ESET: Severokorejští útočníci se zaměřili na IT vývojáře, nabízejí falešné pracovní nabídky a cílí na kryptoměny

24.2.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Výzkumní analytici kyberbezpečnostní společnosti ESET nově popsali aktivity skupiny útočníků, kterou nazvali DeceptiveDevelopment. Útočníci se v těchto případech vydávají za náboráře a své oběti z řad vývojářů softwaru lákají na falešné pracovní nabídky. Obětem se snaží „podstrčit" soubory s projektem k vypracování v rámci domnělého výběrového řízení, ty ale obsahují škodlivé kódy určené ke krádežím informací a kyberšpionáži. Cílem útočníků je finanční zisk, a to konkrétně získání přístupových údajů do kryptoměnových peněženek obětí. Aktivity skupiny se po technické stránce podobají operacím, za kterými stojí útočné skupiny napojené na Severní Koreu, v tuto chvíli však nejsou připisovány žádné známé skupině útočníků. Své oběti si útočníci vybírají globálně s účelem okrást co nejvíce lidí. Odhalené aktivity pozorovali experti z ESETu také v Česku.

Kyberbezpečnostní analytici společnosti ESET pozorují sérii popsaných aktivit již od roku 2024. Oběťmi útoků jsou nezávislí vývojáři softwaru, které se útočníci snaží manipulovat prostřednictvím spearphishingových útoků. Nabízejí obětem falešné nabídky práce na pracovních platformách a webových stránkách. Cílem je odcizit přístupové údaje do jejich kryptoměnových peněženek a další přihlašovací údaje uložené ve webových prohlížečích a specializovaných programech pro správu hesel, tzv. správcích hesel.

„Útočníci z DeceptiveDevelopment v rámci falešného pracovního pohovoru od svých obětí požadují, aby absolvovali test programování. Mají například přidat funkce do existujícího projektu. Soubory určené ke splnění tohoto úkolu jsou obvykle umístěny v soukromých repozitářích na GitHubu nebo na jiných podobných platformách. Nadšený kandidát na zajímavou pracovní pozici se ale v tomto případě setká se soubory obsahujícími malware. Jakmile soubor s projektem stáhne a spustí, dojde ke kompromitaci jeho zařízení," vysvětluje Matěj Havránek, výzkumný analytik z pražské pobočky společnosti ESET, který aktivity DeceptiveDevelopment objevil a analyzoval.

„Aby se útočníci dostali ke svým potenciálním obětem, vytvářejí falešné profily náborářů na sociálních sítích nebo zneužívají již existující profily. Geograficky své oběti nerozlišují a případy jejich aktivit evidujeme celosvětově. Několik desítek případů jsme zachytili také v České republice. Snaží se zacílit na co největší počet lidí, aby tím zvýšili pravděpodobnost zisku finančních prostředků a informací," doplňuje Havránek.

Taktiky, techniky a postupy skupiny DeceptiveDevelopment jsou podobné několika dalším známým operacím, které jsou spojovány s jinými severokorejskými útočníky. Útočníci z DeceptiveDevelopment cílí na vývojáře operačních systémů Windows, Linux a macOS. Kromě finančního zisku z krádeží kryptoměn může být jejich dalším cílem také kyberšpionáž.

Útočníci primárně využívají při svých škodlivých aktivitách dvě rodiny malwaru. Útok probíhá ve dvou fázích. V první fázi slouží škodlivý kód BeaverTail (infostealer a downloader) k odcizení přihlašovacích údajů z databází webových prohlížečů a ke stažení škodlivých kódů pro druhou fázi. V té pak útočníci zapojí škodlivý kód InvisibleFerret (infostealer, RAT), který obsahuje také funkce spywaru a tzv. zadních vrátek (backdooru). Poté, co dojde k napadení zařízení a odcizení cílových údajů, mohou útočníci do zařízení stáhnout také legitimní software AnyDesk pro vzdálenou správu a

monitorování. Pokud jim totiž zařízení oběti přijde dostatečně zajímavé, později se k němu vrátí, aby získali další data.

„Útočníci vydávající se za náboráře pak přímo oslovují své potenciální oběti na pracovních platformách a platformách pro freelancery, nebo tam zveřejňují falešné pracovní nabídky. Zatímco některé profily útočníci sami vytvoří, v některých případech se jedná také o profily skutečných náborářů, nad kterými útočníci převzali kontrolu a upravili je pro své účely. Některé z těchto platforem jsou obecně určené k hledání a nabídkám práce, jiné se ale již primárně zaměřují na kryptoměnové a blockchainové projekty a jsou tedy více v souladu s cíli útočníků. Mezi platformy, na kterých útočníci operují, patří například známý LinkedIn a dále například Upwork, Freelancer.com, We Work Remotely, Moonlight a Crypto Jobs List," vysvětluje Havránek.

Oběti obdrží soubory s projekty buď přímo prostřednictvím přenosu souborů v rámci webových stránek, nebo prostřednictvím odkazu na repozitáře služeb GitHub, GitLab nebo Bitbucket. Útočníci instruují vývojáře k tomu, aby soubory stáhli, přidali do projektů funkce či opravili chyby a následně domnělému náboráři dali vědět o dokončení požadovaného úkolu. Kromě toho po nich útočníci také chtějí, aby upravený soubor spustili a tím otestovali. Právě v této části útočného scénáře dojde k nakažení zařízení škodlivými kódy. Útočníci k tomu, aby ukryli škodlivé kódy v souboru s projektem, využívají chytrý trik – umístí je do jinak neškodné části souboru, obvykle do kódu, který nijak s úkolem nesouvisí a zůstává skrytý.

„Útočníci z DeceptiveDevelopment jsou další skupinou, která svými postupy a technikami doplňuje a rozšiřuje řady aktérů napojených na režim v Severní Koreji. Jejich aktivity jsou také v souladu s pokračujícím trendem, kdy se pozornost útočníků přesouvá z tradičních peněz na kryptoměny," uzavírá Havránek z ESETu.

Podrobné technické informace o skupině útočníků DeceptiveDevelopment najdete 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.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

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.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-severokorejsti-utocnici-se-zamerili-na-it-vyvojare-nabizeji-falesne-pracovni-nabidky-a-cili-na-kryptomeny