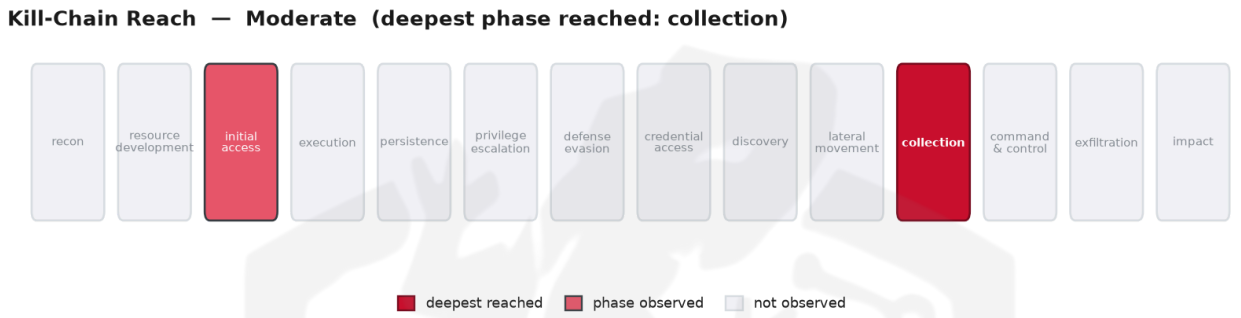
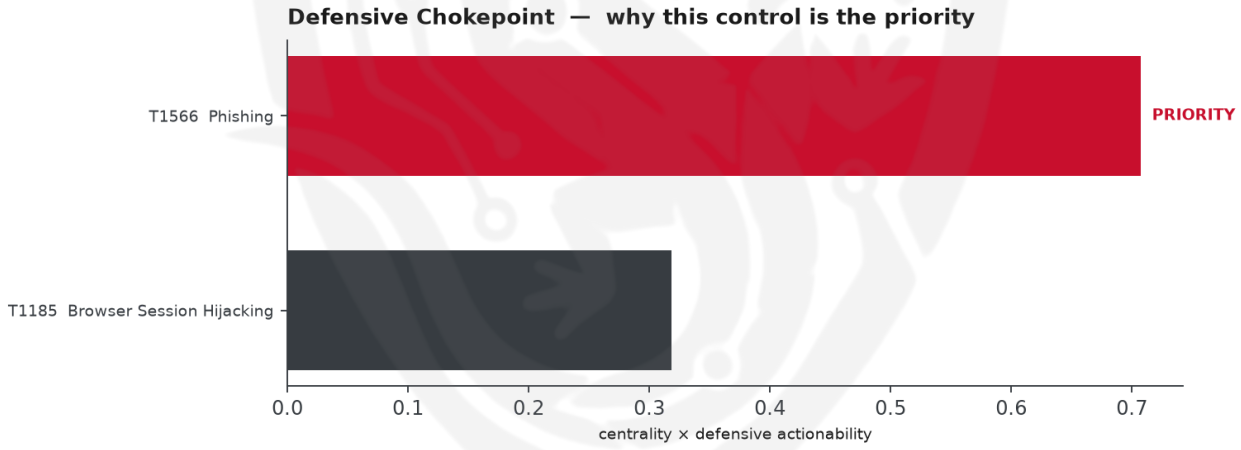
THREAT REPORT: KIRAPAYLOAD'S AITM PHISHING KIT

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 kirapayload, who is utilizing a new AiTM phishing kit that evades URL scanners via Cloaked.gg. The kit is associated with the Blacksite and Tycoon 2FA malware families. Priority should be given to defending against social-engineering delivery methods, as the threat actor is targeting the finance and technology sectors. The observed techniques, inferred from the report, include browser session hijacking and phishing.

Threat Overview

The threat actor, kirapayload, is associated with the Blacksite and Tycoon 2FA malware families. The reporting indicates techniques such as browser session hijacking and phishing are being used. The

victimology suggests that the finance and technology sectors are being targeted, although specific country information is not available.

Attack Chain and Priority Control

The observed techniques, inferred from the report, form a chain that includes browser session hijacking and phishing. The priority technique is T1566 Phishing, which is the graph chokepoint. To mitigate this threat, the priority control is to: Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA.

Infrastructure and Corroboration

There is no observed hosting provider or ASN information available for this threat. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence level of 80% or higher.

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. - T1185 Browser Session Hijacking - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.7071).
- Operational risk: Moderate (score 0.395, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5; 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
AppleJeus	0.5
APT30	0.3536
TA459	0.25
APT12	0.2357
Mofang	0.2357

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	allegro-pl[.]site
Domain	allegro-pl[.]top
Domain	charliesdemons[.]com
Domain	cloaked-demo[.]com
Domain	cloaked[.]gg
Domain	api[.]cloaked[.]gg
Domain	capture[.]cloaked[.]gg
Domain	cdn[.]cloaked[.]gg

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 Phishing (initial-access)
- **Observed here:** T1566 Phishing 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:** T1204 User Execution (execution)
- **Basis:** of the 89+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The kirapayload actor could pivot to T1204 User Execution to maintain their objective by tricking users into executing malicious files, potentially disguised as legitimate documents or applications, which may be downloaded or accessed through compromised websites or email attachments. This technique may be particularly appealing as a follow-up to phishing attempts, as it relies on similar social engineering tactics to deceive users into taking actions that compromise security. To counter this, the mandated defensive control of blocking execution of downloaded HTA/JS/LNK, enforcing mark-of-the-web, disabling Office macros from the internet, and promoting user awareness on lures would likely be effective.

Also plausible (same tactic): T1203 Exploitation for Client Execution (n=38, lift 1.6), T1053 Scheduled Task/Job (n=43, lift 1.3)

Detection and hardening for the pivot (T1204 User Execution)

- **Telemetry:** Endpoint process telemetry; Email/proxy logs
- **Detect:**
  - User double-clicking archive/ISO/LNK contents that spawn interpreters
  - Mark-of-the-Web on delivered files; LOLBIN execution from user temp paths
- **Harden:**
  - Block risky file types; ASR rules; user awareness training
  - Application control to stop execution from user-writable directories
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1017 User Training · DS0009 Process, DS0022 File