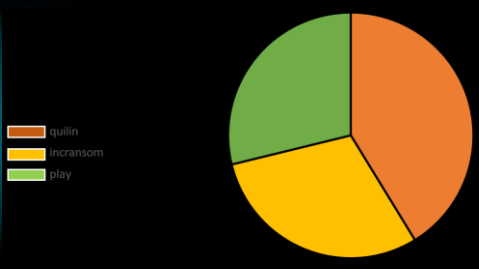
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Hackers have been spotted using SEO poisoning and search engine advertisements to promote fake Microsoft Teams installers that infect Windows devices with the Oyster backdoor, providing initial access to corporate networks.
The Oyster malware is a backdoor that first appeared in mid-2023 and has since been linked to multiple campaigns. The malware provides attackers with remote access to infected devices, allowing them to execute commands, deploy additional payloads, and transfer files.Oyster is commonly spread through malvertising campaigns that impersonate popular IT tools, such as Putty and WinSCP.

A vulnerability in multiple versions of OxygenOS, the Android-based operating system from OnePlus, allows any installed app to access SMS data and metadata without requiring permission or user interaction. While other major Chinese brands like Huawei and Xiaomi aren't available in different countries, OnePlus devices are officially available on the globe. The flaw, tracked as CVE-2025-10184, and discovered by Rapid7 researchers, is currently unpatched and exploitable. The Chinese OEM failed to respond to Rapid7's disclosures to this day, and the cybersecurity company published the technical details along with a proof-of-concept (PoC) exploit.

Global Weekly Notable One

System Binary Proxy Execution: **Defense Evasion**

EDR-Freeze is a novel proof-of-concept tool that temporarily disables EDR and Antivirus processes. Crucially, it operates entirely in user mode, eliminating the need for BYOVD (Bring Your Own Vulnerable Driver) or kernel exploits by leveraging legitimate native Windows components. The method exploits the behavior of the Windows Error Reporting (WER) component WerFaultSecure.exe, which runs with Protected Process Light (PPL) privileges.

EDR-Freeze forces WerFaultSecure to initiate a memory snapshot of the target EDR process. The tool then suspend all threads in the target process to ensure a consistent dump. The technique exploits a race condition: once the EDR is suspended, EDR-Freeze immediately suspends the initiator process, WerFaultSecure. This prevents the security agent from resuming, leaving it indefinitely suspended or “freezed". This suspension provides attackers a window to perform sensitive operations with greatly reduced detection probability.

Threat Hunting Activity

SORINTSEC

TACTIC

Defense Evasion

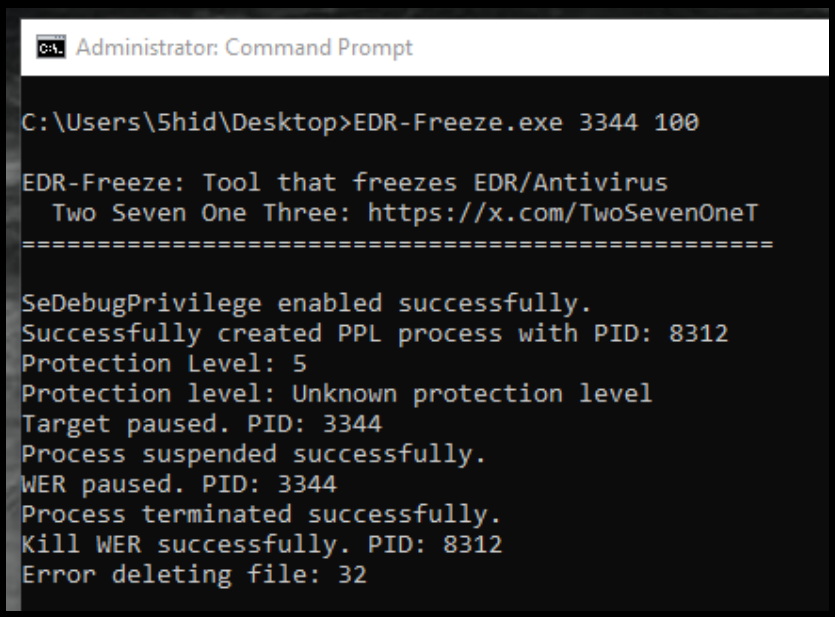
TECHNIQUES

T1218 – System Binary Proxy Execution

Adversaries leverage and abuse trusted processes to hide and masquerade their malware. Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.

