[Op Report] CastleRAT Campaign leads to Hands-on-Keyboard ATO Operations — Deception.Pro Blog

By Jan 7 Written By MalBeacon

Published: 2001-01-07 · Archived: 2026-04-05 16:20:55 UTC

Executive Summary

This Deception.Pro operation captured a **multi-stage malware intrusion culminating in hands-on-keyboard (HoK) activity focused exclusively on account takeover (ATO)**: not ransomware staging or enterprise lateral movement.

The campaign initiated with a **Matanbuchus loader** via a malicious MSI, followed by **NetSupport RAT**, **Remcos RAT**, and ultimately **CastleRAT (aka NightShadeC2)**. Rather than enumerating Active Directory or moving laterally, the actor exfiltrated browser credentials and used CastleRAT to **proxy the replica's live browser session**, attempting logins against financial-institution websites directly from the compromised workstation.

This operation strongly reinforces an emerging pattern: **some access brokers and malware operators are monetizing endpoints immediately through ATO and fraud**, bypassing the traditional "steal creds → sell access → ransomware affiliate" pipeline entirely.

Environment Overview

- **Replica Role:** Senior Real Estate Portfolio Analyst
- **Industry:** Real Estate
- **Replica Organization:** Global commercial and residential real estate firm leveraging AI-driven portfolio analytics
- **Operation Duration:** ~7 days (Dec 4–Dec 11, 2025)

Timeline of Activity

2025-12-04 20:44:13
Initial infection chain triggered via malicious MSI (`CarrierRegistration.msi`). Embedded **Matanbuchus DLL** downloads additional payloads.

- Downloads observed:
  - `TBank231.zip`

- `Petuhon.zip`
- Host: `172.86.123[.]222:80`

2025-12-04 20:44:45
NetSupport RAT deployed via DLL sideloading:

- Path:

  `C:\Users\USER_REDACTED\AppData\Roaming\Player\yuh.exe`

- C2: `88.218.64[.]224:443`

2025-12-04 → 2025-12-07
Credential staging and reconnaissance:

- Browser data archived
- C2 TLS traffic to `diplomitta[.]com (95.164.53[.]39)`

2025-12-08 21:46:12
Remcos RAT deployed via DLL sideloading:

- Path:

  `C:\Users\USER_REDACTED\AppData\Local\DataFileConverter\crash-handler-app.exe`

- C2: `216.126.237[.]122:443`
- Confirmed via JA3 TLS fingerprinting and malware config extraction

2025-12-08 → 2025-12-08 23:42:06
Hands-on-keyboard activity observed:

- Actor launches Microsoft Edge and Chrome browsers via **CastleRAT**
- Live browser sessions tunneled through CastleRAT
- Actor attempts logins to financial-institution websites using exfiltrated browser credentials
- No AD enumeration, no lateral movement

Indicators of Compromise (IOCs)

File Hashes & Malware

- **CarrierRegistration.msi**
  SHA-256:
  `a65336f002b154eab29856ce11d363db89fe8c05bcccc5d0e1611bb355eb0b8d`

- **Stage-Two Downloads**
  - `TBank231.zip` `c1ec8c0e0b538ee0c884a077b4dc8cc7e2765cd30ef60350da5d8d52232f1cf7`
  - `Petuhon.zip` `f6954b64af18386c523988a23c512452fd289e3591218e7dbb76589b9b326d34`

Malicious Paths

- `C:\Users\USER_REDACTED\AppData\Roaming\5687ca6915a1f29a\Update.exe`
- `C:\Users\USER_REDACTED\AppData\Roaming\Player\yuh.exe`
- `C:\Users\USER_REDACTED\AppData\Local\DataFileConverter\crash-handler-app.exe`

