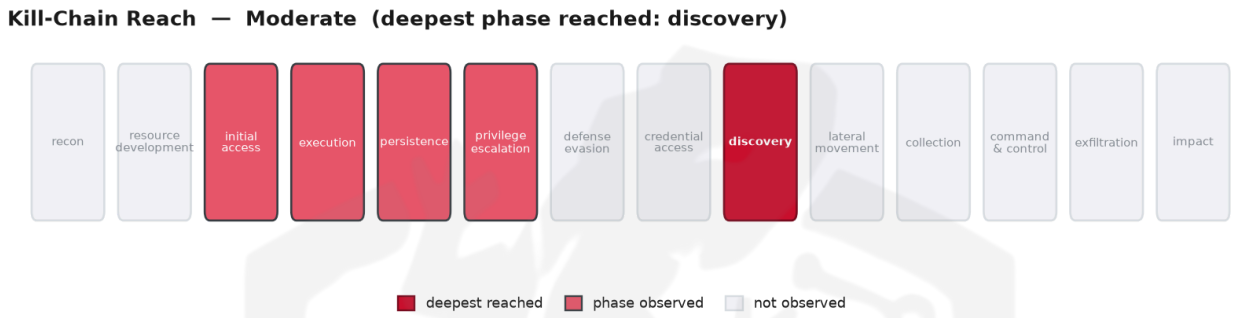
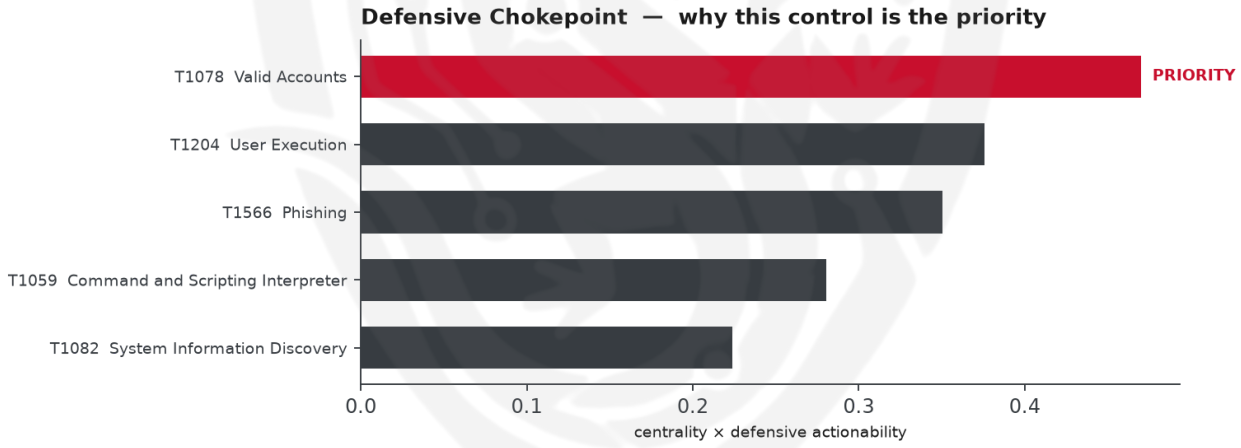
THREAT REPORT: CLICKLOCK STEALER: PASTE ONCE, LOSE EVERYTHING

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 ClickLock Dev, a threat actor involved in the distribution of the ClickLock Stealer malware, among others. The targeted countries and sectors are not specified due to insufficient data. Priority should be given to enforcing multi-factor authentication and managing account privileges to mitigate the threat. The actor's techniques, inferred from the report, suggest a focus on exploiting valid accounts.

Threat Overview

ClickLock Dev is associated with several malware families, including ClickLock Stealer, Atomic Stealer, and others. While the central CVE is not specified, the techniques inferred from the report include

command and scripting interpreter, valid accounts, system information discovery, user execution, and phishing. The victimology of this threat is not clearly defined due to insufficient data.

Attack Chain and Priority Control

The observed techniques, as inferred from the report, form a chain that likely starts with phishing or user execution, leading to the exploitation of valid accounts. The priority technique, as identified by the graph chokepoint, is T1078 Valid Accounts. The concrete control to mitigate this threat is: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

Although specific hosting providers or ASNs are not observed, third-party corroboration from abuse.ch confirms the presence of the AMOS malware family. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, and the highest confidence seen is 0%. This information serves as additional context but does not override the source's assessment.

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 - T1082 System Information Discovery - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.47).
- Operational risk: Moderate (score 0.394, reaches discovery).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4743; 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	0.4743
APT30	0.4472
admin@338	0.4216
Malteiro	0.4104
TA577	0.4045

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: AMOS.
- 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	update-check[.]com	AMOS
Domain	cottonbox[.]co[.]il	
Domain	panalobet[.]ph	
Domain	store[.]grafsynergy[.]com	
URL	hxxp://panalobet[.]ph/wp-content/deng[.]php	
URL	hxxps://cottonbox[.]co[.]il/wp-content/hbd	
URL	hxxps://panalobet[.]ph/wp-content/deng[.]php	
URL	hxxps://panalobet[.]ph/wp-content/themes/twentytwenty/assets/fonts/chromer[.]txt	
URL	hxxps://panalobet[.]ph/wp-content/themes/twentytwenty/assets/images/finderv2[.]jpg	
URL	hxxps://panalobet[.]ph/wp-content/upgrade/zsh[.]txt	
URL	hxxps://panalobet[.]ph/wp-content/upgrade/zsh[.]txt[.]	
URL	hxxps://store[.]grafsynergy[.]com/media/apple[.]png	
URL	hxxps://store[.]grafsynergy[.]com/media/goyim	

Type	Indicator	Context
Hash	0a1fb016bd10bac5455175c79aa4511e5ff1a330	
Hash	2fc970e25570532f9cbe33b7ebfe1f0383a7341a	
Hash	8dda05168ea8610a2449419a47517bc32823d6ec	
Hash	b67aa4f598c0ea625a7409ea7884e10a7bc9c3ff	
Hash	d9617710d4ed8e9b87f6fee0b7014c4101effba0	

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:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 31+ groups that use Valid Accounts, this pairing runs 1.4x above base rate, a disproportionately-coupled move rather than the obvious one.

The ClickLock Dev actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and evade detection, as this technique allows them to execute malicious tasks under the guise of legitimate system maintenance, potentially leveraging the existing valid account credentials they had previously exploited. This technique may be particularly appealing to the actor as it enables them to schedule tasks to run at specific intervals, making it more challenging for defenders to distinguish between legitimate and malicious activity. To counter this potential pivot, the defensive control of alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators should be implemented.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1072 Software Deployment Tools (n=6, lift 2.3)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)

    - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
    - Restrict schtasks/at to administrators; disable the legacy at.exe
    - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File