V září se v Česku objevily především útočné e-mailové kampaně v češtině, v přílohách se ukrýval spyware

13.1.2024 - Lucie Mudráková | ESET software

Spyware Agent Tesla je nadále přední hrozbou pro uživatele operačního systému Windows v České republice.

I přes výraznější pokles detekovaných případů se spyware v září šířil v celé řadě příloh s názvy v češtině a bezpečnostní specialisté tak upozorňují, že spyware neztrácí na své nebezpečnosti. Uživatelům doporučují kontrolovat české překlady, které stále ve většině případů obsahují gramatické chyby a mohou tak sloužit jako varování před škodlivým kódem. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Ačkoli ještě v červenci se spyware Agent Tesla objevoval téměř ve třetině všech detekcí, v září ho bezpečnostní experti evidovali v necelých třinácti procentech všech zachycených případů škodlivého kódu pro operační systém Windows v České republice. Upozorňují však na to, že i přes současný pokles útočníci nadále investují do českých překladů útočných kampaní.

„Spyware Agent Tesla neměl v České republice během září žádnou větší útočnou kampaň. Množství nebezpečných příloh s českými názvy, jichž útočníci zneužívají k jeho šíření, se však vymykalo situaci, kterou v českém prostředí běžně pozorujeme. Zpravidla se totiž setkáváme s e-maily a přílohami v angličtině, které útočníci přímo pro české uživatele nepřekládají. České překlady mohou přitom zvýšit pravděpodobnost, že uživatelé nebezpečné přílohy ve chvilce nepozornosti otevřou a spyware vpustí do svého zařízení," říká k zářijovým číslům pravidelné statistiky Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Dlouhodobě můžeme u nebezpečných příloh šířících spyware pozorovat také jistou strategii. Dokumenty v přílohách mívají dvě koncovky, přičemž tu druhou z nich, příponu .exe, uživatelé nemusí vždy vidět. Namísto toho vidí jen domnělý dokument v programu MS Word, ve formátu PDF nebo obrázek, a ten mohou otevřít a přílohu tak spustit. Jistotu ochrany před spywarem tak mají vždy s bezpečnostním softwarem, který se na koncovky příloh v e-mailech cíleně zaměřuje. Rozhodně by ale neměli rezignovat na to, že název přílohy sami zkontrolují," dodává Jirkal.

Nebezpečné e-mailové přílohy, jejichž prostřednictvím se spyware Agent Tesla v září šířil Českem, měly názvy „děkovný dopis.docx.exe", „Poptavka 00413_pdf.exe", „Zpusob_platby,jpg.exe", „SMLOUVA-pdf.exe".

Česky pojmenované přílohy se v září objevily také v případě spywaru Formbook a password stealeru Fareit. I přes to, že útočníci vsadili v případě zářijových kampaní na češtinu, nebývají překlady vždy správné a kontrola textu a názvů příloh může uživatele včas varovat, že něco není v pořádku.

„Ani spyware Formbook ani password stealer Fareit nebyly v září detekovány ve větším počtu případů. Škodlivý kód Fareit šířili útočníci například v e-mailech, které vydávali za zprávy od bank či logistických firem. Devět z deseti těchto e-mailů bylo přeloženo do češtiny," říká Jirkal.

„Útočníci mají k přípravě útoků k dispozici celou řadu nástrojů, a to dnes již včetně nástrojů umělé inteligence využívajících velkých jazykových modelů, jako je například ChatGPT. Stále se však

uživatelé mohou setkat s jazykovými chybami. V září jsme tyto případy nejvíce viděli právě u password stealeru Fareit," dodává Jirkal.

Spyware patří mezi závažnější škodlivé kódy, které útočníci využívají se záměrem ukrást přihlašovací údaje k různým uživatelským účtům. Odcizené údaje pak mohou využívat k přípravě dalších útoků, jako jsou například útoky hrubou silou. Další možností je údaje prodat na černých trzích jiným útočníkům. V každém případě je cílem finanční zisk.

„Při útocích na hesla je pro uživatele největším rizikem využívání stejných hesel u více jejich online účtů. Běžnou strategií útočníků je totiž odcizená hesla a přihlašovací jména zkoušet dosazovat k různým účtům s cílem je prolomit. Pokud uživatel nemá svůj účet chráněný dalším faktorem, kterým bývá kód z SMS nebo ze spárované aplikace, má útočník dveře k jeho účtu prakticky otevřené," říká Jirkal z ESETu.

Bezpečnostní experti uživatelům doporučují vytvářet alespoň 12místná hesla s využitím různých znaků, jako jsou číslice, velká a malá písmena či speciální znaky. Silným heslem může být i tzv. heslová fráze. Spyware také spolehlivě zastaví kvalitní bezpečnostní software. Řada z nich obsahuje správce hesel, specializované programy, které uchovávají hesla v zabezpečené podobě a automaticky je dosazují při přihlašování do konkrétních účtů.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

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 produktů 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 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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-v-zari-se-v-cesku-objevily-predevsim-utocne-e-mailove-kampane-v-cestine-v-prilohach-se-ukryval-spyware