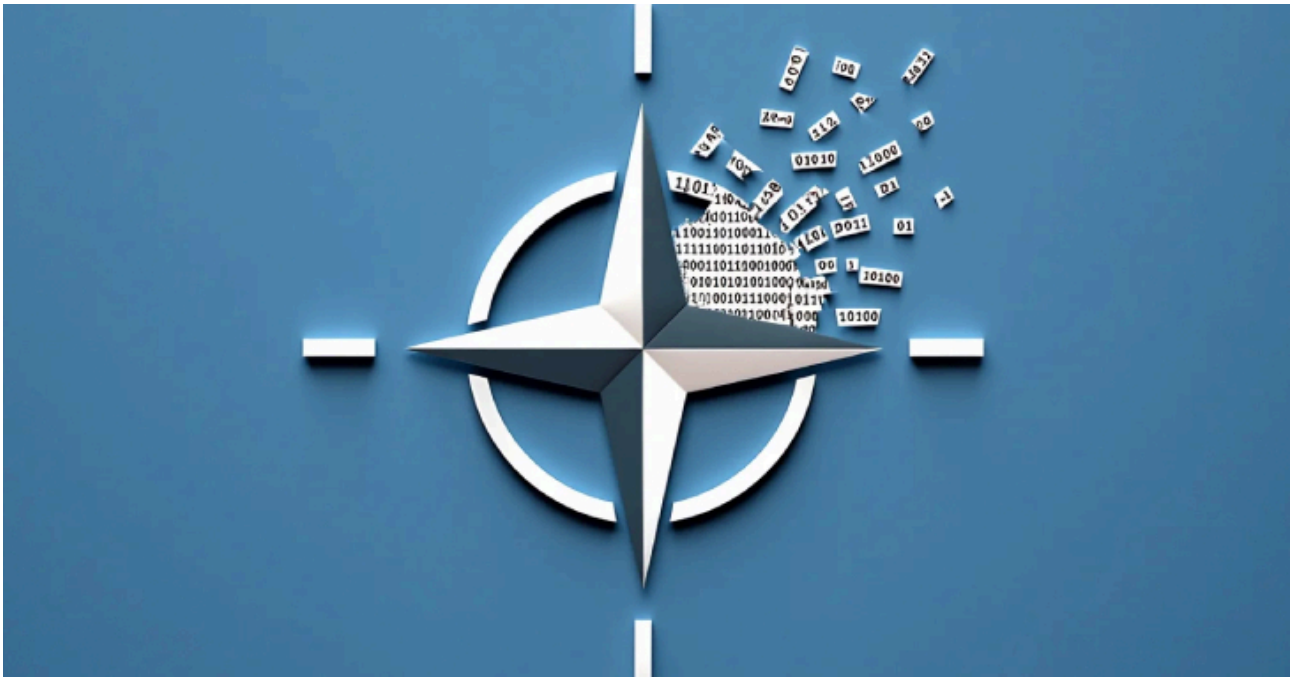
Nebulous Mantis Targets NATO-Linked Entities with Multi-Stage Malware Attacks

By The Hacker News

Published: 2025-04-30 · Archived: 2026-04-05 19:48:59 UTC



Cybersecurity researchers have shed light on a Russian-speaking cyber espionage group called Nebulous Mantis that has deployed a remote access trojan known as RomCom RAT since mid-2022.

RomCom "employs advanced evasion techniques, including living-off-the-land (LOTL) tactics and encrypted command and control (C2) communications, while continuously evolving its infrastructure – leveraging bulletproof hosting to maintain persistence and evade detection," Swiss cybersecurity company PRODAFT said in a report shared with The Hacker News.

Nebulous Mantis, also tracked by the cybersecurity community under the names CIGAR, Cuba, Storm-0978, Tropical Scorpius, UAC-0180, UNC2596, and Void Rabisu, is known to target critical infrastructure, government agencies, political leaders, and NATO-related defense organizations.

Attack chains mounted by the group typically involve the use of spear-phishing emails with weaponized document links to distribute RomCom RAT. The domains and command-and-control (C2) servers used in these campaigns

have been hosted on bulletproof hosting (BPH) services like LuxHost and Aeza. The infrastructure is managed and procured by a threat actor named LARVA-290.

The threat actor is assessed to be active since at least mid-2019, with earlier iterations of the campaign delivering a malware loader codenamed Hancitor.

The first-stage RomCom DLL is designed to connect to a C2 server and download additional payloads using the InterPlanetary File System (IPFS) hosted on attacker-controlled domains, execute commands on the infected host, and execute the final-stage C++ malware.

The final variant also establishes communications with the C2 server to run commands, as well as download and execute more modules that can steal web browser data.

"The threat actor executes tzutil command to identify the system's configured time zone," PRODAFT said. "This system information discovery reveals geographic and operational context that can be used to align attack activities with victim working hours or to evade certain time-based security controls."

