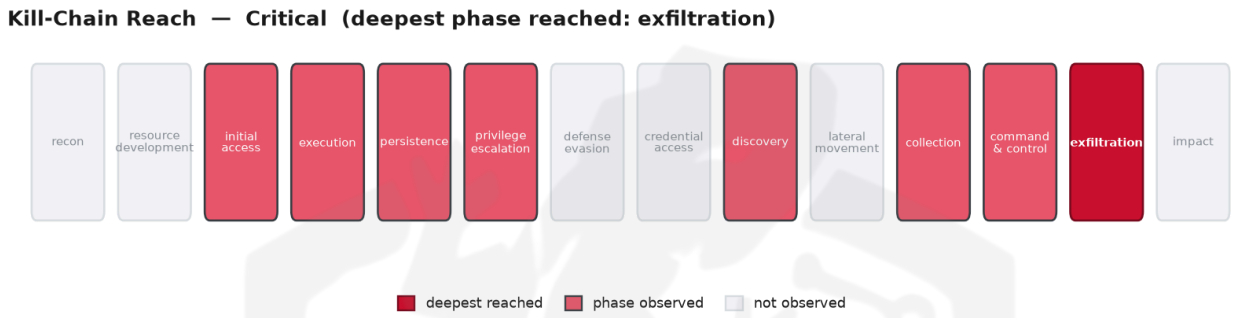
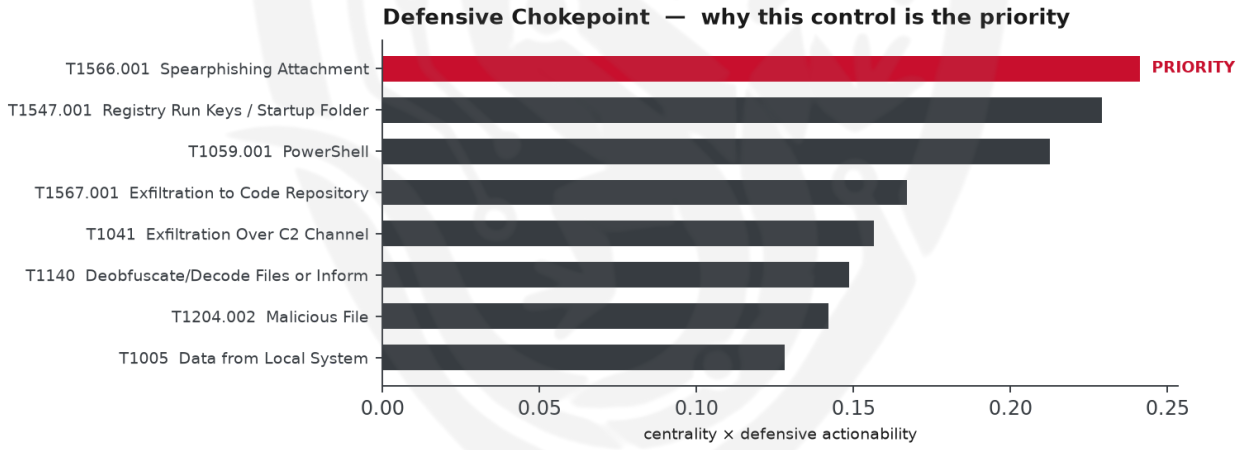
THREAT REPORT: KIMSUKY'S INTEGRATING AI INTO ATTACK OPERATIONS

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 Kimsuky, a threat actor that has been targeting the Government, Defense, and Finance sectors. The observed cluster of activity involves the use of AsyncRAT malware, although the central CVE exploited is currently insufficient. Priority should be given to defensive actions that focus on email attachments and executable contents. The threat actor's ability to exfiltrate data poses a critical operational risk.

Threat Overview

Kimsuky, the attributed threat actor, utilizes the AsyncRAT malware family to target organizations in the Government, Defense, and Finance sectors. The exact vulnerability exploited is not specified due to

insufficient data. The threat actor's tactics involve various techniques, including those related to data staging, encryption, and exfiltration.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, standard encoding, and symmetric cryptography, ultimately leading to data exfiltration. The priority technique identified is T1566.001 Spearphishing Attachment, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to: Sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button.

Infrastructure and Corroboration

The malicious infrastructure associated with this activity is hosted by providers such as Daou Technology and LG Dacom Corporation, as observed in third-party enrichment data. However, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB 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)

- T1053.005 Scheduled Task
- T1132.001 Standard Encoding
- T1074.001 Local Data Staging
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1083 File and Directory Discovery
- T1567.001 Exfiltration to Code Repository
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window
- T1027.002 Software Packing
- T1071.001 Web Protocols

- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2413).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.561; 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
Higaisa	0.561
Inception	0.5544
APT19	0.5398
BRONZE BUTLER	0.5188
Confucius	0.5091

