THREAT HUNTING

LAB

Matanbuchus 3.0: Advanced C++ Loader Evolving MaaS

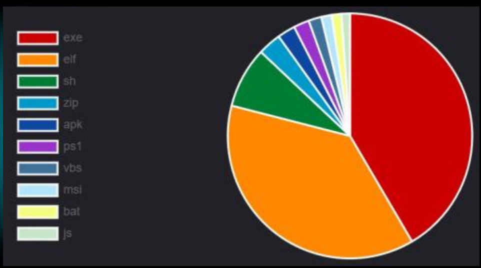
PUBLIC

Index

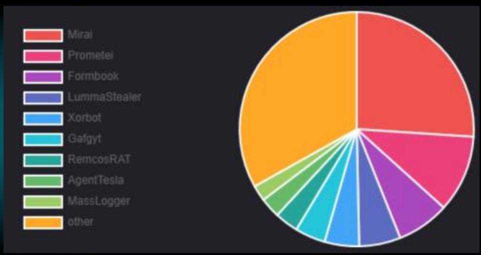
Global Weekly Threat Overview

Cybersecurity researchers have disclosed details of what appears to be a new strain of Shai Hulud on the npm registry with slight modifications from the previous wave observed last month. The npm package that embeds the novel Shai Hulud strain is "@vietmoney/react-big-calendar," which was uploaded to npm back in March 2021 by a user named "hoquocdat." It was updated for the first time on December 28, 2025, to version 0.26.2. The package has been downloaded 698 times since its initial publication. The latest version has been downloaded 197 times. The Shai-Hulud attack first came to light in September 2025, when trojanized npm packages were found stealing sensitive data like API keys, cloud credentials, and npm and GitHub tokens, and exfiltrating them to GitHub repositories using the pilfered tokens. In the second wave spotted in November 2025, the repositories contained the description "Sha1-Hulud: The Second Coming."

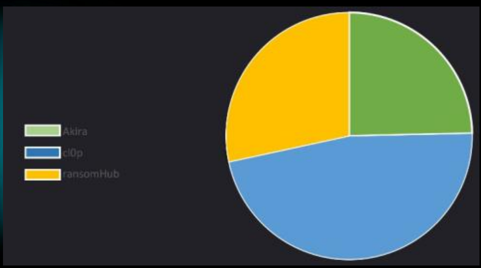
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



IBM has disclosed details of a critical security flaw in API Connect that could allow attackers to gain remote access to the application. The vulnerability, tracked as CVE-2025-13915, is rated 9.8 out of a maximum of 10.0 on the CVSS scoring system. It has been described as an authentication bypass flaw. "IBM API Connect could allow a remote attacker to bypass authentication mechanisms and gain unauthorized access to the application," the tech giant said in a bulletin.

The shortcoming affects the following versions of IBM API Connect -

10.0.8.0 through 10.0.8.5
10.0.11.0

Global Weekly Notable One

Hijack Execution Flow: defense Evasion

Matanbuchus malware emerged in early 2021 when a threat actor using the alias BelialDemon began advertising it on underground forums as a Malware-as-a-Service loader with infrastructure tracing back to domains registered under Austrian ccTLDs and hosted on Google Cloud IPs since February 2021, often themed around fake logins, business planets, and Adobe Flash updates. Primarily targeting enterprise Windows environments in the US and EU Matanbuchus update was released in mid-July 2025 bringing it to version 3.0.

What distinguishes Matanbuchus are features like an heavy C++ implementation with dynamic API resolution via MurmurHash3, per-chunk ChaCha20 decryption of Protobuf-serialized C2 packets mimicking Skype user agents, in-memory shellcode execution via NtAllocateVirtualMemory/NtCreateThreadEx with indirect syscalls and a hardcoded expiration check, making it resilient to static analysis.

