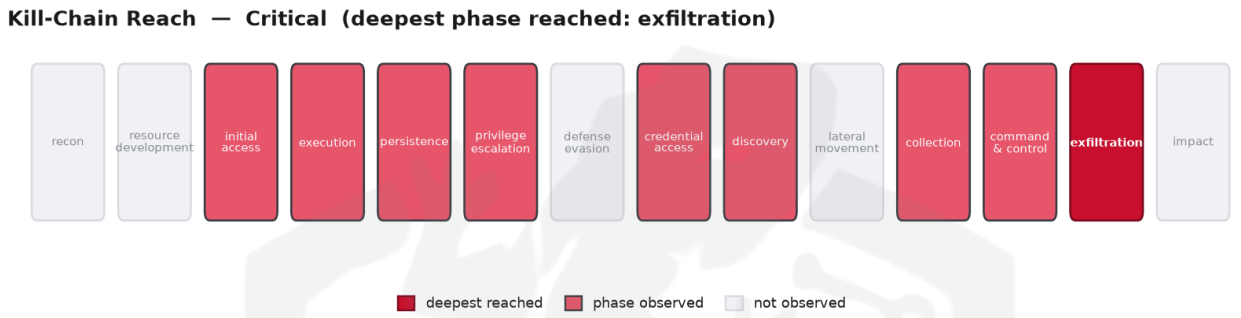
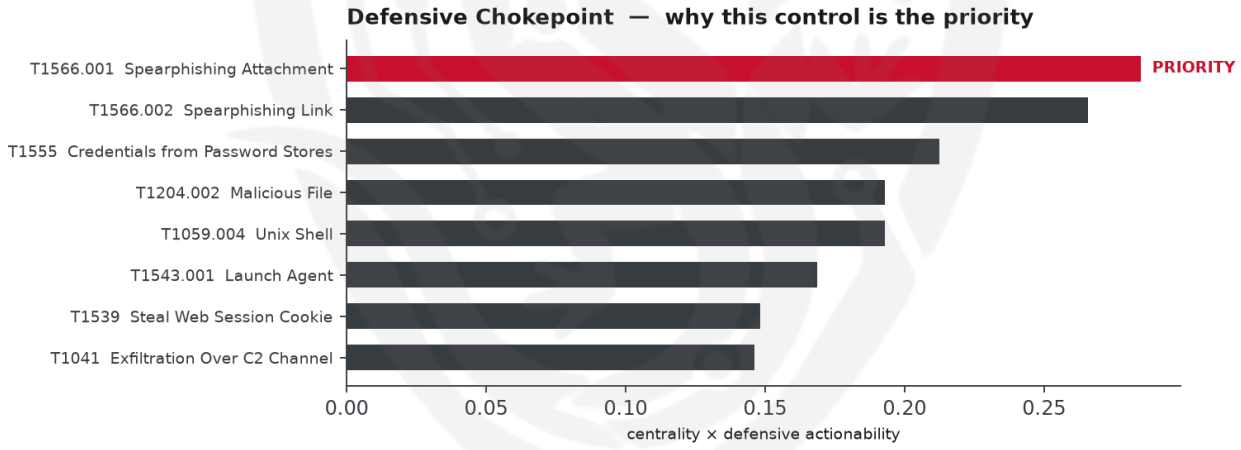
THREAT REPORT: UNKNOWN_ADVERSARY INFOSTEALER CAMPAIGN

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 a series of infostealer malware families, including Remus, ACRStealer, and Vidar, among others. The threat actor is targeting unspecified countries and sectors, with a focus on stealing sensitive information. Priority should be given to defending against spearphishing attacks, particularly those utilizing malicious email attachments. The lack of specific attribution and targeted sectors makes it essential to maintain a high level of vigilance across all systems and networks.

Threat Overview

The threat actor, whose identity is currently unknown, is utilizing a range of malware families to exploit unsuspecting victims. The malware families involved include Remus, ACRStealer, LummaC2, Vidar,

AgentTesla, DarkCloud, and AMOS. While the central vulnerability being exploited is not specified, the techniques used by the threat actor include screen capture, system owner/user discovery, and keylogging, among others.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, with the priority technique being T1566.001 Spearphishing Attachment. This technique serves as a critical chokepoint in the attack chain, allowing the threat actor to gain initial access to victim systems. To mitigate this threat, the priority control is to "Sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button."

Infrastructure and Corroboration

Although the hosting providers and ASNs used by the threat actor are not available, third-party corroboration from abuse.ch confirms the presence of the XWorm malware family. However, according to AbuseIPDB, there are no 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)

- T1113 Screen Capture
- T1033 System Owner/User Discovery
- T1132.001 Standard Encoding
- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1555 Credentials from Password Stores
- T1016 System Network Configuration Discovery
- T1087 Account Discovery
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1543.001 Launch Agent
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow

- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2846).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5011; 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
APT19	0.5011
APT42	0.4411
Windshift	0.4243
FIN4	0.4226
Ajax Security Team	0.4183

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: XWorm.
- 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	apdhlhs3[.]xyz	
Domain	bduwih8[.]pro	
Domain	johncon[.]my	
Hash	d15248555e7a2d9c279d219e6587a74fca9c25720194512a2e4b0757f7a63219	XWorm

Type	Indicator	Context
Hash	02c7d78e6c5816f1df250f995a776aa2	
Hash	03663f2f81da94cd204837e4bde772ff	
Hash	03e99ceede013fe1b50a0e06c1f0a02c	
Hash	042db31ea5443d78aeee714556813a28	XWorm
Hash	04d91c168c7617c38199983858cfbb4e	
Hash	c8c80cde1ae90d6a594980e117977437de97ebb1	XWorm
Hash	dbe028a59ffe936bce9acb56e9c2db93ef6f84fe	
Hash	ac14d191300c2d3aa9f57829b895b7720be1ef3563bace25de731002d52577f7	

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:** T1566.001 Spearphishing Attachment (initial-access)
- **Observed here:** the threat actor used T1566.002 Spearphishing Link here as an alternative initial-access technique.
- **Projected pivot:** T1566.002 Spearphishing Link (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to T1566.002 Spearphishing Link to maintain their campaign momentum by switching from malicious attachments to links that may appear legitimate, potentially deceiving targets into divulging sensitive information or downloading malware. This shift may allow the actor to bypass the recently implemented block on attachments. The defensive control to counter this potential pivot would be to enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Detection and hardening for the pivot (T1566.002 Phishing)

- **Telemetry:** Email security gateway logs; Endpoint (Office child processes); Proxy/DNS
- **Detect:**
  - Office apps (winword/excel) spawning script or LOLBIN child processes
  - Mark-of-the-Web bypass; ISO/IMG/LNK/HTML-smuggling attachments detonating
  - First-contact domains and newly registered domains in mail links
- **Harden:**
  - Attachment sandboxing; block high-risk types (iso, img, lnk, htm) at the gateway

    - Attack-surface-reduction rules for Office child processes; user reporting button
- **MITRE:** M1049 Antivirus/Antimalware, M1031 Network Intrusion Prevention, M1017 User Training, M1021 Restrict Web-Based Content · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic