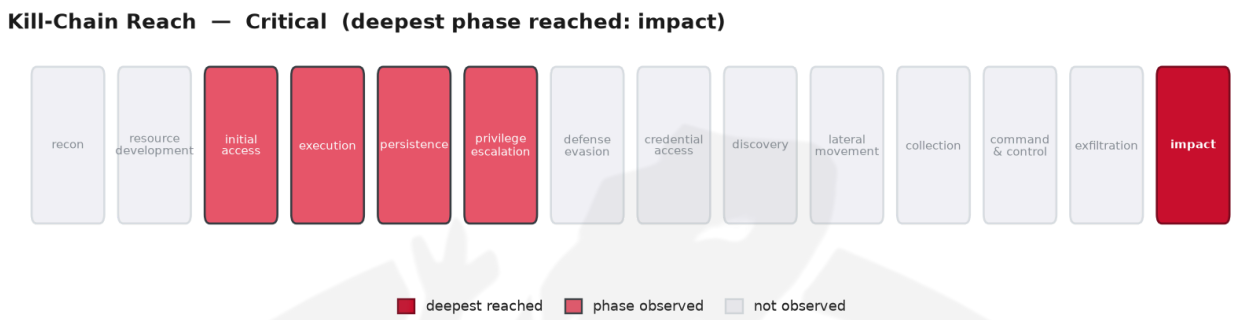
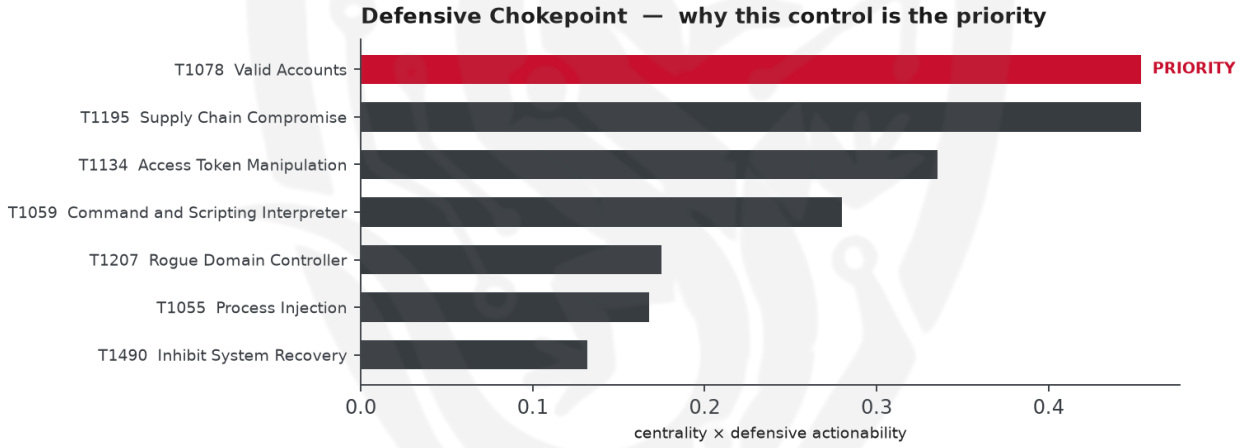
THREAT REPORT: SALAT STEALER CAMPAIGN

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 involves the Salat Stealer malware, targeting unspecified countries and sectors. The priority defensive action should be given to enforcing multi-factor authentication and managing account privileges. The threat actor's identity and motivations remain unclear, but the campaign's impact is considered critical. The reporting indicates techniques such as process injection and command scripting are used, but the primary concern is the exploitation of valid accounts.

Threat Overview

The threat actor, whose identity is not specified, is associated with the Salat Stealer malware family. The exploited vulnerability is not identified, and the victimology is unclear. However, the techniques inferred from the report suggest a focus on leveraging valid accounts and potentially compromising system recovery mechanisms.

Attack Chain and Priority Control

The observed techniques form a chain that includes process injection, command scripting, and access token manipulation, ultimately leading to potential system compromise. The priority technique is T1078 Valid Accounts, which serves as a chokepoint in the attack chain. To mitigate this, the lead control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

The Salat Stealer malware family has been corroborated by abuse.ch. However, there is no information available on the hosting providers or ASNs associated with this campaign, and no indicators have been flagged with high confidence by AbuseIPDB.

Technical Appendix

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

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1055 Process Injection - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1134 Access Token Manipulation - T1195 Supply Chain Compromise - T1207 Rogue Domain Controller - T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.4537).
- Operational risk: Critical (score 0.896, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3086; 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
Suckfly	0.3086
Threat Group-1314	0.3086
BlackByte	0.2513
GOLD SOUTHFIELD	0.2357
PittyTiger	0.2357

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: SalatStealer.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
Domain	xenoexecutor[.]in	
Hash	60118ba6124480d1c28b3d30f380aa64030418ba1774e8437f9cfae5ea191271	SalatStealer
Hash	075b3caa3a754c23f929a1591c6b333c7da1080a5fdf8ea2a3497d1505b60dde	SalatStealer
Hash	7376aaca33eab974ec527d44753d8016c1d305e2db935189a91a57b0ecbb3ccd	SalatStealer
Hash	d6c7ca66c4fef2bf7c62261f58f2f6ab	SalatStealer
Hash	7e6f8597028e4dc2ff63ed330f989fe9dbca3093	SalatStealer
Hash	347e3ef094831fd280628c711804603f695b020e365606174a6ba118ebf56cff	SalatStealer
Hash	742be0bf09856460bc85f9674d6914c7	
Hash	3711d405a68a926f73df57c886845a1c7928b778	
Hash	7018dc48efdf1311d644225e3c9e5f8f6d49863dbaca315f16d25473f127978d	
Hash	fec793499d9df0458b611a71dda23b41ba1c28038a79924ab606937e26e77115	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

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 initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique allows them to leverage the existing Windows infrastructure to gather information and execute tasks, potentially exploiting the same level of access that was previously obtained through valid accounts. This technique may be particularly appealing as it enables the actor to interact with the system in a way that blends in with normal administrative activity, making it harder to detect. To counter this potential move, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command