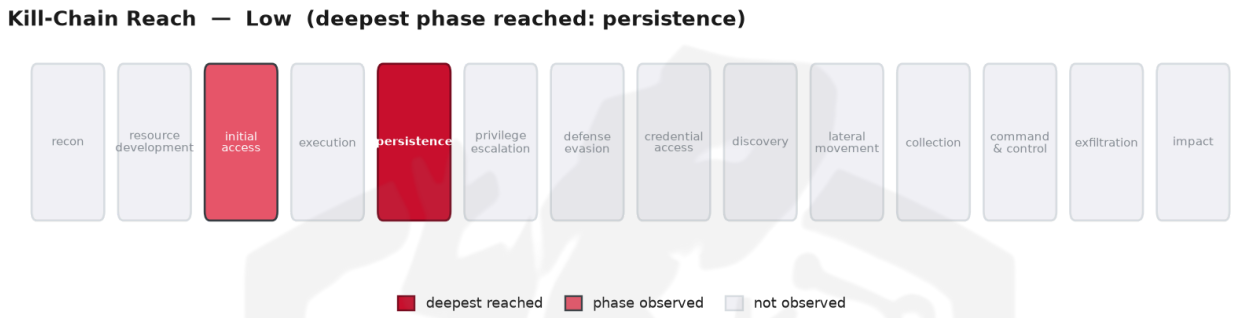
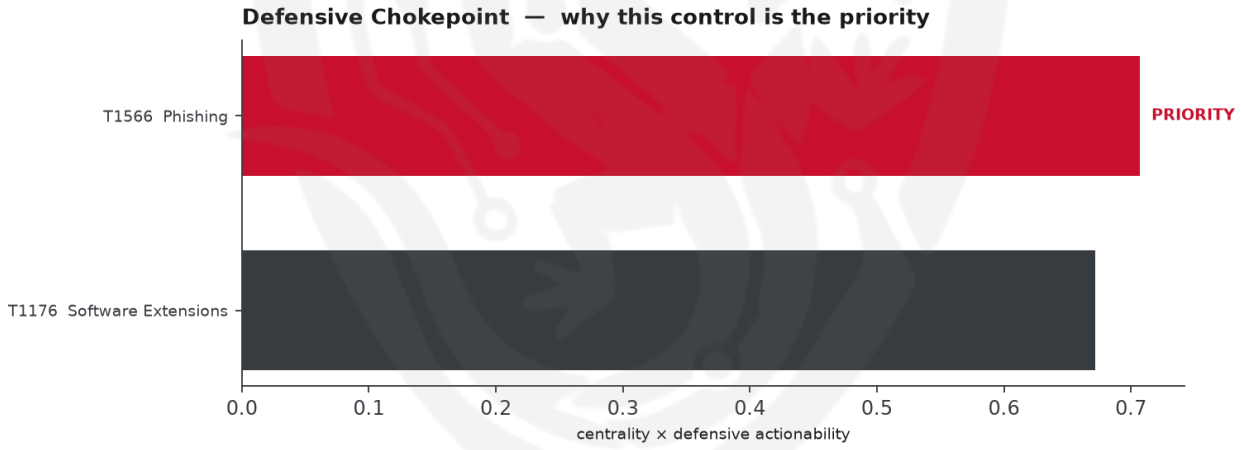
THREAT REPORT: UNATTRIBUTED PHISHING CAMPAIGN TARGETING IRELAND

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 Ireland, with a focus on phishing techniques to gain initial access. The priority defensive action should be taken to prevent phishing attacks, as they pose a significant threat to the targeted organizations. Priority should be given to enabling attachment sandboxing and link rewriting to mitigate these threats. The threat actor's identity and malware families used remain unknown.

Threat Overview

The threat actor, whose identity is unknown, has been using phishing techniques, specifically T1566 Phishing, to target organizations in Ireland. The central vulnerability exploited and the malware families

used are insufficient to determine at this time. The victimology suggests that the threat actor is targeting Irish organizations, but the specific sectors affected are unknown.

Attack Chain and Priority Control

The observed techniques used by the threat actor include T1176 Software Extensions and T1566 Phishing, with T1566 Phishing being the priority technique. The priority control to mitigate this threat 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

The malicious infrastructure associated with this campaign is hosted on Amazon.com Inc. However, there are no corroborated malware families from abuse.ch, and no indicators have been flagged with an 80% or higher confidence level by AbuseIPDB, 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)

- T1176 Software Extensions
- T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.7071).
- Operational risk: Low (score 0.202, reaches persistence).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5; 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
AppleJeus	0.5
APT30	0.3536

Historical Profile	Behavioural Overlap
TA459	0.25
APT12	0.2357
Mofang	0.2357

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	Context
IP	34[.]244[.]249[.]157	AbuseIPDB 0% (IE) · AS16509 Amazon.com Inc.
Domain	anpost[.]ie-sci[.]help	
Domain	service-charge[.]help	

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 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:** T1204 User Execution (execution)
- **Basis:** of the 89+ 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 T1204 User Execution to maintain their objective by tricking users into executing malicious files, which may be disguised as legitimate documents or applications, potentially exploiting the trust users have in files downloaded from the internet. This technique is particularly concerning in this scenario because it could be used in conjunction with social engineering tactics to convince users to execute malicious code, which would likely bypass the phishing block. The defensive control to counter this would be to block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures.

Also plausible (same tactic): T1203 Exploitation for Client Execution (n=38, lift 1.6), T1053 Scheduled Task/Job (n=43, lift 1.3)

Detection and hardening for the pivot (T1204 User Execution)

- **Telemetry:** Endpoint process telemetry; Email/proxy logs
- **Detect:**
  - User double-clicking archive/ISO/LNK contents that spawn interpreters
  - Mark-of-the-Web on delivered files; LOLBIN execution from user temp paths
- **Harden:**
  - Block risky file types; ASR rules; user awareness training
  - Application control to stop execution from user-writable directories
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1017 User Training · DS0009 Process, DS0022 File