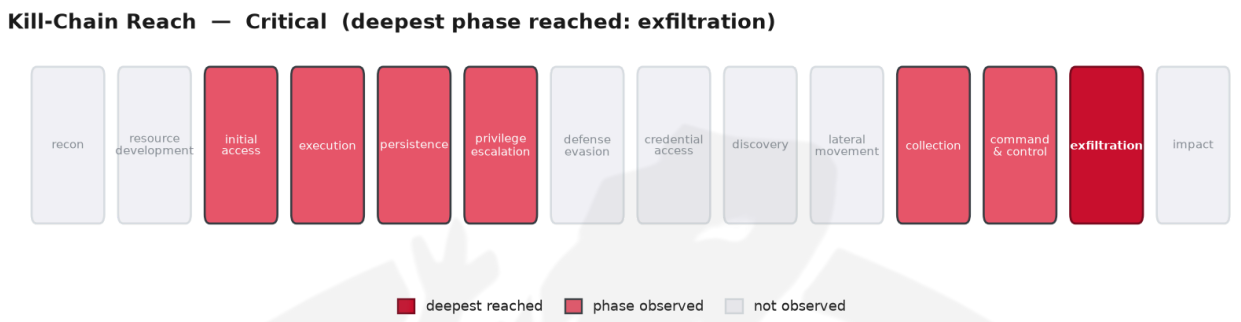
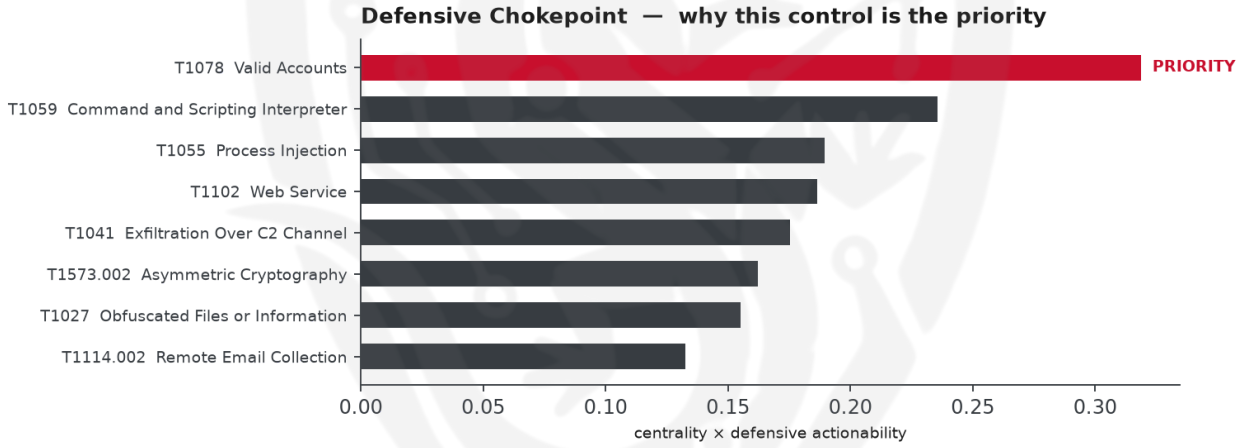
THREAT REPORT: CHRYSENE

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 CHRYSENE, a threat actor that has been observed targeting Israel with various malware families, including CAV3RN, RDAT, and Veaty. The actor's techniques include multiple methods for encoding, cryptography, and exfiltration, indicating a high level of sophistication. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The actor's ability to exfiltrate data poses a significant risk, making defensive action critical.

Threat Overview

CHRYSENE, the observed threat actor, utilizes a range of malware families, including CAV3RN, RDAT, SC5k, OilCheck, OilBooster, Solar, WhisperGate, and Veaty, to target entities in Israel. Although the central CVE exploited is not specified due to insufficient data, the actor employs various techniques such as standard encoding, domain generation algorithms, and symmetric cryptography. The victimology indicates that the actor is interested in data exfiltration, among other goals.

Attack Chain and Priority Control

The attack chain involves a complex series of techniques, including encoding, cryptography, and exfiltration methods. The priority technique identified is T1078 Valid Accounts, which serves as a critical chokepoint in the actor's operations. To counter this, the recommended priority control is to "Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs used by the threat actor, as indicated by "n/a" in the infrastructure observations. 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)

- T1132.001 Standard Encoding
- T1568.002 Domain Generation Algorithms
- T1071.004 DNS
- T1573.001 Symmetric Cryptography
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1059 Command and Scripting Interpreter
- T1102 Web Service
- T1041 Exfiltration Over C2 Channel
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1114.002 Remote Email Collection
- T1573.002 Asymmetric Cryptography
- T1567.002 Exfiltration to Cloud Storage
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1008 Fallback Channels

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3187).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3831; 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
TA551	0.3831
RedEcho	0.3608
Tropic Trooper	0.3546
ZIRCONIUM	0.3465
APT18	0.3368

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	cloudlanecdn[.]com
Domain	clipeditskill[.]com
Domain	accesslinkssl[.]com
Domain	d[.]53466d4c67515a[.]0[.]p[.]cloudlanecdn[.]com
Domain	google[.]com[.]ayalon-print[.]co[.]il
Domain	ns1[.]cloudlanecdn[.]com
Domain	ns2[.]cloudlanecdn[.]com
Domain	ns3[.]cloudlanecdn[.]com
Domain	ns4[.]cloudlanecdn[.]com

Type	Indicator
Hash	75e51774b8f79e5f256eaae639635f911b3e744d4774fd6068dd980255621509
Hash	b3d0f6e4e3be395fd7cf9e8101c89963d77216578cbb117a6ac9bc3564485eff
Hash	f3f3006f8304788251b153d53b305322b8acab0c66ec816b8d9f101bcc851da3
Hash	29b2b8c5d99f05bfcdd0d8d976eb5678
Hash	c092b02fbc0fdf7ee9608dd016673806
Hash	caf021dda726b8ba049c2aa395e505a1
Hash	66c8a4d782ec9e19d67f426376e0ebb5af868590
Hash	83ed3f17a83b083246f90011d33861cdb5734ab3
Hash	beb57441b81e56d1d7ba72acd841f2ffe171a325

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 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid 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 Valid Accounts also use Exploit Public-Facing Application (conditional 0.50, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

With T1078 Valid Accounts blocked, CHRYSENE could preserve the same objective by pivoting to T1190 Exploit Public-Facing Application, a technique commonly paired with it across tracked groups. Defensive countermeasure: 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