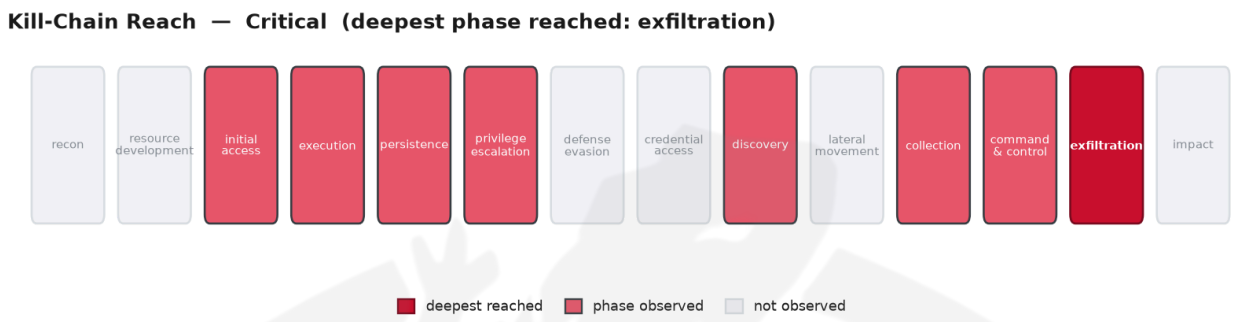
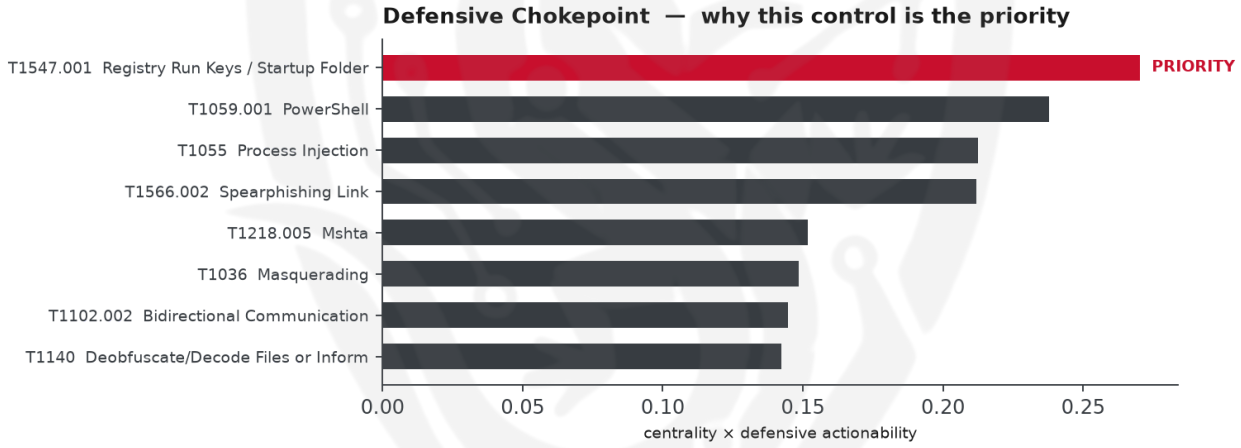
THREAT REPORT: KIMSUKY

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 leveraging the KimJongRAT and MeshAgent malware families to target Japan. The observed cluster of activity prioritizes exploiting system vulnerabilities, with a focus on maintaining persistence and exfiltrating data. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The threat actor's tactics, techniques, and procedures (TTPs) indicate a high level of sophistication, warranting immediate attention to prevent further compromise.

Threat Overview

Kimsuky, the attributed threat actor, utilizes the KimJongRAT and MeshAgent malware families to compromise Japanese targets. Although the central CVE is insufficient, the threat actor employs various techniques, including system owner/user discovery, spearphishing, and process injection, to achieve their

objectives. The victimology suggests a focus on Japanese entities, with the threat actor seeking to exfiltrate sensitive data.

Attack Chain and Priority Control

The observed techniques employed by the threat actor form a complex attack chain, involving system information discovery, malicious file execution, and symmetric cryptography. The priority technique, T1547.001 Registry Run Keys / Startup Folder, serves as a critical chokepoint, enabling the threat actor to maintain persistence on compromised systems. To mitigate this threat, the priority control is to "Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

The malicious infrastructure is hosted on GWY IT Pty Ltd, as observed by third-party sources. Although abuse.ch corroborates the presence of unknown malware, AbuseIPDB flags do not indicate high-confidence malicious activity, with 0 indicators at or above 80% confidence. These findings, attributed to their respective sources, provide additional context to the threat landscape.

Technical Appendix

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

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

- T1033 System Owner/User Discovery
- T1218.011 Rundll32
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1055 Process Injection
- T1218.005 Mshta
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1102.002 Bidirectional Communication
- T1567.002 Exfiltration to Cloud Storage
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2846).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5667; 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
LazyScripter	0.5667
ZIRCONIUM	0.5634
Inception	0.5323
Windshift	0.5217
APT37	0.5196

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Unknown malware.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	104[.]200[.]67[.]46	AbuseIPDB 0% (US) · AS199959 GWY IT Pty Ltd
Domain	lutkdd[.]corpsecs[.]com	Unknown malware

Type	Indicator	Context
Domain	pxqtkc[.]corpsecs[.]com	
Domain	googleoba[.]servequake[.]com	
URL	hxxp://googleoba[.]servequake[.]com:8443/agent[.]ashx	
URL	hxxps://lutkdd[.]corpsecs[.]com	
URL	hxxps://pxqtkc[.]corpsecs[.]com	
Hash	9758e76b601798a30d903bf05052a53df80451e5c156548ce9da828f608b6470	
Hash	221a39856b37e3c682f62427f1e6b965b36a2405764689c914672770a01a1fa9	
Hash	107b5aa3c4ef30b9b832e0a10b1efb1dcf433158bc6af8d890d66c0c9ed50d21	
Hash	e4ccb2328c06710a7f0254cb6315e1b106396b0ff525f9cf3eada6e85d285c1c	

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