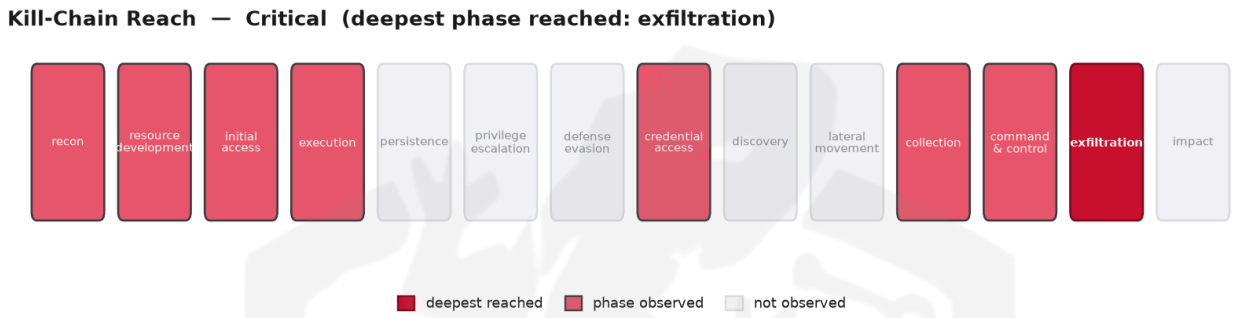
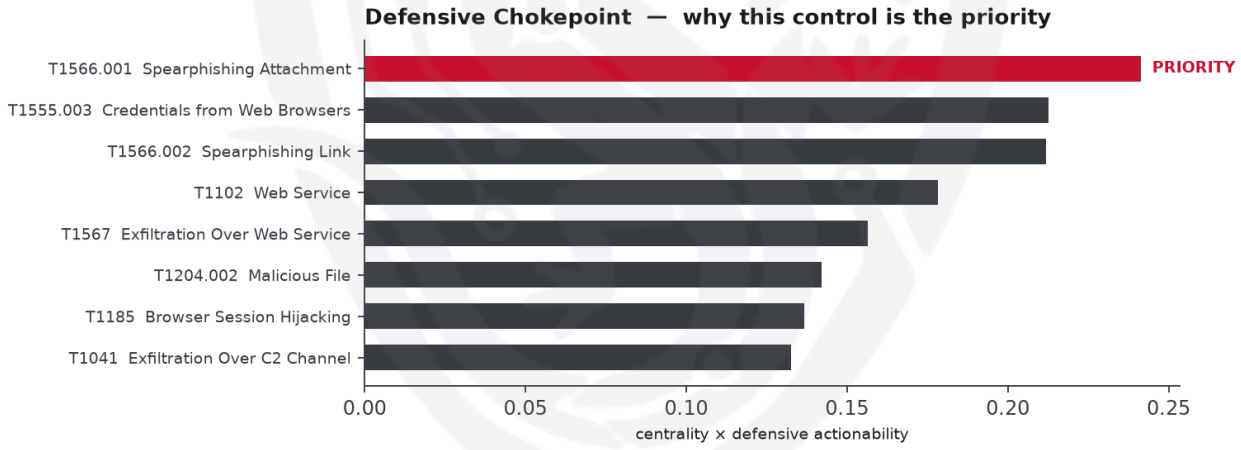
THREAT REPORT: UNKNOWN_ADVERSARY REDLINE C2 CAMPAIGN

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 identified as utilizing the RedLine Stealer malware, among others, to target the manufacturing and transportation sectors. The threat actor's primary technique involves spearphishing attachments, which should be prioritized for defensive action. Priority should be given to sandboxing and detonating email attachments to prevent further compromise. The operational risk band for this threat is considered Critical due to the potential for exfiltration.

Threat Overview

The threat actor, whose identity is insufficient to determine, is utilizing a range of malware families including RedLine Stealer, XLoader, Formbook, Metamorfo, and Casbaneiro. The primary technique

employed by the actor is spearphishing, with a focus on attachments. The targeted sectors are manufacturing and transportation, although the specific country targeted is insufficient to determine.

Attack Chain and Priority Control

The observed techniques employed by the threat actor form a chain that begins with spearphishing and progresses through various stages, including keylogging, email collection, and exfiltration over web services. The priority technique identified is T1566.001 Spearphishing Attachment, which serves as a chokepoint in the attack chain. 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

The malicious infrastructure associated with this campaign is hosted on providers including TheHost LLC, Des Equity LLC, Leaseweb Netherlands B.V., and Athena Cloud. Abuse.ch has corroborated the presence of RedLine Stealer malware, while AbuseIPDB has flagged indicators with a confidence level of up to 1%. These corrobations provide additional context to the threat, but do not override the primary source assessment.

Technical Appendix

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

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

- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1114 Email Collection
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1586.002 Email Accounts
- T1567 Exfiltration Over Web Service
- T1583.001 Domains
- T1185 Browser Session Hijacking
- T1555.003 Credentials from Web Browsers
- T1102 Web Service
- T1583.006 Web Services
- T1598.002 Spearphishing Attachment
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1132 Data Encoding

- T1071.001 Web Protocols
- T1204.001 Malicious Link

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2413).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.491; 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
IndigoZebra	0.491
Ajax Security Team	0.4781
FIN4	0.4648
Mofang	0.441
WIRTE	0.4374

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 1%.
- Malware families corroborated by abuse.ch: RedLine Stealer.
- 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
IP	194[.]156[.]79[.]122	AbuseIPDB 1% (NL) · RedLine Stealer · AS399471 Des Equity LLC
IP	85[.]17[.]40[.]98	AbuseIPDB 0% (NL) · AS60781 Leaseweb Netherlands B.V.
IP	185[.]252[.]24[.]52	AbuseIPDB 0% (UA) · AS56485 TheHost LLC

Type	Indicator	Context
IP	176[.]114[.]8[.]101	AbuseIPDB 0% (UA) · AS56485 TheHost LLC
IP	176[.]114[.]8[.]90	AbuseIPDB 0% (UA) · AS56485 TheHost LLC
IP	185[.]252[.]24[.]74	AbuseIPDB 0% (UA) · AS56485 TheHost LLC
IP	185[.]252[.]24[.]78	AbuseIPDB 0% (UA) · AS56485 TheHost LLC
IP	91[.]108[.]82[.]101	AbuseIPDB 0% (UA) · AS56485 TheHost LLC
IP	91[.]108[.]82[.]73	AbuseIPDB 0% (UA) · AS56485 TheHost LLC
IP	23[.]164[.]48[.]21	AbuseIPDB 0% (CA) · AS398764 Athena Cloud
Domain	acasiallc[.]shop	
Domain	amdocsllc[.]shop	malware_download
Domain	ansysllc[.]shop	
Domain	cimentosservices[.]online	
Domain	epsilongroup[.]online	
Domain	softinsallc[.]online	
Domain	taicom[.]top	
Domain	krysegroupllc[.]online	
Domain	shengan-light[.]com[.]tw	
URL	hxxp://194[.]156[.]79[.]122:55615	
URL	hxxp://85[.]17[.]40[.]98:55615	
URL	hxxp://23[.]164[.]48[.]21:55615	

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 threat actor could pivot to T1566.002 Spearphishing Link to maintain their campaign momentum by sending emails with malicious links instead of attachments, which may allow them to bypass the initial block. This shift would likely involve crafting convincing emails that entice victims to click on the links, potentially leading to the same malicious outcomes as before. The defensive control to counter this potential pivot is 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