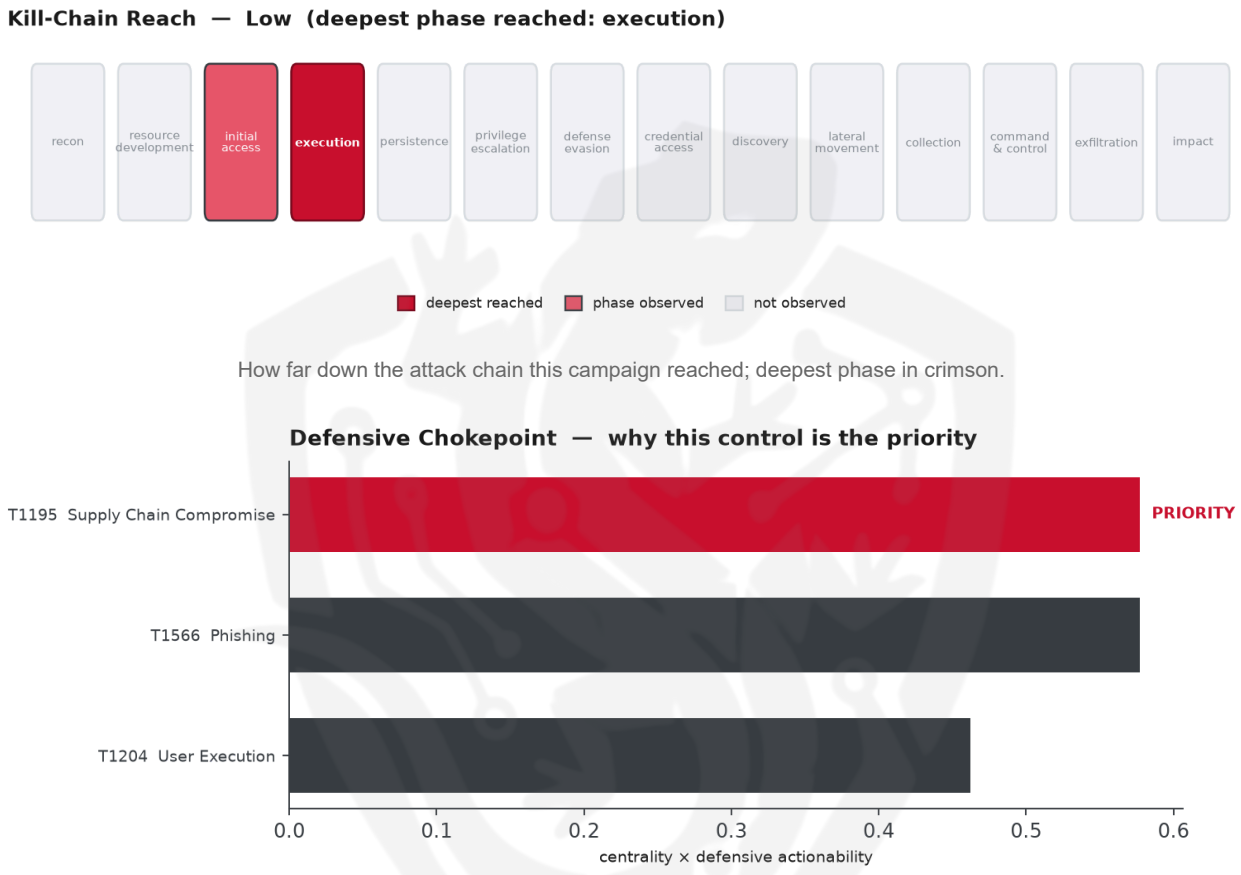
THREAT REPORT: SHINYHUNTERS OAUTH ABUSE

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 ShinyHunters, a threat actor targeting various sectors including Retail, Education, and Manufacturing. The techniques inferred from the report suggest a focus on compromising the software supply chain. Priority should be given to defending SaaS-based applications against OAuth abuse. The observed cluster of activity highlights the importance of verifying software supply chain integrity to prevent potential compromises.

Threat Overview

ShinyHunters, the attributed threat actor, is involved in OAuth abuse, although specific malware families and central CVEs are not identified due to insufficient data. The targeted countries and specific vulnerabilities exploited are also not specified. However, the sectors affected include Retail, Education, and Manufacturing, indicating a broad range of potential victims.

Attack Chain and Priority Control

The techniques inferred from the report include Supply Chain Compromise, User Execution, and Phishing, with the priority technique being T1195 Supply Chain Compromise. This chokepoint in the attack chain underscores the importance of securing the supply chain to prevent further malicious activity. The priority control, as stated, is to "Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels."

Infrastructure and Corroboration

The malicious infrastructure associated with this activity is hosted on providers such as SOLLUTIUM EU Sp z.o.o., Stellar Group SAS, and Virtual Systems LLC, as observed. According to AbuseIPDB, there are no indicators at or above 80% confidence, with the highest confidence seen being 0%. Additionally, abuse.ch does not corroborate any specific malware families in this context. These findings are based on third-party enrichment and serve to corroborate the source's assessment without overriding it.

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. - T1195 Supply Chain Compromise - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1195 Supply Chain Compromise (centrality 0.5774).
- Operational risk: Low (score 0.191, reaches execution).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5774; 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
APT30	0.5774
TA459	0.4082
AppleJeus	0.4082
APT12	0.3849
Mofang	0.3849

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
IP	213[.]111[.]148[.]90	AbuseIPDB 0% (UA) · AS6698 Virtual Systems LLC

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:** T1195 Supply Chain Compromise (initial-access)
- **Observed here:** T1195 Supply Chain Compromise 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:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 10+ groups that use Supply Chain Compromise, this pairing runs 2.7x above base rate, a disproportionately-coupled move rather than the obvious one.

ShinyHunters could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and evade detection, as this technique allows them to execute malicious tasks at specific intervals, potentially

leveraging the existing trust in scheduled tasks to blend in with legitimate system activity. This technique may be particularly appealing to ShinyHunters as it enables them to execute tasks without requiring direct, continuous access to the compromised system, thereby reducing their overall footprint. To counter this potential move, the defensive control would involve alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators.

Also plausible (same tactic): T1203 Exploitation for Client Execution (n=7, lift 2.6), T1047 Windows Management Instrumentation (n=6, lift 2.2)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File