

Threat Talks

ShinyHunters

How a phone call stole the cloud

No malware. No zero-day. No software vulnerability. Just a phone call.

In 2025, ShinyHunters became the headline cybercrime story of the year by talking its way into companies' Salesforce environments. An operator poses as IT support, walks an employee through a "fix", and with one click the employee hands over API access to the entire CRM.

ShinyHunters is not one gang. It is a brand worn by several loosely connected crews in the English-speaking "The Com" ecosystem, alongside Scattered Spider and Lapsus\$. The business model is pure data extortion: pay, or we leak it.

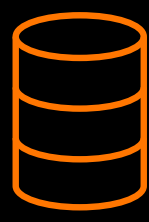
By 2026 the same playbook had spread to Okta, Microsoft 365 and Google Workspace. In February it hit Dutch telecom Odido.



threat-talks.com

In this Threat Talks infographic we discuss:

- ShinyHunters: the SaaS vishing and data extortion playbook



6.2M

Odido customers had names, IBANs, dates of birth and ID details exposed.

Source: NL Times



0

malware, exploits or software vulnerabilities needed. The human is the exploit.

Source: Google Threat Intelligence Group



72 hours

to pay in Bitcoin before the stolen data goes to the leak site.

Source: Google Threat Intelligence Group



4

threat clusters wear the ShinyHunters brand: UNC6040, UNC6240, UNC6661 and UNC6671.

Source: Google Threat Intelligence Group

ShinyHunters

A phone call, a malicious app. Then the whole CRM walks out the door.

ShinyHunters has run a "pay or we leak it" data-extortion model out of the BreachForums ecosystem since around 2020. Google Threat Intelligence Group tracks the activity as separate clusters: UNC6040 handles the intrusion, UNC6240 the extortion, with UNC6661 and UNC6671 added in 2026. The playbook abuses Salesforce and other SaaS platforms exactly as they were designed to be used. By 2026 the group had stood up a "SHINYHUNTERS" leak site and was reportedly building a ransomware-as-a-service called ShinySp1d3r.

Aliases

mSOC confidence score

Threat category

Severity

UNC6040, UNC6240, UNC6661, UNC6671, Bling Libra (Unit 42)

Confirmed

Cyber Attacks, APT Attacks, Social Engineering

High



ATT&CK Technique

T1598.004 - Phishing for Information: Spearphishing Voice

Attack Strategy

Impersonate IT support by phone and talk an employee through a "fix": the human is the exploit

