# Škodlivý kód Agent Tesla v srpnu utlumil svou aktivitu, spyware však v Česku přesto útočil

**18.9.2024 - Lucie Mudráková | ESET software**

**Zatímco počty detekcí spywaru Formbook a spywaru Agent.AES zůstaly v srpnu bez výrazného poklesu nebo nárůstu, u spywaru Agent Tesla zaznamenali bezpečnostní experti výrazný propad v počtu zachycených útoků na uživatele a uživatelky operačního systému Windows v Česku. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. I přesto, že počet případů škodlivého kódu Agent Tesla tentokrát nepřekročil ani sedm procent, spyware je jako typ hrozby v Česku stále aktivní. Bezpečnostní experti situaci monitorují a nevylučují novou vlnu vylepšených útočných kampaní.**

Konec prázdnin a letních dovolených bývá pro útočníky každoročně příležitostí zhodnotit své dosavadní strategie a přeskupit síly pro následující období. Podle posledních detekčních dat společnosti ESET není letošní rok výjimkou. V srpnu se totiž na své letošní minimum v počtu detekcí dostal obávaný spyware Agent Tesla.

„Ani letošní léto se s ohledem na kybernetické hrozby nelišilo od těch předchozích. Poslední velkou aktivitu jsme v případě spywaru Agent Tesla viděli v červnu, kdy se jeho detekce vyšplhaly téměř ke třetině všech zachycených případů. Pak počet jeho detekcí začal klesat a srpnové hodnoty nedosáhly ani sedmi procent. Máme tak za sebou klidný závěr léta. Je nutné však počítat s tím, že po tak výrazném útlumu se již v příštích měsících můžeme setkat se silnějšími a inovovanými útočnými kampaněmi," říká k aktuálnímu vývoji Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

V srpnu se tak v útocích více objevovaly spywary Formbook a Agent.AES. Bezpečnostní specialisté zachytili především infikované přílohy s anglickými názvy, které útočníci tentokrát nepřekládali do češtiny – spyware Formbook se objevoval nejčastěji v příloze „PAYMENT ERROR.exe" a spyware Agent.AES pak v příloze „Order Details.exe". Na spyware Agent Tesla jsme mohli nejčastěji narazit v příloze s názvem „DRAFT MBL LHV3495264 327291535_V2.exe".

Dlouhodobá přítomnost spywaru v Česku není dána jen mírou jeho úspěšnosti, ale také tím, že je to oblíbený nástroj v rukou útočníků. Škodlivé kódy, které se obecně využívají ke krádežím uživatelských dat, přístupových údajů a hesel, jsou rozšířené i díky tomu, že taková data a údaje mají dnes velkou cenu na černém trhu.

Hlavním motivem většiny kybernetických útoků je finanční zisk. Odcizené údaje a data útočníci dále přeprodávají a ty pak slouží k jiným útokům. Mohou je například využít tak, že zkusí dosazovat zjištěná přihlašovací jména a hesla k přihlášení do účtů řady populárních služeb. Cílem je co nejvíce účtů odcizit a dále je zneužít nebo je opět prodat. Bezpečnostní experti proto opakovaně apelují na uživatele, aby měli pro každý svůj online účet vždy unikátní heslo, které pak již znovu nepoužijí.

„Uživatelská hesla nejsou jediným cílem spywaru. Zaměřuje se také na informace o našem chování na internetu či o našem zařízení. Jsou to například informace o spouštěných aplikacích, otevíraných souborech a času, který na zařízení trávíme. Spyware sbírá informace i o nainstalovaném softwaru a o hardwaru našeho zařízení. Na základě těchto údajů si může útočník vytvořit celý profil své oběti a odcizit například i její identitu," vysvětluje Jirkal.

Zdrojem spywaru bývají škodlivé spustitelné soubory s příponou .exe, kterou však řada uživatelů a uživatelek nemusí vůbec postřehnout. Škodlivé soubory mohou mít koncovky dvě, přičemž ta dobře viditelná často vytváří dojem, že se jedná o nezávadný dokument v programu MS Word, ve formátu PDF nebo o obrázek.

Jak bezpečnostní experti upozorňují, obrana před spywarem by měla být složena z několika jednotlivých kroků a jako uživatelé k ní musíme přistupovat z různých úhlů. Na začátku by měla být rozhodně naše obezřetnost.

„Spyware se šíří kromě e-mailových příloh také v různých aplikacích a souborech, na které můžeme narazit na veřejných internetových úložištích nebo fórech. Svou bezpečnost tak může každý z nás podpořit tím, že budeme ostražití v případě nevyžádaných zpráv od neznámých uživatelů, nebo v případě komunikace, která bude vyvolávat dojem naléhavosti a vzbuzovat v nás například strach. V nevyžádaných zprávách bychom nikdy neměli otevírat přiložené soubory, stahovat je do zařízení a klikat na odkazy. Pokud se rozhodneme stáhnout si nějakou aplikaci nebo program mimo oficiální stránky a obchody, je důležité myslet na to, že si vždy stáhneme i něco, co v zařízení mít nechceme. Ať už se bude jednat třeba jen o zdánlivě neškodnou reklamu, nebo právě o spyware," dodává Jirkal z ESETu.

Kvalitní bezpečnostní software je pak další pojistkou pro případy, kdy přes všechnu opatrnost stáhneme malware do svého počítače. Konkrétně v případě škodlivých e-mailů vytvoří program bezpečnou složku, do které detekovanou hrozbu přesune. Uživatelé si mohou poté e-mail ve složce v případě zájmu prohlédnout a pak jej smazat. Pokud bezpečnostní program rozpozná škodlivý kód v nějakém souboru, dokáže spuštění souboru zablokovat a přesunout ho do tzv. karantény, o čemž jsou uživatelé vždy informováni.

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-skodlivy-kod-agent-tesla-v-srpnu-utlumil-svou-aktivitu-spyware-vsak-v-cesku-presto-utocil