

SORINT SEC

THREAT HUNTING

LAB

Living off the Land with ieadvpack.dll: Proxying Script Execution via Malicious .INF Files

PUBLIC

Index

Global Weekly Threat Overview

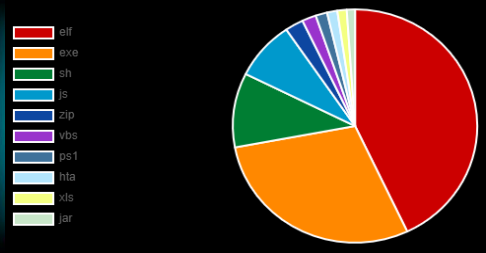
Global Weekly Notable One

Threat Hunting Activity

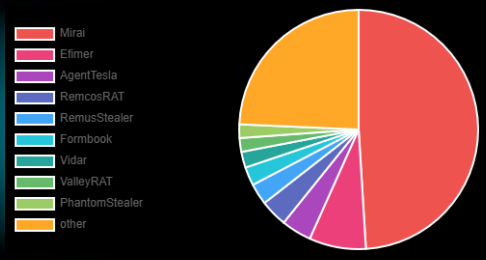
Global Weekly Threat Overview

An OpenSSH authentication-bypass flaw nicknamed "sshole" (CVE-2026-123158) was exploited in the wild less than nine hours after disclosure on November 5, threat intel firm Previdian reported, with at least one confirmed root compromise of a honeypot. On musl-based Linux without PAM (Alpine, OpenWrt, Buildroot, many Docker images), any password longer than 256 bytes lets an attacker log into passwordless accounts, including root on Alpine's default cloud images, due to a 2016 OpenSSH fix interacting badly with musl's crypt(). Patched in OpenSSH 10.6p2; glibc-based distros (Debian, Ubuntu, Fedora) are unaffected. Admins should patch or disable password authentication immediately.

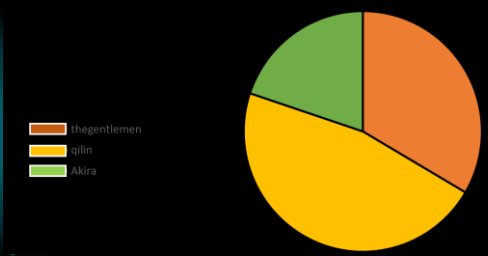
Top 10 file types



Top 10 malware family

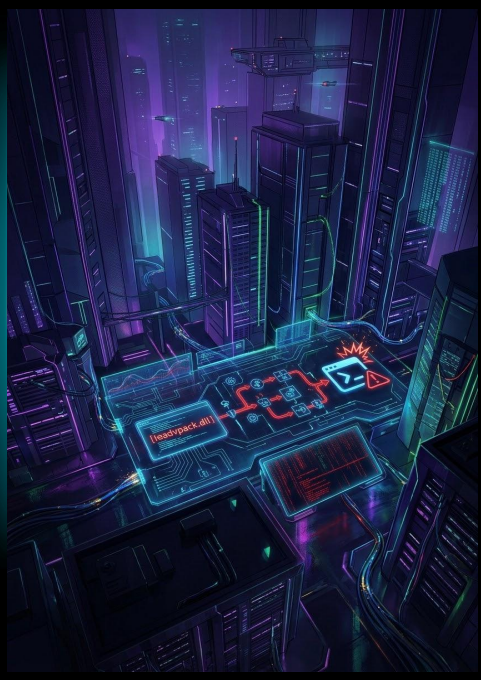


Top 3 Ransomware Group



Microsoft detailed two human-operated intrusions (published October 30) in which attackers impersonated IT help desk staff over Teams, talking employees into opening Quick Assist for remote control, then staging portable Python/Bun/Java runtimes. One intrusion abused an ESC1 certificate template to mint certificates for 11 privileged accounts and ran DCSync before full containment; the other coerced a domain controller via PetitPotam and relayed the NTLM auth to AD CS web enrollment (ESC8), obtaining a DC certificate and a PKINIT TGT. No software flaw was involved, fixes are configuration-only (verified support channels, EPA on enrollment endpoints, certificate auditing).

Global Weekly Notable One



Defense Evasion: System Binary Proxy Execution

'rundll32.exe' is a legitimate, Microsoft-signed Windows binary used to load and call exported functions from DLLs. Because it is a trusted system component present on every Windows install, security tooling and application-allowlisting (AWL) solutions frequently treat its invocations as benign by default making it an attractive proxy for adversaries who want to execute code without dropping or launching an unsigned binary directly.

'ieadvpack.dll' (and its close relative 'advpack.dll'), originally shipped to support Internet Explorer and general Windows software/driver installation routines, exports a function called 'LaunchINFSection'. This function is designed to process a '.inf' file, the standard Windows driver/software installation format, and execute the directives contained in a named section of that file. When invoked through 'rundll32.exe', this legitimate installation mechanism becomes a way to run attacker-supplied code while the only process visibly spawned is the trusted, signed 'rundll32.exe'.

