

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **155** ze dne **15.9.2026**

Rozsáhlá kampaň zaměřená na krádež přihlašovacích údajů ke cloudu Azure zasáhla McDonald's, Vodafone i další nadnárodní společnosti.

Nejrozsáhlejší dataset se týká společnosti McDonald's Corporation, u níž prodejce deklaruje 1,7 milionu záznamů. Následuje Tata Consultancy Services s 800 tisíci záznamy, Vodafone s 425 tisíci záznamy a HCL Technologies s 250 tisíci záznamy.

Mezi dalšími jmenovanými organizacemi figurují InterContinental Hotels Group se 185 tisíci záznamy, Kyndryl se 170 tisíci záznamy, Gap Inc. s 80 tisíci záznamy, Hexaware Technologies s 20 tisíci záznamy a Wyndham Hotels s 9 tisíci záznamy.

Prodejce ke svým tvrzením přiložil datové vzorky. Odkaz ke stažení vzorku u McDonald's byl v době ověřování redakcí Cybernews nefunkční, u ostatních společností se však podařilo obsah ověřit. Vzorky obsahují pole typická pro exporty adresářové služby Microsoft Entra – firemní e-mailové adresy, telefonní čísla, pracovní pozice, celá jména zaměstnanců a adresy pracovišť.

Nejasný způsob průniku

TheHatman opakovaně uvádí, že data získal pomocí kompromitovaných přihlašovacích údajů, přesný způsob vstupu do prostředí obětí však zůstává nepotvrzený. Struktura záznamů podle bezpečnostní společnosti Hudson Rock odpovídá standardním exportům z adresáře Azure.

Hudson Rock identifikovala důkazy propojující infekce infostealer malwarem s kompromitovanými přihlašovacími údaji k Azure u několika postižených společností, včetně TCS, Gap Inc., HCL Technologies a Kyndryl. Infostealery jsou škodlivé programy určené ke krádeži hesel, dat z prohlížečů a relačních cookies z napadených počítačů; ukradené relační informace mohou útočníkovi v některých případech umožnit přístup k online službám bez nutnosti opětovně zadávat heslo oběti.

"Vzhledem k rozsahu postižených organizací se jeví jako vysoce pravděpodobné, že kampaň vychází z cíleného zneužití infekcí infostealerem, nikoli ze systémové zero-day zranitelnosti v Azure," uvedla Hudson Rock. Společnost dodává, že v případě rozšířené zranitelnosti by bylo pravděpodobně zasaženo mnohem širší spektrum organizací včetně menších firem, nikoli výhradně podniky úrovně Fortune 500.

Reakce postižených společností

Redakce Cybernews oslovila všechny jmenované společnosti se žádostí o vyjádření. Podle informací zveřejněných webem Infostealers.com Tata Consultancy Services uvedla, že nemá důkazy o narušení bezpečnosti svého prostředí. Ostatní organizace se k incidentu dosud nevyjádřily.

Riziko sociálního inženýrství

Podle analytiků Cybernews spočívá hlavní riziko pro jednotlivce ve zvýšené hrozbě útoků sociálního inženýrství. Kompromitované přihlašovací údaje mohly být již rotovány, pokud se tak ale nestalo, mohou posloužit k další exfiltraci dat.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **155** ze dne **15.9.2026**

Útočník s přesnými informacemi o zaměstnancích, jejich nadřízených, odděleních a organizační struktuře může sestavit vysoce věrohodnou phishingovou zprávu – například se vydávat za přímého nadřízeného oběti nebo administrátora IT a použít reálné organizační detaily k tomu, aby požadavek působil legitimně.

AV centrum ČR