Kyberhrozbou číslo jedna byl v loňském roce infostealer Formbook

15.1.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Ačkoli prosincová statistika tentokrát nepotvrdila žádné masivní kampaně škodlivých kódů v České republice, poukázala na hrozby, se kterými se budou čeští uživatelé a uživatelky pravděpodobně setkávat i v příštím roce. Jasným rizikem číslo jedna zůstává dle kyberbezpečnostních expertů infostealer Formbook, který se zaměřuje na naše osobní data, a to především na přihlašovací údaje. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Zatímco ještě v listopadu se mohli čeští uživatelé a uživatelky setkat s velkou kampaní škodlivého kódu CloudEye, ke konci roku jeho aktivita výrazně poklesla. Stále však zůstal jednou z hlavních kybernetických hrozeb v Česku. Útočníci v jeho případě vsadili na falešné e-maily s přílohami, které budily dojem, že odesílatelem je pojišťovna. Do čela pravidelné statistiky se pak na konci roku vrátil infostealer Formbook.

„Dalo by se říct, že i poslední statistika kybernetických hrozeb pro operační systém Windows v loňském roce potvrdila případy škodlivých kódů, které jsme monitorovali v průběhu celého uplynulého roku. Výjimkou může být malware CloudEye, který se téměř ve čtvrtině všech zachycených případů objevil v Česku po delší odmlce v listopadu. Přestože je CloudEye, známý také pod názvem GuLoader, propagován jako legitimní služba pro ochranu souborů, ve skutečnosti jde o downloader a kryptor typu malware-as-a-service. Znamená to, že útočníci se již nemusí obtěžovat jeho vývojem, ale mohou jej na černém trhu koupit a využívat úplně stejně, jako si my koupíme nějaký softwarový program. Útočníci jej používají k tomu, aby na napadeném zařízení rozšířili další škodlivé kódy – vyděračský ransomware a infostealery Formbook, Agent Tesla či Rescoms. Jedná se o velmi pokročilý škodlivý kód, který je přizpůsobený k tomu, aby nešel tak snadno analyzovat," shrnuje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Nejsilnější útoky malwaru CloudEye zachytili bezpečnostní experti 10. a 11. prosince 2025. Přílohy útočných e-mailů, které malware ukrývaly, byly nejčastěji pojmenovány „Bank Transfer Confirmation - Advance Payment for PO 4500725711_pdf.js". Čeští uživatelé a uživatelky pak mohli narazit na již zmíněnou přílohu „Predpis_pojistne_smlouvy".

Až na pár měsíců minulého roku byl převládající loňskou hrozbou infostealer Formbook. A potvrdil to i v prosinci, kdy naposledy vystoupal s největším podílem měsíčních detekcí do čela pravidelné statistiky. Nejsilnější kampaň zachytili kyberbezpečnostní experti 18. a 19. prosince. Útočníci jej šířili ve škodlivé příloze s názvem „msedge_elf.dll".

„Útočníci v prosinci šířili infostealer Formbook buď napřímo ve škodlivých přílohách, nebo ukrytý v dalším škodlivém kódu s názvem Agent.ECK. K tomu musíme ale ještě připočíst fakt, že i malware CloudEye mohl na zařízení, které jeho prostřednictvím útočníci napadli, finálně opět stáhnout infostealer Formbook. Závěr roku tak i do budoucna naznačil, před jakým škodlivým kódem bychom se měli mít v Česku na pozoru. Až na pár měsíců, kdy pravděpodobně probíhala příprava nových útoků a vývoj nových verzí tohoto malwaru, byl Formbook vloni jednoznačnou volbou kyberútočníků v našem regionu. Očekávám, že tomu tak zůstane i v následujícím roce," říká Jirkal.

Ani letos bezpečnostní experti nepočítají s tím, že by se úroveň rizika v podobě infostealerů měla v Česku snižovat. Vysokou popularitu našeho regionu jako cíle e-mailových kampaní pak potvrdil i

třetí, prosincový případ škodlivého kódu Agent.HRS. Přes darknet může stahovat například nechvalně proslulý infostealer Agent Tesla. V prosinci byly kampaně připravené na míru českým uživatelům, o čemž svědčila i nebezpečná příloha s názvem „Přenést kopii.exe“, která škodlivý kód ukrývala.

Infostealery útočníkům slouží jako velmi efektivní nástroj k odcizení našich dat. Vyhledávaným cílem jsou pak především naše uživatelská hesla.

„Rok 2026 by měl být z mého pohledu rokem, kdy by uživatelé a uživatelky měli ke svým osobním datům přistupovat podobně jako k financím a věnovat jim náležitou ochranu. V případě správného nakládání s hesly bych rozhodně doporučoval věnovat pozornost tomu, abychom vždy měli pro každý účet jen jedno heslo. Pokud máme více stejných hesel pro různé účty, můžeme útočníkům otevřít dveře na více místech. Hesla také rozhodně nedoporučuji ukládat do souborů v počítači ani do internetových prohlížečů, které nemusí být před infostealery dostatečně zabezpečené. A v neposlední řadě je určitě na místě zvážit profesionální ochranu naší elektronické pošty a celého počítače, která dokáže velmi flexibilně reagovat na různé typy nových hrozeb, se kterými se v budoucnu setkáme,“ dodává Jirkal z ESETu.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete 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 RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

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

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

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/kyberhrozbou-cislo-jedna-byl-v-lonskem-roce-infostealer-formbook