Threat Hunting Activity

TACTIC

Defense Evasion

TECHNIQUES

T1218 - System Binary Proxy Execution

Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. Shared Modules), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations.

Threat Hunting Activity

The technique, documented in the LOLBAS project, works through a chain that abuses legitimate Windows installer plumbing rather than any memory-corruption bug:

1. The adversary prepares a '.inf' file containing a 'DefaultInstall' (or custom-named) section whose directives point to a script, typically a '.sct' (Windows Scriptlet) or '.wsh' file, local or hosted remotely.

2. The adversary invokes 'rundll32.exe', calling 'LaunchINFSection' in 'ieadvpack.dll' and passing the absolute path to the '.inf' file plus the target section name 'rundll32.exe ieadvpack.dll,LaunchINFSection {PATH_ABSOLUTE}.inf,DefaultInstall_SingleUser,1,' or, with the 'DefaultInstall' section implied 'rundll32.exe ieadvpack.dll,LaunchINFSection {PATH_ABSOLUTE}.inf,,1,'

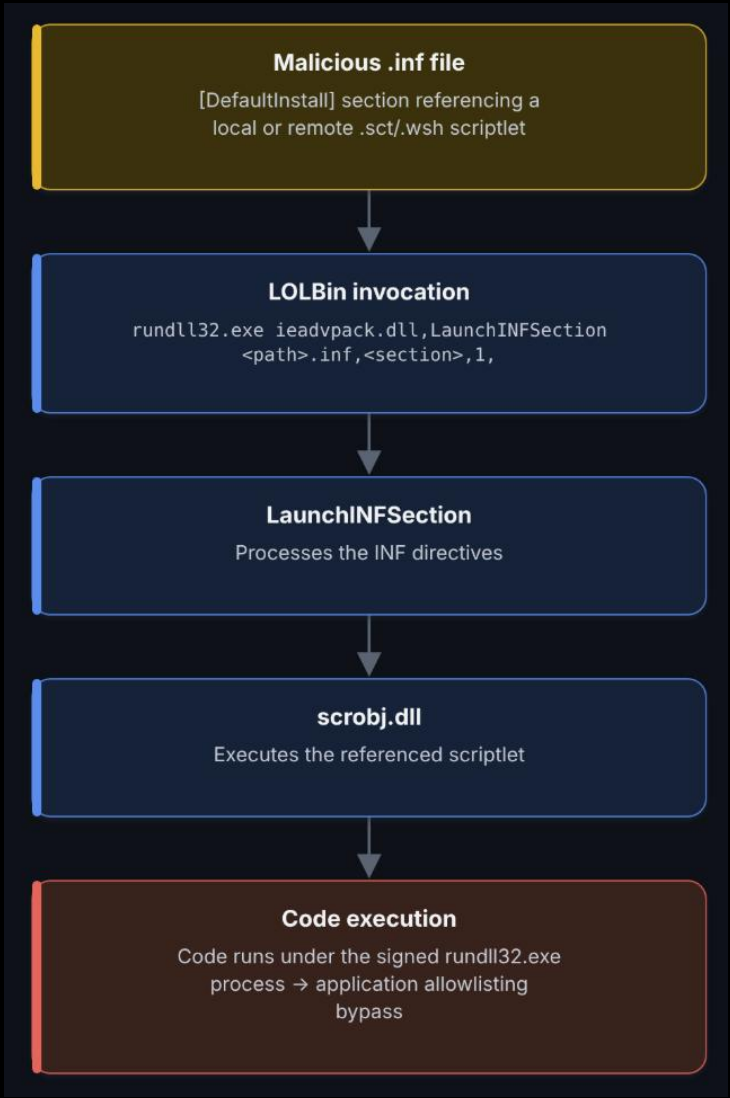
3. 'LaunchINFSection' parses the specified '.inf' directives and, via 'scrobj.dll' (the Windows Script Component runtime), executes the referenced scriptlet content - which can itself be fetched from a remote location, not just a local path.

4. The net effect is arbitrary script execution under the identity of a trusted, signed Microsoft binary, bypassing allowlisting products that permit 'rundll32.exe' by default and evading detections that key on unsigned or unusual process images rather than on command-line content.

This is a long-documented application-allowlisting bypass, still relevant because it requires no vulnerability or patch but only the presence of 'ieadvpack.dll'/'advpack.dll', native to all supported Windows versions, and User-level privileges. While 'syssetup.dll' and 'setupapi.dll' can be used for a similar INF-based execution via 'rundll32.exe', they use different exported functions ('SetupInfObjectInstallAction' and 'InstallHinfSection', respectively), a key detail for precise detection logic.

