V závěru roku zůstal největší hrozbou spyware Agent Tesla, falešné e-mailové přílohy budou nebezpečím i letos

17.1.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Závěrem roku 2023 byly nejčastěji detekovanými hrozbami pro operační systém Windows v Česku spyware Agent Tesla, spyware Formbook a password stealer Fareit. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. Zdrojem malwaru zůstávají nebezpečné e-mailové přílohy, které útočníci vydávají za dokumenty z bank, faktury nebo doklady objednávek. Podle bezpečnostních expertů se tyto hrozby neustále vyvíjejí a na základě stále rostoucího počtu případů je podle nich velmi pravděpodobné, že se s nimi budou čeští uživatelé setkávat i v roce 2024. Nevylučují, že do přípravy útoků se zapojí také nástroje umělé inteligence.

Závěrem roku 2023 byl nejvíce detekovaným škodlivým kódem pro operační systém Windows opět spyware Agent Tesla. Zatímco v listopadu byl nejčastějším škodlivým kódem virus Delf.NBX, kterým útočníci mířili především na země s předpokládanou nižší úrovní zabezpečení, loňský rok již opět uzavřely škodlivé kódy, se kterými se uživatelé v Česku setkávali v průběhu loňského roku nejčastěji.

„V prosinci jsme mohli v českém prostředí opět vidět dobře známou trojici škodlivých kódů – spyware Agent Tesla, spyware Formbook a password stealer Fareit. Všechny tyto tři typy hrozeb se zaměřují na krádež přihlašovacích údajů, především uživatelských hesel," shrnuje prosincové kybernetické hrozby Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Hrozby v podobě e-mailů obsahujících nebezpečné odkazy a přílohy s malwarem se neustále vyvíjejí a počty zachycených případů stále rostou. Očekáváme, že se s nimi budou čeští uživatelé setkávat velmi často i v letošním roce. Můžeme také očekávat, že do tvorby textů pro útočné e-maily zasáhnou nástroje umělé inteligence. Je nicméně otázkou, zda už v letošním roce půjde o častý a v praxi běžně používaný typ hrozby," dodává Jirkal k výhledu na letošní rok a hrozby pro operační systém Windows v Česku.

Útočníci cílí nebezpečnými e-mailovými přílohami na české uživatele jak v globálních kampaních, kdy nepřekládají názvy z angličtiny, tak přímo v česky lokalizovaných e-mailech. Přílohy mají často názvy odkazující na platební transakce nebo domnělé objednávky a dokumenty mají příponu .exe, která je typická pro spustitelný soubor. Přípona není vždy na první pohled viditelná v dlouhém názvu souboru, což je záměr – útočníci nechtějí na netypickou přílohu zbytečně upozorňovat.

„Všechny tři nejčastěji detekované škodlivé kódy se objevovaly průběžně po celý prosinec a nepřekvapí, že celá řada útoků se soustředila kolem vánočních svátků. Prázdniny a svátky jsou pro útočníky oblíbeným obdobím, protože předpokládají, že uživatelé nebudou tolik ve střehu a nebezpečné e-mailové přílohy ve své poště přehlédnou. Příkladem za všechny může být například příloha odkazující na platební doklad České spořitelny, která ukrývala škodlivý kód Fareit," vysvětluje Jirkal.

Spyware Agent Tesla se v prosinci ukrýval například v přílohách s názvy „RFQ_810000004412000000454434000000.exe" či „Factura324546_PDF.exe". Na spyware Formbook mohli uživatelé narazit například v příloze „nákupnú objednávku pdf.exe" a již zmíněný password stealer Fareit se poté objevil v přílohách „P.O-NO 683054_ViT Logistics.exe" a „Ceskasporitelna,

a.s.Swift_260321_scan.exe“. Právě poslední zmíněná příloha se v Česku nejvíce objevovala 24. prosince 2023.

Dlouhodobá přítomnost spywaru a dalšího škodlivého kódu specializovaného na krádeže přihlašovacího údajů vyvíjí tlak na spolehlivou ochranu uživatelských hesel. Ty jsou stále hlavním bezpečnostních prvkem v našich digitálních životech. Podle posledního průzkumu společnosti ESET zaměřeného na dodržování kybernetické bezpečnosti při online nakupování v Česku je stále velmi běžné, že uživatelé svá hesla opakovaně používají. Tím vystavují riziku více svých účtů s osobními či citlivými údaji. Lidí, kteří takto se svými hesly riskují, je podle průzkumu stále třetina.

„Pokud mluvíme o útocích na hesla, spyware je samozřejmě jedním z celé řady strategií, kterou útočníci mohou využít. Dalším způsobem jsou například útoky tzv. hrubou silou, při kterých útočníci využívají databáze uniklých hesel a ty pak při automatizovaných útocích dosazují spolu s přihlašovacími jmény ve snaze účty prolomit. Rizikem pro přihlašovací údaje jsou samozřejmě také techniky sociálního inženýrství, jako je phishing, smishing nebo vishing. Při nich zase útočníci sázejí na manipulativní komunikaci. Nelze očekávat, že by zatím míra útoků na hesla klesala, a proto opakovaně apelujeme na uživatele, aby ochranu hesel nepodceňovali,“ říká Jirkal z ESETu.

Kromě využívání silných hesel, která uživatelé nebudou opakovaně využívat pro více svých účtů, je vhodné zvolit také kvalitní bezpečnostní software, který chrání před pokročilejšími hrozbami, jako je například právě spyware. Bezpečnostní experti také nedoporučují ukládat hesla do nechráněných souborů v počítači ani do internetových prohlížečů, které nejsou před spywarem dostatečně zabezpečené. Řešením pro bezpečné uchovávání přihlašovacích údajů může být správce hesel, specializovaný program, který hesla uchovává v zašifrované podobě a automaticky je dosazuje při přihlašování do online účtů uživatele.

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-v-zaveru-roku-zustal-nejvetsi-hrozbou-spyware-agent-tesla-falesne-e-mailove-prilohy-budou-nebezpecim-i-letos