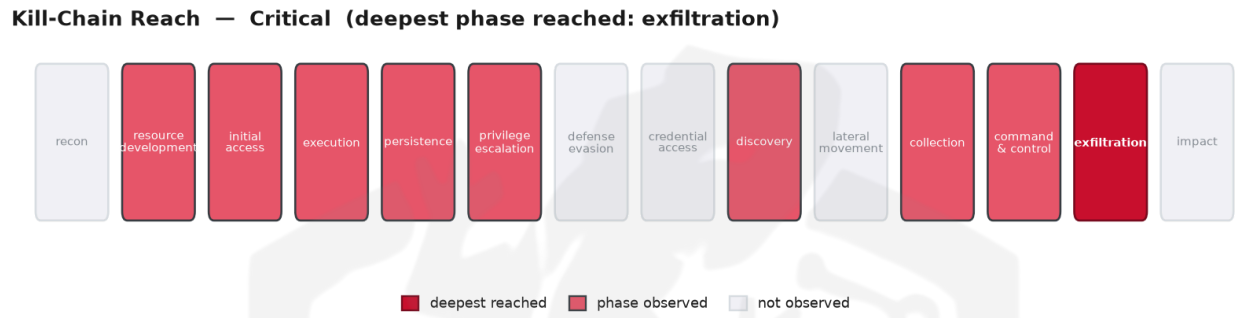
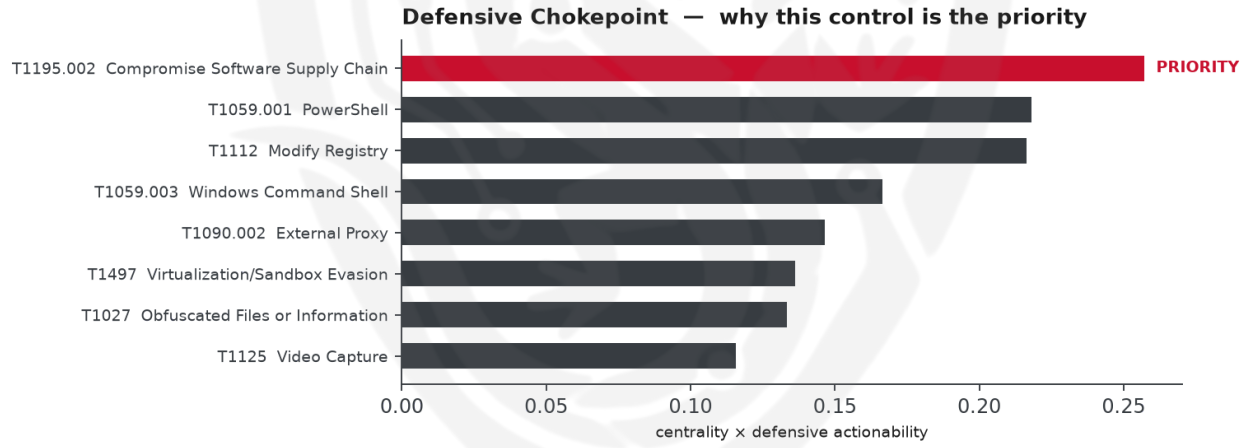
THREAT REPORT: UNKNOWN_ADVERSARY MALICIOUS NUGET TOOLS

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 the distribution of malicious NuGet tools that pose as game cheats to drop a Windows host-surveillance payload, specifically the pepesoft.exe malware family. The targeted country and sectors are unknown. Priority should be given to verifying software supply chain integrity to prevent further compromise. The threat actor's use of compromised software supply chains allows for widespread distribution of malware.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, utilizes the pepesoft.exe malware family to conduct surveillance on compromised Windows hosts. The absence of a central CVE or targeted country information limits the understanding of the attack's scope. However, the techniques employed by

the threat actor, including screen capture, system owner/user discovery, and exfiltration over web services, indicate a high level of sophistication.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with the compromise of the software supply chain, followed by various system discovery and surveillance techniques. The priority technique is T1195.002 Compromise Software Supply Chain, which serves as the initial entry point for the malware. To mitigate this threat, 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, 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)

- T1113 Screen Capture
- T1033 System Owner/User Discovery
- T1548.002 Bypass User Account Control
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1608.001 Upload Malware
- T1567 Exfiltration Over Web Service
- T1112 Modify Registry
- T1090.002 External Proxy
- T1125 Video Capture
- T1016 System Network Configuration Discovery
- T1497 Virtualization/Sandbox Evasion
- T1057 Process Discovery
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1614 System Location Discovery
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1027.002 Software Packing

- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1569.002 Service Execution
- T1124 System Time Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1195.002 Compromise Software Supply Chain (centrality 0.2573).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4545; 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
Medusa Group	0.4545
BlackByte	0.4222
APT38	0.4104
Gamaredon Group	0.3955
Threat Group-3390	0.3953

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	s3[.]ru-3[.]storage[.]selcloud[.]ru
Domain	bots[.]pepesoft[.]ru
Domain	grandrp[.]su

