THREAT HUNTING

LAB

WEEK 21/04/2025 - 25/04/2025

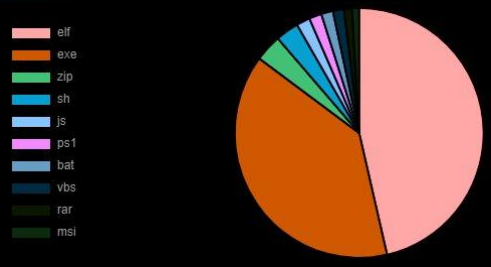
PUBLIC

Index

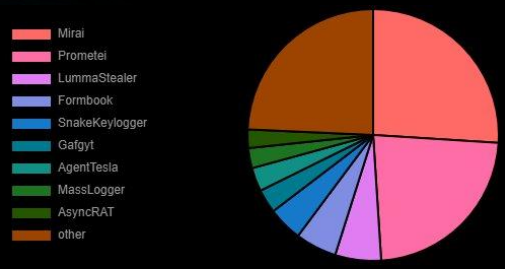
Global Weekly Threat Overview

A new Android malware-as-a-service platform named SuperCard X can facilitate NFC relay attacks, enabling cybercriminals to conduct fraudulent cashouts. The active campaign is targeting customers of banking institutions and card issuers in Italy with an aim to compromise payment card data. There is evidence to suggest that the service is promoted on Telegram channels. SuperCard X employs a multistage approach combining social engineering (via smishing and phone calls), malicious application installation, and NFC data interception for highly effective fraud. The new Android malware, the work of a Chinese-speaking threat actor, has been observed being propagated via three different bogus apps, duping victims into installing them via social engineering techniques like deceptive SMS or WhatsApp messages.

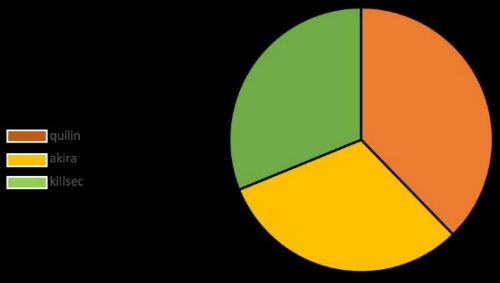
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



ASUS has disclosed a critical security flaw impacting routers with AiCloud enabled that could permit remote attackers to perform unauthorized execution of functions on susceptible devices. The vulnerability, tracked as CVE-2025-2492, has a CVSS score of 9.2.
An improper authentication control vulnerability exists in certain ASUS router firmware series, this vulnerability can be triggered by a crafted request, potentially leading to unauthorized execution of functions. The shortcoming has been addressed with firmware updates for the branches 3.0.0.4_382, 3.0.0.4_386, 3.0.0.4_388, and 3.0.0.6_102.

Global Weekly Notable One

Hide Artifacts: Defense Evasion

LuminousMoth, also known as Bronze President, RedDelta, and Mustang Panda, is a prolific Chinese state-sponsored cyber espionage group active since at least 2012, with a primary focus on government agencies, NGOs, and organizations involved in sensitive geopolitical affairs across Asia, Europe, and the United States. The group is renowned for its sophisticated use of legitimate tools and techniques to achieve execution and evade detection.

A hallmark of LuminousMoth's operations is leveraging legitimate software such as Microsoft's built-in utilities (ike Mavinject.exe) to inject and execute malicious payloads. Recent campaigns have demonstrated LuminousMoth's adaptability and strategic targeting. In late 2024, the group focused on Vietnamese entities, using spear-phishing emails with malicious archive attachments containing LNK or URL files that trigger the execution of their malware when opened by unsuspecting users. These campaigns often exploit current geopolitical events to craft convincing lures, and the group continues to refine its malware arsenal, including custom tools like PlugX, TONESHELL, and PUBLOAD, to enhance espionage capabilities and evade detection.

Global Weekly Notable One

MAVInject.exe, short for Microsoft Application Virtualization Injector, is a legitimate Windows utility designed to inject code into external processes as part of Microsoft's Application Virtualization (App-V) framework. Its primary purpose is to enable virtualized applications to interact with system processes by injecting necessary DLLs into target processes, thereby supporting seamless application virtualization and compatibility.

It retrieves a handle to the target process with specific access rights (such as PROCESS_VM_WRITE and PROCESS_CREATE_THREAD), allocates memory within the target process using VirtualAllocEx, writes the DLL path into this memory via WriteProcessMemory, and finally creates a remote thread in the target process with CreateRemoteThread, which loads the specified DLL using LoadLibraryW. This process allows any DLL, including malicious ones, to be injected into a legitimate running process, effectively masking the execution under a trusted Windows binary.

