Přes milion kompromitovaných účtů v doméně .cz v 2023

4.4.2024 - | PROTEXT

Kvůli této rostoucí hrozbě spustila společnost Kaspersky speciální webovou stránku, která má zvýšit povědomí o tomto problému a poskytnout strategie pro zmírnění souvisejících rizik.

Podle zjištění Kaspersky Digital Footprint Intelligence bylo v roce 2023 napadeno malwarem kradoucím data přibližně 10,000.000 osobních a firemních zařízení, což představuje 643% nárůst za poslední tři roky. Počty nakažených zařízeních byly odvozeny z dynamiky výskytu souborů přihlašovacích údajů nashromážděných infostealery, s nimiž se aktivně obchoduje na nelegálních burzách a které společnost Kaspersky monitoruje, aby pomohla firmám zajistit bezpečnost jejich klientů a zaměstnanců.

I když počet pozorovaných souborů s ukradenými přístupovými údaji - a tedy i počet infekcí - v roce 2023 oproti roku 2022 nepatrně klesl (o 9 %), neznamená to, že by poptávka kyberzločinců po přihlašovacích jménech a heslech stagnovala. Lze předpokládat, že některé přístupové údaje, které byly odcizeny v roce 2023, mohly uniknout na dark web až někdy během letošního roku. Skutečný počet nakažených zařízení je tedy pravděpodobně ještě vyšší než 10 milionů. Podle odhadu společnosti Kaspersky, který vychází z dynamiky výskytu souborů od infostealerů, se počet infekcí, ke kterým došlo v roce 2023, blíží zhruba 16,000.000.

Kyberzločinci ukradnou na jednom infikovaném zařízení v průměru 50,9 přihlašovacích údajů. Aktéři hrozeb tyto údaje buď využívají pro své vlastní škodlivé účely včetně kybernetických útoků, nebo je prodávají či volně šíří na dark webových fórech a stínových kanálech Telegramu.

Tyto přihlašovací údaje mohou umožňovat přístupy k sociálním médiím, online bankovnictví, kryptopeněženkám a různým firemním online službám, jako je e-mail a interní systémy. Podle společnosti Kaspersky došlo za posledních 5 let ke kompromitaci přihlašovacích údajů na 443.000 webových stránkách po celém světě.

Co se týče počtu kompromitovaných účtů, vede doména .com. Na této doméně bylo v roce 2023 odcizeno infostealery téměř 326 milionů přihlašovacích jmen a hesel k webovým stránkám. Následuje doména .br (Brazílie) s 29 miliony kompromitovaných účtů, doména .in (Indie) s 8 miliony, doména .co (Kolumbie) s téměř 6 miliony a doména .vn (Vietnam) s více než 5,5 miliony. V případě domény .cz spojené s Českem bylo v roce 2023 zaznamenáno přes milion kompromitovaných účtů.[1]

"*Hodnota souborů s přihlašovacími údaji se na dark webu liší podle atraktivity dat a způsobu prodeje. Přihlašovací údaje mohou být prodávány formou předplatného s pravidelnými aktualizacemi, pomocí tzv. ‚agregátoru' pro specifické požadavky nebo prostřednictvím 'obchodu', který poskytuje čerstvě získané přihlašovací údaje pouze vybraným kupcům. Ceny v těchto obchodech začínají obvykle na 10 USD za jeden soubor. To ukazuje, jak je pro jednotlivce i firmy - zejména ty, které mají na starosti velké online komunity uživatelů - důležité být stále ve střehu. Únik přihlašovacích údajů představuje velkou hrozbu a umožňuje kyberzločincům provádět různé útoky, například krádeže finančních prostředků nebo citlivých informací, sociální inženýrství nebo vydávání se za někoho jiného*," říká **Sergej Ščerbel**, expert z oddělení Kaspersky Digital Footprint Intelligence.

Na ochranu před infostealery se doporučuje používat komplexní bezpečnostní řešení pro každé zařízení. To pomůže zabránit infekcím a upozornit na nebezpečí, jako jsou podezřelé stránky nebo podvodné e-maily, které mohou být prvotním zdrojem nákazy. Firmy mohou navíc tímto způsobem pomoci svým uživatelům, zaměstnancům a partnerům s ochranou před potenciálními hrozbami díky proaktivnímu monitorování úniků dat a výzvám k okamžité změně zveřejněných hesel.

Další informace o hrozbách souvisejících s infostealery najdete na webu Kaspersky Digital Footprint Intelligence.

[1] Doména nejvyšší úrovně s kódem země (ccTLD) je obvykle vyhrazena pro použití v určité zemi. Mohou ji však využívat i celosvětově působící webové stránky, které se nemusí nutně vztahovat k určité zemi, což ovlivňuje statistiky.

ČTK Connect ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese http://www.protext.cz.

http://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-pres-milion-kompromitovanych-uctu-v-domene-cz-v-2023/2501036