Falešné e-maily obsahující škodlivý kód cílí na vybrané evropské státy, včetně České republiky

21.11.2023 - Rita Gabrielová, Lucie Mudráková | ESET software

Spyware Agent Tesla byl i v říjnu nejčastěji detekovaným škodlivým kódem pro operační systém Windows v Česku. Po jeho boku se opět objevil také malware Agent.QMG, pokročilý škodlivý kód, jehož úkolem je stahovat do napadeného zařízení další malware, a to včetně zmíněného spywaru. Podle analýzy bezpečnostních expertů se útočníci zaměřují na vytipované evropské státy, pro které následně upravují útočné kampaně na míru. V říjnu takto zacílili na české uživatele falešnými e-maily s žádostmi o cenové nabídky nebo s upozorněním na doručení balíku od přepravní společnosti DHL. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Podle pravidelné měsíční statistiky kybernetických hrozeb pro operační systém Windows v říjnu opět mírně posílil spyware Agent Tesla. Nejsilněji na české uživatele útočil ze začátku měsíce. Útočníci k jeho šíření využívají e-mailové přílohy, které záměrně vydávají za různé oficiální dokumenty.

„Od září pozorujeme u spywaru Agent Tesla větší množství příloh, které útočníci překládají do češtiny. Zrovna v tomto případě se nejedná o standardní situaci, protože spyware Agent Tesla je celosvětově rozšířeným škodlivým kódem a útočné kampaně tak spíše evidujeme v angličtině. Aktuálně se v Česku ale objevují stále přílohy, které mají například název děkovný dopis.docx.exe nebo Zpusob_platby,jpg.exe," říká k říjnovému vývoji Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

V říjnu se mezi nejčastějšími škodlivými kódy opět objevil také malware Agent.QMG. Podle bezpečnostních specialistů byl tento škodlivý kód naopak s jasným záměrem zacílen na české uživatele.

„Škodlivý kód Agent.QMG se v Česku nejvíce objevoval na konci října. V jeho případě jsme viděli české překlady již v samotných předmětech e-mailů. Útočníci e-maily zkoušeli vydávat například za žádost o cenovou nabídku nebo za upozornění na balíky od přepravní společnosti DHL. Z podrobnější analýzy jsme také zjistili, že se útočníci primárně specializují na Evropu a cílí postupně na jednotlivé státy. Kromě Česka útočili v říjnu také na Maďarsko, Španělsko, Bulharsko a Itálii," vysvětluje Martin Jirkal.

Dalšími nebezpečnými přílohami, se kterými se čeští uživatelé mohli v říjnu setkat, byla například příloha s názvem „Inquiry_pdf.exe" šířící spyware Agent Tesla, nebo příloha „100037779694.vbe" šířící právě malware Agent.QMG.

Spyware patří v České republice ke stálým rizikům. Jeho prostřednictvím se útočníci zaměřují na odcizení našich osobních údajů, především pak uživatelských hesel. Hesla totiž zůstávají velmi žádanou komoditou – útočníci je mohou využít k řadě dalších útoků, například k útokům tzv. hrubou silou, nebo dále přeprodat na černém trhu.

„Vedle konkrétních typů spywaru, kterými jsou spyware Agent Tesla nebo spyware Formbook, útočníci využívají i další malware, jako je například právě Agent.QMG. Jedná se o sofistikovaný a nebezpečný škodlivý kód, který je přizpůsobený k tomu, aby ho nebylo snadné analyzovat. Jeho

primární funkcí je stahovat do napadeného zařízení spyware a další typy škodlivých kódů. Útočníci jím tak útoky podporují a usnadňují spywaru přístup do našich počítačů," říká Jirkal.

Spolu s útoky na naše hesla roste i nutnost je optimálně a účinně chránit. Heslo nadále zůstává hlavním bezpečnostním prvkem u řady našich online služeb a jako takové je tak zranitelné před řadou útočných strategií, ať už se jedná o útoky škodlivým kódem, nebo o phishing, metodu tzv. sociálního inženýrství, jejímž cílem je hesla a další přístupové údajů získat přímou, manipulativní komunikací s uživateli.

„Z našich zkušeností víme, že uživatelé často nevytvářejí silná hesla, protože se taková hesla špatně pamatují. Tím ale dávají všanc nejen své finance, ale také citlivé osobní údaje a své soukromí. Se správou jim mohou pomoci přitom správci hesel, specializované programy, které bezpečně uchovávají přihlašovací údaje v zašifrované podobě a automaticky je vyplňují při přihlašování do našich účtů. Jsou tak daleko bezpečnější variantou k zapisování hesel na kousek papíru a uživatelé už nemusí tvořit dobře zapamatovatelná, ale slabá hesla, nebo je opakovaně používat u více svých účtů," dodává Jirkal z ESETu.

Správce hesel mohou uživatelé pořídit jako samostatný program, je ale také součástí kvalitních bezpečnostních řešení. Ty navíc uživatele chrání před řadou dalších hrozeb, jako je například spyware, nežádoucí aplikace nebo nebezpečné webové stránky.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

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 produktů 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-falesne-e-maily-obsahujici-skodlivy-kod-cili-na-vybrane-evropske-staty-vcetne-ceske-republiky