ESET objevil malware NGate, který útočníci využili k výběrům peněz z českých bankomatů

28.8.2024 - Lucie Mudráková | ESET software

Bezpečnostní experti společnosti ESET nově objevili a popsali malware NGate, který se stal součástí útoků na klienty českých bank. Útočníci tentokrát zkombinovali využití tohoto malwaru s technikami sociálního inženýrství a s phishingem.

Podle dat společnosti ESET stála za těmito útoky skupina, která na českém území působila od listopadu 2023 a malware pak zapojila do svých kampaní v březnu 2024. Analytici společnosti ESET se nicméně domnívají, že útoky jsou po zatčení jednoho z pachatelů aktuálně pozastaveny. Útočníci dokázali díky malwaru NGate a technologii NFC klonovat data přímo z fyzických platebních karet obětí a přenést je na zařízení útočníka. Ten pak mohl rovnou vybrat peníze obětí z bankomatů. ESET upozorňuje, že se jedná o první využití malwaru pro platformu Android s těmito funkcionalitami v praxi.

Odhalená útočná kampaň, která spadá do kategorie tzv. crimeware, cílila na klienty tří českých bank. Malware NGate má jedinečnou schopnost přenášet data z platebních karet obětí, a to prostřednictvím škodlivé aplikace nainstalované na jejich zařízeních s platformou Android. Útok mohl být proveden díky přenesení dat pomocí technologie NFC. Malware NGate kompromitoval nejdříve chytrý telefon a následně zkopíroval bankovní kartu na chytrý telefon útočníka, na kterém byl proveden tzv. root zařízení (prolomení omezení ze strany jeho výrobce). Hlavním cílem této kampaně bylo umožnit útočníkům neoprávněné výběry z bankovních účtů obětí, a to přímo z bankomatů. V případě, že by tento postup selhal, měli útočníci záložní plán – převést peníze z bankovních účtů obětí na jiné účty.

„Tento nový postup útoku s využitím technologie NFC jsme dosud neviděli v případě žádného dříve objeveného malwaru pro platformu Android. Je založen na nástroji NFCGate, který navrhli studenti na Technické univerzitě v Darmstadtu v Německu, aby dokázali zachytit, analyzovat nebo měnit přenos dat prostřednictvím technologie NFC. Proto jsme tuto novou rodinu malwaru pojmenovali NGate," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Oběti si stáhly a nainstalovaly malware NGate poté, co je útočníci lstí přiměli myslet si, že komunikují se svou bankou. Záminkou pro komunikaci bylo smyšlené napadení jejich zařízení. Ve skutečnosti samy oběti nevědomky nakazily svá zařízení malwarem, když si po kliknutí na podvodný odkaz v SMS zprávě, která je informovala o přeplatku na daních, stáhly a nainstalovaly škodlivou aplikaci.

Podle analytiků z ESETu malware NGate doposud nebyl dostupný v oficiálním obchodě pro platformu Android, Google Play. Nic netušící oběti útoku byly přes odkaz nasměrovány na stránky, které byly od oficiálního obchodu vizuálně jen těžko rozlišitelné.

Malware NGate souvisí podle zjištění společnosti ESET s phishingovými aktivitami útočníků, kteří působili v České republice od listopadu 2023. Tyto aktivity byly pravděpodobně pozastaveny po zatčení podezřelého, ke kterému došlo v březnu 2024, ve stejném měsíci, kdy útočníci do kampaní zapojili malware NGate. Analytici ze společnosti ESET nejdříve zjistili, že se útočníci zaměřili na klienty tří českých bank, a to již na konci listopadu. Malware k obětem doručili prostřednictvím krátkodobých domén, které byly vydávány za legitimní bankovní weby nebo oficiální mobilní

bankovní aplikace dostupné v obchodě Google Play. Ve stejném měsíci společnost ESET o svých zjištěních informovala postižené banky.

Útočníci v popsané kampani využili také potenciál progresivních webových aplikací (PWAs), které vydávali za zmíněné webové stránky bank nebo mobilní bankovní aplikace. Tuto strategii pak ještě zdokonalili použitím „vyšší“ verze PWA, kterou je WebAPK. Vrcholem operace bylo zapojení malwaru NGate.

ESET pak v březnu 2024 zjistil, že malware NGate je hostovaný na stejných doménách, ze kterých se dříve stahovaly již zmíněné škodlivé PWA kódy. Pokud napadení uživatelé malware NGate nainstalovali a spustili, zobrazila se jim falešná webová stránka, která po nich vyžadovala zadání bankovních údajů. Ty byly následně odeslány na server útočníka.

„Kromě těchto phishingových funkcí obsahuje malware NGate také nástroj NFCGate. Útočníci jej v tomto případě zneužili k přenosu dat mezi dvěma zařízeními – zařízením oběti a zařízením pachatele. Některé z funkcí malwaru přitom fungují pouze na tzv. rootnutých zařízeních. V tomto případě bylo však možné přenést data i z takto neupravených, standardních zařízení,“ vysvětluje Jirkal.

Malware NGate také vyzýval oběti k zadání citlivých informací, jako je bankovní identita, datum narození a PIN kód k jejich platebním kartám. Oběti byly vyzvány k tomu, aby na svých chytrých telefonech zapnuly funkci NFC. Poté měly přiložit svou platební kartu na zadní stranu svého chytrého telefonu, dokud škodlivá aplikace kartu nerozpoznala.

„Pro zajištění ochrany před tak složitými útoky je třeba zakročit zároveň proti phishingu, dalším technikám sociálního inženýrství a samotným škodlivým kódům pro platformu Android. Znamená to provádět kontroly URL adres webových stránek, stahovat aplikace pouze z oficiálních obchodů a bezpečně uchovávat PIN kódy – poslední dvě zmíněná opatření přitom mají ve svých rukách částečně samotní uživatelé. Dále je na místě samozřejmě i používání bezpečnostního řešení pro chytré telefony, vypínat funkci NFC, když ji zrovna nevyužíváme a používat případně také ochranná pouzdra na telefony nebo virtuální karty vyžadující naše ověření,“ radí Jirkal z ESETu.

Kyberbezpečnostní hrozbu v podobě malwaru NGate a phishingových útoků analyzovali bezpečnostní experti společnosti ESET poskytující profesionální služby kybernetické bezpečnosti velkým společnostem. Podrobnější technické informace a popis fungování malware NGate najdete v článku na webu welivesecurity.com.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze,

celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-objevil-malware-ngate-ktery-utocnici-vyuzili-k-vyberum-penez-zceskych-bankomatu