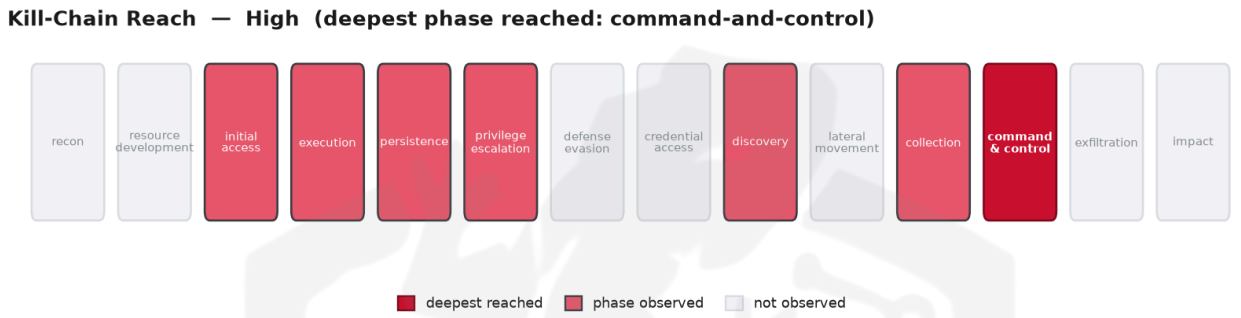
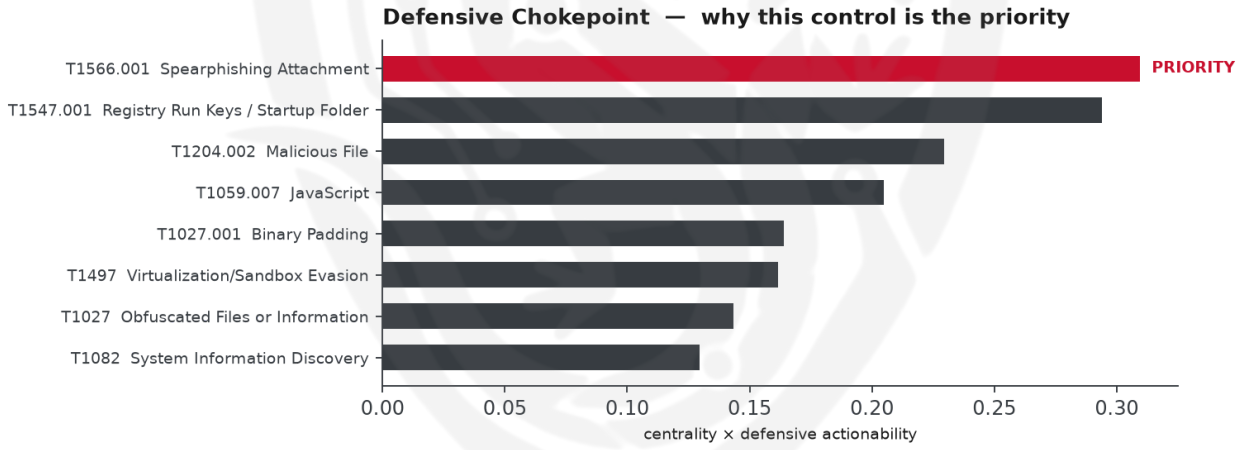
THREAT REPORT: UNKNOWN_ADVERSARY PORTUGAL-FOCUSED PHISHING CAMPAIGN

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 delivering multistage malware to targets in Portugal, primarily in the finance sector, through a phishing campaign. The malware families involved are Lampion and ChePro. Priority should be given to defensive actions that focus on email attachments and executable contents. The threat actor's use of spearphishing attachments as the primary technique poses a significant risk.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, is utilizing the Lampion and ChePro malware families to target organizations in Portugal, specifically those in the finance sector. The absence of a central CVE indicates that the campaign may rely on various vulnerabilities or techniques to achieve

its goals. The actor's tactics include a range of techniques aimed at system discovery, capture, and evasion.

Attack Chain and Priority Control

The attack chain involves multiple techniques, including scheduled tasks, screen capture, system owner/user discovery, and others, ultimately leading to the delivery of malware. The priority technique identified is T1566.001 Spearphishing Attachment, which serves as the initial vector for the campaign. 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

There is currently no information available on the hosting providers or ASNs used by the threat actor, as indicated by the lack of observed hosting providers or ASNs. 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, 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)

- T1053.005 Scheduled Task
- T1113 Screen Capture
- T1033 System Owner/User Discovery
- T1218.011 Rundll32
- T1059.007 JavaScript
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1027.001 Binary Padding
- T1497 Virtualization/Sandbox Evasion
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1012 Query Registry
- T1518.001 Security Software Discovery
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.3096).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6532; 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
Windshift	0.6532
Rancor	0.6
Molerats	0.56
Sidewinder	0.5555
Confucius	0.5292

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	auto-contabilistica[.]com
Domain	autoridade-contabilistica[.]org
Domain	autoridade-financeira[.]com
Domain	fat-contabislitaca[.]com
URL	hxxps://fat-contabislitaca[.]com/js/1898[.]php
Hash	036c8f32012abdcb9a389ae9c284da89505e830bca74eb1aa9ea3794b067aab6
Hash	050e84d134a32ed7c4885a9d57ce37f8ae5f910960b67e2156941961bd5781ba

Type	Indicator
Hash	1541c23f34eb05dfcbede3830741427681d719cee1dfd397a2c04110e0fa81b2
Hash	1bd347ce5deee3d783a038e2d2d224bc30cc074e0471a3897c5409ce99816dc9
Hash	643c0093baec45952a46b0210f7a6f8fb26883b396b66f1cb609c5b55e6dae1e
Hash	7ad89fb0a4a5449a381b8f540238193019673adc7cfb1c008dcd14a745891551
Hash	87efeada5fe39a94cefc6151fd84af223d0e0e2b070daec606274481ed87b87b
Hash	ab46f7c4d3f717bb1e61d2f236917976d2a85be6958ae099fee79ea6e9031e37
Hash	b1c101bd1ba134ffbea61f9fac2b7c8fbd13ca113a37944abdc131ef86da92ac
Hash	c6618bb692fb3f5d7959f8db1fedaaac5e8a36fb901397a008aa2b88874448fd
Hash	d25d32478ae67403484a309591b6409224d26ca3d094c5ccd8428ebef7efcfd1
Hash	fe769fd85a7440751e1508614c8d9ef0de00bece803329bf3318ff863a146216

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:** T1566.001 Spearphishing Attachment was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** 27 of 170 documented groups that use Spearphishing Attachment also use Drive-by Compromise (conditional 0.28, lift 1.5, i.e. ~1.5x base rate). Strongest same-tactic neighbour.

The actor could pivot to T1189 Drive-by Compromise by exploiting vulnerabilities in software or plugins to compromise a user's system, potentially achieving their objective if the user visits a malicious website. This technique may be used in conjunction with social engineering tactics to increase the likelihood of a successful compromise. The defensive control to counter this potential pivot would be to enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.

Also plausible (same tactic): T1195 Supply Chain Compromise (n=9, lift 1.4), T1199 Trusted Relationship (n=9, lift 1.3)

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.