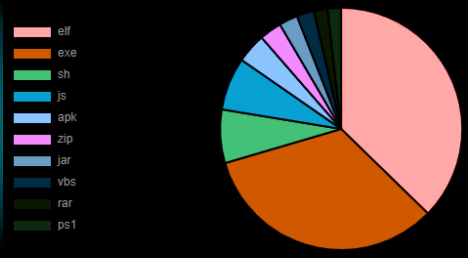

SORINTSEC
THREAT HUNTING
LAB
LegacyHive: Windows ProfSvc enabling cross-user registry Hive Loading
PUBLIC

Index

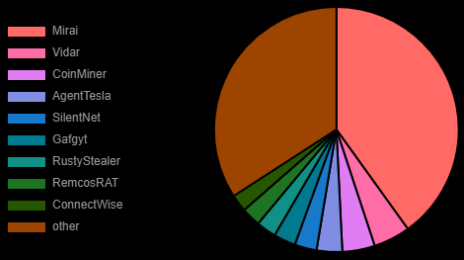
Global Weekly Threat Overview

Public exploits have been released for the critical "wp2shell" remote code execution vulnerabilities affecting WordPress Core.
The wp2shell attack consists of two flaws, tracked as CVE-2026-63030 (REST API batch-route) and CVE-2026-60137 (SQL injection) , that can be chained together to achieve pre-authentication remote code execution against WordPress installs running versions 6.9.x and 7.0.x.
The attack has no preconditions and can be exploited by an anonymous user in a stock install of WordPress with no plugins.

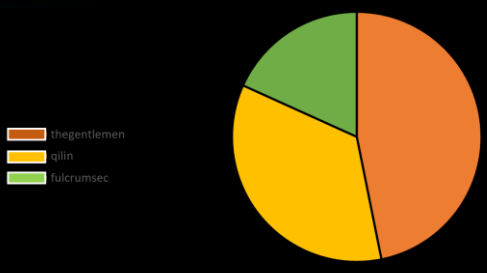
Top 10 file types



Top 10 malware family

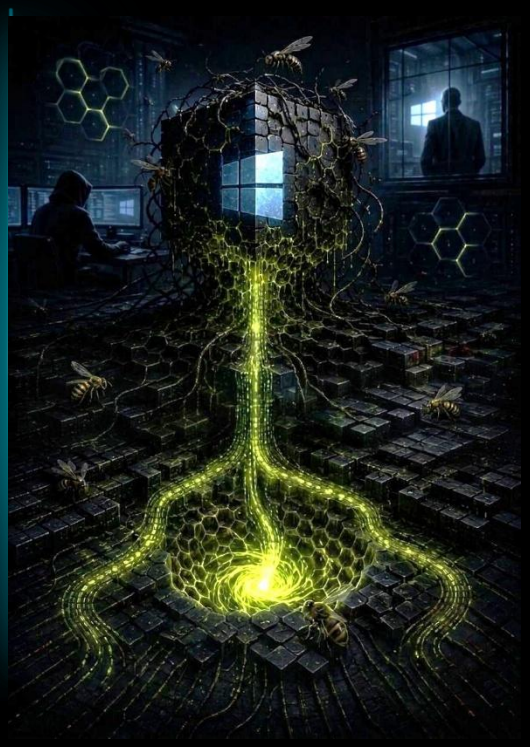


Top 3 Ransomware Group



7-Zip version 26.02 was released on June 25 to fix a remote code execution vulnerability that could allow attackers to execute malicious code by convincing users to open specially crafted compressed files.
According to an advisory from the Zero Day Initiative published this week, a specially crafted XZ data can trigger a heap-based buffer overflow, potentially allowing attackers to execute arbitrary code as the user.
A phishing campaign or social engineering attack could be used to distribute a malicious archive that exploits the flaw to install malware on vulnerable systems.

Global Weekly Notable One



Execution: Hijack Execution Flow

The researcher Nightmare-Eclipse, already known in the security community for repeatedly disclosing impactful Windows zero-day vulnerabilities, has now published a new local privilege escalation flaw dubbed “LegacyHive.” The issue affects the Windows User Profile Service (ProfSvc) and allows a low-privileged local user to abuse registry hive loading logic, object-manager symbolic links, and TOCTOU race conditions to coerce the service into mounting another user’s hive, including that of an administrator,

In practical terms, a successful attack can lead to administrator-level access or SYSTEM-level execution on fully patched Windows systems, with potential impact on confidentiality, integrity, and persistence

Threat Hunting Activity

TACTIC Execution

TECHNIQUES T1574 – Hijack Execution Flow

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

Threat Hunting Activity

The exploit chain described in public analyses combines several primitives: registry poisoning, Object Manager symbolic links, offline registry modification, and a TOCTOU race condition triggered through opportunistic locks. In the public PoC, the attacker prepares a staging directory with permissive access, places a decoy hive there, and then manipulates path resolution so that ProfSvc is redirected toward attacker-controlled locations while it performs hive-loading logic.

The race condition matters because it determines whether the service opens the intended file or the attacker-controlled substitute. The PoC reportedly uses an oplock to pause the service at a precise moment, then swaps or removes a symbolic link before the request completes, so that path resolution falls back to the attacker's desired target. In practical terms, this turns timing into a weapon: the exploit does not need to defeat authentication directly, only to win a narrow file-system and registry-resolution race against a SYSTEM service.

Threat Hunting Activity

Detection can be made looking for anomaly action on UsrClass.dat file, the creation in a non-standard directory is a strong indicator.

file	
creationTime	Jul 20 2026 16:30:09
extension	dat
id	656C9E9CF594AEF5
isDirectory	false
isExecutable	false
location	Local
modificationTime	Jul 20 2026 16:30:09
name	UsrClass.dat
path	C:\tmp\UsrClass.dat
size	0
type	UNKNOWN

PUBLIC