CloudEyE v březnu opět zamířil do Česka, riziko z něj dělá dostupnost na dark webu a schopnost obejít obranu

16.4.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Pravidelný přehled kybernetických hrozeb pro operační systém Windows v Česku potvrdil, že i v březnu byl nejčastěji detekovaným škodlivým kódem malware CloudEyE. V čele statistiky se tak držel již třetí měsíc v řadě, v březnu opět s více než polovičním podílem v rámci všech zachycených škodlivých kódů. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET. Podle zjištění bezpečnostních expertů nakupují útočníci tento malware na černém trhu. Právě jeho dostupnost, schopnost obcházet bezpečnostní software a skryté šíření infostealerů jsou podle nich varovné signály, které by uživatelé a uživatelky neměli podceňovat.

Škodlivý kód CloudEyE se v březnu objevil opět ve více než polovině všech případů zachyceného malwaru v Česku. S ohlédnutím na první čtvrtinu letošního roku zůstává jednoznačně nejvíce detekovaným škodlivým kódem v našem regionu. Na jednu stranu zcela upozadil všechny známé škodlivé kódy pro operační systém Windows, jak ale bezpečnostní experti upozorňují, není to tak jednoznačné, jak by se mohlo zdát. CloudEyE je totiž tzv. loader. Poté, co napadne zařízení, do něj začne stahovat další malware, včetně obávaných infostealerů Formbook, Agent Tesla, SnakeStealer nebo škodlivých kódů Rescoms a PureLogs.

„Malware CloudEyE měl v Česku útočnou kampaň čtvrtého března a pak jsme mohli pozorovat nějaký další útok prakticky každý březnový týden. Jelikož je tento škodlivý kód v čele naší pravidelné statistiky již třetí měsíc v řadě, detailně ho sledujeme jako pravidelnou hrozbu v našem prostředí. Vidíme také, že útočníci tento škodlivý kód stále častěji kupují na černém trhu a reálně tak aplikují strategii, kdy do něj infostealery, o jejichž šíření jim jde především, ukryjí. CloudEyE je totiž velmi pokročilý malware, který je bohužel přizpůsobený tomu, aby obešel méně robustní bezpečnostní software. K šíření kybernetických hrozeb je ideální," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Kyberútoky současnosti musí být hlavně nenápadné

Infostealery jsou typem malwaru, který útočníkům slouží ke krádežím různých informací. Těmi nejcennějšími jsou hesla a další přihlašovací údaje, které jim otevírají cestu k citlivým informacím poptávaným na černém trhu, či rovnou k našim financím. Útočníci infostealery vyvíjejí tak, aby se chovaly co nejmíň nápadně. Malware CloudEyE je tak dalším krokem v této hře na schovávanou – slouží k jejich maskování a k obcházení detekčních nástrojů.

„Březnové útoky škodlivým kódem CloudEyE probíhaly primárně v češtině. Opět se nám tak potvrzuje, že i když útočníci operují po celém světě, evidentně se jim vyplatí příprava útoku na míru českým uživatelům a uživatelkám. Měl by to být pro nás varovný ukazatel. V březnu se útočníci vydávali za značku a jméno reálné firmy a v podvodném e-mailu se snažili své oběti přimět k podepsání domnělé aktualizace smluvních podmínek," říká Jirkal.

Malware CloudEyE šíří útočníci stejně jako jiné infostealery, tedy v přílohách spamových e-mailových kampaní. V březnu jsme mohli nejčastěji narazit na škodlivou přílohu s názvem Smluvní struktura – PDF.js.

Útočníci malware nakoupí na černém trhu

Infostealery jsou v současnosti jednou z největších hrozeb pro firmy i jednotlivce. Velmi tomu nahrává jejich přístupnost. Jako službu (Malware-as-a-service, MaaS) je mohou na černém trhu sehnat i méně zkušení útočníci a napadnout tak tisíce zařízení.

„Infostealery mohou sesbírat celou řadu informací a odeslat je útočníkům. Konkrétně jsou to informace o napadeném zařízení, včetně údajů o hardwaru, data z prohlížečů, soubory cookies, obsah schránky a soubory. Právě proto určitě nedoporučujeme ukládat hesla do prohlížečů, i když se to nabízí jako elegantní a praktické řešení, které nám vyřeší obtíže se zapamatováním hesel. Některé typy infostealerů, tzv. keyloggery, umí dokonce sledovat stisky kláves na klávesnici. I když samozřejmě můžeme uživatelům a uživatelkám doporučit, aby věnovali maximální obezřetnost příchozí e-mailové komunikaci, u pokročilých škodlivých kódů, jako je CloudEyE, je na místě už profesionální ochrana vícevrstvým bezpečnostním softwarem. S tím, jak se budou tyto hrozby stávat dostupnějšími a malware bude stále více přizpůsobený tomu, aby ho nešlo snadno odhalit, je na místě zvážit odpovídající ochranu," dodává Jirkal z ESETu.

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

1. PowerShell/CloudEyE trojan (58,60 %)
2. JS/Agent.UGF trojan (5,15 %)
3. MSIL/Spy.AgentTesla trojan (4,34 %)
4. JS/Agent.TFX trojan (3,96 %)
5. Win64/Aotera trojan (3,39 %)
6. JS/Agent.RIB trojan (1,49 %)
7. MSIL/Spy.SnakeStealer trojan (1,43 %)
8. MSIL/Spy.Agent.DRY trojan (1,01 %)
9. Win32/Formbook trojan (0,85 %)
10. Win64/Inoci trojan (0,75 %)

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 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.

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/eset-cloudeye-v-breznu-opet-zamiril-do-ceska-riziko-z-nej-dela-dostupnost-na-dark-webu-a-schopnost-obejit-obranu