ESET: Více než polovina lednových útoků na Česko měla za cíl naše přihlašovací údaje

18.2.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Na základě lednové statistiky kybernetických hrozeb pro operační systém Windows v Česku opět stoupla aktivita škodlivých kódů Formbook a Agent.AES. Oba jsou přitom v posledních měsících v bezpečnostní komunitě skloňovány jako pokračovatelé a nástupci spywaru Agent Tesla, jehož detekční čísla nadále klesají. V lednu se v Česku objevovaly spíše globálně cílené kampaně a české překlady názvů nebezpečných e-mailových příloh byly spíše výjimkou. Vyplývá to z detekčních dat společnosti ESET. Bezpečnostní experti kromě profesionální ochrany v podobě moderního bezpečnostního řešení doporučují pečlivě kontrolovat přípony názvů příloh v e-mailové komunikaci. Uživatele mohou upozornit na to, že otevírají nějaký spustitelný soubor, a ne dokument ve formátu PDF či soubor programu MS Word nebo Excel.

Infostealer Formbook se v lednu opět objevil ve více než 40 procentech případů a vrátil se tak na hodnoty z loňského listopadu. V počtu detekcí pak „posílil“ také škodlivý kód Agent.AES s podílem 10 procent všech zachycených případů. Naposledy se přitom na úrovni těchto hodnot objevil během letních měsíců. Infostealery jsou dlouhodobou hrozbou pro operační systém Windows nejen v Česku. Jedná se o typ spywaru, který útočníci využívají pro špionážní aktivity a odcizení uživatelských dat, především přihlašovacích údajů do našich účtů. V zařízení se mohou chovat velmi nenápadně a trvá poměrně dlouho, než je uživatelé odhalí.

„V případě infostealeru Formbook jsme zachytili dvě velké útočné kampaně 6. a 16. ledna. Zdrojem škodlivého kódu zůstávají nebezpečné e-mailové přílohy, které vzbuzují dojem, že se jedná o nějaké faktury nebo objednávky. V lednu jsme mohli pozorovat hlavně globální útoky v angličtině, české překlady se objevovaly pouze v malém množství v případě spywaru Agent Tesla,“ komentuje lednová čísla z pravidelné statistiky pro operační systém Windows Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. „V lednu se na přední místa opět vrátil také škodlivý kód Agent.AES. Jedná se rovněž o malware, který řadíme mezi spyware a který útočníci využívají pro krádeže přihlašovacích údajů a dalších dat. Ačkoli je nyní nejvíce aktivním škodlivým kódem Formbook, je to právě malware Agent.AES, který je považován za jednoho z možných nástupců nechvalně proslulého spywaru Agent Tesla,“ vysvětluje Jirkal.

Dlouhodobá „jednička“ mezi spywary, Agent Tesla, začal slábnout koncem minulého roku a bezpečnostní experti potvrzují, že se jedná o trvalý stav. Podle jejich informací totiž autoři škodlivého kódu již neplánují pokračovat v jeho vývoji. Infostealer Formbook se v lednu nejčastěji objevoval v přílohách „CSZ inquiry for MH raw material.exe“ či „PO No. 0146850827805 HSP0059842.exe“. Malware Agent.AES zachytili experti z ESETu nejčastěji v příloze s názvem „Payment Error.cmd“.

„I když se aktuálně prostředí hrozeb pro české uživatele a uživatelky dynamicky proměňuje, v otázce ochrany před infostealery a dalšími typy spywaru zůstávají naše doporučení stejná – věnovat pozornost zprávám, které máme ve svých e-mailových schránkách. E-mailové přílohy se většinou zobrazují tak, že pořádně nevidíme skutečnou příponu názvu souboru, který je ke zprávě přiložený. Právě ale přípona nám může naznačit, že jsme v příloze obdrželi něco jiného než obrázek nebo dokument. Pokud se podíváme na škodlivé přílohy z letošního ledna, můžeme vidět, že mají příponu .exe nebo .cmd. Jedná se o spustitelné soubory, nikoli o formáty, ve kterých bychom faktury a objednávky standardně očekávali – v PDF souborech nebo souborech programů Excel či Word,“ říká Jirkal.

V případě spywaru Agent Tesla detekční čísla stále zcela viditelně klesají. V lednu ho bezpečnostní experti zachytili pouze v necelých třech procentech případů. Podle nich se jedná především o staré kampaně z méně používaných e-mailových účtů. Spyware ukrývaly přílohy s názvy „SGJ780097-JWVY8560I-HHWQEUUIT6F6.bat“, „Zpusob_platby‚jpg.exe“ nebo „Poptavka 00413_pdf.exe“.

„I když se v případě škodlivého kódu Agent Tesla jednalo v lednu o starší kampaně, které jsme vídali již v minulosti, neznamená to, že by byl méně nebezpečný. Ostražitost je na místě do té doby, dokud budou útočníci udržovat servery, na kterých shromažďují data obětí, aktivní. Řada infostealerů totiž funguje jako služba, kterou si lze koupit – malware-as-a-service,“ vysvětluje Jirkal. „Protože infostealery mohou krást vaše data po dlouhou dobu bez odhalení, spolehlivou ochranou je především profesionální bezpečnostní software, který zařízení pravidelně kontroluje na přítomnost škodlivého kódu. Moderní bezpečnostní řešení obsahují také celou řadu dalších užitečných funkcionalit, například tzv. správce hesel. Jedná se o specializované programy, které uchovávají naše přihlašovací údaje v bezpečné zašifrované podobě a automaticky je doplní, když se přihlašujeme do našich účtů, ať už se jedná o e-mail, internetové bankovnictví nebo e-shop,“ dodává Jirkal z ESETu.

Moderní bezpečnostní programy kromě obrany před kybernetickými hrozbami poskytují i praktické nástroje k ochraně našeho soukromí. Zabezpečená složka ESET Folder Guard chrání cenná data uživatelů před malwarem, který se je snaží poškodit. Uživatelé mohou vytvořit až několik zabezpečených složek, ke kterým budou mít přístup jen důvěryhodné a uživatelem povolené aplikace. Funkce Ochrana identity pak monitoruje černý trh s prodejem osobních údajů a upozorní uživatele, pokud se s jeho údaji obchoduje na dark webu.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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 TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.

tel: +420 720 829 561
vitezslav.pelc@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-vice-nez-polovina-lednovych-utoku-na-cesko-mela-za-cil-nase-prihlasovaci-udaje