

Azure Data Exfiltration: TheHatman Campaign Exposes Millions of Records | The CyberSec Guru | The CyberSec

By The CyberSec Guru

Published: 2026-08-17 · Archived: 2026-09-03 02:00:44 UTC

The modern enterprise security perimeter has fundamentally collapsed, shifting away from fortified network firewalls and landing squarely on the fragile concept of digital identity. A sprawling and sophisticated data exfiltration campaign currently unfolding across underground cybercrime forums serves as a stark reminder of this reality. Operating under the alias “TheHatman,” a highly organized threat actor has systematically listed and sold internal employee directories stolen from some of the world’s largest and most recognizable corporations. This operation is not a traditional infrastructure breach exploiting a zero-day vulnerability within Microsoft Azure or the underlying cloud architecture. Instead, it represents a catastrophic failure of enterprise identity hygiene, where compromised credentials, hijacked session tokens, and overly permissive application integrations have granted malicious actors unrestricted read access to entire corporate directories. The sheer volume of the data is staggering, targeting massive multinational firms across diverse sectors and exposing millions of sensitive records. By analyzing the mechanics of this campaign, security professionals can understand the critical vulnerabilities inherent in modern cloud environments and the urgent need to redefine how organizations protect their most valuable asset: their digital identities. The cloud environment is only as secure as the weakest authenticated session, and this campaign proves that attackers no longer need to break encryption or bypass network controls when they can simply log in as a trusted insider.

The Scope of the Compromise: A Fortune 500 Roll Call

Over the past week, TheHatman has flooded dark web marketplaces and exclusive cybercrime forums with listings for at least nine Fortune 500-level enterprises, spanning IT services, hospitality, telecommunications, retail, and logistics. The campaign deliberately targets organizations with massive, complex workforces and extensive global footprints. McDonald’s Corporation tops the list of compromised entities, with the threat actor advertising a dataset containing more than 1.7 million exposed employee records. This is followed closely by Tata Consultancy Services, offering roughly 800,000 records, and the telecommunications giant Vodafone, which has seen approximately 425,000 internal records put up for sale. The volume of these initial dumps indicates a highly systematic approach to data harvesting, prioritizing organizational depth over opportunistic, smaller-scale breaches. Targeting managed service providers and massive IT consultancies is a deliberate strategy; compromising the directory of a firm like Kyndryl or TCS not only yields a massive dataset but also exposes the identities of personnel who likely possess administrative access to the environments of their downstream clients.


Gap Inc. 80K+ Azure Internal Employee Dump | Full Name, Email, Title, Phone, Address
 I'm selling Gap Inc. internal employee dump downloaded directly from Azure Tenant using compromised credentials. Data contains over 80,000 records (including employee accounts, service accounts, and other tenant account records). Download...
 TheHatman · Thread · Today at 5:09 AM · Replies: 0 · Forum: Sellers Place


McDonalds 1.7M+ Azure Internal Employee Dump | Full Name, Email, Title, Phone, Address
 I'm selling McDonald's Corporation internal employee dump downloaded directly from Azure Tenant using compromised credentials. Data contains over 1.7 million records (including employee accounts, service accounts, and other...)
 TheHatman · Thread · Today at 4:08 AM · Replies: 0 · Forum: Sellers Place


Vodafone 425K+ Azure Internal Employee Dump | Full Name, Email, Title, Phone, Address
 I'm selling Vodafone internal employee dump downloaded directly from Azure Tenant using compromised credentials. Data contains over 425,000 records (including employee accounts, service accounts, and other tenant account records...)
 TheHatman · Thread · Today at 2:16 AM · Replies: 0 · Forum: Sellers Place


TCS (Tata Consultancy) 800K+ Azure dump | Full Name, Email, Title, Phone, Address
 I'm selling TCS (Tata Consultancy Services) internal employee dump downloaded directly from Azure Tenant using compromised credentials. Data contains over 800,000 records (including employee accounts, service accounts, and...)
 TheHatman · Thread · Monday at 1:07 AM · Replies: 0 · Forum: Sellers Place


HCL Technologies 250K+ Azure dump | Full Name, Email, Title, Phone, Address
 TheHatman · Thread · Aug 7, 2026 · Replies: 0 · Forum: Sellers Place


InterContinental Hotels 185K+ Azure dump | Full Name, Email, Title, Phone, Address
 I'm selling InterContinental Hotels Group (IHG) internal employee database, downloaded directly from Azure/Entra portal using compromised credentials. Data contains over 185,000 records (including employee accounts, Reports, User Group Membership, etc.), including...
 TheHatman · Thread · Aug 2, 2026 · Replies: 0 · Forum: Sellers Place


Wyndham Hotels 9K+ Azure/Entra dump | Full Name, Email, Title, Phone, Address
 I'm selling Wyndham Hotels internal employee database, downloaded directly from Azure/Entra portal using compromised credentials. Data contains over 9,000 records (including employee accounts, Reports, User Group Membership, etc.), including employee accounts...
 TheHatman · Thread · Aug 2, 2026 · Replies: 0 · Forum: Sellers Place


Hexaware 20K+ Azure/Entra dump | Full Name, Email, Employee ID, Phone, Address
 I'm selling Hexaware internal employee database, downloaded directly from Azure/Entra portal using compromised credentials. Data contains over 20,000 records (including employee accounts, Reports, User Group Membership, etc.), including employee accounts...
 TheHatman · Thread · Aug 1, 2026 · Replies: 0 · Forum: Sellers Place


Kyndryl.com 170K+ Azure/Entra dump
 I'm selling Kyndryl internal dump, downloaded directly from Azure/Entra portal using compromised credentials. Data contains over 170,000 records, including employee accounts, Reports, User Group Membership, etc., including employee accounts...
 TheHatman · Thread · Aug 1, 2026 · Replies: 0 · Forum: Sellers Place

Multiple Fortune 500 Companies Azure Data Exfiltrated

To fully grasp the scale of this coordinated exfiltration effort, it is necessary to examine the specific volume of records extracted from each targeted tenant. The data below represents the staggering amount of internal corporate intelligence currently being brokered on underground forums, validated by threat intelligence researchers who have confirmed the structural integrity of the leaked datasets.

Organization	Exposed Records
McDonald's Corporation	~1,700,000+
TCS (Tata Consultancy Services)	~800,000+
Vodafone	~425,000+
HCL Technologies	~250,000+

Organization	Exposed Records
InterContinental Hotels Group (IHG)	~185,000+
Kyndryl	~170,000+
Gap Inc.	~80,000+
Hexaware Technologies	~20,000+
Wyndham Hotels	~9,000+

Cybersecurity researchers who have reviewed sample datasets from these forum posts confirm that the information appears highly credible. The validation relies on the presence of legitimate corporate email domains and field structures that align precisely with standard Microsoft Azure and Entra ID directory exports. The fact that only massive multinational firms appear in this specific campaign, rather than a broad cross-section of smaller businesses, strongly suggests a targeted exploitation of high-value stolen credentials rather than an underlying, systemic vulnerability in the Azure platform itself. If a core platform flaw were responsible, the victim list would inevitably include a wide array of small and medium-sized businesses that share the same underlying cloud infrastructure.

Anatomy of the Exfiltrated Data: Beyond Basic PII

The severity of this campaign becomes apparent when analyzing the specific data fields contained within the leaked directories. This is not a simple dump of names and email addresses scraped from public-facing websites; it is a complete, structured export of the internal organizational schema. Across all the affected tenant dumps, the leaked fields consistently include foundational corporate directory attributes that map the exact hierarchy and operational structure of the victim companies. Core identity and contact information forms the baseline, featuring full names, corporate email addresses drawn from both active company domains and tenant-specific fallback structures, direct phone numbers, and physical office addresses. The inclusion of tenant-specific fallback structures, specifically the legacy `.onmicrosoft.com` routing addresses, is particularly notable. These addresses are often forgotten by security teams but remain fully functional within the identity provider, providing attackers with alternative aliases to use during social engineering campaigns or to bypass email filtering rules that only scrutinize the primary corporate domain.

DisplayName	GivenName	Surname	JobTitle	UserPrincipalName	Email	EmployeeId	City	Country	CompanyName	Department
[REDACTED]	Carolyn	[REDACTED]	Stocens	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Anna	[REDACTED]	Labor R	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Ervin	[REDACTED]	Special	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Anda	[REDACTED]	BUSINESS	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Abigail	[REDACTED]	Marketi	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Ebitimi	[REDACTED]	Special	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	David	[REDACTED]	DIR-ENT	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Anthony	[REDACTED]	Sullivan	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Beata	[REDACTED]	SR MGR-	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Deanna	[REDACTED]	SUPV-AR	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Alyssa	[REDACTED]	Mallerd	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	David	[REDACTED]	SR MGR-	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Elisabeth	[REDACTED]	Scheaf	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Brian	[REDACTED]	MGR-DIG	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Andreas	[REDACTED]	Hertzfe	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	aterini	[REDACTED]	Senior	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	ement	[REDACTED]	SR MGR-	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	a (US Stores)	[REDACTED]	Kayla	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	hne' (US Stores)	[REDACTED]	Ajahne'	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	IA (US Stores)	[REDACTED]	MATRIA	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	elle (US Stores)	[REDACTED]	Gabriel	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	(US Stores)	[REDACTED]	Jake	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	(US Stores)	[REDACTED]	Ana	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	CISCO (US Stores)	[REDACTED]	FRANCIS	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	on Dyron	[REDACTED]	Greene	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	IA (US Stores)	[REDACTED]	Elaina	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	ERIA (US Stores)	[REDACTED]	VALERIA	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	(US Stores)	[REDACTED]	maria	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	ordan (US Stores)	[REDACTED]	Jordan	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	assidy (US Stores)	[REDACTED]	Chassid	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	IAIA (US Stores)	[REDACTED]	DAYAIA	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	o Giovanni (US Stores)	[REDACTED]	Giovanni	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Taylor (US Stores)	[REDACTED]	Taylor	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

