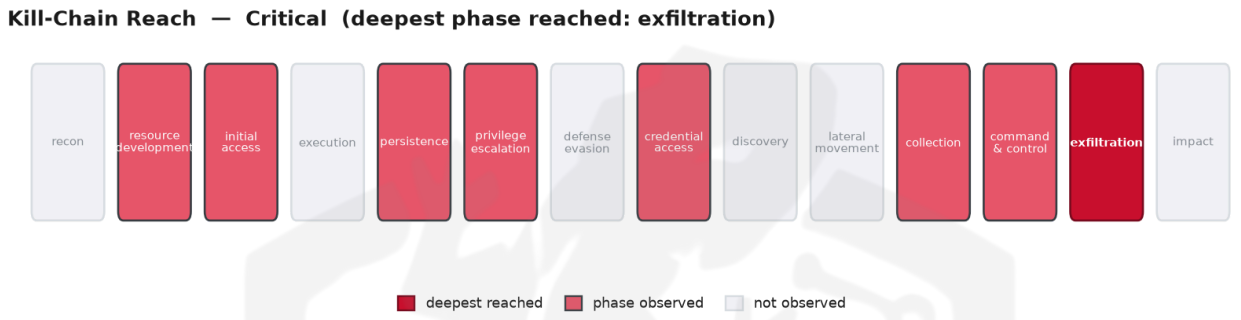
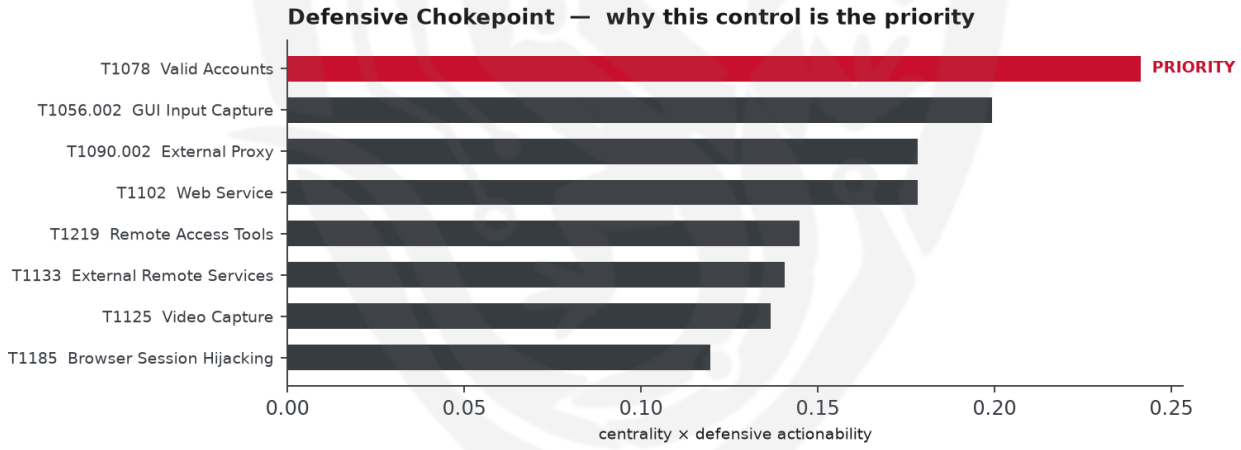
THREAT REPORT: PURPLEDELTA CONDUCTS FRAUDULENT EMPLOYMENT OPERATIONS

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

PurpleDelta is observed running a fraudulent employment campaign that targets organizations in the technology, healthcare, finance, media, and NGO sectors. The operation leverages a broad set of credential-focused techniques, including the use of valid accounts and external remote services, to gain and maintain access. No specific malware family or CVE is identified in the source material. Priority should be given to enforcing multi-factor authentication on all accounts, disabling dormant or over-privileged accounts, and alerting on impossible-travel and anomalous log-on activity.

Threat Overview

The source attributes this activity to PurpleDelta. Malware families are listed as data insufficient, and no vulnerability (CVE) is cited. The campaign focuses on victims across technology, healthcare, finance,

media, and non-governmental organizations.

