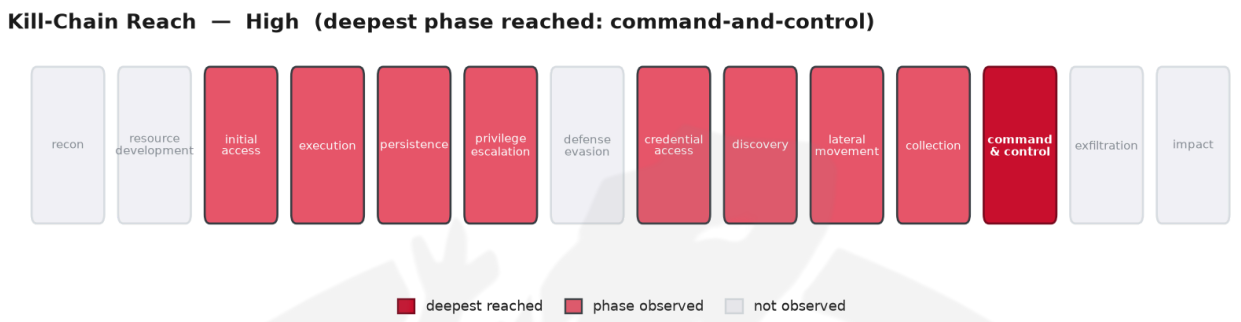
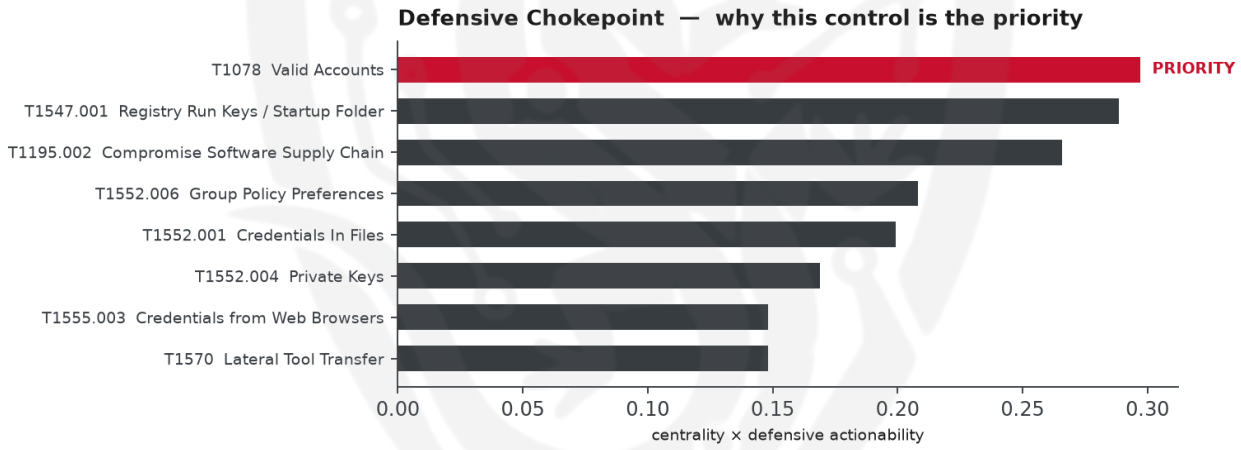
THREAT REPORT: TEAMPCP

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 TeamPCP, a threat actor who has compromised software dependencies and development tools, targeting the technology sector. The malware families used include rope.pyz, transformers.pyz, and managed.pyz. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's use of valid accounts is a key technique in their attack chain.

Threat Overview

TeamPCP, the attributed threat actor, has been observed using various malware families, including rope.pyz, transformers.pyz, and managed.pyz, to compromise software dependencies and development tools. The targeted sector is technology, although the specific country targeted is not specified. The threat actor's techniques include compromising software dependencies, using password managers, and exploiting native APIs.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including compromising software dependencies, using valid accounts, and exploiting native APIs. The priority technique is T1078 Valid Accounts, which is the graph chokepoint. To mitigate this threat, the priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence 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)

- T1195.001 Compromise Software Dependencies and Development Tools
- T1555.005 Password Managers
- T1106 Native API
- T1005 Data from Local System
- T1555.003 Credentials from Web Browsers
- T1552.004 Private Keys
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1552.006 Group Policy Preferences
- T1087.004 Cloud Account
- T1547.001 Registry Run Keys / Startup Folder
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1573.002 Asymmetric Cryptography
- T1570 Lateral Tool Transfer
- T1059.006 Python
- T1071.001 Web Protocols
- T1021.001 Remote Desktop Protocol
- T1552.007 Container API

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2973).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3975; 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
RedCurl	0.3975
APT33	0.3649
Inception	0.3631
APT18	0.3629
Dark Caracal	0.3532

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	t[.]m-kosche[.]com
Domain	check[.]git-service[.]com
URL	hxxps://check[.]git-service[.]com/rope[.]pyz
URL	hxxps://t[.]m-kosche[.]com/rope[.]pyz
Hash	069ac1dc7f7649b76bc72a11ac700f373804bfd81dab7e561157b703999f44ce
Hash	7d80b3ef74ad7992b93c31966962612e4e2ceb93e7727cdbd1d2a9af47d44ba8
Hash	877ff2531a63393c4cb9c3c86908b62d9c4fc3db971bc231c48537faae6cb3ec
Hash	aeaf583e20347bf850e2fabdcd6f4982996ba023f8c2cd56bbd299cfd56516f5

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** TeamPCP used T1195.001 Compromise Software Dependencies and Development Tools here as an alternative initial-access technique.
- **Projected pivot:** T1195.001 Compromise Software Dependencies and Development Tools (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

TeamPCP could pivot to compromising software dependencies and development tools, such as T1195.001, to maintain access and achieve their objectives if they had been relying on valid accounts that are now blocked. They may attempt to exploit vulnerabilities in software dependencies or manipulate development tools to regain a foothold. To counter this potential move, the defensive control of verifying software supply chain integrity, including signing and maintaining a Software Bill of Materials (SBOM), pinning and monitoring third-party dependencies, and update channels, would likely be an effective measure.

- **Defensive countermeasure:** Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels.