Polsko a Česko se v březnu ocitly pod útokem, zdrojem malwaru byly opět hlavně škodlivé mobilní hry

23.4.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Evropě i v březnu kralovaly škodlivé kódy z rodiny malwaru Hiddad, které bezpečnostní experti řadí podle jejich funkcí k tzv. reklamnímu malwaru. Terčem škodlivých kampaní bylo tentokrát nejvíce Polsko a Česká republika. Upozorňují, že útočníci si mohou testovat vhodné regiony pro další zacílení svých útoků. Podobně jako v předchozích měsících se v čele pravidelné statistiky i v březnu udržel škodlivý kód Agent.FNM. Podle posledních informací bezpečnostních expertů mohou útočníci jeho pomocí napadnout nejen samotný chytrý telefon, ale také celou síť, ke které se připojuje. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Trojský kůň Hiddad se řadí ke škodlivému reklamnímu malwaru a na základě analýzy škodlivých kódů pro platformu Android byl za první čtvrtletí letošního roku nejčastěji detekovanou kybernetickou hrozbou v Evropě. Útočníci k jeho šíření využívají falešné verze mobilních her. I když je zpravidla velmi často mění, aby ztížili své odhalení, v případě trojského koně Hiddad i v březnu vsadili na škodlivou verzi RPG bojové hry Shadow Fight 2.

„Útočníci v případě trojského koně Hiddad v březnu primárně útočili na Polsko a Česko. Obecně byl březen měsícem, ve kterém vidíme zvýšený zájem útočníků o Českou republiku. Jednalo se sice o globálně zaměřené útoky v angličtině, útočníci si tím ale mohli něco testovat. Jakmile si vyhodnotí, že útoky na náš region jim mohou přinést kýžené zisky, strategie se může rychle změnit na lokálně cílené útoky na české uživatele a uživatelky," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Stále stejná verze škodlivé hry, kterou útočníci využívají k šíření škodlivého kódu, může podle bezpečnostních expertů poukazovat na to, že uživatelé nevěnují tolik pozornosti varovným ukazatelům, nebo hrozbu v podobě adwaru podceňují. Právě ale škodlivá reklama může být prvotní fází pro další typy útoků. Po kliknutí nás mohou útočníci odvést na nebezpečné webové stránky obsahující další škodlivé kódy nebo můžeme rovnou stáhnout již daleko nebezpečnější malware. Kromě toho bychom neměli zapomínat ani na to, že adware mohou útočníci využívat ke sledování našich aktivit na internetu. A ze získaných informací připravit další útoky.

Váš telefon se může stát součástí botnetu

V evropských zemích se v březnu nadále objevoval také škodlivý kód Agent.FNM. Strategií útočníků je maskovat jej za populární streamovací aplikace, jako je Netflix nebo Amazon Prime. V březnu pak útočníci zkoušeli zneužít také jména méně známých služeb, jako jsou StreamFire a SportsFire. Tyto útoky byly nejvíce pozorovány ve Španělsku nebo Německu, mimo EU pak také ve Velké Británii. Česká republika byla co do počtu případů osmou nejpostiženější zemí v rámci EU.

„Malware Agent.FNM je příkladem toho, že i mobilní telefony mohou útočníci využít ve větších útocích. Dávno určitě neplatí, že pro ně nejsou tak atraktivní jako notebooky a stolní počítače s tradičními operačními systémy. Cílem tohoto útoku je zneužít vaše zařízení, tedy chytrý mobilní telefon, k útokům na jiné cíle. Útočníci přidají vaše zařízení do takzvaného botnetu. Mohou tak získat přístup i k sítím, ke kterým se prostřednictvím telefonu připojujete, a to jak doma, tak například v

práci. Strategií útočníků je navíc škodlivou aplikaci po stažení v zařízení schovat, a tím si k němu zajistit dlouhodobý a nikým nepozorovaný přístup," doplňuje Jirkal.

Škodlivé aplikace a hry si najdou oběti i mezi dětmi

Jak bezpečnostní experti dlouhodobě sledují a upozorňují, obětmi útoků na platformu Android mohou být často i děti. Ať již mají děti svůj první chytrý telefon, nebo si na hraní mobilních her zatím půjčují ten rodičů, doporučují seznámit je se základy kybernetické bezpečnosti.

„Rizikem nejsou jen falešné verze nějakých složitějších strategických nebo bojových her pro platformu Android, útočníci zneužívají i velmi jednoduché aplikace nebo hry, kde můžeme předpokládat, že se k nim dostanou i děti. V březnu to byl případ další varianty škodlivého kódu z rodiny Hiddad, který se vyšplhal mezi tři nejčastější hrozby měsíce. V tomto případě šlo o jednodušší hru Single Line – Drawing Puzzle, ve které musí hráč najednou spojit všechny definované body a nakreslit zadaný tvar bez toho, aby zvedl prst z obrazovky. Je to typ hry, se kterou za vámi mohou přijít děti, že si ji chtějí stáhnout," říká Jirkal. „Osobně svým dětem nikdy nedovoluji, aby si instalovaly nějaké hry samy, i když samozřejmě záleží na jejich věku – větší kontrolu určitě doporučuji u žáků prvního stupně, zatímco u starších dětí už musíme předpokládat, že si na svém telefonu budou chtít stáhnout, co chtějí. Tak jako tak bych je co nejdříve naučil pečlivě procházet recenze jiných uživatelů a uživatelek a nestahovat hry, které nemají alespoň 100 hodnocení a převážně pozitivní recenze," dodává Jirkal z ESETu.

Pravidla mezi dětmi doporučují experti nastavit po vzájemné diskusi a dohodě. Rodiče s nimi například mohou uzavřít tzv. digitální dohodu, ve které společně nastaví pravidla bezpečného prohlížení internetu, frekvenci a dobu používání chytrých zařízení či hraní her nebo principy bezpečného využívání sociálních sítí.

Nejčastější kybernetické hrozby pro platformu Android v zemích EU za březen 2026:

1. Android/Hiddad.BDJ trojan (16,15 %)
2. Android/Agent.FNM trojan (11,57 %)
3. Android/Hiddad.BDM trojan (4,81 %)
4. Android/Andreed trojan (2,05 %)
5. Android/Triada trojan (1,94 %)
6. Android/Spy.Banker.BCX trojan (1,41 %)
7. Android/TrojanDownloader.Agent.BHA trojan (1,28 %)
8. Android/TrojanDropper.Agent.MZU trojan (1,12 %)
9. Android/Spy.Banker.BGB trojan (1,02 %)
10. Android/TrojanDropper.Agent.NAA trojan (1,02 %)

Uživatelé řešení ESET jsou před výše uvedenými typy hrozeb automaticky chráněni.

O společnosti ESET

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení digitální bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních

zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete 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.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/polsko-a-cesko-se-v-breznu-ocitly-pod-utokem-zdrojem-malwaru-byly-opet-hlavne-skodlive-mobilni-hry