Evasion

No malware or exploit; calls routed through Mullvad VPN / Tor to mask origin

Complexity

Low

Target Type

Help desks and staff at SaaS-heavy multinationals



ATT&CK Mitigation

M1032 - Multi-factor Authentication

Attack Vector

Credential reuse and MFA self-enrollment for lateral movement

Detection

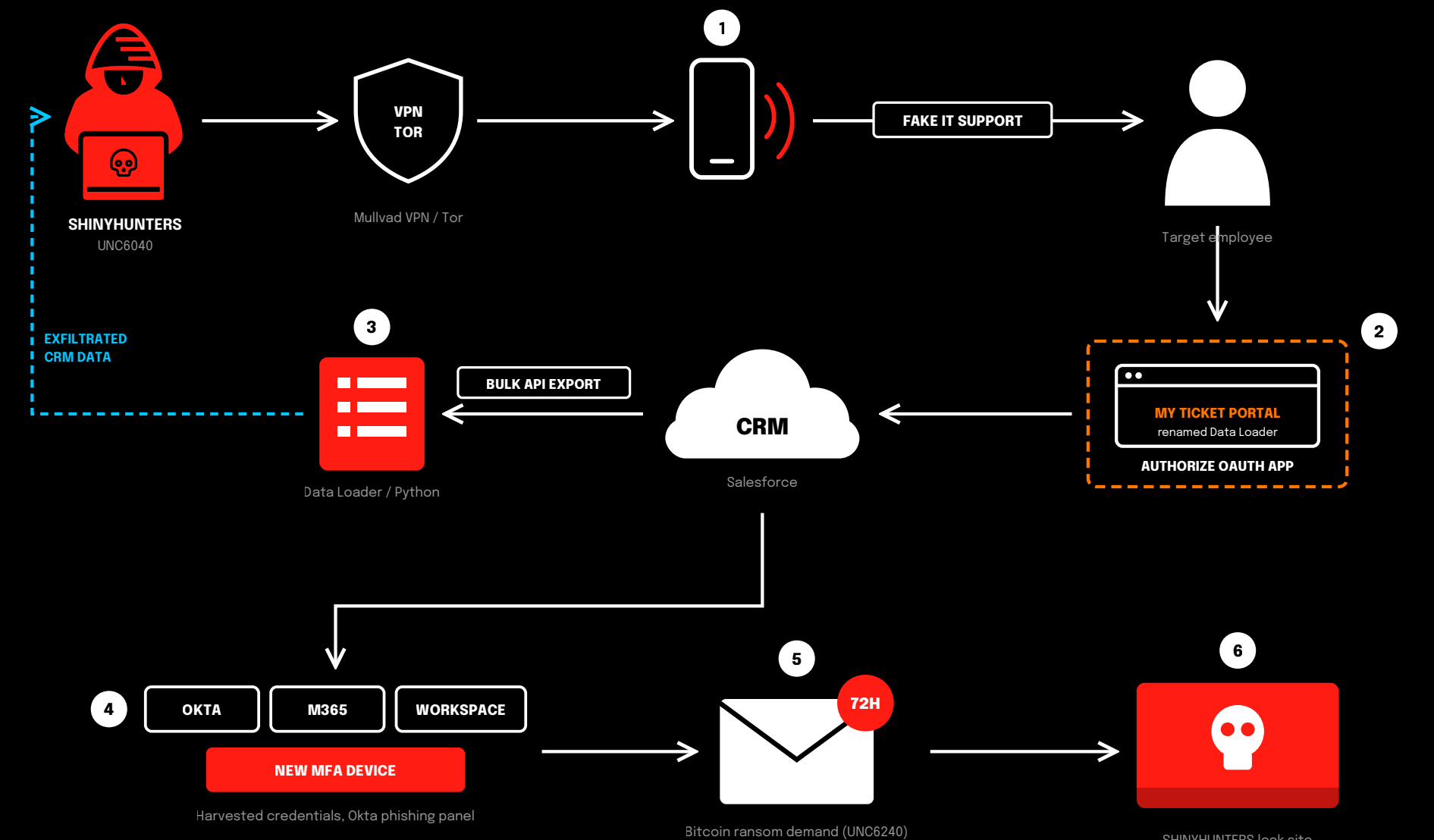
New MFA device enrollments; impossible-travel and cross-SaaS login anomalies (Okta/M365)

Threat Level

High

Threat Actor Type

The Com / SaaS-extortion ecosystem



Vishing and initial access

1 An attacker posing as IT support calls an employee. No malware, no exploit: the human is the entry point.

M Verify IT-support callers out of band. Train help desks against "authorize this app" requests.

Malicious OAuth app authorization

2 The victim approves a fake Data Loader app ("My Ticket Portal"), handing over API access to the CRM.

M Restrict who can authorize connected apps. Require admin review for new OAuth apps.

Bulk API exfiltration

3 The attacker bulk-exports CRM data via the API. Authorized traffic looks like normal activity.

M Alert on bulk exports and VPN/Tor logins. Cap export rights with least privilege.

Lateral movement

4 Stolen credentials let the attacker pivot to Okta, M365 and Google Workspace. Alert emails get deleted.

M Segment SaaS platforms, use phishing-resistant MFA and monitor new MFA device enrollments.

Delayed extortion

5 Weeks later, "ShinyHunters" demands Bitcoin within 72 hours, backed by proof samples and DDoS pressure.

M Have an extortion playbook ready. Expect inflated record counts (8M claimed vs 6.2M at Odido).

Data leak and publication

6 Victims who refuse to pay see their data leaked in waves. Odido: millions of records, including IBANs and IDs.

M Prepare breach notification in advance. The perimeter held but the trust model failed.

Taxonomy

ATT&CK Technique

Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation

Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy

Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector

What is the primary method of attack.

Evasion

Tactics used by the attacker to avoid detection or bypass security.

Detection

Mechanism to identify malicious activities or system anomalies.

Complexity

How easy it is to exploit the vulnerability or carry out the attack.

Threat Level

How severe the threat is.

Target Type

The category of organization that may potentially be targeted.

Threat Actor Type

What type of threat actor may be involved.

Contact us @
team@threat-talks.com



threat-talks.com

ON2IT
ZERO TRUST INNOVATORS

amsix