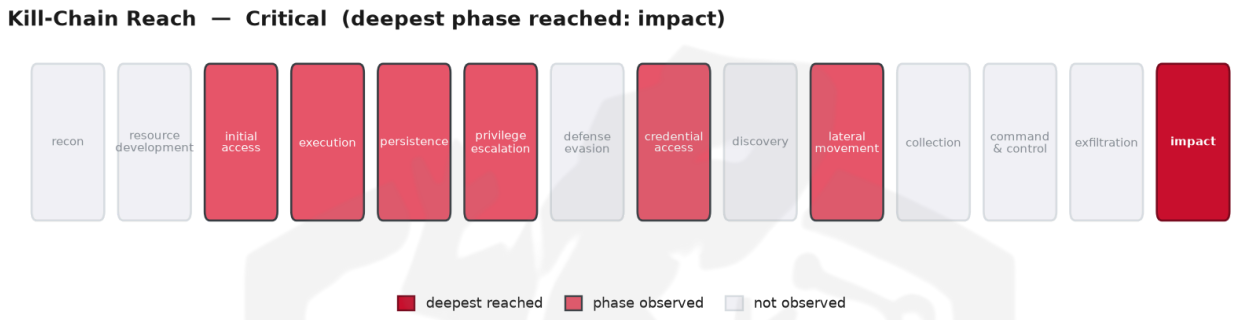
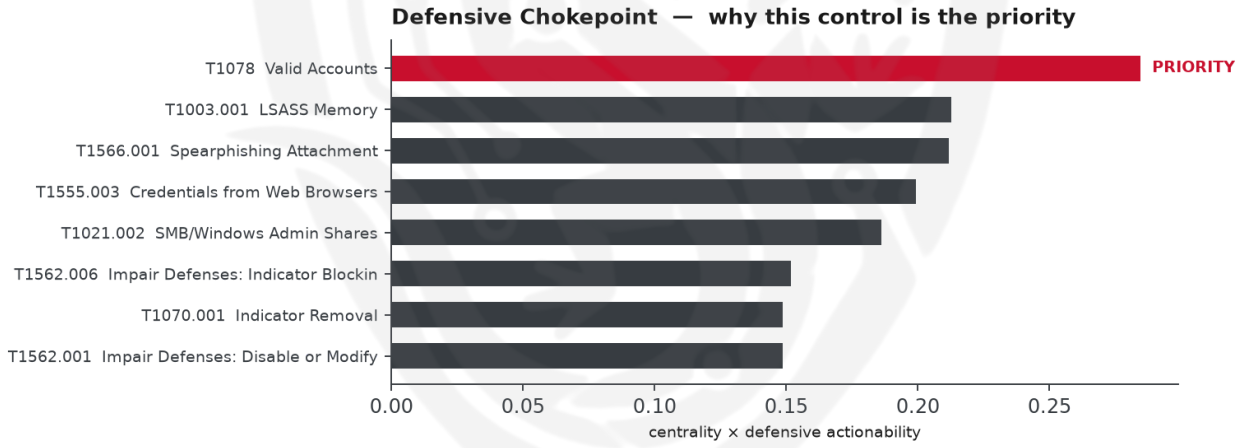
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 observed cluster of activity has been linked to the Avalon and CrownX malware families, although the targeted country and sectors remain unknown. The threat actor's use of various techniques, including scheduled tasks and spearphishing attachments, has allowed them to gain access to victim systems. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The operational risk band for this threat is Critical, indicating a high potential for impact.

Threat Overview

The threat actor, whose identity is unknown, has been observed using the Avalon and CrownX malware families to carry out their attacks. Although the central CVE exploited by the threat actor is unknown, they have been seen using a range of techniques to gain access to and control over victim systems. The

victimology of the threat is also unknown, making it difficult to determine the specific targets of the campaign.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with initial access techniques such as spearphishing attachments and scheduled tasks. The threat actor then uses techniques such as stealing web session cookies and deobfuscating files to maintain access and evade detection. The priority technique in this chain is T1078 Valid Accounts, which allows the threat actor to use legitimate accounts to access and control victim systems. To mitigate this threat, the 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 available information on the hosting providers or ASNs used by the threat actor, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher by AbuseIPDB, 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)

- T1053.005 Scheduled Task
- T1561.002 Disk Structure Wipe
- T1539 Steal Web Session Cookie
- T1218.004 InstallUtil
- T1566.001 Spearphishing Attachment
- T1140 Deobfuscate/Decode Files or Information
- T1021.002 SMB/Windows Admin Shares
- T1555.003 Credentials from Web Browsers
- T1070.001 Indicator Removal
- T1003.001 LSASS Memory
- T1562.006 Impair Defenses: Indicator Blocking
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1070.004 File Deletion
- T1027.002 Software Packing
- T1204.001 Malicious Link
- T1055.001 Dynamic-link Library Injection

- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2846).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.424; 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
Sandworm Team	0.424
Molerats	0.4234
FIN8	0.4115
Silence	0.4109
Malteiro	0.3974

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	helloxcherry[.]com
URL	hxxps://helloxcherry[.]com/cdn/static/c3587edc48c37656b29bcd3da9458eea/update
Hash	c3587edc48c37656b29bcd3da9458eea
Hash	4b7301f02b8312ae6de614981f325dbbabee32166630618fdff74615d9a487ba
Hash	59a260716d05c20229c6a46fe0a2fb5b80fa30c9c73a850222d9d3454426a60a

Type	Indicator
Hash	607cb58b8a592885eef5cfbe35ddce962741b0775c575f58cb3a96ca0ee893a6
Hash	adbc18f15019ef2ba6890b7996445c14350d57ba772eb33182889bc14ac47085
Hash	b7d50d0406afcd2efd87bf3bf8c4211719ba9817dd2e0ad62af10c933e765e28
Hash	c725815cbb07ab5be8903e74ef8aea46ef9c25e4a3bc626ae94bfc1ae21df6e3
Hash	e3ec5926a167d6e3359f98cdfb7ac3b2cce97652843056505d02e6d2898573c6

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:** the threat actor used T1566.001 Spearphishing Attachment here as an alternative initial-access technique.
- **Projected pivot:** T1566.001 Spearphishing Attachment (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to T1566.001 Spearphishing Attachment to maintain their objective by sending targeted emails with malicious attachments, which may bypass the blocked valid account control and potentially deceive users into executing the attachment. This technique could be used to deliver malware or establish a foothold in the network, and the actor may tailor the spearphishing emails to increase the likelihood of success. The defensive control to counter this would be to implement a system where you Sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button.

Detection and hardening for the pivot (T1566.001 Phishing)

- **Telemetry:** Email security gateway logs; Endpoint (Office child processes); Proxy/DNS
- **Detect:**
  - Office apps (winword/excel) spawning script or LOLBIN child processes
  - Mark-of-the-Web bypass; ISO/IMG/LNK/HTML-smuggling attachments detonating
  - First-contact domains and newly registered domains in mail links
- **Harden:**
  - Attachment sandboxing; block high-risk types (iso, img, lnk, htm) at the gateway
  - Attack-surface-reduction rules for Office child processes; user reporting button
- **MITRE:** M1049 Antivirus/Antimalware, M1031 Network Intrusion Prevention, M1017 User Training, M1021 Restrict Web-Based Content · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic