Zneužívání NFC je při kyberútocích v Česku stále častější, ESET je připisuje jedné skupině útočníků

12.5.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Společnost ESET upozorňuje na nárůst výskytu škodlivého kódu NGate v České republice a na Slovensku, který cílí na uživatele zařízení s platformou Android. ESET na tuto hrozbu upozorňuje již od roku 2024, kdy kyberbezpečnostní experti odhalili malware pro Android schopný zneužít technologii NFC ke krádeži peněz z bankomatu. Aktuální telemetrická data společnosti ESET ukazují, že od října 2025 aktivita útočníků výrazně vzrostla a kampaně ve zvýšené míře pokračovaly i během prvních měsíců roku 2026.

Za první čtyři měsíce roku 2026 zaznamenala společnost ESET na zařízeních s platformou Android v Česku a na Slovensku více detekcí škodlivého kódu NGate než za celý rok 2025. Ještě výraznější rozdíl je vidět při meziročním srovnání stejného období – v prvních čtyřech měsících roku 2026 zaznamenala přibližně 15× více detekcí než ve stejném období roku 2025.

„NGate je příkladem hrozby, při které útočníci kombinují sociální inženýrství, škodlivý kód a zneužití důvěry uživatelů. Bez aktivní spolupráce oběti se NGate do zařízení nedostane. Přestože jsme na tuto hrozbu upozornili už v létě 2024, naše data ukazují, že útočníci v regionu Slovenska a Česka zůstávají aktivní a od října 2025 dokonce sledujeme výrazné zvýšení jejich aktivity," říká Lukáš Štefanko, bezpečnostní expert společnosti ESET, který škodlivý kód analyzoval.

Podle analýzy společnosti ESET nejde o náhodné nebo izolované incidenty. Útoky velmi pravděpodobně souvisejí s jedním aktérem nebo organizovanou skupinou. Přibližně 90 % detekovaných NGate aplikací komunikovalo se stejným serverem kontrolovaným útočníky a exfiltrovalo stejný typ dat včetně NFC tokenů.

Útok začíná telefonátem a manipulací oběti

Malware NGate se do zařízení oběti nedostane bez její aktivní spolupráce. Útoky jsou postavené především na sociálním inženýrství. V mnoha případech instalaci škodlivé aplikace předchází telefonát od útočníka, který se vydává za zaměstnance banky nebo jiné důvěryhodné instituce. Na konci roku 2025 útočníci například manipulovali své oběti, aby si stáhli do zařízení falešnou aplikaci České národní banky.

Útočník může oběť upozorňovat na údajný problém s bankovním účtem nebo tvrdit, že získala finanční prostředky, které je potřeba „převést" na platební kartu. Následně se ji snaží přesvědčit, aby si ručně nainstalovala aplikaci z falešné webové stránky nebo přes komunikační aplikace, jako jsou WhatsApp či Telegram.

V některých případech útočníci používají i aplikace pro vzdálenou správu zařízení. Oběť je nejprve navedena, aby si z oficiálního obchodu Google Play nainstalovala legitimně vypadající aplikaci pro vzdálený přístup. Po udělení oprávnění může útočník přímo v zařízení oběti nainstalovat NGate, aniž by uživatel plně chápal, co se v telefonu děje.

Falešné aplikace napodobují důvěryhodné služby

Podvodné aplikace se vydávají za legitimní finanční služby, nejčastěji za banky, státní instituce nebo kryptoměnové platformy. Jejich cílem je vyvolat důvěru a přesvědčit oběť, že komunikuje s oficiální službou nebo aplikací.

Po spuštění může škodlivá aplikace odeslat kontakty oběti na server útočníků. Zároveň může uživatele vyzvat, aby přiložil platební kartu k zadní straně smartphonu (kde se nachází NFC čip) a následně zadal PIN k platební kartě.

Zajímavým znakem některých detekovaných NGate aplikací bylo, že jejich název obsahoval jméno konkrétního uživatele místo názvu banky nebo služby. To naznačuje vysokou míru personalizace a cílenou manipulaci obětí.

„U těchto útoků je klíčová důvěra oběti. Útočníci se nespoléhají pouze na technickou stránku malwaru, ale především na přesvědčivý příběh, telefonickou manipulaci a vytvoření pocitu naléhavosti. Uživatel by nikdy neměl instalovat aplikaci na základě telefonátu ani přikládat platební kartu k telefonu na výzvu volajícího nebo neznámé aplikace," doplňuje Štefanko z ESETu.

Jak se chránit

- Nikdy neinstalujte aplikace na základě telefonátu. Banka po vás nebude chtít instalaci aplikace přes telefon ani manipulaci s platební kartou.
- Nepřikládejte platební kartu k telefonu na výzvu volajícího nebo jiné mobilní aplikace.
- Nevkládejte PIN platební karty do mobilní aplikace.
- Stahujte aplikace pouze z oficiálních obchodů, a i tam si ověřujte jejich vydavatele.
- Buďte obezřetní při telefonátech, které vytvářejí tlak, naléhavost nebo se se odvolávají na problém s účtem.
- Používejte spolehlivé bezpečnostní řešení pro mobilní zařízení.
- Funkci NFC mějte zapnutou jen tehdy, když ji skutečně používáte.

O společnosti ESET

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické 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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/zneuzivani-nfc-je-pri-kyberutocich-v-cesku-stale-castejsi-eset-je-pripisuje-jedne-skupine-utocniku