Threat Hunting Activity

SORINTSEC

TACTIC

Defense Evasion

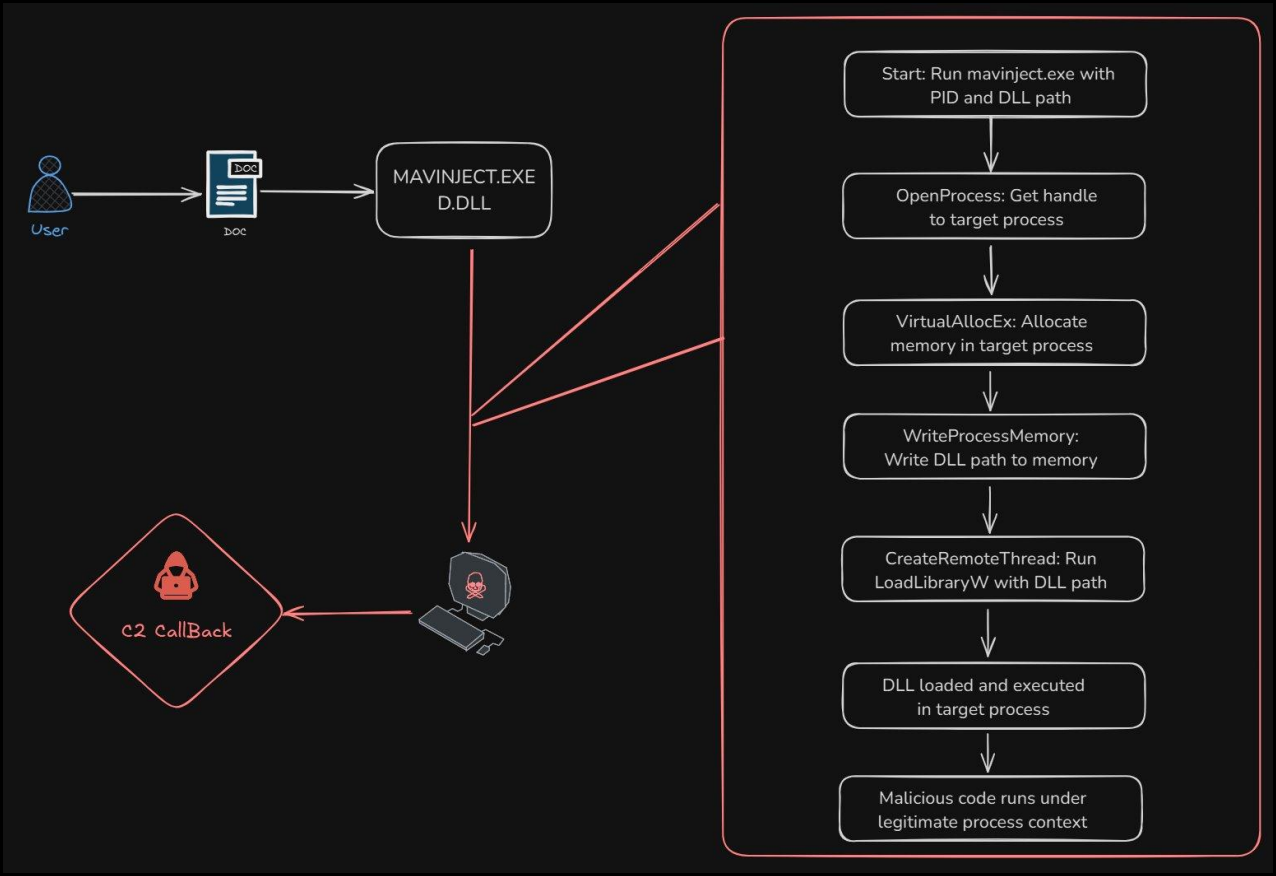
TECHNIQUES

T1218 – System Binary Proxy Execution

Adversaries may carry out malicious operations using a virtual instance to avoid detection. A wide variety of virtualization technologies exist that allow for the emulation of a computer or computing environment. By running malicious code inside of a virtual instance, adversaries can hide artifacts associated with their behavior from security tools that are unable to monitor activity inside the virtual instance.

Threat Hunting Activity

When MAVInject.exe performs DLL injection, it leverages a series of wellestablished Windows API calls to insert malicious code into a running process. The process begins by identifying and opening the target process with sufficient privileges using OpenProcess. Next, MAVInject.exe allocates memory within the target process's address space via VirtualAllocEx, creating a space to store the path to the malicious DLL. It then writes the DLL path into this allocated memory using WriteProcessMemory. MAVInject.exe then retrieves the address of the LoadLibrary function with GetProcAddress, it creates a new thread in the target process using CreateRemoteThread, instructing it to execute LoadLibrary with the injected DLL path as its argument. This causes the target process to load and execute the DLL



Threat Hunting Activity

Targeting the PID of a user process it can execute malicious code with user privileges.

