Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ⚔ ATTACK REPORT

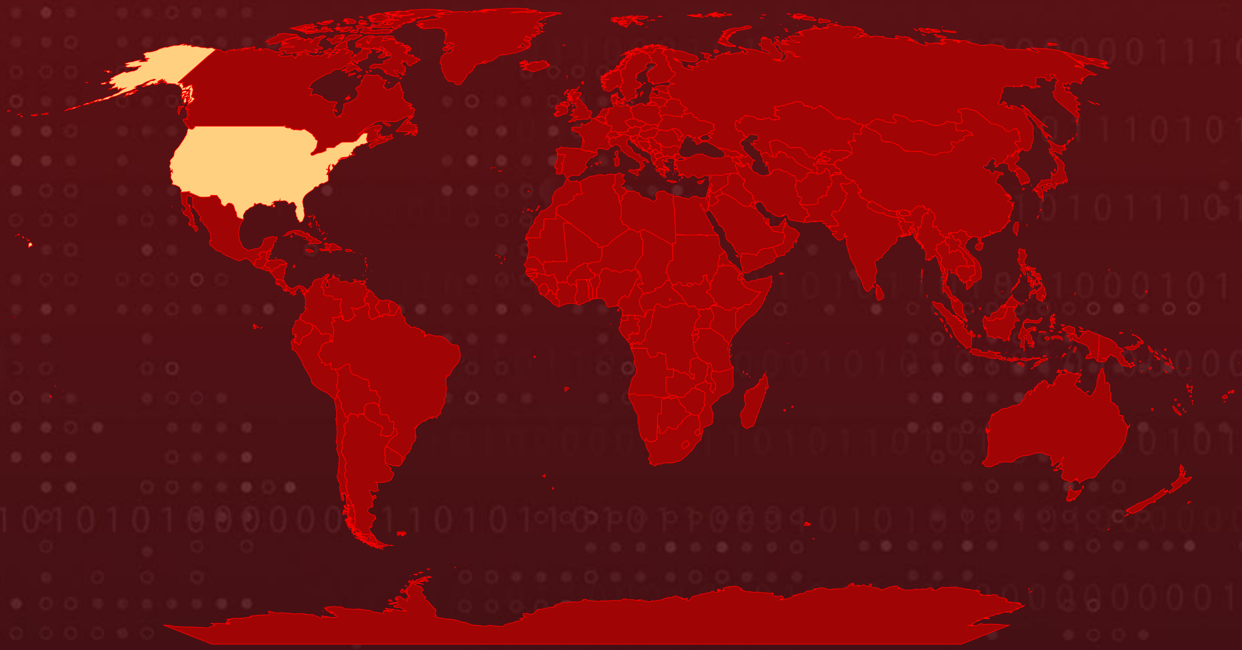
# Silent Escalation: CLFS Zero-Day Used in Targeted Attack

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| May 8, 2025 | A1 | TA2025139 |

# Summary

**Attack Discovered:** April 2025
**Targeted Country:** U.S.
**Malware:** Grixba infostealer
**Attack:** A U.S. organization was hit by a stealthy cyberattack linked to the Play ransomware operation, who took advantage of a flaw in Windows tracked as CVE-2025-29824 to gain higher system access. Using a custom-built infostealer called Grixba and cleverly disguised tools, the attackers quietly collected sensitive data and moved through the network undetected underscoring the rising risk of zero-day exploits and sophisticated hacking tactics.

## Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2025-29824 | Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability | Microsoft Windows | ✓ | ✓ | ✓ |

# Attack Details

#1 A U.S. based organization recently fell victim to a cyberattack linked to the Play ransomware group. The attackers exploited a previously unknown Windows vulnerability to gain higher privileges on the system before Microsoft had released a patch. This zero-day vulnerability CVE-2025-29824 was leveraged alongside the use of Grixba, a custom-built infostealer associated with Balloonfly, a cybercriminal group known to deploy Play ransomware since mid-2022.

#2 The attackers specifically targeted a Windows machine on the victim's network possibly one facing the internet, like a Cisco ASA firewall. They dropped multiple malicious tools and samples, including Grixba and an exploit for CVE-2025-29824. In one stage of the attack, they ran a command to enumerate all systems listed in the Active Directory, saving this information to a CSV file. Notably, these malicious files were placed in the "Music" folder and disguised as legitimate Palo Alto software, blending into the environment.

#3 The main part of the attack focused on a flaw in the Common Log File System (CLFS), a part of the Windows operating system. The attackers started by using a command called CreateFileW() to open a fake log file in a specific way. This action made Windows create a file structure in memory and send a request to the CLFS system to handle it. While doing so, Windows also created extra pieces of data to track the request, including one hidden structure called CClfsLogCcb. This hidden part was used to manage and control the log file access during the attack.

#4 The exploitation technique involved racing two threads to perform simultaneous I/O operations on the same file. One thread issued a CloseHandle() command, while the other issued a Device Control request. Due to the lack of guaranteed execution order between these two system calls, the attackers exploited a timing flaw to manipulate kernel memory an advanced tactic for gaining unauthorized control.

#5 During this process, two notable files were created. One which served as a log file artifact of the attack, while the second was a batch script used to elevate privileges and extract sensitive system registry hives. The attackers executed these batch files through scripted commands to maintain persistence and escalate access.

#6 Microsoft has since patched the vulnerability (CVE-2025-29824), acknowledging that it had been exploited in limited, targeted attacks across the U.S., Venezuela, Spain, and Saudi Arabia. In some cases, the exploit was observed in use by the PipeMagic malware commonly linked to Storm-2460, another ransomware actor. Interestingly, Storm-2460's use of the exploit differed from Balloonfly's approach, with execution occurring in-memory via a dllhost.exe process, showcasing varying techniques across threat actors.

# Recommendations

**Keep Systems Up-to-Date:** Make sure to promptly apply patches for vulnerability like CVE-2025-29824 in Microsoft Windows CLFS system that attackers can exploit. Stay informed by news and alerts so you can quickly patch any known zero-day vulnerabilities before they're used in real attacks.

**Watch for Suspicious Behavior:** Keep an eye out for strange system activity like unusual use of Windows functions or multiple system operations happening at the same time which could be signs of an exploit in progress. Set up alerts for any unexpected changes to folders or if new files appear without a clear reason. These can be clues that an attacker is trying to gain control.

**Secure and Audit Active Directory:** Make it harder for attackers to move around your network by breaking it into smaller, secure segments and only giving users the minimum access they truly need. Regularly review who has access to what, clean up old or unused accounts, and watch for unusual activity.

**Block Command-and-Control (C2) Connections:** Set up firewalls and proxy rules to block traffic to known bad IP addresses or sketchy domains often used by attackers. Use DNS filtering tools to stop your systems from reaching out to attacker-controlled servers, helping to cut off communication before any real damage is done.

**Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0042<br>Resource Development | TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence |
| TA0004<br>Privilege Escalation | TA0005<br>Defense Evasion | TA0010<br>Exfiltration | TA0011<br>Command and Control |

|  |  |  |  |
|---|---|---|---|
| **T1588**<br>Obtain Capabilities | **T1588.006**<br>Vulnerabilities | **T1588.005**<br>Exploits | **T1190**<br>Exploit Public-Facing Application |
| **T1036**<br>Masquerading | **T1059**<br>Command and Scripting Interpreter | **T1059.001**<br>PowerShell | **T1068**<br>Exploitation for Privilege Escalation |
| **T1136**<br>Create Account | **T1106**<br>Native API | **T1574**<br>Hijack Execution Flow | **T1574.001**<br>DLL |
| **T1053**<br>Scheduled Task/Job | **T1105**<br>Ingress Tool Transfer |  |  |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 6030c4381b8b5d5c5734341292316723a89f1bdbd2d10bb67c4d06b1242afd05,<br>858efe4f9037e5efebadaaa70aa8ad096f7244c4c4aeade72c51ddad23d05bfe,<br>9c21adbcb2888daf14ef55c4fa1f41eaa6cbfbe20d85c3e1da61a96a53ba18f9,<br>6d7374b4f977f689389c7155192b5db70ee44a7645625ecf8163c00da8828388,<br>b2cba01ae6707ce694073018d948f82340b9c41fb2b2bc49769f9a0be37071e1,<br>293b455b5b7e1c2063a8781f3c169cf8ef2b1d06e6b7a086b7b44f37f55729bd,<br>af260c172baffd0e8b2671fd0c84e607ac9b2c8beb57df43cf5df6e103cbb7ad,<br>430d1364d0d0a60facd9b73e674faddf63a8f77649cd10ba855df7e49189980b,<br>ba05d05d51d4f7bfceb3821a3754e7432248f5c3d5a450391a0631d56bbce4c2,<br>b3ee068bf282575ac7eb715dd779254889e0b8a55aba2b7a1700fc8aa4dcb1da |

## Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824

## References

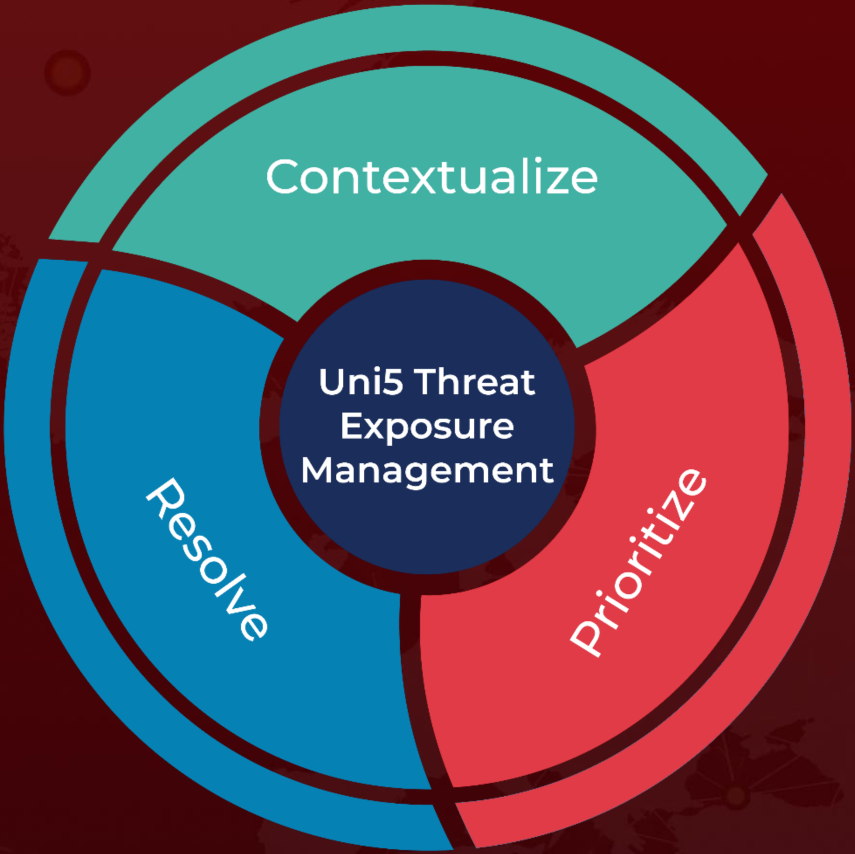
https://www.security.com/threat-intelligence/play-ransomware-zero-day

https://hivepro.com/threat-advisory/microsofts-april-2025-patch-tuesday-fixes-active-zero-day-exploits/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

**May 8, 2025 • 5:40 AM**

More at www.hivepro.com