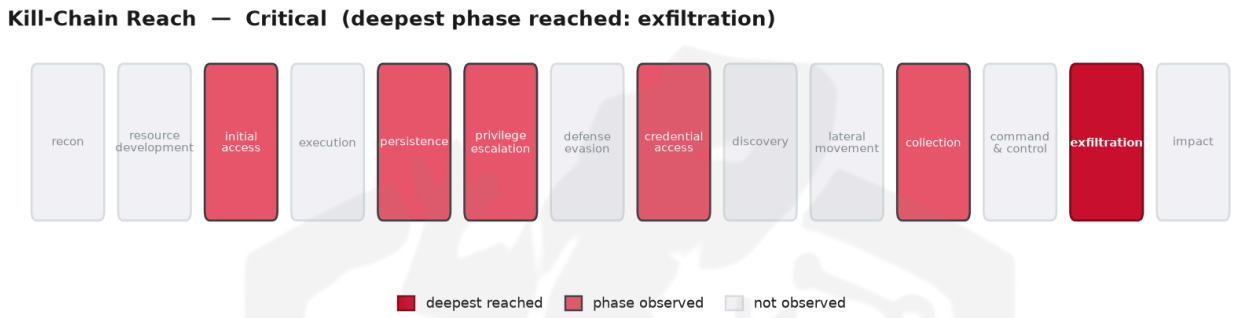
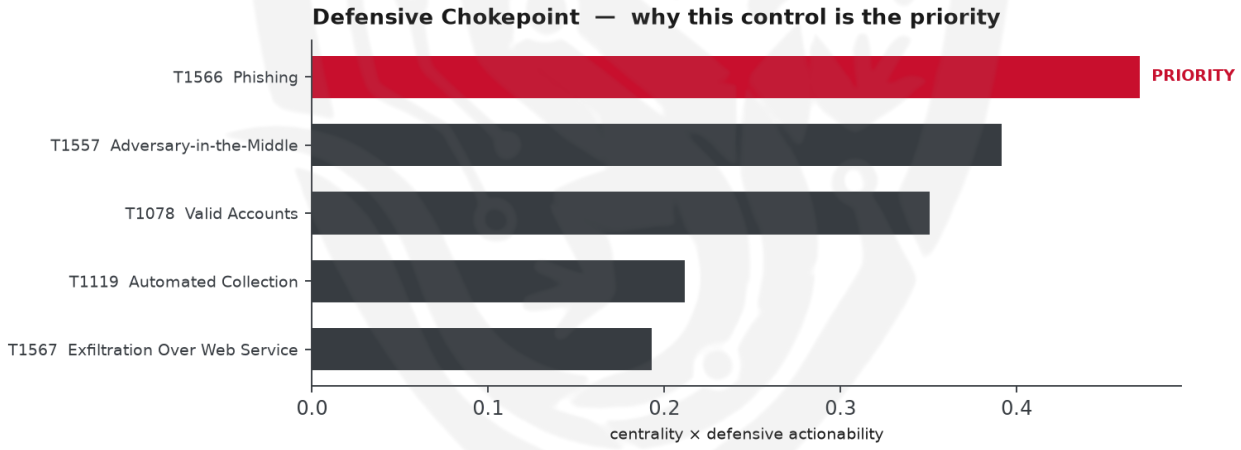
THREAT REPORT: UNC6671 CONDUCTS MULTI-BRAND VISHING EXTORTION CAMPAIGN

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 threat actor UNC6671 is operating a vishing-based extortion campaign that targets a wide array of sectors, including finance, technology, and cloud service providers. The report does not identify specific malware families or CVEs associated with the activity. Observed techniques span credential abuse, automated data collection, man-in-the-middle attacks, phishing, and web-service exfiltration. Priority should be given to hardening against social-engineering delivery across email, links, and voice/callback lures as detailed in the source-provided control.

