V červenci zůstaly největšími riziky pro české počítače škodlivé kódy, které kradou přihlašovací údaje

19.8.2024 - Lucie Mudráková | ESET software

Podle červencové statistiky kybernetických hrozeb pro operační systém Windows v České republice je nejčastějším škodlivým kódem stále spyware, a to v zastoupení škodlivých kódů Agent Tesla, Formbook a Agent.AES. I když spyware Agent Tesla neměl v červenci tak výraznou útočnou kampaň jako v předešlém měsíci, stále zůstává v Česku největší kybernetickou hrozbou. Uživatelé a uživatelky se mohli tentokrát setkat především s globálními útoky a čeština se v překladech názvů nebezpečných příloh objevila spíše okrajově. Bezpečnostní experti nabádají k opatrnosti při práci s elektronickou poštou a upozorňují na trend, kdy útočníci mohou šířit malware kradoucí citlivé informace i prostřednictvím napodobenin známých aplikací, včetně nástrojů AI. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Podle nejnovějších detekčních dat spyware Agent Tesla v červenci nezopakoval svou silnou aktivitu z předchozího období. S podílem kolem desetiny všech zachycených případů se naopak vrátil k běžnému počtu detekcí v letošním roce. V červenci ho na předních místech pravidelné statistiky doplnily také spywary Formbook a Agent.AES.

„Spyware Agent Tesla sice zůstává hrozbou číslo jedna pro české uživatele a uživatelky, masivní útočnou kampaň ze začátku léta v červenci ale nezopakoval. Můžeme říct, že červenec byl z tohoto pohledu klidným měsícem. Mezi detekovanými e-mailovými přílohami se sice objevila příloha s českým názvem objednávka, obecně ale vidíme, že útoky byly v červenci opět zacíleny spíše globálně na různé státy. S cíleným útokem na Česko se však ještě setkat můžeme. Je běžné, že útočníci se po výraznější aktivitě na čas opět stáhnou, aby předešlý útok vyhodnotili a investovali do přípravy dalších strategií a metod," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Spyware je spolu s infostealery škodlivým kódem, který je určený ke krádeži citlivých informací – například přihlašovacích údajů do různých účtů. Šíří se nejčastěji prostřednictvím e-mailových příloh, které útočníci maskují za různé dokumenty. Spyware Agent Tesla se v červenci ukrýval například v přílohách s názvy „PO 4500005168 NIKOLAPO 4500005168 NIKOLA.exe" nebo „Objednávka IMG_PO #00702441355 - č. 2400228341_pdf.exe". Spyware Formbook pak nejčastěji šířila příloha „Custom Clearance 5816641785332.exe" a spyware Agent.AES se v příloze „Order Details.exe" nejčastěji objevoval v e-mailech, které útočníci vydávali za notifikace k nákupům přes internet.

Útočníci stejně jako odborníci na marketing připravují své útoky na míru konkrétním cílovým skupinám. Podle poslední zprávy ESET Threat Report H1 2024 se již od konce loňského roku začaly objevovat případy, kdy útočníci maskovali infostealery za nástroje generativní umělé inteligence – jednalo se například o napodobeniny služeb Midjourney, Sora nebo Gemini. K jejich šíření využívali také podvodná sdělení na sociálních sítích.

„V posledních několika měsících se nám opět potvrzuje, že mezi útočníky a těmi, kdo se snaží digitální životy uživatelů chránit, probíhá stále neutuchající závod v kontextu rychlého technologického vývoje. I když vývoj nástrojů generativní umělé inteligence doprovází i ochranná

opatření, která mají zabránit jejich zneužití, útočníci známá jména přesto využili k šíření malwaru. Můžeme bohužel očekávat, že tento trend bude i nadále pokračovat," říká Jirkal.

Slavná jména AI asistentů jako Sora od OpenAI či Gemini od Google využívali útočníci k šíření škodlivého kódu Rilide Stealer. Škodlivý kód Vidar infostelaer se poté objevoval v údajné desktopové aplikaci Midjourney pro operační systém Windows, přestože v době útoku nebyla tato aplikace oficiálně k dispozici. S ohledem na popularitu AI nástrojů by se před zneužitím těchto aplikací měli mít podle bezpečnostních expertů na pozoru také uživatelé a uživatelky v Česku.

Kromě vlastní obezřetnosti při stahování aplikací do zařízení bychom podle bezpečnostních specialistů měli dbát na opatrnost i při práci s elektronickou poštou a dalšími komunikačními aplikacemi. E-mail je i přes rostoucí popularitu chatovacích aplikací stále rozšířeným způsobem komunikace, a to především ve firmách a dalších institucích.

„Útočníci vydávají nebezpečné přílohy velmi často za faktury a doklady objednávek. Zmást tak mohou zaměstnance, kteří denně pracují s větším objemem e-mailové komunikace. Dlouhé názvy příloh jsou často zvolené záměrně, protože se v názvu schová přípona .exe označující spustitelný soubor, která není tak běžná a může nás upozornit na to, že něco není v pořádku. Příloha se pak nejčastěji tváří jako dokument v programu MS Word, ve formátu PDF nebo například jako obrázek," vysvětluje Jirkal z ESETu.

Účinnou ochranou před spywarem je také moderní bezpečnostní program. Dokáže rozpoznat škodlivý e-mail a přesune ho do bezpečné složky, kterou za účelem naší ochrany vytvoří. V předmětu e-mailu pak uživatelé mohou vidět, že se jedná o detekovanou hrozbu a mohou si e-mail ve vytvořené složce v případě zájmu prohlédnout a následně smazat. Pokud se škodlivý kód ukrývá v aplikaci nebo v souboru, bezpečnostní řešení zkontroluje doménu a URL adresu stránek, ze kterých je aplikace stahována. Při samotném spuštění pak proběhne také detekce rezidentní ochranou souborového systému a v případě, že program objeví škodlivý kód, je spuštění zablokováno a soubory jsou přesunuty do karantény, o čemž jsou uživatelé informováni prostřednictvím dialogového okna.

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 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 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-cervenci-zustaly-nejvetsimi-riziky-pro-ceske-pocitace-skodlive-kody-ktere-kradou-prihlasovaci-udaje