Global Weekly Notable One

A Dynamic Link Library (DLL) constitutes a modular Windows binary (.dll file) containing reusable code, functions, and resources that applications load at runtime via LoadLibrary API calls or implicit linking specified in the PE executable's import table, allowing shared functionality like UI rendering or system hooks without duplicating code across processes; legitimate DLLs from Microsoft or vendors reside in trusted paths like %System32% or %ProgramFiles%, but attackers craft dropper DLLs mimicking expected imports to hijack execution flow.

DLL sideloading exploits the search order precedence where Windows probes for DLL dependencies first in the launching executable's directory, then current working directory, %Windows%, %System32%, and registered PATH locations, permitting a malicious DLL with the same name as a legitimate import placed alongside the benign EXE to get loaded preferentially. Matanbuchus 3.0, a C++-based backdoor loader, leverages DLL sideloading via HRUpdate.exe—a legitimate executable from HR software vendors—to proxy execution of its malicious loader DLL. HRUpdate.exe then spawning unexpected children from non-standard paths enabling initial foothold without dropping obvious malware artifacts.

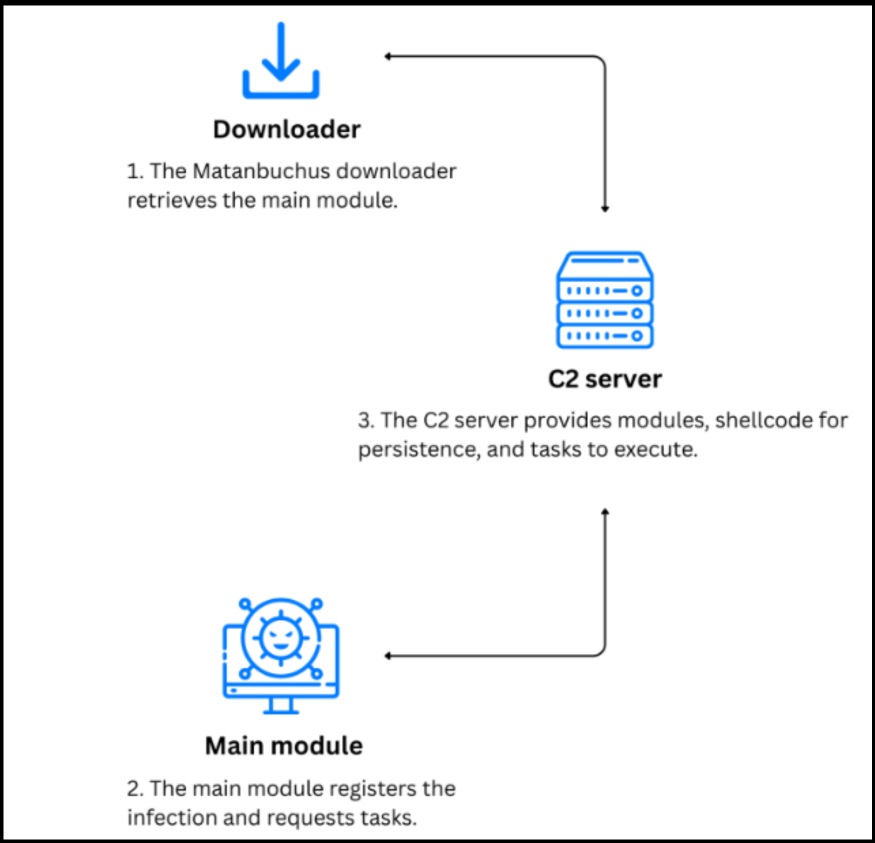
Threat Hunting Activity

TACTIC	Defense Evasion
TECHNIQUES	T1574 – Hijack Execution Flow

Adversaries may abuse dynamic-link library files (DLLs) in order to achieve persistence, escalate privileges, and evade defenses. DLLs are libraries that contain code and data that can be simultaneously utilized by multiple programs. While DLLs are not malicious by nature, they can be abused through mechanisms such as side-loading, hijacking search order, and phantom DLL hijacking.