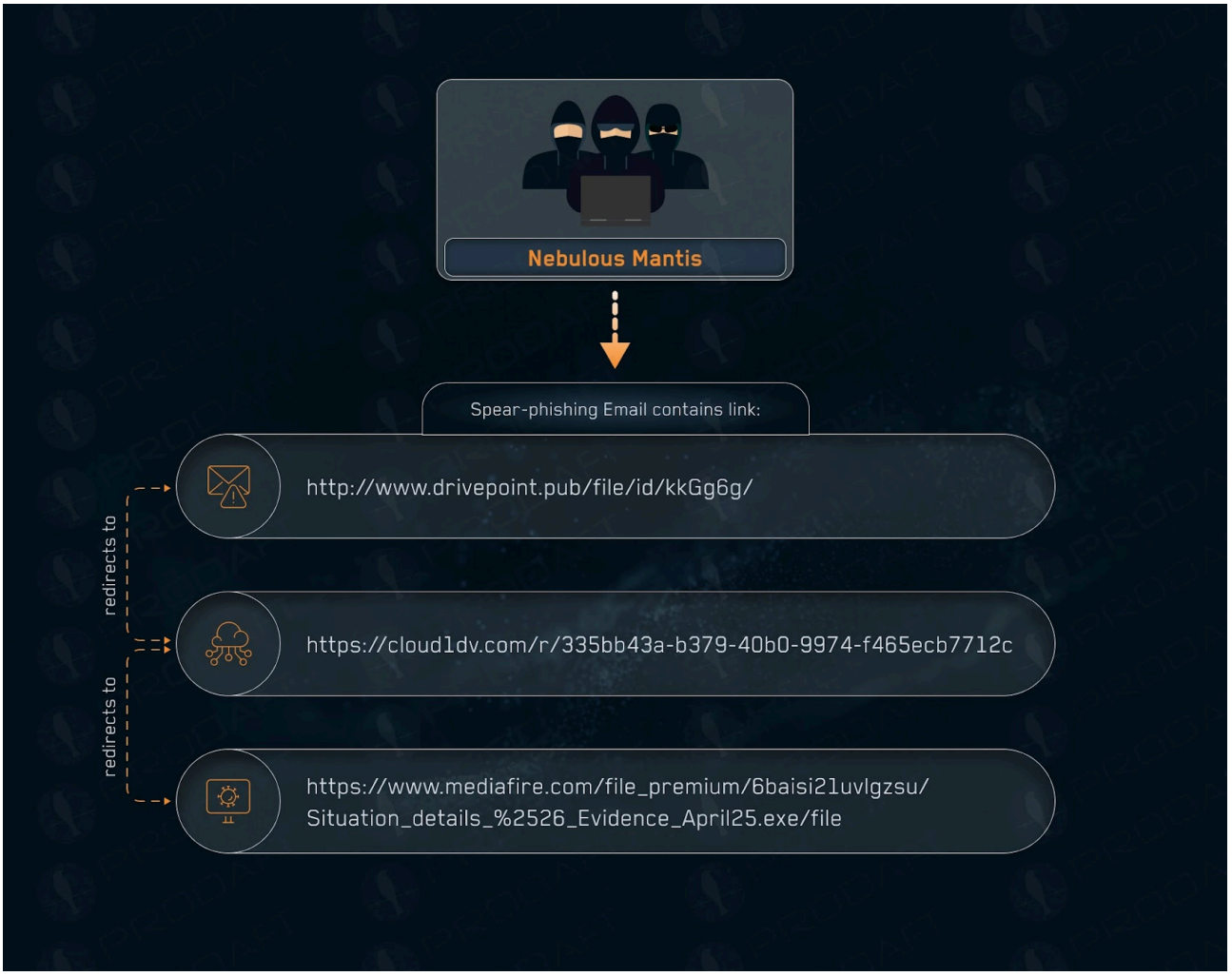
RomCom, besides manipulating Windows Registry to set up persistence using COM hijacking, is equipped to harvest credentials, perform system reconnaissance, enumerate Active Directory, conduct lateral movement, and collect data of interest, including files, credentials, configuration details, and Microsoft Outlook backups.

RomCom variants and victims are managed by means of a dedicated C2 panel, allowing the operators to view device details and issue over 40 commands remotely to carry out a variety of data-gathering tasks.

"Nebulous Mantis operates as a sophisticated threat group employing a multi-phase intrusion methodology to gain initial access, execution, persistence, and data exfiltration," the company said.

"Throughout the attack lifecycle, Nebulous Mantis exhibits operational discipline in minimizing their footprint, carefully balancing aggressive intelligence collection with stealth requirements, suggesting either state-sponsored backing or professional cybercriminal organization with significant resources."

The disclosure comes weeks after PRODAFT exposed a ransomware group named Ruthless Mantis (aka PTI-288) that specializes in double extortion by collaborating with affiliate programs, such as Ragnar Locker, INC Ransom, and others.



Led by a threat actor dubbed LARVA-127, the financially motivated threat actor utilizes an array of legitimate and custom tools to facilitate each and every phase of the attack cycle: discovery, persistence, privilege escalation, defense evasion, credential harvesting, lateral movement, and C2 frameworks like Brute Ratel c4 and Ragnar Loader.

"Although Ruthless Mantis is composed of highly experienced core members, they also actively integrate newcomers to continually enhance the effectiveness and speed of their operations," it said.

"Ruthless Mantis has significantly expanded its arsenal of tools and methods, providing them with state-of-the-art resources to streamline processes and boost operational efficiency."

RomCom Campaign Targets U.K. Orgs

U.K.-based cybersecurity company Bridewell said it discovered a new campaign orchestrated by the RomCom threat actor that involved using externally facing customer feedback portals to submit phishing emails to two of its customers in the retail and hospitality, and CNI sectors.

"Contained within the feedback forms were user complaints pertaining to events facilities operated by the target or recruitment enquiries, including links to further information supporting the complaints stored on Google Drive and Microsoft OneDrive impersonation domains hosted threat actor-controlled VPS infrastructure," researchers Joshua Penny and Yashraj Solanki said.

The campaign, codenamed Operation Deceptive Prospect, is said to have been ongoing since 2024, with the attack chain leading to the deployment of an executable downloader masquerading as a PDF document.

"The name of the signature further supports our hypothesis that there is technical overlap with RomCom from a tooling perspective as well," the researchers added.

Source: https://thehackernews.com/2025/04/nebulous-mantis-targets-nato-linked.html