

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **152** ze dne **12.8.2026**

ESET: Hackeři v Česku pokračují v šíření infostealerů, aktuálně mohou připravovat novou vlnu útoků.

Zatímco v květnu byla Česká republika cílem masivního útoku škodlivého kódu ModLoader, v červnu se situace v našem regionu uklidnila. Stejně jako v předešlých měsících se v čele pravidelné statistiky držel malware CloudEyE. Počet jeho detekcí se však oproti předešlému měsíci propadl skoro na polovinu. Jak bezpečnostní experti z ESETu již informovali, Česká republika se nyní potýká s útoky specializovaného malwaru, jehož úkolem je v první fázi napadnout zařízení a pak do něj stahovat další škodlivé kódy. Nejčastěji se přitom jedná o infostealery, oblíbený nástroj hackerů, který využívají ke krádežím dat.

"V červnu se malware CloudEyE nejčastěji objevoval v polovině měsíce. Narazit jsme na něj mohli v e-mailu, konkrétně ve škodlivých přílohách. Českou verzi přílohy útočníci vydávali opět za objednávku. Hlavním úkolem škodlivého kódu bylo stahovat do napadeného zařízení infostealery Agent Tesla, Formbook či SnakeStealer, což jsou všechno škodlivé kódy, se kterými jsme se již v minulosti v Česku setkávali," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. "Ačkoli vidíme, že v červnu došlo v případě malwaru CloudEyE k poklesu detekcí, a ani ModLoader nezopakoval vlnu útoků z letošního května, nelze budoucí kampaně vyloučit. Útočníci nyní testují nové, méně známé škodlivé kódy a v následujícím období teprve uvidíme, jak jim tyto nástroje vyhovují nebo zda se nevrátí ke starým metodám. Malware první linie, jak CloudEyE, downloadery a loader ModLoader označujeme, je aktuálně dlouhodobě využívanou strategií, kterou budou útočníci velmi pravděpodobně ještě vyvíjet," dodává Jirkal.

Proč jsou infostealery tak populární?

Aktuální vývoj kybernetických hrozeb pro operační systém Windows v České republice ukazuje, jak útočníci ve snaze využít infostealery volí pokročilejší postupy. Na rozdíl od dřívějších útoků nyní více využívají jako prostředníka další malware, který nevzbuzuje tolik pozornosti a snáze tak pronikne ke svému cíli.

"Infostealery jsou univerzální zbraní, pokud se útočníci chtějí dostat k našim datům. Co se týká údajů o zařízení, útočníci jejich pomocí dokážou získat například uživatelské jméno, verzi operačního systému Windows, hardwarové specifikace či informace o geolokaci apod. Dále jsou jejich cílem data o prohlížení webu, zejména pak soubory cookies, nebo obsah schránky, což je rizikem právě proto, že se tam mohou nacházet hesla, údaje o bankovních účtech nebo adresy kryptoměnových peněženek. Útočníci také vyhledávají data z nainstalovaných aplikací či soubory. Některé infostealery mohou sledovat i stisky kláves, ty pak označujeme jako keyloggery. Svatým grálem infostealerů jsou ale hesla, je to vlastně to nejcennější, co mohou útočníci po napadení počítače získat. V aktuálních případech jsme dokonce viděli, jak se útočníci zaměřují i na správce hesel, což jsou specializované programy určené k bezpečnému uchovávání hesel a jejich správě. Hesla následně útočníkům otevírají cestu k našim účtům a zároveň se jedná o položku, kterou velmi dobře zpeněží na černém trhu," vysvětluje Jirkal.

"V případě infostealerů bych doporučoval kombinovat bezpečnostní software s celkovou obezřetností před nevyžádanými příchodními e-maily. Základem je nikdy neklikat na odkazy ani nestahovat soubory v podezřelé komunikaci. Varovnými znaky bývá například adresa odesílatele, zvláště

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **152** ze dne **12.8.2026**

pokud se jedná o nějakou známou instituci. Pokud taková zpráva přijde náhle a chce se po nás nějaká nestandardní reakce, vždy je na místě zprávu důkladně zkontrolovat a případně se na danou instituci obrátit ještě i jinou cestou a požadavek si potvrdit," dodává Jirkal z ESETu.

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

1. PowerShell/CloudEyE trojan (22,25 %)
2. JS/Agent.URN trojan (17,91 %)
3. JS/TrojanDropper.ModiLoader trojan (7,85 %)
4. Win32/Formbook trojan (7,46 %)
5. JS/Agent.UUB trojan (5,00 %)
6. VBS/Agent.UDG trojan (2,99 %)
7. VBS/Agent.TKB trojan (1,91 %)
8. Win64/Aotera trojan (1,53 %)
9. JS/Agent.USA trojan (1,46 %)
10. MSIL/Spy.AgentTesla trojan (1,30 %)

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

AV centrum ČR