

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **118** ze dne **9.9.2025**

Jdou po vašich datech: Co jsou to infostealery?

Ve světě kyberkriminality jsou informace prostředkem k dosažení vydělávání peněz. Proto se malware kradoucí informace (tzv. infostealery) stal hlavním nástrojem pro krádeže identity, převzetí účtů a krádeže kryptoměn. V Česku patří infostealery k nejrozšířenějšímu typu malware. Ukradené údaje se často prodávají na dark webu nebo otevírají cestu k dalším útokům.

Mnoho infostealerů má původ v legendárním malwaru Zeus – bankovním trojským koni určeném ke krádeži přihlašovacích údajů k online bankovníctví. Po úniku jeho zdrojového kódu v roce 2011 se objevily nové verze a odstartovaly tak rozšíření infostealerů. Dnes existují varianty pro Windows, macOS, iOS i Android.

Jaké informace infostealery kradou?

Útočníky zajímají všechny údaje, které lze nějak zpeněžit. Oblíbeným cílem jsou přihlašovací údaje a tzv. cookies session, což jsou malé datové soubory, které mohou hackerům umožnit obejít vícefaktorovou autentizaci (MFA). Jedna zpráva odhaduje, že 75 % přihlašovacích údajů ukradených v loňském roce bylo odcizeno prostřednictvím infostealerů. Typicky jde o tato data:

- Přihlašovací údaje
- Čísla platebních karet, bankovních účtů a kryptopeněženek
- Osobní údaje jako jména a adresy
- E-mailové adresy a telefonní čísla
- Historii prohlížení, uložené formuláře a hesla
- Informace o systému a uložené soubory

Jak infostealery fungují?

Cílem těchto škodlivých kódů je tiše a rychle najít citlivé informace a odeslat je útočníkovi. Používají třeba techniky, které umožní zachytit údaje z formulářů před odesláním nebo škodlivý kód, který zaznamená stisknuté klávesy, pořídí snímky obrazovky nebo dokáže získat data uložená v clipboardu (poté co stisknete CTRL+C).

Tyto informace lze zneužít přímo k odcizení účtů v různých službách (kde máme často uložené informace o platebních kartách), krádeži identity, podvodům, šíření dalšího malware nebo vydírání. Mimo to se dají také prodat na dark webu.

Jak se infostealery šíří?

Pokud víte, kde se s malware můžete setkat, lze se mu snáze ubránit. Jeden z nejběžnějších způsobů, jak rozšířit škodlivé kódy, zůstává phishing v e-mailu nebo SMS. Typicky taková zpráva působí důležitě a obsahuje odkaz na podvodnou stránku nebo přílohu, odkud si malware uživatel nevědomky stáhne.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **118** ze dne **9.9.2025**

Další možností jsou falešné stránky, může jít o web s podvodným formulářem nebo odkazem ke stažení malware. Na takové webové stránky odkazují lákavé reklamy ze sociálních sítí nebo zcela legitimních stránek, které obvykle čtete.

Infostealery určené pro android detekujeme často v aplikacích z neoficiálních zdrojů. Nejčastěji jde o falešné verze populárních nebo placených služeb, cracknuté verze her (tedy ty s prolomeným licenčním kódem) a podobně.

Méně často se útočníkům podaří tzv. ztrojanizovat legitimní aplikace a webové stránky. Na to je ale nutné „hacknout“ původní službu, což je velmi technicky náročné.

Jak vypadá hrozba dnes?

Podle ESET Threat Report H1 2025 je trh s infostealery obrovský. Útočníci totiž pronajímají své škodlivé kódy. Tomuto obchodnímu modelu říkáme malware jako služba (MaaS). Každý si může kód koupit, zaplatit za jeho rozšíření a dostat databázi ukradených dat. Už není nutné mít technologické znalosti a umět programovat.

Některé konkrétní typy útočníci neustále vyvíjí, například Formbook je v provozu od roku 2021. Nově ale útočníci přidali sofistikované obfuskací techniky, tyto techniky pomáhají obcházet zabezpečení. Jiné varianty, jako například RedLine, dokázala zastavit policie. Jejich místo na slunci ale převzali tvůrci Lumma Stealer. Ten funguje jako malware-as-a-service, tedy jako malware na zakázku. Kdokoliv si takový škodlivý kód může koupit na darkwebu.

Jak se chránit před infostealery?

- Mějte aktualizovaný bezpečnostní software na všech zařízeních.
- Buďte obezřetní vůči phishingu – neklikejte na podezřelé odkazy, ověřujte odesílatele.
- Stahujte aplikace pouze z oficiálních obchodů a vyhýbejte se pirátskému softwaru.
- Aktualizujte operační systém a aplikace.
- Buďte opatrní na sociálních sítích – nevěřte podezřelým nabídkám.
- Používejte silná a unikátní hesla – ideálně s dvoufázovým ověřením (2FA).

Zdroj: AVcentrum ČR