

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **146** ze dne **9.6.2026**

Zneužívání NFC je při kyberútocích (v Česku) stále častější.

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,“ uvedl 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.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **146** ze dne **9.6.2026**

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 nespolehají 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,“ doplnil Štefanko z ESETu.

AV centrum ČR