Threat Overview

UNC6671 is the identified actor behind the campaign. No specific malware family is disclosed (Data Insufficient), and no vulnerability (CVE) is cited. The campaign’s victimology spans finance, technology,

transportation, hospitality, healthcare, legal, manufacturing, real estate, insurance, energy, retail, construction, media, aerospace, defense, and telecommunications sectors.

Attack Chain and Priority Control

The reporting indicates a chain that begins with phishing (T1566) to obtain initial access, followed by the use of valid accounts (T1078) to move laterally, automated collection of data (T1119), potential adversary-in-the-middle positioning (T1557), and finally exfiltration over web services (T1567).

Priority technique: T1566 Phishing

Concrete control (source verbatim): 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.

Infrastructure and Corroboration

The enrichment data reports no observable hosting providers or ASNs linked to this activity. Abuse-ch does not corroborate any malware families, and AbuseIPDB flags no indicators with confidence ≥ 80 %. Consequently, there are no additional infrastructure or reputation details to augment the source findings.

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. - T1078 Valid Accounts - T1119 Automated Collection - T1557 Adversary-in-the-Middle - T1566 Phishing - T1567 Exfiltration Over Web Service

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.47).
- Operational risk: Critical (score 0.822, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3162; 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	0.3162
POLONIUM	0.2697
PittyTiger	0.2582
Confucius	0.2535
APT30	0.2236

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
IP	107[.]128[.]45[.]122
IP	38[.]42[.]59[.]171
IP	47[.]218[.]103[.]146
IP	76[.]103[.]148[.]180
Domain	oktaenroll[.]com
Domain	idokta[.]com
Domain	myoktasso[.]com
Domain	mypasskeysso[.]com
Domain	setupssopasskey[.]com
Domain	passkeyms[.]com
Domain	keyokta[.]com

Type	Indicator
Domain	portalpasskey[.]com
Domain	oktaportalsso[.]com
Domain	passkeyportal[.]com
Domain	passkeyportalsetup[.]com
Domain	addoktapasskey[.]com
Domain	deploypasskey[.]com
Domain	mysecurepasskey[.]com
Domain	activatemypasskey[.]com
Domain	createpasskey[.]com
Domain	registerpasskey[.]com
Domain	setupsso[.]com
Domain	passkeycenter[.]com
Domain	passkeyregister[.]com
Domain	secureauthpasskey[.]com
Domain	createmypasskey[.]com
Domain	passkeyset[.]com
Domain	passkeyokta[.]com
Domain	passkeyadd[.]com
Domain	passkeydeploy[.]com
Domain	setpasskey[.]com
Domain	addmypasskey[.]com
Domain	passkey-portal[.]com
Domain	passkeyregistration[.]com
Domain	portalsetuphub[.]com
Domain	mynewpasskey[.]com

Type	Indicator
Domain	myconnectkey[.]com
Domain	enablepasskey2fa[.]com
Domain	passkeyuser[.]com
Domain	passkeyenroll[.]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 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:** T1204 User Execution (execution)
- **Basis:** of the 89+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

If phishing attempts are blocked, the group could pivot to placing a malicious HTA, JavaScript, or LNK file on an internal web portal or shared drive and rely on a user to click or open the file, thereby achieving execution through the User Execution behavior described in T1204. Block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures.

Also plausible (same tactic): T1203 Exploitation for Client Execution (n=38, lift 1.6), T1053 Scheduled Task/Job (n=43, lift 1.3)

Detection and hardening for the pivot (T1204 User Execution)

- **Telemetry:** Endpoint process telemetry; Email/proxy logs
- **Detect:**
  - User double-clicking archive/ISO/LNK contents that spawn interpreters
  - Mark-of-the-Web on delivered files; LOLBIN execution from user temp paths
- **Harden:**
  - Block risky file types; ASR rules; user awareness training
  - Application control to stop execution from user-writable directories
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1017 User Training · DS0009 Process, DS0022 File