

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **158** ze dne **6.10.2026**

V Česku narostly případy dropperu, který útočníci prodávají jako nástroj k obcházení zabezpečení

Podle očekávání bezpečnostních expertů došlo v srpnu k mírnému poklesu detekcí malwaru CloudEyE. Zatímco ještě v červenci se objevoval téměř v polovině všech případů škodlivého kódu v Česku, v srpnu ho detekovali zhruba ve dvou pětinach případů. I když se nejedná o nijak radikální pokles, potvrzuje tento vývoj jejich teorii, že období po výrazně vyšším počtu zachycených útoků bývá klidnější a útočníci mohou v tuto dobu vyhodnocovat minulé kampaně a vylepšovat je.

"Malware CloudEyE byl s přehledem nejčastěji detekovanou hrozbou i v srpnu. S ohledem na blížící se konec roku je velmi pravděpodobné, že se stane hlavní letošní kyberhrozbou v Česku. Nebudeme ale předbíhat. Zatím to sice vypadá, že se útočníkům vyplácí tento škodlivý kód opakovaně využívat ke krádeži našich dat, dokážou zároveň své kampaně velmi rychle a flexibilně upravovat. Malware CloudEyE rozhodně není jediným škodlivým kódem, na který bychom si měli dávat v případě operačního systému Windows v Česku pozor," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

CloudEyE je škodlivý kód, který funguje jako loader. Jeho primárním úkolem je zajistit útočníkům přístup k napadenému zařízení, do kterého pak dokáže stáhnout další malware. V srpnu však v Česku vzrostly případy dalšího malwaru, který je mezi zavedenými škodlivými kódy novinkou – dropperu LausivLoader. Zatímco ještě v červenci se objevoval v jednotkách procent případů, v srpnu jeho detekce povyskočily na 17 procent.

"LausivLoader je komerční nástroj, který mohou útočníci pořídit na webu brazilsko-portugalského provozovatele. Opět bych zde rád zdůraznil, že přesně takto může pořízení malwaru vypadat – jako normální nákup nějakého softwaru na internetu. Poskytovatelé tohoto nástroje také inzerují, že umožňuje obcházení ochrany operačního systému Windows," vysvětluje Jirkal. "LausivLoader funguje jako dropper. Představí si to můžeme jako obal, který do sebe už rovnou pojme další malware a po napadení cílového počítače ho rozbalí. V první fázi tak měly oběti tohoto útoku dojem, že stahují nějaký obrázek. Zachytili jsme i případy podvržených obrázků z platformy WhatsApp. Obrázek již ale v sobě obsahoval škodlivý kód, který následně v zařízení začal stahovat další malware," dodává Jirkal.

Pokročilý útok začíná falešným e-mailem

Útočníci šíří škodlivé kódy pro operační systém Windows pomocí podvodných e-mailů. Malware pak ukryjí do přesvědčivé e-mailové přílohy, kterou vydávají za nějaké oficiální dokumenty – faktury, doklady objednávek nebo plateb. V okamžiku, kdy uživatelé a uživatelky přílohu otevrou, spustí s tím i malware. V Česku se přitom ve většině případů jedná o nebezpečné infostealery jako Formbook nebo SnakeStealer, které se již cíleně zaměřují například na naše hesla a další uživatelská data.

"Falešné phishingové e-maily jsou mnohokrát velmi účinnou metodou, jak přimět samotnou oběť, aby útočníky pustila do svého zařízení bez toho, aniž by přístup museli nějak složitě prolomit. To je dnes již příliš náročné a nevyplácí se jim to. V přístupu k obraně před tímto typem útoků je tak klíčová i obezřetnost v e-mailové schránce. Platí zde jednoduché pravidlo – pokud obdržíme nějakou zprávu bez předchozího vyžádání, automaticky bychom k ní měli přistupovat skepticky a zkontrolovat adresu odesílatele. V takových zprávách nedoporučujeme klikat na odkazy ani stahovat a otevírat

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **158** ze dne **6.10.2026**

přiložené soubory. Kromě bezpečné správy hesel a zabezpečení účtů dalším faktorem je spolehlivou pojistkou před kybernetickým útokem bezpečnostní software. Infostealery včas rozezná a zamezí jejich činnosti v napadeném zařízení," dodává Jirkal z ESETu.

Před technikami sociálního inženýrství, kam spadá například již zmíněný phishing, a dalšími moderními kybernetickými podvody varuje ESET společně s Českou bankovní asociací také v rámci kyberkampaně #nePINdej!, která běží od září do konce roku a dlouhodobě upozorňuje na podvody namířené na klienty tuzemských bank. Bezpečnostní experti z ESETu se podíleli také na obsahu letošního Kybertestu. Navrhli testové otázky, vysvětlení odpovědí i příklady podvodných scénářů, které vycházejí z vlastního výzkumu hrozeb.

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

1. PowerShell/CloudEyE trojan (39,54 %)
2. VBS/LausivLoader trojan (17,09 %)
3. Win32/Formbook trojan (2,85 %)
4. MSIL/Spy.AgentTesla trojan (2,68 %)
5. Win64/Inoci trojan (1,36 %)
6. JS/Agent.VCT trojan (1,18 %)
7. JS/Agent.VCM trojan (1,16 %)
8. MSIL/PhantomStealer trojan (1,10 %)
9. JS/Agent.RIB trojan (1,05 %)
10. JS/Agent.VEC trojan (1,01 %)

Uživatelé a uživatelky řešení ESET jsou před těmito hrozbami chráněni.

AV centrum ČR