ESET objevil nový phishingový útok využívaný v bankovních podvodech, cílem byli klienti českých bank

22.8.2024 - Lucie Mudráková | ESET software

Bezpečnostní analytici ze společnosti ESET objevili a popsali novou podobu phishingových kampaní využívaných pro bankovní podvody.

Standardní phishingové techniky doručení škodlivého kódu byly tentokrát kombinovány s novou metodou – útočníci se zaměřili na uživatele platforem Android a iOS prostřednictvím aplikací PWA, a v případě platformy Android také prostřednictvím WebAPK. Instalace neobsahovaly ve zjištěných případech žádná varování o tom, že dochází k instalacím aplikací třetích stran. Většina pozorovaných aplikací cílila na klienty českých bank, experti společnosti ESET nicméně zaznamenali také aplikace zaměřené na banky v Maďarsku a Gruzii. Na základě analyzovaných dat dospěli k závěru, že za kampaněmi stály dvě různé skupiny útočníků. Společnost ESET informovala o těchto hrozbách banky obětí a pomohla také několik phishingových domén a řídících serverů odstranit.

Bezpečnostní experti společnosti ESET objevili neobvyklý typ phishingové kampaně, která byla převážně zaměřena na klienty českých bank. Nově objevená phishingová technika se oproti jiným vyznačuje tím, že útočníci dokáží přimět oběti k instalaci phishingových aplikací z webové stránky třetí strany, aniž by se oběť dozvěděla, že se jedná o aplikaci z neoficiálního zdroje. Na platformě Android to může vést dokonce k tiché instalaci speciálního typu aplikace APK (Android Application Package – softwarový balík pro distribuci a instalaci aplikací), která vypadá, jako by byla nainstalována z oficiálního obchodu Google Play.

Nově popsaná hrozba cílila také na uživatele chytrých telefonů iPhone s operačním systémem iOS. Phishingové webové stránky zaměřené na platformu iOS instruovaly oběti k tomu, aby přidaly aplikaci PWA (Progressive Web App – Progresivní webová aplikace) na své domovské obrazovky.

„V případě obou platforem, Android i iOS, byly phishingové aplikace do značné míry nerozeznatelné od skutečných bankovních aplikací, které napodobují. PWA aplikace byly v podstatě webové stránky zabalené do zdánlivě samostatné aplikace, přičemž zdání její opravdovosti bylo podpořeno také využitím tzv. nativních systémových výzev – notifikací telefonu. PWA aplikace jsou, stejně jako webové stránky, dostupné pro různé operační systémy, což vysvětluje, jak mohou tyto phishingové kampaně cílit na uživatele platformy iOS i Android. Pro uživatele chytrých telefonů iPhone může taková kampaň nabourat zažité předpoklady o bezpečnosti ‚uzavřeného ekosystému' platformy iOS," říká Jakub Osmani, bezpečnostní analytik pražské výzkumné pobočky společnosti ESET, který novou phishingovou metodu analyzoval.

Odhalené phishingové kampaně využívaly tři různé způsoby, jak doručit škodlivé webové adresy obětem. Mezi těmito mechanismy byly automatizované hlasové hovory, SMS zprávy a malvertising (škodlivá reklama) na sociálních sítích. Hlasový hovor byl realizován prostřednictvím automatizovaného hovoru, ve kterém útočníci „varovali" uživatele před zastaralou bankovní aplikací a podněcovali je tak k okamžité aktualizaci. Uživatelé byli následně vyzváni, aby vybrali následující krok na číselné klávesnici. Po stisknutí správného tlačítka jim byla prostřednictvím SMS zprávy odeslána phishingová URL adresa.

„Rozesílání falešných URL adres probíhalo podle našich zjištění na náhodná česká telefonní čísla. Zpráva obsahovala phishingový odkaz a text, kterým chtěli útočníci zmanipulovat oběť tak, aby na odkaz klikla. Škodlivá kampaň se šířila také prostřednictvím registrovaných reklam na sociálních sítích společnosti Meta, jako jsou Instagram a Facebook. Tyto reklamy vyzývaly k nějaké akci, například ke stažení aktualizace v podobě omezené nabídky pro uživatele," vysvětluje Osmani.

V případě platformy Android se po kliknutí na škodlivou URL adresu objevovaly dvě další, rozdílné varianty tohoto phishingového útoku – buď vysoce kvalitní phishingová stránka napodobující oficiální stránku obchodu Google Play s bankovní aplikací ke stažení, nebo napodobenina webové stránky opět zobrazující možnost stažení bankovní aplikace. V dalším kroku pak byly oběti vyzvány k tomu, aby „novou verzi" bankovní aplikace nainstalovaly.

Popsaná phishingová kampaň a její metody jsou možné pouze díky technologii progresivních webových aplikací – PWAs. PWAs jsou vytvořené pomocí tradičních technologií webových aplikací, které mohou fungovat na více platformách a zařízeních. WebAPK aplikace lze pak považovat za vyšší verze progresivních webových aplikací. Prohlížeč Chrome generuje nativní aplikaci APK pro Android z PWA. WebAPK aplikace pak vypadají jako běžné nativní aplikace, což jsou aplikace určené pouze pro jeden operační systém – v tomto případě vypadají jako nativní aplikace pro platformu Android. Instalace aplikace WebAPK navíc v rámci této phishingové kampaně nevyvolává žádná varování o „instalaci aplikace z nedůvěryhodného zdroje". Taková aplikace bude dokonce nainstalována i v případě, kdy není povolena instalace aplikací třetích stran.

Za kampaněmi stály podle analytiků z ESETu dvě různé skupiny útočníků. Jedna skupina použila bota na sociální platformě Telegram k zaznamenávání všech zadaných informací od obětí do skupinového chatu prostřednictvím oficiálního Telegram API. Druhá skupina použila tradiční řídící C&C server s administrativním panelem.

„Na základě skutečnosti, že útočníci v rámci zjištěných kampaní využívali dvě odlišné řídící infrastruktury, je pravděpodobné, že za phishingovými kampaněmi proti českým bankám stály dvě samostatné skupiny útočníků," uzavírá Osmani z ESETu.

Většina z analyzovaných případů se odehrála v České republice, pouze dvě phishingové aplikace se objevily mimo český region, a to konkrétně v Maďarsku a Gruzii. Veškeré citlivé informace, které analytici společnosti ESET v těchto případech zachytili, byly okamžitě zaslány postiženým bankám k dalšímu zpracování. ESET také pomohl s odstraněním několika phishingových domén a řídících serverů.

Inovativní phishingovou kampaň analyzovali v Česku bezpečnostní experti společnosti ESET poskytující profesionální služby kybernetické bezpečnosti velkým společnostem. Více technických informací k popsané phishingové kampani najdete v článku na webu welivesecurity.com.

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/eset-objevil-novy-phishingovy-utok-vyuzivany-v-bankovnich-podvodech-cilem-byli-klienti-ceskych-bank