ESET: Největším rizikem pro počítače v Česku byl v září spyware Formbook

22.10.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

Spyware Formbook, který se v Česku vyskytuje dlouhodobě po boku spywaru Agent Tesla, byl v září již druhým měsícem nejčastěji detekovanou hrozbou pro uživatele operačního systému Windows. Vyplývá to z pravidelné statistiky kybernetických hrozeb společnosti ESET. Útočníci jej šíří především v globálních e-mailových kampaních a nebezpečné přílohy se tak v jeho případě zatím neobjevují s českými názvy. S ohledem na jeho dosavadní růst lze podle expertů očekávat podobný vývoj i v následujících měsících. Spyware útočníci využívají ke krádežím našich dat. Rizikem je především pro nedostatečně zabezpečená uživatelská hesla.

Zatímco v září počet případů spywaru Agent Tesla dále klesal až k hranici osmi procent všech zachycených případů, spyware Formbook opět posílil a počet jeho detekcí v září vzrostl na 16 procent. Spyware Formbook poprvé převzal vedoucí roli v pravidelné statistice letos v srpnu.

„Od začátku roku pozorujeme, že se spyware Agent Tesla střídavě objevuje v čele statistiky anebo ho dočasně vystřídá jiný škodlivý kód. U spywaru Formbook to ale zatím vypadá, že bude v následujících měsících naopak ještě posilovat. Pro uživatele se však situace příliš nemění. Nadále by měli zůstat ostražití před nebezpečnými e-mailovými přílohami, protože i v případě spywaru Formbook útočníci využívají osvědčené strategie, jejichž úspěšnost nejen v Česku dlouhodobě testují," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Spyware Formbook byl nejvíce aktivní 4. září. Útočníci šířili škodlivý kód především v příloze s názvem „PO#86637.exe". Přílohu vydávali za shrnutí objednávky z e-shopu. Útoky se zatím podle bezpečnostních expertů neobjevily v češtině.

„Uživatelé a uživatelky by v případě spywaru neměli podcenit profesionální zabezpečení svých dat. Spyware je totiž poměrně obtížně odhalitelný a dlouhou dobu může bez povšimnutí škodit v napadeném zařízení. Útočníci využívají spyware ke krádeži celé řady dat, jako jsou naše soubory, data o našem chování na internetu a samozřejmě naše přihlašovací údaje do různých účtů. Zvlášť nebezpečný je pro naše hesla, která ukládáme například do internetových prohlížečů namísto do šifrovaných správců hesel. V konečném důsledku mohou útočníci sesbírat jednotlivé střípky informací o naší osobě a využít je ke krádeži naší identity," vysvětluje Jirkal.

Útočníci dlouhodobě využívají e-mailovou komunikaci k doručení spywaru ke svým obětem. Zejména v případě zaměstnanců firem, kteří denně pracují s velkým objemem elektronické pošty, je riziko napadení spywarem vysoké. Nevyhýbá se ale ani uživatelům z řad domácností, které se útočníci snaží zmást přílohami s názvy, které odkazují na nějaké objednávky.

„V případě třech nejčastějších škodlivých kódů za září se přílohy s českými názvy objevovaly jen u spywaru Agent.AES, kde jsme zachytili přílohu s názvem kopie platby. Jak ale v případě tohoto spywaru, tak i v případě spywaru Agent Tesla jsme pak pozorovali řadu příloh s anglickými názvy odkazujícími na faktury. V závěru roku, kdy nás čeká nejsilnější sezóna z pohledu nakupování na internetu, může takový e-mail zapadnout mezi řadu ostatních legitimních zpráv a uživatelé pak mohou přílohu snadno spustit," říká Jirkal.

Nejvíce využívaná příloha šířící spyware Agent Tesla se v září jmenovala „Order 240916.exe".

Spyware Agent.AES se pak ukrýval v přílohách s názvy „Outstanding Payment Against Overdue Invoices.exe“, nebo v již zmíněné příloze „kopie platby09886673.exe“.

Jak ukázal nedávný průzkum společnosti ESET, někteří uživatelé a uživatelky stále ještě nenakládají správně se svými uživatelskými hesly. Čtvrtina z nás je stále tvoří 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“. Řadu našich osobních informací přitom mohou útočníci najít veřejně na různých sociálních sítích. Příliš jednoduchá hesla pak mohou snadno prolomit automatizované útoky.

„Lidé tvoří jednoduchá hesla většinou proto, aby si je mohli dobře pamatovat z hlavy. Taková hesla ale nejsou dost složitá a bezpečná. Uživatelé mohou navíc využívat jedno stejné heslo do více služeb, což ale bývá také velmi častým důvodem prolomení účtu,“ dodává Jirkal z ESETu.

Hesla experti doporučují doplnit ještě dalším faktorem, například kódem v SMS nebo ve spárované ověřovací aplikaci. S uchováváním hesel mohou uživatelům pomoci také specializovaní správci hesel, jako např. ESET Password Manager. Uživatel do nich zadá všechna svá hesla, které program chrání šifrováním a automaticky je doplňuje při přihlášení k jednotlivým účtům. Uživatel si pak pamatuje jen jedno heslo, a to pro přihlášení do této služby. Kvalitní bezpečnostní software jim pomůže také odchytit škodlivé e-maily a zablokovat spuštění souboru, ve kterém rozpozná škodlivý kód.

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-nejvetsim-rizikem-pro-pocitace-v-cesku-byl-v-zari-spyware-formbook