Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

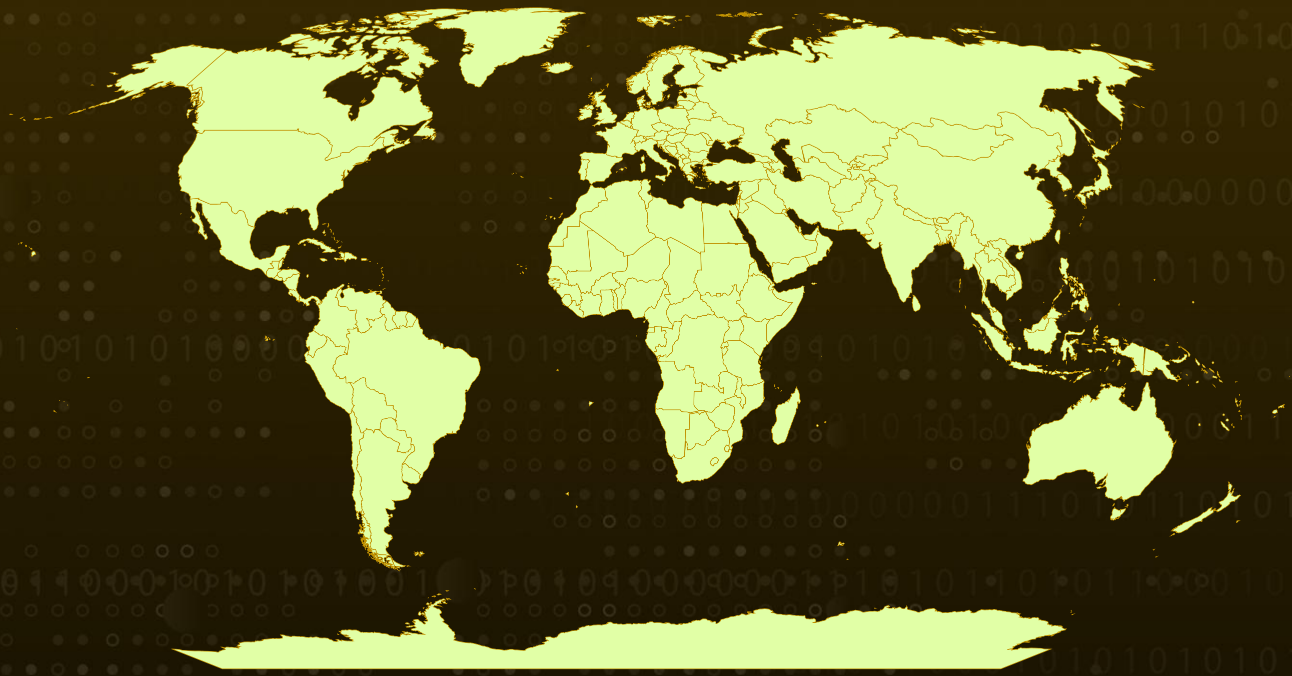
OysterLoader Threat Model: Silent, Signed, Systematic

Date of Publication	Admiralty Code	TA Number
February 19, 2026	A1	TA2026048

Summary

First Seen: September 2023
Targeted Regions: Global
Targeted Platforms: Windows
Targeted Products: PuTTY, WinSCP, Google Authenticator, Microsoft Teams, Google Chrome
Targeted Industries: Technology, IT
Malware: OysterLoader (aka Broomstick, CleanUp, CleanUpLoader)
Attack: OysterLoader, a sophisticated multi-stage malware loader, continues evolving in 2026 with enhanced obfuscation and C2 methods. It primarily spreads via malvertising campaigns, redirecting users to fake download sites for popular software. The loader, signed with valid certificates from legitimate companies, installs malicious payloads like Rhysida ransomware and Vidar infostealer. Since its initial discovery, OysterLoader has undergone sustained development with updated C2 endpoints, obfuscation methods, and fingerprinting schemas, signaling active and committed threat actor operations.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

🟨 Targeted 🟫 Non-Targeted

Attack Details

#1

OysterLoader, a sophisticated multi-stage malware loader, continues to evolve into 2026, refining its command-and-control (C2) infrastructure and obfuscation methods. Written in C++, it serves as a delivery mechanism for ransomware payloads like Rhysida and commodity malware such as Vidar infostealer. The loader primarily spreads through malvertising campaigns, exploiting search engine results to direct users to counterfeit websites posing as legitimate download portals for software such as Microsoft Teams, Google Chrome, PuTTY, and WinSCP. These fraudulent sites use typosquatted domains, to deceive victims. The malicious installers, signed with valid Authenticode certificates from companies to further enhance the illusion of authenticity. OysterLoader's distribution methods have also expanded through integration with the Gootloader malware framework, broadening its initial access vectors.

