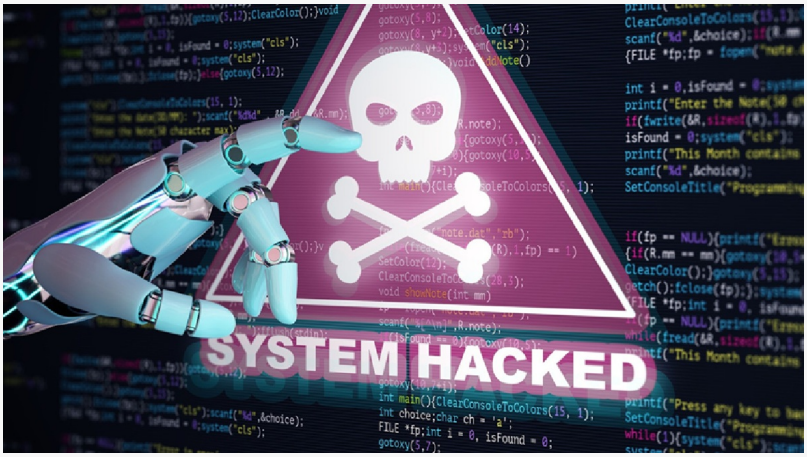
ESET discovers PromptLock, the first AI-powered ransomware

DUBAI , DUBAI, UNITED ARAB EMIRATES, August 29, 2025 /EINPresswire.com/ -- ESET researchers have uncovered a new type of ransomware that leverages generative artificial intelligence (GenAI) to execute attacks. Named PromptLock, the malware runs a locally accessible AI language model to generate malicious scripts in real time. During infection, the AI autonomously decides which files to search, copy, or encrypt — marking a potential turning point in how cybercriminals operate.



“The emergence of tools like PromptLock highlights a significant shift in the cyber threat landscape,” said Anton Cherepanov, senior malware researcher at ESET, who analyzed the malware alongside fellow researcher Peter Strýček.

PromptLock creates Lua scripts that are compatible across platforms, including Windows, Linux, and macOS. It scans local files, analyzes their content, and — based on predefined text prompts — determines whether to exfiltrate or encrypt the data. A destructive function is already embedded in the code, though it remains inactive for now.

The ransomware uses the SPECK 128-bit encryption algorithm and is written in Golang. Early variants have already surfaced on the malware analysis platform VirusTotal. While ESET considers PromptLock a proof of concept, the threat it represents is very real.

“With the help of AI, launching sophisticated attacks has become dramatically easier — eliminating the need for teams of skilled developers,” added Cherepanov. “A well-configured AI model is now enough to create complex, self-adapting malware. If properly implemented, such threats could severely complicate detection and make the work of cybersecurity defenders considerably more challenging.”

PromptLock uses a freely available language model accessed via an API, meaning the generated malicious scripts are served directly to the infected device. Notably, the prompt includes a Bitcoin address reportedly linked to Bitcoin creator Satoshi Nakamoto.

ESET has published technical details to raise awareness within the cybersecurity community. The malware has been classified as Filecoder.PromptLock.A.

Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here