ESET: Útočníci se v listopadu na platformě Android zaměřili na bankovní účty, riziko se týkalo i Česka

19.12.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastěji detekovaným škodlivým kódem pro platformu Android v zemích EU byl v listopadu opět špionážní malware Spy.Banker.DOK. Do popředí se dostal tentokrát již druhým měsícem v řadě a útočníci jej opět ukryli pod falešnou verzi aktualizace prohlížeče Chrome. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Zatímco Spy.Banker.DOK má funkce špionážního malwaru a může být rizikem pro bankovní aplikace, další z listopadových hrozeb, bankovní trojský kůň Mamont, se zaměřuje přímo na krádež přihlašovacích údajů do bankovnictví. V pěti procentech případů byla v listopadu jeho cílem dokonce i Česká republika. Dvojici škodlivých kódů pak doplnil již tradičně před svátky adware Andreed, standardně maskovaný za populární mobilní hry.

Špionážní malware Spy.Banker.DOK zůstal oblíbenou zbraní kybernetických útočníků již druhým měsícem. Případy tohoto škodlivého kódu kontinuálně rostly až do 16. listopadu. Útočníci jej opět šířili v tzv. dropperech, což jsou také škodlivé kódy, které využívají jako doručovací obálky. Hlavní malware je pak těžší odhalit.

„Již před měsícem jsme varovali před nebezpečnou verzí aktualizace pro prohlížeč Chrome, a také v listopadu využili útočníci tuto zástěrku k tomu, aby skryli malware Spy.Banker.DOK a my si ho nepozorovaně stáhli do zařízení," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „V tomto případě bylo hlavním cílem útočníků v listopadu Španělsko. Vzorky malwaru jsme ale prakticky pozorovali po celém evropském prostoru. Jako špionážní malware má Spy.Banker.DOK řadu charakteristických vlastností, o kterých by měli uživatelé a uživatelky vědět: dokáže číst SMS zprávy či je dokonce posílat, nahrávat hovory nebo pořizovat fotografie. Jakmile se dostane do telefonu, získá také plný přístup k našim souborům. Může dokonce instalovat bez našeho vědomí další aplikace a nahrávat uživatelskou obrazovku. Rizikem může být především pro bankovní aplikace," dodává Jirkal.

V listopadu se do popředí pravidelné statistiky vrátil adware Andreed. Kyberbezpečnostní experti na něj pravidelně upozorňují v souvislosti s prázdninami a svátky. Útočníci jej šíří především prostřednictvím různých mobilních her a z této podstaty jsou jeho cílem uživatelé a uživatelky všech věkových kategorií.

„V listopadu jsme nejvíce případů adwaru Andreed zachytili v Nizozemsku, České republice a Německu. Více zastoupený je ale také například v Polsku," vysvětluje Jirkal. „Zajímavostí tohoto škodlivého kódu je to, že jej většina uživatelů a uživatelek ani nepovažuje za škodlivý. Adware má většinou negativní vliv hlavně na výkon zařízení a obtěžuje nás agresivními vyskakujícími okny. Co možná ale někteří uživatelé a uživatelky nevědí, je to, že některé typy adwaru dokážou sledovat naši činnost při prohlížení internetu a sekundárně stahovat daleko závažnější škodlivé kódy," varuje Jirkal.

Adware Andreed útočníci v listopadu schovávali pod falešné verze her GTA San Andreas a Survival: Across The Ocean.

Třetím nejčastějším škodlivým kódem byl v listopadu dropper Agent.NAV. Útočníci jeho prostřednictvím šířili bankovního trojského koně Mamont. Nejvíce v ohrožení byli v listopadu uživatelé a uživatelky v Německu, Itálii a Španělsku, v pěti procentech všech zachycených útoků cílil ale také na Českou republiku.

„V případě trojského koně Mamont můžeme opět dobře vidět, jak útočníci přizpůsobují své kampaně nadcházejícím Vánocům. Ještě v říjnu jsme totiž tuto kybernetickou hrozbu nezachytili. Jeho poznávacím znakem je ta skutečnost, že se nejčastěji šíří jako různé falešné verze volnočasových aplikací – televizních stanic, nástrojů pro modifikace obrázků, různých her nebo jako falešná verze aplikace Spotify. Jakmile stáhneme a spustíme trojského koně Mamont, zaměří se na naše přihlašovací údaje do bankovnictví. Rád bych na tomto místě proto doporučil pár jednoduchých pravidel, které pomohou, zvlášť před Vánoci, zamezit zbytečným krádežím našich peněz. Ve zprávách od neznámých odesílatelů opravdu nikdy neklikejte na odkazy a nestahujte aplikace odjinud než z oficiálního obchodu pro platformu Android, Google Play. Pokud někde totiž narazíte na nějakou skvělou aplikaci se službami zdarma, i když jsou standardně placené, vždy by vás mělo zarazit, že tady něco nehraje," radí Martin Jirkal z ESETu.

Už jen do 31. prosince 2025 nabízí společnost ESET svá řešení v akci 3za2. Zákazníci z řad domácností i firem mají možnost získat tříleté předplatné za cenu dvou let. Více informací o kampani, včetně seznamu konkrétních řešení a podrobných podmínek, najdete na webových stránkách společnosti ESET.

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-utocnici-se-v-listopadu-na-platforme-android-zamerili-na-bankovni-ucty-riziko-se-tykalo-i-ceska