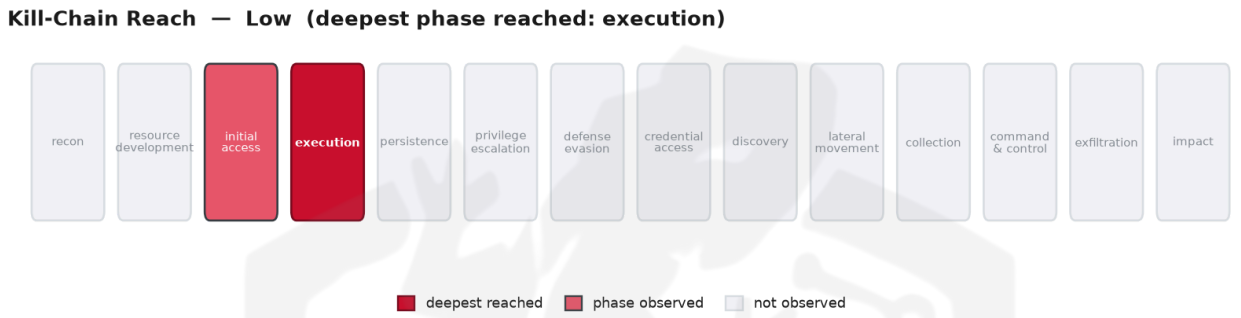
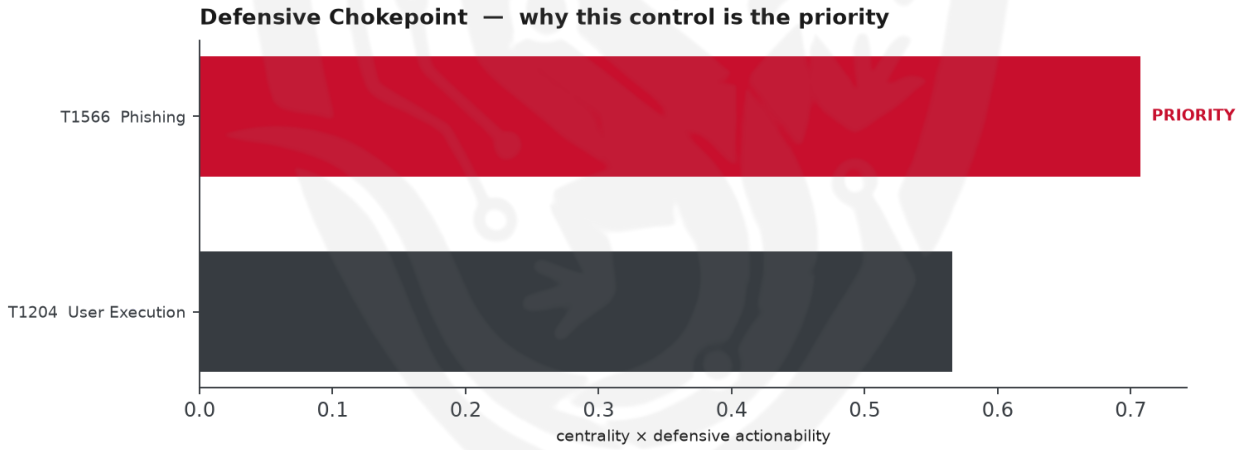
THREAT REPORT: DEVICE CODE PHISHING CAMPAIGN EXPLOITS MFA BYPASS VIA PHISHING

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 leverages phishing to coerce users into submitting device codes, thereby bypassing multi-factor authentication. No specific malware families or CVEs are identified. Priority defensive action is to harden against social-engineering delivery across email, links, and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA.

Threat Overview

The threat actor employs phishing (T1566) to trick users into providing device codes, enabling an MFA bypass. No malware families or CVEs are reported, and the victimology remains unspecified.

Attack Chain and Priority Control

The observed techniques form a chain: T1204 User Execution followed by T1566 Phishing. The priority technique is T1566 Phishing.
Priority action: Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA.

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. - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.7071).
- Operational risk: Low (score 0.17, reaches execution).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.7071; 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	0.7071
TA459	0.5
AppleJeus	0.5
APT12	0.4714

Historical Profile	Behavioural Overlap
Mofang	0.4714

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	html[.]phish[.]microsoft
Domain	cholaw-kr[.]co
Domain	rlcounsel[.]com
Domain	up88qope1z[.]hlpadditives[.]com
Domain	zr6dgshpvf[.]flosli[.]com
Domain	eusei[.]com
Domain	zrdesignlabo[.]com
Domain	profileupdate-collaboration[.]stefan-dufva[.]workers[.]dev

---

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:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1566 Phishing blocked, the threat actor could preserve the same objective by pivoting to T1203 Exploitation for Client Execution, a technique disproportionately paired with it across tracked groups.

Defensive countermeasure: Patch client applications (Office, browsers, PDF); enable exploit mitigations (ASLR/DEP/CFG); application isolation.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=43, lift 1.3), T1106 Native API (n=18, lift 1.6)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log