Přehled hrozeb pro Android: Útočníci v září lákali na falešné investice, využili jména firem OpenAI a IBM

29.10.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

Na platformě Android v Česku vzrostly v září především detekce adwaru Andreed, a to na více než 18 procent všech zachycených případů. Zatímco detekce bankovního trojského koně Cerberus v září klesly, do popředí pravidelné statistiky se vyšplhaly škodlivá aplikace FakeApp.AFZ a trojský kůň Agent.FBG. V případě škodlivého kódu FakeApp.AFZ pak útočníci opět využili strategii, při které jej vydávali za investiční aplikace zneužívající jména služeb IBM a OpenAI. Tyto falešné aplikace pak obětem nabízely možnosti investování do kryptoměn, přičemž cílem útočníků bylo pouze odcizit jejich peníze. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Na platformě Android v Česku vzrostly v září především detekce reklamního škodlivého kódu – adwaru Andreed. Ten se stále více přibližuje hranici pětiny všech detekcí v České republice, které v letošním roce zatím ještě nedosáhl.

„I přes výraznější růst detekcí adwaru Andreed na sebe v září strhly pozornost především zachycené případy škodlivých kódů, které se na předních místech naší statistiky pro platformu Android zatím neobjevovaly. V případě škodlivé aplikace FakeApp.AFZ nám analýza potvrdila, že s ní útočníci cílili na uživatele, kteří mají zájem o investování do kryptoměn. Také v případě trojského koně Agent.FBG některé informace nasvědčují tomu, že útočníci chtěli využívat zařízení obětí k těžení kryptoměn. Opět v těchto případech využívají osvědčené postupy. Škodlivé kódy zabalí do domnělých aplikací, které zneužívají známé značky. FakeApp.AFZ takto šířili například v napodobeninách aplikací od IBM nebo OpenAI. Trojského koně Agent.FBG jsme pak v září nejčastěji objevili v cracknuté verzi populární herní platformy Roblox," říká k nejnovějším zjištěním Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Kromě výše zmíněných případů byly rizikem znovu také falešné verze her pro chytré telefony – Mini Ninjas a Heroes of Might & Magic III. V září byly opět zdrojem adwaru Andreed.

„Aktuálně pozorujeme, jak útočníci čím dál tím sebevědoměji zneužívají známá jména mobilních her a aplikací. Vědí, že fanoušci technologií dnes například rádi zkouší vše kolem nástrojů umělé inteligence. Jednoduše tak škodlivý kód schovají do aplikace s atraktivním názvem. Uživatelé by neměli dát na pochybné a příliš výhodné nabídky různých aplikací a nástrojů mimo oficiální obchody s aplikacemi. V opačném případě mohou vždy počítat s tím, že do svého chytrého telefonu stáhnou obsah, který tam nechtějí. I reklamní škodlivý kód může mít negativní vliv na výkon a fungování jejich zařízení a inzerovat odkazy na stránky, na kterých mohou narazit na závažnější typy hrozeb," dodává Jirkal.

Motivem drtivé většiny kybernetických útoků jsou peníze. K jejich získání útočníci využívají nejen k tomu určené škodlivé kódy, které dokáží například prolomit hesla do našich účtů, ale snaží se získat také naše data, která mohou velmi dobře zpeněžit prodejem na černém trhu. Další taktikou, například k získání našich hesel do internetového bankovnictví nebo údajů k platební kartě, je manipulativní komunikace. S tou se můžeme nejvíce setkat v případě útoků pomocí technik sociálního inženýrství – phishingu, vishingu nebo smishingu. Útočníci mohou navíc všechny metody libovolně kombinovat v promyšlených útočných kampaních.

„V případě škodlivého kódu FakeApp.AFZ můžeme vidět jeden z dalších způsobů, jak se útočníci snaží získat naše finance. FakeApp.AFZ má podobu jednoduché aplikace, která uživatelům zobrazuje webové stránky. Tváří se ale nejdříve jako služba firem IBM či OpenAI. Jakmile uživatelé aplikaci otevřou, zaregistrují se do tzv. cryptoscamu. To znamená, že jim škodlivá aplikace nabídne možnost zhodnotit si peníze investicemi do kryptoměn a známá značka má pomoci k tomu, aby vše působilo bezpečně a spolehlivě. Existují dokonce případy, kdy oběti zkouší investovat malé částky a pak je bez problémů vyberou, jako by se jednalo o legitimní službu. Škodlivá aplikace obětem ukazuje, jak jejich peníze vydělávají a tím je motivuje, aby jich posílali víc. Své peníze však po čase oběti nebudou moci vybrat a definitivně o ně přijdou. Lidem bych doporučil, aby si ještě před začátkem investování zjistili co nejvíce informací o vybrané službě na internetu. Další podvedení lidé si to totiž určitě nenechají pro sebe a na podvod upozorní," vysvětluje Jirkal.

Uživatelé a uživatelky nejen v České republice čelí dnes stále většímu počtu situací, kdy mohou na kybernetické hrozby narazit při řadě běžných každodenních aktivit. Útočníci jsou vynalézaví a vydělávání peněz v podobě kybernetických útoků může být dnes i dobře organizovanou činností, kterou bychom čekali spíše u velkých organizací a firem. Ani v případě chytrých telefonů s platformou Android by tak uživatelé neměli podceňovat kvalitní ochranu v podobě bezpečnostního softwaru, který včas a preventivně zasáhne proti kybernetickým útokům.

„Kybernetické hrozby se vyvíjejí rychle a s tím, jak se naše životy stále více digitalizují, začíná být složité předvídat, odkud by mohl potenciální útok přijít. Proto by uživatelé měli zvážit pořízení bezpečnostního programu, který všechny možné scénáře pohlídá za ně," říká Jirkal a dodává: „Rozhodně to ale není tak, že by uživatelé měli rezignovat na nějakou obezřetnost na internetu. Je stále mnoho kroků, kterými mohou sami podpořit svou online bezpečnost. Ať už mluvíme o bezpečném stahování aplikací a programů výhradně z oficiálních zdrojů nebo opatrnosti při nakládání s příchozí nevyžádanou komunikací v e-mailech nebo v chatovacích aplikacích."

Bezpečností software kontroluje stahované aplikace. Program v případě, že nějakou aplikaci nebo soubor rozpozná jako nebezpečnou, spustí tzv. rezidentní ochranu souborového systému, která stažení či spuštění aplikace zablokuje a umístí ji do karantény. Uživatelé jsou o tomto postupu vždy informováni samotným bezpečnostním programem.

Bezpečnostní software pak nabízí také další nástroje k ochraně naší digitální identity, jako je virtuální privátní síť VPN nebo správce hesel, například ESET Password Manager.

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.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-android-utocnici-v-zari-lakali-na-falesne-investice-vyuzili-jmena-firem-openai-a-ibm