ESET: Malware s funkcí nebezpečného kurýra stál v červenci za téměř polovinou všech útoků na české počítače

17.8.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastěji detekovaným škodlivým kódem pro operační systém Windows v Česku zůstal i v červenci malware CloudEyE. Je navržený tak, aby komplikoval své odhalení a analýzu. Jeho hlavním cílem je do napadeného zařízení stahovat infostealery.

- V červenci se v Česku dále objevily škodlivé kódy Agent.UWE a LausivLoader, které také slouží ke stahování a spuštění dalšího malwaru.
- V červenci se malware šířil především globálními e-mailovými kampaněmi s minimálním zastoupením češtiny. Výjimkou byla příloha CZ894_ZCU466˙pdf.js, která ukrývala malware CloudEyE.
- Prevencí by podle bezpečnostních expertů měla být pečlivá kontrola příchozí elektronické pošty, především u kancelářských profesí, a využívání specializovaného bezpečnostního softwaru.

Praha, 17. srpna 2026 – Malware CloudEyE si nadále drží svou unikátní pozici mezi nejčastěji detekovanými škodlivými kódy pro operační systém Windows v Česku. Po jasné převaze v první části roku se v červenci objevil v téměř polovině všech zachycených případů škodlivého kódu v našem regionu. Vyplývá to z pravidelné analýzy od společnosti ESET. Bezpečnostní experti v červenci zachytili další typy škodlivých kódů, které podobně jako CloudEyE plní funkci kurýra pro další malware: Agent.UWE a LausivLoader. V případě úspěšného doručení do napadeného počítače pak stahují a spouští hlavní riziko pro počítače v České republice – infostealery.

Bezpečnostní experti z ESETu v červenci opět zachytili specializované typy škodlivých kódů, které útočníkům slouží jako nástroje pro stahování dalšího malwaru do napadených počítačů. V první fázi útoku nejdříve napadnou cílové zařízení, v navazující fázi pak začnou stahovat a spouštět další malware, nejčastěji tzv. infostealery.

„V červenci jsme v České republice opět nejčastěji detekovali malware CloudEyE. V čele pravidelné statistiky ho tentokrát doplnily škodlivé kódy Agent.UWE a LausivLoader. Opět jsme tu tak měli trojici malwaru, který do napadeného zařízení stahuje další škodlivé kódy. Podobně jako infostealery můžeme na tyto škodlivé kódy narazit v e-mailových přílohách, ve kterých je útočníci schovávají do souborů připomínajících doklady k objednávkám, faktury apod. Čeština se v útocích tentokrát prakticky neobjevovala, kromě přílohy s označením CZ894_ZCU466˙pdf.js, pod kterou se ukrýval právě malware CloudEyE. Přesto je překvapivé, že se nám podařilo útoky zachytit v tak velkém objemu. Je tak vidět, že i anglicky označené soubory a dokumenty připomínající faktury mohou být v Česku nebezpečné, stejně jako přílohy označené jen znaky a čísly, které příjemce zpráv evidentně neodradí od jejich stažení a spuštění," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Loadery a downloadery, mezi které řadíme například malware CloudEye a Agent.UWE, jsou nástroje obvykle využívané ve vícefázových útocích. Jejich úkolem je zakrýt škodlivou činnost a odvést pozornost od hlavní úkolu – stažení a spuštění škodlivého kódu, velmi často infostealerů Agent Tesla,

Formbook či SnakeStealer. Škodlivý kód LausivLoader funguje zase jako tzv. dropper. Představit si ho můžeme jako obal, který do sebe už rovnou pojme další malware, přičemž po napadení cílového počítače ho rozbalí.

„Kromě bezpečnostního softwaru, který považuji v případě těchto útoků za nejlepší obranné řešení, mohou uživatelé a uživatelky snížit riziko také pečlivou kontrolou příchozí e-mailové komunikace. S ohledem na skutečnost, že se většina škodlivých příloh vydává za faktury a objednávky, jsou z mého pohledu v ohrožení především kancelářské profese pracující každý den s velkým množstvím elektronické pošty. Pokud komunikace přijde bez předchozího vyžádání, je třeba vždy zpozornět, zkontrolovat adresu odesílatele i formát přílohy. Na první pohled sice může vypadat jako soubor PDF nebo obrázek, skutečná přípona ale většinou poukazuje na nějaký spustitelný soubor," doporučuje Jirkal.

CloudEyE: Kurýr v první linii

Malware CloudEyE funguje jako kurýr, který je navíc navržený tak, aby komplikoval své odhalení a analýzu. Útočníci tento malware vyvíjejí dlouhodobě a přidávají mu stále nové funkcionality.

„Už od začátku letošního roku si můžeme všimnout, jak se počet zachycených detekcí v jednotlivých měsících proměňuje – jeden měsíc se CloudEyE objevuje až v polovině zachycených případů, někdy i nad touto hranicí, zatímco v následujícím měsíci počet detekcí spadne na zhruba pětinu všech případů, někdy dokonce i méně. Tato střídání vysvětlujeme tím, že útočníci si vždy vezmou měsíc po větších útocích na vyhodnocení a přípravu nových kampaní. Dost dobře mohou také ve slabších měsících malware mezitím i vylepšovat," říká Jirkal.

Jeho hlavním úkolem je stahovat do počítače infostealery, které se zaměřují na naše osobní data i údaje o napadeném zařízení. Staly se také nástrojem pro krádeže našich hesel, které se dají velmi dobře zpeněžit na černém trhu nebo využít k dalším útokům.

„Bezpečná správa hesel je v digitálním světě již základem a nutností. Určitě stále platí, že bychom hesla neměli ukládat do internetových prohlížečů, ani si je sepsat někam do souboru a uložit do počítače. K bezpečné správě hesel jsou určené specializované programy, které je ukládají v šifrované podobě, tzv. správci hesel. Uživatelům a uživatelkám také nedoporučujeme, aby stejná hesla využívali u více účtů. Pro každý online účet bychom měli mít skutečně pouze jedno unikátní heslo. Existující hesla bych pak všude, kde to daná služba umožnuje, doplnil vícefázovým ověřováním – dalším faktorem, kterým své přihlášení potvrzujeme. Obvykle se jedná o otisk prstu, nebo o potvrzovací kód z SMS či autentizační aplikace," dodává Jirkal z ESETu.

Bezpečnostní software dokáže zamezit škodlivému kódu v přístupu 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 červenec 2026:

1. PowerShell/CloudEyE trojan (46,30 %)
2. JS/Agent.UWE trojan (10,50 %)
3. VBS/LausivLoader trojan (3,48 %)
4. JS/ModiLoader trojan (2,68 %)
5. Win32/Formbook trojan (2,16 %)
6. Win64/Aotera trojan (1,70 %)

7. MSIL/Spy.AgentTesla trojan (1,33 %)
8. JS/Agent.VAJ trojan (1,23 %)
9. MSIL/PhantomStealer trojan (1,16 %)
10. PowerShell/Starter trojan (1,05 %)

Uživatelé a uživatelky 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-malware-s-funkci-nebezpecneho-kuryra-stal-v-cervenci-za-temer-polovinou-vsech-utoku-na-ceske-pocitace