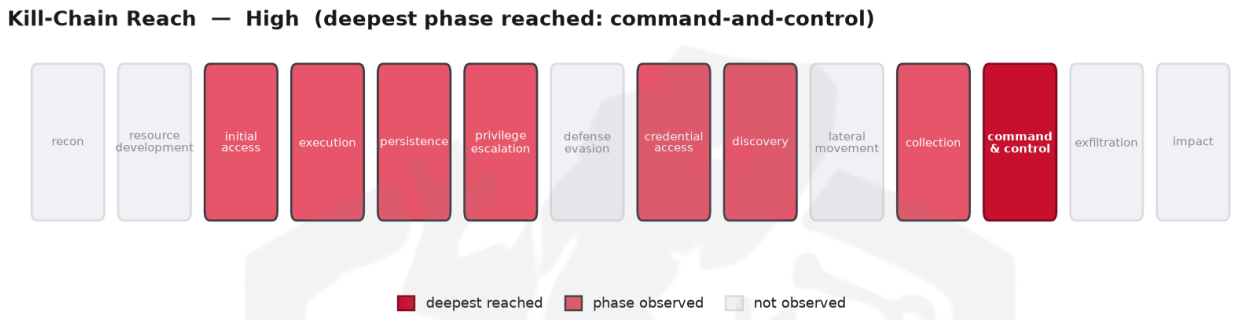
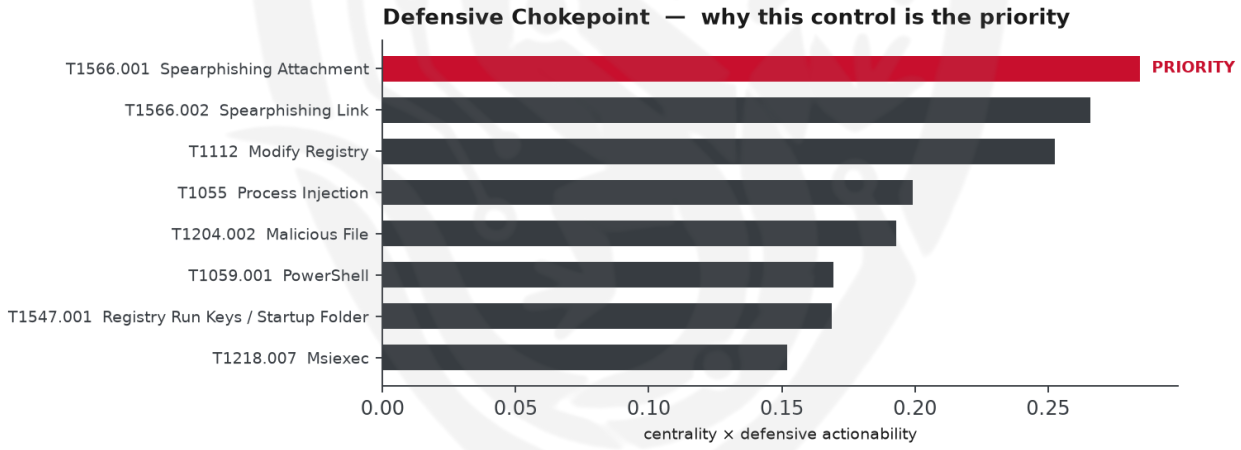
THREAT REPORT: UNKNOWN_ADVERSARY PHISHING CAMPAIGN

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 identified as a sophisticated phishing campaign, leveraging various techniques to compromise targets. The campaign's evolution and tactics suggest a high level of operational risk, warranting priority defensive action. The primary concern is the initial infection vector, which requires immediate attention to prevent further compromise. Priority should be given to safeguarding against email-borne threats.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, employs a range of techniques to achieve their objectives. While specific malware families and exploited vulnerabilities are not identified, the

campaign involves multiple tactics, including scheduled tasks, archive utilities, and encoding schemes. The victimology and targeted sectors are also not specified, adding to the complexity of this threat.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, archive utilities, and encoding schemes, ultimately leading to the execution of malicious code. The priority technique identified is T1566.001 Spearphishing Attachment, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended 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 no specific information available on the hosting providers or ASNs observed in relation to 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, 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
- T1560.001 Archive via Utility
- T1132.001 Standard Encoding
- T1056.001 Keylogging
- T1071.004 DNS
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1553.002 Code Signing
- T1082 System Information Discovery
- T1218.007 Msiexec
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1497 Virtualization/Sandbox Evasion
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window

- T1204.001 Malicious Link

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2846).
- 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 0.6364; 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
Molerats	0.6364
APT19	0.5625
Gallmaker	0.4797
Gorgon Group	0.4792
Machete	0.4716

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	italy-news[.]info
Domain	lootrioya[.]info
Domain	document-auth[.]icu
Hash	7b7981c99d59595fe15377df84695bb72ce0b85560a3935f930657b2d162e5ef
Hash	adcd15f3d6b87f84d106ea426fa824fd20c9d64f6d199ce92580884290785f30

Type	Indicator
Hash	d7d2f0ee187549f3f4a114d716be12521fbf62d6d26e2ac23d2a32d521d08fd8
Hash	79e205576bdad2cce593ae850b0c9e31
Hash	e5989c374fa9cb1bc53b202032257a3c
Hash	5442dea013b109ac4d0cdc52248b758a6cb9684c
Hash	e46d05b8aa8f1b1a5e81da2ebe2bf8e94cbe85fe
Hash	7596699747d2b284df77d2c83714aa00
Hash	5cf01e24f6bafa64815d1bd2f3323ea091d504cc

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 evading initial defenses. This shift may allow them to continue targeting users with phishing attempts, adapting their tactics to bypass the initial block. The defensive control to counter this 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