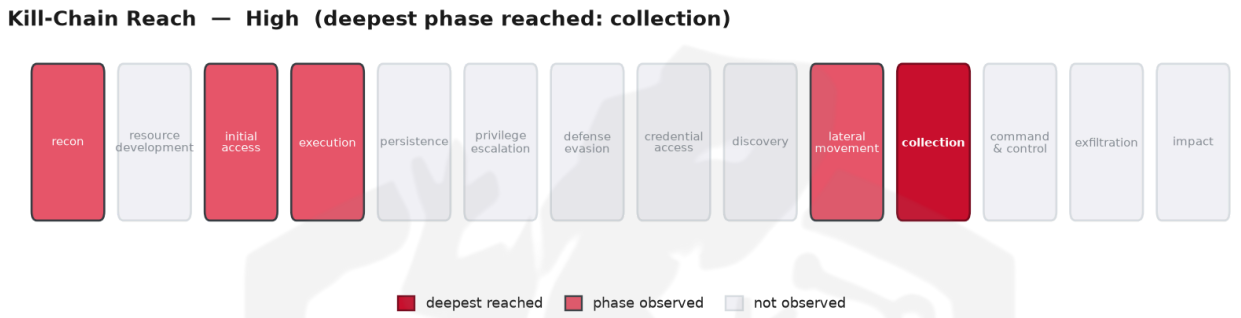
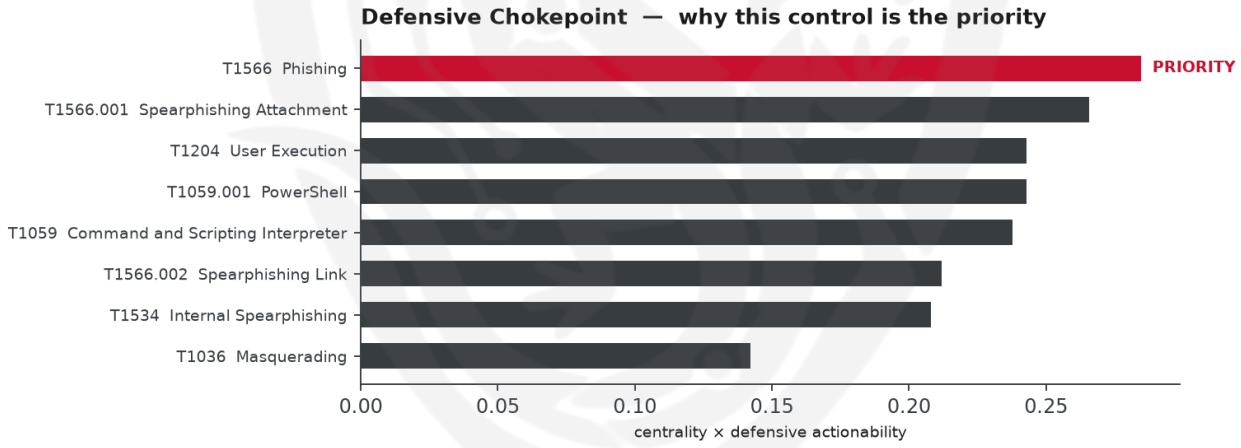
THREAT REPORT: UNATTRIBUTED PHISHING CAMPAIGN TARGETS MULTIPLE SECTORS

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 targeting various sectors, including Retail, Technology, Finance, and others, through phishing techniques. The threat actor's identity and specific malware families used are currently unknown. Priority should be given to defensive actions that mitigate phishing attacks. Enablement of attachment sandboxing and link rewriting are crucial in preventing these types of attacks.

Threat Overview

The threat actor, whose identity is currently unknown, has been observed using various techniques to target multiple sectors. The techniques used include email collection, masquerading, and phishing, among others. The victimology suggests a broad range of targets across different industries.

Attack Chain and Priority Control

The observed techniques form a chain that starts with email collection and masquerading, leading to phishing and potential execution of malicious files. The priority technique identified is T1566 Phishing, which serves as a chokepoint in the attack chain. To mitigate this, 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 this campaign. 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.

Technical Appendix

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

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

- T1114 Email Collection
- T1036.005 Match Legitimate Resource Name or Location
- T1564 Hide Artifacts
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1036 Masquerading
- T1059 Command and Scripting Interpreter
- T1204 User Execution
- T1059.001 PowerShell
- T1534 Internal Spearphishing
- T1566 Phishing
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window
- T1598 Phishing for Information
- T1059.003 Windows Command Shell
- T1213 Data from Information Repositories
- T1204.001 Malicious Link
- T1566.003 Spearphishing via Service

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2943).

- Operational risk: High (score 0.604, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6742; 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
Nomadic Octopus	0.6742
Machete	0.5423
Mofang	0.5217
DarkHydrus	0.5164
Transparent Tribe	0.5129

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	x2mails[.]com
Domain	acceptable-use-policy-calendly[.]de
Domain	cocinternal[.]com
Domain	compliance-protectionoutlook[.]de
Domain	na[.]businesshellosign[.]de

Type	Indicator
Domain	gadellinet[.]com
Domain	harteprn[.]com
Domain	9i6pokerdepot[.]com
Domain	ecajovna[.]sk
Domain	ilyff[.]com
Domain	j-gmails[.]com
Domain	cocinternal[.]cm
Domain	t90141296286[.]p[.]clickup-attachments[.]com
URL	hxxps://t90141296286[.]p[.]clickup-attachments[.]com/t90141296286/fb39c3a9-3161-40ad-847b-0683e0409d6f/Financial_report[.]bat
Hash	11420d6d693bf8b19195e6b98fedd03b9bcbc770b6988bc64cb788bfabe1a49d
Hash	5db1ecbbb2c90c51d81bda138d4300b90ea5eb2885cce1bd921d692214aecbc6
Hash	b5a3346082ac566b4494e6175f1cd9873b64abe6c902db49bd4e8088876c9ead
Hash	467f4c566f8a49fa9bc5d36f50f89568
Hash	99ce8ecb93b9a43c5697bfa9cbd13b7b
Hash	7d509d135292020a317b0f7a2f444b665396e891
Hash	f5d0ee4f6eb348d10ccaa4f24cae392782b9bfa3

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:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, which may be exposed due to unpatched or outdated versions, thereby allowing them to execute malicious code on the client-side. This technique may be particularly appealing as a follow-up to phishing attempts, as it can be used to exploit the trust gained through social engineering. To counter this potential pivot, the mandated defensive control of patching client applications, enabling exploit mitigations such as ASLR, DEP, and CFG, and implementing application isolation would likely be effective.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=43, lift 1.3), T1106 Native API (n=18, lift 1.6)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log