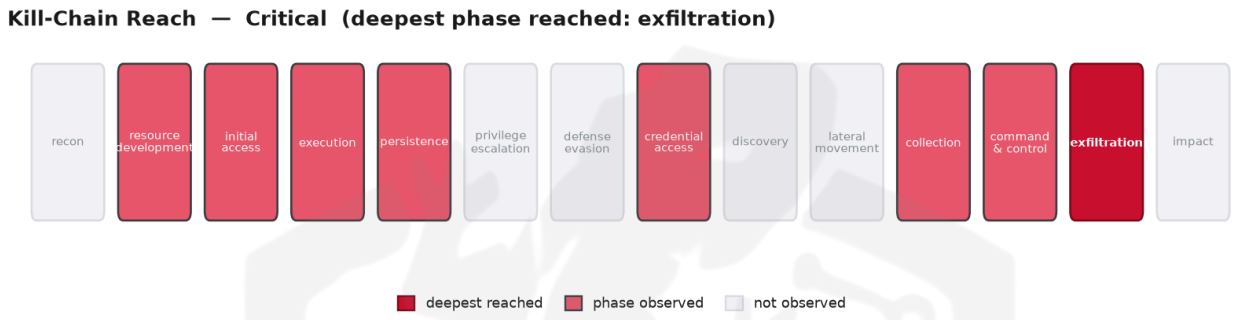
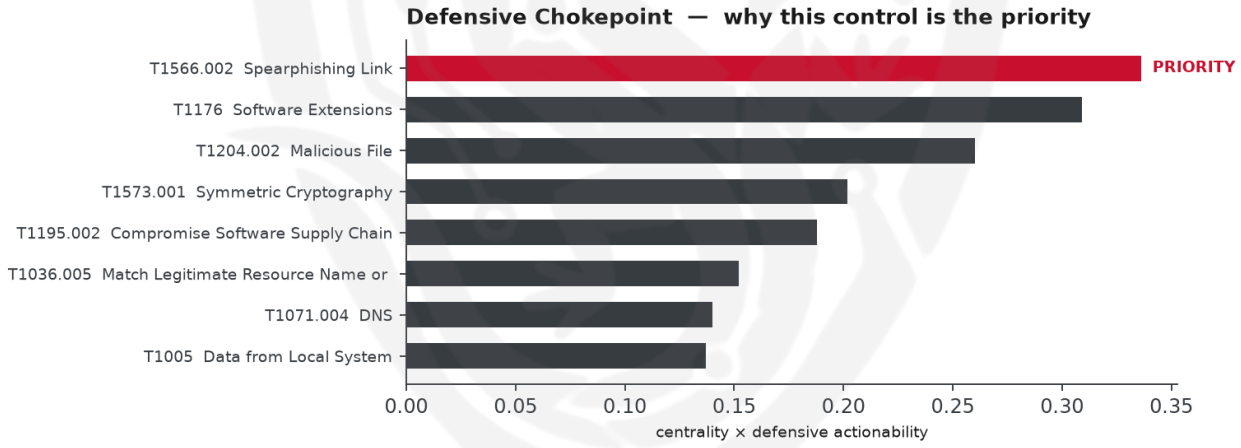
# THREAT REPORT: UNKNOWN_ADVERSARY MODHEADER MALWARE

## 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 associated with the ModHeader malware family, although the threat actor and targeted country remain unknown. The malware's impact is significant, and priority should be given to defensive actions that prevent its spread. The lack of specific information on the central CVE exploited by this malware adds to the complexity of the threat. Enablement of attachment sandboxing and link rewriting is crucial in mitigating this threat.

## Threat Overview

The threat actor, referred to here as the observed cluster of activity, utilizes the ModHeader malware family to compromise systems. The absence of a identified central CVE or specific targeted sectors makes it challenging to pinpoint the exact vulnerability exploited. However, the techniques employed include

stealing web session cookies, using symmetric cryptography, and exfiltrating data over a command and control channel, indicating a sophisticated approach to data theft.

## Attack Chain and Priority Control

The attack chain involves various techniques, including archive via utility, standard encoding, and stealing web session cookies, ultimately leading to data exfiltration. The priority technique identified is T1566.002 Spearphishing Link, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button."

## Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in relation to this malware. 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%. This lack of corroboration highlights the need for continued vigilance and monitoring to understand the infrastructure behind this threat.

---

## Technical Appendix

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

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

- T1560.001 Archive via Utility
- T1132.001 Standard Encoding
- T1539 Steal Web Session Cookie
- T1071.004 DNS
- T1074.001 Local Data Staging
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.002 Spearphishing Link
- T1176 Software Extensions
- T1005 Data from Local System
- T1583.001 Domains
- T1041 Exfiltration Over C2 Channel
- T1195.002 Compromise Software Supply Chain
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

### Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.3361).
- Operational risk: Critical (score 0.968, reaches exfiltration).

### Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4237; 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 |
|---|---|
| WIRTE | 0.4237 |
| Ferocious Kitten | 0.4139 |
| MuddyWater | 0.4046 |
| BRONZE BUTLER | 0.3863 |
| BITTER | 0.3846 |

### 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 | api[.]stanfordstudies[.]com |
| URL | hxxps://modheader[.]com/api/ad-settings |

---

## 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:** T1566.002 Spearphishing Link (initial-access)

- **Observed here:** the threat actor used T1195.002 Compromise Software Supply Chain here as an alternative initial-access technique.
- **Projected pivot:** T1195.002 Compromise Software Supply Chain (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to compromising the software supply chain, as seen in T1195.002, by targeting vendors or third-party dependencies to embed malicious code, which may allow them to maintain access and achieve their objectives despite the block on spearphishing links. This technique could be particularly effective if the actor can compromise a widely used software component, which would likely spread the malicious code to multiple systems. To counter this, the mandated defensive control of verifying software supply chain integrity, such as through signing, SBOM, and monitoring third-party dependencies and update channels, should be implemented.

- **Defensive countermeasure:** Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels.