Falešný Netflix ukrýval v únoru škodlivý kód, napadené mobilní telefony sloužily k dalším útokům

30.3.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

V případě platformy Android v Evropě kyberútočníci v únoru nevymýšleli žádné nové strategie svých kampaní. Nejčastějším malwarem zůstal trojský kůň Hiddad s funkcemi adwaru, a to včetně stejné falešné verze mobilní hry, jejímž prostřednictvím ho útočníci šířili již předchozí měsíc. Spolu s Německem a Polskem byla v únoru jeho nejčastější cílovou zemí Česká republika. Rizikem zůstal i škodlivý kód Agent.FNM, který útočníci vydávali za prémiovou verzi oblíbené streamovací služby Netflix. Jak bezpečnostní experti zjistili, kromě získání dat z napadených zařízení je cílem tohoto malwaru také zneužití telefonu oběti k dalším útokům. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

V únoru zůstal největší kybernetickou hrozbou pro platformu Android v Evropě adware. Konkrétně se opět jednalo o trojského koně Hiddad. Útočníci tentokrát nezměnili ani falešnou verzi hry, jejímž prostřednictvím škodlivý kód už od ledna šíří – i v únoru zvolili mobilní hru Shadow Fight 2 a svým obětem se snažili podstrčit její škodlivou verzi obsahující právě zmíněného trojského koně.

„Kromě mobilních her se trojský kůň opakovaně objevuje i ve falešných aplikacích k editování videí, zobrazování PDF souborů a v celé řadě podobných nástrojů. Všechny tyto aplikace se zpravidla objevují v méně známých obchodech třetích stran, proto je za mě nejdůležitější o tomto riziku vědět a předcházet mu – například tím, že aplikace a hry budeme vždy stahovat pouze z oficiálního obchodu s aplikacemi a budeme se vyvarovat různých pochybných webových stránek a úložišť. Taková opatrnost je určitě na místě, protože Česká republika byla v únoru spolu s Polskem a Německem nejvíce zasaženou zemí tímto škodlivým kódem," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Prémiová verze Netflixu ukrývala malware

Oproti minulému měsíci mírně vzrostl počet detekcí škodlivého kódu Agent.FNM, který se od nového roku drží v těsném závěsu za adwarem. Dle nejnovější analýzy bezpečnostní experti zjistili, že poté, co infikuje zařízení, přidá ho do tzv. botnetu. Největším rizikem je v Itálii a ve Španělsku, v několika procentech případů se však v únoru objevil i u nás, v České republice.

„Při poslední bližší analýze tohoto škodlivého kódu, který se v evropském regionu pohybuje již od konce minulého roku, jsme zase o něco více poodkryli jeho chování a motivace útočníků, kteří ho využívají. Cílem útočníků je zneužít vaše zařízení k útokům na jiné cíle, dokonce vaše zařízení mohou za tímto účelem ‚prodat' jiným útočníkům. Kromě mobilního telefonu mohou takto získat přístup i k sítím, ke kterým se připojujete, jak doma, tak například v práci. Podobně, jako v přechozích případech, útočníci škodlivý kód maskují za falešné verze streamovacích služeb. V únoru se nejčastěji jednalo o škodlivou verzi služby Netflix. Aplikaci nic netušící oběti stahovaly především v domnění, že si pořizují její prémiovou variantu," vysvětluje Jirkal.

Bezpečnostní experti společnosti ESET varují, že tento škodlivý kód nemusí běžní uživatelé a uživatelky v zařízení vůbec odhalit. Jak totiž zjistili, první týden po stažení se aplikace chová standardně a nevykazuje žádné škodlivé aktivity. Po uplynutí této doby se ale v zařízení skryje a

působí dojmem, že došlo k jejímu smazání. Díky této strategii pak mají útočníci zajištěný přístup k zařízení oběti bez toho, aniž by někdo pojal podezření.

Útočníci si krátí cestu k našim datům přes to, co nás baví

Také v případě třetího nejčastěji zachyceného únorového škodlivého kódu, trojského koně Triada, vsadili útočníci na populární aplikace, u kterých předpokládají, že je budou uživatelé a uživatelky nejvíce shánět a stahovat. Jednalo se o falešné verze nástrojů určených k práci s audio obsahem. Triada se v únoru nejvíce šířila Španělskem a Polskem, hned po těchto zemích ale byla nejčastěji přítomna i v Česku.

„Jakmile někde vidíte, že můžete získat něco výhodně či dokonce zdarma bez toho, aniž byste pro to něco museli udělat, měli byste zpozornět. Dnes nás vždy nějaká online služba bude něco stát – ať už přímo peníze, nebo uživatelská data, která dnes mají velkou cenu. To bychom měli mít vždy na paměti, pokud na nějakou takovou nabídku narazíme. Naše data v rukou kyberútočníků totiž můžou sloužit k přípravě dalších útoků nebo skončit na černém trhu, kde je může kdokoli další využít proti nám. Platit budeme v konečném důsledku vždy," říká Jirkal z ESETu.

Uživatelé a uživatelky by měli i v případě mobilního telefonu zvážit profesionální kyberbezpečnostní ochranu. Moderní bezpečnostní software je totiž dokáže kromě malwaru varovat i před potenciálně nechtěnými aplikacemi nebo nebezpečnými webovými stránkami. Společnost ESET navíc nyní přichází s časově omezenou akční nabídkou u svých řešení pro domácnosti a koncové uživatele. Od 25. března do 27. dubna 2026 nabízí prodlouženou dobu ochrany u nejprodávanější varianty ESET Home Security Premium. Nabídka je dostupná pro nové i stávající zákazníky napříč všemi prodejními kanály. Více informací najdou uživatelé a uživatelky na webových stránkách.

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

1. Android/Hiddad.BDJ trojan (16,91 %)
2. Android/Agent.FNM trojan (12,15 %)
3. Android/Triada trojan (2,34 %)
4. Android/Agent.EQD trojan (2,15 %)
5. Android/Andreed trojan (1,96 %)
6. Android/Hiddad.BDE trojan (1,77 %)
7. Android/Agent.FJL trojan (1,69 %)
8. Android/Spy.SpinOk trojan (1,66 %)
9. Android/Agent.FNP trojan (1,49 %)
10. Android/TrojanDropper.Agent.NAA trojan (1,39 %)

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