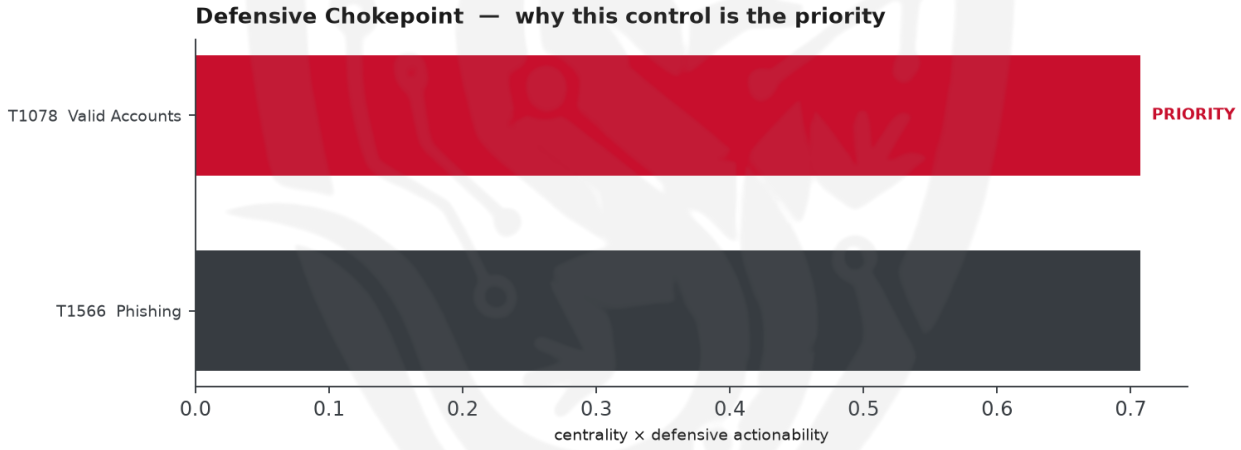
THREAT REPORT: PINK'S FAKE HELPDESK CALLS

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 Pink, a threat actor using fake helpdesk calls to steal credentials. The targeted country and sectors are not specified, but the threat actor's techniques pose a risk to various organizations. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate this threat. The operational risk band is considered low, but it can still reach privilege-escalation levels.

Threat Overview

The threat actor, attributed to Pink by the source, is using techniques inferred from the report, including valid accounts and phishing, to steal credentials. The malware families and central CVE used in this campaign are not specified due to insufficient data. The victimology of this campaign is also not well-defined, with targeted countries and sectors not provided.

Attack Chain and Priority Control

The observed techniques, inferred from the report, involve the use of valid accounts and phishing to gain initial access. The priority technique in this chain is T1078 Valid Accounts, which is the graph chokepoint. To mitigate this threat, the priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with 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. - T1078 Valid Accounts - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.7071).
- Operational risk: Low (score 0.235, reaches privilege-escalation).

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
PittyTiger	0.4082

Historical Profile	Behavioural Overlap
APT30	0.3536
FIN4	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	deploypasskey[.]com
Domain	passkeyadd[.]com
Domain	passkeydeploy[.]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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts 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 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

Pink could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique would allow them to leverage the existing Windows Management Instrumentation (WMI) infrastructure to execute commands and gather information, potentially bypassing the restrictions imposed by the blocked T1078 Valid Accounts control. This technique may be particularly appealing to Pink as it enables them to interact with the target system in a way that blends in with normal administrative activity, making it harder to detect. 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): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

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