ESET: V říjnu se na chytré telefony zaměřil špionážní malware

26.11.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastěji zachyceným škodlivým kódem v evropském regionu byl v říjnu Spy.Banker.DOK. Svými funkcemi pomáhá útočníkům špehovat chování uživatelů a uživatelek a provádět za ně některé úkony, jako je například rozesílání SMS zpráv, pořizování fotografií nebo instalování aplikací bez jejich vědomí. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Dalším kybernetickým rizikem pak i v říjnu zatím zůstal trojský kůň Triada a upozornil na sebe škodlivý kód Clicker.OZ, který za nás dokáže reagovat na placenou reklamu a vydělávat tak prostřednictvím našeho telefonu útočníkům peníze.

V říjnu se v Evropě nejčastěji objevoval špionážní škodlivý kód Spy.Banker.DOK. Útočníci tak opět potvrdili, že se tento typ hrozby nevyhýbá ani chytrým mobilním telefonům a datům, která v nich uchováváme. Malware tentokrát šířili v tzv. dropperech - škodlivých kódech, které využijí jako obálku k tomu, aby do našich zařízení doručili nepozorovaně hlavní malware.

„Malware Spy.Banker.DOK si nic netušící uživatelé stáhnou do svých zařízení jako aktualizaci pro prohlížeč Chrome. Jeho funkcionality pak jasně odkazují na schopnosti špionážních kódů, které známe z jiných platforem. 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. Na základě provedené analýzy víme, že může být rizikový především pro bankovní aplikace. Útočníci všechny tyto získané informace mohou využít nejen k prolomení přístupu do našich účtů, ale i k přípravě phishingových útoků, protože díky získaným informacím o nás mohou leccos zjistit a působit pak v manipulativní komunikaci opravdu přesvědčivě," popisuje aktuální hrozbu na platformě Android Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Nejvíce případů detekcí malwaru Spy.Banker.DOK zachytili bezpečnostní experti v Polsku, ve Španělsku a Itálii. Zasaženy byly ale i další země v rámci EU, včetně Německa či Řecka. S ohledem na tento široký výskyt proto znovu připomínají důležitost stahování aplikací pouze z oficiálních webových stránek a obchodu Google Play. Právě méně známé obchody třetích stran, internetová úložiště a fóra jsou nejčastějšími zdroji nebezpečných verzí aplikací a programů.

Také v České republice pak byly v říjnu zachyceny další dva škodlivé kódy z popředí pravidelné statistiky kyberhrozeb pro Android – trojský kůň Triada a Clicker.OZ. Oba spadají do kategorie škodlivých kódů, které různě využívají online reklamu.

„Trojský kůň Triada byl ještě v předchozím sledovaném měsíci na špičce pravidelné statistiky, a i nyní s podílem více než 4 procenta všech detekcí v Evropě zůstává stabilním rizikem – nejvíce ve Španělsku a Polsku. Případy ale pravidelně detekujeme i u nás v Česku," říká Jirkal. „Útočníci konkrétně trojského koně Triada šířili v říjnu pod zástěrkou aplikace pro přehrávání videa či jako update pro službu Facebook Messenger. Jako každý jiný adware, i Triada podporuje šíření nevyžádané agresivní reklamy a spamu," doplňuje.

„Škodlivý kód Clicker.OZ pak funguje ještě trochu jinak. Doslova za vás klikne na reklamní okno. Možná si říkáte, proč by to útočníci dělali. Ty důvody jsou většinou jednoduché. Z počtu prokliků mohou získat peníze a vaše zařízení tak zneužívají k tomu, aby to vypadalo, že jste to právě vy, kdo

reaguje na placenou reklamu," pokračuje Jirkal. „Clicker.OZ si uživatelé v říjnu nejčastěji stahovali v domnělém balíčku knihoven – čili kodeků – k přehrávání video a audio obsahu. Útočníci jej ale schovali i pod falešný prohlížeč Chromium," dodává Jirkal z ESETu.

Jakmile reklamní škodlivé kódy infikují vaše zařízení, je poměrně obtížné je odhalit a mohou tam tak nepozorovaně zůstat i několik měsíců. Nejen před adwarem, ale také před dalšími závažnými typy škodlivých kódů či nechtěnými aplikacemi a nebezpečnými webovými stránkami vás pak ochrání kvalitní bezpečnostní software. Společnost ESET nyní svá řešení nabízí v akci 3za2 – od 1. září do 31. prosince 2025 mají zákazníci z řad domácností i firem 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

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-v-rijnu-se-na-chytre-telefony-zameril-spionazni-malware