

A large white graphic element consisting of a thick L-shaped line, forming a partial frame around the title text.

THREAT HUNTING

LAB

ShieldCrash - ShieldBreak/CVE-2026-69414 bypass

Global Weekly Threat Overview

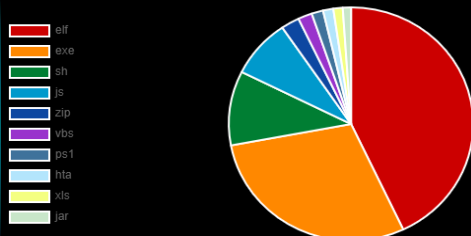
Global Weekly Notable One

Threat Hunting Activity

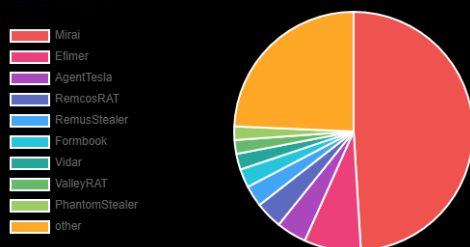
Global Weekly Threat Overview

Microsoft disclosed two separate campaigns this week. The first is an executive-impersonation invoice fraud operation that sent over one million scam emails between August 3-5, 2026, using generative AI to craft CEO/CFO-themed messages tied to fabricated ServiceNow invoices, targeting US finance departments across IT, consumer goods, real estate and manufacturing to trigger fraudulent ACH transfers via lookalike domains such as "service-nowinc[.]com". The second campaign uses passkey-themed social engineering to trick users into registering attacker-controlled authentication methods after suspicious sign-ins, leading to cloud account takeover and data exfiltration, with activity overlapping a cybercrime cluster linked to ShinyHunters.

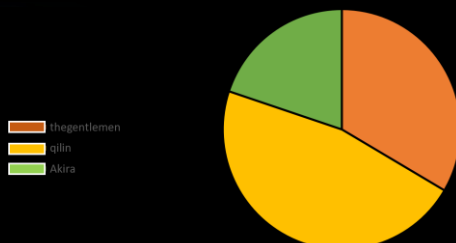
Top 10 file types



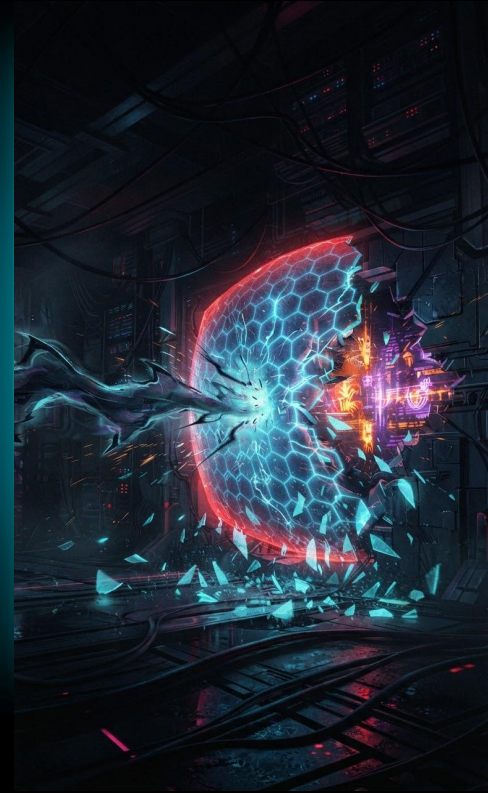
Top 10 malware family



Top 3 Ransomware Group



Researchers from KU Leuven, ETH Zurich, Durham University and Google disclosed DDRop, the first active hardware "interposer" attack to break Intel TDX and AMD SEV-SNP confidential computing on DDR5 memory. A sub-\$200 circuit board inserted between CPU and RAM silently drops write commands, causing the processor to keep reading stale-but-validly-encrypted data as current, without the confidential-computing integrity engine noticing. It requires brief physical/software access to the server and works even against fully patched Intel TDX systems. No simple fix exists since the gap is architectural; the team will present at ACM CCS 2026 and has released the interposer design, firmware and PoC code publicly.



Privilege Escalation: Exploitation for Privilege Escalation

A newly released proof-of-concept demonstrates that a previously patched local privilege escalation vulnerability in a major endpoint security engine can still be triggered under specific conditions, despite the vendor's fix. The underlying flaw sits in how the security engine handles file content during cloud-file hydration through Windows' Cloud Filter API: a user-mode callback lets a low-privileged local process interfere with the data the engine ultimately scans, in combination with filesystem and Object Manager tricks that redirect which file gets processed.

This is the third bypass generation in a chain that started months earlier with an original zero-day, patched, then reopened by a first bypass, patched again, and now reopened a second time. The newly released PoC demonstrates arbitrary file read as NT AUTHORITY\SYSTEM on fully patched, currently supported Windows versions, though it does not yet provide arbitrary write or a full interactive SYSTEM shell. No vendor fix is available for this specific bypass at time of writing.

