Hrozby pro Android: V dubnu se nejvíce šířil adware, k jeho maskování útočníci využili kultovní hry

2.6.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Praha, 26. května 2025 – na základě dat z dubnové statistiky nejčastějších kybernetických hrozeb pro platformu Android v zemích EU jsou mezi útočníky opět nejvíce oblíbené populární mobilní hry, které šíří adware. Jak ale bezpečnostní experti upozorňují, i přes pokles v počtu detekcí se nadále budeme setkávat s falešnými verzemi jinak placených služeb, které útočníci nabízejí zdarma – například s falešnou modifikací pro získání prémiové verze Spotify nebo falešnou VPN aplikací. Rozvoj těchto rizik očekávají také v kontextu nadcházející letní sezóny. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Zatímco ještě v březnu byl mezi útočníky nejoblíbenějším škodlivým kódem trojský kůň Agent.GKE, který vydávali za škodlivou modifikaci pro aplikaci Spotify, v dubnu se do čela pravidelné statistiky opět vyšplhal adware Andreed. Adware se nejen v Česku, ale i v ostatních evropských zemích šíří především prostřednictvím falešných verzí mobilních her nebo herních modifikací. Jeho úkolem je zobrazovat škodlivou reklamu a přimět uživatele ke kliknutí. V dubnu byly nejstahovanější škodlivé verze starších populárních her Dead Effect 2 a Grand Theft Auto: Chinatown Wars.

„Adware Andreed se stabilně drží mezi největšími riziky pro platformu Android v našem regionu. Nejčastěji jsme jej v dubnu detekovali nejen v Česku, ale také například v Polsku a Německu nebo v Portugalsku. Aktuálně si útočníci opět připravili nové verze mobilních her. Dynamicky je proměňují a střídají podle toho, co zrovna na uživatele nejvíce funguje. Prázdninová a letní sezóna je navíc za dveřmi a v tomto období pravidelně pozorujeme jejich zvýšený počet," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce ESET.

Mobilní hry jako způsob šíření škodlivých kódů útočníci volí záměrně. K jejich úspěchům může přispívat i skutečnost, že uživatelé v současnosti využívají několik různých verzí platformy Android, a ne pro všechny mohou být hry dostupné. Omezení se mohou týkat také jen určitých zemí.

„I když může být pro uživatele velmi lákavé stahovat mobilní hry i mimo oficiální obchod Google Play, určitě bych jim to nedoporučoval. Podle jednoho z posledních průzkumů od ESET to však vypadá, že konkrétně Češi už jsou v tomto ohledu dostatečně uvědomělí a stahují pouze ze známých a oficiálních míst. K dalším doporučením určitě patří věnovat čas uživatelským recenzím. Přečíst bychom si je měli vždy, když chceme nějakou aplikaci stáhnout, protože špatné zkušenosti si druzí většinou nenechají pro sebe a upozorní na ně. A v neposlední řadě i na mobilní telefon patří bezpečnostní software, který nás jistí v případech, kdy stejně škodlivou aplikaci stáhneme a reálně bude hrozit, že vpustíme škodlivé kódy k našim datům," shrnuje doporučení k ochraně mobilních telefonů Jirkal.

Zatímco detekce trojského koně Agent.GKE, který stojí za šířením škodlivé modifikace pro Spotify, v dubnu znatelně klesly, mírně vzrostl počet případů dalšího trojského koně, Agent.EQD. Oba typy škodlivých kódů se v Evropě drží již několik měsíců. Prostřednictvím trojského koně Agent.EQD útočníci lákají na bezplatnou VPN síť.

„Dobrou zprávou je, že podle našich dat nepatří Češi k nejčastějším obětem falešného upgradu pro

Spotify. I když se i u nás případy samozřejmě najdou, nejohroženějšími zeměmi byly v dubnu Španělsko, Polsko a Francie. I přes aktuální pokles případů to zatím nevypadá, že by se této strategie útočníci jen tak vzdali a s lákadlem v podobě bezplatného prémiového streamování hudby se budeme i nadále setkávat," říká Jirkal. „V případě trojského koně Agent.EQD také zatím nepozorujeme změny. Podle našich analýz by v tuto chvíli neměly servery škodlivé aplikace fungovat, útočníci se mohou ale kdykoli rozhodnout jejich činnost obnovit. V minulých případech zapojovali nic netušící uživatele, kteří si domnělou VPN stáhli, do DDoS útoků, což se klidně může stát znovu. Nejsilněji jsou případy tohoto škodlivého kódu zastoupeny v Německu, přítomný je ale i v České republice," dodává Martin Jirkal z ESETu.

Bezpečnostní experti opakovaně upozorňují, že v případě poskytovatelů VPN sítí se zdánlivá úspora uživatelům a uživatelkám nevyplatí. Úkolem VPN je poskytnout jim soukromí, bezpečnost a určitou míru anonymity. Díky VPN je online činnost hůře sledovatelná. Z tohoto důvodu by se proto měli vždy obracet na renomované poskytovatele a nezdráhat se pořídit si kvalitní placenou službu, která bude dbát na ochranu jejich dat. Spolehlivé VPN lze zakoupit samostatně i jako součást moderních bezpečnostních řešení.

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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-android-v-dubnu-se-nejvice-siril-adware-k-jeho-maskovani-utocnici-vyuzili-kultovni-hry