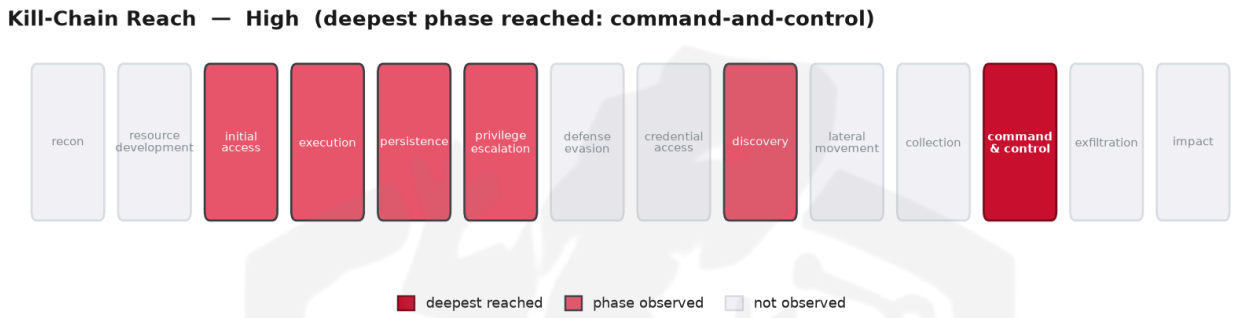
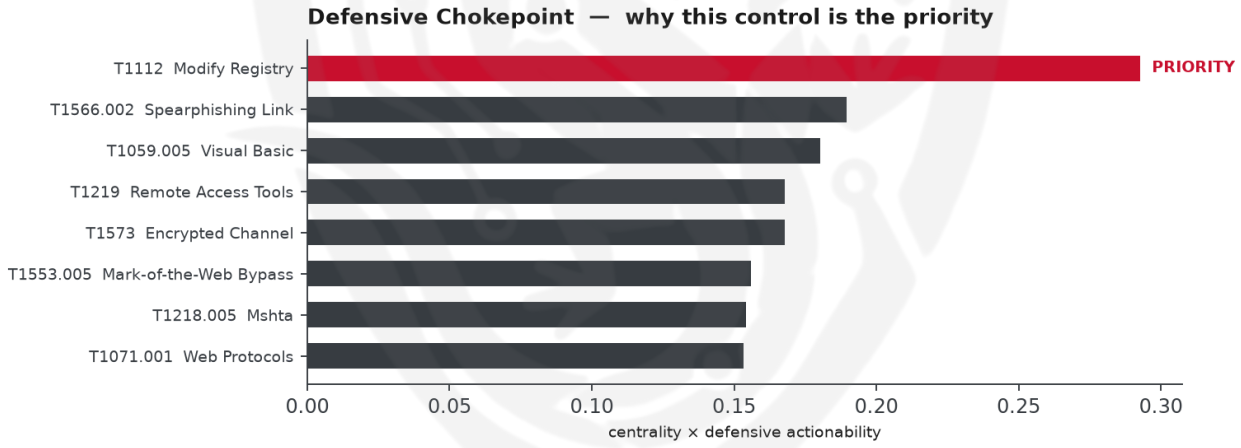
THREAT REPORT: UNKNOWN_ADVERSARY MALICIOUS VBS SCRIPTS

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 observed cluster of activity is distributing malicious VBS scripts via WhatsApp, targeting multiple countries including Australia, Brazil, and the United Kingdom. The malware families involved include ValleyRAT, gh0st RAT, Mydoor, and Moudoor. Priority should be given to monitoring sensitive registry keys for modification to defend against this threat. The threat actor's activities have been observed to reach a high operational risk band, indicating a significant command-and-control capability.

Threat Overview

The threat actor, whose identity is insufficient to determine, is utilizing a range of malware families including ValleyRAT, gh0st RAT, Mydoor, and Moudoor. The central vulnerability exploited is currently

unknown. The victimology spans across multiple countries and sectors, although specific sector information is insufficient.