A sample of the leaked McDonald's data

The exposure extends far beyond basic personally identifiable information, delving deep into the operational metadata of the enterprise. The datasets include granular organizational data such as unique employee IDs, specific job titles, departmental assignments, internal administrative notes, manager assignments, and direct report mappings. Technical samples reviewed by researchers reveal standard directory attributes like `DisplayName`, `UserPrincipalName`, and `EmployeeId` being exported in bulk. This level of detail provides a complete, navigable organizational chart for malicious actors, eliminating the need for noisy network reconnaissance. The inclusion of access and group mapping information is particularly alarming. The dumps reportedly contain user group memberships, service account details, and, most critically, explicit listings of Global Administrator accounts. Exposing this kind of privileged account data hands attackers a ready-made blueprint for targeted privilege escalation. In the hands of an initial access broker, knowing exactly which service accounts possess elevated permissions, and which human administrators manage those accounts, drastically reduces the time required to establish persistence and move laterally within a compromised cloud environment.

The Mechanics of the Intrusion: Infostealers and Session Hijacking

While TheHatman has repeatedly claimed that the data was obtained using compromised credentials, the precise initial entry point remains a subject of intense analysis among threat intelligence professionals. The speed, scale, and consistency of the data dumps point to a highly automated exfiltration process that was executed immediately after initial footholds were established. The prevailing theory, heavily supported by forensic evidence gathered by cybersecurity researchers at Hudson Rock, points to the rampant proliferation of infostealer malware as the primary catalyst for these breaches. Modern infostealers are sophisticated pieces of malware designed to silently infiltrate employee workstations and harvest a wide array of sensitive data. These malware families operate by directly parsing the local SQLite databases and encrypted storage files utilized by Chromium-based browsers and email clients, extracting the raw authentication material stored on the endpoint. To bypass the Windows Data Protection API (DPAPI), which encrypts browser storage keys, these infostealers execute within the context of the

logged-in user, allowing them to seamlessly decrypt and extract the underlying master keys required to read the stored cookies and passwords.

More importantly for cloud security, these infostealers are engineered to extract local state files and active session tokens directly from the victim's machine. When an employee authenticates to the Azure portal or Microsoft 365, the identity provider issues a session token or cookie that maintains their authenticated state, allowing them to navigate the environment without repeatedly entering their password and MFA code. If an infostealer compromises that endpoint, it can siphon these active cookies and transmit them to a command-and-control server. Attackers can then inject these stolen cookies into their own browsers, effectively cloning the victim's authenticated session in a technique commonly known as a Pass-the-Cookie attack. If the victim organization has not enforced strict token binding or Conditional Access policies that tie session validity to specific device states, this technique completely bypasses multi-factor authentication. The attacker is not breaking through the authentication prompt; they are walking through the front door using a session that the identity provider already considers fully verified. Researchers have identified compromised Azure credentials tied directly to infostealer infections linked to most of the affected companies, including machines traced to employees at Tata Consultancy Services, Gap Inc., HCL Technologies, and Kyndryl. In one particularly damning example, a single compromised device reportedly contained dozens of corporate credentials and hundreds of sensitive session cookies, including direct, unimpeded access to a Kyndryl Azure Active Directory account.

Over-Privileged APIs and Third-Party Integrations

While endpoint compromise via infostealers provides a clear pathway to session hijacking, the systematic extraction of millions of records also highlights the persistent danger of over-privileged application integrations and third-party APIs. Enterprise environments frequently rely on a vast ecosystem of third-party software, human resources platforms, internal scripting tools, and SaaS applications that require read access to the corporate directory to function correctly. Over time, as these applications are deployed and configured, they are often granted overly broad permissions, such as full directory read access via the Microsoft Graph API, simply to ensure compatibility and reduce friction during the onboarding process. Developers and IT administrators routinely assign the `Directory.Read.All` application permission to service principals, granting the application the ability to read every user, group, and role assignment within the tenant without requiring a signed-in user. This accumulation of technical debt creates a massive, often unmonitored attack surface.

