SORINT.SEC

THREAT HUNTING

LAB

WEEK 01/12/2025 – 05/12/2025

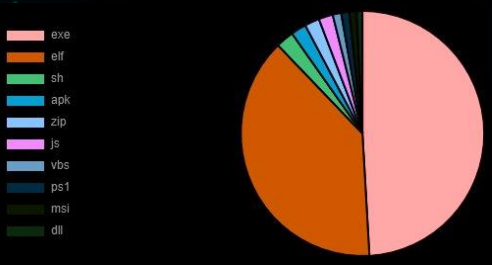
PUBLIC

Index

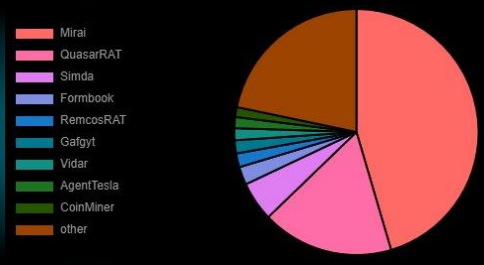
Global Weekly Threat Overview

Google on Monday released monthly security updates for the Android operating system, including two vulnerabilities that it said have been exploited in the wild.
The patch addresses a total of 107 security flaws spanning different components, including Framework, System, Kernel, as well as those from Arm, Imagination Technologies, MediaTek, Qualcomm, and Unison. The two high-severity vulnerability that have been exploited are CVE-2025-48633 (an information disclosure vulnerability in Framework) and CVE-2025-48572 (an elevation of privilege vulnerability in Framework)

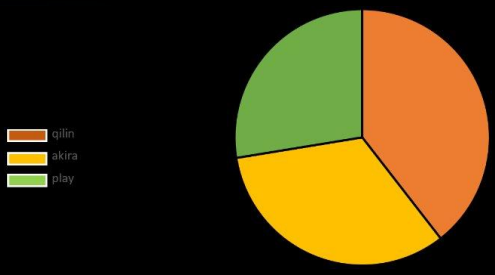
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



The threat actor known as Tomiris has been attributed to attacks targeting foreign ministries, intergovernmental organizations, and government entities in Russia with an aim to establish remote access and deploy additional tools. These attacks highlight a notable shift in Tomiris's tactics, namely the increased use of implants that leverage public services (e.g., Telegram and Discord) as command-and-control (C2) servers. This approach likely aims to blend malicious traffic with legitimate service activity to evade detection by security tools.

Global Weekly Notable One

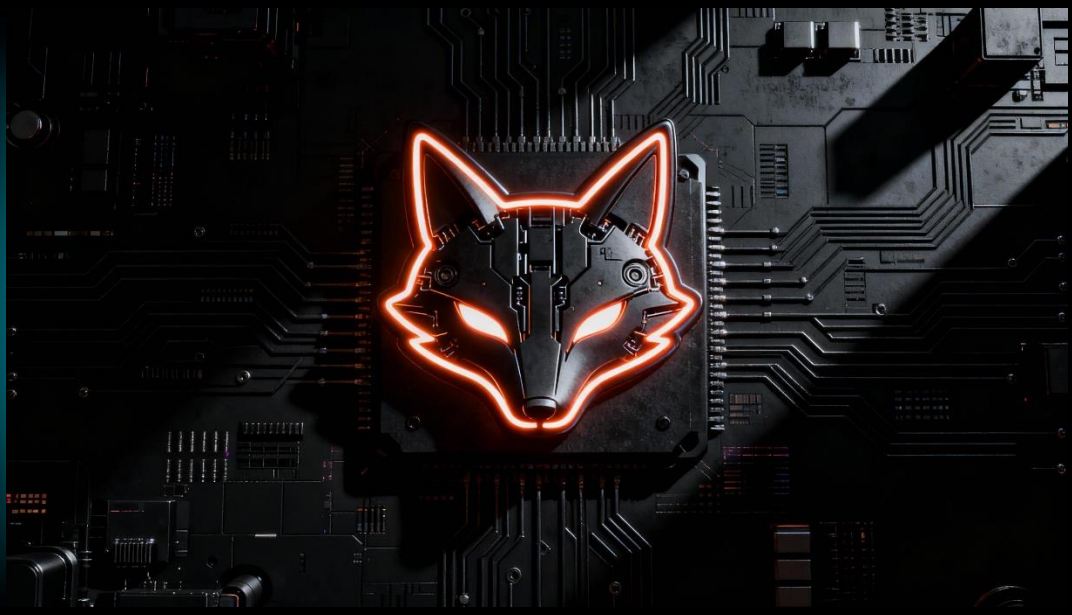
Abuse Elevation Control Mechanism: **Privilege Escalation**

User Account Control (UAC) is a Windows security feature designed to prevent unauthorized elevation of privileges by prompting users for approval before allowing administrative-level actions. UAC is crucial in mitigating the risk of malware silently gaining high-level system access. However, advanced threat actors exploit design quirks in Windows components to bypass UAC prompts, gaining elevated privileges without user consent, thus enabling stealthy execution of malicious code.

One sophisticated UAC bypass technique involves abusing the ICMLuaUtil elevated COM interface, part of the CMSTPLUA UAC COM class family. ICMLuaUtil is a legitimate Windows Component Object Model (COM) interface intended for system operations requiring elevated privileges, such as certain installers or system maintenance tasks. Attackers leverage this by crafting calls to ICMLuaUtil, which inherently possesses elevated execution rights, to launch arbitrary processes with elevated privileges invisibly.

