ESET: V Česku narůstají útoky malwarem první linie, experti varují před škodlivým kódem ModiLoader

15.6.2026 - | ESET software spol. s r.o. - Eset.com

V květnu opět meziměsíčně vzrostly případy malwaru CloudEyE. Tentokrát se objevil ve více než třetině všech detekcí škodlivého kódu pro operační systém Windows v České republice. Nejednalo se ale o jediný škodlivý kód, který se na české uživatele a uživatelky zaměřil – květnová statistika upozornila také na rostoucí případy škodlivého kódu ModiLoader, jehož útoky na Česko nebývají tak časté. Tento obrat se pak bohužel potvrdil 11. června, kdy jej bezpečnostní experti z ESETu zachytili ve velkém útoku na tisíce počítačů. Vyplývá to z pravidelné analýzy škodlivých kódů od společnosti ESET.

Květen byl optikou zachycených případů malwaru CloudEyE opět měsícem, kdy vzrostl objem jeho útoků na české počítače. Jedná se o škodlivý kód typu loader, který lze pořídit na dark webu. Útočníci jej využívají k první fázi útoku, aby následně s jeho pomocí stáhli do napadeného zařízení hlavní škodlivý kód. Bezpečnostní experti velmi často pozorují, že touto hlavní zbraní jsou infostelaery, a často také ransomware.

„Bohužel již několik měsíců pozorujeme nárůst případů takzvaného malwaru první linie. Jeho hlavním úkolem je být co nejméně nápadný a nevzbuzovat žádné podezření. Jakmile ale získá vstup do zařízení, začne dle požadavku útočníků stahovat další škodlivé kódy,“ říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. *„Známe dokonce případy, kdy spolu pak začnou v cílovém zařízení páchat škody infostealer a ransomware – útočníci nejdříve odcizí ze zařízení veškeré osobní údaje, včetně hesel, a následně zařízení zašifrují. Oběť v dalším kroku začnou vydírat a požadovat zaplacení výkupného,*“ dodává Jirkal.

Malware CloudEyE se v Česku šíří především v podobě škodlivé přílohy v podvodných e-mailech. V květnu útočníci zvolili ke zmatení českých uživatelů a uživatelek přílohy s názvy „20260513-00821.js“ a „Oficiální DOKUMENČNÍ DOPIS DOC č. 0225_02 úterý, květen 2026 (07) doc.js“. Jak bezpečnostní experti připomínají, dlouhé názvy příloh útočníci volí záměrně, aby uživatelé nepojali podezření kvůli příponě souboru, která není pro klasický dokument obvyklá.

ModiLoader jako aktuální hrozba pro malé a středně velké české firmy

Již minulý měsíc bezpečnostní experti upozorňovali na downloadery, škodlivé kódy určené ke stahování závažnějšího typu malwaru. I v květnu malware CloudEyE doplnily. Jednalo se o downloader Agent.UIN, experti z ESETu však varují především před malwarem ModiLoader.

„Ačkoli ModiLoader není v našem regionu žádnou novinkou, útoky vidíme spíše ojediněle. V květnu se přitom na Českou republikou zaměřil s nebývalou silou a bylo tak zřejmé, že tentokrát to bude jiné. To se potvrdilo už 11. června, kdy jsme zachytili velký útok tohoto malwaru na malé a střední firmy v České republice,“ říká Jirkal. *„Útočníci k první fázi zvolili phishingovou zprávu a k jejímu rozeslání zneužili kompromitované účty dvou firem, které působí v Česku. Po stažení kompromitované přílohy se spustil ModiLoader, a ten následně v zařízení spustil dobře známý infostealer Formbook, jehož hlavním cílem jsou data uživatelů, především hesla. O tom, že útok byl*

připravený přímo na Česko, svědčí i škodlivá příloha ukrývající tento malware, kterou útočníci pojmenovali Objednávka 392600784. Útok jsme zachytili na tisících počítačů v Česku a opět se tak potvrzuje, že ačkoli strategie s falešnými objednávkami není vůbec nová, stále funguje, a to až se znepokojivou úspěšností,“ dodává Jirkal.

Jak se chránit před loadery a downloadery

S ohledem na způsob, jakým se výše popsané škodlivé kódy mohou dostat do zařízení, zůstávají doporučení bezpečnostních expertů stejná jako v případě infostealerů – maximální opatrnost při práci s příchozí poštou a zvážit zabezpečení profesionálním softwarem.

„Ať už se bavíme na úrovni jednotlivých uživatelů nebo o zaměstnancích ve firmách, vždy je naprosto klíčová pravidelná informovanost o kybernetických hrozbách, se kterými se mohou v současnosti setkat. Jakmile totiž ví, jakými způsoby se na ně mohou útočníci zaměřit, je pak snazší takový útok rozpoznat. K tomuto účelu mohou dobře sloužit i pravidelná kyberbezpečností školení a různá testování, která zkouší i připravenost na útoky pomocí technik sociálního inženýrství. Takové útoky, typicky v podobě nějaké falešné zprávy v e-mailu, ale i v SMS nebo chatovacích aplikacích, bývají velmi úspěšné, protože se zaměřují na naše emoce. Pokud se na ně lidé dobře připraví, velmi ztíží útočníkům jejich práci. Bezpečnostní software pak funguje jako pojistka v případech, kdy se jim stejně podaří dostat k našim datům,“ doplňuje Jirkal z ESETu.

Bezpečnostní software 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.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

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

1. PowerShell/CloudEyE trojan (38,70 %)
2. JS/Agent.UIN trojan (12,93 %)
3. JS/TrojanDropper.ModiLoader trojan (4,98 %)
4. JS/Agent.UQA trojan (3,98 %)
5. JS/Agent.UNV trojan (3,96 %)
6. JS/Agent.RIB trojan (2,70 %)
7. Win64/Aotera Trojan (2,36 %)
8. PowerShell/Starter trojan (2,04 %)
9. Win64/Inoci trojan (2,01 %)
10. MSIL/Spy.SnakeStealer trojan (1,96 %)

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