

THREAT ADVISORY

NeedyMantis Malware: A New Threat Revealed



Services Performed By:

UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:

September 30, 2026

TLP:GREEN



Executive Snapshot

NeedyMantis is a modular post-compromise malware framework Microsoft disclosed on September 28, 2026. It was observed in targeted intrusions dating back to at least October 2025. It matters because of what it represents, not just what it does: a purpose-built tool used specifically after an attacker already has a foothold, designed to maintain long-term access and quietly extend an operator's capabilities through additional modules. The malware's architecture, built around custom encrypted archives, disguised file formats, and DLL sideloading into trusted software, is engineered specifically to resist analysis and blend into legitimate activity.

The malware's use has been tied to Storm-3069, the actor behind the DAEMON Tools supply-chain compromise, and observed activity aligns with patterns Microsoft associates with China-based threat actors (though full attribution to a single operator remains unconfirmed). Victims have spanned the telecommunication industry, universities, medical nonprofits, intergovernmental organizations, and government contractors. This indicates a selective targeting pattern consistent with deliberate intelligence-gathering rather than more simple criminal intent.

Priorities for detecting and deterring this threat:

- Monitor for DLL sideloading into known legitimate applications, particularly unexpected DLLs bundled alongside common open-source tools.
- Watch for outbound network connections using unusual or outdated user-agent strings inconsistent with the initiating application.
- Flag hands-on-keyboard activity involving credential and lateral-movement toolkits following any suspected initial compromise.
- Extend monitoring to post-compromise behavior, not just initial access, since this malware is deployed after a foothold already exists.



TIDE Team Analysis

NeedyMantis malware is best understood not as an initial-access tool, but as a persistence and follow-on capability deployed once an attacker is already inside a target environment. According to a recent Microsoft blog detailing the discovery, the malware was found while researchers were pivoting off indicators tied to a previously reported supply-chain compromise involving DAEMON Tools software. That investigative thread led Microsoft to identify a broader malware family with a distinct architecture and toolset, used by at least one actor Microsoft tracks as Storm-3069, and potentially by additional operators as well.

Microsoft has not formally attributed Storm-3069 to a specific nation-state but assesses that observed activity originates from China based on targeting patterns and operational characteristics consistent with other China-based actors. Identified victim organizations to date include telecommunications firms, medical nonprofits organizations, intergovernmental organizations, government contractors, and universities. This mix of targets points toward deliberate, selective targeting aligned with intelligence-collection interests rather than financially motivated crime. Microsoft has been careful to note that it hasn't confirmed whether every instance of NeedyMantis activity traces back to the same operator, leaving open the possibility that this tooling is shared or distributed among more than one group.

Since NeedyMantis is deployed post-compromise, initial access methods vary by intrusion; in one documented case, an operator used Impacket for hands-on-keyboard activity, transferring a legitimate application, a malicious loader DLL, and a companion archive from a network share onto the target. The malware depends heavily on DLL sideloading, masquerading as required components of trusted software, including translation tools, remote-access utilities, text editors, and files tied to recognizable technology brands.

Its execution unfolds in stages: an initial loader unpacks a custom-encrypted archive, which delivers a second loader that decodes a further-obfuscated core component. That component handles command-and-control communication over an encrypted WebSocket channel, layering encoding and encryption to mask its traffic. Rather than embedding every function upfront, it supports a narrow set of commands centered on loading and unloading modules, letting operators expand capability later in ways the base framework doesn't reveal. Obfuscated strings, disguised constants, and anti-debugging checks are woven throughout to resist analysis.

No single technique here is novel, but the combination, custom file formats, layered loaders, and modular extensibility, reflects meaningful engineering investment. Paired with narrow targeting of sensitive-sector victims and a clear preference for stealth over speed, NeedyMantis illustrates how state-linked actors are currently building tooling meant to persist quietly within high-value networks.

