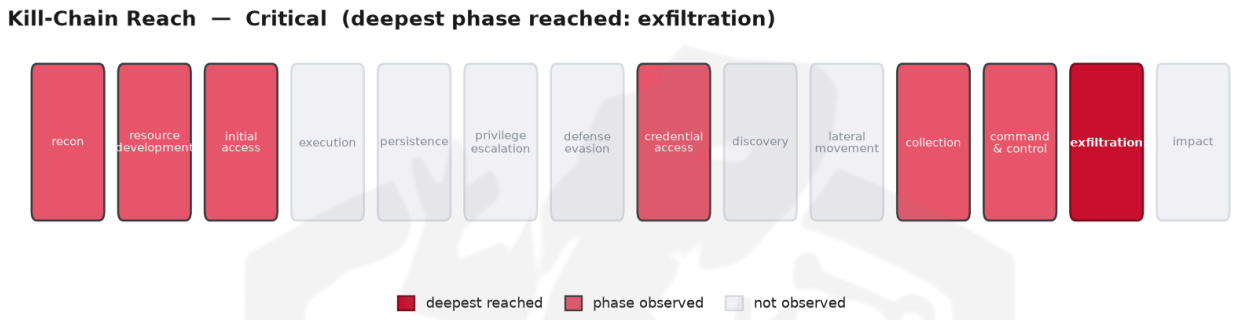
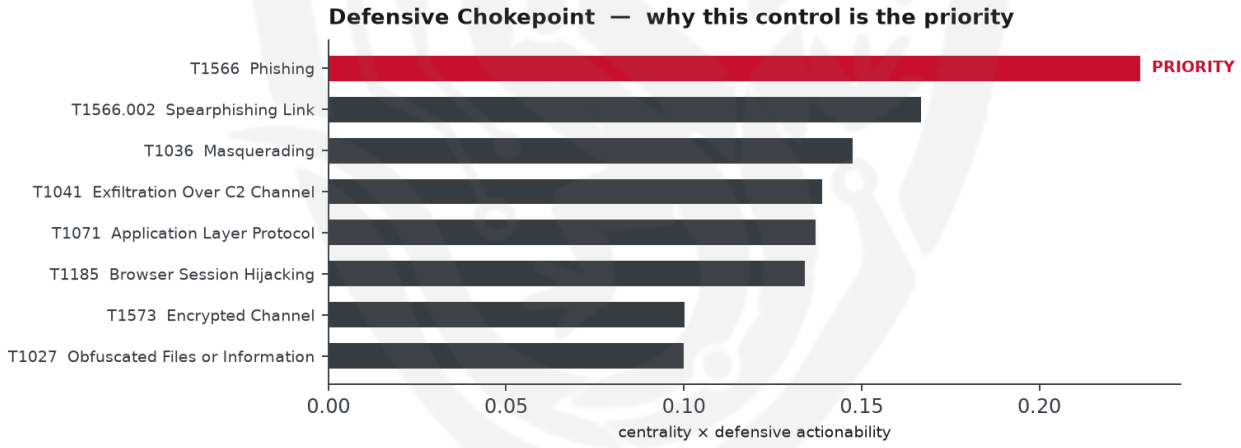
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 observed cluster of activity has been linked to the exploitation of CVE-2024-6387, with the primary technique being phishing. The targeted country and sectors are currently unknown. Priority should be given to patching the vulnerability and implementing additional security measures to prevent further exploitation. The threat actor's use of phishing as a primary technique highlights the importance of user education and reporting suspicious activity.

Threat Overview

The threat actor, whose identity is currently unknown, is exploiting the CVE-2024-6387 vulnerability, utilizing various techniques including phishing, keylogging, and masquerading. The victimology of this

campaign is not well understood due to insufficient data. However, it is clear that the actor is using a range of tactics to gain access to systems and potentially exfiltrate sensitive information.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with the acquisition of infrastructure and moving through various stages, including phishing, keylogging, and exfiltration. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to: Patch CVE-2024-6387 on all affected systems as the top priority, then: 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 currently no corroboration from third-party sources regarding the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, 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, expert-tagged by source)

- T1583 Acquire Infrastructure
- T1056.001 Keylogging
- T1036.005 Match Legitimate Resource Name or Location
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1071 Application Layer Protocol
- T1586.002 Email Accounts
- T1608.001 Upload Malware
- T1583.001 Domains
- T1036 Masquerading
- T1185 Browser Session Hijacking
- T1586 Compromise Accounts
- T1608 Stage Capabilities
- T1583.006 Web Services
- T1041 Exfiltration Over C2 Channel
- T1566 Phishing
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1056 Input Capture

- T1598 Phishing for Information
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2284).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4714; 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	0.4714
BITTER	0.428
APT42	0.4138
LazyScripter	0.3984
RedEcho	0.3858

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	usps[.]xupqnqz[.]one
Domain	gwrpfjx[.]life
Domain	xupqnqz[.]one
Domain	xupqrnn[.]one
URL	hxxp://xupqrnn[.]one/us?__theme_site_ticket=

Type	Indicator
URL	hxxps://usps[.]xupqnqz[.]one/uqjmw
Hash	4fe8bec780537aa223406965415c1f85e83eec1f4e2181cf82e2a7b7516026e6
Hash	8e5546c83d764e1287b55cbe868a45344a6f0afa9782d798d03b2b7cfc53ec38