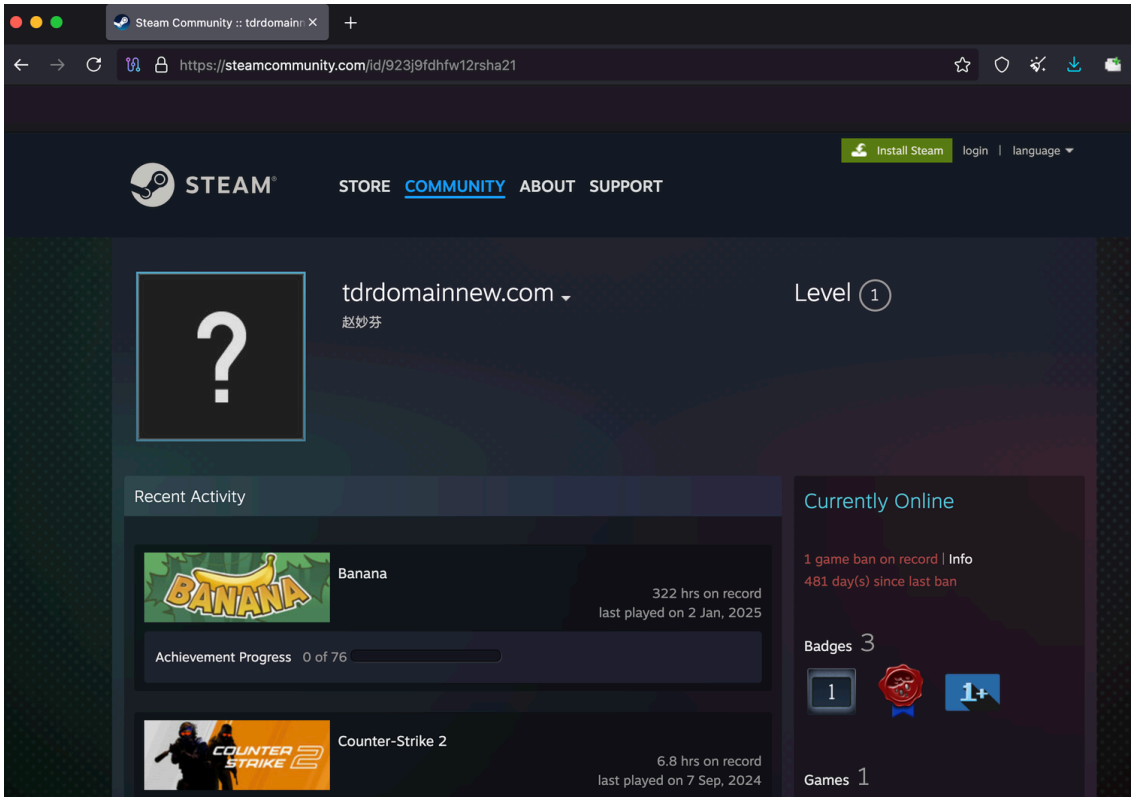
Network IOCs

C2 Infrastructure

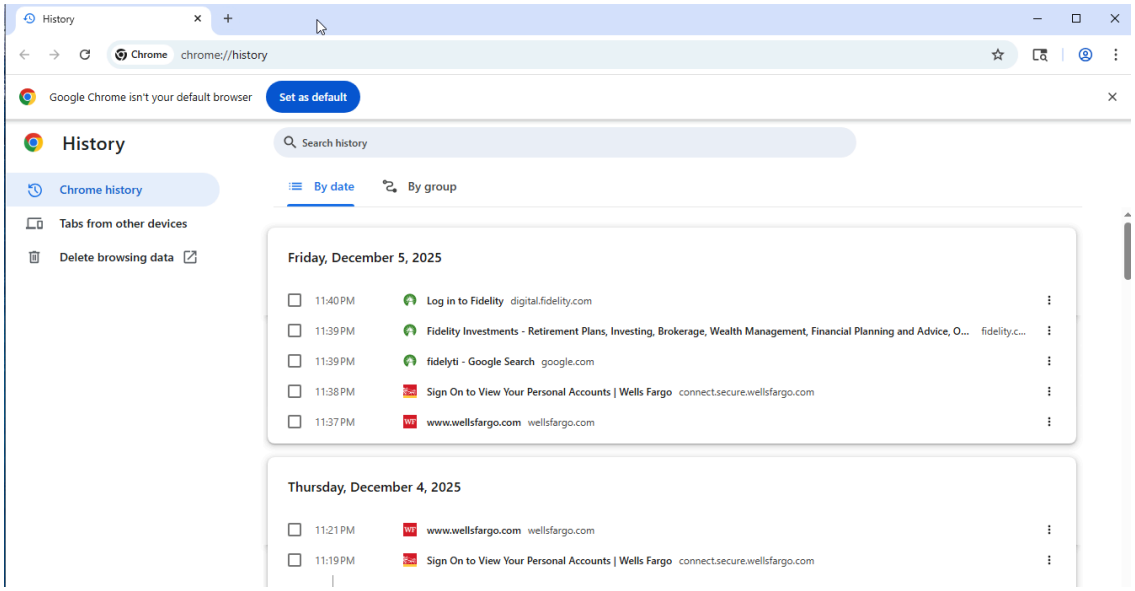
- `216.126.237[.]122:443` — Remcos RAT
- `88.218.64[.]224:443` — NetSupport RAT
- `95.164.53[.]39` (`diplomitta[.]com`)
- `172.86.123[.]222` — Matanbuchus payload host

CastleRAT / NightShadeC2 Dead-Drops

- Steam profile → `tdrdomainnew[.]com` (`207.189.164[.]112`)
- Steam profile → `secondtdr[.]com` (`62.60.248[.]38`)



Example Steam profile page leveraged by CastleRAT as a command-and-control dead-drop mechanism.



Chrome browser history from the replica workstation, capturing websites visited by the threat actor during live HoK activity.

Source: https://blog.deception.pro/blog/castlerat-dec2025-hok-ato