If the OAuth tokens, client secrets, or service principal credentials governing these integrations are mishandled, stored in plain text within code repositories, or compromised via a supply-chain attack, a threat actor can leverage them to script the automated extraction of millions of user records. The sheer volume of data released by TheHatman suggests that once an initial foothold was achieved—whether through a stolen session cookie or a compromised service account—the attackers utilized automated scripts, likely leveraging PowerShell modules or Python libraries, to paginate through the tenant and download the directory in bulk. This automated approach allows a single compromised identity with the right API permissions to exfiltrate an entire global workforce's directory structure in a matter of hours, completely bypassing traditional network egress monitoring that might flag the transfer of large, unstructured files. The abuse of these excessive read privileges underscores the critical need for continuous governance over non-human identities and application registrations within the cloud tenant, as these silent integrations often possess more pervasive access than standard human users.

Stay Ahead of Cyber Threats

Get the latest cybersecurity news, critical vulnerabilities, threat intelligence, tutorials, and exclusive giveaways delivered straight to your inbox. No spam. Unsubscribe anytime.

[Subscribe to the Newsletter →](#)

Weaponization: From Directory Dumps to Business Email Compromise

The real-world risk of an exposed corporate directory extends far beyond the initial privacy violation and the embarrassment of a public data leak. Threat actors and downstream cybercriminal syndicates routinely weaponize this structured data to engineer highly convincing Business Email Compromise and spear-phishing campaigns. By understanding the exact reporting lines, job titles, and departmental structures of a target company, attackers can impersonate authoritative figures with devastating precision. A fraudster armed with this data does not need to guess who handles wire transfers, who manages vendor relationships, or who has the authority to approve emergency payments. They can identify the exact manager of a targeted finance employee, spoof that manager's communication style, and issue an urgent, context-aware directive designed to bypass standard verification protocols and trick the employee into initiating a fraudulent transfer. The structured data is frequently ingested into malicious Customer Relationship Management systems used by fraud rings, allowing them to track targets, manage communication threads, and automate the timing of their extortion or fraud attempts based on the target's working hours and time zone.

Beyond financial fraud, the exposure of service accounts and global administrator names functions as a highly curated targeting map for initial access brokers and ransomware crews. These advanced threat groups are constantly looking for the fastest, most reliable route into critical infrastructure. Knowing the specific identities of the IT personnel responsible for managing the cloud environment allows attackers to launch highly focused social engineering campaigns against helpdesk staff or deploy Adversary-in-the-Middle phishing kits specifically tailored to the exposed administrators. By impersonating a known global administrator or leveraging the exposed internal organizational notes, attackers can manipulate support personnel into resetting passwords, generating temporary authentication codes, or adding malicious devices to the trusted device list. This targeted approach to privilege escalation is significantly more effective than broad, indiscriminate phishing attempts, and it relies entirely on the rich, structured metadata that was carelessly exposed through these Azure directory dumps. The transition from a simple data leak to a full-scale network compromise is drastically accelerated when the attackers already possess a complete map of the organization's internal hierarchy and privilege architecture.

Organizations must treat this sprawling exfiltration campaign as a definitive wake-up call regarding the state of their cloud security posture. The era of relying on legacy perimeter defenses and basic password policies is over; credential hygiene and rigorous identity governance now determine an enterprise's true exposure to sophisticated threat actors. Mitigating this class of attack requires a fundamental shift toward continuous, proactive monitoring and the implementation of advanced identity protection controls. Security teams must integrate continuous dark web and infostealer monitoring into their security operations workflows, allowing defenders to detect and revoke compromised credentials before they can be leveraged to siphon millions of sensitive corporate records. Automated alerting must be configured to trigger immediate password resets and session revocations the moment a corporate credential appears in a known infostealer log database.

At the technical level, enforcing strict, risk-based Conditional Access policies is non-negotiable. Organizations must mandate the use of phishing-resistant authentication methods, such as FIDO2 security keys or Windows Hello for Business, which cannot be easily harvested by infostealers or intercepted by adversary-in-the-middle phishing kits. To counter token theft, enterprises must implement token protection mechanisms, such as Microsoft Entra ID Token Protection, which cryptographically binds session tokens to the specific device and user they were issued to. This ensures that even if an attacker successfully steals a session cookie from an infected workstation, that token will be rendered completely useless when injected into an unmanaged, external machine. Security architects must also enforce Privileged Identity Management to eliminate standing access for Global Administrators, requiring just-in-time elevation that is strictly audited and time-bound. Finally, security architects must conduct rigorous, recurring audits of third-party API permissions and application registrations. Enforcing the principle of least privilege, removing unnecessary directory read access, and routinely rotating service principal credentials are essential steps to close the gap before attackers exploit the silent, over-permissioned integrations that currently plague modern enterprise environments. The identity perimeter is the only perimeter that matters in a cloud-native world, and defending it requires constant vigilance and uncompromising technical rigor.

Source: <https://theybersecguru.com/news/azure-data-exfiltration-thehatman-campaign/>