#2

Upon execution, the malware initiates a four-stage infection process. The first stage, TextShell, employs API call flooding-hundreds of legitimate Windows DLL calls, including GDI functions-to evade heuristic detectors, confuse sandboxes, and hinder reverse engineering. It also checks for debuggers using methods like IsDebuggerPresent, trapping execution in infinite loops if detected. The packer dynamically resolves critical API functions through custom hashing, making signature detection difficult.

#3

The third stage serves as an intermediate downloader, validating the environment, creating a mutex to prevent duplicate instances, and establishing communication with C2 servers. The C2 protocol has evolved from a simple two-endpoint model to a more complex three-step process. This begins with an empty GET request, followed by a system fingerprint submission, and ends with dynamic beaconing to new endpoints.

#4

In the fourth stage, OysterLoader ensures persistence and prepares for payload delivery. It drops a DLL into the %APPDATA% or Temp directory and creates a scheduled task, ClearMngs, to execute the DLL via rundll32.exe at intervals ranging from 13 minutes to three hours. Additionally, it uses Registry Run Keys for persistence.

Recommendations

Block Unsigned and Untrusted MSI Installers: Configure endpoint protection policies to prevent execution of MSI files that are not signed by verified, trusted publishers. Implement application whitelisting to restrict software installation to approved sources only.

Monitor for Suspicious Scheduled Task Creation: Deploy detection rules to alert on the creation of scheduled tasks that invoke rundll32.exe to load DLLs from user-writable directories such as %APPDATA% and %TEMP%. Specifically monitor for task names matching known patterns like ClearMngs.

Detect Anomalous API Call Patterns: Tune endpoint detection and response (EDR) solutions to identify processes exhibiting high volumes of GDI and system API calls that are inconsistent with their declared purpose, which may indicate API flooding obfuscation techniques.

Enforce TLS Inspection for Outbound Traffic: Implement TLS inspection on egress traffic to identify custom HTTP headers, non-standard user-agent strings, and anomalous Base64-encoded payloads characteristic of OysterLoader C2 communications.

Hunt for Known Mutex Values: Conduct threat hunting across the enterprise for the creation of mutex objects matching known OysterLoader patterns, such as ITrkfSaV-4c7KwdfnC-Ds165XU4C-lH6R9pk1, to identify potentially compromised endpoints.

Restrict Rundll32 Usage: Implement policies to monitor and restrict the use of rundll32.exe for loading DLLs from non-standard or user-writable locations. Alert on any rundll32.exe invocations referencing DLLs in %TEMP%, %APPDATA%, or other suspicious paths.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1189: Drive-by Compromise	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1106: Native API	
	T1129: Shared Modules	
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1027: Obfuscated Files or Information	T1027.007: Dynamic API Resolution
		T1027.002: Software Packing
	T1140: Deobfuscate/Decode Files or Information	
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Checks
	T1622: Debugger Evasion	

