SORINT.SEC

THREAT HUNTING

LAB

Rhysida's OysterLoader:
Multi-Stage Fake Installer Campaign

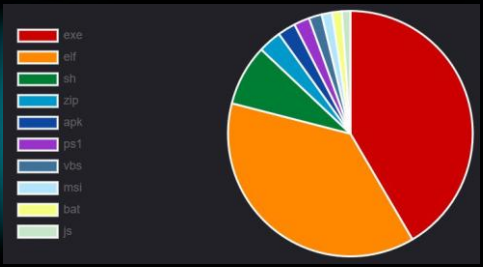
PUBLIC

Index

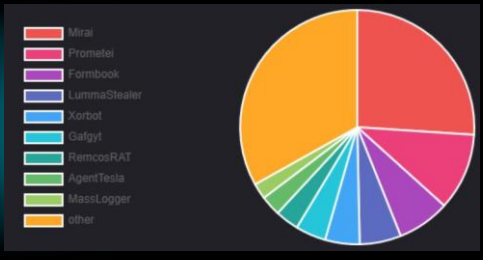
Global Weekly Threat Overview

A suspected Chinese state-backed hacking group has been quietly exploiting a critical Dell security flaw in zero-day attacks that started in mid-2024. Security researchers from Mandiant and the Google Threat Intelligence Group (GTIG) revealed that the UNC6201 group exploited a maximum-severity hardcoded-credential vulnerability (tracked as CVE-2026-22769) in Dell RecoverPoint for Virtual Machines, a solution used for VMware virtual machine backup and recovery. This is considered critical as an unauthenticated remote attacker with knowledge of the hardcoded credential could potentially exploit this vulnerability leading to unauthorized access to the underlying operating system and root-level persistence. Dell recommends that customers upgrade or apply one of the remediations as soon as possible.

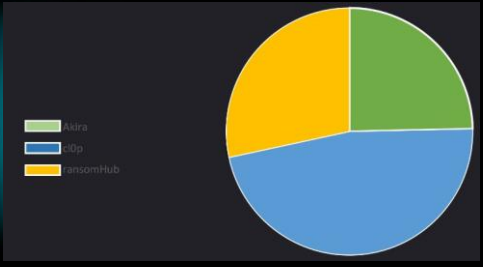
Top 10 file types



Top 10 malware family

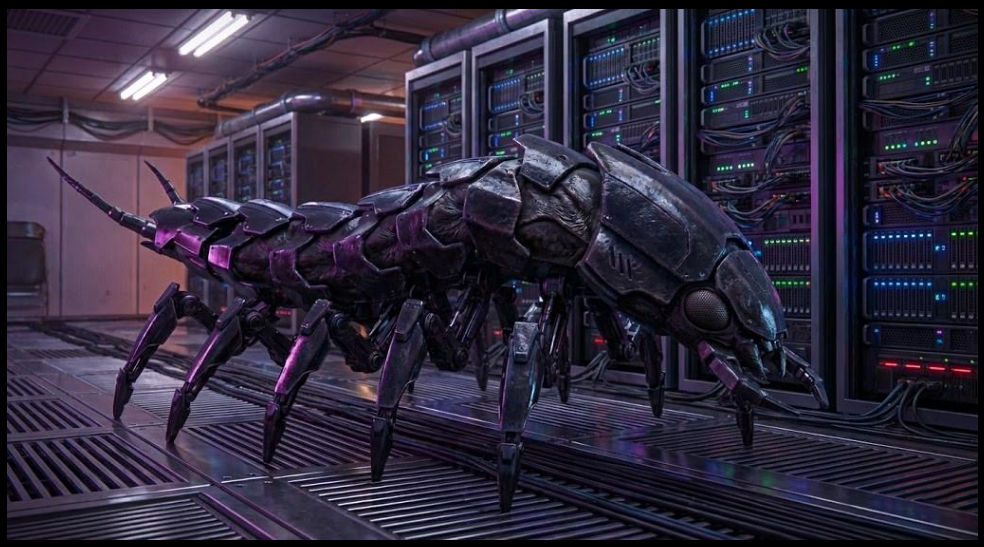


Top 3 Ransomware Group



A newly discovered and sophisticated Android malware called Keenadu has been found embedded in firmware from multiple device brands, enabling it to compromise all installed applications and gain unrestricted control over infected devices. According to a report from cybersecurity company Kaspersky, Keenadu has multiple distribution mechanisms, including compromised firmware images delivered over-the-air (OTA), via other backdoors, embedded in system apps, modified apps from unofficial sources, and even through apps on Google Play. As of February 2026, Kaspersky has confirmed 13,000 infected devices, many located in Russia, Japan, Germany, Brazil, and the Netherlands.

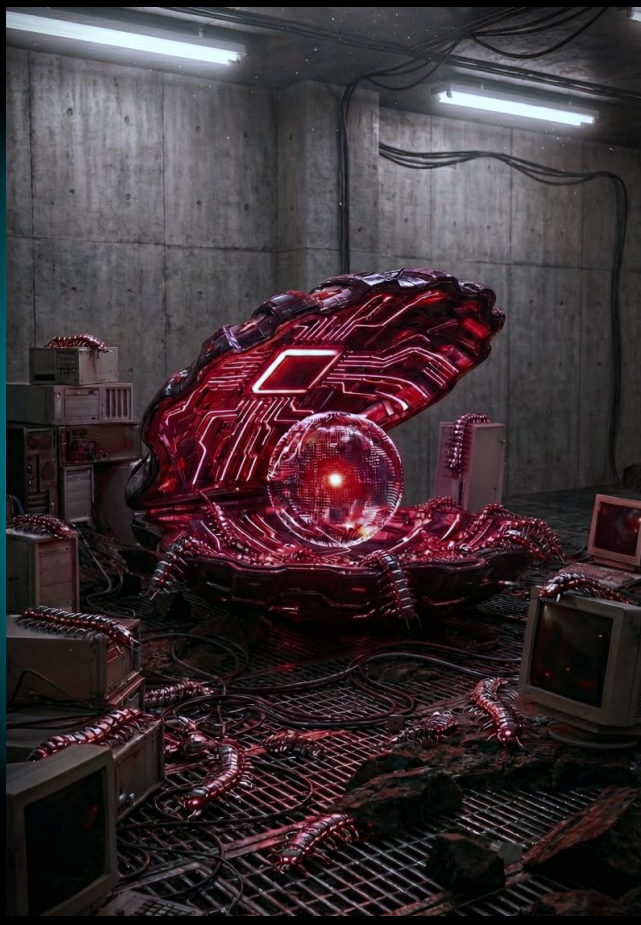
Global Weekly Notable One



Rhysida is a Ransomware-as-a-Service (RaaS) group that emerged in May 2023, targeting sectors like government, healthcare, education, manufacturing, and technology. They gain initial access via phishing, exploited public-facing apps, stolen VPN credentials, or valid accounts bought on dark web markets. Operators deploy Cobalt Strike beacons for lateral movement, reconnaissance with tools like net commands and ipconfig, and persistence via AnyDesk or scheduled tasks.

Rhysida employs double-extortion, exfiltrating data using tools like DataGrabber before encrypting files with ChaCha20 algorithm and 4096-bit RSA keys, appending ".rhysida" extensions. They demand Bitcoin ransoms via TOR portals, threatening leaks on their site if unpaid; Lacking mature features like VSS deletion, they sometimes skip encryption for pure extortion.

Global Weekly Notable One



Scheduled Task: persistence

The OysterLoader campaign, orchestrated by the Rhysida ransomware gang, primarily utilizes search engine malvertising to lure users into downloading malicious installers from typo-squatted websites. These fake installers, often impersonating tools like Microsoft Teams, are code-signed to bypass security filters and silently deploy a multi-stage backdoor. This initial phase successfully establishes a foothold on enterprise devices by leveraging deceptive delivery methods.

Upon execution, the malware progresses through four distinct stages involving anti-debugging checks, custom decompression, and host fingerprinting. It ensures persistence by creating scheduled tasks while communicating with command-and-control servers through obfuscated JSON messages and non-standard encoding. Ultimately, this sophisticated chain serves as a conduit for delivering high-impact payloads, specifically the Rhysida ransomware or the Vidar infostealer, within compromised networks.

