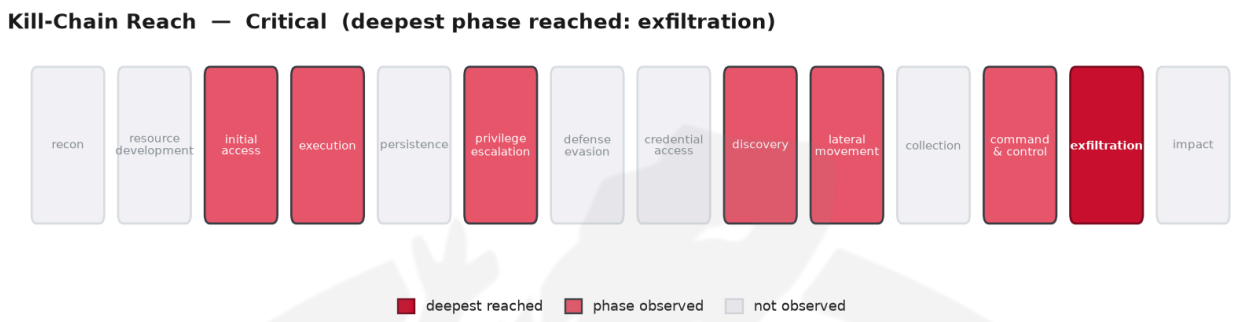
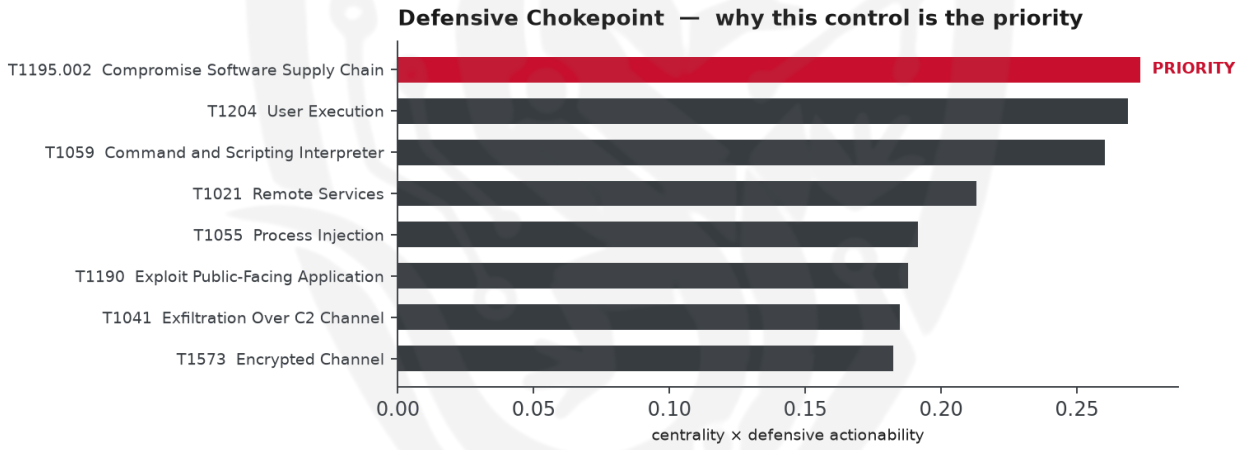
THREAT REPORT: APT32

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 APT32, a threat actor that has been observed targeting various sectors, including Finance, Construction, and Transportation. The malware families used by the actor include SPECTRALVIPER, Denis, SOUNDBITE, PHOREAL, and WINDSHIELD. Priority should be given to verifying the software supply chain integrity to prevent compromise. The actor's ability to compromise the software supply chain poses a critical risk, reaching the level of exfiltration.

Threat Overview

The threat actor, APT32, utilizes a range of malware families, including SPECTRALVIPER, Denis, SOUNDBITE, PHOREAL, and WINDSHIELD, to target organizations in the Finance, Construction, and Transportation sectors. The central vulnerability exploited by the actor is currently unknown. The actor's techniques include code signing, system information discovery, and exploit public-facing application, among others.

Attack Chain and Priority Control

The observed techniques used by APT32 form a complex attack chain, with the priority technique being T1195.002 Compromise Software Supply Chain. This technique is the graph chokepoint, highlighting the importance of securing the software supply chain. The priority control is to Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher 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)

- T1553.002 Code Signing
- T1082 System Information Discovery
- T1190 Exploit Public-Facing Application
- T1036 Masquerading
- T1055 Process Injection
- T1021 Remote Services
- T1059 Command and Scripting Interpreter
- T1204 User Execution
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1195.002 Compromise Software Supply Chain
- T1570 Lateral Tool Transfer
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1195.002 Compromise Software Supply Chain (centrality 0.2735).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5026; 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
Daggerfly	0.5026
Windshift	0.3746
Moses Staff	0.3591
Higaisa	0.3583
Rocke	0.3569

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	cnrp7[.]org
Domain	nguoitieudung[.]com[.]vn
Domain	anessallie[.]com
Domain	arkoimmerma[.]com
Domain	carosseda[.]com
Domain	eighrimeau[.]com
Domain	hieryells[.]com
Domain	tefanortin[.]com
Domain	adineohler[.]com
Domain	aisicoin[.]com

Type	Indicator
Domain	alicervois[.]com
Domain	antenham[.]com
Domain	arinaurna[.]com
Domain	aulolloy[.]com
Domain	avidilleneu[.]com
Domain	avidsontre[.]com
Domain	aximilian[.]com
Domain	biasatts[.]com
Domain	braydenhateaub[.]com
Domain	chascloud[.]com
Domain	dreyoddu[.]com
Domain	dwarduong[.]com
Domain	eckenbaue[.]com
Domain	errellawle[.]com
Domain	erstin[.]com
Domain	frahreiner[.]com
Domain	hristophe[.]com
Domain	ichardt[.]com
Domain	icmannaws[.]com
Domain	iecopeland[.]com
Domain	irkaimboeuf[.]com
Domain	jamedalue[.]com
Domain	jamyer[.]com
Domain	jeanessbinder[.]com
Domain	jeffreyue[.]com

Type	Indicator
Domain	keoucha[.]com
Domain	laudiaouc[.]com
Domain	lbertussbau[.]com
Domain	loridanase[.]com
Domain	marrmann[.]com