Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

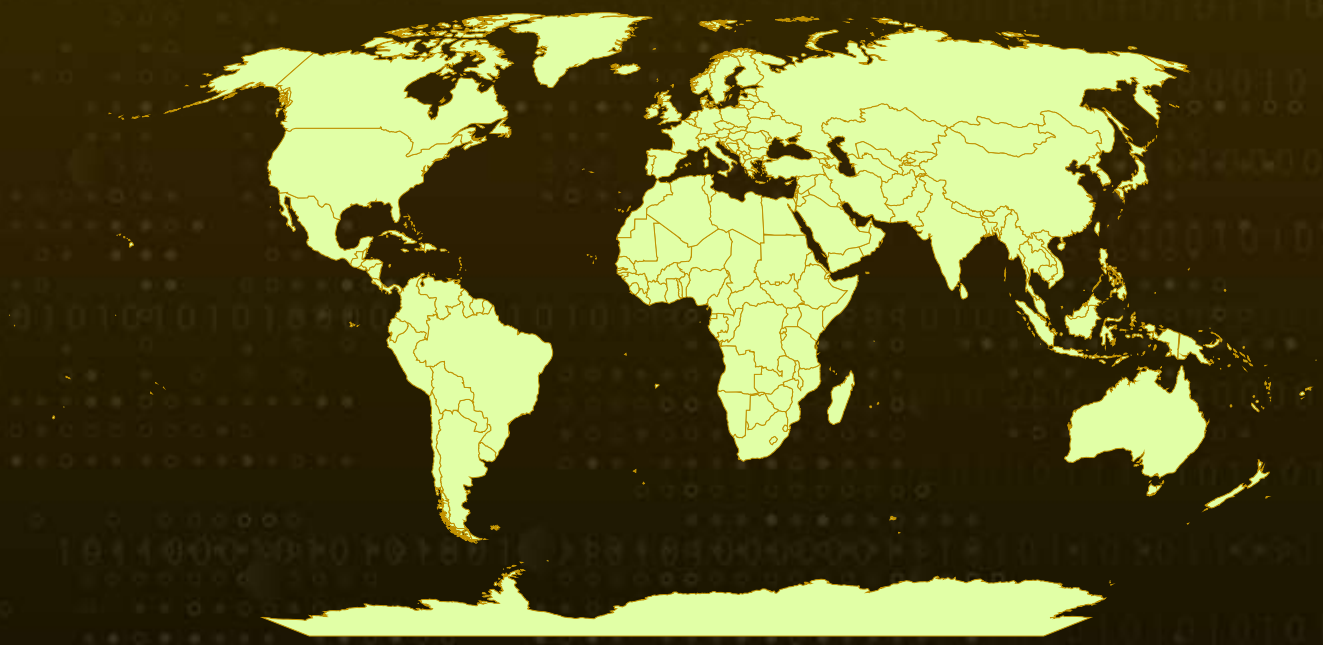
LabubaRAT: A Rust-Based Remote Access Framework

Date of Publication	Admiralty Code	TA Number
July 16, 2026	A1	TA2026200

Summary

First Seen: June 2026
Targeted Region: Worldwide
Targeted Platform: Windows (64-bit)
Targeted Products: NVIDIA Container Runtime Toolkit (impersonated); Google Chrome, Mozilla Firefox, Microsoft Edge, and Brave (browsers inventoried); Microsoft Defender, CrowdStrike, SentinelOne, Carbon Black, Sophos, Malwarebytes, Bitdefender, ESET, Kaspersky, McAfee, Symantec, and Trend Micro (endpoint security products profiled)
Malware: LabubaRAT
Attack: LabubaRAT is a new remote access tool that disguises itself as NVIDIA software to infect Windows computers. Instead of hardcoding its control server, it accepts configuration at startup, allowing attackers to reuse the same malware across multiple targets. The malware also profiles infected computers to identify security tools and browsers before awaiting operator commands, indicating it was built as a reusable framework designed for Malware-as-a-Service deployments.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

LabubaRAT is a new Rust-based remote access trojan designed for Windows systems. The malware disguises itself as NVIDIA software by using a fake executable named nvidia-sysruntime.exe, complete with fabricated NVIDIA metadata and a legitimate-looking debug path. Instead of relying on a hardcoded command-and-control server, it accepts configuration details through command-line arguments or environment variables at startup. Once installed, it stores its settings in a local SQLite database. It achieves persistence by adding itself to the Windows startup registry, typically using encoded configuration strings to keep the command line less conspicuous.

