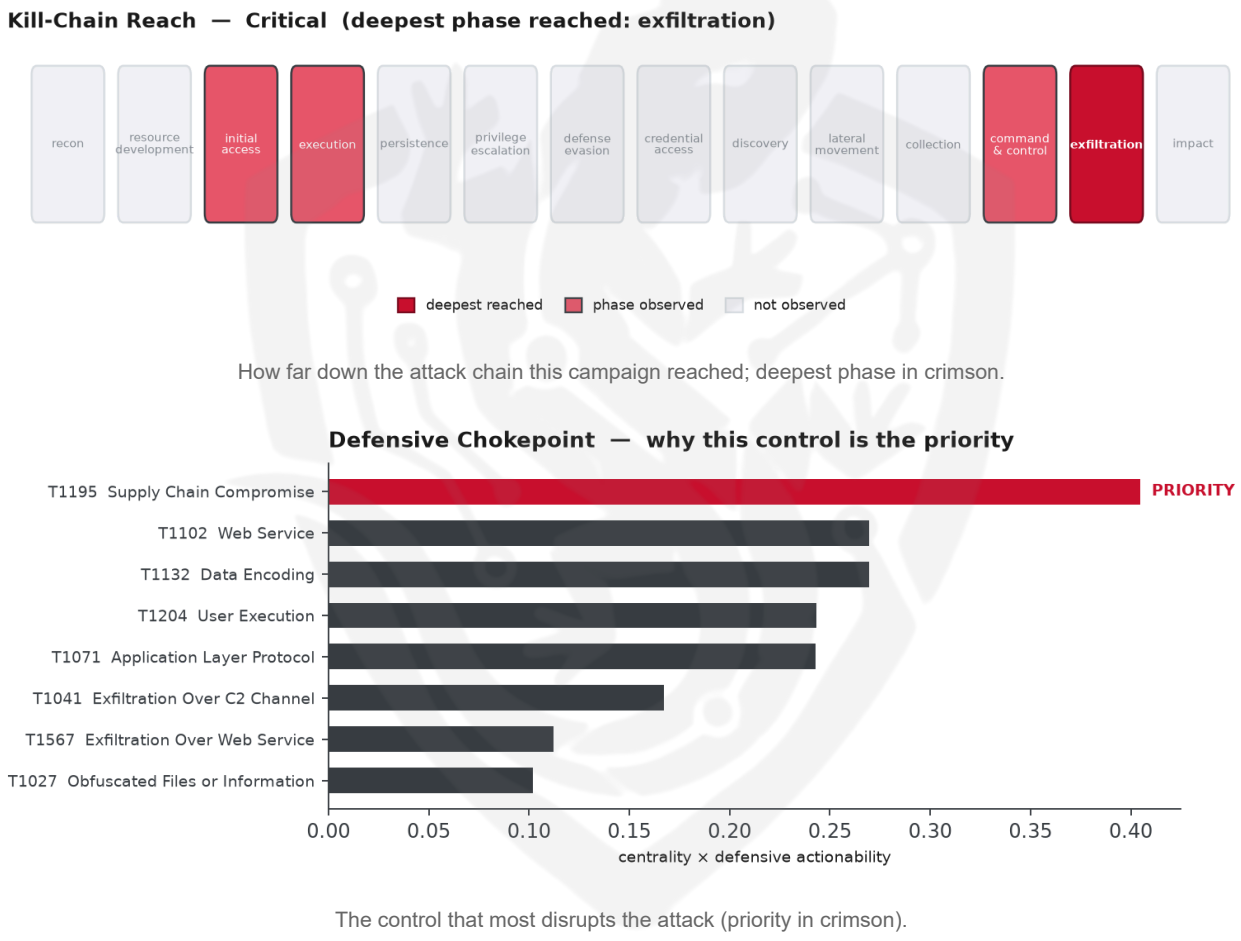
THREAT REPORT: TYPOSQUATTING CAMPAIGN TARGETS SECURE PAYMENT APPS VIA NPM AND PYPI

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 involves a coordinated campaign targeting secure payment applications through typosquats on npm and PyPI. The techniques inferred from the report suggest a complex attack chain, with a priority defensive action focused on verifying software supply chain integrity. Priority should be given to securing the software supply chain to prevent further compromise. The campaign's impact is considered critical due to the potential for exfiltration.

Threat Overview

The threat actor, whose identity is not specified, is leveraging a campaign that targets secure payment applications through typosquats on npm and PyPI. The reporting indicates the use of various techniques,

including obfuscated files, exfiltration over C2 channels, and supply chain compromise. The victimology and targeted sectors are not specified, but the campaign's techniques suggest a sophisticated attack.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including obfuscated files, exfiltration, and supply chain compromise. The priority technique is T1195 Supply Chain Compromise, which serves as a graph chokepoint. To mitigate this threat, the priority action is to: Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels.

