Spyware v dubnu překročil hranici pětiny všech detekcí, v Česku ho stále šíří spam

16.5.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Ke stabilně detekovaným škodlivým kódům pro operační systém Windows v Česku – spywaru Agent Tesla a spywaru Formbook – se v dubnu připojil na předních místech detekční statistiky malware Agent.QMG, který bezpečnostní specialisté pozorovali již na podzim loňského roku.

Nebezpečné e-mailové přílohy, jejichž prostřednictvím se tyto škodlivé kódy dlouhodobě šíří Českem, se tentokrát neobjevovaly v českém překladu. Bezpečnostní specialisté uživatelům a uživatelkám doporučují, aby k obraně svých dat využili kromě opatrného nakládání se svou online komunikací i správně nastavenou antispamovou ochranu. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Po březnovém útlumu se dubnová detekční čísla spywaru Agent Tesla opět vyšplhala nahoru. S více než pětinou zachycených případů byl tento malware nejsilnější od začátku letošního roku.

„Spyware Agent Tesla se stále drží v čele pravidelné statistiky hrozeb a v dubnu dokonce oproti předchozím obdobím o něco posílil. Jeho cílem zůstávají přihlašovací údaje do našich účtů, a to především hesla, která mají svou cenu na černém trhu. Sloužit totiž mohou k přípravě dalších kampaní, jako jsou například útoky tzv. hrubou silou, během kterých útočníci zkoušejí prolomit naše účty za pomoci automatizovaného dosazování velkého množství hesel," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Škodlivé kódy se v případě operačního systému Windows v Česku šíří dlouhodobě prostřednictvím spamových kampaní, které obsahují nebezpečné e-mailové přílohy s různými názvy. Pokud uživatelé přílohu stáhnou a otevřou, vpustí škodlivý kód do svého počítače.

Společným znakem všech nejčastějších škodlivých kódů dubnové statistiky byly tentokrát přílohy bez českých překladů. Spyware Agent Tesla se nejčastěji objevil 3. dubna, a to v přílohách s názvy „PO.exe", „PO116/PO116.exe" a „PO-095325.scr". Spyware Formbook, další z dlouhodobě přítomných škodlivých kódů pro operační systém Windows v Česku, se pak nejvíce ukrýval v příloze s názvem „RFQ ML - CONTG. 0992-19-PD.exe". Malware Agent.QMG, který se na předních místech statistiky opět objevil po několika měsících, zase nejčastěji obsahovala příloha „Žiadosť o cenu #2414976·pdf.vbs". Ačkoli se v tomto případě do Česka dostal e-mail se slovenským překladem, českou verzi bezpečnostní specialisté ani v případě tohoto škodlivého kódu nezachytili.

„Kromě spywaru využívají útočníci k odcizení našich dat samozřejmě i další malware, jako je například právě Agent.QMG," vysvětluje Jirkal a dodává: „Škodlivý kód Agent.QMG je již poměrně sofistikovaný a nebezpečný. Je také 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 ostatní útoky podporují a usnadňují spywaru přístup do našich počítačů."

Podle bezpečnostních expertů je pro bezpečnost naší elektronické pošty důležité využívat kvalitní bezpečnostní software a zároveň se řídit osvědčenými bezpečnostními zásadami, mezi které patří například opatrnost při otevírání spamových e-mailů od neznámých uživatelů a správná tvorba a správa našich přihlašovacích údajů. Jak ukázal poslední průzkum společnosti ESET, v Česku máme stále sklony vytvářet hesla z osobních údajů. Kvůli tomu jsou ale naše hesla zbytečně zranitelná vůči

útokům.

„Měli bychom mít vždy na paměti, že před pokročilými hrozbami, mezi které se spyware již směle řadí, nás vždy nejspolehlivěji ochrání pouze bezpečnostní program, který ho dokáže včas identifikovat a zastavit. V souvislosti se spamem však musíme nejen v Česku čelit čím dál více i manipulativní komunikaci využívající techniky sociálního inženýrství, které zase včas dokážeme odhalit spíše díky naší obezřetnosti a skepsi k dnešní online komunikaci. Vždy tak uživatelům a uživatelkám připomínáme, že naprostým základem je neotevírat a neklikat na přílohy a odkazy ve zprávách od neznámého odesílatele a důkladně si prověřovat znění i podobu každého e-mailu, zprávy v chatu nebo v SMS, která nám přijde bez předchozího vyžádání a neočekávaně," doplňuje Jirkal z ESETu.

Nebezpečné e-mailové přílohy nejsou v českém prostředí novou strategií a můžeme se před nimi chránit například dobře nastavenou antispamovou ochranou. Se správou našich přihlašovacích údajů nám pak může pomoci například správce hesel, program, který hesla uchovává v zašifrované podobě a automaticky je dosazuje při přihlašování do našich účtů. Obě funkce jsou dnes již součástí kvalitních a komplexních bezpečnostních řešení.

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-spyware-v-dubnu-prekrocil-hranici-petiny-vsech-detekci-v-cesku-ho-stale-siri-spam