LOGPOINT

Detecting ‘LameHug’ malware

Jul 31, 2025 13:00 CEST

Logpoint releases detection advisory for the AI-powered ‘LameHug’ malware

LaneHug doesn’t follow a script. It asks a Large Language Model (LLM) how to attack and adapts in real time. Logpoint releases capabilities to help SOC teams detect the new threat.

Copenhagen, July 31, 2025 – For the first time, malware based on artificial intelligence (AI) has been used in a live cyberattack attributed to APT28: LameHug. The Ukrainian CERT (CERT-UA) uncovered this development.

Logpoint's security researchers have now published a technical assessment of the malware to give SOC teams the actionable insights necessary to detect the new threat.

LameHug isn't the typical malware with hardcoded commands. It prompts a large language model (LLM) to assess the victim's network and then construct attack strategies to increase the damage inflicted. Logpoint encourages Critical National Infrastructure (CNI) and Managed Security Service Providers (MSSPs) to be alert as the expectation is that APT28 will expand the use of AI-enabled attacks and others will follow.

"We're entering a new era of cyber threats. LameHug doesn't follow predefined instructions, it asks an LLM how to attack in the most efficient way based on the victims' systems. It's getting cheaper and quicker to generate bespoke payloads and carry out targeted attacks," says Christian Have, CTO at Logpoint. "To keep up we must reconsider how we detect, respond, and defend. AI can't just be part of the problem. It must be part of the solution."

At the heart of LameHug is a link to Qwen 2.5-Coder-32B-Instruct via the Hugging Face API. Once it infects a system, it uses natural language prompts to generate Windows commands, automating system reconnaissance and exfiltrating documents over SFTP or HTTP POST. It's adaptive. It's quiet. And it's real.

Two additional variants, AI_generator_uncensored_Canvas_PRO_v0.9.exe and image.py, have been spotted in the wild. Each one tailored to achieve the same goal: get in, steal data, and get out smarter and faster.

CERT-UA's report notes the malware arrived via a phishing email, impersonating a Ukrainian government official. The attached ZIP contained a Python-based executable created with PyInstaller, later classified as LameHug. It's a blend of the familiar and the cutting edge and that's what makes it so dangerous.

"AI innovation accelerates in the ransomware economy. We expect AI to schedule phishing, negotiate ransom payments, and deploy on-device tiny-LLMs that never touch the cloud," says Have. "Defenders will have to detect "prompt packs" instead of malware, which means that signals will be weak. As defenders we can use LLMs to connect the dots and find intent in

signals that look harmless on their own. They will help us see the sequence behind an attack as it unfolds."

Novel strategies necessitate modern approaches to defense. To help SOC teams meet this new class of threat, Logpoint is releasing the following capabilities:

- Threat hunting queries based on known indicators of compromise (IoCs), and tactics, techniques and procedures (TTPs)
- Detection logic and log sources to uncover suspicious API activity
- SOAR playbooks to automate containment, investigation, and remediation

All available on Logpoint's platform.

Read the full advisory from Logpoint here.

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's SIEM and NDR technologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98