Ruští hackeři zaútočili na Polsko, cílem byla energetická infrastruktura

1.2.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Společnost ESET zveřejnila nejnovější informace o kybernetickém útoku, který koncem loňského prosince mířil na energetickou infrastrukturu Polska. Podle dostupných důkazů přisuzují experti útok APT skupině Sandworm, která má vazby na ruskou vojenskou rozvědku GRU. Jednalo se o škodlivý kód typu wiper, který je určený k ničení napadených dat a systémů a který byl společností ESET několikrát detekován na Ukrajině v době ruské invaze v únoru 2022. Kybernetický útok nebyl podle zatím dostupných informací úspěšný.

Podle zveřejněných informací byl polský energetický sektor na konci loňského roku terčem významného kybernetického útoku. Společnost ESET v souvislosti s tím potvrzuje, že zaznamenala pokus o kybernetický útok 29. prosince 2025.

Útočníci nasadili škodlivý kód typu wiper, který bezpečnostní experti z ESETu pojmenovali DynoWiper a dále jej analyzovali. Wiper je škodlivý kód, který není, na rozdíl například od ransomwaru, určený k finančnímu zisku. Jeho hlavním cílem je zničit klíčová data a systémy. V tuto chvíli bezpečnostní experti nemají informace o tom, že by byl kyberútok úspěšný a došlo tak k jakémukoli narušení fungování energetické infrastruktury země. Také situace v České republice, jako přímé sousední země Polska, je podle bezpečnostních expertů standardní.

„Na základě analýzy tohoto škodlivého kódu a souvisejících taktik, technik a postupů připisujeme útok s velkou pravděpodobností APT skupině Sandworm. Důvodem je výrazná podobnost s řadou předchozích útoků za použití wiperů, které jsme u této skupiny již v minulosti viděli. Termínem APT jsou označovány pokročilé trvalé hrozby. Jedná se o útočníky nebo skupiny útočníků, kteří získávají přístupy do počítačových sítí zpravidla významných soukromých či vládních organizací. V mnohých případech je jejich aktivita financována státy. Hackeři ze skupiny Sandworm jsou spojováni s ruskou vojenskou zpravodajskou službou GRU," říká Robert Šuman, vedoucí pražské výzkumné pobočky společnosti ESET.

Zatímco podrobnosti o zamýšleném dopadu tohoto útoku jsou stále předmětem vyšetřování, je důležité zdůraznit jeho načasování. Hackeři se rozhodli útok provést uprostřed zimy, 10 let od útoku organizovaného skupinou Sandworm proti ukrajinské energetické síti. V prosinci 2015 to byl tehdy vůbec první výpadek elektřiny způsobený malwarem, kdy skupina použila škodlivý kód BlackEnergy k získání přístupu ke kritickým systémům několika elektrických rozvoden. Následkem kyberútoku zůstalo přibližně 230 000 lidí několik hodin bez elektřiny.

Bezpečnostní řešení společnosti ESET detekují škodlivý kód DynoWiper jako Win32/KillFiles.NMO. Další detaily včetně indikátorů kompromitace uvedla společnost ESET do zpráv APT Activity Reports, které v rámci služby ESET Threat Intelligence poskytuje svým zákazníkům.

Bezpečnostní experti hrozbu nadále analyzují a v případě nových zjištění poskytnou další informace.

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/eset-rusti-hackeri-zautocili-na-polsko-cilem-byla-energeticka-infrastruktura