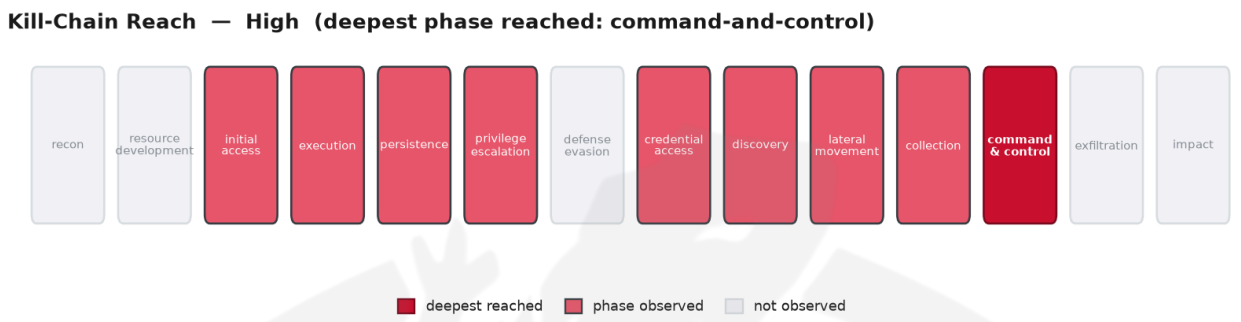
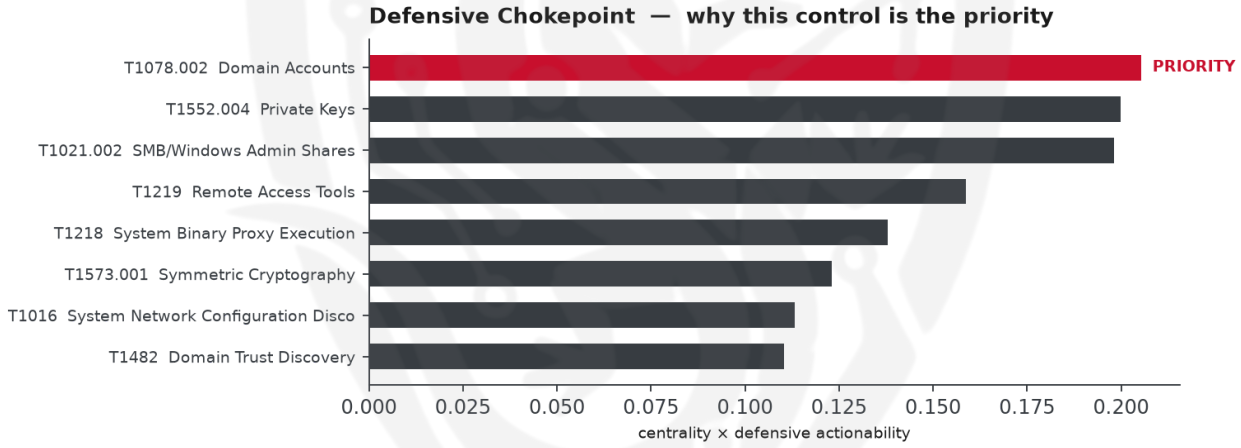
THREAT REPORT: CAVERN MANTICORE

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The source attributes this activity to Cavern Manticore, a threat actor targeting Israel, specifically the Government and Technology sectors. The actor's techniques and tactics indicate a high level of operational risk, with a focus on gaining and maintaining access to targeted systems. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's activities have been observed to reach the level of command-and-control, indicating a significant level of compromise.

Threat Overview

Cavern Manticore, the attributed threat actor, has been observed utilizing various techniques to gain access to and control targeted systems. Although the specific malware families and central CVE used are insufficiently documented, the actor's tactics involve a range of techniques, including archive utility,

standard encoding, password guessing, and symmetric cryptography. The targeted country is Israel, with a focus on the Government and Technology sectors.

