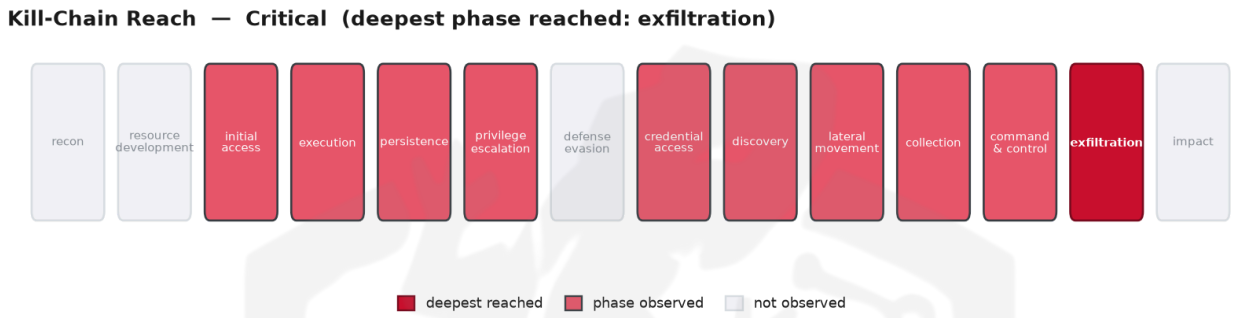
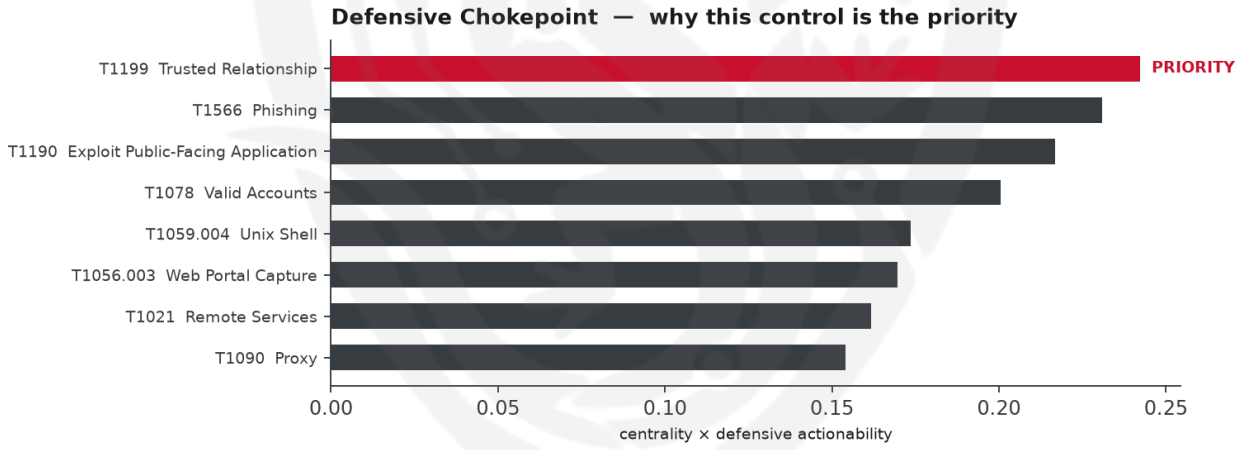
THREAT REPORT: KIMSUKY'S GOMIR FAMILY VARIANT ATTACK

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 targeting a South Korean groupware vendor using a new Gomir family variant. The attack involves various techniques, including screen capture, symmetric cryptography, and exfiltration over a command and control channel. Priority should be given to auditing and least-privileging trusted third-party connections to prevent further exploitation. The technology sector is the primary target of this attack.

Threat Overview

Kimsuky, the attributed threat actor, has been observed using a new Gomir family variant, along with other malware families such as HttpTroy, BirdTroy, and TrollStealer. The victimology of this attack is focused on

the technology sector, with the threat actor exploiting various techniques to gain access to sensitive information. The central vulnerability exploited in this attack is currently unknown.

Attack Chain and Priority Control

The observed techniques used by Kimsuky form a complex attack chain, involving initial access, execution, and exfiltration of sensitive data. The priority technique in this chain is T1199 Trusted Relationship, which is the graph chokepoint. To mitigate this threat, the priority control is to "Audit and least-privilege trusted third-party/B2B connections; monitor partner-account activity."

Infrastructure and Corroboration

The malicious infrastructure used in this attack is hosted on Interserver Inc, as observed by third-party sources. However, 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)

- T1113 Screen Capture
- T1132.001 Standard Encoding
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1053.003 Cron
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1021 Remote Services
- T1056.003 Web Portal Capture
- T1016 System Network Configuration Discovery
- T1090 Proxy
- T1083 File and Directory Discovery
- T1036.004 Masquerade Task or Service
- T1049 System Network Connections Discovery
- T1041 Exfiltration Over C2 Channel
- T1199 Trusted Relationship
- T1566 Phishing
- T1059.004 Unix Shell
- T1078 Valid Accounts
- T1102.002 Bidirectional Communication

- T1567.002 Exfiltration to Cloud Storage
- T1570 Lateral Tool Transfer
- T1070.004 File Deletion
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1543.002 Systemd Service

Analytical Scores

- Priority technique (graph chokepoint): T1199 Trusted Relationship (centrality 0.2423).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4417; 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
APT39	0.4417
ZIRCONIUM	0.4338
Sandworm Team	0.4188
Magic Hound	0.4188
MuddyWater	0.4188

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	163[.]245[.]195[.]172	AbuseIPDB 0% (US) · AS26666 Inter server Inc

Type	Indicator	Context
IP	69[.]10[.]50[.]165	AbuseIPDB 0% (US) · AS26666 Inter server Inc
Domain	commit[.]hanbiro[.]o-r[.]kr	
Domain	node828765[.]dwservice[.]net	
Domain	node896147[.]dwservice[.]net	
Domain	auth[.]samecloud[.]o-r[.]kr	
Domain	global[.]webjine[.]o-r[.]kr	
Domain	node449013[.]dwservice[.]net	
Domain	oauth[.]shacloud[.]o-r[.]kr	
Domain	oobe[.]webjine[.]o-r[.]kr	
Domain	www[.]ilskdeid[.]o-r[.]kr	
URL	hxxps://www[.]dwservice[.]net/	
URL	hxxp://auth[.]samecloud[.]o-r[.]kr/index[.]php	
URL	hxxp://www[.]ilskdeid[.]o-r[.]kr:8000/	
URL	hxxps://auth[.]samecloud[.]o-r[.]kr/index[.]php	
URL	hxxps://commit[.]hanbiro[.]o-r[.]kr/index[.]php	
URL	hxxps://global[.]webjine[.]o-r[.]kr/index[.]php	
URL	hxxps://oauth[.]shacloud[.]o-r[.]kr:8443	
URL	hxxps://oobe[.]webjine[.]o-r[.]kr/index[.]php	
Hash	84e9b066bebd49036b7fc71b5f5f8d83	
Hash	a452a860f973c7a43ea804c17e9427d2	

Type	Indicator	Context
Hash	aa61e76255a6e13313439655bc02bdf5	
Hash	b1c72139f2cdd9419562369fc6ced4fc	
Hash	bf215181b5140522137b3d4f6b73544a	
Hash	c2e37232556357944a04edf1dec3934b	
Hash	ca98a51cebdc802d255030b4baa44ca0	
Hash	dff787bce68c7653495f153c0534cb96	
Hash	e6c6fa32da47d9341b778bfa424abb4c	
Hash	e911f8f7c49476806ada37f3ebb7a28a	
Hash	3fb6111490cac9f5c4b34f9fed459f01c10d2314	
Hash	f3ed0bcc692555fea83c6556abaa5dc2b91bcb38	
Hash	01b1c767f62e48efeb86410fd014fed4295ccb084bfcd6d5b9197638b615a648	
Hash	073d9dd98a9ca3cd03901c31ba57811a1632e316923022640670ce00622cd8a9	

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:** T1199 Trusted Relationship (initial-access)
- **Observed here:** Kimsuky used T1078 Valid Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

Kimsuky could pivot to using T1078 Valid Accounts by attempting to compromise or obtain credentials for existing accounts, which may allow them to maintain access to the target network and continue their objectives. They may try to leverage these valid accounts to blend in with normal user activity, potentially evading detection. To counter this, the defensive control of Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons should be implemented.

Detection and hardening for the pivot (T1078 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account