Infostealery z Česka nezmizely, útočníci k jejich skrytému stahování využívají speciální škodlivé kódy

20.5.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Ačkoli byl nejčastějším škodlivým kódem v Česku i v dubnu malware CloudEyE, bezpečnostní experti v tomto měsíci zaznamenali v našem regionu také zvýšený výskyt tzv. downloaderů. Útočníci je využívají k tomu, aby nepozorovaně nakazili zařízení oběti. Slouží totiž jako první fáze útoku, na kterou naváže stažení škodlivého obsahu podle přání útočníka – v případě Česka nejčastěji obávaných infostealerů. Bezpečnostní experti se domnívají, že k aktuální skladbě malwaru pro operační systém Windows v Česku přispívá změna trendů na dark webu. Právě na černém trhu mohou i méně zkušení útočníci sehnat škodlivý kód ve formě služby za poplatek. Vyplývá to z pravidelné analýzy škodlivých kódů od společnosti ESET.

Podle bezpečnostních expertů byl duben měsícem, ve kterém byly v Česku výrazněji aktivní škodlivé kódy typu downloader. Jejich funkcí je stahovat do zařízení další malware. V čele pravidelného monitoringu pro operační systém Windows přesto zůstal malware CloudEyE. I tento škodlivý kód útočníci využívají k tomu, aby jeho prostřednictvím do zařízení stáhli další hrozby. Bezpečnostní experti ve světle posledního přehledu kybernetických hrozeb poukazují na proměnu chování kyberútočníků: stále častěji volí malware, který funguje jako prostředník útoku, dokáže hlavní škodlivý kód skrýt a lze jej pořídit na černém trhu.

„Malware CloudEyE, škodlivý kód typu loader, se v dubnu objevoval v pětině všech zachycených případů škodlivého kódu pro operační systém Windows v České republice. Jeho aktivita sice byla při srovnání s předchozím měsícem zhruba poloviční, je to ale hrozba číslo jedna v našem regionu. V dubnu se útoky vyznačovaly velmi zdařilými překlady do češtiny – i CloudEyE se totiž šíří prostřednictvím škodlivých e-mailů a příloh, které útočníci vydávají za různé oficiální dokumenty. Tuto strategii dobře známe od infostealerů. Právě tyto škodlivé kódy, ať už se bavíme o infostealerech Agent Tesla, Formbook nebo SnakeStealer, bývají velmi často malwarem, který CloudEyE pomůže dostat do cílového zařízení a spustit jej," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Nebezpečnými přílohami e-mailů v případě malwaru CloudEyE byly v dubnu především „31032026001836.js" a „Vyuctovani_40667838_2604˙pdf.bat". V názvu druhého příkladu škodlivé přílohy bezpečnostní experti poukazují na praktiku útočníků, kdy před příponou pdf použijí speciální znak, aby přílohu nezachytily nástroje, které hledají kybernetické hrozby s příponami .pdf.bat a další možné kombinace, jako .doc.exe apod.

Downloadery jsou první fází, následně plní příkazy

Mezi nejčastěji zastoupenými škodlivými kódy v Česku se v dubnu objevily také downloadery. Jakmile se downloader dostane do zařízení, stáhne škodlivý obsah z internetu dle zadání útočníka.

„Downloadery Agent.UIN i Agent.UHW jsou sice dva rozdílné škodlivé kódy, v dubnových útocích se nicméně chovaly velmi podobně. Útoky probíhaly na rozdíl od malwaru CloudEyE v angličtině. Útočníci tyto škodlivé kódy opět distribuovali ve škodlivých přílohách e-mailů, které vydávali za doklady k nákupům a objednávkám. Oba škodlivé kódy následně stahovaly malware napsaný v

programovacím jazyce C#. Na základě této skutečnosti a dalších závěrů z analýzy to vypadá, že hlavním cílem bylo nakazit počítače obětí opět infostealery," říká Jirkal.

V případě downloaderu Agent.UIN se v útočných e-mailech objevovala nebezpečná příloha s názvem „PO-HTSS_0410026_pdf.js." U downloaderu Agent.UHW pak šlo především o přílohu „Purchase Order -April -700013779980990902736660022009110055 3_pdf.js".

Byznys na černém trhu

Podle bezpečnostních expertů mohou stát za proměnami útočných strategií také aktuální trendy na černém trhu. Útočníci totiž hledají formy monetizace svých služeb podobně, jako to známe u standardních obchodních modelů. Právě v kontextu fungování dark webu bezpečnostní experti varují, že malware může být v současnosti dostupnější i pro méně technicky zdatné útočníky a objem kybernetických útoků tak může být vyšší.

„Dark web neboli temný web je součástí tzv. deep webu, který je opakem internetu, který známe z každodenního používání. Pokud byste ho chtěli prohlížet jako klasický internet, budete potřebovat speciální prohlížeč a znát přesnou adresu stránky, kterou chcete navštívit. Na dark webu často končí ukradené přihlašovací údaje a další citlivá data uživatelů. Obchoduje se tam i s různými škodlivými kódy, které jejich autoři nabízejí formou služby – představit si to můžeme, jako když si předplácíte nějaký legální a populární program či online službu. Obchody probíhající na temných tržištích jsou díky anonymitě používaných technologií důvěrné a relativně nevystopovatelné. Zároveň zde neexistují žádné státní regulace, placení daní nebo cla," vysvětluje Jirkal.

„V otázkách obrany proto opět platí to samé – maximální ochrana a bezpečná správa přihlašovacích údajů, a to především hesel, k jejichž krádeži útočníci právě infostealery využívají. Seznam míst, ze kterých může útok přijít, se stále rozrůstá, a to také díky stále zdařilejším formám phishingu nebo dalším technikám sociálního inženýrství. Nikdy byste neměli svá hesla opakovaně používat pro více různých účtů. Heslo bych pak doporučil doplnit také vícefázovým ověřením. I kdyby heslo přesto útočníkům padlo do rukou, vícefázové ověření jim převzetí účtu výrazně ztíží," dodává Jirkal z ESETu.

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

1. PowerShell/CloudEyE trojan (21,51 %)
2. JS/Agent.UIN trojan (8,24 %)
3. JS/Agent.UHW trojan (8,12 %)
4. BAT/Agent.SBM trojan (7,24 %)
5. JS/Agent.RIB trojan (4,25 %)
6. MSIL/Spy.SnakeStealer trojan (4,11 %)
7. Win64/Aotera trojan (3,19 %)
8. MSIL/Spy.AgentTesla trojan (3,12 %)
9. MSIL/XWorm trojan (2,71 %)
10. JS/Agent.UGF trojan (2,23 %)

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-infostealery-z-ceska-nezmizely-utocnici-k-jejich-skrytemu-stahovani-vyuzivaji-specialni-skodlive-kody