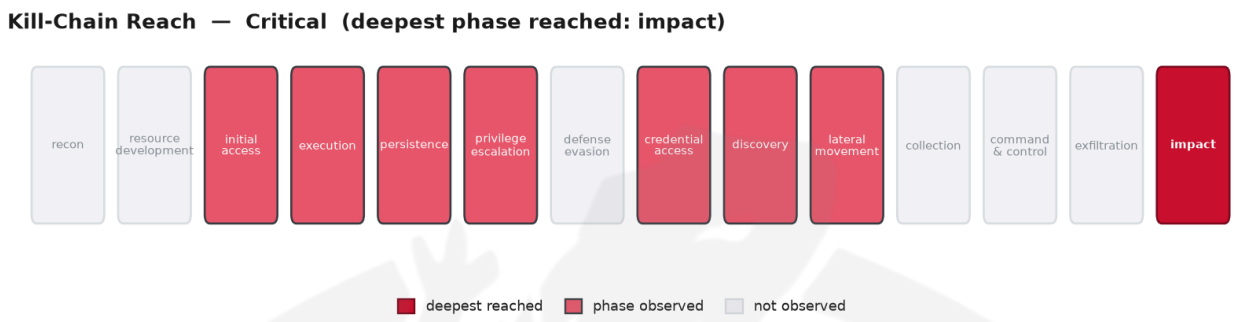
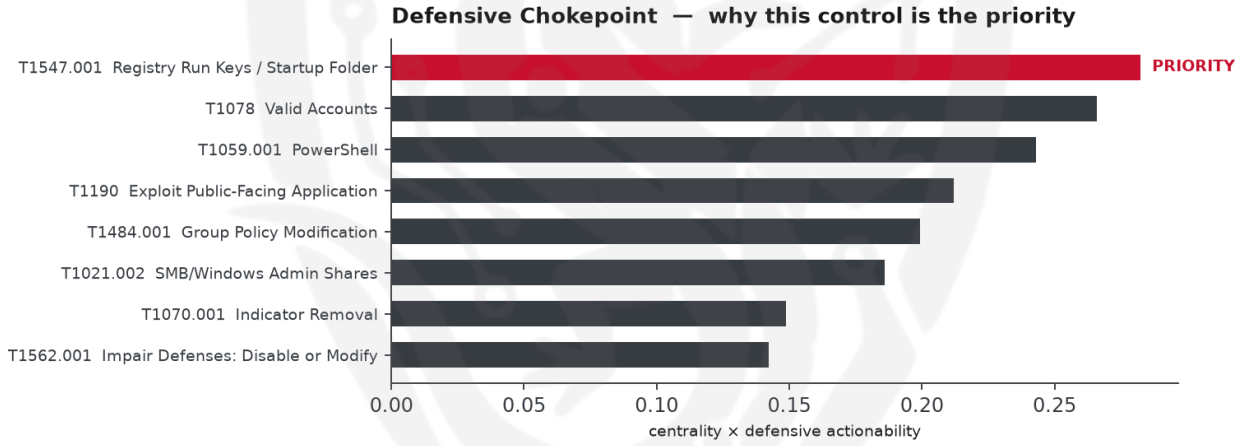
THREAT REPORT: THE GENTLEMEN

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 Gentlemen threat actor has been observed targeting various sectors in Brazil, China, Indonesia, Taiwan, and Thailand, utilizing a range of malware families including SharkLoader, Cobalt Strike, and ZiChatBot. The actor's tactics involve exploiting multiple techniques to gain unauthorized access and persist within the network. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The actor's activities pose a critical operational risk, reaching the impact stage.

Threat Overview

The Gentlemen threat actor is utilizing a custom set of backdoors and evolving tactics, including the use of SharkLoader, Cobalt Strike, ZiChatBot, MgBot, ReverseSocks, PowerCloud, AppleSeed, and CoolClient malware families. The targeted sectors include Manufacturing, Technology, Healthcare, Finance, Construction, and Transportation. The central vulnerability exploited is currently insufficient to determine.