This technique is notable in sophisticated campaigns such as the Silver Fox APT's ValleyRAT operation, where ICMLuaUtil-based UAC bypass is leveraged in multi-stage payload execution chains to maintain stealth and elevated access while evading conventional UAC controls and static detection methods.

Global Weekly Notable One



Abuse Elevation Control Mechanism: **Privilege Escalation**

The Silver Fox APT group, active since at least 2022, is a China-aligned advanced persistent threat actor known for highly sophisticated, multi-stage malware campaigns targeting primarily Chinese-speaking environments.

Silver Fox's campaigns rely on elaborate infection chains combining multiple layers of obfuscation, endpoint security tampering, kernel-level driver attacks, and execution of complex payloads such as ValleyRat, a multicomponent remote access trojan (RAT) used for persistent monitoring and control of victim systems.
A key element of privilege escalation within Silver Fox’s infection chain is the UAC bypass via the ICMLuaUtil elevated COM interface, part of the CMSTPLUA UAC COM class bypass family.

Threat Hunting Activity

TACTIC	Privilege Escalation
TECHNIQUES	T1548 – Abuse Elevation Control Mechanism

Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.

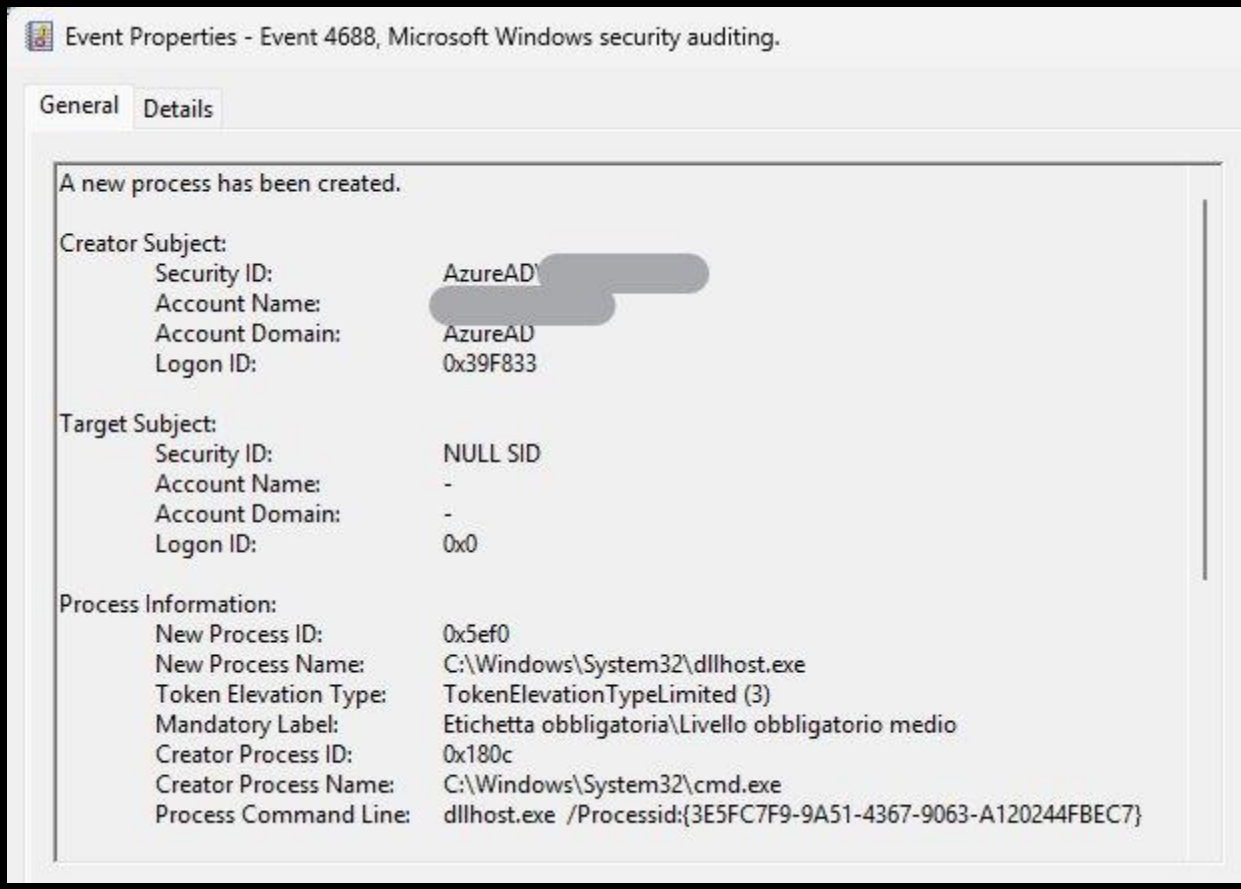
Threat Hunting Activity

This technique works because Windows trusts the ICMLuaUtil COM interface, running its invoked processes with elevated rights but without triggering the usual UAC prompt. The binary used by Silver Fox unpacks itself at runtime and then it invokes dllhost.exe with the /Processid argument specifying the ICMLuaUtil CLSID, thereby requesting the Windows COM subsystem to launch a new elevated process under the context of this trusted auto-elevated interface.

```
C:\>dllhost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
```

Threat Hunting Activity

Detection can be made monitoring Event ID 4688 looking for dllhost.exe execution and suspicious CLSID



PUBLIC