Threat Hunting Activity

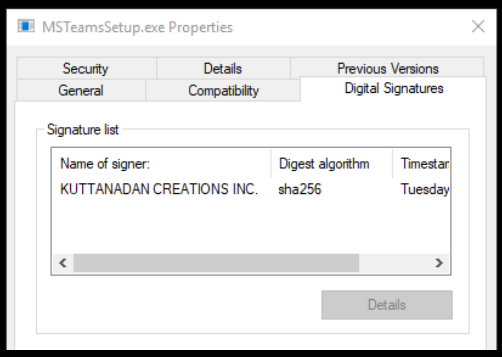
TACTIC Persistence

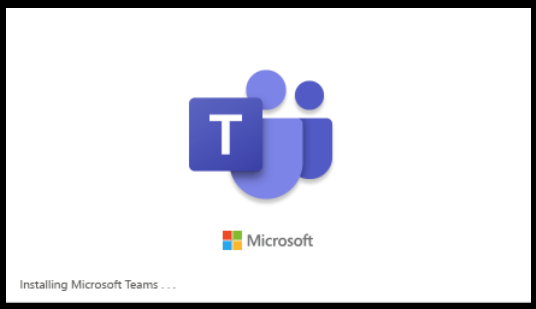
TECHNIQUES T1053 – Scheduled Task

The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

Threat Hunting Activity

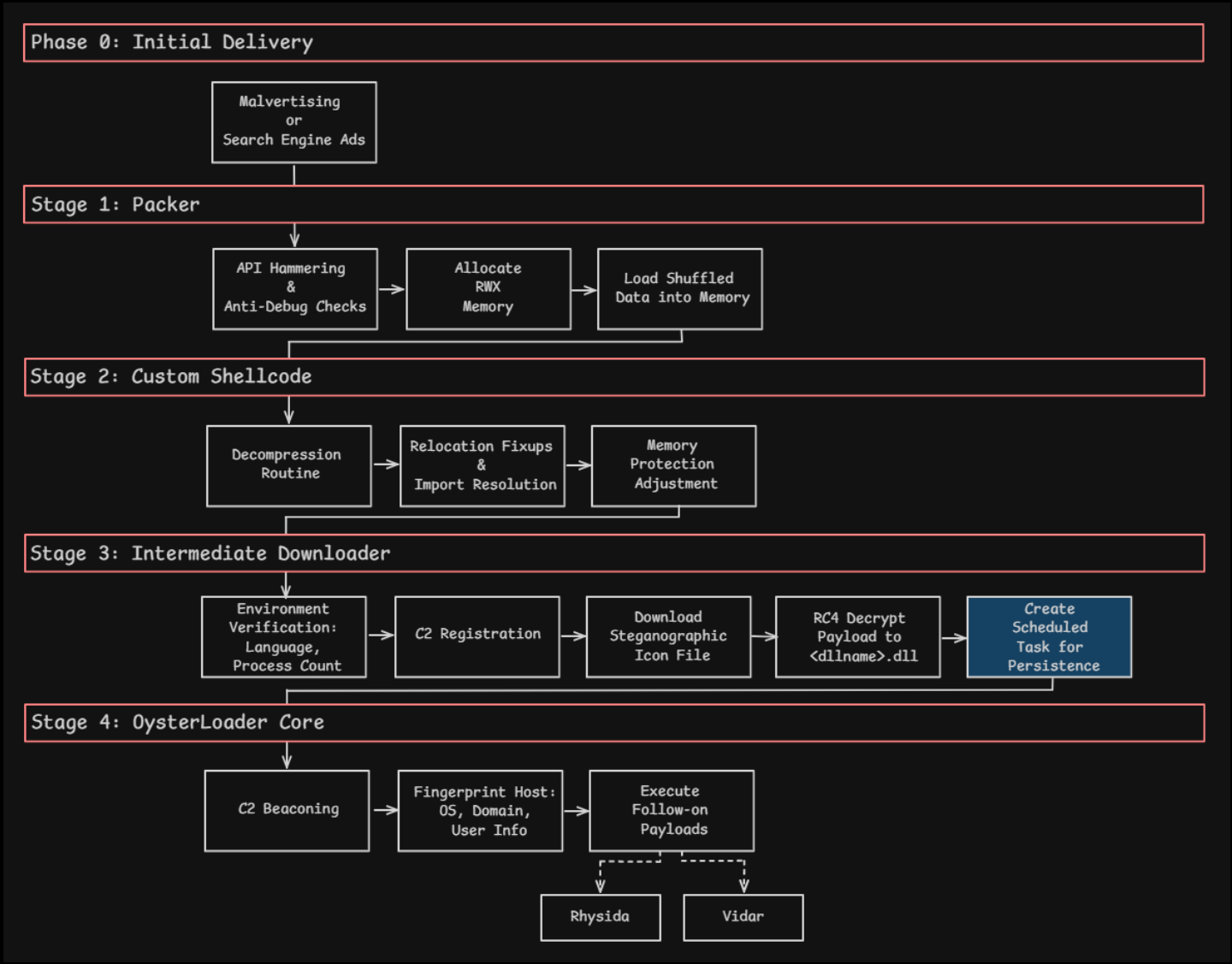
OysterLoader delivery begins with malvertising, directing users to typo-squatted sites impersonating software like Microsoft Teams. Victims download code-signed malicious installers, such as MSTeamsSetup.exe. To avoid suspicion, these files drop the backdoor while simultaneously launching the genuine Teams installer to deceive the user.





