Hrozby pro Android: Škodlivé kódy i v červenci šířila falešná aplikace Google Chrome

27.8.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Také v červenci se v čele nejčastějších kybernetických hrozeb pro platformu Android objevil škodlivý kód Agent.MUY, který útočníci maskují za falešnou aplikaci prohlížeče Chrome. Zneužívají jej především k šíření dalších škodlivých kódů do napadených mobilních telefonů svých obětí. Zatímco Agent.MUY je hrozbou předně pro Španělsko a Portugalsko, v České republice se v červenci objevoval známý adware Andreed, a to dokonce s podílem 30 % všech zachycených detekcí v zemích EU. Dvojici těchto škodlivých kódů pak doplnil ještě malware Clicker.OZ, který nutí uživatele a uživatelky klikat na nebezpečné reklamy. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Již druhým měsícem se na prvním místě pravidelné statistiky pro platformu Android drží škodlivý kód Agent.MUY. Jedná se o tzv. dropper – malware, jehož úkolem je do našich zařízení nepozorovaně dopravit různé kybernetické hrozby. Jeho fungování si můžeme představit jako obálku, která schová další škodlivé kódy, aby bylo pro detekční nástroje složitější je odhalit.

„Primární destinací tohoto škodlivého kódu nadále zůstalo Španělsko a Portugalsko. České republice se v červenci spíše vyhýbal. Rozhodně je ale důležité, aby o něm uživatelé a uživatelky v Česku měli povědomí, protože zrovna kybernetické hrozby na platformě Android se poměrně dynamicky vyvíjejí a co platí jeden měsíc, může být ten další zase trochu jinak," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Útočníci maskují malware Agent.MUY za falešnou aplikaci prohlížeče Chrome. Bezpečnostní experti proto zdůrazňují, aby uživatelé a uživatelky tuto aplikaci vždy stahovali pouze z oficiálního obchodu pro platformu Android – Google Play. Stránky obchodů třetích stran nebo internetová fóra mohou být právě s ohledem na přítomnost škodlivého kódu v různě upravených či dokonce falešných verzích aplikací rizikové.

Adware Andreed se stále drží na stabilních hodnotách. V červenci na něj mohli uživatelé a uživatelky narazit stále ve falešné verzi hry GTA: Chinatown Wars nebo v aplikaci s omalovánkami ze světa My Little Pony.

„Z celoevropského měřítka to byl v červenci právě adware Andreed, který jsme tentokrát nejvíce zachytili právě v České republice. Jednalo se o podíl až 30 % v rámci všech evropských zemí, které sledujeme. Kromě České republiky jsme jej nejvíce detekovali také v Německu, Polsku a Maďarsku," říká Jirkal. „S adwarem Andreed si mnoho uživatelů nedělá žádné starosti. Berou to tak, že je prostě jen obtěžuje vyskakovacími reklamními okny. Adware je nicméně zákeřný v tom, že dokáže také řadě dalších škodlivých kódů usnadnit cestu do zařízení. Ty přitom už nemusí vůbec být tak nevinné – například spyware," dodává Jirkal.

Na Českou republiku a Slovensko se pak v červenci útočníci zaměřili také prostřednictvím škodlivého kódu Clicker.OZ. Jak už pojmenování napovídá, útočníci se jeho prostřednictvím snaží přimět uživatele a uživatelky ke kliknutí na zobrazovanou reklamu. Nejčastěji na něj pak mohli narazit lidé ve Velké Británii nebo v Německu.

„Škodlivý kód Clicker.OZ je schovaný v podvodné aplikaci, která je zacílena hlavně na reklamní agentury a jejich zaměstnance. Ke škodlivé aktivitě zneužívá jejich zařízení. Útočníci škodlivý kód vydávají za tzv. Code pack neboli balíček ovládačů, které mají lidem pomoci v práci s různými formáty videí nebo hudebních souborů. Kromě zobrazování reklamy ke kliknutí dokáže tento škodlivý kód také vypnout nebo zapnout Wi-Fi a posílat útočníkům snímky obrazovky," vysvětluje Jirkal z ESETu.

Bezpečnostní experti stále čekají na čísla detekcí za měsíc srpen, již nyní však potvrzují, že letošní letní prázdniny byly z pohledu aktivity škodlivých kódů poměrně rušné. Útočníci se na platformu Android zaměřují především prostřednictvím falešných a škodlivých aplikací, které vydávají za známé hry nebo služby s nějakou výhodou – ať už ve zvýhodněném balíčku či zcela zdarma. Uživatelé a uživatelky by tak měli aplikace a hry pro své mobilní telefony stahovat pouze z ověřených a legitimních obchodů a vyvarovat se méně známých obchodů třetích stran či internetových fór. Pokud přeci jen stáhnou škodlivou aplikaci a na svém telefonu ji spustí, nejlépe je v takovém případě ochrání kvalitní a renomovaná kyberbezpečnostní aplikace, která škodlivý kód včas rozpozná.

Uživatelé produktů 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/hrozby-pro-android-skodlive-kody-i-v-cervenci-sirila-falesna-aplikace-google-chrome