ESET: Velký návrat spywaru Agent Tesla, v červnu se jeho detekce vyšplhaly ke třetině všech případů

19.7.2024 - Lucie Mudráková | ESET software

Počet detekcí spywaru Agent Tesla, který je v Česku dlouhodobě stabilním malwarem, dosáhl v červnu téměř třetiny všech případů škodlivého kódu pro operační systém Windows v Česku.

Podle bezpečnostních expertů se jednalo o nejsilnější útok letošního roku. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. Útočníci spyware šířili prostřednictvím e-mailových zpráv od německé společnosti, která u českých obětí chtěla objednat zboží. Celá zpráva byla lokalizována do češtiny, včetně falešných kontaktních údajů a adresy webových stránek.

V červnu zachytili bezpečnostní experti velký útok spywaru Agent Tesla na Českou republiku. Ještě v květnu byl přitom spyware v útlumu a na pomyslné první příčce pravidelné statistiky ho vystřídal škodlivý kód Agent.RWL. Minulý měsíc byl však spyware znovu detekován v téměř třetině všech zachycených případů.

„Za poslední rok, kdy prostředí kybernetických hrozeb v Česku pro operační systém Windows pravidelně monitorujeme, se jednalo bezesporu o největší útok spywaru Agent Tesla. Oproti silnému útoku z října loňského roku byla výše červnových detekcí téměř trojnásobná," shrnuje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Při bližší analýze škodlivé e-mailové zprávy, která obsahovala přílohu s ukrytým spywarem, jsme viděli, že útočníci přeložili do češtiny také kontaktní údaje domnělé společnosti, která obětem zasílala falešnou přílohu s názvem objednávka. Telefonní číslo mělo předvolbu +420 a doména webových stránek firmy pak příponu .cz. Reálně kontaktní údaje neexistovaly, zdá se tak, že útočníci využívají jeden společný vzor útočné zprávy, kterou pak automaticky překládají do dalších jazyků," vysvětluje Jirkal.

Nebezpečná e-mailová příloha, která obsahovala spyware Agent Tesla, měla v červnu název „Objednávka IMG_PO #00702441355 - č. 2400228341_pdf.exe". Útočníci vydávali e-mail za zprávu od německé firmy IWK Verpackungstechnik S.r.o, která měla zájem o nákup zboží. Podle bezpečnostních specialistů tak e-mail cílil především na zaměstnance českých firem. Spyware je dlouhodobě jednou z největších hrozeb pro české uživatele. Jeho prostřednictvím se útočníci zaměřují na odcizení přihlašovacích údajů, především uživatelských hesel.

Mezi dalšími předními škodlivými kódy se i v červnu umístil dobře známý spyware Formbook a škodlivý kód Agent.BTQ, který se na předních místech statistiky objevil letos poprvé. Útočníci ho stejně jako spyware Agent Tesla zacílili přímo na Českou republiku, a to v příloze s názvem „Vyuctovani_2024_07-1206812497˙pdf.exe". Spyware Formbook se v červnu objevil jen v celosvětových kampaních v příloze „RFQ#10112023Q4.exe". Podle bezpečnostních specialistů u něj tentokrát nebyly české překlady příliš běžné.

„Škodlivý kód Agent.BTQ se v naší statistice objevil bez předchozích významnějších detekcí stejně, jako v květnu malware Agent.RWL. Jedná se o pokročilejší škodlivý kód, který může do počítače stahovat další malware. To, že se dva měsíce po sobě objevily v Česku jiné kódy, než je dlouhodobě detekovaný spyware, svědčí o tom, že útočníci pravděpodobně nakupují pokročilejší škodlivé kódy od

jiných útočníků," říká Jirkal.

Malware se v případě operačního systému Windows nejčastěji šíří prostřednictvím škodlivých e-mailových příloh. Útočníci je vydávají za různé faktury nebo objednávky a mohou tak zmást především zaměstnance firem, kteří denně pracují s větším objemem e-mailové komunikace. Přípona .exe pak poukazuje na nějaký spustitelný soubor, nikoli na klasické dokumenty. Uživatelé nemusí takový soubor na první pohled rozeznat. Dokumenty v přílohách mohou mít dvě koncovky, přičemž tu druhou z nich, příponu .exe, uživatelé nemusí vždy vidět. Příloha se naopak může jevit jako dokument v programu MS Word, ve formátu PDF nebo jako obrázek.

Účinnou obranou před spywarem je vždy bezpečnostní software. I sebeopatrnější uživatelé a uživatelky díky němu mají jistotu, že i když nechtěně otevřou přílohu se škodlivým kódem, zůstanou jejich data v bezpečí. Spyware se dlouhodobě zaměřuje na krádeže osobních údajů, včetně těch přihlašovacích. V nebezpečí jsou především naše hesla, uložená v internetových prohlížečích, které nejsou přes spywarem a infostealery dostatečně zabezpečené.

„Řada lidí si velmi často myslí, že na ně kyberútočník pravděpodobně nezacílí. Mohou si říkat, že útočníci se zaměřují především na cíle, od kterých mohou odcizit velké množství peněz. Je důležité si ale uvědomit, že penězi dnes můžeme vyvažovat i naše data. Útočník si nehledá konkrétní oběti, ale pomocí automatizovaných procesů dnes dokáže zacílit na velké množství náhodně vybraných lidí. Získané údaje může využít k přípravě dalších útoků, nebo je prodat na černém trhu," dodává Jirkal z ESETu.

Moderní bezpečnostní řešení vyhledává škodlivé soubory, chrání uživatele a uživatelky proti škodlivým stránkám a chrání jejich online bankovnictví. Bezpečnostní software se zaměřuje také přímo na koncovky příloh v e-mailech. Mimo řadu funkcionalit obsahují bezpečnostní řešení také další praktické nástroje pro každodenní digitální život – například správce hesel pro správné a bezpečné nakládání s našimi hesly nebo virtuální privátní síť, VPN, pro bezpečné a soukromé prohlížení 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 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.

Lucie Mudráková
Specialistka PR a komunikace

ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-velky-navrat-spywaru-agent-tesla-v-cervnu-se-jeho-detekce-vysplhaly-ke-tretine-vsech-pripadu