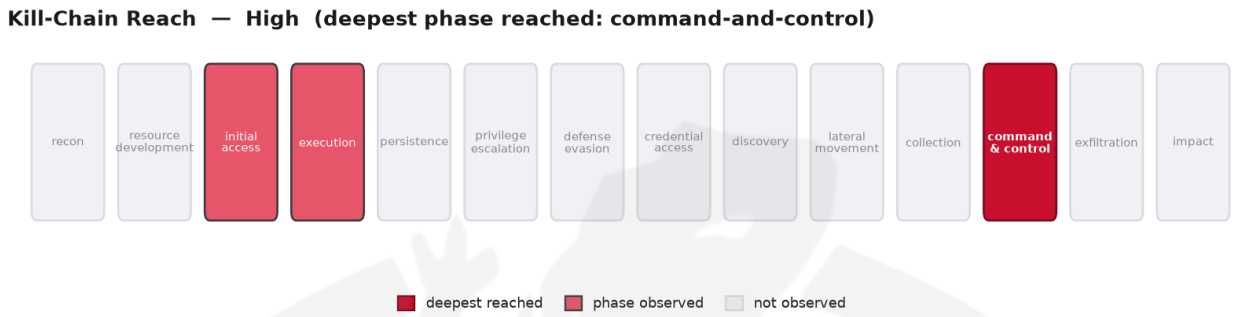
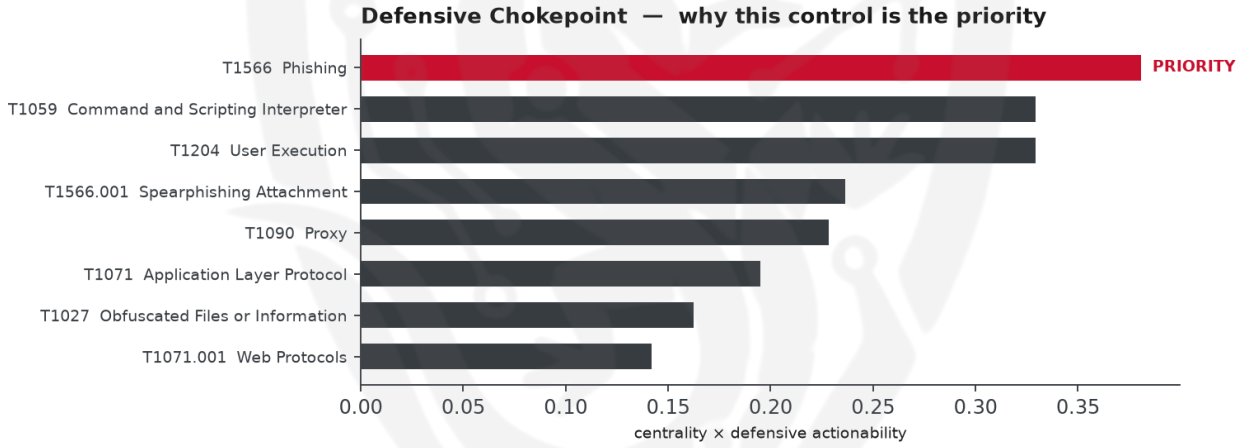
THREAT REPORT: RAZOR TIGER

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 source attributes this activity to RAZOR TIGER. The threat actor has been observed using a lure document, No.9374.docx, to initiate the attack. Priority should be given to defensive actions that mitigate the threat, particularly focusing on phishing techniques. The observed activity is considered high risk due to its potential to reach command-and-control levels.

Threat Overview

The threat actor, attributed to RAZOR TIGER by the source, utilizes various techniques, including malicious files and spearphishing attachments, to target victims. The central vulnerability and targeted sectors are not specified due to insufficient data. However, the techniques employed by the actor include application layer protocol, proxy, command and scripting interpreter, and others, indicating a complex attack chain.

Attack Chain and Priority Control

The attack chain involves multiple techniques, starting with the use of malicious files and spearphishing attachments, followed by the exploitation of application layer protocols and the use of proxies. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended 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 observed hosting provider or ASN associated with the malicious infrastructure. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB 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)

- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1071 Application Layer Protocol
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1204 User Execution
- T1566 Phishing
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.3807).
- Operational risk: High (score 0.594, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6325; 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
APT30	0.6325
Rancor	0.6325
TA551	0.5934
Windshift	0.5809
Nomadic Octopus	0.5721

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
Hash	64f2681ad0940e6c2c9c76e6834117bf

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:** RAZOR TIGER used T1566.001 Spearphishing Attachment here as an alternative initial-access technique.
- **Projected pivot:** T1566.001 Spearphishing Attachment (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

RAZOR TIGER could pivot to using T1566.001 Spearphishing Attachment to keep their objective after the block, as this technique may allow them to evade initial defenses by targeting specific individuals with tailored attachments. This approach would likely involve crafting attachments that appear legitimate but contain malicious content, which could be sent to key personnel in an attempt to gain a foothold. The defensive control to counter this would be to implement a system that includes sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button.

Detection and hardening for the pivot (T1566.001 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