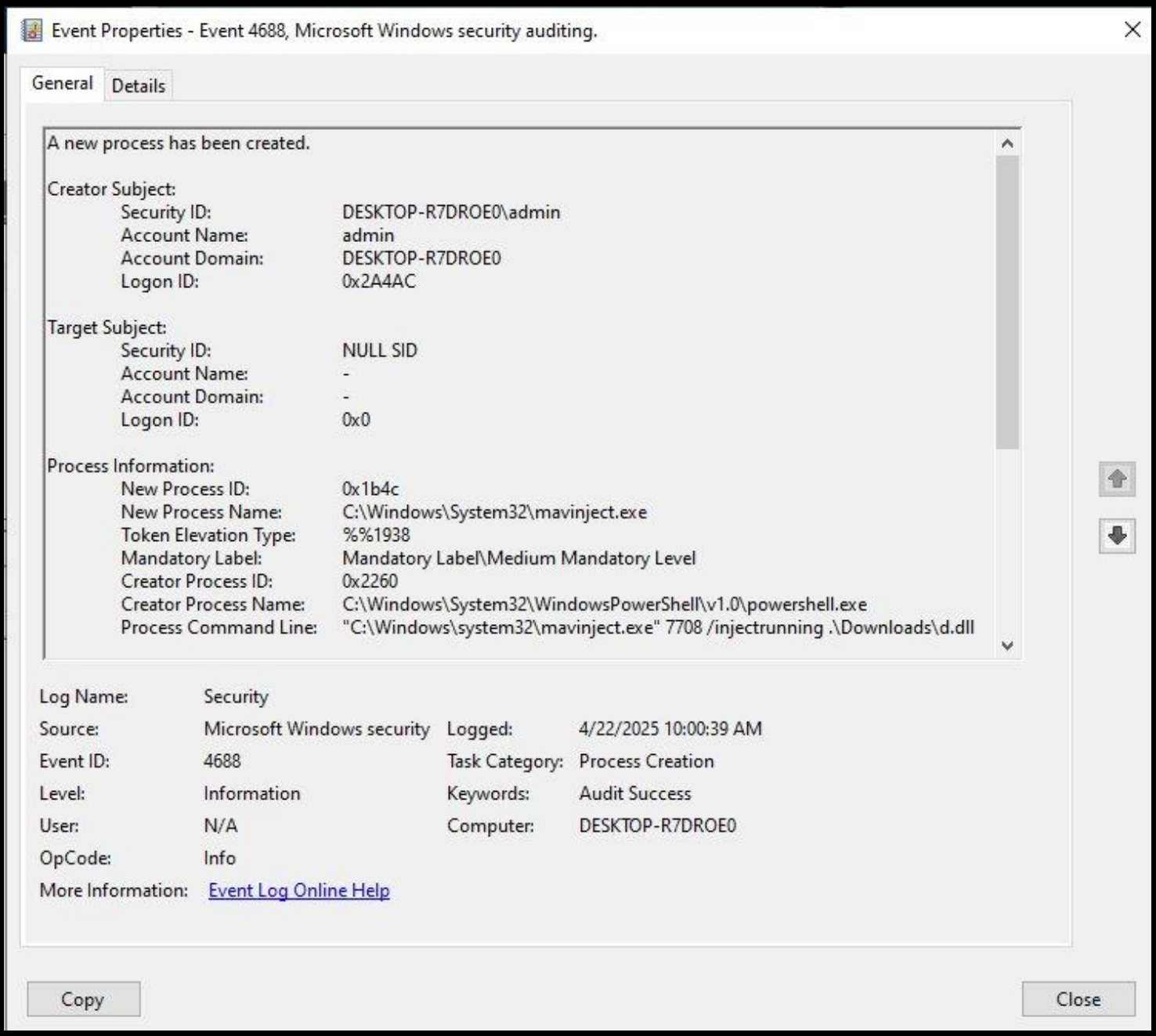
```
PS C:\Users\admin> mavinject.exe 7708 /injectrunning .\Downloads\d.dll
PS C:\Users\admin>
```

Once executed the code is executed into notepad context and a callback to C2 is received.

external	internal	user	computer	process
192.168.138.129	192.168.138.129	admin	DESKTOP-R7DROE0	notepad.exe

Threat Hunting Activity

Once executed the code is executed into notepad context and a callback to C2 is received.



EID 4688

PUBLIC