ESET: Špionážní malware v lednu ztrácel na škodlivou reklamu, ta zamířila hlavně do Česka a Polska

18.2.2026 - | ESET software

Poté, co byl na konci loňského roku největším rizikem špionážní škodlivý kód Agent.FNM, se v lednu na platformu Android vrátil ve velkém reklamní malware – trojský kůň Hiddad. V kontextu všech zachycených kybernetických hrozeb se objevil v pětině všech případů. V lednu s ním navíc útočníci zamířili nejčastěji na Českou republiku a Polsko. Ani malware Agent.FNM však zatím není minulostí. Objevoval se konzistentně během celého uplynulého měsíce. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Platforma Android v lednu opět potvrdila svou pověstnou proměnlivost v otázce kybernetických rizik. Zatímco ještě na konci roku převládal v Evropě špionážní škodlivý kód Agent.FNM, už v lednu ho opět vystřídal reklamní malware. V pětině všech zachycených škodlivých kódů se tentokrát totiž objevil trojský kůň Hiddad, který zobrazuje agresivní reklamu, skrývá se v zařízení a dokáže stahovat další hrozby. Jeho hlavním cílem bylo v lednu Polsko a Česká republika.

„Jak můžeme vidět z naší poslední analýzy, poté, co útočníci na konci loňského roku vyzkoušeli na platformě Android nový špionážní malware, se už v lednu opět vrátili k reklamnímu škodlivému kódu. Není to ale tentokrát starý známý adware Andreed. V lednu totiž poměrně znatelně stoupl počet případů trojského koně Hiddad," shrnuje aktuální situaci na platformě Android Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Adware neboli reklamní malware ke svému šíření využívá širokou paletu falešných verzí mobilních aplikací a her. Trojský kůň Hiddad se v lednu nejvíce skrýval ve škodlivých verzích hry Shadow Fight 2 a v nástrojích k editování videa či obrázků.

„Malware rodina Hiddad se kromě zobrazování agresivní reklamy vyznačuje ještě dalšími funkcemi, které by pro nás měly být varováním. Tento škodlivý kód se dokáže v systému Android dobře skrývat a není ho snadné odhalit. Ukrytý tak dokáže dělat škody dlouhou dobu. Umí sbírat informace o našem chování na internetu a o našem telefonu. Zároveň do zařízení stahuje další malware podle preferencí útočníka. Rozhodně tedy neplatí, že reklamní škodlivý kód představuje menší nebezpečí, jak by se někdo mohl mylně domnívat," vysvětluje Jirkal.

To, zda bude adware nadále přední hrozbou na platformě Android, se podle bezpečnostních expertů teprve ukáže. Špionážní malware Agent.FNM byl v lednu druhým nejčastějším rizikem, a to konzistentně po celý sledovaný měsíc. Jeho cílovou stanicí byla tentokrát spíše západní část Evropy, v jednotkách procent se objevil ale i v Česku. S ohledem na tento malware a potenciální rizika trojského koně Hiddad doporučují stahovat aplikace a hry pouze z oficiálního obchodu Google Play a zvážit pořízení moderního bezpečnostní softwaru.

V jednotkách procent případů zachytili bezpečnostní experti v lednu také škodlivý kód v mobilní aplikaci pro správu IP kamery. Podle jejich analýzy se sice jednalo o neznámého výrobce, aplikace byla nicméně dostupná v legitimních obchodech. Nejvíce případů se opět objevilo v Polsku a České republice. V tuto chvíli se však podle všeho podařilo výrobci incident již napravit.

„Podle dat, které se nám podařilo k tomuto případu získat, se jednalo o škodlivý kód, který do zařízení stahoval další škodlivý obsah. Útok nicméně trval jen pár dní a zdá se, že výrobci se podařilo vše napravit. Situaci však nadále sledujeme. Rád bych zde poukázal ještě na jeden rozměr kyberhrozeb v případě platformy Android, a to jsou nekvalitní výrobky od neznámých značek s připojením k internetu. Pokud je škodlivý kód původem z legitimní aplikace výrobce, svědčí to o tom, že má velmi slabé zabezpečení. Obecně bych proto doporučoval nepořizovat si zařízení neznámých značek, i když by to znamenalo úsporu peněz – v konečném důsledku to za to nestojí," dodává Jirkal z ESETu.

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

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-spionazni-malware-v-lednu-ztracel-na-skodlivou-reklamu-ta-zamirila-hlavne-do-ceska-a-polska