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1055: Process Injection	T1055.012: Process Hollowing
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1016: System Network Configuration Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1001: Data Obfuscation	T1001.002: Steganography
	T1132: Data Encoding	T1132.001: Standard Encoding
		T1132.002: Non-Standard Encoding
	T1105: Ingress Tool Transfer	
	T1573: Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	supfoundrysettlers[.]us, whereverhomebe[.]com, retdirectyourman[.]eu, prodfindfeatures[.]com, micrsoft-teams-download[.]com, impresoralaser[.]pro
Filename	CleanUp30.dll, COPYING3.dll, MSTeamsSetup_c_l_.exe, TMSSetup.exe, CleanUp.dll, DiskCleanUp.lnk
IPv4	85[.]239[.]53[.]66, 51[.]222[.]96[.]108, 135[.]125[.]241[.]45, 149[.]248[.]79[.]62, 64[.]95[.]10[.]243, 206[.]166[.]251[.]114
Mutex	ITrkfSaV-4c7KwdfnC-Ds165XU4C-lH6R9pk1
SHA256	9601f3921c2cd270b6da0ba265c06bae94fd7d4dc512e8cb82718eaa24accc43, 574c70e84ecdad901385a1ebf38f2ee74c446034e97c33949b52f3a2fddcd822, cfc2fe7236da1609b0db1b2981ca318bfd5fbbb65c945b5f26df26d9f948cbb4, 82b246d8e6ffba1abaffbd386470c45cef8383ad19394c7c0622c9e62128cb94
URLs	hxxps[:]//grandideapay[.]com/api/v2/facade, hxxp[:]//nucleusgate[.]com/api/v2/facade, hxxps[:]//cardlowestgroup[.]com/api/v2/facade, hxxps[:]//socialcloudguru[.]com/api/v2/facade, hxxps[:]//coretether[.]com/api/v2/facade, hxxps[:]//registrywave[.]com/api/v2/facade

References

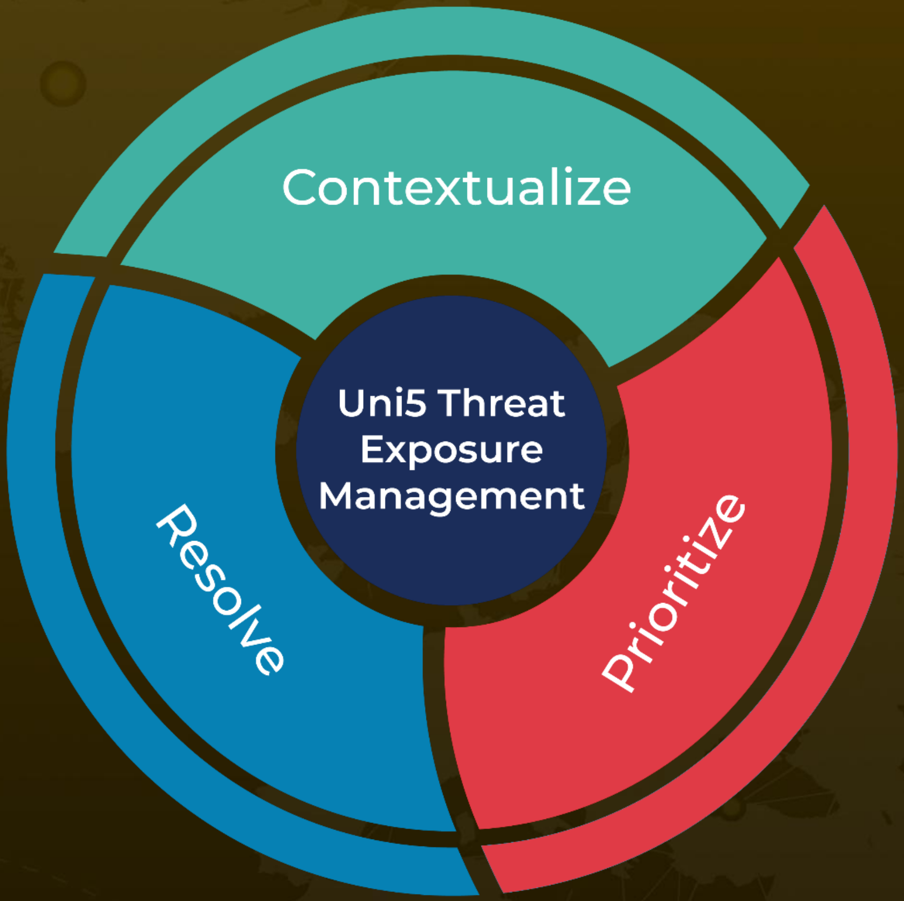
https://blog.sekoia.io/oysterloader-unmasked-the-multi-stage-evasion-loader/

https://www.rapid7.com/blog/post/2024/06/17/malvertising-campaign-leads-to-execution-of-oyster-backdoor/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 19, 2026 • 06:00 AM

More at www.hivepro.com