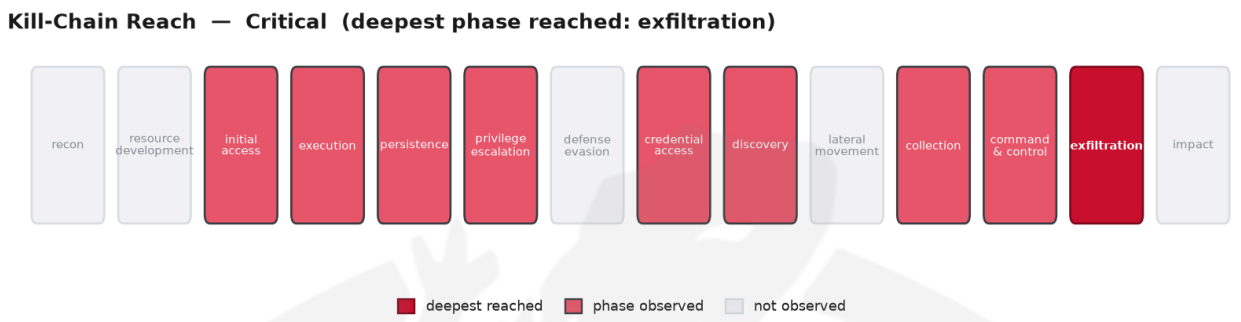
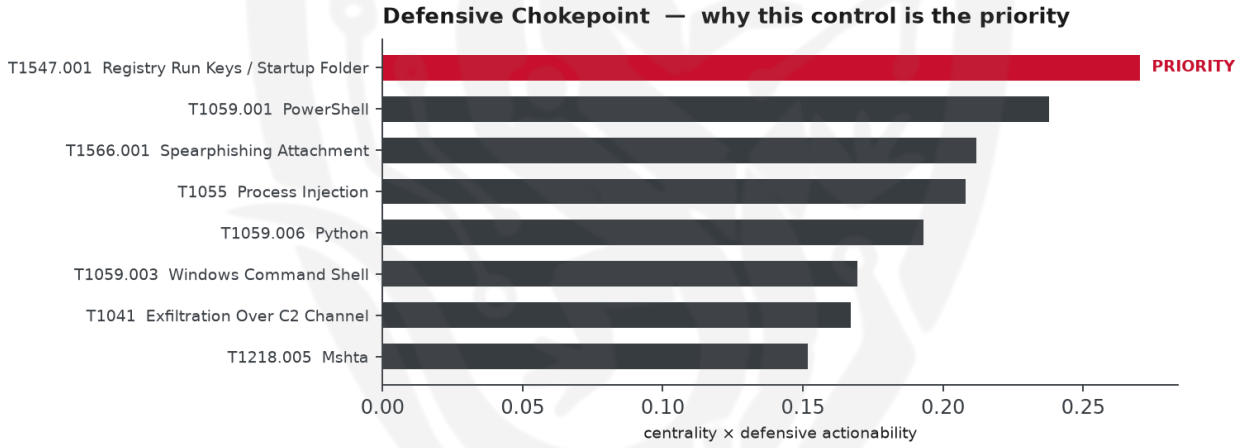
# THREAT REPORT: KIMSUKY APT ATTACKS

## 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 observed utilizing various malware families, including AutoIt backdoor, XenoRAT, PebbleDash, and PrxClient. The targeted country and sectors are not specified, but the actor's techniques suggest a high level of sophistication. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to prevent further malicious activity. The threat actor's ability to exfiltrate data poses a critical operational risk.

## Threat Overview

Kimsuky, the attributed threat actor, has been observed using a range of malware families, including AutoIt backdoor, XenoRAT, PebbleDash, and PrxClient. The central CVE exploited is not specified, but the actor's techniques include scheduled tasks, screen capture, keylogging, and malicious file execution. The

victimology is not well-defined, but the actor's use of spearphishing attachments and system information discovery suggests a targeted approach.

## Attack Chain and Priority Control

The observed techniques used by Kimsuky form a complex attack chain, involving initial access, execution, persistence, and exfiltration. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a chokepoint in the attack chain. 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

There is no observable hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by 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
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1055 Process Injection
- T1218.005 Mshta
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1059.006 Python
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer
- T1102.001 Dead Drop Resolver

## 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 0.5615; 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 |
|---|---|
| Confucius | 0.5615 |
| APT37 | 0.5579 |
| Rancor | 0.5571 |
| LazyScripter | 0.5425 |
| BRONZE BUTLER | 0.5364 |

## 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 | bohyeonsanvil[.]com |
| Domain | kumhosports[.]com |
| Hash | 03e4bef86f3e3e6ea23eb6f017af0c98 |
| Hash | 05c07339603994b36dcfefcce720d03d |
| Hash | 07bb21d28ae4ab07d62f8deb4343aaeb |
| Hash | 07ed2c9ed61b60078af0164f061696be |

| Type | Indicator |
| --- | --- |
| Hash | 0b1de625a89da12bd1fdd292b341bad3 |

## 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:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** T1547.001 Registry Run Keys / Startup Folder was the persistence control point here; the pivot is drawn from Kimsuky's own documented ATT&CK repertoire.
- **Projected pivot:** T1543 Create or Modify System Process (persistence)
- **Basis:** documented in Kimsuky's own ATT&CK repertoire, and disproportionately paired with Registry Run Keys / Startup Folder across tracked groups (lift 1.8, ~1.8x base rate). Their move, not a generic one.

The Kimsuky actor could pivot to creating or modifying system processes (T1543) to maintain persistence and evade detection, as this technique allows them to blend in with legitimate system activity and potentially exploit trusted system processes to achieve their objectives. By creating or modifying system processes, Kimsuky may attempt to bypass the blocked registry run keys/startup folder control, as system processes can be used to execute malicious code without relying on registry keys or startup folders. To counter this, the mandated defensive control of restricting service/daemon creation to admins and monitoring service and driver installs would likely be effective.

**Also plausible (same tactic):** T1098 Account Manipulation (n=12, lift 2.0), T1112 Modify Registry (n=17, lift 1.7)

**Detection and hardening for the pivot (T1543 Create or Modify System Process)**

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process