Threat Hunting Activity

TACTIC

Privilege Escalation

TECHNIQUES

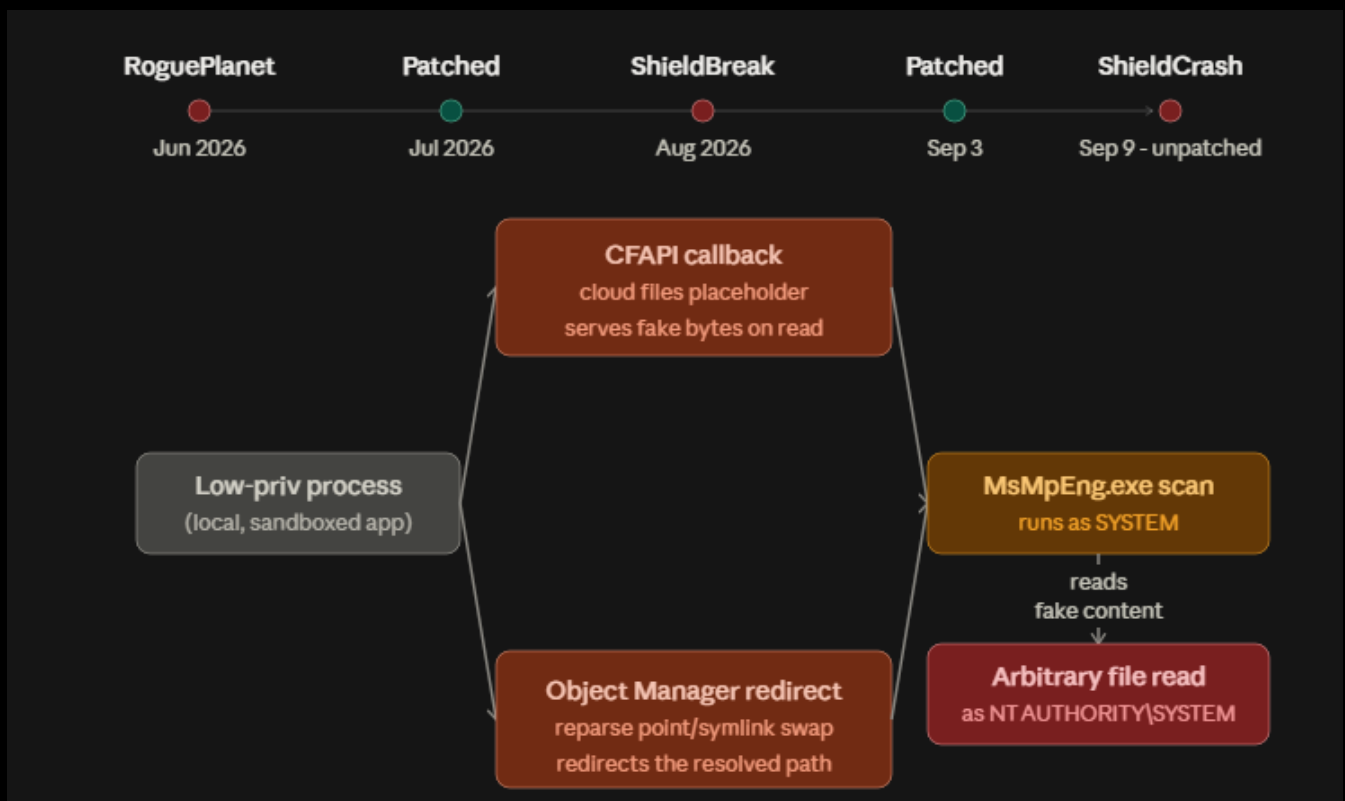
T1068 – Exploitation for Privilege Escalation

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

Threat Hunting Activity

The local process registers a user-mode callback tied to the Cloud Filter API (CFAPI), the mechanism Windows uses to fetch placeholder file content on demand. When the security engine's privileged scanning component requests the content of a file to inspect it, the attacker's callback is positioned to influence the data actually returned. In parallel, filesystem and Object Manager primitives are used to make the engine open or resolve a different file object than the one it believes it is scanning. The combined effect is that the engine, running with SYSTEM-level privileges, ends up processing attacker-supplied content or reading an attacker-chosen file path while operating inside its own privileged context.

The originally patched vulnerability closed off the specific redirection primitive used at the time; the new bypass shows that under specific conditions the same fundamental race between "what the engine decided to scan" and "what content is actually delivered via CFAPI" can still be triggered, granting arbitrary file read as SYSTEM.



Threat Hunting Activity

Detection can focus on Sysmon Event ID 7 for anomalous or unbacked modules loaded into the Defender scanning process (MsMpEng.exe), correlated with Windows Defender Operational Event ID 5007 for unexpected engine/configuration changes around the same timeframe.

Level	Date and time	Source	Event ID	Task category
Information	09:41:13.540	Windows Defender	5007	None
General Details Windows Defender configuration has changed. Old value: Platform Version 4.18.2408.9 New value: Platform Version 4.18.2409.7				

Level	Date and time	Source	Event ID	Task category
Information	09:41:12.104	Sysmon	7	Image loaded
Information	09:41:13.552	Sysmon	7	Image loaded
Information	09:41:13.601	Sysmon	7	Image loaded
General Details Image loaded: UtcTime: 2026-09-09 09:41:13.552 ProcessGuid: {a1b2c3d4-1111-2222-3333-abcde1234567} ProcessId: 4128 Image: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2409.7\MsMpEng.exe ImageLoaded: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2409.7\mpfilter.sys Signed: true Signature: Microsoft Windows SignatureStatus: Valid				

The background is a dark, atmospheric scene with a glowing red sphere in the center, surrounded by a white rectangular frame. The sphere has a hexagonal pattern and is emitting a red glow. The frame is a simple white rectangle. The overall color palette is dark with red and blue highlights.

THREAT HUNTING



SORINT_{SEC}