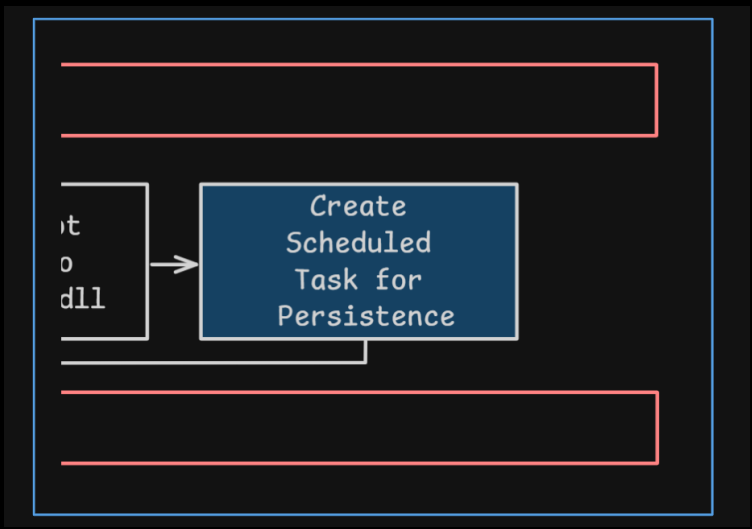
Threat Hunting Activity

OysterLoader executes in four different stages. Initially, a TextShell packer uses API hammering and anti-debugging to load shellcode. This shellcode performs custom decompression and relocation fixups. An intermediate downloader then verifies the environment, establishes persistence, and decrypts the final stage. Finally, the core DLL fingerprints the system to deploy ransomware.



Threat Hunting Activity

The malware ensures persistence by creating scheduled tasks via schtasks.exe to repeatedly execute its malicious DLLs. Common tasks include ClearMngs, running every three hours, and COPYING, running every 13 minutes. These tasks use rundll32.exe to launch the backdoor, securing long-term access for proceed in the infection chain.



To detect this behavior we can do it by monitoring new scheduled tasks created with used flags and OysterLoader names, correlating with the executions of 'rundll32.exe' executing DLLs from the observed directory with the used exported function and the same known OysterLoader names.

```
C:\Windows\System32\schtasks.exe /Create /SC MINUTE /MO 13 /TN "COPYING3" /TR
"C:\Windows\System32\rundll32.exe C:\Users\<redacted>\AppData\Roaming\<15 random
alphanum>\COPYING3.dll DllRegisterServer"
```

PUBLIC