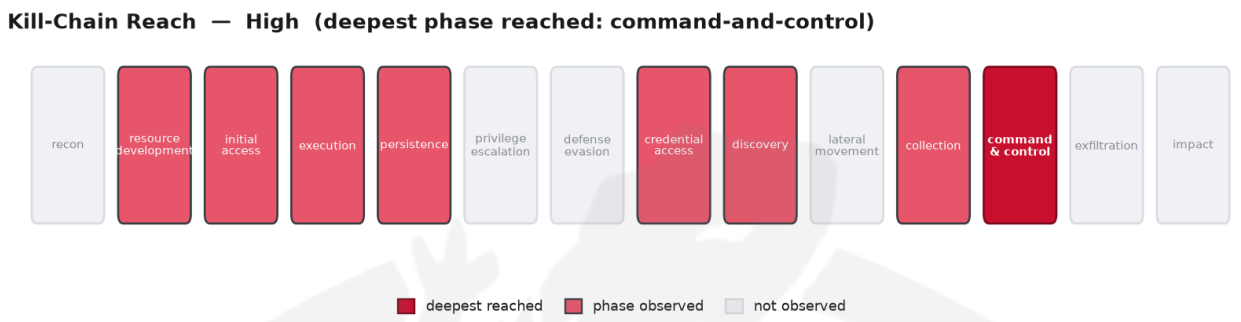
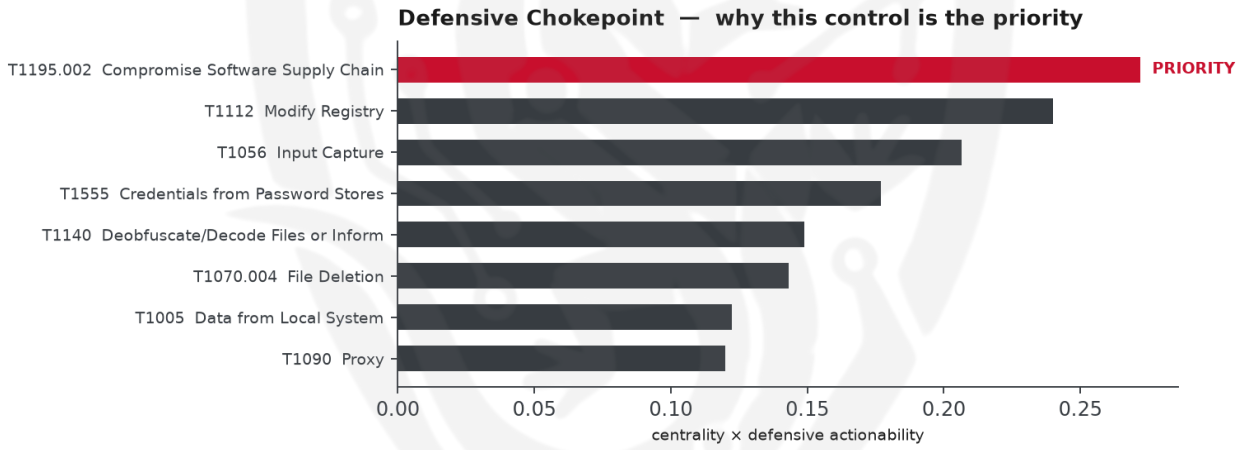
THREAT REPORT: APT37

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 APT37, a threat actor that has compromised a gaming platform in a supply-chain attack. The malware families used in this attack include BirdCall and ROKRAT - S0240. Priority should be given to verifying the software supply chain integrity to prevent further compromises. The attack highlights the importance of securing the software supply chain to prevent such attacks.

Threat Overview

The threat actor, attributed to APT37 by the source, has used the BirdCall and ROKRAT - S0240 malware families to compromise a gaming platform. The victimology and targeted country are not specified due to insufficient data. The central CVE exploited in this attack is also not available due to insufficient data.

