ESET: V Česku opět vzrostly případy infostealeru Formbook

20.8.2025 - | ESET software

Také v červenci útočníci pokračovali v šíření infostealeru Formbook a opět do této aktivity zapojili další škodlivý kód, který jim měl pomoci nejen v Česku obávanou hrozbu skrýt před odhalením. Tuto strategii bezpečnostní experti pozorovali již v předchozích měsících. Ačkoli tentokrát útočníci nevsadili na české překlady útočných e-mailů ani škodlivých příloh, detekce infostealeru Formbook vzrostly už na více než čtvrtinu všech zachycených kybernetických hrozeb pro operační systém Windows v Česku. Kromě těchto případů rostly také detekce škodlivého kódu Snake Stealer nebo infostealeru Agent Tesla. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Kybernetičtí útočníci se i v červenci snažili ve velkém šířit infostealer Formbook, jehož detekce tentokrát opět povyrostly na více než čtvrtinu všech zachycených případů škodlivého kódu v Česku. Již v minulých měsících bezpečnostní experti z ESETu upozorňovali na to, že k tomu mohou útočníci využívat organizované kampaně a další škodlivé kódy. A podobnou útočnou strategii objevili i v červenci.

„Nejvíce detekcí infostealeru Formbook jsme sledovali na začátku července. Následně ale útočníci opět sáhli ke stejné metodě z předchozích měsíců a infostealer Formbook schovali pod jiný škodlivý kód, tentokrát pod Agent.ECK. Odhalila to naše podrobnější investigace," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Útočné kampaně škodlivého kódu Agent.ECK, který ukrýval obávaný infostealer, byly nejsilnější 14. a 28. července. Nebezpečné e-mailové přílohy, které jsou primárními zdroji infostealerů nejen v České republice, tentokrát neměly české názvy. Nejčastěji se objevovala příloha s názvem „Scanned Copy PO.exe".

„Typicky zde vidíme, jak útočníci střídají podobu svých kampaní. Nejedná se o nic neobvyklého. Ještě v červnu jsme upozorňovali na velmi zdařilé a uvěřitelné překlady e-mailů a názvů příloh do češtiny. V červenci ale útočníci opět zůstali u angličtiny. Počet detekcí infostealeru Formbook se přitom zase o něco zvýšil. Opět tak apeluji na uživatele a uživatelky, aby si do boje s útočníky vzali spolehlivé obranné nástroje a strategie: obezřetnost u příchozí nevyžádané pošty spolu s kvalitním bezpečnostním softwarem," doporučuje Jirkal.

Oproti předchozímu měsíci o něco narostly také detekce dalšího obávaného infostealeru, který bezpečnostní experti z ESETu sledují pod názvem Agent.AES. Známý je nicméně i pod jménem Snake Stealer či Snake Keylogger.

„Snake Stealer je ve světě kyberbezpečnosti aktuálně velmi sledovanou hrozbou. Podle naší poslední zprávy ESET Threat Report H1 2025 byl tento malware v období od prosince 2024 do května 2025 celosvětově infostealerem číslo jedna. Útočníci díky němu dokážou zaznamenávat stisky kláves, odcizit uložené přihlašovací údaje, pořizovat snímky obrazovky a sbírat data ze schránky. Spolu s infostealerem Formbook je vnímáme jako nástupce nechvalně proslulého infostealeru Agent.Tesla, který začal slábnout na přelomu letošního roku. Stále monitorujeme, zda některý z těchto dvou malwarů dosáhne jednoznačné převahy a převezme finálně pomyslnou štafetu," říká Martin Jirkal a dodává: „U zmíněného infostealeru Agent.Tesla jsme v červenci také zaznamenali mírný nárůst detekcí a v jeho případě se dokonce objevila verze škodlivé přílohy v češtině s názvem Poptavka

00413_pdf.exe. Jak jsme již ale upozorňovali dříve, s těmito občasnými výkyvy se budeme i v případě tohoto škodlivého kódu ještě nějaký čas setkávat. I když byl oficiálně oznámen jeho konec přímo útočníky, kteří jej vyvíjeli, jeho starší verze včetně českých příloh se mohou stále prodávat na černém trhu a jiným útočníkům ještě nějaký ten čas dobře sloužit," uzavírá Martin Jirkal z ESETu.

Spolehlivou pojistkou před nechtěným otevřením škodlivé přílohy a vpuštěním škodlivého kódu do zařízení je bezpečnostní software. 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. Nebezpečné e-maily nejsou jen hrozbou pro jednotlivce, ale také pro firmy a jejich zaměstnance. Součástí aktualizované platformy ESET PROTECT pro firemní zákazníky z letošního jara je proto také nová ochrana proti spoofingu a útokům využívajícím homoglyfy. Nově je součástí stávajícího řešení ESET Cloud Office Security (ECOS). Útočníkům brání v tom, aby se vydávali za důvěryhodné zdroje či osoby a rozpozná, pokud chtějí maskovat škodlivé domény nebo URL adresy záměnou písmen z jiných abeced. ESET Cloud Office Security navíc nyní také obsahuje funkci zpětného stažení e-mailů, která umožňuje rychle odvolat a umístit do karantény jakékoli doručené e-maily, které vyhodnotí jako podezřelé.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-v-cesku-opet-vzrostly-pripady-infostealeru-formbook