ESET: Ruské kybernetické útoky na Ukrajinu zesilují, útočníci nasadili nový ničivý wiper a zneužívají zranitelnosti

2.6.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Praha, 20. května 2025 — Společnost ESET zveřejnila svou nejnovější zprávu o aktivitách skupin útočníků zaměřených na pokročilé přetrvávající hrozby (APT). Jedná se o útočníky obvykle z řad státních organizací nebo organizací, které pracují na objednávku států. Během sledovaného období od října 2024 do března 2025 bezpečnostní experti z ESETu zjistili, že útočníci napojení na Rusko, zejména skupiny Sednit a Gamaredon, vedli agresivní kampaně zaměřené primárně na Ukrajinu a země EU. Skupina Sandworm, která je rovněž spojována s Ruskem, zesílila své ničivé operace proti ukrajinským energetickým společnostem a nasadila nový škodlivý kód typu wiper s názvem ZEROLOT. Útočníci napojení na Čínu pokračovali ve svých špionážních aktivitách. Ve sledovaném období se nadále zaměřovali na evropské organizace. Skupiny spojované s režimem v Severní Koreji rozšířily své kampaně, ve kterých využívají techniky sociálního inženýrství a falešné pracovní nabídky.

Kybernetické útoky Ruskem podporovaných skupin útočníků byly nejvíce intenzivní na Ukrajině. Nejaktivnější skupinou zaměřenou na Ukrajinu zůstala Gamaredon. Útočníci z tohoto uskupení vylepšili techniky maskování malwaru, tzv. obfuskaci (úpravy zdrojového kódu s cílem znemožnit jeho analýzu), a představili nástroj PteroBox určený ke krádeži souborů zasílaných přes službu Dropbox.

„APT skupinu Gamaredon sledujeme dlouhodobě. Jedná se o útočníky, kteří nevyužívají sofistikované nástroje, byť patří mezi státem podporované skupiny, které k tomu obvykle mají finanční prostředky. Spolupracují s další APT skupinou InvisiMole, která za ně tento nedostatek kompenzuje. Skupina Gamaredon se historicky specializovala především na Ukrajinu, i když v poslední době můžeme vidět rozšíření jejích aktivit i na státy NATO," říká Robert Šuman, vedoucí pražské výzkumné pobočky společnosti ESET. „Další nechvalně proslulá skupina napojená na Rusko, Sandworm, ve sledovaném období silně útočila na ukrajinskou energetickou infrastrukturu. Ta byla jejím cílem již několikrát v minulosti. V nedávných případech nasadila nový typ wiperu s názvem ZEROLOT. Útočníci k tomu účelu zneužili zásady skupiny – Group Policy – ve službě Active Directory u postižených organizací," dodává Šuman.

Skupina Sednit, známá také pod jmény FancyBear nebo APT28, zdokonalila zneužívání zranitelností ve webmailových službách. Ve sledovaném období tito útočníci rozšířili svou operaci RoundPress z platformy Roundcube i na služby Horde, MDaemon a Zimbra. Bezpečnostní experti z ESETu zjistili, že skupina úspěšně zneužila zero-day zranitelnost v e-mailovém serveru MDaemon (CVE-2024-11182) proti ukrajinským firmám. V několika případech skupina Sednit využila také cílené spearphishingové e-mailové kampaně. Ty jí posloužily jako návnada v útocích na obranné firmy v Bulharsku a na Ukrajině. Další skupina napojená na Rusko, RomCom, prokázala své pokročilé schopnosti tím, že zneužila zranitelnosti ve webovém prohlížeči Mozilla Firefox (CVE-2024-9680) a v operačním systému Microsoft Windows (CVE-2024-49039).

Útočníci napojení na Čínu pokračovali ve svých kampaních proti vládním a akademickým institucím. Útočníci s podporou Severní Koreje pak výrazně zintenzivnili své operace zaměřené na Jižní Koreu, přičemž se zvlášť soustředili na jednotlivce, soukromé firmy, ambasády a diplomatické pracovníky.

