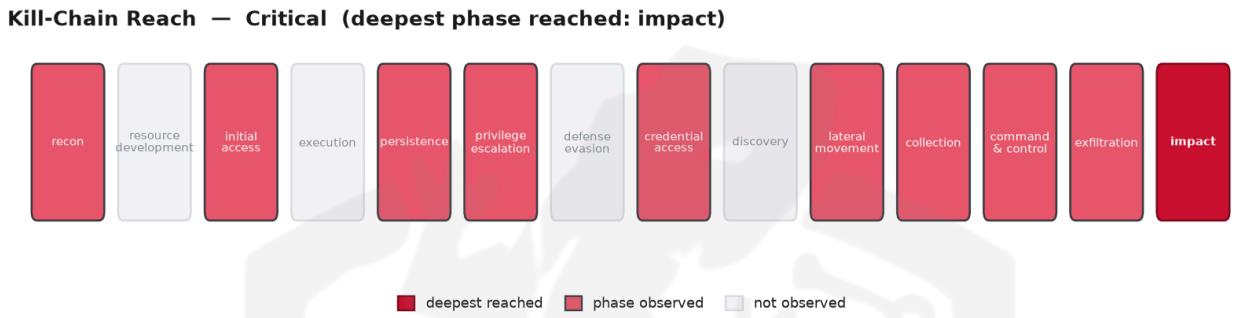
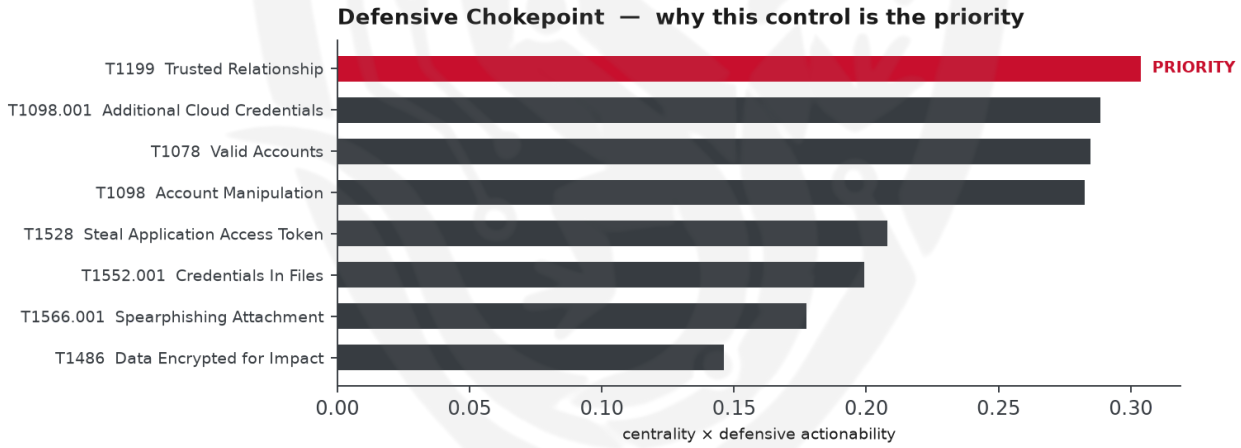
THREAT REPORT: UNKNOWN_ADVERSARY SUPPLY CHAIN INCIDENT

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 has resulted in the unauthorized access of customer CRM data, highlighting the need for immediate defensive action. The threat actor has exploited various techniques to gain access to sensitive information. Priority should be given to auditing and least-privileging trusted third-party connections to prevent further incidents. The operational risk band for this incident is critical, indicating a high level of potential impact.

Threat Overview

The observed cluster of activity has utilized multiple techniques, including Sharepoint, Email Collection, Spearphishing, and Data from Cloud Storage, to target unknown sectors and countries. The central vulnerability exploited is unknown, and the malware families used are also insufficiently identified. The

victimology of this incident is unclear, but it is evident that the threat actor has successfully accessed sensitive customer data.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including initial access through spearphishing or other means, followed by the exploitation of trusted relationships and the collection of sensitive data from cloud storage. The priority technique in this chain is T1199 Trusted Relationship, which serves as a critical chokepoint. To mitigate this threat, the priority control is to "Audit and least-privilege trusted third-party/B2B connections; monitor partner-account activity."

Infrastructure and Corroboration

The malicious infrastructure associated with this incident is hosted on providers such as SOLLUTIUM EU Sp z.o.o. and Stellar Group SAS, as observed by third-party sources. However, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, 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, expert-tagged by source)

- T1213.002 Sharepoint
- T1114 Email Collection
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1530 Data from Cloud Storage
- T1589.002 Email Addresses
- T1589.003 Employee Names
- T1552.001 Credentials In Files
- T1528 Steal Application Access Token
- T1098.001 Additional Cloud Credentials
- T1199 Trusted Relationship
- T1098 Account Manipulation
- T1078 Valid Accounts
- T1486 Data Encrypted for Impact
- T1567.002 Exfiltration to Cloud Storage
- T1598 Phishing for Information
- T1213 Data from Information Repositories
- T1071.001 Web Protocols
- T1550.001 Application Access Token
- T1078.004 Cloud Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1199 Trusted Relationship (centrality 0.3037).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3862; 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
HAFNIUM	0.3862
FIN4	0.307
APT28	0.2935
Scattered Spider	0.2798
LAPSUS$	0.274

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	138[.]226[.]246[.]94	AbuseIPDB 0% (NL) · AS43641 SOLLUTIUM EU Sp z.o.o.
IP	94[.]154[.]32[.]160	AbuseIPDB 0% (FR) · AS214961 Stellar Group SAS
Domain	baccarat[.]com[.]au	

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:** T1199 Trusted Relationship (initial-access)
- **Observed here:** the threat actor used T1078 Valid Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1078 Valid Accounts by attempting to compromise or obtain credentials for existing accounts, which may allow them to maintain access to the target network. This could involve exploiting weak passwords, phishing, or other credential theft methods, which would likely be used to regain a foothold after the trusted relationship was blocked. The defensive control to counter this would be to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account