

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **133** ze dne **10.2.2026**

Kyberhrozbou číslo jedna byl v loňském roce infostealer Formbook

Zatímco ještě v listopadu se mohli čeští uživatelé a uživatelky setkat s velkou kampaní škodlivého kódu CloudEye, ke konci roku jeho aktivita výrazně poklesla. Stále však zůstal jednou z hlavních kybernetických hrozeb v Česku. Útočníci v jeho případě vsadili na falešné e-maily s přílohami, které budily dojem, že odesílatelem je pojišťovna. Do čela pravidelné statistiky se pak na konci roku vrátil infostealer Formbook.

"Dalo by se říct, že i poslední statistika kybernetických hrozeb pro operační systém Windows v loňském roce potvrdila případy škodlivých kódů, které jsme monitorovali v průběhu celého uplynulého roku. Výjimkou může být malware CloudEye, který se téměř ve čtvrtině všech zachycených případů objevil v Česku po delší odmlce v listopadu. Přestože je CloudEye, známý také pod názvem GuLoader, propagován jako legitimní služba pro ochranu souborů, ve skutečnosti jde o downloader a kryptor typu malware-as-a-service. Znamená to, že útočníci se již nemusí obtěžovat jeho vývojem, ale mohou jej na černém trhu koupit a využívat úplně stejně, jako si my koupíme nějaký softwarový program. Útočníci jej používají k tomu, aby na napadeném zařízení rozšířili další škodlivé kódy – vyděračský ransomware a infostealery Formbook, Agent Tesla či Rescoms. Jedná se o velmi pokročilý škodlivý kód, který je přizpůsobený k tomu, aby nešel tak snadno analyzovat," shrnuje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Nejsilnější útoky malwaru CloudEye zachytili bezpečnostní experti 10. a 11. prosince 2025. Přílohy útočných e-mailů, které malware ukrývaly, byly nejčastěji pojmenovány "Bank Transfer Confirmation - Advance Payment for PO 4500725711_pdf.js". Čeští uživatelé a uživatelky pak mohli narazit na již zmíněnou přílohu "Predpis_pojistne_smlouvy".

Infostealer Formbook – kyberhrozba číslo jedna v Česku

Až na pár měsíců minulého roku byl převládající loňskou hrozbou infostealer Formbook. A potvrdil to i v prosinci, kdy naposledy vystoupal s největším podílem měsíčních detekcí do čela pravidelné statistiky. Nejsilnější kampaň zachytili kyberbezpečnostní experti 18. a 19. prosince. Útočníci jej šířili ve škodlivé příloze s názvem "msedge_elf.dll".

"Útočníci v prosinci šířili infostealer Formbook buď přímo ve škodlivých přílohách, nebo ukrytý v dalším škodlivém kódu s názvem Agent.ECK. K tomu musíme ale ještě připočíst fakt, že i malware CloudEye mohl na zařízení, které jeho prostřednictvím útočníci napadli, finálně opět stáhnout infostealer Formbook. Závěr roku tak i do budoucna naznačil, před jakým škodlivým kódem bychom se měli mít v Česku na pozoru. Až na pár měsíců, kdy pravděpodobně probíhala příprava nových útoků a vývoj nových verzí tohoto malwaru, byl Formbook vloni jednoznačnou volbou kyberútočníků v našem regionu. Očekávám, že tomu tak zůstane i v následujícím roce," říká Jirkal.

Obrana před infostealery v roce 2026

Ani letos bezpečnostní experti nepočítají s tím, že by se úroveň rizika v podobě infostealerů měla v Česku snižovat. Vysokou popularitu našeho regionu jako cíle e-mailových kampaní pak potvrdil i třetí, prosincový případ škodlivého kódu Agent.HRS. Přes darknet může stahovat například nechvalně proslulý infostealer Agent Tesla. V prosinci byly kampaně připravené na míru českým uživatelům, o

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **133** ze dne **10.2.2026**

čemž svědčila i nebezpečná příloha s názvem "Přenést kopii.exe", která škodlivý kód ukrývala.

Infostealery útočníkům slouží jako velmi efektivní nástroj k odcizení našich dat. Vyhledávaným cílem jsou pak především naše uživatelská hesla.

"Rok 2026 by měl být z mého pohledu rokem, kdy by uživatelé a uživatelky měli ke svým osobním datům přistupovat podobně jako k financím a věnovat jim náležitou ochranu. V případě správného nakládání s hesly bych rozhodně doporučoval věnovat pozornost tomu, abychom vždy měli pro každý účet jen jedno heslo. Pokud máme více stejných hesel pro různé účty, můžeme útočníkům otevřít dveře na více místech. Hesla také rozhodně nedoporučuji ukládat do souborů v počítači ani do internetových prohlížečů, které nemusí být před infostealery dostatečně zabezpečené. A v neposlední řadě je určitě na místě zvážit profesionální ochranu naší elektronické pošty a celého počítače, která dokáže velmi flexibilně reagovat na různé typy nových hrozeb, se kterými se v budoucnu setkáme," dodává Jirkal z ESETu.

Nejčastější kybernetické hrozby pro operační systém Windows v České republice za prosinec 2025:

- Win32/Formbook trojan (8,75 %)
- PowerShell/CloudEye trojan (6,50 %)
- Win64/Agent.HRS trojan (6,27 %)
- MSIL/Spy.AgentTesla trojan (3,28 %)
- Win32/Expiro virus (2,98 %)
- Win64/Aotera trojan (2,77 %)
- MSIL/Spy.SnakeStealer trojan (2,12 %)
- MSIL/Spy.Agent.AES trojan (1,64 %)
- VBS/Agent.TEM trojan (1,63 %)
- Win64/Inoci trojan (1,23 %)

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

AV centrum ČR