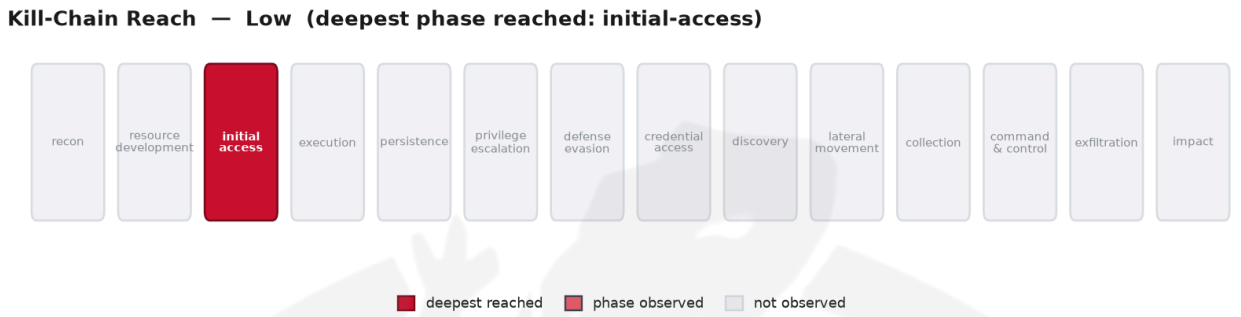
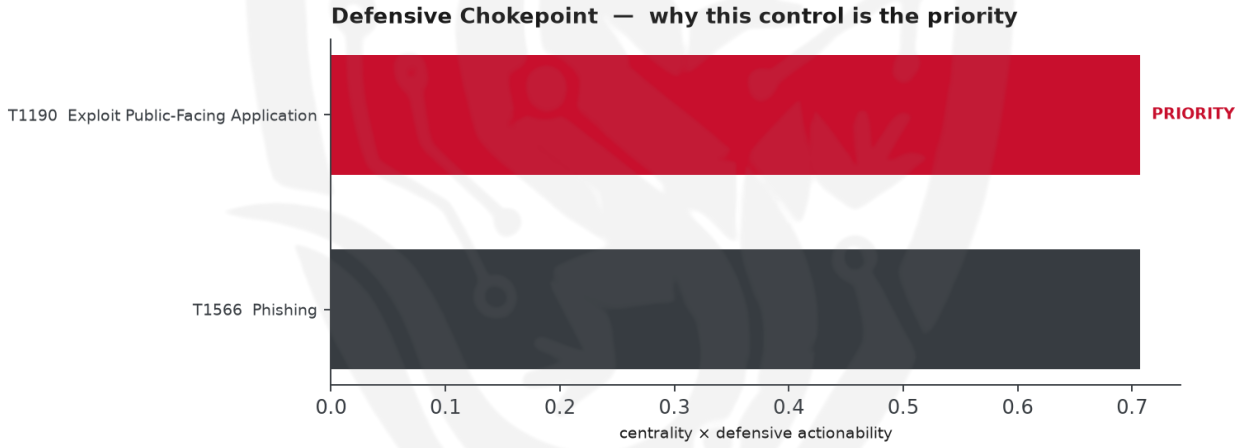
THREAT REPORT: TA2730 FAKE CRYPTO SCAMS

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 TA2730, a threat actor targeting the finance sector with fake crypto scams. The reporting indicates techniques inferred from the report include exploiting public-facing applications and phishing. Priority should be given to patching public-facing vulnerabilities to prevent initial access. The operational risk band is considered low, reaching initial-access level.

Threat Overview

TA2730, the observed threat actor, is involved in fake crypto scams, targeting the finance sector. While specific malware families and central CVEs are not identified due to insufficient data, the techniques inferred from the report suggest a focus on exploiting public-facing applications and phishing.

Attack Chain and Priority Control

The attack chain involves techniques such as exploiting public-facing applications and phishing, with the priority technique being T1190 Exploit Public-Facing Application. The priority control is to Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Infrastructure and Corroboration

There is no observed hosting provider or ASN information available for this activity. 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, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1190 Exploit Public-Facing Application - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.7071).
- Operational risk: Low (score 0.138, reaches initial-access).

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
GOLD SOUTHFIELD	0.4082
APT30	0.3536

Historical Profile	Behavioural Overlap
BlackTech	0.3162
Axiom	0.3015

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	8fv4dxp7lx035f8ylk7[.]live
Domain	467jtzbkqcfl22t9hxh[.]live
Domain	ddgaoylh4h420fvm7o5[.]live
Domain	u7aq3ocwrexd70ulpdj[.]live
Domain	zavpejjyz432d577l2e[.]live
Domain	cd7yt860whhm7g7ylj8[.]live
Domain	g8iqelymkc4eya9zs49[.]live
Domain	hy0zu0fuf7rc2ou5aje[.]live
Domain	k1rg2oz4zpzw91pdx90[.]live
Domain	ogqw9cpz7t7et3j1rur[.]live
Domain	adanispacex[.]com
Domain	fidelityspacex[.]site
Domain	fidelityspacexipo[.]site
Domain	muskspacexipo[.]com
Domain	muskspacexipo[.]vip
Domain	robinhoodspacex[.]com
Domain	spacexshares[.]xyz

Type	Indicator
Domain	mail[.]musksapcex[.]space

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application 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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The adversary, TA2730, could pivot to T1047 Windows Management Instrumentation to maintain access and gather information, as this technique allows them to leverage the existing Windows Management Instrumentation (WMI) infrastructure to execute commands and query system information, potentially evading detection. This technique may be particularly appealing as it enables the adversary to interact with the system in a way that appears legitimate, making it harder to distinguish from normal administrative activity. To counter this potential move, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1059 Command and Scripting Interpreter (n=38, lift 1.2)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command