

Škodlivý kód CloudEyE je zpět, v lednu se v Česku objevil ve dvou třetinách všech útoků

12.2.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Největší lednovou kybernetickou hrozbou pro operační systém Windows byl v Česku opět malware CloudEyE. Útoky byly tentokrát připravené přímo pro české uživatele a uživatelky. Zatímco bezpečnostní experti zachytili tento škodlivý kód v bezmála dvou třetinách všech případů, zaznamenali zároveň větší propad u infostealeru Formbook, který českému prostředí hrozeb pravidelně dominuje. K nějakému výraznému zvratu ve skladbě kyberhrozeb u nás ale dle nich nedochází - infostealer Formbook a řadu dalších hrozeb totiž skrytě šíří právě škodlivý kód CloudEyE. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Zatímco ještě na konci roku klesly případy malwaru CloudEyE na necelých 7 procent, hned zkraje ledna se jeho přítomnost v Česku skokově zvýšila.

„Nárůst případů škodlivého kódu CloudEyE jsme zaznamenali už během loňského listopadu. Tehdy se objevil s podílem pětiny všech zachycených detekcí. V prosinci se ale zase poměrně výrazně propadl. V lednu jsme jej opět zachytili s dramatickým nárůstem, a to v několika vlnách útoků na větší část Evropy,“ říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. „Česká republika byla v lednu mezi vybranými zeměmi, na které se útočníci spolu s tímto malwarem zaměřili. Podobně jako infostealer Formbook ho šíří v e-mailových spamových kampaních a ukrývají pod přílohy s názvy, kterými chtějí upoutat naši pozornost a přimět nás k jejich stažení a otevření. Hlavním úkolem tohoto škodlivého kódu je dostat do počítače jiný malware. Velmi často se jedná právě o [infostealery](#) určené ke krádežím osobních dat, především hesel. K tomu všemu má úroveň nebezpečí v podobě škodlivého kódu CloudEyE ještě jeden rozměr, na který bychom neměli zapomínat - jako nástroj je na [černém trhu](#) dostupný ke koupi jakémukoli útočníkovi, který může do našich zařízení nasadit škodlivý kód, který se mu zrovna bude hodit,“ dodává Jirkal z ESETu.

Škodlivé přílohy, které ukrývaly malware CloudEyE, měly v lednu názvy „2026-13-01-0273.js“, „IMG2026-01-15-3472.js“ nebo „SMLOUVA.js“. V České republice se pak objevovaly také přílohy pojmenované jako „Rozsah prací pro nabídky“. Malware CloudEyE v našem prostředí standardně šíří škodlivé kódy Agent Tesla, Rescoms či Formbook.

„Na základě naší lednové statistiky se může zdát, že infostealer Formbook, který byl v loňském roce největší kyberhrozbou v Česku, nahradil právě CloudEyE. Není to ale bohužel tak jednoduché. Spíše vidíme, že útočníci začali infostealer Formbook schovávat pod jiné škodlivé kódy, aby podpořili jeho šíření. Z tohoto důvodu tak nemůžeme říct, že by se stával méně nebezpečným, spíše naopak,“ vysvětluje Jirkal a dodává: „Hesla zcela jednoznačně zůstávají lovnou zvěří útočníků i v letošním roce. Jejich metody se navíc vyvíjejí s tím, jak jim s generováním podvodných e-mailových zpráv a názvů v různých jazycích mohou pomáhat [nástroje umělé inteligence](#). Určitě je tak na místě nepodceňovat základy bezpečného nakládání s našimi hesly - tvořit ideálně dostatečně dlouhá hesla obsahující znaky, číslice, velká a malá písmena, pro každý svůj účet mít unikátní heslo, které již nikde znovu nepoužívám, a neukládat je nikam do souborů v počítači ani do internetových prohlížečů.“

Hesla neohrožují jen infostealery

I přestože se škodlivý kód Agent.RIB v lednu objevil jen v několika procentech případů, jeho přítomnost na předních místech statistiky upoutala pozornost bezpečnostních expertů. Je totiž dalším příkladem, jak mohou útočníci získávat naše hesla a přístup k účtům. Nejedná se přitom o pokročilý škodlivý kód, jako jsou infostealery.

„Agent.RIB je opravdu velmi jednoduchý škodlivý kód, přesným opakem toho, co v našich pravidelných statistikách kyberhrozeb vidáme. Útočníci ho také šířili e-mailem. Ve zprávě odeslali svým obětem HTML soubor v příloze, který po otevření načetl webovou stránku s formulářem pro zadání přihlašovacího jména a hesla. Jakmile se tak stalo, údaje se odeslaly útočnickovi na platformu Telegram. Útok již pak nijak nepokračoval, šlo zcela evidentně jen o sběr uživatelských hesel. Ty pak útočník může využít k získání přístupu k našim účtům, například pomocí útoku nazývaného [credential stuffing](#). Pomocí speciálního softwaru mohou útočníci zadat získaná přihlašovací jména a hesla do velkého množství webových stránek. Riziko prolomení je v těchto případech největší u takových účtů, u kterých používáme opakovaně stejná hesla a nemáme u nich nastavené [vícefázové ověření](#),“ říká Jirkal z ESETu.

Kromě obezřetnosti u příchozí e-mailové komunikace je nedílnou součástí ochrany našich dat moderní [bezpečnostní software](#), který dokáže zamezit přístupu škodlivého kódu do našeho zařízení. Škodlivý e-mail dokáže včas rozpoznat a přesune jej do bezpečné složky, kterou za tímto účelem vytvoří. V předmětu e-mailu pak uživatelé uvidí, že se jedná o hrozbu. Zprávu si mohou následně ve vytvořené složce prohlédnout a smazat.

Nejčastější kybernetické hrozby pro operační systém Windows v České republice za leden 2026:

1. PowerShell/CloudEyE trojan (61,86 %)
2. JS/Agent.RIB trojan (3,16 %)
3. Win32/Formbook trojan (3,02 %)
4. VBS/Agent.TGD trojan (2,81 %)
5. Win64/Aotera trojan (2,19 %)
6. MSIL/Spy.AgentTesla trojan (2,00 %)
7. Win64/Filecoder trojan (0,81 %)
8. Win32/Expiro virus (0,74 %)
9. MSIL/Cassandra trojan (0,64 %)
10. MSIL/Spy.Agent.AES trojan (0,59 %)

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

O společnosti ESET

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

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu [Dvojklík.cz](https://dvojklík.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](#).

Kontakt pro media:

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/skodlivy-kod-cloudeye-je-zpet-v-lednu-se-v-cesku-objevil-ve-dvou-tretinach-vsech-utoku>