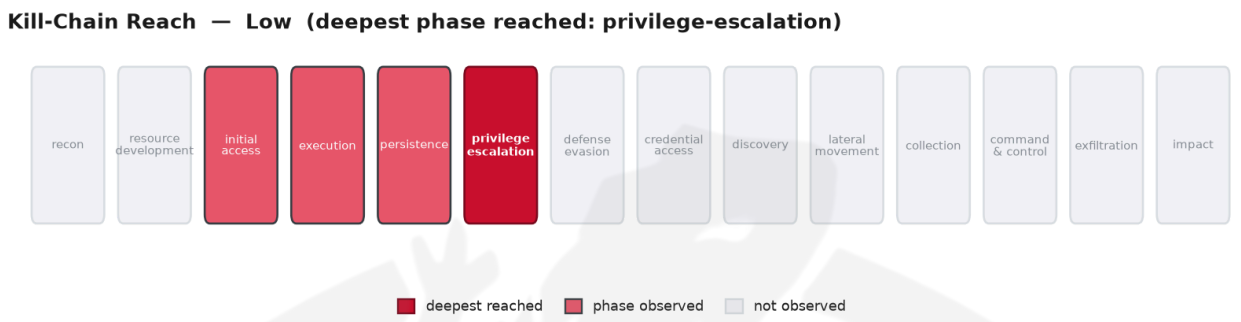
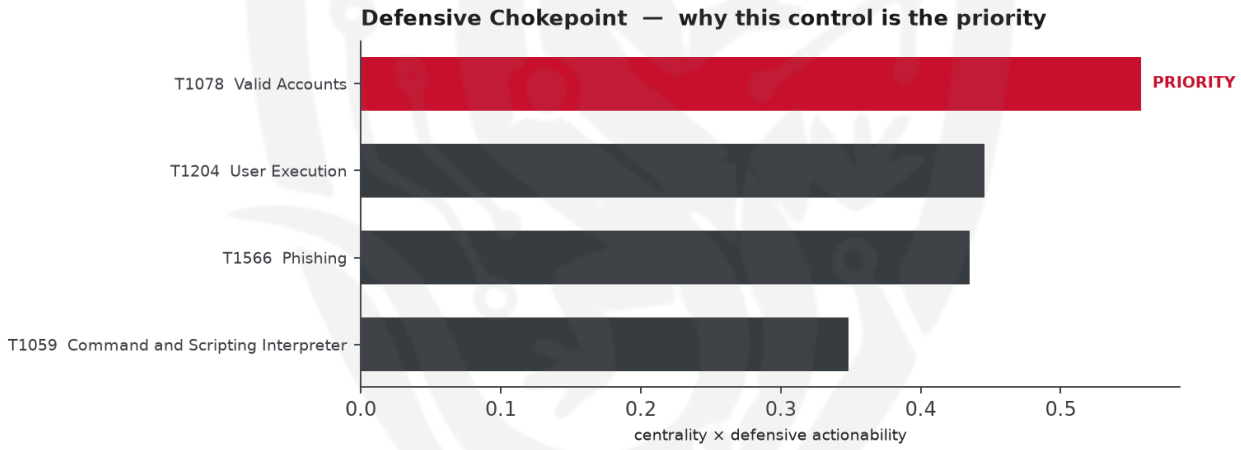
THREAT REPORT: O1OO1'S SILABRAT CAMPAIGN

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 source attributes this activity to o1oo1, who has been observed utilizing the SilabRAT, Hijackloader, and AsmCrypt malware families. While specific targets and countries are not identified due to insufficient data, the threat actor's techniques suggest a focus on exploiting valid accounts for initial access. Priority should be given to enforcing multi-factor authentication and managing account privileges to mitigate this threat.

Threat Overview

o1oo1 is associated with the use of SilabRAT, Hijackloader, and AsmCrypt malware. The reporting indicates techniques inferred from the report include command and scripting interpreter, valid accounts, user execution, and phishing. However, the central CVE exploited remains insufficiently documented.

Attack Chain and Priority Control

The observed techniques suggest a chain of events starting with phishing or other user execution tactics, potentially leading to the use of command and scripting interpreters. The priority technique identified is the use of valid accounts (T1078), which serves as a critical chokepoint in the attack chain. The concrete control to mitigate this 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 specific information available on the hosting providers or ASNs used by the threat actor. 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, 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. - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.5573).
- Operational risk: Low (score 0.276, reaches privilege-escalation).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5303; 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
TA459	0.5303
APT30	0.5

Historical Profile	Behavioural Overlap
TA577	0.4523
Nomadic Octopus	0.4523
Gallmaker	0.4523

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
Hash	3a6adbe0081b2488e0f137496e92591e0c29148154b2d99faadab9cc435b879b
Hash	79f8da9f9fb4ac7c16d9c210f1f6ef418357a3e7bf602b1dd03a490596fa58c5
Hash	fb56e66920c84ef9e51db0ea23144f5755daef97cbff8613b05ab56d0dc9d623
Hash	fbce30a0c852972fdc24f1b6a7c270512a50ef1a7c6c88c88b92a2dcbdfdd023

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 o1oo1 actor could pivot to T1047 Windows Management Instrumentation to maintain access and gather information, as this technique would likely allow them to leverage the existing Windows infrastructure to execute commands and query system information without relying on compromised credentials. This technique in particular may be appealing because it enables the actor to interact with the system in a way that blends in with normal administrative activity, making it potentially harder to detect. To

counter this potential pivot, 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