Operace Endgame: Experti z českého ESETu se podíleli na zásahu proti botnetu Amadey a infostealeru Stealc

29.6.2026 - Lucie Mudráková | ESET software

Společnost ESET se zapojila do koordinované globální operace, jejímž cílem bylo narušit aktivity botnetu Amadey a infostealeru Stealc.

- Úkolem operace bylo zabavit nebo vyřadit z provozu všechny známé kontrolní a řídicí servery (C&C) obou malwarů, a tím přímo narušit infrastrukturu, na níž jsou útočníci v ekosystému MaaS (Malware-as-a-Service) závislí.
- Experti z českých výzkumných poboček poskytli svým partnerům technickou analýzu, statistická data, seznam známých kontrolních serverů, šifrovací klíče, identifikátory kampaní a další informace.
- V podrobnější zprávě pak experti nabízí přehled o fungování těchto rodin malwarů a jejich partnerů v ekosystému MaaS.

Praha, 29. června 2026 – Bezpečnostní experti z českých poboček společnosti ESET pomohli narušit aktivity botnetu Amadey a infostealeru Stealc. V rámci globální Operace Endgame poskytli svým partnerům technickou analýzu a informace o infrastruktuře a partnerské síti obou škodlivých kódů. Útočníci je provozují v ekosystému MaaS (Malware-as-a-Service), kdy malware nabízejí k zakoupení na černém trhu potenciálním zájemcům (svým budoucím partnerům). Mezinárodní operaci koordinovalo oddělení Microsoft Digital Crimes Unit (DCU) ve spolupráci se společnostmi BitSight, Lumen a Mitsui Bussan Secure Directions (MBSD). Operace byla zaměřena na veškerou známou síťovou infrastrukturu, kterou útočníci využívali, s cílem ochromit jejich kyberkriminální aktivity. Současně s tím v rámci této operace vyšetřovalo infostealer Stealc také Evropské centrum pro boj proti kyberkriminalitě (EC3) při Europolu, a to společně s evropskými orgány činnými v trestním řízení, včetně německého Spolkového kriminálního úřadu či nizozemské a dánské státní policie, a společnostmi IBM nebo Proofpoint.

Z dat telemetrie společnosti ESET vyplývá, že botnet Amadey působil globálně bez výrazného regionálního zaměření. Nejvyšší míru detekcí experti zaznamenali v Indii, Turecku, Egyptě, Mexiku a Španělsku. Infostealer Stealc se také šířil globálně bez specifického regionálního zaměření. Nejvyšší míra detekcí pak byla zaznamenána ve Spojených státech, Polsku a Itálii.

„Společnost ESET sleduje botnet Amadey i infostealer Stealc již tři roky. Pro potřeby této operace jsme sdíleli statistiky pokrývající období od čtvrtého čtvrtletí roku 2025 do prvního pololetí 2026, a to spolu s technickými indikátory a konfiguračními daty získanými ze zpracovaných vzorků malwaru," vysvětluje Jakub Tomanek, bezpečnostní expert z pražské pobočky společnosti ESET, který se na operaci podílel. „Vzorky škodlivých kódů Amadey a Stealc analyzovaly naše automatizované systémy a identifikovaly data, která jsou nejrelevantnější pro sledování ve velkém měřítku. Patří mezi ně C&C servery, identifikátory verzí malwaru, šifrovací klíče, URL adresy, identifikátory kampaní a další hodnoty, které malware využívá pro komunikaci s infrastrukturou kontrolovanou útočníky," dodává.

Díky tomuto sdílení informací mohly orgány činné v trestním řízení s vysokou mírou jistoty identifikovat, prioritizovat a podnikat kroky proti infrastruktuře útočníků.

Byznys na dark webu

Amadey je modulární malware typu loader. Jeho hlavním účelem je distribuovat další škodlivý kód do kompromitovaných systémů, přičemž nabízí také moduly pro exfiltraci dat a získání vzdáleného přístupu. Stealc je naopak typickým infostealerem, který jeho autoři nabízejí v podobě služby dalším útočníkům. Zaměřuje se na přihlašovací údaje, soubory cookies, kryptoměnové peněženky, rozšíření prohlížečů a další soubory, které si útočníci určí.

Autoři obou rodin malwaru je nabízejí jako službu a propagují na darknetových fórech. V obou ekosystémech získávají jejich zájemci (partneři) administrativní panel, který si mají nasadit v rámci vlastní serverové infrastruktury. To od nich vyžaduje určitou míru technických dovedností, a zároveň jim to poskytuje přímou kontrolu nad daty obětí a distribucí malwaru.

O tom, jakou metodou budou malware šířit, rozhodují jednotliví partneři. Data společnosti ESET konzistentně poukazují na to, že oba škodlivé kódy byly distribuovány přes široký výběr kanálů. Nejčastějšími způsoby šíření byly falešné aktualizace softwaru, instalátory cracknutých programů a škodlivé loadery třetích stran.

Malware za příplatek nebo jako předplatné

Botnet Amadey fungoval tak, že si partneři zakoupili licenci a následně platili další poplatek při každém vytvoření nové verze malwaru (například při přechodu na nový kontrolní server). Jeho provozovatelé tedy neposkytovali partnerům nástroj pro tvorbu nových verzí malwaru. Vzorky škodlivého kódu byly na vyžádání kompilovány zvlášť pro každého partnera. Služba nabízí tři moduly pro další exfiltraci dat a získání přístupu: modul pro sledování schránky (clipboardu), modul pro krádež přihlašovacích údajů a modul vzdáleného přístupu. Cena služby činí 600 USD v bitcoinech za jednu licenci, přičemž za každou novou verzi malwaru se účtuje dalších 50 USD.

Provozovatelé infostealeru Stealc zvolili k partnerům přívětivější přístup a v rámci předplatného nabízeli neomezené generování verzí malwaru. To snižovalo provozní náklady spojené s obměnou infrastruktury a usnadňovalo partnerům vytváření nových vzorků podle potřeby. Infostealer se zaměřuje na širokou škálu zdrojů dat, včetně přihlašovacích údajů uložených ve webových prohlížečích, e-mailových klientech, FTP klientech, herních platformách, souborů kryptoměnových peněženek a rozšíření prohlížečů. Stealc se prodává ve formě předplatného, přičemž nejlevnější varianta stojí 1 000 USD na šest měsíců.

Bezpečnostní experti z českého ESETu budou i nadále sledovat oba malwary a monitorovat případné pokusy o obnovu jejich operační infrastruktury.

Více informací

Více podrobností o Operaci Endgame a škodlivých kódech najdete také v článku na webu welivesecurity.com.

O společnosti ESET

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

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.

Kontakt pro media:

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/operace-endgame-experti-z-ceskeho-eset u-se-podileli-na-zasahu-proti-botnetu-amadey-a-infostealeru-stealc