Attack Chain and Priority Control

The observed techniques used by Cavern Manticore form a complex attack chain, involving multiple steps to gain and maintain access to targeted systems. The priority technique, T1078.002 Domain Accounts, serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with Cavern Manticore's activities. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1560.001 Archive via Utility
- T1132.001 Standard Encoding
- T1110.001 Password Guessing
- T1003.004 LSA Secrets
- T1087.002 Domain Account
- T1573.001 Symmetric Cryptography
- T1087.001 Local Account
- T1135 Network Share Discovery
- T1219 Remote Access Tools
- T1218 System Binary Proxy Execution
- T1021.002 SMB/Windows Admin Shares
- T1552.004 Private Keys
- T1016 System Network Configuration Discovery
- T1482 Domain Trust Discovery
- T1083 File and Directory Discovery
- T1049 System Network Connections Discovery
- T1069.001 Local Groups
- T1078.002 Domain Accounts
- T1071.001 Web Protocols
- T1018 Remote System Discovery
- T1046 Network Service Discovery

- T1574.002 Hijack Execution Flow
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1078.002 Domain Accounts (centrality 0.2053).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4293; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Chimera	0.4293
Lotus Blossom	0.4229
Volt Typhoon	0.3927
FIN13	0.3904
APT3	0.3866

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator
Domain	auth[.]hospitalinstallation[.]com
Domain	adserviceupdate[.]com
Domain	hospitalinstallation[.]com
Domain	hygienehistory[.]com
Domain	google[.]com[.]hospitalinstallation[.]com

Type	Indicator
URL	hxxps://adserviceupdate[.]com/cac[.]aspx
URL	hxxps://hygienehistory[.]com/cac[.]aspx
Hash	a9336884e006503bc821f3f0d36f141f
Hash	d0bba7c040ecffd8cc31a62330a144eb
Hash	0f57a2bb4c0696170b73e2d35f17c5a6f2f910d7
Hash	843d2017c4ded1dbb694dd4bf20bcd9e92af92f6
Hash	0a3663648a46771a5a5423ad01e91a4e7ba825595e99fa934cb35cbb4848adc8
Hash	2cb1ad3b22db8e3666ea138fee88034a87a87cf43db3d3265a675ebf221379b0
Hash	30cb4679c4b8599eeb3d63a551716475c6332bdc4d4b4e3de0964aadb3092a10
Hash	37e123bd7998af4eae32718ce254776f36365a80ba56952593dab46f536d4066
Hash	5394d3b220de4695f731647e3a70545f951a8912ceb0c6585efab8d6842e8b42
Hash	541b1f417b9e42078c3355693a8a492b6a76048850f6549a429e0be99e6819cb
Hash	5dc08bda6919a57a85e5f38b857985fa71529ca39c8299868d5a49a987e19b18
Hash	7d586fb7f94182a8e2a0e53c7e4deb898066da029da5cd9972a94a59ca6d255a
Hash	8e9425c0b46eeb516610ae913d13f2b3f44a023043cb099277031d4ec38a6134
Hash	92cae0ad7f98f51a14bcc0ee05e372ebdc29ea96ea7bd161bd3f55198767603b
Hash	a4aa217def4c38f4ecacdf47b1cd687f60cc74c18ab75195be3c4357a790bf41
Hash	b630c96d3763182533d4fb9b614134382bd644cb02c6c1c3ade848b6ecc31e86
Hash	cbc9485db715e1b8cc384fe94b4cceadca4006cda8a5e28adc8848529cfafc93
Hash	ccf218189c3aadb1c761da14bfda3bae686769031e1e1b10007648bd72e34748

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1078.002 Domain Accounts (initial-access)

- **Observed here:** T1078.002 Domain Accounts was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1190 Exploit Public-Facing Application (initial-access)
- **Basis:** 32 of 170 documented groups that use Domain Accounts also use Exploit Public-Facing Application (conditional 0.50, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

Cavern Manticore could pivot to exploiting a public-facing application, as indicated by T1190, in an attempt to regain a foothold and achieve their objectives, potentially by targeting a vulnerable web server or application that was not properly secured. This shift may allow them to bypass the domain account restrictions that were just imposed. To counter this potential move, the mandated defensive control is to patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Also plausible (same tactic): T1133 External Remote Services (n=25, lift 2.4), T1199 Trusted Relationship (n=10, lift 2.2)

Detection and hardening for the pivot (T1190 Exploit Public-Facing Application)

- **Telemetry:** WAF / reverse-proxy logs; Web server logs; EDR on the DMZ host
- **Detect:**
  - Exploit strings and anomalous request paths in access logs; 500s spikes
  - The web/app service account spawning shells or network tools
  - Outbound connections from a server that should never initiate them
- **Harden:**
  - Patch internet-facing software fast; virtual-patch at the WAF meanwhile
  - Egress filtering from DMZ hosts; least-privilege service accounts
- **MITRE:** M1051 Update Software, M1050 Exploit Protection, M1016 Vulnerability Scanning, M1030 Network Segmentation · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic