Na české uživatele a uživatelky v květnu opět zacílily e-mailové přílohy v českém překladu

26.6.2024 - Lucie Mudráková | ESET software

Ačkoli stálou hrozbou zůstává v Česku spyware Agent Tesla, v květnu se do čela statistiky nejčastějších škodlivých kódů pro operační systém Windows vyšplhal downloader Agent.RWL.

Podle analýzy bezpečnostních expertů se jedná o pokročilý malware s neobvyklými funkcemi. Oba typy škodlivých kódů se po čase opět šířily e-mailovými přílohami, jejichž názvy byly přeložené do češtiny. Útočníci tak cíleně mířili na uživatele a uživatelky v Česku. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Téměř ve třetině všech zachycených detekcí pro operační systém Windows v Česku se v květnu na předních místech statistiky objevil downloader Agent.RWL. Poprvé od začátku letošního roku tak v květnu nepotvrdil spyware Agent Tesla svou dominantní pozici v pravidelné statistice kybernetických hrozeb. Škodlivý kód Agent.RWL byl nejaktivnější v první polovině měsíce, kdy pak především 10. a 13. května cílil přímo na české uživatele a uživatelky. Šířil se prostřednictvím e-mailových příloh s názvy „objednávku_Sollau-000000035_24_826_MBZ_100524_N_200.hta“ nebo „1751155914_456409723_KHI_CZ_240506_0946_P.hta“.

„Malware Agent.RWL patří k velmi pokročilým škodlivým kódům. Po tom, co infikuje počítač, stahuje do něj další škodlivé kódy z Google Drive. Malware tentokrát obsahoval i tzv. killswitch, což nám opět potvrdilo, že se nejedná o běžnou kybernetickou hrozbu, se kterou se čeští uživatelé systému Windows pravidelně setkávají. Jedná se o funkcionalitu, která dokáže infekci v systému zastavit. To využívají například autoři škodlivých kódů, aby sami nenakazili svá zařízení,“ vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET a dodává: „V následujícím období budeme sledovat, zda se v útocích neobjeví časem nová, vylepšená verze tohoto malwaru. Poměrně vysoký podíl zachycených květnových detekcí však může uživatele již nyní upozornit na to, jak je důležité nepodcenit zabezpečení jejich počítačů.“

Kybernetické hrozby pro operační systém Windows se nejen v Česku dlouhodobě šíří prostřednictvím nebezpečných e-mailových příloh. Čeští uživatelé a uživatelky se mohou často setkat s globálními útočnými kampaněmi v angličtině, ojedinělé ale nejsou ani cílené útoky, kdy mohou být znění e-mailu a názvy příloh přeložené do češtiny. Pokud uživatelé přílohu stáhnou a otevřou, vpustí malware do svého počítače. Útočníci dlouhodobě sází na názvy příloh, které nějakým způsobem odkazují na faktury, účtenky a objednávky.

Také spyware Agent Tesla, který je dlouhodobě největším rizikem v případě operačního systému Windows v Česku, se objevil především na začátku května. Spyware je typem škodlivého kódu, který má za úkol krást naše údaje. Útočníci ho využívají často ke krádežím uživatelských hesel, která jim mohou dále posloužit v přípravě útoků, jako jsou například automatizované útoky hrubou silou (tzv. brute-force attacks). Odcizené přihlašovací údaje mají také velkou cenu na černém trhu. Spyware Agent Tesla se v květnu nejčastěji objevoval v e-mailové příloze s názvem „Objednávka č. 234000675-48.exe“.

„Počet detekcí spywaru Agent Tesla v květnové statistice oproti dubnu znatelně poklesl. Na druhou stranu ho útočníci po několika měsících opět zacílili přímo na Českou republiku, a to v příloze s názvem objednávka. Tento případ nám potvrzuje, že útoky šité na míru českým uživatelům nejsou

minulostí, a i po několikaměsíční přestávce se k nim útočníci zase vrací," říká Jirkal.

Oba typy škodlivých kódů doplnil v květnu spyware Formbook. Objevoval se nejčastěji v příloze Document 151-512024.exe.

Heslo nadále zůstává jednou z hlavních garancí naší bezpečnosti na internetu. Jak ale ukázal nedávný průzkum, ne vždy s nimi správně nakládáme. Čtvrtina z nás totiž stále tvoří hesla na základě osobních informací, jako je například jméno domácího mazlíčka, datum narození anebo adresa (26 %). Také 12 % z nás se spoléhá na jednoduchá slovní spojení, jako je např. „heslo123". To je ale podle bezpečnostních specialistů velmi nebezpečné. Řadu našich osobních informací mohou útočníci najít veřejně na různých sociálních sítích a příliš jednoduchá hesla pak mohou snadno prolomit právě automatizované útoky.

„Podle průzkumu zaměřeného na naše zvyky ve správě hesel více než polovina dotázaných uvedla, že si hesla pamatuje z hlavy. Taková hesla ale zpravidla nebývají dost složitá a bezpečná. Navíc mohou uživatelé ve snaze zapamatovat si co nejvíce svých hesel využívat jedny přihlašovací údaje do více různých služeb. Právě ale tohle je ve většině případů fatální. Velmi často stojí recyklování hesel například za ztrátami přístupů do našich účtů na sociálních sítích – útočníci nejenže prolomí heslo do tohoto účtu, ale pokud nám stejné heslo chrání například i e-mailovou schránku, útočníci mohou snadno prolomit přístup i sem a manipulovat s našimi zprávami. Je proto nezbytné, aby pro každý účet existovalo pouze jedno unikátní a dostatečně složité heslo, nejlépe doplněné ještě dalším faktorem ověření naší totožnosti – kódem v SMS nebo ve spárované ověřovací aplikaci," říká Jirkal z ESETu.

Se správou našich hesel nám může pomoci také specializovaný program, který hesla uchovává v zašifrované podobě a automaticky je dosazuje při přihlašování do našich online účtů. Správci hesel, jak se tyto programy nazývají, bývají dnes již součástí komplexních bezpečnostních řešení. Ty také mohou uživatelům nabídnout kvalitní antispamovou ochranu jejich elektronické pošty.

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.

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-na-ceske-uzivatele-a-uzivatelky-v-kvetnu-opet-zacilily-e-mailove-prilohy-v-ceskem-prekladu