ESET: Útočníci využívají nejsilnější nákupní sezónu roku k šíření spywaru

21.11.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

Již třetím měsícem zůstává v čele pravidelné statistiky kybernetických hrozeb pro operační systém Windows v Česku spyware Formbook. Ve větším útoku jej v říjnu i nadále doplňoval spyware Agent Tesla. Bezpečnostní experti z ESETu v říjnu opět zachytili zvýšené množství nebezpečných e-mailových příloh s českými překlady, které útočníci dlouhodobě využívají k šíření těchto škodlivých kódů. Není podle nich pochyb, že se útočníci připravují na každoroční hlavní sezónu nakupování, a to právě i zacílením přímo na české uživatele a uživatelky. Vyplývá to z pravidelné statistiky kybernetických hrozeb společnosti ESET.

Spyware Formbook zůstal i v říjnu nejčastějším škodlivým kódem pro operační systém Windows v Česku. Počet jeho detekcí nicméně oproti minulému měsíci klesl o necelá čtyři procenta. Ve velkém útoku se k tomuto škodlivému kódu přidal i známý spyware Agent Tesla. V případě obou škodlivých kódů se v říjnu do Česka opět vrátily útoky s českými překlady.

„Zatímco v minulých měsících jsme vídali češtinu spíše ojediněle, v říjnu jsme opět zaznamenali nárůst e-mailových příloh, které byly přeloženy do češtiny. Útočníci přílohy opět maskují za objednávky a faktury. Především v případě spywaru Agent Tesla jsme mohli pozorovat velký útok v polovině října. Útočníci spyware ukryli do škodlivé přílohy, kterou vydávali za fakturu," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

„Útočné kampaně aktuálně sledujeme, nejedná se ale o nijak nestandardní situaci. Blíží se závěr roku, který je vždy z pohledu nakupování na internetu nejsilnějším obdobím. Proto bych uživatelům doporučil, aby hrozby v podobě falešných e-mailů nepodceňovali. Právě před Vánoci budeme mít všichni e-mailové schránky plné potvrzení objednávek a faktur a nebezpečný e-mail se škodlivou přílohou se v záplavě těchto zpráv může snadno ztratit," varuje Jirkal a vzápětí dodává: „Uživatelům bych na prvním místě doporučil, aby u e-mailových zpráv kontrolovali adresu odesílatele. Určitě by si měli všímat, zda text neobsahuje strojové překlady do češtiny. V předvánočním shonu se může zdát nereálné zpomalit, právě ale nepozornost a spuštění neznámé přílohy nebo neopatrné kliknutí na škodlivý odkaz může vpustit škodlivé kódy do našich zařízení."

Spyware Formbook se v říjnu nejčastěji ukrýval v přílohách s názvy „SPA-198-2024.exe" a „OBJEDNAT.scr". Zdrojem spywaru Agent Tesla pak byla již zmíněná příloha s českým překladem „faktura 10-2024 vyúčtování k platbě.xlsx.exe". Spyware Agent.AES se sice neobjevil v kampaních s českými překlady, i v jeho případě však přílohy odkazovaly na platby – jednalo se například o přílohy s názvy „payment advice.exe" nebo „PAYMENtT SLIP.exe".

Společným znakem nebezpečných e-mailových příloh šířících spyware je přípona .exe. Ta poukazuje na nějaký spustitelný soubor. Aby útočníci uživatele zmátli, přílohy využívané v jejich útocích mívají zpravidla koncovky dvě, přičemž právě přípona .exe nemusí být vůbec viditelná. Uživatelé se naopak domnívají, že jim odesílatel přiložil ke zprávě například dokument v programu MS Word, ve formátu PDF nebo obrázek.

„Útočníci proti nám často využívají osvědčené triky, protože velmi dobře znají lidskou psychiku. A jsou to právě období velkých svátků nebo prázdnin, kdy naši pozornost zkouší nejvíc. Spyware již patří k závažnějším typům kybernetických hrozeb. Jeho cílem je odcizit naše osobní data, z nichž některá mohou spadat do kategorie opravdu citlivých dat – například údaje o bankovních účtech a

kartách. V počítači může zůstat nějakou dobu bez povšimnutí. Útočníci mohou získaná hesla a osobní data využít k přípravě dalších útoků nebo je prodají na dark webu. Uživatelům bych určitě doporučil zvážit profesionální ochranu jejich zařízení moderním bezpečnostním softwarem," říká Jirkal. „Právě letos na podzim jsme představili aktualizovanou nabídku pro domácnosti doplněnou o několik nových funkcí. Nová zabezpečená složka ESET Folder Guard například chrání cenná data uživatelů před malwarem, který se je snaží poškodit. Uživatelé mohou vytvořit až několik zabezpečených složek, ke kterým budou mít přístup jen důvěryhodné a uživatelem povolené aplikace. Další nová funkce, Ochrana identity, pak monitoruje černý trh s prodejem osobních údajů a upozorní uživatele, pokud se s jeho údaji obchoduje na dark webu," dodává Jirkal z ESETu.

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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-utocnici-vyuzivaji-nejsilnejsi-nakupni-sezonu-roku-k-sireni-spywaru