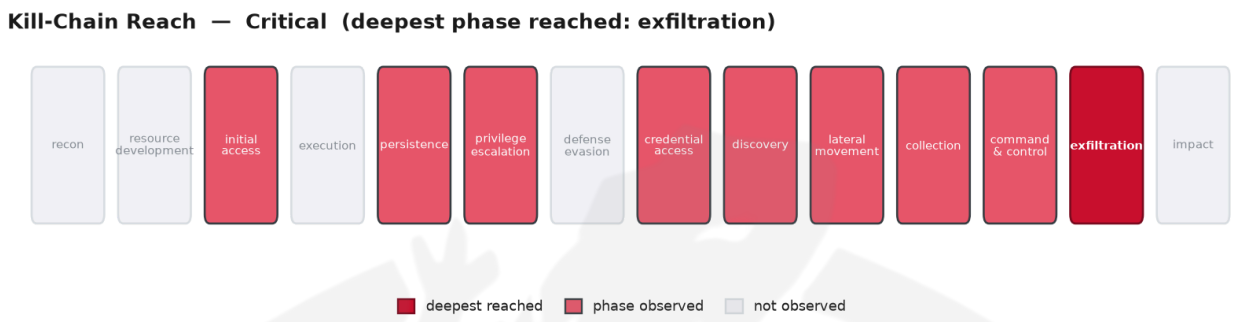
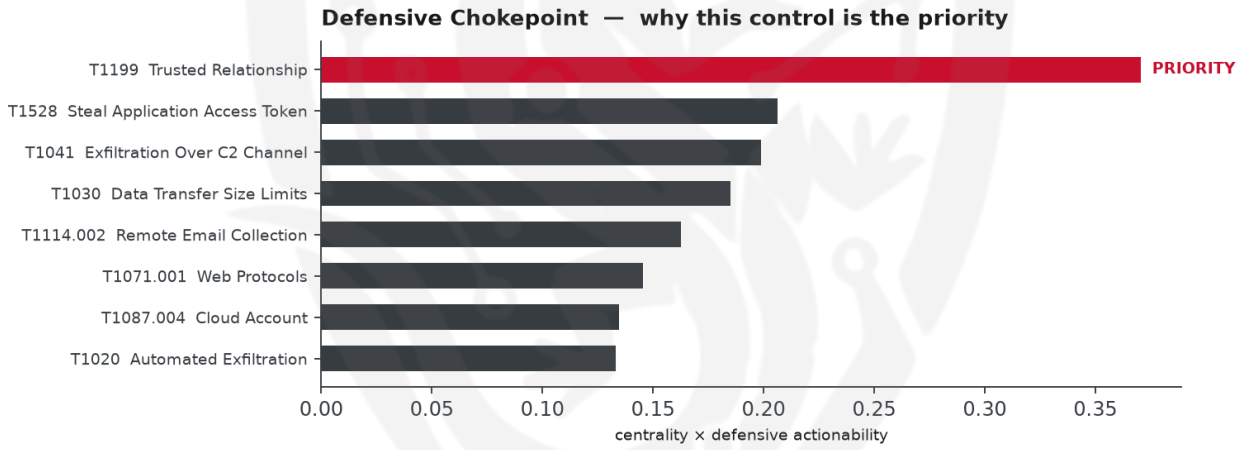
THREAT REPORT: ICARUS

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 Icarus, a threat actor who has been observed targeting Salesforce instances in a supply chain attack. The actor's techniques include exfiltration over web services and stealing application access tokens, highlighting the need for vigilance. Priority should be given to auditing and least-privileging trusted third-party connections to mitigate the risk of data exfiltration. The operational risk band is deemed Critical, indicating a high level of potential impact.

Threat Overview

Icarus, the attributed threat actor, has been observed utilizing various techniques to compromise Salesforce instances, including Sharepoint and exfiltration over web services. Although specific malware families and central CVEs are not identified due to insufficient data, the actor's methods involve exploiting trusted relationships and stealing application access tokens. The victimology and targeted sectors remain unclear, but the threat actor's actions underscore the importance of robust security measures.

Attack Chain and Priority Control

The observed techniques employed by Icarus form a complex attack chain, involving the exploitation of trusted relationships, exfiltration over web services, and the theft of application access tokens. The priority technique identified is T1199 Trusted Relationship, which serves as a critical chokepoint in the attack chain. To counter this, the recommended 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 Icarus' activities has been observed to be hosted by providers such as SOLLUTIUM EU Sp z.o.o. and Stellar Group SAS, according to third-party enrichment data. However, 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, expert-tagged by source)

- T1213.002 Sharepoint
- T1567 Exfiltration Over Web Service
- T1020 Automated Exfiltration
- T1528 Steal Application Access Token
- T1087.004 Cloud Account
- T1041 Exfiltration Over C2 Channel
- T1199 Trusted Relationship
- T1114.002 Remote Email Collection
- T1030 Data Transfer Size Limits
- 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 0.3705).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3482; 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	0.3482
Ke3chang	0.3267
APT28	0.2905
Chimera	0.2863
VOID MANTICORE	0.278

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	212[.]86[.]125[.]24	AbuseIPDB 0% (NL) · AS43641 SOLLUTIUM EU Sp z.o.o.
IP	94[.]154[.]32[.]160	AbuseIPDB 0% (FR) · AS214961 Stellar Group SAS

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.k@3sdragon.eu

- **Control applied:** T1199 Trusted Relationship (initial-access)
- **Observed here:** Icarus used T1078.004 Cloud Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078.004 Cloud Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

Icarus could pivot to exploiting Cloud Accounts (T1078.004) to maintain access and achieve their objectives, potentially by targeting cloud-based identities and credentials that may not have been directly impacted by the blocked Trusted Relationship technique. They may attempt to leverage cloud account access to regain a foothold or move laterally within the environment. To counter this, the defensive control 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 (T1078.004 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs
- **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
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account