

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

NeedyMantis: The Patient Predator Hiding in Plain Sight

Date of Publication

September 30, 2026

Admiralty Code

A1

TA Number

TA2026288

Summary

First Seen: October 2025

Targeted Regions: Worldwide

Targeted Platform: Windows

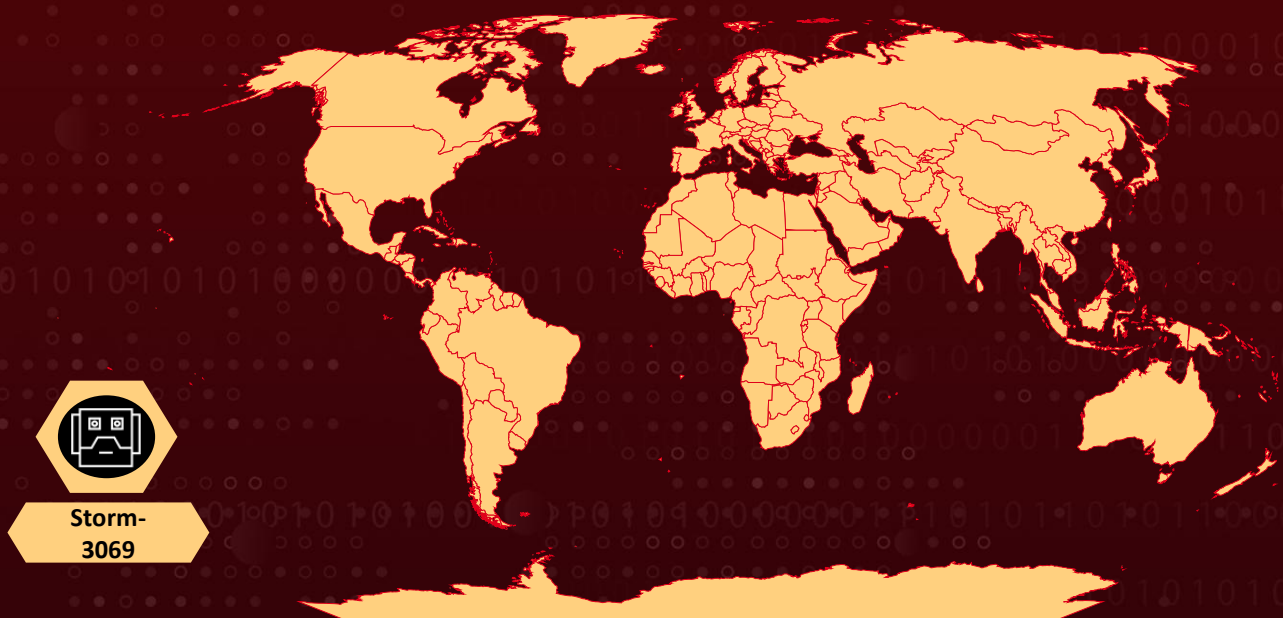
Targeted Industries: Telecommunications, Education, Healthcare, Nonprofits, Government

Threat Actor: Storm-3069

Malware: NeedyMantis

Attack: NeedyMantis is a modular, post-compromise backdoor used by the China-based actor Storm-3069 to maintain long-term access to already breached networks in telecommunications, education, healthcare, nonprofit, and government. It is delivered through DLL sideloading inside bundles of legitimate software such as Poedit, curl, Vim, and TightVNC, unpacks through layered loaders, custom encrypted archives, and a custom executable format, and then talks to its operators over HTTPS, which upgrades to an RC4-protected WebSockets channel through which new modules can be loaded on demand.

✂ Attack Regions



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

Targeted

Non-Targeted



THREAT ADVISORY • ATTACK REPORT (Red)

2

Hive Pro

Attack Details

#1

NeedyMantis is a stealthy modular malware used by Storm-3069, a China-based threat actor, to stay hidden inside networks it has already broken into. It is not used to break in. Instead, the attackers install it after they gain access so they can keep coming back, quietly watch the environment, and add new capabilities whenever they need them. Active since at least October 2025, with a newer version appearing in May 2026, it hides inside trusted software and talks to its operators through ordinary-looking web traffic, which makes it hard to spot.

#2

The malware was discovered during investigations into the DAEMON Tools supply chain compromise, but there is no evidence that NeedyMantis itself was spread through that incident. Storm-3069 has not been tied to any known Chinese state-sponsored group, and a possible link to UNC6863, a suspected China-nexus cluster behind the DAEMON Tools activity, remains unconfirmed.

#3

The attackers deliver NeedyMantis through DLL sideloading. They place a trusted program such as Poedit, curl, Vim, or TightVNC next to a malicious DLL named after a file that program expects to load, along with an encrypted archive. When the trusted program starts, it loads the malicious DLL without raising suspicion. To reach more machines, the operators used the Impacket toolkit to copy this bundle from a network share and run it on other devices.

