Přehled hrozeb pro Android: Česko v říjnu zasypaly falešné hry různých žánrů

25.11.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

Zdrojem adwaru Andreed a trojského koně Agent.FBE byly v říjnu závodní, strategické i bojové a dobrodružné mobilní hry. K šíření škodlivé aplikace FakeApp.AFZ útočníci opět zneužili popularitu nástrojů umělé inteligence. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET. Bezpečnostní experti varují, že snahou útočníků může být přesměrovat uživatele na nebezpečné webové stránky nebo je prostřednictvím škodlivého kódu přihlásit k falešnému investování. Upozorňují také, že cílem těchto kybernetických hrozeb mohou být i nejmenší uživatelé z řad dětí.

Na základě nejnovější analýzy detekčních dat bezpečnostní experti v říjnu zatím potvrdili, že dominantními hrozbami jsou pro české telefony s platformou Android falešné verze mobilních her. V říjnu se staly zdrojem adwaru Andreed a trojského koně Agent.FBE.

„Na základě posledních analýz můžeme říct, že Česko zaplavily cracknuté verze her, které obsahují různé typy kybernetických hrozeb. V tuto chvíli zcela vytlačily jiný malware, a to i bankovního trojského koně Cerberus. V říjnu se jednalo o širokou paletu různých herních žánrů. Adware Andreed se objevoval nejvíce ve hře se závodní tématikou Car Parking Multiplayer. Trojský kůň Agent.FBE se šířil v dobrodružných, bitevních i strategických hrách. Útočníci v jeho případě zneužili také verzi známé plošinovky – hry Geometry Dash. Ačkoli by se mohlo zdát, že tato stále se opakující strategie už nebude fungovat, opak je evidentně pravdou. Útočníci zcela jistě zkouší šířit i méně nebezpečný škodlivý kód prostřednictvím aplikací pro volný čas. Očekávají, že uživatelé všech věkových kategorií budou před koncem roku tuto zábavu vyhledávat," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

V říjnu pak výše zmíněné hrozby doplnila škodlivá aplikace FakeApp.AFZ, na kterou bezpečnostní experti z ESETu upozornili již minulý měsíc. Útočníci ji nejčastěji šířili ve falešné verzi aplikace Super AI.

„Ačkoli všechny říjnové hrozby pro platformu Android nepatří k těm nejzávažnějším typům škodlivých kódů, jako je například spyware nebo ransomware, i adware nebo trojské koně mohou představovat rizika pro naše finance a data. Mohou například provádět v zařízení změny, kterých si uživatelé na první pohled nevšimnou, nebo odkazovat na nebezpečné webové phishingové stránky. Útočníci škodlivé kódy zabalí do domnělých aplikací známých značek. Proto bych rád apeloval na uživatele, aby dbali na to, odkud si aplikace pro své chytré telefony stahují. Na jejich falešné a nebezpečné verze narazí především v neoficiálních obchodech třetích stran, které nabízejí hry ve výhodných balíčcích, zcela zdarma nebo ve verzích, které nikde jinde nejsou dostupné. Doporučil bych jim také, aby si o těchto rizicích promluvili se svými dětmi, které, pokud mají své první smartphony, patří také mezi cíle útočníků," varuje Jirkal.

Také v říjnu zneužili útočníci popularity nástrojů umělé inteligence. Pod falešnou verzi nástroje Super AI – Powered by ChatGPT ukryli škodlivou aplikaci FakeApp.AFZ, která může po otevření zaregistrovat uživatele do tzv. cryptoscamu.

„Útočníci využívají škodlivý kód FakeApp.AFZ k zacílení na oběti, které zajímá investování. Má podobu jednoduché aplikace, která uživatelům zobrazuje webové stránky s možnostmi investovat své peníze. Známý nástroj a značka má působit jako návnada a přesvědčit je, že je vše bezpečné a

spolehlivé. Útočníci dokonce nechají peníze svých obětí chvíli vydělávat a umožní jim je vybrat, aby si u nich vybudovali důvěru a oni posílali postupně stále větší částky. Je ale samozřejmě jen otázka času, kdy o ně uživatelé definitivně přijdou," vysvětluje podvod Jirkal.

Bezpečnostní experti lidem doporučují, aby si ještě před začátkem investování zjistili co nejvíce informací o vybrané službě na internetu. Další podvedení lidé si to totiž pravděpodobně nenechají pro sebe a na podvod upozorní. V případě internetových podvodů je podle nich důležitá celková obezřetnost a zdravá skepse. Platí to jak pro služby, které jsou někde v nabídce zadarmo, tak i pro ty, které slibují pohádkové zbohatnutí. I v případě hrozeb v podobě adwaru a trojských koní by si uživatelé měli pořídit spolehlivý bezpečnostní software, který jim dnes nabízí ke klasické ochraně před malwarem i řadu užitečných funkcí.

„Pro ochranu svých dat mohou uživatelé využít například zabezpečenou složku ESET Folder Guard, kterou jsme představili v aktualizované nabídce řešení pro domácnosti letos na podzim. Chrání cenná data uživatelů před malwarem, který se je snaží poškodit. Uživatelé mohou vytvořit až několik zabezpečených složek, ke kterým budou mít přístup jen důvěryhodné a uživatelem povolené aplikace," dodává Jirkal z ESETu.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-android-cesko-v-rijnu-zasypaly-falesne-hry-ruznych-zanru