

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **134** ze dne **24.2.2026**

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

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 uživateli, 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.

Mobilní hrozby v roce 2026

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.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **134** ze dne **24.2.2026**

"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.

Nejčastější kybernetické hrozby pro platformu Android v zemích EU za prosinec 2025:

1. Android/Agent.FNM trojan (19,66 %)
2. Android/Andreed trojan (2,74 %)
3. Android/Hiddad.BDE trojan (2,51 %)
4. Android/Spy.SpinOk trojan (2,12 %)
5. Android/Agent.EQD trojan (1,89 %)
6. Android/Agent.FNS trojan (1,85 %)
7. Android/TrojanDropper.Agent.GKE trojan (1,84 %)
8. Android/TrojanDropper.Agent.MLG trojan (1,57 %)
9. Android/Agent.FJL trojan (1,48 %)
10. Android/Spy.Banker.BGB trojan (1,46 %)

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

AV centrum ČR