Závěrem léta byl největším rizikem pro telefony s platformou Android trojský kůň SparkKitty

19.9.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Praha, 19. září 2025 – Bezpečnostní experti v srpnu nejčastěji detekovali trojského koně Spy.SparkKitty. Jeho cílem jsou naše data z telefonu, a to především naše fotky a snímky obrazovky. Útočníci škodlivý kód šíří prostřednictvím škodlivých verzí aplikací ke sledování kurzu kryptoměn, uživatelé a uživatelky ale na něj mohli narazit i ve falešné aplikaci populární sociální sítě TikTok. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Dále se na přední místa vyšplhal také trojský kůň Triada a dvojici pak doplnil známý adware Andreed.

Nejčastějším srpnovým škodlivým kódem byl tentokrát v evropském regionu trojský kůň Spy.SparkKitty. Jeho oběťmi byli hlavně uživatelé a uživatelky v sousedním Polsku, bezpečnostní experti však doplňují, že jeho případy zachytili také v České republice.

„Jak napovídá název samotného škodlivého kódu, máme na platformě Android opět tu čest s malwarem, který se snaží odcizit naše data z telefonu. Hlavním cílem Spy.SparkKitty jsou naše fotografie. Útočníci sází na to, že ve své galerii můžeme mít kromě fotek z dovolených nebo svých domácích mazlíčků i snímky obrazovky s citlivými informacemi," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Útočníci jej většinou ukrývají do falešných aplikací, které mají údajně pomáhat se sledováním kurzů kryptoměn. Objevily se ale i případy modifikované aplikace populární sociální sítě TikTok, která trojského koně také ukrývala. Takové aplikace se zpravidla objevují v menších a méně známých obchodech s mobilními aplikacemi, mohou se ale bohužel objevit i v oficiálním obchodu Google Play. Zajímavostí tohoto škodlivého kódu je také skutečnost, že je rizikem i pro uživatele a uživatelky platformy iOS, tedy iPhonů," doplňuje Jirkal.

Škodlivé aplikace poté, co si vyžádají přístup ke galerii fotografií v telefonu, je odesílají na řídící server útočníků. Bezpečnostní experti tak znovu připomínají, aby uživatelé dbali na opatrnost při udělování práv aplikacím, které si stáhnou do svého zařízení a pokud mají pocit, že mohou mít v telefonu škodlivý kód, doporučují pořízení kyberbezpečnostního programu, který v zařízení přítomnost škodlivého kódu zkontroluje. Obecně také nedoporučují pořizovat snímky obrazovky s důležitými osobními a přihlašovacími údaji. Kromě zneužití informací k získání přístupu k účtům mohou útočníci fotografie využít i k vydírání svých obětí.

Dalším trojským koněm, který se umístil na předních místech statistiky, byl Triada. Ten je dobře známým škodlivým kódem i v Česku. Naposledy se například objevoval v aplikaci určené ke čtení z ruky. Tentokrát útočníci vsadili na falešné aplikace a soubory s updaty, které slibovaly zobrazování videa v lepším rozlišení.

„Trojský kůň Triada v srpnu cílil na celou Evropu. Je to škodlivý kód, který zobrazuje především nevyžádanou reklamu a spam. Rozhodně bychom ho ale neměli podceňovat, podobně jako adware Andreed, naší stálici mezi nejčastějším malwarem v evropských zemích. Ten se v srpnu opět objevoval typicky v mobilních hrách, tentokrát nejčastěji v ‚Geometry Jump' nebo ‚Hacker or Dev Tycoon? Tap Sim'. Opět je vidět, že se útočníci nebojí být ve výběru her, jejichž falešné verze zneužijí k šíření škodlivého kódu, kreativní. Adware Andreed se v srpnu nejvíce objevoval v Polsku, a právě také u nás, v Česku," dodává Jirkal z ESETu.

Škodlivé kódy zobrazující agresivní reklamu mají uživatelé a uživatelky ve zvyku spíše podceňovat, protože se domnívají, že se nejedná o závažnou hrozbu. Pod zdánlivě neškodným reklamním sdělením se ale mohou ukrývat odkazy na nebezpečné webové stránky, které mohou být zdrojem daleko závažnějšího malwaru. Kromě pořízení kvalitní kyberbezpečnostní ochrany je tak na místě i rozumný přístup ke stahování aplikací a jejich využívání. Bezpečnostní experti například doporučují, abychom stahovali aplikace, které opravdu využijeme, udělovali jim jen nezbytná oprávnění a pokud je nějakou dobu nepoužíváme, je vhodné je z telefonu odinstalovat.

Profesionální kyberbezpečnostní ochranu v našich chytrých telefonech máme ve zvyku spíše podceňovat, zatímco útočníci na ně cílí stejně jako na počítače a notebooky. 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

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/zaverem-leta-byl-nejvetsim-rizikem-pro-telefony-s-platformou-android-trojsky-kun-sparkkitty