Cílem severokorejských hackerů se stali vývojáři dronů ve střední a jihovýchodní Evropě

27.10.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Podle nejnovějšího výzkumu společnosti ESET se cílem severokorejské APT skupiny Lazarus stalo několik společností působících v obranném průmyslu v regionu střední a jihovýchodní Evropy. Některé jsou významně zapojeny do oblasti vývoje bezpilotních leteckých prostředků (UAV – unmanned aerial vehicle), kam spadají například také drony.

- APT neboli Advanced Persistent Threat je seskupení kybernetických útočníků, kteří se zaměřují na pokročilé přetrvávající hrozby. Obvykle pocházejí z řad státních organizací nebo organizací, které pracují na objednávku států.
- Útoky skupiny Lazarus na společnosti vyvíjející technologie UAV jsou v souladu s nedávno hlášenými pokroky v severokorejském programu vývoje dronů.
- Hlavním cílem útočníků byla pravděpodobně krádež obchodního tajemství a výrobního know-how.
- Na základě techniky sociálního inženýrství, kterou útočníci využili k získání počátečního přístupu, metody trojanizace open-source projektů z GitHubu a nasazení škodlivého kódu ScoringMathTea považují experti z ESETu tyto útoky za novou vlnu operace DreamJob skupiny Lazarus.

Výzkumní analytici z pražské pobočky společnosti ESET zaznamenali nový případ v rámci operace DreamJob. Jedná se o kampaň, kterou ESET sleduje v souvislosti s APT skupinou Lazarus napojenou na režim v Severní Koreji. Cílem nově objeveného útoku byly evropské společnosti působící v obranném průmyslu, z nichž jsou některé výrazně zapojeny do vývoje bezpilotních leteckých prostředků (UAV) – dronů. Tyto skutečnosti naznačují, že operace může souviset se současným úsilím Severní Koreje rozšířit svůj program výroby dronů. Útoky postupně zasáhly tři společnosti působící v obranném sektoru ve střední a jihovýchodní Evropě. Útočníci získali počáteční přístup prostřednictvím využité metody sociálního inženýrství. Hlavním škodlivým kódem kampaně byl trojský kůň ScoringMathTea, který útočníkům poskytl plnou kontrolu nad kompromitovaným zařízením. Předpokládaným hlavním cílem útočníků bylo získat obchodní tajemství a výrobní know-how obětí.

„V případě operace DreamJob je poznávacím prvkem využité metody sociálního inženýrství lukrativní, ale falešná pracovní nabídka doplněná škodlivým kódem. Oběť obvykle obdrží podvodný dokument s popisem pracovní pozice a trojanizovanou čtečku PDF souborů pro jeho otevření. S vysokou mírou jistoty připisujeme tyto aktivity APT skupině Lazarus, zejména kvůli jejím kampaním známým jako operace DreamJob a také proto, že napadené sektory v Evropě – letectví, obrana či strojírenství – odpovídají cílům v předchozích případech této operace," vysvětluje Peter Kálnai, výzkumný analytik z pražské výzkumné pobočky společnosti ESET, který nejnovější útoky operace DreamJob objevil a analyzoval.

Tři napadené evropské organizace vyrábějí různé typy vojenského vybavení (nebo jeho částí), přičemž mnohé z nich jsou v současnosti nasazeny na Ukrajině v rámci vojenské pomoci z evropských zemí. V době zaznamenané aktivity operace DreamJob byli severokorejští vojáci

rozmístěni v Rusku, aby pomohli Moskvě odrazit ukrajinskou ofenzivu v Kurské oblasti. Je tedy možné, že útočníci měli zájem získat prostřednictvím operace DreamJob citlivé informace o některých západních zbraňových systémech, které jsou aktuálně využívány ve válce mezi Ruskem a Ukrajinou.

Napadené organizace se navíc podílejí na výrobě technologií, které Severní Korea vyrábí také a u nichž se může snažit zdokonalit vlastní návrhy a procesy. Zájem o know-how související s vývojem UAV odráží nedávné mediální zprávy, které naznačily, že Pchjongjang výrazně investuje v rámci vlastních kapacit pro výrobu dronů. Severní Korea se při rozvoji těchto aktivit silně spoléhá na reverzní inženýrství a krádež duševního vlastnictví.

„Na základě našich analýz je pravděpodobné, že operace DreamJob se přinejmenším částečně zaměřovala na krádež výrobního tajemství a know-how týkajícího se technologie UAV. Zmínka o dronech, kterou jsme zaznamenali v jednom zachyceném škodlivém kódu, tuto hypotézu významně potvrzuje," říká Kálnai. „Našli jsme důkazy, že jedna z napadených společností se podílí na výrobě nejméně dvou modelů bezpilotních leteckých prostředků, které jsou v současnosti nasazeny na Ukrajině a s nimiž se severokorejští vojáci mohli setkat na frontě. Tato společnost je také součástí dodavatelského řetězce pro pokročilé drony s jedním rotorem. Jedná se o typ letounu, který Pchjongjang aktivně vyvíjí," dodává.

Nejvýznamnějším vývojovým posunem je pro skupinu zavedení nových knihoven pro lepší vyhýbání se detekci. „Po dobu téměř tří let si skupina Lazarus udržuje konzistentní modus operandi, využívá svůj preferovaný hlavní škodlivý kód ScoringMathTea a používá obdobné metody trojanizace open-source projektů dostupných na GitHubu. Tato předvídatelná, ale účinná strategie poskytuje dostatek různých možností k obcházení bezpečnostní detekce, i když nestačí k zakrytí identity skupiny," doplňuje Kálnai z ESETu.

Hlavním škodlivým kódem je trojský kůň ScoringMathTea. Jeho první výskyt lze vysledovat do října 2022 k příspěvkům na VirusTotal z Portugalska a Německa, kde jej útočníci vydávali za pracovní nabídky od letecké společnosti Airbus. Jeho funkcionality ukazují na obvyklé nástroje skupiny Lazarus: manipulace se soubory a procesy, výměna konfigurace, sběr informací o systému oběti, otevření TCP připojení a provádění lokálních příkazů či stahování nových škodlivých kódů z kontrolního serveru. Podle ESETu byl škodlivý kód ScoringMathTea zaznamenán při útocích na indickou technologickou společnost v lednu 2023, polskou obrannou společnost v březnu 2023, britskou společnost pro průmyslovou automatizaci v říjnu 2023 a italskou leteckou společnost v září 2025. Zdá se, že jde o jeden z hlavních škodlivých kódů v kampaních v rámci operace DreamJob.

APT skupina Lazarus je aktivní nejméně od roku 2009. Má na svědomí známé incidenty, jako je například útok na společnost Sony Pictures Entertainment, kybernetické loupeže za desítky milionů dolarů v roce 2016, masivní rozšíření ransomwaru WannaCryptor (alias WannaCry) v roce 2017 a dlouhou historii útoků narušujících jihokorejskou veřejnou a kritickou infrastrukturu, a to nejméně od roku 2011. Americké organizace US-CERT a FBI tuto skupinu nazývají HIDDEN COBRA. Je aktivní ve všech třech pilířích současných kyberkriminálních aktivit: kyberšpionáži, kybersabotáži a snaze o finanční zisk.

Operace DreamJob je krycí název pro její kampaně, které se primárně opírají o metody sociálního inženýrství, konkrétně o falešné pracovní nabídky pro prestižní nebo vysoce profilované pozice. Její cíle spadají převážně do leteckého a obranného sektoru, následně cílí i na strojírenské a technologické společnosti či na sektor médií a zábavy.

Více informací o APT skupině Lazarus a nejnovější verzi operace DreamJob najdete na webových stránkách WeLiveSecurity.com.

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 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/cilem-severokorejskych-hackeru-se-stali-vyvojari-dronu-ve-stredni-a-jihovychodni-evrope