# Kaspersky: 53 % zařízení infikovaných infostealery patří firmám

**19.4.2024 - | PROTEXT**

**Společnost Kaspersky odhalila znepokojivý trend: firemní zařízení čelí rostoucí hrozbě ze strany zlodějů informací. Podle údajů získaných ze souborů záznamů, které byly pořízeny infostealery a jsou dostupné na dark webu, se podíl firemních uživatelů napadených tímto typem malwaru zvýšil od roku 2020 o 34 procentních bodů.**

V roce 2023 dospěli odborníci k závěru, že každé druhé zařízení (53 %) infikované malwarem kradoucím přihlašovací údaje je firemní, jelikož největší podíl infostealerových infekcí byl zjištěn ve verzi Windows 10 Enterprise. Níže uvedený graf znázorňuje rozšíření těchto infekcí u různých verzí systému Windows 10 v letech 2020 až 2023.

Kyberzločincům může stačit infikovat jen jedno zařízení, aby dokázali proniknout do všech účtů – osobních i firemních. Statistiky společnosti Kaspersky ukazují, že jeden soubor odcizených přihlašovacích údajů s firemními e-maily umožňuje přístup k průměrně 1,85 firemním webovým aplikacím, včetně webových mailových aplikací, systémů pro zpracování dat zákazníků, interních portálů apod.

*„Zajímalo nás, zda firemní uživatelé spouštějí malware opakovaně, čímž umožňují kyberzločincům další přístup k datům nashromážděným z dříve infikovaného zařízení, aniž by ho museli sami znovu infikovat,“* komentuje **Sergej Ščerbel**, expert z týmu Kaspersky Digital Footprint Intelligence. *„Abychom to prozkoumali, analyzovali jsme vzorek souborů záznamů obsahujících data, která se pravděpodobně týkají 50 bankovních organizací v různých regionech. Zjistili jsme, že 21 % zaměstnanců spustilo škodlivý software znovu a 35 % z těchto opětovných infekcí proběhlo více než tři dny po první infekci. To může naznačovat několik zásadních bezpečnostních problémů, například nedostatečnou informovanost zaměstnanců, neúčinnost opatření pro odhalování incidentů a reakcí na ně, mylné přesvědčení, že v případě napadení účtu stačí změnit heslo, nebo neochotu incidenty vyšetřit.“*

Další informace o hrozbách infostealerů můžete najít na webu Kaspersky Digital Footprint Intelligence. Pro minimalizaci dopadu úniku dat způsobeného činností infostealerů doporučujeme postupovat podle následujících kroků:

Pro lepší ochranu před infekcemi infostealery vypracujte plán pro zvyšování bezpečnostního povědomí zaměstnanců a provádějte pravidelná školení a hodnocení kyberbezpečnosti.

https://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-53-zarizeni-infikovanych-infostealery-patri-firmam/2507861