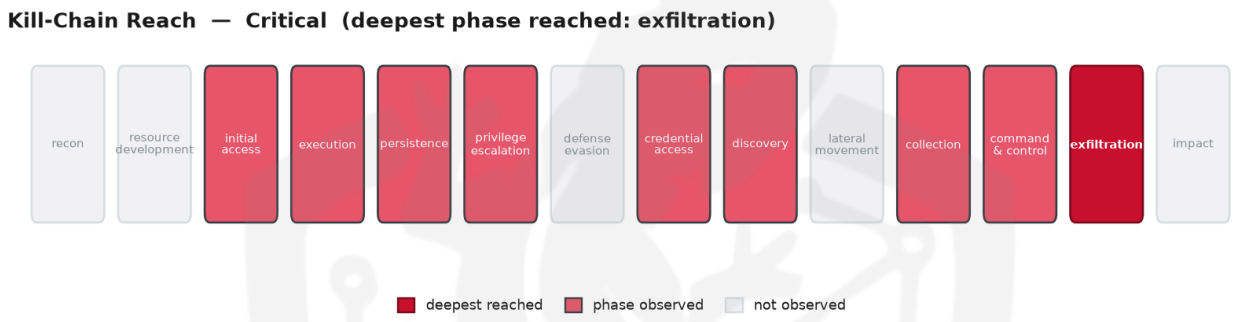
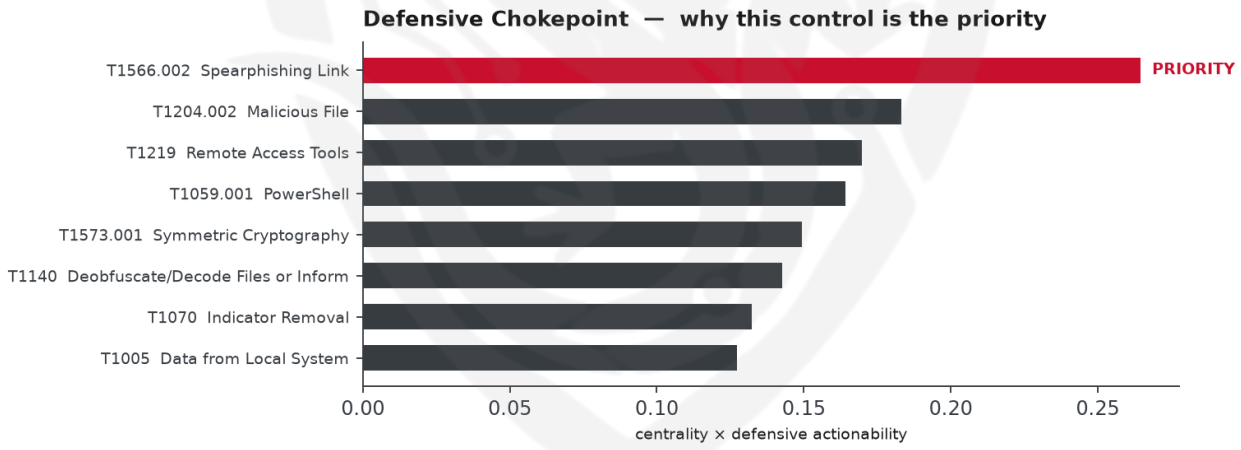
THREAT REPORT: KIMSUKY CAMPAIGN LEVERAGING LEGITIMATE REMOTE CONTROL TOOLS IN NORTHEAST ASIA

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

Kimsuky is observed abusing legitimate remote-control utilities to conduct operations targeting entities in Japan. The activity does not reference a specific malware family or CVE. The campaign’s primary delivery method is spearphishing links, and the source recommends hardening against social-engineering delivery across email, links, and voice/callback lures. Defensive teams should prioritize attachment sandboxing, link rewriting, macro restrictions, user training, a report-phish capability, and phishing-resistant MFA.

Threat Overview

The source attributes this activity to Kimsuky. No specific malware families or vulnerabilities were identified. The observed operations focus on victims located in Japan, with sector details not provided.

Attack Chain and Priority Control

The observed techniques follow a typical intrusion workflow: initial spearphishing link (T1566.002) delivers a malicious file (T1204.002), which is executed via PowerShell (T1059.001) or Windows Command Shell (T1059.003). The payload leverages remote-access tools (T1219) and scheduled tasks (T1053.005) to maintain persistence, while employing encoding (T1132.001), deobfuscation (T1140), and symmetric cryptography (T1573.001) to hide its activity. System and credential discovery (T1082, T1083, T1012, T1518.001) enables data collection (T1114, T1005) and exfiltration over the C2 channel (T1041). The priority technique is **T1566.002 Spearphishing Link**, and the concrete control prescribed is:

Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA.

Infrastructure and Corroboration

According to the enrichment data, no hosting providers or ASN information were observed for the malicious infrastructure. Abuse.ch did not corroborate any malware families, and AbuseIPDB reported no indicators with confidence ≥ 80 %. These observations are drawn directly from the third-party enrichment block.

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
- T1056.001 Keylogging
- T1548.002 Bypass User Account Control
- T1114 Email Collection
- T1564 Hide Artifacts
- 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
- T1219 Remote Access Tools
- T1010 Application Window Discovery
- T1070 Indicator Removal
- T1083 File and Directory Discovery

- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1012 Query Registry
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1059.005 Visual Basic

Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.2646).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5029; 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	0.5029
Stealth Falcon	0.4792
RedCurl	0.4719
FIN4	0.4671
Cobalt Group	0.4587

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
URL	hxxp://103[.]249[.]117[.]183/receive[.]php
URL	hxxp://103[.]77[.]242[.]187/receive[.]php

Type	Indicator
URL	hxxp://160[.]187[.]147[.]119/any/app[.]vmd
URL	hxxp://160[.]187[.]147[.]119/any/attach[.]vmd
URL	hxxp://160[.]187[.]147[.]119/any/bimage[.]vmd
URL	hxxp://160[.]187[.]147[.]119/any/mnfst[.]vmd
URL	hxxp://160[.]187[.]147[.]119/any/sch[.]vmd
URL	hxxp://160[.]187[.]147[.]119/any/vpost[.]vmd
Hash	eb80f7bddb699784baa9fbf2941eaf4a
Hash	b9ad79eaf7a4133f95f24c3b9d976c72f34264dc5c99030f0e57992cb5621f78
Hash	df6abbfd20e731689f3c7d2a55f45ac83fbbc40b
Hash	a2191f29f58b9f0cb576b7459ed6680d
Hash	c08ea73bac08ea4f4665e9e0b0fdd2a8
Hash	c774b3980151881d9d546710126b5ded
Hash	cac69a696fc155717dabe641f22db0c9
Hash	d7dbce5d25aa483d9c5ec1223ed6bf6e
Hash	e7da02737751f2f171aed28694b9554e
Hash	e8aaa4f579e6be788929d3548b31bf6d
Hash	f3620e42e9c726c65ea7e14e3bf35464
Hash	f6f7a94c11ea0ee01cbbe674cfac7851

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:** T1566.002 Spearphishing Link (initial-access)
- **Observed here:** T1566.002 Spearphishing Link 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 Link across tracked groups (lift 1.6, ~1.6x base rate). Their move, not a generic one.

With T1566.002 Spearphishing Link blocked, Kimsuky could preserve the same objective by pivoting to T1106 Native API, a technique from Kimsuky's documented repertoire. Defensive countermeasure: 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