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	112[.]216[.]9[.]171	AbuseIPDB 0% (KR) · AS3786 LG Dacom Corporation
IP	27[.]102[.]137[.]126	AbuseIPDB 0% (KR) · AS45996 Daou Technology
IP	27[.]102[.]138[.]44	AbuseIPDB 0% (KR) · AS45996 Daou Technology
IP	27[.]102[.]137[.]159	

Type	Indicator	Context
Hash	30d5f17d5e3f85be18220a7cab0b9fff	
Hash	a4f72ce8b5736fe3ca2083cfe21bd51697f12e900e307c357cb8523b8f86e3ec	
Hash	22180919f562fb9f6e50d7f20b2eb3f94eb009c212b74b45cf77659fe8274d5b	
Hash	4453b9e985f452365995c399f5292c92764570f03e6a066d7845320dd4ad09a1	
Hash	aa9d5dd632bb90addca480eaa5ff4382	
Hash	5746f3e78351439caebfa3721e8feea36b67263f	
Hash	4b0358c7e4afa54bc489a6199cca132b5f4a330892eb15bf06c0c4da9e020df2	
Hash	9be8f2be7ad882e8423c269a0540b7c73d6470311ddfcfcd318ff9d1983e2935	
Hash	e34d73a1da492c9a79a9729f2f7d9d4b5a2448f44934bd5552bd0bbbe1586767	
Hash	7bc61d1bbc90d66d9988fd3baacd7834b1d2dfefe6d4ac999a194bccb9ba7dfc	
Hash	02ebc2356f9f700bbdac444cdefa0da2	
Hash	0d8ceb7dea7d471afa2f8e753b13d2d6	
Hash	1f378c0efc13669dada1fe340c6837bd	
Hash	2669731cb5ff664dfb5fbfc37637876d	
Hash	2ab3df4762fbde5d86e99a1ad147850e	
Hash	2e76d5316663a3dc472398b1c01cb9a8	

Type	Indicator	Context
Hash	2eb77109cce1e8afca6245c2963e52a6	
Hash	302725413076d1aeaee2d7f2b3692646	
Hash	30792a0c0dfad55fb2b19d3e30e9a7d4	
Hash	37cec428257cd41153cf43d7f1a12652	
Hash	3b9d40f3d620ec87960b4350d42ccc03	
Hash	3e2110d233d4543830e14c78d53900f4	
Hash	422a221851ea6ad15f53cd3aea51c8af	
Hash	49bdbe7e6cbb88842afcce3a9fe60e9b	
Hash	4d87fef16790cbe1df72007d99149665	
Hash	5577fffb5b5acd3771ef9dc696498f1e	
Hash	5af95590a33b9bc64d95808f1fc71b78	
Hash	5c5672bb14e1d2f07a8318ffec19b213	
Hash	6add815cd61d6514f81a23ab8c23405a	
Hash	73ff669fc282653bd6c42cf87ade9337	
Hash	7f12fa589f56f6203c692715b3958d30	
Hash	8406075af0a1e9ec09bafdc0de01f138	

Type	Indicator	Context
Hash	8c859a03814443c6f0da341ee594c352	
Hash	a1c07ac866fb6b388e38c6bb1d4bbe94	
Hash	a343d8bcf02a0554fa271452a512f3ce	
Hash	a435292106026e257789036a70ee1a14	

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

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:** T1566.001 Spearphishing Attachment (initial-access)
- **Observed here:** T1566.001 Spearphishing Attachment was the initial-access control point here; the pivot escalates to execution, drawn from Kimsuky's own documented ATT&CK repertoire.
- **Projected pivot:** T1106 Native API (execution)
- **Basis:** documented in Kimsuky's own ATT&CK repertoire, and disproportionately paired with Spearphishing Attachment across tracked groups (lift 1.6, ~1.6x base rate). Their move, not a generic one.

Kimsuky could pivot to using T1106 Native API to bypass security controls and maintain access, as this technique allows them to interact directly with the operating system, potentially evading detection by traditional signature-based security tools. By leveraging Native API, Kimsuky may attempt to execute malicious code or hide their activities, taking advantage of the lack of visibility into API calls. To counter this, the mandated defensive control is to Enable EDR API-telemetry; alert on unusual direct Native API use from non-system processes.

Also plausible (same tactic): T1559 Inter-Process Communication (n=13, lift 1.6)

Detection and hardening for the pivot (T1106 Native API)

- **Telemetry:** EDR API/syscall telemetry; Sysmon (process access + image load)
- **Detect:**
  - Direct/indirect syscalls bypassing usermode hooks; VirtualAllocEx/WriteProcessMemory/CreateRemoteThread from unusual parents
  - Sysmon 8 (CreateRemoteThread), 10 (process access to lsass/other), 25 (process tampering/hollowing)

    - Execution from unbacked (private, non-image) memory regions
- **Harden:**
    - EDR with kernel-level telemetry resilient to usermode unhooking
    - Application control on unsigned code; behavioural detection of injection sequences over single API calls
- **MITRE:** M1040 Behavior Prevention on Endpoint, M1038 Execution Prevention · DS0009 Process, DS0011 Module, DS0017 Command