Threat Hunting Activity

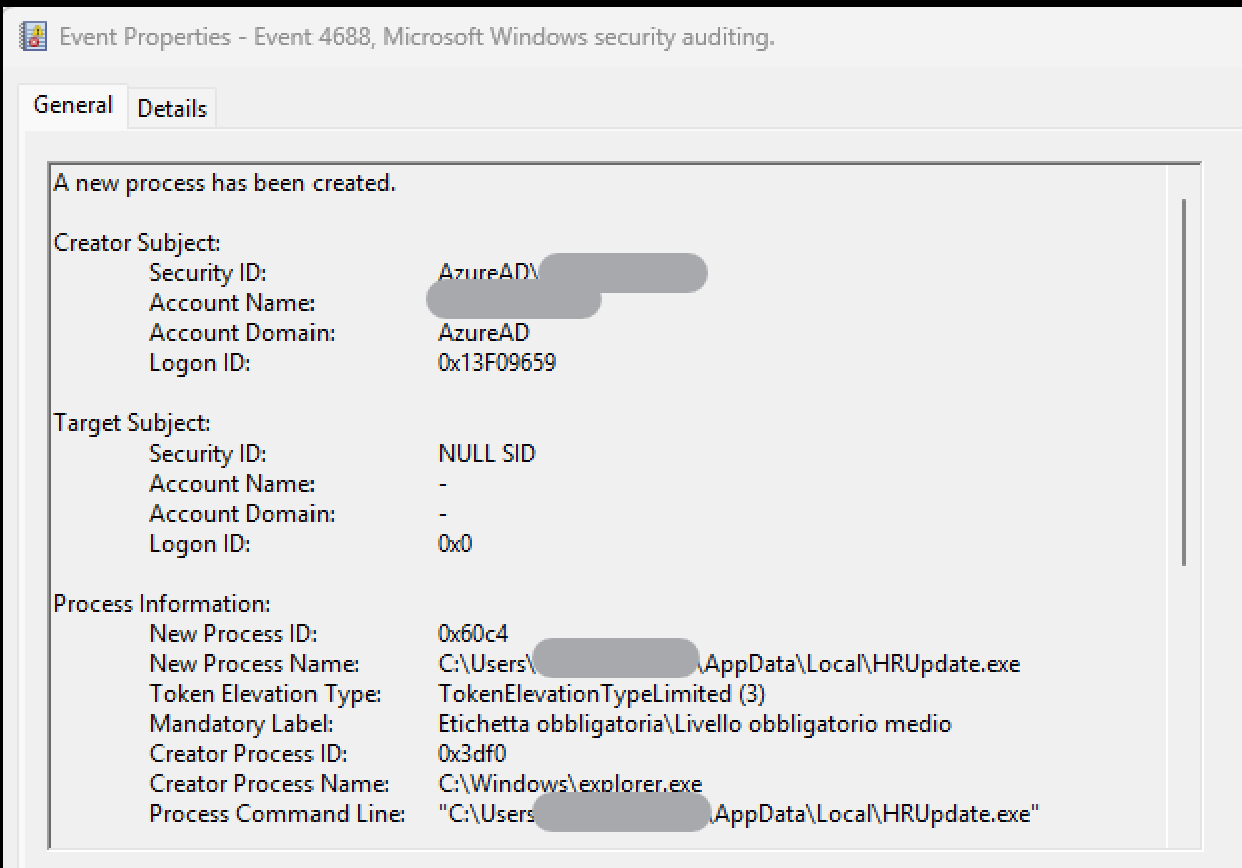
For the first download phase the malware introduce into victim system a legit software that then load a malicious dll during the execution. In this case the software chosen is a component of a free AV solution found into MS Store called “Huorong Internet Security”. The executable HRUpdare is vulnerable to dll sideloading.



Once executed the matanbuchus downloader module is retrieved and the communication with the c2 server is initiated.

Threat Hunting Activity

Detection can be made monitoring event id 4688



Event ID 4688


THREAT
HUNTING
SORINT.SEC