

Spyware Formbook potvrdil, že je novou hrozbou číslo jedna pro české počítače

17.12.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

V listopadu se počet detekcí spywaru Formbook nečekaně přiblížil k podílu téměř poloviny všech zachycených případů v Česku. Vyplývá to z pravidelné statistiky kybernetických hrozeb pro operační systém Windows v České republice od společnosti ESET.

V listopadu se nejvíce objevovaly nebezpečné e-mailové přílohy s českými překlady, které útočníci v některých případech vydávali i za domnělé faktury s vyúčtováním energií.

Podle expertů společnosti ESET již spyware Formbook definitivně nahradil v Česku dlouhodobě dominující spyware Agent Tesla. Ten se pro tuto chvíli drží co do počtu detekcí na druhé příčce pravidelné statistiky. Podobně jako ostatní typy spywaru, i Formbook útočníci používají ke krádežím citlivých informací z počítačů s operačním systémem Windows. Formbook se specializuje na naše údaje uložené v prohlížečích, dokáže pořizovat snímky obrazovky, zaznamenávat stisknuté klávesy a stahovat a spouštět další soubory.

„Spyware Formbook stál v listopadu téměř za polovinou všech případů škodlivého kódu v Česku. Útočné kampaně, ve kterých ho útočníci využili, byly nejsilnější v období od 13. do 15. listopadu. Útočníci nadále pokračují v rozesílání falešných e-mailů, které vydávají za informace k objednávkám nebo nákupům. Již od minulého měsíce si navíc opět dávají práci s překlady názvů nebezpečných příloh obsahujících spyware do češtiny – nejčastěji zastoupená příloha se jmenovala Úhrada faktury k platbě 12. listopadu 2024.xlsx.exe,“ říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

V listopadu bezpečnostní experti zachytili také kampaně spywaru Agent.BWU. Byly zacílené na celý region střední Evropy. Na české uživatele a uživatelky pak konkrétně cílily e-mailové přílohy, které útočníci vydávali za faktury s vyúčtováním energií.

„Vynalézavost útočníků je velká a dokládá to i jejich dobrá znalost chování uživatelů a přehled pohledávek, které pravidelně v určité období musí zaplatit. Vánoce pro ně bohužel bývají z pohledu útoků úspěšným obdobím, protože řada z nás může ve spěchu falešný e-mail přehlédnout a přílohu se spywarem spustit,“ vysvětluje Jirkal a dodává: „Spyware se zaměřuje na naše hesla a přístupové údaje do různých online účtů. Pokud bych měl uživatele upozornit na jednu oblast, které by v kontextu této hrozby měly věnovat pozornost, tak jsou to naše hesla a jejich bezpečná správa. Úplně tím základním pravidlem je to, že si pro každý účet vytvoříte jedinečné heslo, které nikde nebudete opakovat. V případě jeho krádeže totiž zamezíte tomu, aby útočníci po jeho získání prolomili stejnou kombinací vašeho e-mailu a hesla i jiné účty pomocí automatizovaných útoků.“

Podle nejnovějšího průzkumu od společnosti ESET, který byl zaměřen na nákupní chování českých uživatelů a uživatelek na internetu, pouze čtvrtina z nás správně využívá unikátní heslo pro přihlášení do našich účtů v e-shopech. Třetina z nás pak hesla používá opakovaně nebo je minimálně obměňuje. Meziročně se v tomto chování bohužel příliš nelepšíme, a to ani v kontextu stále připomínané hrozby v podobě spywaru.

„Dostatečně silné heslo by mělo mít minimálně 12 znaků včetně velkých a malých písmen, číslic nebo speciálních znaků. Dále je také důležité, jak svá hesla spravujeme a uchováváme. V našem posledním průzkumu lidé nejčastěji odpovídali, že si hesla pamatují z hlavy, někdy si je zapisují na papír, nebo

je uloží do prohlížeče. Právě ale internetové prohlížeče mohou být vůči spywaru zranitelné. Speciální programy, tzv. správce hesel, využívá 15 % lidí. Jedná se přitom o nejspolehlivější nástroj k bezpečnému uchovávání přihlašovacích údajů v zašifrované podobě," říká Jirkal z ESETu.

Správce hesel si mohou uživatelé pořídit samostatně nebo v rámci moderního bezpečnostního softwaru. Usnadňuje používání unikátních silných hesel, která jsou příliš složitá k zapamatování z hlavy. Uživatelé si musí pamatovat jen jedno heslo, a to pro přístup do této služby.

Moderní bezpečnostní software je navíc vhodnou profesionální ochranou před spywarem a pojistkou, pokud přeci jen v nepozornosti otevřeme nebezpečnou e-mailovou přílohu se škodlivým kódem. 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 výzkumná a 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

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.cz

<https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-spyware-formbook-potvrdil-ze-je-novou-hrozbou-cislo-jedna-pro-ceske-pocitace>