ESET: Spyware v lednu posílil na pětinu všech detekcí

16.2.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Nebezpečné e-mailové přílohy šířící spyware Agent Tesla, spyware Formbook a password stealer Fareit byly nejčastějšími lednovými hrozbami pro uživatele operačního systému Windows v Česku.

Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. Přílohy útočníci dlouhodobě vydávají za doklady k objednávkám či za faktury. V lednu byly opět buď součástí větších, globálních kampaní, nebo v českém překladu cíleně zaměřeny na uživatele v České republice. Bezpečnostní experti především doporučují nepodcenit kvalitní antispamovou ochranu elektronické pošty.

Spyware a další škodlivé kódy, které se zaměřují na naše přihlašovací údaje, zůstávají hlavními hrozbami pro uživatele operačního systému Windows v Česku. V lednu se s více než 15 procenty všech detekovaných případů objevil v čele statistiky opět spyware Agent Tesla. Také další dva dlouhodobě přítomné škodlivé kódy, spyware Formbook a password stealer Fareit, v lednové statistice nechyběly.

„Větší kampaně měly v lednu spyware Agent Tesla a spyware Formbook. Nebezpečné e-mailové přílohy, jejichž prostřednictvím se tento typ škodlivého kódu šíří Českem dlouhodobě, ale ve většině případů nebyly přeloženy do češtiny. Naopak u třetího nejčastěji detekovaného škodlivého kódu, password stealeru Fareit, jsme objevili větší objem českých e-mailů. Podle dlouhodobého pozorování je to právě poslední jmenovaný škodlivý kód, u kterého zpravidla detekujeme nejvíce hrozeb šitých na míru českým uživatelům," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Password stealer Fareit se v lednu objevoval v příloze s názvem „P.O-NO 683054_ViT Logistics.exe" a v česky pojmenované příloze „Faktura pro potvrzení_INV_604-0335.exe".

V případě spywaru Agent Tesla se v lednu objevovaly nebezpečné přílohy s názvy „10.PURCHASEORDER_TLGPOS2024JAN_AppendicesABDE_PRODUCTS_XLSX.exe" či „Poptavka 00413_pdf.exe". Spyware Formbook pak bezpečnostní specialisté z ESETu objevili v přílohách „DHL DOC IMG010342024.exe" či „nákupní objednávka pdf.exe".

Podle dlouhodobého sledování bezpečnostních expertů se útočníci stále drží osvědčené strategie, kdy přílohy ukrývající spyware vydávají za doklady objednávek a za faktury. Především zaměstnanci firem, kteří běžně pracují s větším objemem e-mailové komunikace, mohou takový e-mail v záplavě jiných zpráv snadno přehlédnout a nebezpečnou přílohu v zařízení spustit.

„Ačkoli soubory mají příponu .exe, která poukazuje na nějaký spustitelný soubor, nikoli na klasické dokumenty, uživatelé nemusí takový soubor na první pohled rozeznat. Dokumenty v přílohách mívají dvě koncovky, přičemž tu druhou z nich, příponu .exe, uživatelé nemusí vždy vidět. Naopak, e-mailová příloha se může jevit jako dokument v programu MS Word, ve formátu PDF nebo jako obrázek, na který uživatelé mohou kliknout v domnění, že se nejedná o nic nebezpečného. Před otevřením by si však měli název přílohy dobře prohlédnout, a to zvlášť v případech, kdy jim zpráva přišla z adresy, na kterou běžně nekomunikují, nebo jim takový e-mail přijde poprvé. Jistotu ochrany před spywarem mají každopádně vždy s bezpečnostním softwarem, který se na koncovky příloh v

e-mailech cíleně zaměřuje," vysvětluje Jirkal.

Bezpečnostní specialisté vždy na prvním místě uživatelům doporučují, aby se zaměřili na vytváření silných a unikátních hesel. Takové heslo by mělo obsahovat alespoň 12 různých znaků, jako jsou číslice, velká a malá písmena či speciální znaky. Silným heslem může být i tzv. heslová fráze – věta nebo sousloví, které se uživatelům dobře pamatuje a dává smysl jen jim. Pro každý online účet by pak uživatelé měli mít heslo, které nikde jinde nepoužívají. Lidí, kteří přitom v Česku s hesly riskují a „recyklují" je pro více svých účtů, je podle posledního průzkumu o dodržování kybernetické bezpečnosti při online nakupování stále třetina. Odcizené přihlašovací údaje jsou častým zbožím na černých trzích, kde je mohou útočníci dobře zpeněžit. Seznamy odcizených hesel pak mohou sloužit k přípravě útoků tzv. hrubou silou.

„Nebezpečné e-mailové přílohy jsou strategií, která mezi útočníky rozhodně není nová, a uživatelé se tak před ní mohou chránit například dobře nastavenou antispamovou ochranou. Nemusí tak riskovat, že nebezpečný e-mail přehlédnou a spyware vpustí do svého počítače. Šikovným pomocníkem pro bezpečné uchovávání hesel je pak správce hesel. V něm mohou mít uživatelé všechna svá hesla i v těch nejsložitějších podobách a program je za ně automaticky vyplňuje při přihlašování do jejich účtů. Pamatují si pak už jen jedno heslo, a to k přihlášení právě do tohoto programu," říká Jirkal z ESETu.

Správce hesel i antispamová ochrana je součástí moderních bezpečnostních řešení, která dnes uživatele chrání nejen před malwarem, ale nabízí právě celou řadu nástrojů a funkcí pro celkové zabezpečení digitálního života na internetu.

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.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

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-spyware-v-lednu-posilil-na-petinu-vsech-detekci