MALWARE PROFILE	
NeedyMantis	
Modular post-compromise backdoor framework	
ALSO No additional aliases publicly documented at this time	
OPERATORS	Storm-3069 (Microsoft designator; DAEMON Tools supply chain actor; China-based activity, unattributed to a specific nation-state sponsor)
ACTIVE SINCE	October 2025
FUNCTIONALITY	Backdoor Loader Post-Compromise Implant
TARGETING	Telecommunications organizations, universities, medical nonprofits, intergovernmental organizations, and government contractors
OBSERVED C2	corp.tripswithengine[.]com, contacted over an encrypted WebSocket-based channel.
NOTABLE TTPs	
01	DLL sideloading into legitimate open source and commercial software
02	Multi-stage loader chain combining native code and x64 shellcode
03	Custom encrypted and compressed file archive format for staging components
04	Obfuscated stack strings and constant values to hinder reverse engineering
05	Anti-debugging checks using process and thread level flags
06	WebSocket based command and control communications
07	RC4 encrypted C2 protocol with randomized key exchange
08	Modular design allowing operators to load and unload capability after deployment



Why It Matters

NeedyMantis matters to stakeholders first and foremost because of what its existence signals: a well-resourced actor investing specifically in the tooling used after a breach has already occurred, rather than in the breach itself. That distinction should reframe how organizations think about defense. Many security programs are weighted heavily toward preventing initial compromise (e.g., patching, phishing training, perimeter defenses) while investing comparatively less in detecting and disrupting what happens after an attacker is already inside. This malware is a direct illustration of why that imbalance is risky: even if every initial-access control works as intended most of the time, a single successful intrusion can be followed by tooling purpose-built to stay hidden and maintain access indefinitely.

The targeting pattern is also significant. Telecommunications providers, educational institutions, nonprofits, intergovernmental entities, and government contractors are not targets chosen at random; they represent sectors that either hold sensitive information directly or serve as connective infrastructure to organizations that do. Any organization operating in or adjacent to these sectors should treat this disclosure as a signal that selective, patient intrusion attempts are an active part of the current threat environment, not a hypothetical concern reserved for headline-grabbing breaches.

The malware's reliance on DLL sideloading into legitimate, often widely-trusted open-source software is a reminder that trust in a familiar application name or vendor isn't a substitute for verifying what's actually running in one's environment. Organizations that allow broad use of utility software without controls on what accompanies it may be creating exactly the kind of opportunity this malware is designed to exploit once an attacker gains a foothold.

There's also a discovery-and-disclosure dimension worth highlighting. This malware family was found not through a direct investigation of NeedyMantis itself, but by pivoting off indicators from an entirely separate, previously reported supply-chain compromise. That speaks to both the payoff of sustained threat-intelligence follow-up and an uncomfortable truth: tooling like this can go unnoticed indefinitely unless another investigation happens to surface a lead back to it, or defenders actively hunt for its specific signatures.

Finally, the malware's extensible, modular design means its full range of capability isn't entirely known. Stakeholders should treat this as an active, evolving threat rather than a fully characterized and closed case, and should expect follow-on reporting as additional modules or activity come to light.



How to Respond

- Monitor for DLL sideloading behavior, particularly unexpected or newly appearing DLLs bundled with legitimate open-source utilities, since this is the primary method NeedyMantis uses to gain execution.
- Lean into behavior-based detection capable of flagging obfuscated script execution and shellcode loading, since this malware's loaders rely heavily on obfuscation to evade static, signature-based detection.
- Extend monitoring and hunting efforts to post-compromise activity specifically, including hands-on-keyboard toolkits like Impacket, since this malware is deployed only after initial access has already been achieved.
- Enable endpoint detection and response in blocking mode alongside network protection features, so that malicious post-breach artifacts can be remediated even if an initial detection is missed elsewhere.
- Treat this malware as an evolving threat with unconfirmed full capability, and revisit detection and response planning as follow-on reporting on its modules and additional operators emerges.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity. UltraViolet is also maximizing detection coverage proactively through [Equinox](#).
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com |  UltraViolet Cyber |   @uv_cyber