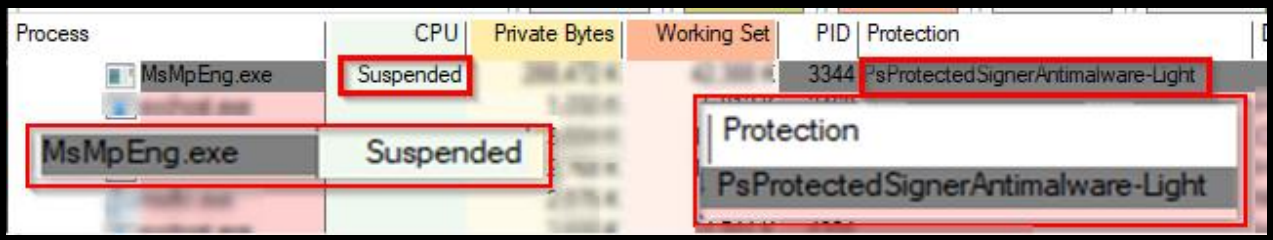
Threat Hunting Activity

EDR-Freeze targets security agents that utilize Protected Process Light (PPL) protection to harden themselves against user-mode tampering. To bypass this, the tool leverages the PPL hierarchy by launching the native Windows component WerFaultSecure.exe with PPL protection at the WinTCB level. This high-priority signer level allows the dumper process to operate against the protected EDR.



EDR-freeze execution against MsMpEng Windows Defender process

The indefinite suspension is achieved through a race condition: once the target EDR process is suspended, EDR-Freeze immediately suspends the initiator, WerFaultSecure.exe. Because the process required to resume the EDR is now blocked, the security agent remains indefinitely suspended.



PPL Windows Defender suspended process

Threat Hunting Activity

The source code of the EDR-Freeze tool automates the launch of the native Windows component WerFaultSecure.exe as a Protected Process Light (PPL) and passes a specific set of command-line parameters to force it to initiate a memory dump of the target security agent.

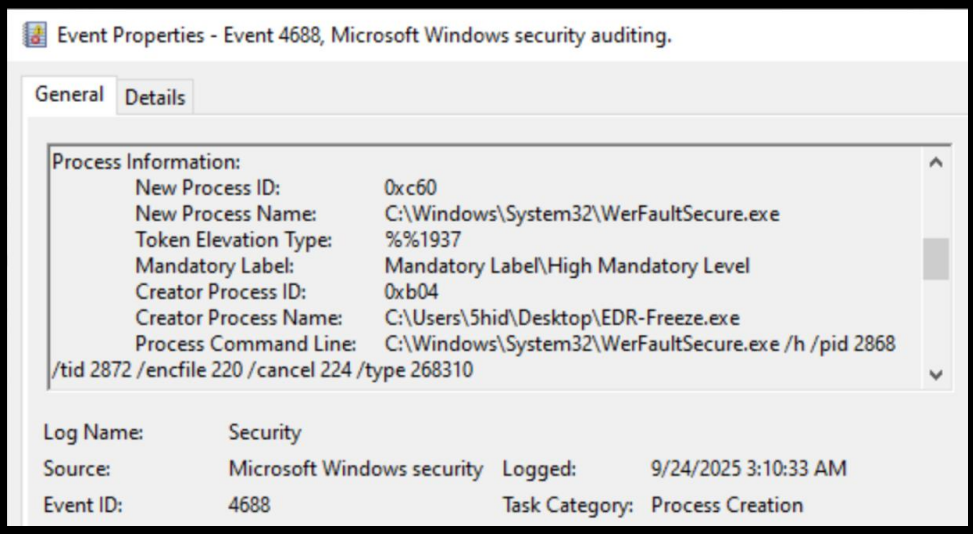
```
51      std::wstring werPath = L"C:\\Windows\\System32\\WerFaultSecure.exe";
52      std::wstringstream cmd;
53      cmd << werPath
54          << L" /h"
55          << L" /pid " << targetPID
56          << L" /tid " << targetTID
57          << L" /encfile " << HandleToDecimal(hEncDump)
58          << L" /cancel " << HandleToDecimal(hCancel)
59          << L" /type 268310"; // dump full
```

EDR-freeze source code

Despite most of the values of the parameters could be different based on the target and the attacker chosen scope, the parameter "/type " and the related value "268310" refers to an instruction to create a full dump of the process memory in WerFaultSecure.exe context.

Threat Hunting Activity

Detection can be made monitoring EID 4688 looking for uncommon WerFaultSecure parameters correlating with process that generate the execution.



EID 4688

PUBLIC