#2

The malware uses a flexible configuration system that accepts settings such as organization name, API key, group designation, and server address as separate arguments or as a single Base64 string. This approach allows the same binary to be reused across different targets and campaigns without modification. Before waiting for operator commands, the malware profiles the infected computer. It gathers basic details like hostname, CPU model, and RAM, then checks what browsers and security software are installed. It looks for popular antivirus solutions, including Microsoft Defender, CrowdStrike, SentinelOne, and others by examining the Windows registry.

#3

Notably, the malware itself does not include credential-stealing or network-spreading capabilities-those actions are left to the operator, who can use the malware's built-in remote access features to run additional tools as needed. The malware communicates over multiple channels-standard HTTPS requests with authentication tokens, embedded Microsoft Edge components, or DNS tunneling with encoded commands. It supports file transfers, screenshot capture, shell and PowerShell execution, JavaScript through Windows Script Host, and the ability to act as a network proxy. Three additional server IP addresses in Germany share the same control panel interface, suggesting this malware was deployed across multiple locations starting in early June 2026, indicating it was built as reusable infrastructure for multiple campaigns.

Recommendations

Enforce Signed-Binary Policy for Vendor-Themed Executables: Alert on unsigned executables that carry vendor version metadata claiming NVIDIA, Intel, AMD, or similar trusted origin, particularly when they execute from user-writable paths, temporary directories, or outside standard Program Files locations.

Detect Base64-Encoded Command Lines Paired with Persistence: Build detections for HKCU\Software\Microsoft\Windows\CurrentVersion\Run entries that launch binaries with long Base64-like command-line arguments, especially where the decoded value reveals configuration fields such as --org, --key, --group, --server, --dns-domain, or --dns-resolver.

Hunt for Local Enrollment Artifacts: Search endpoints for the SQLite database nvctr_sys.db (and matching -wal and -shm files), the single-instance mutex Local\NVIDIAContainerMonitor_SingleInstance, and stored keys such as server_url, device_token, dns_domain, and polling interval values.

Monitor Unusual Parents for Shell and Script Execution: Alert on uncommon parent processes spawning cmd.exe, powershell.exe, wscript.exe, or cscript.exe; flag temporary files with a wupd_ prefix; and monitor for screen-capture GDI API sequences (GetDC, CreateCompatibleBitmap, BitBlt, GetDIBits) originating from non-graphics processes.

Strengthen Windows Script Host Coverage: Where possible, disable or restrict Windows Script Host on endpoints that do not require it, and where restriction is not feasible, enable Script Block and Module Logging equivalents for wscript.exe and cscript.exe so JScript execution matches the visibility available for PowerShell.

Segment and Monitor for SOCKS5 Relay Behavior: Apply network segmentation so that endpoints cannot arbitrarily initiate outbound tunnels to internet infrastructure, and detect SOCKS5 handshake patterns and long-lived outbound sessions from workstations that should not act as proxies.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.001: PowerShell
		T1059.007: JavaScript
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1012: Query Registry	
	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
Collection	T1113: Screen Capture	
	T1560: Archive Collected Data	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.004: DNS
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1573: Encrypted Channel	
	T1090: Proxy	
	T1105: Ingress Tool Transfer	
	T1568: Dynamic Resolution	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	b7443b0ab48d2f5786d1b6f3a580f02621e9ae5a3877ee3a44e01df13d984328
MD5	d8bf355a198fb5db3ea65cfdfcdfbd19
Filename	nvidia-sysruntime.exe, nvctr_sys.db
File Path	nvidia_container.pdb, C:\Users\funt\.cargo\registry\
Mutex	Local\NVIDIAContainerMonitor_SingleInstance
URL	hxxps[:]//pipicka[.]xyz
IPv4	191[.]44[.]109[.]130, 87[.]120[.]108[.]18, 168[.]222[.]254[.]204

References

https://blackpointcyber.com/blog/labubarat-a-rust-based-remote-access-tool-masquerading-as-nvidia-software/

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 Demo of **HivePro**.

REPORT GENERATED ON

July 16, 2026 • 06:00 AM

More at www.hivepro.com