ESET: Snake Keylogger nebo Infostealer Formbook? Kyberhrozby se v Česku každý měsíc rychle střídají

17.4.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Pořadí nejčastěji detekovaných škodlivých kódů pro operační systém Windows v Česku se aktuálně mění z měsíce na měsíc. Zatímco ještě v únoru byl největším rizikem malware Agent.AES, známý také jako Snake Keylogger, v březnu jej se stejným počtem zachycených detekcí opět vystřídal infostealer Formbook. Bezpečnostní experti tak situaci stále monitorují, a to v prostředí, ve kterém před několika měsíci došlo k útlumu dlouhodobě dominantního infostealeru Agent Tesla. Podle nich útočníci škodlivé kódy velmi dynamicky vyvíjejí a o to větší nebezpečí mohou představovat pro uživatele a uživatelky. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Nejsilnější útočné kampaně infostealeru Formbook probíhaly z 10. na 11. března a pak koncem měsíce, 28. a 31. března. Nejčastější škodlivá příloha se tentokrát jmenovala „Purchase Order 139022.exe“. Bezpečnostní experti při bližším pohledu potvrdili, že útočníci se ve všech případech snažili své oběti nalákat na e-mail s informacemi o doručování balíku.

„Infostealer Formbook má aktuálně jasně ohraničené útočné kampaně a mimo ně byli útočníci v březnu aktivní spíše ojediněle. V první polovině měsíce a koncem března však byly zachycené útoky silné. Mohlo by se zdát, že infostealer je tak méně nebezpečný, ale opak je spíše pravdou, protože aktuální útoky jsou zacílené na konkrétní státy a útočníci do nich investují více zdrojů. Využívají i zcela nové verze způsobů útoku,“ vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Infostealer Formbook se v březnu objevil se stejným počtem detekcí, jako v únoru Snake Keylogger alias Agent.AES. Došlo tak k tomu, že si tyto dva škodlivé kódy prakticky vyměnily své pozice. Keylogger zaznamenává stisky kláves na klávesnici, dokáže ale odcizit data dalšími způsoby, které jsou typické pro tento typ škodlivých kódů. Útočníci jej neustále vyvíjejí. Dokážou s jeho využitím odcizit hesla z komunikačních platforem nebo e-mailových klientů, z FTP, webových prohlížečů nebo bezdrátových sítí. V březnu vyzkoušeli strategii, při které se pokusili zmást uživatele domnělými oskenovanými dokumenty v příloze e-mailů – „Scanned Copy.exe“ a „Scan Doc.exe“. Po jejich spuštění keylogger infikoval počítač oběti.

„V březnu jsme mohli opět vidět, jak nestabilní je aktuální situace poté, co autor infostealeru Agent Tesla ukončil jeho vývoj a jeho čísla se po několika letech dominantní převahy skokově propadly. Jak o infostealeru Formbook, tak o malwaru Agent.AES se mluví jako o jeho možných nástupcích. Evidentně zatím ani jeden z těchto škodlivých kódů nemá takovou převahu, jakou se právě vyznačoval Agent Tesla. Může za tím být i skutečnost, že oba typy škodlivých kódů útočníci dynamicky vyvíjejí, proto vždy u jednoho z nich zaznamenáme ve sledovaném měsíci pokles počtu detekcí. Není to dobrá zpráva pro uživatele a uživatelky, protože se budou setkávat se stále pokročilejšími a nebezpečnějšími verzemi malwaru,“ říká Jirkal.

Ačkoli i ve firmách jsou dnes stále více využívány různé komunikační platformy, e-mail stále zůstává oblíbeným prostředkem pro spojení s druhými lidmi a službami. Může za tím stát i jeho hojné využití jako přihlašovacího jména u celé řady internetových obchodů a služeb.

„Kromě infostealerů mohou útočníci prostřednictvím e-mailů šířit i ransomware nebo se vydávat za někoho jiného a manipulovat s námi. Této technice říkáme phishing, můžeme ale mluvit i o spoofingu, kdy útočník zfalšuje adresu odesílatele e-mailu tak, že vypadá legitimně. S tím, jak dnes žijeme rychle a musíme zvládat denně velký objem elektronické komunikace, můžeme snadno přehlédnout varovné ukazatele a nechtěně kliknout na nebezpečný odkaz nebo stáhnout a spustit škodlivou přílohu. Pro účinnou obranu před těmito hrozbami je tak za mě ideální kombinovat kvalitní bezpečnostní řešení s tvorbou silných unikátních hesel a využíváním vícefázového ověřování. Cílem infostealerů jsou naše data, především uživatelská hesla, která se dají dobře zpeněžit na černém trhu nebo rovnou využít k přípravě nového útoku. Jakmile útočníci odcizí jedno naše heslo, které využíváme na více místech, velmi rychle prolomí naše další účty," shrnuje Jirkal z ESETu.

Společnost ESET v březnu aktualizovala svou platformu ESET PROTECT, která je součástí řešení pro firemní zákazníky. Kromě nové funkce Obnova po útoku ransomwarem, která je dostupná v řešeních ESET PROTECT Advanced a vyšších, je součástí aktualizace také nová ochrana proti spoofingu a útokům využívajícím homoglyfy. Nově je součástí stávajícího řešení ESET Cloud Office Security (ECOS). Útočníkům brání v tom, aby se vydávali za důvěryhodné zdroje či osoby a rozpozná, pokud chtějí maskovat škodlivé domény nebo URL adresy záměnou písmen z jiných abeced. ESET Cloud Office Security navíc nyní také obsahuje funkci zpětného stažení e-mailů, která umožňuje rychle odvolat a umístit do karantény jakékoli doručené e-maily, které vyhodnotí jako podezřelé.

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.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

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.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-snake-keylogger-nebo-infostealer-formbook-kyberhrozby-se-v-cesku-kazdy-mesic-rychle-stridaji