Čínská APT skupina Mustang Panda zůstala v rámci asijského regionu nejaktivnější. Jejími cíli byly vládní instituce a společnosti působící v oblasti námořní dopravy. V rámci těchto útoků skupina využívala trojského koně Korplug a škodlivá USB zařízení. Útočníci ze skupiny DigitalRecyclers pokračovali v útocích na vládní instituce zemí EU. Využívali při nich virtuální privátní síť KMA VPN a škodlivé kódy, tzv. zadní vrátka (backdoory) RClient, HydroRShell a GiftBox. Skupina PerplexedGoblin použila ve sledovaném období svůj nový špionážní backdoor proti vládní instituci ve střední Evropě. Společnost ESET tento škodlivý kód pojmenovala NanoSlate. Útočníci ze skupiny Webworm cílili na srbskou vládní organizaci prostřednictvím VPN sítě SoftEther.

„Uvedené případy dokazují, jak je mezi útočnými skupinami napojenými na Čínu v oblibě využívání VPN služeb. Obecně můžeme říct, že útoky na síťovou infrastrukturu, DNS nebo VPN služby a routery jsou jejich doménou. Často využívají techniku, které říkáme man-in-the-middle, díky které dokážou ovládnout nějaký klíčový síťový prvek. Mají také výhodu v tom, že mohou ovlivňovat klíčové síťové uzly v Číně, které jsou pod kontrolou tamějšího režimu, nikoli mezinárodních institucí. Útoky čínských skupin lze pozorovat po celém světě, včetně České republiky," říká Šuman z ESETu.

Útočníci napojení na režim v Severní Koreji byli obzvláště aktivní v kampaních, které slibovaly finanční zisk. Skupina útočníků DeceptiveDevelopment výrazně rozšířila oblasti, na které se zaměřuje, když k nalákání obětí využila falešné pracovní nabídky. Cílem byla krádež přístupových údajů do kryptoměnových peněženek a přihlašovacích údajů z webových prohlížečů a správců hesel. Skupina využívala inovativní techniky sociálního inženýrství k šíření škodlivého kódu WeaselStore určeného pro různé platformy a operační systémy.

Další významnou událostí mezi severokorejskými APT skupinami pak byla krádež kryptoměn na burze Bybit. FBI tento útok připsala skupině TraderTraitor. Součástí tohoto útoku byla kompromitace dodavatelského řetězce – konkrétně poskytovatele kryptoměnové peněženky Safe{Wallet}. Útok měl za následek ztrátu v přibližné hodnotě 1,5 miliardy dolarů (USD).

Ostatní skupiny napojené na Severní Koreu mezitím vykazovaly kolísání v intenzitě svých operací. Po citelném loňském poklesu se skupiny Kimsuky a Konni vrátily na začátku roku 2025 na obvyklou úroveň svých aktivit. Změnily však své zacílení. Místo na anglicky mluvící think-tanky, nevládní organizace a experty na KLDR se nyní zaměřují především na jihokorejské subjekty a diplomatický personál. Skupina Andariel se po roce nečinnosti znovu objevila na scéně spolu se sofistikovaným útokem na jihokorejskou firmu vyvíjející průmyslový software.

Zájem skupin napojených na Írán se nadále soustředil na oblast Blízkého východu. Jejich cíli byly převážně izraelské vládní instituce a organizace z oblasti výroby a inženýrství.

Společnost ESET kromě výše uvedených případů zaznamenala výrazný, celosvětový nárůst kybernetických útoků na technologické firmy, který je z velké části připisován zvýšené aktivitě výše zmíněné APT skupiny DeceptiveDevelopment.

Celé znění nejnovější zprávy ESET APT Activity Report určené pro širokou veřejnost najdete zde.

Informace sdílené v neveřejných zprávách jsou primárně založeny na vlastních telemetrických datech společnosti ESET. Data byla ověřena kyberbezpečnostními experty z výzkumných poboček společnosti, kteří připravují podrobné technické zprávy a pravidelné aktualizace o aktivitách konkrétních APT skupin. ESET APT Reports PREMIUM pomáhají organizacím, které mají za úkol chránit občany, kritickou národní infrastrukturu a cenná aktiva před kybernetickými útoky vedenými zločinci nebo státními aktéry. Více informací o ESET APT Reports PREMIUM a o poskytování kvalitního, v praxi využitelného taktického a strategického zpravodajství o kybernetických hrozbách, je k dispozici na stránce ESET Threat Intelligence.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení digitální 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 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, 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 TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-ruske-kyberneticke-utoky-na-ukrajinu-zesiluji-utocnici-nasadili-novy-nicivy-wiper-a-zneuzivaji-zranitelnosti