ESET: Hackeři spojovaní s ruskou FSB společně zaútočili na vysoce postavené ukrajinské cíle

23.9.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Výzkumní experti ze společnosti ESET odhalili první známé případy spolupráce mezi APT skupinami Gamaredon a Turla. APT skupina neboli Advanced Persistent Threat je uskupení kybernetických útočníků, kteří se zaměřují na pokročilé přetrvávající hrozby. Obvykle se jedná o kyberzločince z řad státních organizací nebo organizací, které pracují na objednávku států. APT skupiny Gamaredon i Turla jsou spojovány s hlavní ruskou zpravodajskou agenturou FSB a společně zaútočily na vysoce postavené cíle na Ukrajině.

Na napadených zařízeních nasadili útočníci ze skupiny Gamaredon širokou škálu nástrojů. V jednom případě byli díky nim útočníci ze skupiny Turla schopni vydávat své příkazy.

„V průběhu tohoto roku jsme detekovali aktivity skupiny Turla na sedmi zařízeních na Ukrajině. Vzhledem k tomu, že skupina Gamaredon kompromituje stovky, ne-li tisíce zařízení, se zdá, že útočníci z Turla mají zájem pouze o konkrétní cíle, pravděpodobně ty, které obsahují vysoce citlivé informace," říká Robert Šuman, vedoucí pražské výzkumné pobočky společnosti ESET.

V únoru 2025 bezpečnostní experti z ESETu zaznamenali spuštění backdooru Kazuar skupiny Turla prostřednictvím nástrojů PteroGraphin a PteroOdd skupiny Gamaredon, a to na zařízení na Ukrajině. Nástroj PteroGraphin útočníci využili k restartování backdooru Kazuar v3, a to pravděpodobně poté, co došlo k jeho pádu nebo se nespustil automaticky. Útočníci z Turla tedy nástroj PteroGraphin pravděpodobně použili jako metodu obnovy. Poprvé se tak podařilo propojit tyto dvě skupiny na základě technických indikátorů. V dubnu a červnu 2025 pak experti z ESETu zaznamenali, že backdoor Kazuar v2 útočníci nasadili pomocí nástrojů PteroOdd a PteroPaste patřících opět skupině Gamaredon.

Backdoor Kazuar v3 je nejnovější verze škodlivého kódu z malware rodiny Kazuar. Jedná se o pokročilý špionážní malware napsaný v programovacím jazyce C#, který, jak se ESET domnívá, používá výhradně skupina Turla. Poprvé jej kyberbezpečnostní specialisté objevili v roce 2016. Dalším malwarem, který nasadila v rámci zjištěných aktivit skupina Gamaredon, byly nástroje PteroLNK, PteroStew a PteroEffigy.

„Skupina Gamaredon je známá tím, že využívá spearphishing a škodlivé soubory LNK na ovladačích, které lze odinstalovat. Jeden z těchto vektorů s největší pravděpodobností použila při kompromitaci. S vysokou mírou jistoty věříme, že obě skupiny – každá samostatně napojená na FSB – spolupracují a že Gamaredon umožňuje skupině Turla počáteční přístup k jejím cílům," říká Šuman a dodává: „APT skupinu Gamaredon sledujeme dlouhodobě. Kromě nyní nově odhalené spojitosti se skupinou Turla spolupracuje například i s další APT skupinou InvisiMole, kde sledujeme podobný vzorec chování."

Jak již bylo zmíněno, obě skupiny jsou součástí ruské FSB. Podle Služby bezpečnosti Ukrajiny provozují skupinu Gamaredon důstojníci 18. centra FSB (známého také jako Centrum informační bezpečnosti) na Krymu, které je součástí kontrarozvědné služby FSB. Pokud jde o skupinu Turla, britské Národní centrum kybernetické bezpečnosti (NCSC) ji spojuje s 16. centrem FSB, což je hlavní ruská agentura signálového zpravodajství.

Z organizačního hlediska stojí za zmínku, že tyto dvě entity běžně spojované s APT skupinami Turla a Gamaredon mají dlouhou historii spolupráce, která sahá až do období studené války. Invaze na Ukrajinu v roce 2022 pravděpodobně tuto konvergenci posílila, přičemž data společnosti ESET jasně ukazují, že aktivity skupin Gamaredon a Turla se v posledních měsících zaměřují na ukrajinský obranný sektor.

APT skupina Gamaredon je aktivní nejméně od roku 2013. Je zodpovědná za mnoho útoků, převážně proti ukrajinským vládním institucím. APT skupina Turla, známá také jako Snake, je nechvalně proslulá kyberšpionážní skupina, která je aktivní nejméně od roku 2004, možná už od konce 90. let. Zaměřuje se především na vysoce postavené cíle, jako jsou vlády a diplomatické subjekty v Evropě, Střední Asii a na Blízkém východě. Je známo, že pronikla do významných organizací, jako byly Ministerstvo obrany (nyní války) Spojených států amerických v roce 2008 a švýcarská obranná společnost RUAG v roce 2014.

Podrobnější analýzu a technický rozbor interakcí APT skupin Turla a Gamaredon najdete na webových stránkách www.welivesecurity.com. Informace o fungování APT skupin najdete také v podcastu RESET.

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-hackeri-spojovani-s-ruskou-fsb-spolecne-zautocili-na-vysoce-postavene-ukrajinske-cile