Attack Chain and Priority Control

The observed techniques form a complex chain, including Windows Management Instrumentation, bypassing user account control, and using malicious files. The priority technique is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure is hosted on CTG Server Limited, as observed. Abuse.ch has corroborated the presence of Ghost RAT malware, providing additional context to the threat. However, according to AbuseIPDB, there are no indicators with a 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)

- T1047 Windows Management Instrumentation
- T1548.002 Bypass User Account Control
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1219 Remote Access Tools
- T1070.006 Timestomp
- T1112 Modify Registry
- T1553.005 Mark-of-the-Web Bypass
- T1218.005 Mshta
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer
- T1564.001 Hidden Files and Directories
- T1564.004 NTFS File Attributes

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3082).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4629; 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
Windshift	0.4629
APT19	0.4343
Evilnum	0.4336
APT38	0.4307
Rancor	0.4252

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Ghost RAT.
- 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	202[.]61[.]160[.]201	AbuseIPDB 0% (SG) · Ghost RAT · AS152194 CTG Server Limited
IP	202[.]61[.]160[.]137	
IP	202[.]61[.]160[.]160	
IP	202[.]61[.]160[.]202	
IP	202[.]61[.]160[.]208	

Type	Indicator	Context
IP	38[.]55[.]151[.]63	
Domain	baoxis[.]cc	
Domain	invoice[.]msopsa[.]top	
Domain	temu[.]baskwms[.]top	
Hash	02bb20455cc592a69c080abac770ce90	
Hash	31037a42ca048e06e69a78f55bc2eff5	
Hash	887ec87e4a19759cad25d4bc0956d2b965d3041d	
Hash	f0fde01b1e36503227252f6cb6b3b075f93a2c1a	
Hash	452259dc297f56cf22c7932e8fbcefe821ef9c31271340 74fae585f89355d397	
Hash	50c74b468c217776b8890b841baefec8b196b14083a7 873a9201c838a8e4c90a	
Hash	05d188f071d097f5b6bd8138749b4b14	
Hash	0ba93109757776a44de9d8c88baa4963	
Hash	1a3cc75466ffb1971482f7abf7aabc3f	
Hash	1c47c63e5ed25060d95359c57c77b107	
Hash	1d94fbe9cab21278cc3f104bea334d08	
Hash	20209b3a32769afc6a75694b8d8839dd	
Hash	2c6f05f1f309d89b2236e6c8b59c88f9	
Hash	3b1aba44dd3d9b6339b6f56e2f42034b	
Hash	4044e4b6471c9de7b0a4ba37d9d9df9a	
Hash	4f0593e8e0e8fac49429e9b45ebf7fa1	
Hash	5002eca748205d544618e3bd2dedc223	
Hash	5b6bbcc06cf08cc99e1afeda486d42fb	

Type	Indicator	Context
Hash	6359e6236471cbe434d0ef4c42b7f879	
Hash	63ac85195b73753333316a889cf5880f	
Hash	66442f2457eca8f47385b1fb2c6fcab8	
Hash	66705384a7ad81d14c34fc6c054a0ecf	
Hash	68c16c46f8afb9e00bbaba0207fb0a46	
Hash	6c39900d77dcba158e1d27c7619cb06d	
Hash	6fb6a55424adfb61e31f06aef33273e5	
Hash	7403cbcc5a9c32384d431856dc48fcc9	
Hash	74fd9f91fc93b6288b4fc253ea5b3e20	
Hash	7849061c536a3efb05a56d504694e7e7	
Hash	79ecd61b09b0f2d54b34586c916c4ec9	
Hash	7f16449cd0c4862d1eadf8a5742bf09a	
Hash	7f81c1bc8cfd588e8998968e2621456e	

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:** T1112 Modify Registry (persistence)
- **Observed here:** T1112 Modify Registry was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (persistence)
- **Basis:** 19 of 170 documented groups that use Modify Registry also use Scheduled Task/Job (conditional 0.66, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious tasks at a later time, potentially evading detection by blending in with legitimate system activity. This technique may be particularly appealing as it allows the actor to schedule tasks that could re-establish access or continue malicious activities, potentially bypassing the initial block. The defensive

control to counter this would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1078 Valid Accounts (n=18, lift 1.6), T1547 Boot or Logon Autostart Execution (n=17, lift 1.7)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File