ESET odhalil PromptLock, první ransomware poháněný umělou inteligencí

28.8.2025 - Lucie Mudráková | ESET software

Bezpečnostní experti společnosti ESET odhalili nový typ ransomwaru, který k útokům využívá generativní umělou inteligenci. Malware s názvem PromptLock dokáže lokálně spustit dostupný AI jazykový model, který v reálném čase generuje škodlivé skripty. Během útoku pak AI na základě promptu rozhoduje, které soubory vyhledat, zkopírovat, zašifrovat nebo nenávratně zničit. Aktuální odhalení může znamenat zásadní změnu v tom, jak kyberzločinci útočí.

„Vznik nástrojů jako PromptLock představuje významný posun v oblasti kybernetických hrozeb," uvedl Anton Cherepanov, seniorní expert na výzkum malwaru ve společnosti ESET, který jej analyzoval společně s kolegou Peterem Strýčkem.

Malware PromptLock vytváří skripty v programovacím jazyce Lua, které jsou kompatibilní napříč operačními systémy, včetně Windows, Linuxu a macOS. Prohledává lokální soubory, analyzuje jejich obsah a na základě předdefinovaných textových „promptů" rozhoduje, zda data exfiltrovat nebo zašifrovat. V kódu je již obsažena také destruktivní funkce ke zničení dat, zatím ale zůstává neaktivní.

Ransomware využívá šifrovací algoritmus SPECK s 128bitovým klíčem a je napsán v jazyce Golang. Jeho první varianty se již objevily na platformě VirusTotal určené k analýze škodlivých kódů. Přestože ESET považuje PromptLock za první funkční ukázku (tzv. proof of concept), hrozba, kterou představuje, je velmi reálná.

„Doposud byl s AI spojován ransomwarový gang FunkSec, který se netajil tím, že využívá AI při vývoji. PromptLock posouvá integraci AI mnohem dále, a škodlivý kód generuje automaticky v průběhu útoku, což představuje zásadní změnu v principu využívání AI. Generovaný kód může být například obtížnější odhalit. Jelikož se zatím jedná spíše o funkční ukázku, bude zajímavé sledovat, jestli se některá z aktivních ransomware skupin rozhodne podobný postup aplikovat," doplňuje Jakub Souček, vedoucí výzkumného týmu v pražské pobočce společnosti ESET.

Ransomware PromptLock využívá volně dostupný jazykový model přístupný přes API, což znamená, že generované škodlivé skripty jsou přímo doručovány na napadené zařízení. Zajímavostí je, že prompt obsahuje bitcoinovou adresu údajně spojenou s tvůrcem Bitcoinu, Satoshim Nakamotem.

Společnost ESET zveřejnila technické detaily z výzkumu tohoto malwaru, aby zvýšila povědomí o této hrozbě v kyberbezpečnostní komunitě. Malware byl klasifikován pod označením Filecoder.PromptLock.A.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-odhalil-promptlock-prvni-ransomware-pohaneny-umelou-inteligenci