ESET: Cílem trojského koně CloudEye bylo v listopadu Česko, stál za čtvrtinou detekcí pro operační systém Windows

9.12.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Téměř za čtvrtinou všech zachycených případů škodlivého kódu pro operační systém Windows v Česku stál tentokrát trojský kůň CloudEye. V kontextu této proměny v čele pravidelné statistiky zaznamenali bezpečnostní experti významnější oslabení infostealeru Formbook, ale i znepokojivý nárůst případů infostealeru Agent Tesla, jehož vývoj přitom útočníci na konci loňského roku ukončili. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET. I v případě trojského koně CloudEye platí pro uživatele a uživatelky bezpečnostní doporučení pro práci s jejich příchozí elektronickou poštou. Experti mimo jiné také upozorňují na důležitost pravidelných aktualizací, jejichž ignorování může i starým verzím škodlivého kódu umožnit vstup do našich zařízení.

Podle bezpečnostních expertů z ESETu začíná trojský kůň CloudEye pomalu získávat mezi útočníky celosvětovou popularitu. Jak upozorňují, dříve evidovali tento škodlivý kód pod označením GuLoader, před kterým ESET varoval například na jaře roku 2023. V letošním listopadu byl v Česku detekován ve větších kampaních hned dvakrát – nejdříve jako škodlivý kód Agent.QMG a podruhé jako CloudEye. Jedná se o stejný malware, který pod různými verzemi útočníci zkoušeli doručit nebezpečnými e-maily do zařízení obětí.

„Škodlivý kód, který označujeme jako CloudEye, není v Česku novinkou. V takové míře jsme jej ale nějakou dobu v našem prostředí neviděli. Za listopad jeho detekce povyskočily téměř na čtvrtinu všech případů škodlivých kódů pro operační systém Windows," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. „Přítomnost tohoto škodlivého kódu v Česku není dobrou zprávou. Opět nám to ukazuje, že útočníci chtějí aktuální období před koncem roku maximálně vytěžit ve svůj prospěch. Jedná se o velmi sofistikovaný malware, který je přizpůsobený k tomu, aby nešel tak snadno analyzovat. Jeho primární funkcí je stahovat do zařízení další škodlivé kódy. V Česku to vždy byly hlavně infostealery Agent Tesla a Formbook, které se v listopadu také objevily na předních místech naší statistiky," doplňuje Jirkal.

Stejně jako v předchozích měsících si útočníci vybrali po sobě dva jdoucí týdny, ve kterých se plně soustředili na šíření malwaru CloudEye. Útoky byly přizpůsobeny českým uživatelům a uživatelkám. Nejčastěji jsme mohli na tento malware narazit při spuštění e-mailové přílohy „PO_54333677011_678978687_Žádná recenze.vbs". Samotný e-mail pak útočníci vydávali za shrnutí objednávky. Dále se objevovaly také přílohy „Zmluva-pdf.js" či „NV11036587-, Predpis_pojistne_smlouvy_c_3268222706.bat".

Ačkoli se v tuto chvíli jedná o jiný škodlivý kód, než je standardně infostealer Formbook, obrana zůstává dle kyberbezpečnostních expertů stejná – kromě využívání kvalitního bezpečnostního programu je důležitá také preventivní ostražitost při práci s elektronickou poštou. Lidé by dle nich měli již dopředu počítat s tím, že se v jejich e-mailové schránce může objevit nebezpečná zpráva a v nevyžádané komunikaci by nikdy neměli stahovat a spouštět přílohy nebo klikat na odkazy.

Zatímco také u infostealeru Agent Tesla zaznamenali experti z ESETu znepokojivý nárůst počtu detekcí, významnější propad pak evidovali u infostealeru Formbook. Kampaně těchto škodlivých kódů nebyly tentokrát cílené přímo na Česko.

„Vysoký počet detekcí v případě infostealeru Agent Tesla není dobrou zprávou. Útočníkům se evidentně stále vyplácí využívat staré verze tohoto škodlivého kódu a více než 15procentní podíl detekcí to v tomto případě dokládá. Většina bezpečnostních řešení by měla být na tento škodlivý kód již perfektně připravená a varovným ukazatelem je tak skutečnost, že takový malware může být úspěšný jen na špatně chráněných a neaktualizovaných počítačích. Vypadá to, že nás v oblasti počítačové bezpečnosti čeká v Česku ještě spousta práce," připomíná Jirkal.

Podle bezpečnostních expertů je v případě infostealerů důležitá ochrana v podobě profesionálního bezpečnostního softwaru. Ten dokáže vytvořit bezpečnou složku, do které zjištěnou hrozbu přesune. Uživatelé si poté mohou e-mail ve složce v případě zájmu prohlédnout a pak jej smazat. Bezpečnostní experti pak upozorňují ještě na pravidelné aktualizace softwaru a všech programů v našich zařízeních, které jako uživatelé leckdy odkládáme.

„Určitě to velmi dobře znáte, systém vám ohlásí potřebu aktualizace s nutným restartováním počítače, vy máte zrovna něco rozdělaného, tak to odložíte a mnohdy na to možná zapomenete. Právě ale aktualizovaný operační systém je v přístupu k bezpečnosti našich zařízení, dat a přihlašovacích údajů, které jsou kořistí infostealerů především, naprosto klíčové. Aktuálně se jedná o velkou výzvu především v souvislosti s ukončením podpory operačního systému Windows 10, který podle našeho posledního průzkumu stále využívá zhruba třetina lidí. Ačkoli uživatelé a uživatelky dostali možnost si podporu o rok prodloužit, určitě bych doporučoval provést upgrade na vyšší verzi co nejdříve, protože kybernetické hrozby rozhodně nepočkají a jak vidíme, útočníci udělají všechno proto, aby svoje zbraně přizpůsobili," dodává Jirkal z ESETu.

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

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-cilem-trojskeho-kone-cloudeye-bylo-v-listopadu-cesko-stal-za-ctvrtinou-detekci-pro-operacni-system-windows