

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **21** ze dne **3.11.2022**

Hrozby pro Android: Útočníci maskují malware k nepoznání, v září zneužívali hry nebo titulky k filmům

Adware Andreed zůstává nejčastějším škodlivým kódem pro platformu Android v České republice. Nadále se šíří především prostřednictvím mobilních her – v září ho útočníci maskovali především za hru The Battle of Polytopia. Mezi škodlivými kódy se tentokrát objevil dropper Agent.KEQ, který nepozorovaně provádí průzkum v chytrém telefonu, aby na něj mohli útočníci zacílit daleko složitějším malwarem. V září byl po delší odmlce znovu detekován také adware Hiddad, který se také dokáže nepozorovaně skrýt v zařízení a opět zobrazuje agresivní reklamu nebo dokáže uživatele odvést na nebezpečné webové stránky. Bezpečnostní experti tak varují především před výhodnými nabídkami známých nástrojů a her ke stažení mimo oficiální obchod Google Play.

Adware Andreed zůstává nadále nejčastěji detekovaným škodlivým kódem v Česku – v září se objevoval ve více než pětině všech případů. Ačkoli adware nepatří mezi stejně závažné hrozby, jako je například spyware nebo ransomware, a zobrazuje ve většině případů především agresivní reklamu, i on může být rizikem. Často se totiž zaměřuje na informace o našem chování na internetu, může stáhnout do zařízení daleko škodlivější malware anebo nás přesměrovat na podvodné webové stránky.

„Již několik měsíců pozorujeme v případě adwaru Andreed stejnou strategii – útočníci adware distribuují prostřednictvím jednoho obchodu třetí strany, kde ho mohou uživatelé stáhnout v domnění, že stahují nějakou mobilní hru. Verze těchto her ale nejsou oficiální a i přesto, že se hra může standardně spustit a fungovat, jejím hlavním úkolem je zobrazovat uživateli reklamu,“ vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Adware Andreed se již v minulých měsících šířil například prostřednictvím falešných verzí her Buddy Toss, Chuchel či House Designer: Fix & Flip. V září se pak šířil prostřednictvím neoficiální verze hry The Battle of Polytopia.

Útočníci škodlivý kód co nejvíce maskovali

Bezpečnostní experti již v srpnu upozornili na proměňující se prostředí kybernetických hrozeb pro platformu Android v Česku. V září se pak nově mezi nejčastější škodlivé kódy vyšplhal dropper Agent.KEQ.

„Dropper, tedy škodlivé kódy, jejichž úkolem je do zařízení dopravit skrytě další malware, jsme na předních místech v naší pravidelné statistice nějakou dobu nevidali,“ říká Jirkal. *„Dropper Agent.KEQ jsme v září detekovali v desetině všech případů. Jedná se o velmi jednoduchý škodlivý kód, jehož úkolem je stáhnout do zařízení jiný, složitější malware. Útočníci ho využívají k tomu, aby si udělali v zařízení nejdříve průzkum a zjistili, jakým dalším škodlivým kódem se jim vyplatí útočit. V tom je tento dropper právě nebezpečný. Podle našich dat vše také napovídá tomu, že dropper uživatelé nepoznají podle žádné ikony, v tomto případě se nevydává za žádnou známou aplikaci. Naopak se pravděpodobně šíří prostřednictvím podvodných webových stránek pro stahování nelegálního obsahu. V několika případech se dokonce vydával za filmové titulky,“* dodává Jirkal.

V jednotkách procent případů se v září objevil také trojský kůň Hiddad.AYF. Jedná se o adware, který patří do větší rodiny malwaru Hiddad. V Česku se škodlivý kód z této rodiny objevoval také minulý rok na podzim.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **21** ze dne **3.11.2022**

„Malware Hiddad zobrazuje reklamu skrytým způsobem – to znamená, že uživatel prakticky nemá možnost zjistit, ze které aplikace se daná reklama zobrazuje. Spustí reklamu jako externí službu a uživatel nevidí žádnou ikonu v telefonu nebo aktivitu na pozadí systému,“ vysvětluje Jirkal. „Hiddad.AYF byl aktivní hlavně koncem září a uživatelé ho mohli stáhnout v domněnku, že stahují různé nástroje na modifikace chytrého telefonu, jako je například změna pozadí hlavní obrazovky, nebo přizpůsobení podoby obrazovky při volání.“

Experti varují: Blíží se hlavní sezóna mobilního malwaru

Bezpečnostní experti upozorňují, že s blížícím se koncem roku a obdobím svátků a prázdnin můžeme opět čekat zvýšenou aktivitu kybernetických útočníků.

„Útočníci využívají sezóny ke konci roku k šíření adwaru a dalších škodlivých kódů pravidelně. Mohou tak nejvíce využít svou strategii, kdy na uživatele, kteří bývají v tuto dobu více aktivní na svých mobilních telefonech, lákají na výhodné stažení známých her či jejich modifikací s různými cheaty neboli herními výhodami pro hráče. Výjimkou nejsou ani výhodné nabídky dalších prémiových placených programů. Nabízejí je buď úplně zdarma, nebo v balících s dalším softwarem a nejčastěji na ně můžete narazit v různých neoficiálních obchodech s aplikacemi,“ říká Jirkal z ESETu.

Uživatelé se nejlépe vyhnou malwaru a adwaru ve svých zařízeních s platformou Android tím, že budou všechny aplikace a programy stahovat pouze z oficiálního obchodu Google Play. Nejen před sofistikovaným malwarem, ale také před odkazy na různé podvodné stránky je ochrání kvalitní bezpečnostní software.

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

- Android/Andreed trojan (24,38 %)
- Android/TrojanDropper.Agent.KEQ trojan (10,73 %)
- Android/Hiddad.AYF trojan (4,92 %)
- Android/TrojanDropper.Agent.JDU trojan (4,40 %)
- Android/TrojanDropper.Agent.FHG trojan (4,10 %)
- Android/Spy.Cerberus trojan (3,75 %)
- Android/Triada trojan (3,46 %)
- Android/Agent.CZB trojan (2,17 %)
- Android/TrojanDropper.Agent.GKW trojan (2,05 %)
- Android/Spy.Agent.CAG trojan (1,93 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: ESET