Závěr roku potvrdil změny v rozložení kyberhrozeb v Česku, v čele se nadále drží škodlivý kód Formbook

23.1.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Na poli kybernetických hrozeb v České republice se potvrzují predikce bezpečnostních expertů z konce loňského roku.

Spyware Agent Tesla se již několikátý měsíc objevuje pouze v několika jednotkách procent případů a pro následující období se očekává jeho další oslabování a postupné vymizení ze statistik. Škodlivý kód Formbook sice nezopakoval skoro poloviční podíl všech detekcí z loňského listopadu, i s podílem 15 % všech zachycených hrozeb však nadále vede pravidelnou statistiku pro operační systém Windows. Bezpečnostní experti situaci v Česku monitorují a očekávají další možné změny v rozložení škodlivého kódu. Vyplývá to z detekčních dat společnosti ESET.

Detekce škodlivého kódu Formbook sice v prosinci oproti listopadu klesly na 15 % všech zachycených detekcí v Česku, stále však drží markantní náskok před spywarem Agent Tesla. Známý spyware, který kraloval české scéně kybernetických hrozeb pro operační systém Windows několik uplynulých let, se i v prosinci objevil pouze v jednotkách procent případů. Již dřívější závěry kyberbezpečnostních expertů se tak potvrzují – konec roku 2024 znamenal pravděpodobně dlouhodobější změny v rozložení škodlivých kódů, které útočníci využívají ve svých kampaních.

„Infostealer Formbook je typem spywaru, který shromažďuje data ze schránky zařízení, stisky na klávesnici, snímky obrazovky i z mezipaměti prohlížeče. Podobně jako spyware Agent Tesla jsou jeho častým cílem také uživatelská hesla. Jedná se o škodlivý kód, který označujeme jako MaaS – malware as a service. Znamená to, že jeho autoři jej prodávají na různých neoficiálních fórech dalším útočníkům a tím přispívají k jeho masovému rozšíření. Typicky se šíří v podobě škodlivé přílohy v phishingovém e-mailu, před kterými opakovaně varujeme. I závěrem loňského roku měly tyto e-mailové přílohy nejčastěji podobu faktur nebo potvrzení o zásilkách jedné známé přepravní služby," komentuje vývoj kybernetických hrozeb v Česku Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Závěrem loňského roku začal výrazně slábnout spyware Agent Tesla, který si jistě zaslouží označení jednoho z nejdéle přítomných škodlivých kódů v České republice. Podle informací bezpečnostních expertů se objevují informace, že autor tohoto spywaru již nechce pokračovat v jeho vývoji. Očekávají tak, že i nadále bude slábnout až postupně ze statistiky zmizí úplně.

„Řada českých uživatelů a uživatelek se může ptát, co to tedy pro ně aktuálně znamená. Bez ohledu na to, který infostealer se právě objevuje ve statistice nejčastěji, je důležité nadále chránit svá data pomocí kvalitních bezpečnostních nástrojů a mít se na pozoru při čtení své elektronické pošty. Infostealery představují nezanedbatelné riziko pro naše přihlašovací údaje, proto je rozhodně nedoporučuji ukládat do počítače ani do internetových prohlížečů, které nemusí být před tímto typem útoků dostatečně zabezpečené. Vhodnou ochranou jsou v tomto případě správci hesel, programy specializované pro šifrované ukládání a bezpečnou správu našich přihlašovacích údajů," dodává Jirkal.

Skoro pětina českých uživatelů a uživatelek hodnotí bezpečnost svých hesel na základě toho, že si je

dobře pamatují. Jak ale bezpečnostních experti upozorňují, dobře zapamatovatelná hesla nemusí být dostatečně složitá a snadno se mohou stát terčem útočníků, kteří je bez obtíží prolomí. Nejčastěji si hesla pamatujeme právě z hlavy, zatímco specializovaný program pro správu našich hesel využívá jen část z nás.

„Základem bezpečného nakládání s hesly je rozhodně využívat vždy jedno unikátní heslo pro každý svůj online účet. Pokud se útočníci zmocní jednoho z vašich hesel, nedostanou se tak do dalších účtů. A oni to rozhodně zkusí. Slouží jim k tomu například automatizované útoky. Pro lepší správu svých hesel mohou uživatelé tvořit namísto nahodilého shluku různých znaků i tzv. heslové fráze, které si lépe zapamatují. Typicky se jedná o nějakou větu, která dává smysl jen vám a dobře se vám pamatuje. Vyvarujte se jen známých textů z písní a hlášek z filmů. Všechna svá hesla opatřete také dalším faktorem ověření – kódem z SMS nebo ze spárované ověřovací aplikace," radí Jirkal z ESETu.

Spolehlivou pojistkou před nechtěným otevřením škodlivé přílohy a vpuštěním škodlivého kódu do zařízení je bezpečnostní software. Dokáže vytvořit bezpečnou složku, do které zjištěnou hrozbu přesune. Uživatelé si poté mohou e-mail ve složce v případě zájmu prohlédnout a pak jej smazat. Pokud bezpečnostní program rozpozná škodlivý kód v nějakém souboru, dokáže spuštění souboru zablokovat a přesunout ho do tzv. karantény, o čemž jsou uživatelé vždy informováni.

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 anebo v podcastu TruePositive.

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.

Lucie Mudráková

Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.cz

ni-kyberhrozeb-v-cesku-v-cele-se-nadale-drzi-skodlivy-kod-formbook