

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo 6 ze dne 22.2.2022

Útočníci využili k šíření bankovního malwaru neoficiální verzi nástroje Google Photos.

V lednu se malware Cerberus objevil ve více než polovině všech detekovaných hrozeb pro platformu Android v Česku. Útočníci k jeho šíření využili například nelegitimní kopii galerie pro prohlížení a sdílení fotek od Google.

Zatímco v prosinci nebyl bankovní trojský kůň Cerberus v Česku výrazně aktivní, v lednu ho bezpečnostní analytici objevili v nadpoloviční většině všech detekovaných hrozeb pro platformu Android. Útočníci k jeho šíření využili například neoficiální verzi aplikace Google Photos, která slouží k prohlížení a sdílení fotek v zařízení. Mezi nejčastějšími hrozbami zůstal nadále také malware Banker.APP nebo Agent.IEG, který se v lednu šířil prostřednictvím nástrojů pro přehrávání hudby. Vyplývá to z pravidelné statistiky hrozeb od společnosti ESET.

V lednu na uživatele operačního systému Android útočil nejsilněji trojský kůň Cerberus. Tento škodlivý kód se v Česku vyskytuje dlouhodobě a je rizikem především pro bankovní služby. Šířil se nejčastěji prostřednictvím malwaru Spy.Cerberus, který se maskoval za aplikaci Google Photos 5. Bezpečnostní specialisté ho objevili ve více než polovině všech detekcí.

„Na základě našich dat můžeme potvrdit, že v lednu se v případě malwaru Cerberus jednalo o velkou kampaň. Zatímco v prosinci jsme u největší rodiny tohoto malwaru zaznamenali pokles o více než desetinu detekcí, v lednu Cerberus zaútočil opět silněji a momentálně v jeho případě pozorujeme nárůst o 14 procent,“ říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Bankovní malware se v Česku šíří prostřednictvím tzv. dropperů, škodlivého kódu, který napodobuje známé nástroje a služby. Útočníci motivují uživatele ke stažení často tím, že známé programy nabízejí ke stažení zdarma nebo v době, kdy už v oficiálních obchodech nejsou dostupné. Uživatelé ale většinou stáhnou s takto nabízenými nelegitimními aplikacemi do zařízení další, daleko škodlivější malware.

V lednu útočníci vsadili také na aplikace pro přehrávání hudby

S výrazně menším podílem detekcí byly v lednu detekovány škodlivé kódy Banker.APP a Agent.IEG. Oba dva typy malware se v Česku objevily již v prosinci.

„Malware Banker.APP se mezi detekovanými hrozbami nově objevil v prosinci loňského roku a vypadá to, že začíná být v českém prostředí populární,“ říká Jirkal. *„Opět je rizikem především pro bankovní služby. Dokáže například překrýt přihlašovací okno do bankovní aplikace svým, čímž původní okno s přihlášením věrně napodobí. Uživatel má většinou malou šanci tuto změnu postřehnout. Zadá do falešného okna své přihlašovací údaje, které mu tímto způsobem škodlivý kód odcizí,“* vysvětluje Jirkal.

Malware Agent.IEG, který se v Česku objevuje pravidelně od loňského podzimu, v lednu oslabil. Ke svému šíření využil například neoficiální verze aplikací pro přehrávání hudby.

„Dropper Agent.IEG se v lednu vydával například za aplikace MX Player, Music Downloader nebo Reproductor MX. Je tak zřejmé, že v tomto případě se útočníci zaměřili na uživatele, kteří do svých zařízení stahují nástroje pro přehrávání hudby,“ dodává Jirkal.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo 6 ze dne 22.2.2022

Pozor na stahování aplikací zdarma

Lednové statistiky potvrdily, že bankovní malware zatím zůstává v Česku rizikem i pro letošní rok. Podle bezpečnostních specialistů je tak důležité nezapomínat na zabezpečení ani v případě chytrých telefonů či tabletů s operačním systémem Android. Kromě toho je důležité pravidelně systém i aplikace v zařízení aktualizovat a vyvarovat se rizikovému chování, jako je například stahování aplikací mimo oficiální obchod Google Play. V případě, že uživatelé přistupují prostřednictvím svého mobilního zařízení do internetového bankovníctví, snižují riziko odcizení citlivých údajů používáním oficiální aplikace od poskytovatele bankovních služeb.

„Útočníci umí velmi dobře pracovat s emocemi uživatelů a zkoušejí na nich různé strategie. Patří tam tak i nabídky na aplikace, které mohou být v oficiálním obchodě zpoplatněné nebo nedostupné. Stažení takové aplikace, která navíc odkazuje na nějaký aktuální trend, může být pro uživatele opravdu lákavé. Platí ovšem, že pokud je někde k bezplatnému stažení jinak drahý profesionální program nebo hra, pravděpodobnost, že spolu s aplikací stáhne uživatel také malware, je vysoká,“ říká Jirkal z ESETu.

Nejčastější kybernetické hrozby v České republice pro platformu Android za leden 2022:

1. Android/Spy.Cerberus (62,79 %)
2. Android/Spy.Banker.APP (5,54 %)
3. Android/TrojanDropper.Agent.IEG trojan (4,37 %)
4. Android/TrojanDropper.Agent.DWZ trojan (2,69 %)
5. Android/Andreed trojan (1,69 %)
6. Android/GriftHorse trojan (1,38 %)
7. Android/TrojanDownloader.Agent.YW trojan (1,13 %)
8. Android/Spy.Agent.BYH trojan (1,09 %)
9. Android/TrojanDropper.Agent.GKW trojan (0,70 %)
10. Android/TrojanDropper.Agent.GLC trojan (0,69 %)

zdroj: AVcentrum ČR