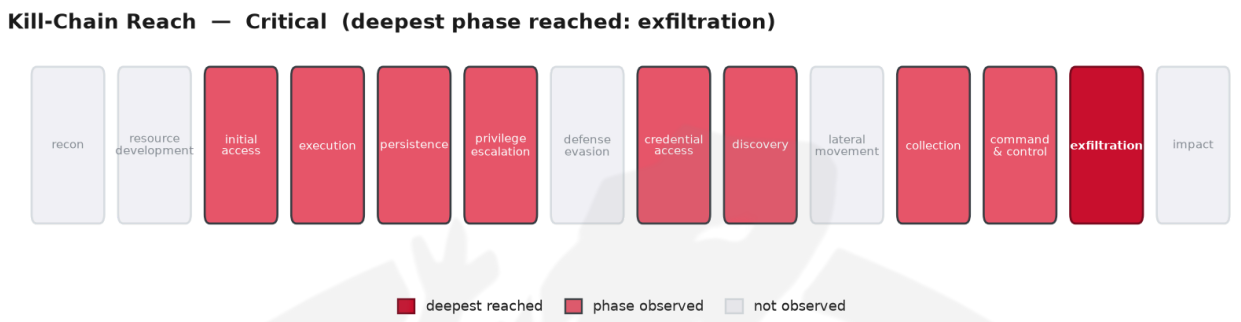
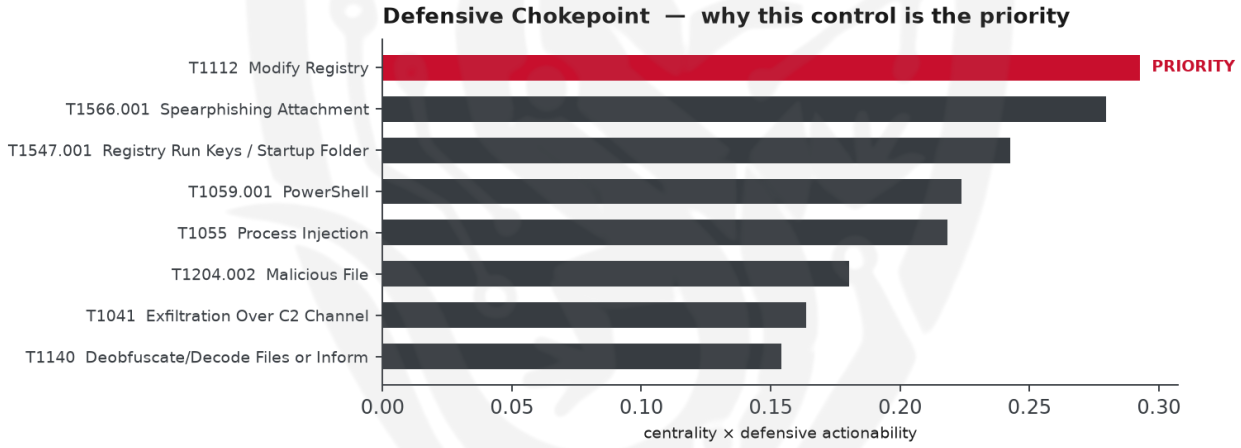
THREAT REPORT: APT37 NARWHALRAT CAMPAIGN

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, who has been observed leveraging NarwhalRAT and ROKRAT malware to target unspecified countries and sectors. The threat actor utilizes various techniques, including phishing and dead-drop C2, to gain access to systems. Priority should be given to monitoring sensitive registry keys for modification to prevent further exploitation. The operational risk band for this threat is Critical, as it reaches the stage of exfiltration.

Threat Overview

APT37, the attributed threat actor, has been observed using the NarwhalRAT and ROKRAT malware families. Although the central CVE is insufficient, the threat actor exploits various vulnerabilities to carry out their attacks. The victimology of this campaign is not well-defined due to insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques used by APT37 form a complex attack chain, involving scheduled tasks, screen capture, keylogging, and data exfiltration over C2 channels. The priority technique in this chain is T1112 Modify Registry, which serves as a critical chokepoint. To mitigate this threat, the recommended priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on providers such as Hostway IDC, KT Cloud Co. Ltd, and LG Dacom Corporation, as observed by third-party sources. However, there are no malware families corroborated by abuse.ch, and no indicators have reached an 80% confidence level on 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)

- T1053.005 Scheduled Task
- T1113 Screen Capture
- T1056.001 Keylogging
- T1025 Data from Removable Media
- T1204.002 Malicious File
- T1497.001 System Checks
- T1566.001 Spearphishing Attachment
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3082).

- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.512; 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
BRONZE BUTLER	0.512
Dark Caracal	0.5112
Gamaredon Group	0.5061
APT39	0.4815
Silence	0.4814

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	Context
IP	211[.]239[.]157[.]126	AbuseIPDB 0% (KR) · AS9952 Hostway IDC
IP	218[.]150[.]78[.]198	AbuseIPDB 0% (KR) · AS152232 KT Cloud Co. Ltd
IP	121[.]254[.]222[.]10	AbuseIPDB 0% (KR) · AS3786 LG Dacom Corporation
IP	121[.]254[.]222[.]80	AbuseIPDB 0% (KR) · AS3786 LG Dacom Corporation
IP	218[.]150[.]78[.]231	AbuseIPDB 0% (KR) · AS152232 KT Cloud Co. Ltd
IP	61[.]100[.]9[.]206	AbuseIPDB 0% (KR) · AS9952 Hostway IDC

Type	Indicator	Context
Domain	crwellfood[.]com	
Domain	fe01[.]co[.]kr	
Domain	novel21[.]co[.]kr	
Domain	webhostingkorea[.]com	
Domain	www[.]novel21[.]co[.]kr	
URL	hxxp://www[.]novel21[.]co[.]kr/data/editor/2110/index[.]php	
Hash	3715092aa00f380cefe8b4d2eddb7d08	
Hash	7cef19f9c4480adac0cd4702ff98f46c	
Hash	7eb9cee1f696727752169f25cf79a338	
Hash	b6b0602310bb2d4360c52685119aac1b	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.