ESET: Škodlivá reklama už jim nestačí, útočníkům v honbě za našimi daty z telefonů pomáhá spyware

20.1.2026 - | ESET software

Dlouhodobě převládající riziko v podobě adwaru je v případě platformy Android v Evropě již několikátým měsícem na ústupu. I prosinec loňského roku potvrdil tento trend – v čele pravidelné statistiky se totiž umístil nový typ škodlivého kódu s funkcemi spywaru, a to dokonce v pětině všech zachycených případů. Útočníci tento malware šířili plošně přes velké množství škodlivých aplikací, přičemž zneužívali hlavně jména známých streamovacích platforem. Dokázali ale škodlivý kód přidat i do legitimní aplikace pro stahování videí z internetu, a to bez vědomí jejího vývojáře. Bezpečnostní experti tak ve svém výhledu pro rok 2026 varují nejen před známými hrozbami jako jsou falešné hry ukrývající adware, ale i před zcela novými případy pokročilejšího škodlivého kódu. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Špionážní škodlivý kód, který bezpečnostní experti označují jako Agent.FNM, je nový typ malwaru, který sbírá informace o napadeném mobilním telefonu. Útočníci jeho prostřednictvím dokážou zjistit například výrobce a model zařízení, IP adresu, operátora nebo jaký typ internetového připojení využíváme. Získaná data pak mohou prodávat na černém trhu nebo využívat k přípravě dalších útoků.

„Kromě toho, že tento špionážní škodlivý kód získává informace o uživatelích, dokáže například také zpomalit internet na napadeném zařízení, a to na základě sledování, jak se na internetu chováme. Útočníci jej v prosinci šířili ve falešných verzích celé řady populárních streamovacích aplikací – jmenovat můžeme Netflix, Spotify či Amazon Prime. Objevili jsme ale také škodlivou aplikaci WhatsApp či VPN zdarma," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Ačkoli se tento spyware vyskytoval především ve Španělsku a Nizozemsku, případy jsme zachytili i v Česku. Varováním by měl být proto široký záběr útočníků napříč zeměmi a fakt, že už jen v průběhu prosince se škodlivý kód několikrát vyvíjel. Vypadá to, že tu máme nový typ hrozby, který rozhodně budeme nadále sledovat. Jak totiž ukázaly uplynulé měsíce v závěru roku 2025, škodlivé mobilní hry ustoupily do pozadí a útočníci sahají i po malwaru, který známe spíše z prostředí osobních počítačů. To jen poukazuje na důležitost ochrany našich dat i v mobilních zařízeních," dodává Jirkal.

Bezpečnostní experti vždy opakují důležitost stahování mobilních aplikací z prověřených zdrojů. Nejrizikovější jsou z tohoto pohledu méně známé obchody třetích stran nebo různá internetová fóra a úložiště. Doporučují proto spoléhat se především na obchod s aplikacemi pro platformu Android, Google Play. Neopomínají nicméně zdůraznit, že i legitimní aplikace se mohou stát obětí útočníků.

„K vyššímu prosincovému číslu detekcí malwaru Agent.FNM přispěl bohužel případ, kdy se útočníkům podařilo infikovat oficiální aplikaci SmartTube. Bez vědomí vývojáře zkrátka přidali škodlivý kód k jeho kódu. I když je již aplikace v oficiálních obchodech v pořádku, přesto se tyto případy mohou objevovat. Zde doporučuji věnovat chvilku času uživatelským recenzím. Špatnou zkušenost si ostatní většinou pro sebe nenechají. Projít je by měla být taková povinná rutina vždy, když si chceme nějakou novou aplikaci stáhnout. Bezpečnost uživatelé a uživatelky samozřejmě podpoří i profesionálním kyberbezpečnostním softwarem, který na nebezpečnou aplikaci vždy včas upozorní," říká Martin Jirkal.

Pokud je z pohledu kybernetických hrozeb něčím platforma Android specifická, tak je to vysoká proměnlivost škodlivých kódů v čase. Aplikace od různých vývojářů a široká skupina uživatelů od nejmenších dětí po seniory z ní dělá atraktivní cíl kybernetických útoků. Podle bezpečnostních expertů se tak i v následujícím roce budeme setkávat například s adwarem, škodlivou reklamou přítomnou i v České republice, tak s vysoce sofistikovanými škodlivými kódy, které mohou být součástí větších útoků organizovaných skupin. Takovým příkladem může být malware Ngate, pomocí kterého útočníci dokázali během loňských útoků zneužít technologii NFC k přenosu dat z platebních karet svých obětí. Malware šířili ve falešné aplikaci ČNB.

„Vyloučit letos bohužel nemůžeme ani zapojení AI – jak do přípravy útoků, tak do jejich průběhu. Existují již náznaky, že velké jazykové modely pomáhají generovat škodlivý kód, což snižuje vstupní bariéru pro kyberzločince, kteří nemají takové zkušenosti a vědomosti, aby útok sami připravili," dodává Jirkal z ESETu.

Uživatelé řešení ESET jsou před výše uvedenými typy hrozeb automaticky chráněni.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení digitální 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-skodliva-reklama-uz-jim-nestaci-utocnikum-v-honbe-za-nasimi-daty-z-telefonu-pomaha-spyware