#4

Once running, the malware unpacks itself in stages. The first loader checks whether it is being analyzed, then decrypts the archive, which mixes the real payload with harmless 7-Zip, Sysinternals, and Windows files to blend in. Inside is a second loader disguised as a PowerShell script that is actually shellcode, plus a configuration file and a communications module named after real Windows libraries. The final component is stored in a custom file format that standard analysis tools cannot easily read. An older version stayed on infected systems by installing itself as a Windows service.

#5

After setup, NeedyMantis contacts its command server over HTTPS using an outdated Firefox user agent and sends back a basic host profile: computer name, username, running processes, and the contents of the Program Files folder. The connection then switches to an encrypted WebSockets channel, through which operators can load or remove extra modules on demand.

Recommendations



Block the NeedyMantis C2 Host: Block and alert on outbound traffic to corp[.]tripswithengine[.]com at DNS, proxy, and firewall layers, and review historical DNS and proxy logs for prior connections to identify already compromised hosts.



Hunt for Sideloaded DLLs in Unusual Locations: Search endpoints for the listed loader paths and for WinSparkle.dll, libcurl.dll, vim64.dll, dbghelp.dll, jli.dll, and nvml.dll sitting beside Poedit, curl, Vim, or TightVNC binaries in ProgramData or other writable folders, and validate any copy that is unsigned, recently written, or accompanied by an unexplained archive file.



Validate Filename-Based Indicators Before Blocking: Several NeedyMantis components reuse names of legitimate Windows libraries such as dbghelp.dll, dnsapi.dll, and ws2_32.dll, so match on path, hash, and signer rather than filename alone to avoid disrupting legitimate software.



Detect the firefox/21.0 User-Agent and WebSockets Upgrades: Create network and proxy rules for the outdated firefox/21.0 User-Agent and for HTTPS sessions that upgrade to WebSockets from non-browser processes such as Poedit.exe, curl, Vim, or TightVNC.



Monitor for Impacket-Driven Lateral Tool Transfer: Alert on Impacket execution patterns and on legitimate application binaries, DLLs, and archive files being copied from network shares and executed on remote hosts, and restrict administrative share access to approved management systems.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	<u>T1129</u> : Shared Modules	
Persistence	<u>T1543</u> : Create or Modify System Process	<u>T1543.003</u> : Windows Service
Defense Evasion	<u>T1574</u> : Hijack Execution Flow	<u>T1574.002</u> : DLL
	<u>T1036</u> : Masquerading	<u>T1036.005</u> : Match Legitimate Resource Name or Location
		<u>T1036.008</u> : Masquerade File Type
	<u>T1027</u> : Obfuscated Files or Information	<u>T1027.013</u> : Encrypted/Encoded File
		<u>T1027.015</u> : Compression
		<u>T1027.007</u> : Dynamic API Resolution
	<u>T1140</u> : Deobfuscate/Decode Files or Information	
	<u>T1622</u> : Debugger Evasion	
Discovery	<u>T1082</u> : System Information Discovery	
	<u>T1033</u> : System Owner/User Discovery	
	<u>T1057</u> : Process Discovery	
	<u>T1083</u> : File and Directory Discovery	



Tactic	Technique	Sub-technique
Lateral Movement	<u>T1570</u> : Lateral Tool Transfer	
	<u>T1021</u> : Remote Services	<u>T1021.002</u> : SMB/Windows Admin Shares
Command and Control	<u>T1071</u> : Application Layer Protocol	<u>T1071.001</u> : Web Protocols
	<u>T1573</u> : Encrypted Channel	<u>T1573.001</u> : Symmetric Cryptography
	<u>T1132</u> : Data Encoding	<u>T1132.001</u> : Standard Encoding
	<u>T1105</u> : Ingress Tool Transfer	
Exfiltration	<u>T1041</u> : Exfiltration Over C2 Channel	

🔪 Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e842dd7642c8e04b5ec20b6393848a9c904e4832930950c16664fe7800ba382e, 9cb68f986043a576e19d32184c583b7d8f571c7219d8dc0065dced1c13f077ef, c82520eb03c084226be4eafbff46f56dca0aa8804a2a7f23a085a96afe71ef77
Domain	corp[.]tripswithengine[.]com
URL	hxxps[:]//corp[.]tripswithengine[.]com[:]443/library/zip/
Filename	WinSparkle.dll, libcurl.dll, vim64.dll, dbghelp.dll, jli.dll, nvml.dll, encryptbase64.ps1, msvcrt140.dll, 300.c, 300.s, m.l

TYPE	VALUE
File Path	%ProgramFiles%\Poedit\WinSparkle.dll, %ProgramData%\USOShared\libcurl.dll, %ProgramData%\VIM\vim64.dll, %ProgramData%\TightVNC\VIM\vim64.dll, %ProgramData%\office\dbghelp.dll, %ProgramData%\broadcom\dbghelp.dll, %ProgramData%\Intel\jli.dll, %ProgramFiles%\modifiable\nvml.dll, %ProgramData%\ics\nvml.dll



References

<https://www.microsoft.com/en-us/security/blog/2026/09/28/needymantis-unpacking-a-post-compromise-malware-family-used-in-targeted-operations/>



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

September 30, 2026 • 04:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com