WhatsApp je opět ve službách kyberútočníků, tentokrát přes něj šíří škodlivý kód pro platformu Android

22.5.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Českou republiku a Polsko nadále zaplavují škodlivé verze mobilních her z neoficiálních zdrojů, které ukrývají trojské koně Hiddad. Vyplývá to z dubnové analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Vedle těchto kyberhrozeb zůstal v dubnu rizikem také malware Agent.FNM. Útočníci jej šíří maskovaný za škodlivé verze populárních streamovacích aplikací prostřednictvím chatovací platformy WhatsApp. Jeho cílem je přidat napadené zařízení do tzv. botnetu a zajistit útočníkům přístup nejen k zařízení, ale i k síti, ke které se připojuje.

Na platformě Android se v dubnu opakovala stejná situace jako předešlý měsíc – nejčastějšími kyberhrozbami byly trojské koně z malware rodiny Hiddad. Zatímco v případě škodlivého kódu Hiddad.BDJ útočníci zneužívali verzi mobilní hry Shadow Fight 2, u škodlivého kódu Hiddad.BDM se pak jednalo o verzi fotbalové hry FreeKick Legend: Goal. Právě škodlivé verze mobilních her z neoficiálních zdrojů slouží k zamaskování malwaru a jeho snazšímu stáhnutí samotnými uživateli.

„Ačkoli jsme na platformě Android v evropském regionu pozorovali prakticky totožné rozložení kybernetických hrozeb jako v březnu, je třeba zvlášť upozornit na dubnovou aktivitu škodlivého kódu Agent.FNM, který útočníci maskují za populární streamovací aplikace. Podle našich analýz se tento škodlivý kód šířil ve velkém přes chatovací aplikaci WhatsApp. Rád bych tak na uživatele a uživatelky apeloval, aby byly obzvláště opatrní, pokud jim odkaz k instalaci nějaké aplikace přijde touto cestou. O útočníky totiž může jít i v případě, kdy nám odkaz přijde od blízké osoby. Nikdy totiž nemáte jistotu, že se dotyčný či dotyčná také nestali obětí útočníka," varuje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Nejčastější případy útoků malwarem Agent.FNM zaznamenali bezpečnostní experti ve Španělsku a mimo EU také například ve Velké Británii. V České republice zatím evidují minimum případů. S ohledem na to, že se útok šíří přes oblíbenou komunikační platformu, se ale situace může dle nich rychle změnit. Jen v České republice podle jednoho z posledních průzkumů společnosti ESET používá aplikaci WhatsApp 89 % uživatelů a uživatelek. Jak průzkum také ale ukázal, kromě dvoufaktorové autentizace další bezpečnostní nástroje k zabezpečení našich konverzací spíše nevyužíváme. Malware Agent.FNM je přitom ve srovnání s trojským koněm Hiddad příkladem pokročilého škodlivého kódu. Napadené zařízení zneužije k útokům na jiné cíle prostřednictvím takzvaného botnetu. Útočníci tak mohou získat přístup i k sítím, ke kterým se prostřednictvím telefonu připojujeme, a to jak doma, tak například v práci.

Pro všechny nejčastěji zachycené dubnové škodlivé kódy na platformě Android v Evropě platí stejná kyberbezpečnostní doporučení – stahovat veškeré aplikace pouze z oficiálních obchodů. I zde se však vyplatí sledovat recenze a to, zda má aplikace nějakou doložitelnou historii svého fungování, například, že v obchodu není k dispozici jen krátce. Naopak aplikace z neoficiálních obchodů, veřejných fór či úložišť bývají s velkou jistotou upraveny útočníky.

„Jak u škodlivého kódu Hiddad.BDJ, tak u malwaru Agent.FNM jsme v dubnu viděli konstantní útoky rozložené rovnoměrně do celého měsíce. Jelikož se prakticky jedná o pokračování stejných kampaní, jako jsme pozorovali už v březnu, nemyslím si, že by tyto útoky v brzké době zcela vymizely," říká

Jirkal a dodává: „Ochranu mobilních telefonů míváme tendenci podceňovat, protože nám kybernetické hrozby pro platformu Android nepřijdou nijak závažné. Typicky lidé argumentují tím, že se jedná hlavně o adware, který je vedle ransomwaru nebo infostealerů prakticky neškodný. Není to ale pravda. Adware může figurovat ve větších a vícestupňových útocích, a i tento škodlivý kód dokáže sbírat informace o našem telefonu a chování na internetu. V případě malwaru Agent.FNM pak už určitě přichází na řadu zabezpečení moderním bezpečnostním softwarem," dodává Jirkal z ESETu.

Bezpečnostní software kontroluje stahované aplikace a v případě, že nějakou aplikaci nebo soubor rozpozná jako nebezpečný, stažení či spuštění aplikace zablokuje a umístí ji do karantény. Uživatelé jsou o tomto postupu vždy informováni samotným bezpečnostním programem.

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

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 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/eset-whatsapp-je-opet-ve-sluzbach-kyberutocniku-tentokrat-pres-nej-siri-skodlivy-kod-pro-platformu-android