Type	Indicator
URL	hxxps://s3[.]ru-3[.]storage[.]selcloud[.]ru
Hash	d5385526f2f3e52c7d96087611c6cd4e479bf61828400efdb3ca09406d981609
Hash	9a2091e6625fc11cfd8f39c17aa271604e66322ee045028946274b988103e35b
Hash	900ddb81d27e03967209fee4d17d13deb68eef0e1f10936eb520ca10575cb49e
Hash	ab58a90eb3682c6dc3389cd700a64f68a19c0dac3d0fa8e3df97ae041f96d4e1
Hash	e6e1049158ceb1971c61388349c81fa6047a7aecb4ff2089ef54a50dcc35dbc0
Hash	d9f7ca9f93a7d188d51db308877b15d0beae932ca0bf4705384fbedf54b454c1
Hash	4d13f1136b13c871c65141b77ec7208488334ac4be511800196adcd328666305
Hash	011926de3d0cc2b970627b9bf0de003e731f8576602dff756d2ab54a9de61972
Hash	79c09e1ffb4804c14ff27d41ec08d4390455c92d65717be0aeeec2697297d76a
Hash	5f3a9ebf7039097b3cdbca8609b5b68af07eeb1dbf716ba2817a97fc7c543854
Hash	23808e7638f7a00b1ef9b9f4ca524f8a46cf63be6f6b79fec8e4a3fd1cc82a1e
Hash	e8c2618565aa31d7ffe909ebc99040bafcc0ea8df7f5d92fa673bb7ffacb14c9
Hash	6eefe9d5f030d403c72bd4e4caf5bbb9dbc2bd5e15ebb07de153494f458e5eb9
Hash	8ab256dd839aec6638cd46374f4a6664e534b9341bbcdfd9b763e5a27c51ddb7
Hash	6c1f828e4d8395dde8293868c65ba8d86b3b9672ebbbb16e932624706d37d832
Hash	6cbd4bc491deb11040e2b2f91b0b4e129af551a802fc78cb42e0e985297ef44c
Hash	5d9843126db4223dc2a8a9cd4a627286fe1a6345e33b28e9c98b5fe56fe89da6
Hash	c9f3e7766dbe728d84a1243447faa5f5eba0645bf13089074d128ea7663e7f5b
Hash	a2a5e473dba85959b21b7e8a184bc255d5f2dacdf7411b91d212fb1217d2518b
Hash	ba7fc544994f126cb7485ce52d265d2f32e93c4f1ea1fcd6fcdee3918f271979
Hash	567952daf0ab7b36b017aac9963791188dea0fbf2e99c7cc6f6652ee540f4840
Hash	cc853b3e4504c890d275ac2327f18acd7e4c5b99ca056181f3f5694781f2cf45
Hash	476c6f36a22156e53548a87291989a21d6c905dcbd9e1bf68ff5bc12e5c8bb07
Hash	774e40046f353e3f916f39e3d13d6499da35705a479cfb89288c21017aaf5461

Type	Indicator
Hash	23e4d8af5425dae022793450190c8d30809b2986dd879eb4bff557cdacf49c86
Hash	95577498d23fe750221a5badfc25b5e9f020dcf4d80c79a019b090e3c3b0a32a
Hash	2a4fed04d792b9c2fdf9c1456a08ca23eda5fef50c0b409ab294ad489e12d801
Hash	7e42d25e707d29d5d185a4c5dc71019f744e88a30b66bbf06949194ff32dbc48
Hash	d59e1914d76499fa51bf861f418c84bda0b48913dc39bd2e73756e326e4ccbb0
Hash	17b1d836c2f15a97be0350879943b04e14bc076cf09e31df0d73258ee10f7e7c
Hash	01d2afea0f2201a3b59765a1a60ba324ff4b8fdd25f23a0e05824b97f195b27c
Hash	21b4be57bd3743738393f44d9464e212
Hash	5bd610283d9c4b4ead45ca4f1b35d0f4
Hash	d6b2c2d2851a63b90e7210a943d0fdf6
Hash	642bfeae924b9d4e6ed642b5946ac8e745cfc531

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:** T1195.002 Compromise Software Supply Chain (initial-access)
- **Observed here:** T1195.002 Compromise Software Supply Chain was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1566 Phishing (initial-access)
- **Basis:** 9 of 170 documented groups that use Compromise Software Supply Chain also use Phishing (conditional 0.82, lift 1.4, i.e. ~1.4x base rate). Strongest same-tactic neighbour.

The actor could pivot to T1566 Phishing to maintain their objective by attempting to deceive users into divulging sensitive information or gaining initial access, potentially leveraging social engineering tactics to bypass the blocked software supply chain compromise. This approach may allow the actor to regain momentum in their campaign, exploiting human vulnerabilities rather than relying on compromised software. The defensive control to counter this potential pivot would be to enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Also plausible (same tactic): T1133 External Remote Services (n=7, lift 3.9), T1190 Exploit Public-Facing Application (n=7, lift 2.5)

Detection and hardening for the pivot (T1566 Phishing)

- **Telemetry:** Email security gateway logs; Endpoint (Office child processes); Proxy/DNS
- **Detect:**
  - Office apps (winword/excel) spawning script or LOLBIN child processes
  - Mark-of-the-Web bypass; ISO/IMG/LNK/HTML-smuggling attachments detonating
  - First-contact domains and newly registered domains in mail links
- **Harden:**
  - Attachment sandboxing; block high-risk types (iso, img, lnk, htm) at the gateway
  - Attack-surface-reduction rules for Office child processes; user reporting button
- **MITRE:** M1049 Antivirus/Antimalware, M1031 Network Intrusion Prevention, M1017 User Training, M1021 Restrict Web-Based Content · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic