ESET odhalil PromptSpy, první hrozbu pro platformu Android využívající generativní AI

23.2.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

PromptSpy je první známý škodlivý kód pro platformu Android, který během útoku využívá generativní AI.

- Útočníci využívají model Google Gemini k interpretaci prvků na obrazovce napadeného zařízení a k tomu, aby dával dynamické pokyny malwaru PromptSpy jak provést za uživatele konkrétní gesto, aby zůstal v seznamu nedávných aplikací.
- Hlavním cílem PromptSpy (již bez asistence generativní AI) je nasadit modul Virtual Network Computing (VNC) na zařízení oběti, což útočníkům umožní vidět její obrazovku a provádět akce na dálku.
- PromptSpy dokáže zachytit data z uzamčené obrazovky, blokovat odinstalování, shromažďovat informace o zařízení, pořizovat snímky obrazovky, nahrávat aktivitu obrazovky jako video atd.

Kyberbezpečnostní specialisté společnosti ESET objevili PromptSpy, první známý malware pro platformu Android, který zneužívá generativní AI k tomu, aby zůstal v napadeném zařízení trvale přítomný. Je to vůbec poprvé, co byla generativní umělá inteligence použitá tímto způsobem. Protože se útočníci spoléhají na to, že pomocí promptování AI modelu (konkrétně Google Gemini) zmanipulují uživatelské rozhraní, pojmenovala společnost ESET tuto malware rodinu PromptSpy. Škodlivý kód dokáže zachytit data z uzamčené obrazovky, blokovat pokusy o odinstalování, shromažďovat informace o zařízení, pořizovat snímky obrazovky, nahrávat aktivitu obrazovky v podobě videa atd. Po malwaru PromptLock, který jako první známý případ ransomwaru poháněného AI odhalili experti z ESETu v srpnu 2025, se jedná o jejich druhý objev škodlivého kódu, který využívá v útocích umělou inteligenci.

Na základě stop, které souvisejí se zvolenou jazykovou lokalizací a distribučními vektory pozorovanými během analýzy, se zdá, že jde o finančně motivovanou kampaň a primárně cílí na uživatele v Argentině. Malware PromptSpy však dosud nebyl zachycen v telemetrii společnosti ESET, a je možné, že se jedná o tzv. proof of concept.

„Malware pro platformu Android často spoléhá na navigaci založenou na uživatelském rozhraní. Využití generativní AI tak útočníkům umožňuje přizpůsobit se prakticky jakémukoli zařízení, rozvržení nebo verzi operačního systému. To může výrazně rozšířit množinu potenciálních obětí," říká Lukáš Štefanko, bezpečnostní expert společnosti ESET, který PromptSpy objevil. „Hlavním účelem malwaru PromptSpy je nasadit vestavěný modul VNC, který operátorům poskytne vzdálený přístup k zařízení oběti. Tento škodlivý kód pro platformu Android také zneužívá Služby usnadnění k blokování odinstalace, a to překrytím této možnosti neviditelnými prvky. Dokáže také zachytit data z uzamčené obrazovky a nahrát aktivitu obrazovky jako video. Se svým řídícím serverem komunikuje pomocí šifrování AES," dodává Štefanko.

Role Google Gemini

Ačkoli je generativní AI využitá jen v poměrně malé části kódu PromptSpy — v té, která je zodpovědná za dosažení odolnosti proti vypnutí — přesto má významný dopad na přizpůsobivost škodlivého kódu. Model Gemini je konkrétně využíván k poskytování podrobných instrukcí, jak škodlivou aplikaci „uzamknout" nebo tj. připnout v seznamu nedávných aplikací (často je to znázorněno ikonou visacího zámku v seznamu). Tím se zabrání jejímu snadnému vypnutí. AI model a

prompt jsou předdefinovány v kódu a nelze je měnit.

Malware PromptSpy se šíří jako aplikace prostřednictvím k tomu určené webové stránky a nikdy nebyl dostupný v obchodě Google Play. Společnost ESET jako partner App Defense Alliance přesto sdílela zjištění se společností Google. Uživatelé platformy Android jsou proti známým verzím tohoto malwaru automaticky chráněni díky službě Google Play Protect, která je ve výchozím nastavení povolena na zařízeních s Google Play Services.

„I když PromptSpy používá Gemini jen v jedné ze svých funkcí, stále to ukazuje, jak může implementace těchto nástrojů pomoct škodlivému kódu, aby byl dynamičtější, a útočníkům umožnit automatizovat akce, které by byly tradičními skripty obtížně proveditelné," říká Štefanko z ESETu.

Vzhledem k tomu, že název škodlivé aplikace je MorganArg a její ikona je zjevně inspirována bankou Morgan Chase, malware se nejspíše vydává za tuto instituci. MorganArg, pravděpodobně zkratka pro „Morgan Argentina", se také objevuje jako název webové stránky zachycené v mezipaměti (cache) vyhledávače Google. To naznačuje, že je malware zacílen regionálně.

Protože PromptSpy blokuje odinstalaci tím, že tuto možnost na obrazovce překryje neviditelnými prvky, jediný způsob, jak jej oběť může odstranit, je restartovat zařízení do nouzového režimu (Safe Mode), kde jsou aplikace třetích stran deaktivovány a lze je normálně odinstalovat. Pro vstup do nouzového režimu by uživatelé obvykle měli stisknout a podržet tlačítko napájení, dlouze podržet možnost Vypnout a potvrdit výzvu k restartu do nouzového režimu (přesný postup se může lišit podle zařízení a výrobce). Jakmile se telefon restartuje v nouzovém režimu, může uživatel přejít do Nastavení → Aplikace → MorganArg a odinstalovat jej.

Více informací

Podrobnější analýzu malwaru PromptSpy si můžete přečíst v nejnovějším článku na odborném webu WeLiveSecurity.com.

O společnosti ESET

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-promptspy-prvni-hrozbu-pro-platformu-android-vyuzivajici-generativni-ai