Attack Chain and Priority Control

The observed chain begins with the compromise of legitimate credentials (T1078 Valid Accounts), followed by the establishment of external remote services (T1133) and the use of remote access tools (T1219). The actor then harvests screen and video captures (T1113, T1125), hijacks browser sessions (T1185), and extracts data via web services (T1102, T1567). Throughout, the adversary maintains persistence through compromised email, SharePoint, and social media accounts (T1586.002, T1585.002, T1585.001). The chokepoint technique is **T1078 Valid Accounts**, and the concrete control recommended is: **Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.**

Infrastructure and Corroboration

Third-party enrichment shows the malicious infrastructure is hosted by providers including 1&1 Versatel GmbH, Wattage Hosting LLC, Oculus Networks Inc, and Cloud Software - FZCO, as reported by the source pulse. AbuseIPDB flags no indicators with high confidence, and abuse.ch does not corroborate any malware families.

Technical Appendix

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

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

- T1113 Screen Capture
- T1213.002 Sharepoint
- T1133 External Remote Services
- T1586.002 Email Accounts
- T1567 Exfiltration Over Web Service
- T1219 Remote Access Tools
- T1185 Browser Session Hijacking
- T1585.002 Email Accounts
- T1090.002 External Proxy
- T1125 Video Capture
- T1586 Compromise Accounts
- T1102 Web Service
- T1056.002 GUI Input Capture
- T1588.002 Tool
- T1078 Valid Accounts
- T1585.001 Social Media Accounts
- T1102.002 Bidirectional Communication
- T1585 Establish Accounts

- T1213 Data from Information Repositories
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2721).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4308; 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
POLONIUM	0.4308
PittyTiger	0.3536
VOID MANTICORE	0.3283
Carbanak	0.3273
Sandworm Team	0.3128

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	Context
IP	104[.]253[.]147[.]147	AbuseIPDB 0% (BE) · AS5511 Orange S.A.
IP	104[.]253[.]51[.]76	AbuseIPDB 0% (US) · AS25893 Wattage Hosting LLC
IP	104[.]253[.]72[.]75	AbuseIPDB 0% (US) · AS398781 Oculus Networks Inc
IP	104[.]253[.]134[.]123	AbuseIPDB 0% (FR) · AS211273 Cloud Software - FZCO
IP	218[.]24[.]120[.]118	AbuseIPDB 0% (CN) · AS4837 China Unicom China169 Backbone

Type	Indicator	Context
IP	104[.]253[.]1[.]79	AbuseIPDB 0% (US) · AS49791 Newserverlife LLC
IP	104[.]253[.]103[.]238	AbuseIPDB 0% (KR) · AS4766 Korea Telecom
IP	104[.]253[.]111[.]106	AbuseIPDB 0% (DE) · AS8881 1&1 Versatel GmbH
IP	104[.]253[.]112[.]86	AbuseIPDB 0% (DE) · AS8881 1&1 Versatel GmbH
IP	104[.]253[.]121[.]146	AbuseIPDB 0% (US) · AS211273 Cloud Software - FZCO
IP	104[.]253[.]17[.]141	AbuseIPDB 0% (US) · AS25893 Wattage Hosting LLC
IP	104[.]253[.]19[.]244	AbuseIPDB 0% (US) · AS400536 NodeStop LLC
IP	104[.]253[.]199[.]214	AbuseIPDB 0% (DE) · AS8881 1&1 Versatel GmbH
IP	104[.]253[.]251[.]19	AbuseIPDB 0% (IL) · AS398781 Oculus Networks Inc
IP	104[.]253[.]34[.]67	AbuseIPDB 0% (US) · AS5650 Frontier Communications of America Inc.
IP	104[.]253[.]47[.]239	AbuseIPDB 0% (AU) · AS3356 Level 3 Parent LLC
IP	104[.]253[.]56[.]226	AbuseIPDB 0% (US) · AS396073 Majestic Hosting Solutions LLC
IP	104[.]253[.]90[.]150	AbuseIPDB 0% (IT) · AS64445 NetJoin srl

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

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.

With T1078 Valid Accounts blocked, PurpleDelta could preserve the same objective by pivoting to T1047 Windows Management Instrumentation, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: 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