Attack Chain and Priority Control

The observed techniques used by the threat actor include establishing accounts, network service discovery, virtualization/sandbox evasion, and compromising the software supply chain. The priority technique in this attack chain is T1195.002 Compromise Software Supply Chain, which is the graph chokepoint. The priority control to mitigate this attack 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 in this attack. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1585 Establish Accounts
- T1046 Network Service Discovery
- T1497 Virtualization/Sandbox Evasion
- T1480.001 Environmental Keying
- T1083 File and Directory Discovery
- T1082 System Information Discovery
- T1555 Credentials from Password Stores
- T1005 Data from Local System
- T1587.001 Malware
- T1056 Input Capture
- T1140 Deobfuscate/Decode Files or Information
- T1584.004 Server
- T1070.004 File Deletion
- T1195.002 Compromise Software Supply Chain
- T1112 Modify Registry
- T1113 Screen Capture
- T1090 Proxy
- T1608.001 Upload Malware
- T1027 Obfuscated Files or Information
- T1059.003 Windows Command Shell
- T1115 Clipboard Data

Analytical Scores

- Priority technique (graph chokepoint): T1195.002 Compromise Software Supply Chain (centrality 0.2721).

- 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 0.3724; 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
OilRig	0.3724
Sandworm Team	0.362
Contagious Interview	0.3588
Group5	0.3571
Windigo	0.3571

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	1980food[.]co[.]kr
Domain	cndsoft[.]co[.]kr
Domain	colorncopy[.]co[.]kr
Domain	sejonghaeun[.]com
Domain	www[.]inodea[.]com
Domain	www[.]lawwell[.]co[.]kr
Domain	inodea[.]com
Domain	sqgame[.]com

Type	Indicator
Domain	sqgame[.]com[.]cn
Domain	www[.]sqgame[.]net
Domain	xiazai[.]sqgame[.]com[.]cn
Hash	21ca0287ec5eaee8fb2f5d0542e378267d6ca0a6
Hash	2c6cc71b7e7e4b28c2c176b504bc5bdb687c4d41
Hash	5b70453ab58824a65ed0b6175c903aa022a87d6a
Hash	d9a369e328ea4f1b8304b6e11b50275f798e9d6b
Hash	f9f6c0184cee9c1e4e15c2a73e56d7b927ea685b
Hash	7331602726f61959d8f0e7820d457370
Hash	03e3ece9f48cf4104aafc535790ca2fb3c6b26cf
Hash	33d887ca2e57fa03fc807dfba5376bf96718ee88f56e90d95ee4896a2c019bd0
Hash	23a1eacad84be4f2c5830755b1948582
Hash	3d3d2dc34f01bcf890f185a5421836c7
Hash	72ac1287a8d71b27c437ec1f379ab506
Hash	a0830ce48537ba052f1d3b905d11a5bf
Hash	a48b62e55a692bf6d1046d2be64d7150
Hash	01a33066fbc6253304c92760916329abd50c3191
Hash	2b81f78ec4c3f8d6cf8f677d141c5d13c35333af
Hash	409c5acaed587f62f7e23da47f72c4d9ec3144d9
Hash	59a9b9d47ae36411b277544f25ad2cc955d8dd2c
Hash	7356d7868c81499fb4e720f7c9530e5763b4c1d0
Hash	95bdb94f6767a3cce6d92363bbf5bc84b786bdb0
Hash	b06110e0feb7592872e380b7e3b8f77d80dd1108
Hash	fc0c691db7e2d2bd3b0b4c1e24d18df72168b7d9
Hash	185633e5dbe9235fc7e6a1ccb8631650afefd8f7da88c5c07d9b99ea38159822

Type	Indicator
Hash	415b253a81e67c8c860a97c73edc9017ce732b3c025d943d3b1a445b4ac82822
Hash	5aa7afd790481ad98357636fa4d9927ae01111409c8d7ce69998d2485c1d5e6f
Hash	95cda8431419f77407484ab72dc1e356421dcd801eccabe8869f77ee0eb58eb2
Hash	dfa9c6adac98311d0f62e0eeecb947d92f7bda41ddf4ce9a6f9e20af7990422d
Hash	a8fe823d451d636d0a0366c0629ef5c3

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.

If APT37's software supply chain compromise efforts are blocked, they could pivot to phishing, potentially using T1566 to trick users into divulging sensitive information or installing malware, which may allow them to maintain their objective of gaining access to the target network. This shift in tactics may involve crafting convincing emails or messages that exploit user trust, which would likely be a key factor in the success of the phishing attempt. To counter this potential move, the defensive control of enabling attachment sandboxing and link rewriting, blocking macro-enabled Office docs from the internet zone, and deploying a user report-phish button should be implemented.

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