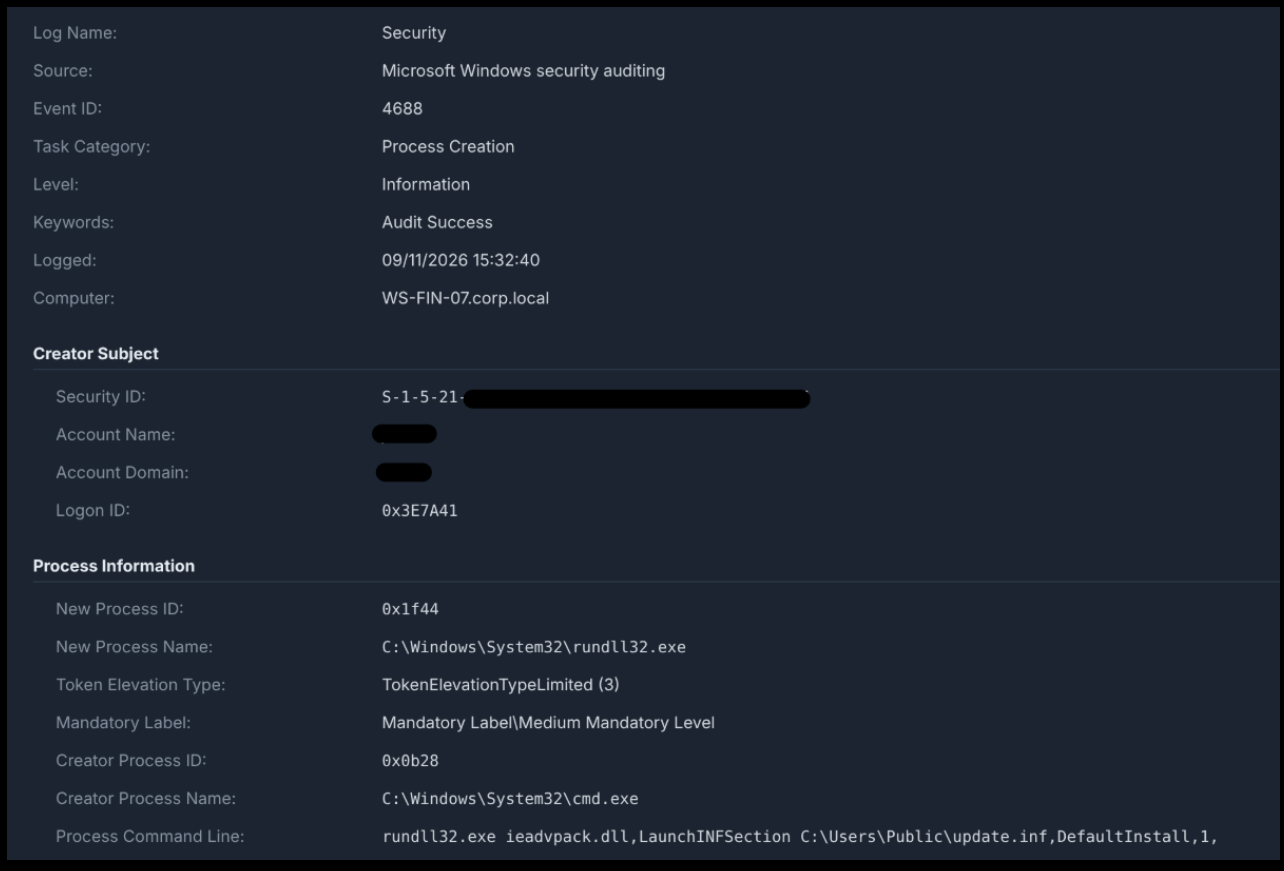
Threat Hunting Activity

This is a long-documented application-allowlisting bypass, still relevant because it requires no vulnerability or patch but only the presence of 'ieadvpack.dll'/'advpack.dll', native to all supported Windows versions, and User-level privileges. While 'syssetup.dll' and 'setupapi.dll' can be used for a similar INF-based execution via 'rundll32.exe', they use different exported functions ('SetupInfObjectInstallAction' and 'InstallHinfSection', respectively), a key detail for precise detection logic.



Threat Hunting Activity

Detection can be built on Event ID 4688 filtered for 'rundll32.exe' processes whose command line contains function names like 'LaunchINFSection', 'SetupInfObjectInstallAction', or 'InstallHinfSection' combined with 'ieadvpack.dll', 'advpack.dll', 'syssetup.dll' or 'setupapi.dll'. These command-line patterns are essentially never seen in normal administrative use.



Log Name:	Security
Source:	Microsoft Windows security auditing
Event ID:	4688
Task Category:	Process Creation
Level:	Information
Keywords:	Audit Success
Logged:	09/11/2026 15:32:40
Computer:	WS-FIN-07.corp.local

Creator Subject

Security ID:	S-1-5-21-[redacted]
Account Name:	[redacted]
Account Domain:	[redacted]
Logon ID:	0x3E7A41

Process Information

New Process ID:	0x1f44
New Process Name:	C:\Windows\System32\rundll32.exe
Token Elevation Type:	TokenElevationTypeLimited (3)
Mandatory Label:	Mandatory Label\Medium Mandatory Level
Creator Process ID:	0x0b28
Creator Process Name:	C:\Windows\System32\cmd.exe
Process Command Line:	rundll32.exe ieadvpack.dll,LaunchINFSection C:\Users\Public\update.inf,DefaultInstall,1,



PUBLIC