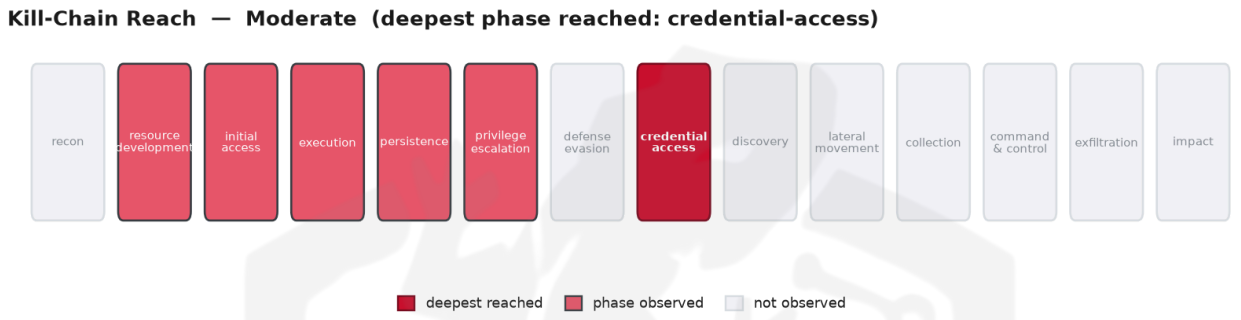
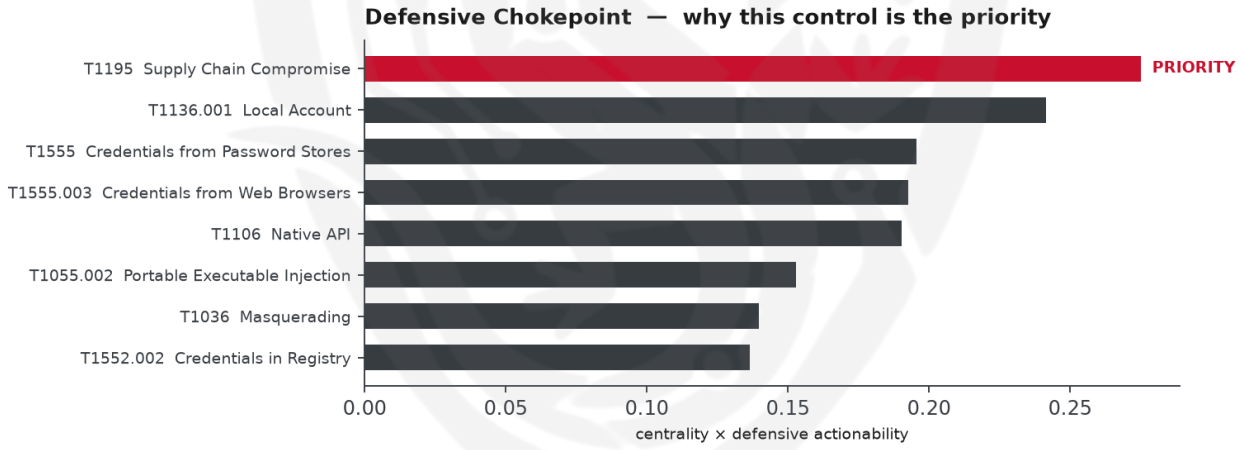
THREAT REPORT: OPERATION ENDGAME DISRUPTS AMADEY AND STEALC MALWARE

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 disrupting Amadey and Stealc malware, among others, with a focus on stealing web session cookies and credentials. The threat actor's targets and motivations are not well understood, but priority should be given to defending against supply chain compromise. The malware families involved include Amadey, Stealc, Lumma Stealer, and Danabot, highlighting the need for vigilance in software supply chain integrity.

Threat Overview

The observed cluster of activity involves the use of various malware families, including Amadey, Stealc, Lumma Stealer, and Danabot, to exploit unknown vulnerabilities and steal sensitive information. The

victimology is not well understood, but the techniques used suggest a focus on credential access and supply chain compromise.

Attack Chain and Priority Control

The attack chain involves a range of techniques, including rundll32, shared modules, and stealing web session cookies, ultimately leading to supply chain compromise. The priority technique is T1195 Supply Chain Compromise, which is the graph chokepoint. To defend against this, the priority control is to Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels.

Infrastructure and Corroboration

The malware families involved have been corroborated by third-party sources, with abuse.ch confirming the presence of Amadey. However, there is no information on the hosting providers or ASNs observed, and AbuseIPDB has not flagged any indicators with high confidence.

Technical Appendix

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

Observed Techniques (ATT&CK, expert-tagged by source)

- T1218.011 Rundll32
- T1129 Shared Modules
- T1539 Steal Web Session Cookie
- T1587.001 Malware
- T1204.002 Malicious File
- T1552.002 Credentials in Registry
- T1218.007 Msiexec
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1608.001 Upload Malware
- T1195 Supply Chain Compromise
- T1555 Credentials from Password Stores
- T1036 Masquerading
- T1555.003 Credentials from Web Browsers
- T1583.004 Server
- T1136.001 Local Account
- T1588.001 Malware
- T1055.002 Portable Executable Injection
- T1552.001 Credentials In Files
- T1480 Execution Guardrails
- T1528 Steal Application Access Token

- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1059.003 Windows Command Shell

Analytical Scores

- Priority technique (graph chokepoint): T1195 Supply Chain Compromise (centrality 0.2973).
- Operational risk: Moderate (score 0.507, reaches credential-access).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4734; 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
TA505	0.4734
LazyScripter	0.4629
Gorgon Group	0.3877
Molerats	0.3719
RedCurl	0.371

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Amadey.
- 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	mi[.]overlapsnowbound[.]com	
Hash	ff8d2afd9d7f0a828592fee34ca55d1a3542f7ed	Amadey

Type	Indicator	Context
Hash	09002d4668a778853e8da5c488c6e421c0628357	
Hash	11a42ef076686cb27ba2c8845301943652a5aadc	
Hash	32d0c3300825b0bb991c4a8f1e6244f0ad2da989	
Hash	38d744543b2051e6f749af171b5ef8d6df8aac7b	
Hash	5f3f99b14243404c7cf57b40bb101244cce394bf	
Hash	87867ad29e621bf9ebf57e1757f75090842458be	
Hash	b4101027bf2f1261402bf6318c6eb016ce249037	
Hash	c0e178d26e1e67985a9c67e649d71d54642e0eed	
Hash	f61e3a643f2417e1a1ab2c83bbdbfc8a7cb96756	

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:** T1195 Supply Chain Compromise (initial-access)
- **Observed here:** T1195 Supply Chain Compromise 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 10+ groups that use Supply Chain Compromise, this pairing runs 2.7x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to using T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially by creating a new scheduled task that blends in with legitimate system activity, which would allow them to continue their objective despite the initial supply chain compromise being blocked. This technique may be particularly appealing as it enables the actor to execute code without needing to maintain a constant connection to the compromised system. To counter this, 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): T1203 Exploitation for Client Execution (n=7, lift 2.6), T1047 Windows Management Instrumentation (n=6, lift 2.2)

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