Hrozby pro Android: Útočníci zneužívají hry i CapCut

31.7.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Kyberútočníci si neberou dovolenou ani v létě. Je ale zřejmé, že zneužívají nejoblíbenější aplikace určené pro komunikaci, například WhatsApp, poslech hudby – Spotify a úpravu videa – CapCut, a hry. Právě kvůli malwaru ve hrách je nutné o rizicích mluvit zejména s dětmi. Nejčastěji jde o hrozby typu dropper nebo adware zobrazující reklamu. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Dle červnové statistiky kybernetických hrozeb pro platformu Android se na předních místech umístily tři různé škodlivé kódy - dropper Agent.MUY , trojan Agent.FJL a adware Andreed. Podle expertů z ESETu mají tyto hrozby společný znak – zneužívají důvěru uživatelů, nepozornost během letních měsíců a ochotu instalovat si aplikace z neoficiálních zdrojů. Některé škodlivé kódy útočníci maskují jako běžné aplikace, jiné se tváří jako aktualizace systému nebo známých programů. V pozadí pak mohou stahovat další malware, zobrazovat agresivní reklamy nebo krást citlivá data.

„V létě pravidelně vidíme nárůst malware, který se šíří v aplikacích určených ke komunikaci či zábavě. Je zřejmé, že útočníci spoléhají na to, že na cestách stahujeme narychlo hru nebo prohlížeč. Dobře vědí, že na dovolených a výletech naše obezřetnost opadá. Tento vývoj budeme pravděpodobně sledovat celé léto. Proto bych apeloval na uživatele, aby si aplikace na cesty volili obezřetně a stahovali je jen z oficiálních zdrojů,“ shrnuje červnový přehled kybernetických hrozeb pro platformu Android Martin Jirkal, vedoucí analytického týmu v pražské pobočce ESET.

Výraznější nárůst experti detekovali u Agent.MUY. Tento typ malware (tzv. dropper) slouží ke stažení dalšího, obvykle nenápadného malware. Co přesně stahuje se různí – někdy to může být spyware, jindy bankovní trojský kůň nebo adware. Útočníci jej vydávají za prohlížeč Chrome. Zaměřuje se intenzivně na Španělsko a Portugalsko, ale ESET jej detekuje po cele Evropské unii

Na mobilní zařízení útočí Agent.FJL, detekce pochází zejména z Německa a Nizozemí, ale vysoký podíl má i Česko. Útočníci jej vydávají za modifikované verze WhatsAppu (např. WhatsApp Plus), Spotify nebo video editor CapCut. Občas se šíří i skrz aplikace pro dospělé. Běžný je také adware Andreed. Tento typ malware uživatelé někdy podceňují, protože „pouze“ zobrazuje reklamu. Nicméně tyto reklamy mohou odkazovat na podvodné stránky, a mohou dokonce znemožnit používání zařízení. Je velmi nebezpečný hlavně kvůli tomu, že se šíří prostřednictvím nelegálně upravených mobilních her, které si mohou snadno stáhnouti děti. V červnu jej experti z ESET detekovali například v Grand Theft Auto: Chinatown Wars nebo omalovánkách ze světa My Little Pony.

„Malware Andreed šíří stránky třetí strany. Jde o různé seznamy Android aplikací ke stažení. Tyto aplikace mohou být dokonce zcela legitimní. Na stránce najdete řadu služeb ke stažení zdarma. Tvůrci stránky, ale každou aplikaci modifikují tak, aby zobrazovala reklamy. Úpravy proběhnou často bez vědomí původních tvůrců aplikace,“ vysvětluje Jirkal. *„Tyto reklamy mohou odkazovat ke stažení dalšího malware nebo na phishingové stránky. Proto je potřeba mít se před nimi na pozoru.“*

Konkrétní aplikace, které malware šíří se velmi rychle mění. Na Androidu se stále opakuje jeden scénář – uživatelé chtějí něco zdarma nebo dříve než ostatní. Nevědomky si stáhnou modifikovanou aplikaci a vpustí útočníka do telefonu.

Odborníci doporučují držet se několika základních zásad, jak se před podobnými hrozbami chránit. Především je důležité stahovat aplikace výhradně z oficiálních obchodů, tím je pro ekosystém Android pouze Google Play. Využívejte spolehlivou bezpečnostní aplikaci. Aplikace i operační systém aktualizujte, když vás k tomu vyzve.

Aplikacím udělujte co nejméně oprávnění. Škodlivá verze aplikace se může prozradit právě tím, že po uživatelích požaduje obrovské množství oprávnění (přístup ke kameře, mikrofonu, fotografiím, poloze apod.).

Vyhněte se klikání na podezřelé reklamy a odkazy, protože i jediný omyl může vést k nechtěné instalaci škodlivého softwaru.

ESET doporučuje nevšímat si lákadel typu „prémiové aplikace zdarma“ a místo toho vsadit na jistotu – aktualizace, oficiální obchody a bezpečnostní nástroj.

„Malware se běžně šíří i aplikacemi, které využívají i nejmladší uživatelé a uživatelky. Útočníci škodlivé verze nabízejí zdarma nebo za výhodnějších podmínek. Stává se také, že daná aplikace ještě není přístupná v Česku nebo pro všechny verze operačního systému. V takových případech se lidé často rozhodnou obejít stahování aplikací z oficiálního obchodu Google Play,“ vysvětluje Jirkal. *„V kyberbezpečnosti platí, že pokud zní něco až moc dobře, patrně jde o podvod. Varujte i děti, aby si hry stahovali jen z Google Play a raději zaplatili férově licenci, než si stáhli rizikový malware.“*

Uživatelé produktů ESET jsou před těmito hrozbami 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 TruePositive 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/hrozby-pro-android-utocnici-zneuzivaji-hry-i-capcut