

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **140** ze dne **14.4.2026**

Úniky dat slábnou. Kybernetičtí zločinci přecházejí na efektivnější infostealery

Společná analýza kyberbezpečnostní společnosti NordVPN a platformy pro sledování hrozeb NordStellar mapuje vývoj v letech 2024 a 2025. V tomto období klesl počet kompromitovaných databází o 36 procent, konkrétně z 4 804 na 3 069 případů. Paralelně s tímto poklesem zaznamenaly analytické systémy nárůst logů z infostealerů o 35 procent, a to z 19,5 milionu na více než 26 milionů.

Mantas Sabeckis, seniorní výzkumník hrozeb ve společnosti Nord Security, vysvětluje, že klesající počet plošných úniků dat znamená nalezení efektivnější cesty pro získání citlivých informací.

Jediná infekce infostealerem dokáže nepozorovaně odcizit uložená hesla, soubory cookie, data z automatického doplňování a session tokeny. Jde o méně nápadný proces než narušení podnikové infrastruktury, dopady na koncového uživatele však dosahují stejné závažnosti.

Změna útočné strategie a měřítko efektivity

Zpráva 2026 Threat Report od společnosti Cloudflare popisuje širší posun v psychologii útočníků. Ti vyměňují technologickou sofistikovanost za propustnost a masový zásah. Zpráva pro tento jev používá termín měřítko efektivity (MOE), který definuje poměr mezi vynaloženým úsilím a operačním výsledkem. Využití odcizeného session tokenu přináší útočníkům lepší výsledky s nižšími náklady než nasazení drahých zero-day exploitů.

Data z roku 2025 poskytují konkrétní srovnání obou vektorů útoku. Kompromitované databáze zapříčinily únik téměř 34 milionů hesel, zatímco infostealery jich ve stejném období získaly 624 milionů, což představuje více než osmnáctinásobný objem. V kategorii e-mailových adres odhalily plošné úniky 542 milionů záznamů a infostealery zachytily 380 milionů. Rozdíl mezi těmito hodnotami se v posledních letech rychle zmenšuje.

Technický ředitel společnosti NordVPN Marijus Briedis poukazuje na zásadní rozdíl v detekci a reakci na oba typy hrozeb. Při narušení podnikové databáze organizace spouští standardní procesy pro ochranu koncových uživatelů, resetují hesla a izolují škody. Infekce infostealerem naproti tomu probíhá bez systémového varování. Přihlašovací údaje končí na dark webu a uživatelé zjišťují kompromitaci účtů až po jejich reálném zneužití.

AV centrum ČR