ESET: Vrátil se škodlivý kód Agent Tesla, v srpnu předcházel masivnímu útoku na naše data

11.9.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Zatímco kybernetickou hrozbou číslo jedna pro počítače s operačním systémem Windows v Česku nadále zůstává infostealer Formbook, bezpečnostní experti v srpnu zaznamenali nezvyklý návrat nechvalně proslulého škodlivého kódu Agent Tesla, který rovněž spadá do kategorie infostealerů. Útoky na sebe nápadně navazovaly a pravděpodobně za nimi mohli stát ti stejní útočníci. Přílohy e-mailů, kterými se škodlivé kódy šíří do zařízení obětí, měly tentokrát názvy nejen v angličtině, ale také v češtině. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Podobně jako v předchozím měsíci, i v srpnu útočníci využili k šíření infostealeru Formbook malware Agent.ECK. Strategii, ve které si na pomoc vezmou další škodlivé kódy, zapojili v případě aktuálně nejaktivnějšího infostealeru v Česku již několikátý měsíc po sobě.

„Velmi silnou útočnou kampaň jsme tentokrát pozorovali již na začátku minulého měsíce, tedy 5. srpna. V tomto hlavním útoku se objevovaly infikované e-mailové přílohy, kterými se infostealer dlouhodobě šíří do našich e-mailových schránek, pouze s názvy v angličtině. V samotném e-mailu bylo minimum textu. Na konci srpna se však opět objevily e-mailové přílohy s názvy v češtině. Útočníci stále zkoušejí to samé – svým obětem zasílají domnělé účtenky a potvrzení o platbách. Cílem jsou naše data a přihlašovací údaje, která lze dobře zpeněžit na černém trhu a využít v přípravě dalších útoků," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Velký návrat sledovali bezpečnostní experti v srpnu u infostealeru Agent Tesla. Tento škodlivý kód patřil v několika uplynulých letech k předním zbraním hackerů nejen v útocích na Českou republiku. Autoři tohoto škodlivého kódu však na konci loňského roku oznámili ukončení jeho vývoje a postupně jej začal nahrazovat jiný malware, například již zmíněný Formbook.

„Ačkoli se infostealer Agent Tesla vrátil na přední místa naší pravidelné statistiky pro operační systém Windows v Česku, jedná se stále o historickou verzi útoku, nikoli o nový typ. Většina kvalitních a moderních bezpečnostních řešení by si s ním tak měla poradit," vysvětluje Jirkal a dodává: „Jak jsme nicméně při bližší analýze odhalili, útoky s použitím infostealeru Agent Tesla probíhaly těsně před velkými útoky infostealeru Formbook na začátku srpna. Pak proběhlo ještě několik útoků vždy na začátku jednotlivých srpnových týdnů, a po nich vždy následovaly, i když už méně silné, útoky infostealerem Formbook. Domníváme se tak, že útočné kampaně mohly být vzájemně propojeny a že za nimi stála jedna útočná skupina."

Zatímco v červenci zůstali útočníci hlavně u angličtiny, v srpnu už začali opět zapojovat české překlady názvů e-mailových příloh. Na infostealer Formbook jsme mohli v srpnu narazit například v přílohách „FULL - TG 517.exe" v e-mailech s předmětem „Additional DOCUMENTS BOOKING". V menší míře se pak objevovaly přílohy s názvy „Účtenka.exe" s předmětem e-mailu „Toto je potvrzení o platbě za fakturu 73936 zaplacenou dne 28.10.2021". V případě infostealeru Agent Tesla se mohli lidé v Česku setkat s přílohami s názvy „RFQ_AUGUST 254524_PDF.exe" či „Your Leave_For Mid Year_Till _Decembre 2025 JPG.exe". Infostealer SnakeStealer se nejvíce ukrýval v přílohách „Statement of Account 2025.zip" nebo „kopie platby09886673.exe".

„Riziko, že nechtěně otevřeme škodlivou přílohu, může být poměrně veliké, i když si třeba říkáme, že dáváme pozor. Zvlášť to třeba hrozí v případě, že očekáváme větší množství zásilek, nebo denně odbavíme velké množství e-mailů obchodního charakteru. Řada těchto příloh se navíc tváří neškodně, jako soubory MS Office, PDF nebo obrázky. Příloha upozorňující na spustitelný podezřelý soubor, tedy .exe, nemusí být na první pohled v dlouhém názvu viditelná. S ohledem na přetrvávající přítomnost infostealerů v našem regionu doporučujeme maximální obezřetnost a zvážit i profesionální ochranu našich dat," doplňuje Martin Jirkal z ESETu.

Spolehlivou pojistkou před nechtěným otevřením škodlivé přílohy a vpuštěním škodlivého kódu do zařízení je bezpečnostní software. Moderní řešení dokáže vytvořit bezpečnou složku, do které zjištěnou hrozbu v e-mailu přesune. Uživatelé si poté mohou e-mail ve složce v případě zájmu prohlédnout a následně jej smazat. Společnost ESET svá řešení nyní nabízí v akci 3za2 – od 1. září do 31. prosince 2025 mají zákazníci z řad domácností i firem možnost získat tříleté předplatné za cenu dvou let. Více informací o kampani, včetně seznamu konkrétních řešení a podrobných podmínek, najdete na webových stránkách společnosti ESET.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

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

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-vratil-se-skodlivy-kod-agent-tesla-v-srpnu-predchazel-masivnimu-utoku-na-nase-data