Infrastructure and Corroboration

There is no observable hosting provider or ASN associated with this campaign, and no malware families have been corroborated by abuse.ch. Additionally, 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, 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. - T1027 Obfuscated Files or Information - T1041 Exfiltration Over C2 Channel - T1071 Application Layer Protocol - T1102 Web Service - T1132 Data Encoding - T1195 Supply Chain Compromise - T1204 User Execution - T1567 Exfiltration Over Web Service

Analytical Scores

- Priority technique (graph chokepoint): T1195 Supply Chain Compromise (centrality 0.4047).
- Operational risk: Critical (score 0.885, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3536; 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
BlackOasis	0.3536
TA551	0.2949
ZIRCONIUM	0.2728
Confucius	0.2673
LazyScripter	0.2582

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	caliber-spinner-finishing[.]ngrok-free[.]dev
URL	hxxps://caliber-spinner-finishing[.]ngrok-free[.]dev:443/
Hash	ce09810adca70ebec87bc455380ef629ceaa2a0d926149d9115604060167682c
Hash	b2ea8d69f6792a87327ffde2ee4551bb6b99617f53e1ba71bf9a70f45dbc57ea
Hash	8a70a5c1075f2dea4db94633ddc64b0d03d0385fdeda7c226acc944331febf43
Hash	c8b4d17c1f0aa7c50f2fa23d7c328482a4ad2c4da4d600f358ebdf200cbefd83
Hash	9fd06d823d54183cc91625fdc6decffe8db2863f6499a955656ebdcc089792cf
Hash	615805652b2f006e69512b90d0d63883d7ae1ede69d86384fd77bd46235b2369
Hash	6dc672e3bab8bcf80c66b2f95150067fb47429d4cf65eb95215e5f3abc7cade5
Hash	4a4b5c1bc1e948c853cb0978c07c7b8d1540c7b1ded95f8d5ad25c126cb6c7b0
Hash	9727c804c4354e481d2ff9d4934bd1b2518293a9ca34a14f5c7ae9d0cd30ce94
Hash	313853a82bce61052c00e6a6af85b5069e007a76122c727f31661bc636b12f14
Hash	2cbfc4e4b1de5e68ab81fba7e1b0c711b4d26197b48ea4db6819c9cea223b0ed
Hash	a0313822513f9b89479f666888a4784a3fc99b4cc4566213dcda66b03b47120c

Type	Indicator
Hash	3a0dd3479eaf85b65e5abd63d6451f98506faddee47cf4bebd9f91296abb29f0
Hash	39371ac7061168dd3d890061267b3875bc4b30dca5e28d40dbc27a4396439ff1
Hash	c51c0b6c7817443b021aff44d4416c09fd039849db81860b9b5144e789fa3987
Hash	6e251c3d2bde8fff0487c1eecd359c4a544a09fd708755020e4b1c53ad6b8dd1
Hash	cd7255730b6a7a3895d622d37d0e8f984d2d280689acef56ff195d663e7723ad
Hash	5c4faef80c83c7ec0925a4aacb4bddabe82b91066ac41305907ba277cd7b3b85
Hash	50cb7550224d8d227a0625e7f53be86924d8e057e403b6b91b83ea20df834048
Hash	1bae9f2fb9866422f07345501fa2cb4c3a99f2652c8c9decdc27ffbf9714e7bc
Hash	1df8c579ffcbf5527b1856bd1774601a5188b380e442c5a0fbd400bd86a4501b
Hash	b29973eda4d0c090608c15a976688cad0b2114fdc0dcb89ad37515287ba13aad
Hash	9e9655f54bfac8a937d78ac506722bae1468ead4cc9ee95b35e0f8ef17ee13d9
Hash	67e4d6a4f53098e48bfa6ecceeaa754592bc249b83404bcfb8542977ae36dac4
Hash	1bfa32548676d32b7639d3171e2f9feefba5026dc336968c91f4ae2b152c5410
Hash	2bc8af4bd2f539630f7800f3491b64c7e2bffe12e955d0d4f03a4f6a4b0018bd
Hash	eae055c5736366811d2a4b1f78ff206486e7f7445040122efbe023ecd2d20bcc
Hash	d4ed2d87942fbefa5d7b7f19fb6f2e9bc293c96bf577bb97ed3ca56185abcf25
Hash	447484c76a06918d7f6f6c6f95ee2bced6dd2e9b282c6f5b92b2b7c0976381d5
Hash	f43cb68850a2506805d60ff466f54eba331e1cc2a513b329f5121e0c39104418
Hash	1314fc888ca5b3ea91a04e1f5b63039ffc7fc3832b8d809a28ad549c6f9d4f23
Hash	af66bc2b516d1ef71af9b6ee9f8f5af0a99fed562b34809cd55071b94c2d1304
Hash	b157a66826d27512c3618817fee924e53d14cabb2c4c7f454affde37350f55f0
Hash	2303a74a5fac917279f1078e03a4bfd6afbb89462f97d7344ed10e6e9e9e92b7
Hash	5242c5086d75a492d14e474de7c8f34b18ec0a8a9ce6d77eec8675a9572d9d23
Hash	1d567795a366b9edcfef7f1fa2d398b7cb41890dd3b2f3f1f9803de0cdba0c89
Hash	c2e4483abea830ba8b8230540ace51788d0712bed9006697ddddb9cbf133c151

Type	Indicator
Hash	390bca9d70efa42cb792f7f677189821a24527cd4298ab2acb954df0abb5c1c3

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.

The actor could pivot to using T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially leveraging the existing access gained from the initial supply chain compromise to create a new scheduled task that blends in with legitimate system activity. This technique may be particularly appealing as it allows the actor to execute code without needing to maintain a constant connection to the compromised system, making it harder to detect. To counter this, the defensive control would involve alerting on new scheduled tasks (Event ID 4698); restricting schtasks/at to admins; baseline 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