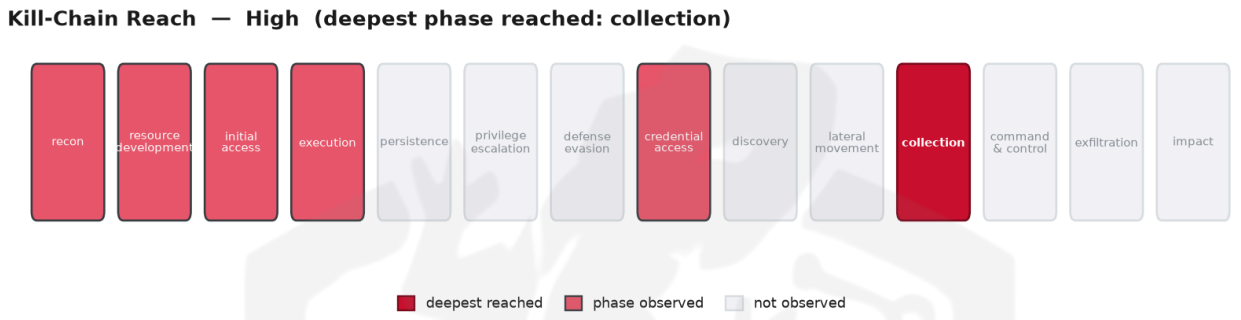
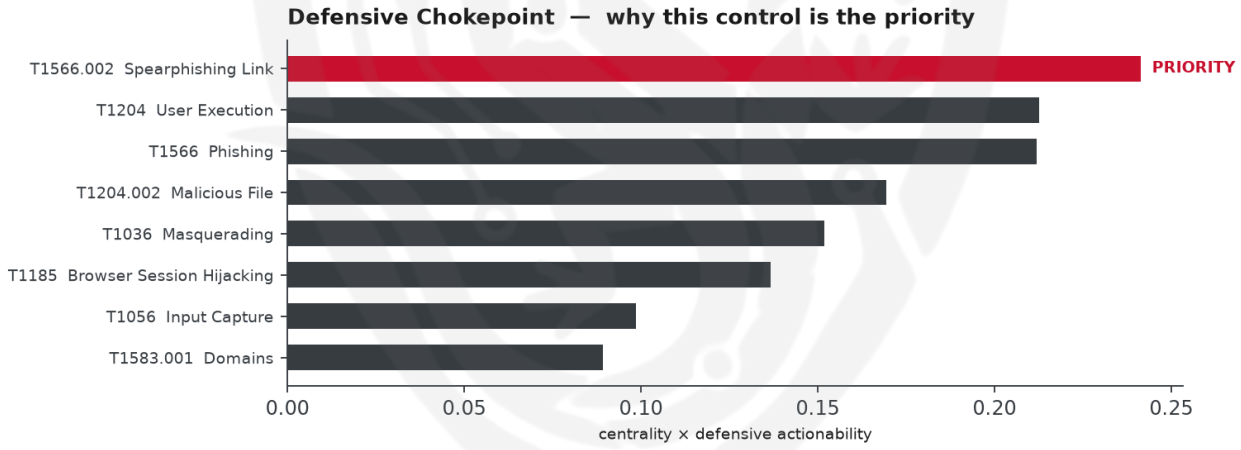
THREAT REPORT: UNKNOWN_ADVERSARY BRANDED GAMBLING CAMPAIGN

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 is targeting individuals in Canada, Germany, Spain, and the United Kingdom, primarily in the finance, retail, and media sectors. The threat actor is exploiting trusted brand names to drive casino traffic, and priority should be given to defending against spearphishing attacks. The campaign's impact is considered high risk, reaching the 'collection' stage of operational risk. Defensive measures should focus on mitigating the effects of phishing and malicious file uploads.

Threat Overview

The threat actor, whose identity is unknown, is engaging in a campaign that involves exploiting trusted brand names to drive traffic to casino websites. The malware families and central CVE used in this

campaign are not specified. The targeted countries include Canada, Germany, Spain, and the United Kingdom, with the finance, retail, and media sectors being primarily affected.

Attack Chain and Priority Control

The observed techniques in this campaign form a chain that includes acquiring infrastructure, stealing web session cookies, searching victim-owned websites, and uploading malware. The priority technique in this chain is T1566.002 Spearphishing Link, which is the graph chokepoint. To mitigate this threat, 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 available information on the hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher. The highest AbuseIPDB confidence seen is 0%, indicating a lack of corroboration from these third-party sources.

Technical Appendix

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

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

- T1583 Acquire Infrastructure
- T1539 Steal Web Session Cookie
- T1594 Search Victim-Owned Websites
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1608.001 Upload Malware
- T1583.001 Domains
- T1036 Masquerading
- T1185 Browser Session Hijacking
- T1586 Compromise Accounts
- T1583.006 Web Services
- T1204 User Execution
- T1588.002 Tool
- T1566 Phishing
- T1585.001 Social Media Accounts
- T1056 Input Capture
- T1585 Establish Accounts
- T1566.003 Spearphishing via Service

Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.2413).
- Operational risk: High (score 0.604, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5658; 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
Ferocious Kitten	0.5658
Star Blizzard	0.5618
IndigoZebra	0.5417
EXOTIC LILY	0.5335
CURIUM	0.4259

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	topstatus[.]site
Domain	rewardsmonzo[.]website
Domain	optimismphantasm[.]shop
Domain	revvo-online[.]website
Domain	ridereuphoric[.]shop
Domain	seekerlucid[.]shop

Type	Indicator
Domain	345rodeoslot[.]com
Domain	87roulettino12[.]com
Domain	blinbd[.]com
Domain	lemniscal[.]live
Domain	monzoslots[.]life
Domain	seekerlucis[.]shop
Domain	spinlynx36[.]com
Domain	tesscogames[.]com

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:** T1566.002 Spearphishing Link (initial-access)
- **Observed here:** the threat actor used T1566 Phishing here as an alternative initial-access technique.
- **Projected pivot:** T1566 Phishing (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to using T1566 Phishing to keep their objective after the block, potentially by using alternative phishing tactics such as spearphishing via email attachments or other vectors, which may allow them to bypass the initial block. This could involve using convincing emails or messages that trick users into divulging sensitive information or performing certain actions. The defensive countermeasure would likely involve 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 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