Attack Chain and Priority Control

The observed techniques employed by The Gentlemen form a complex attack chain, involving network discovery, service execution, and impairment of defenses. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To counter this, 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

Although there is no specific information on hosting providers or ASNs observed, abuse.ch has corroborated the presence of the Gentlemen malware family. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These findings provide additional context but do not override the primary source information.

Technical Appendix

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

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

- T1543.003 Windows Service
- T1040 Network Sniffing
- T1135 Network Share Discovery
- T1070.003 Clear Command History
- T1190 Exploit Public-Facing Application
- T1562.002 Impair Defenses: Disable Windows Event Logging
- T1021.002 SMB/Windows Admin Shares
- T1484.001 Group Policy Modification
- T1070.001 Indicator Removal
- T1087 Account Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1018 Remote System Discovery
- T1046 Network Service Discovery
- T1569.002 Service Execution
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2973).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4774; 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
BlackByte	0.4774
APT41	0.4188
Medusa Group	0.4058
Cinnamon Tempest	0.4003
DarkVishnya	0.3963

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Gentlemen.
- 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	81[.]177[.]215[.]15	
Domain	rsat[.]activedirectory[.]ds-lds[.]tools	
Hash	9321a61a25c7961d9f36852ecaa86f55	
Hash	6afc6b04cf73dd461e4a4956365f25c1f1162387	
Hash	f8965fdce668692c3785afa3559159f9a18287bc0d53abb21902895a8ecf221b	

Type	Indicator	Context
Hash	5af1dae21425dda8311a2044209c308525135e1733eeff5dd20649946c6e054c	
Hash	b6b51508ad6f462c45fe102c85d246c8	
Hash	96f0dbf52aed0afd43e44500116b04b674f7358e	
Hash	7556ae58c215b8245a43f764f0676c7a8f0fdd1a	
Hash	8f0577d28c4ff5f71b149f444bfaba8e	
Hash	9ddae47ff968343a8c32a5344060257fdc08e2a7bdb9a227c8b3a584ee3c9f1e	
Hash	eef8a950952696b018aa9c6da2f5d7ad	
Hash	1fa071303fb846308571e64727501fb98b1c2be6	
Hash	5abe477517f51d81061d2e69a9adebdcda80d36667d0afabe103fda4802d33db	
Hash	5b4f59236a9b950bcd5191b35d19125f60cfb9e1a1e1aa2e4f914b6745dde9df	
Hash	68fec379f2ae76c3d2ce913f7be650cea1d06990	
Hash	5761bd63da03686fc480245da7bd1e9f	
Hash	6ae7c9a7ea0b8c40a64225734f6bd01d	Gentlemen
Hash	8468cb5888fb383d25f9144c2b2f61c414cea3f8	
Hash	b67958afc982cafbe1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6	Gentlemen
Hash	c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73	Gentlemen
Hash	3b46a729db7ae6af8b19711c9452194d	Gentlemen
Hash	5aea74bf3e70f38eb596f8002b3c02514daee4f0	
Hash	1af419b36a5edefef387409e2b3248c9223f7dc49a4f7b15ea095d371c3a70b2	Gentlemen
Hash	10ca9a4040001560d053b7e7885c1b95	Gentlemen
Hash	e7cc7b32d844ec6a2f41f0efbc64a0783afb56e4	
Hash	02944c8a5535cdb5b2cbb893db2d5acf	Gentlemen
Hash	3c471ebc947cdf32240a90ffadf49b13	Gentlemen
Hash	4be8bb62f0ebbcf4ce52c35ab6f794f5	Gentlemen
Hash	53c616677bc7e2a0a03127f19166d007	Gentlemen

Type	Indicator	Context
Hash	554e699c96b332468f1ae69c1ae81ef9	
Hash	5c3b9821fc82a9028cb63b9671950919	Gentlemen
Hash	5f0b2c6d9f442754258bf4dd841c8341	Gentlemen
Hash	608faf58353b65c45ef9833358ac3787	Gentlemen
Hash	73f0a8c3ea794a04e80c32038249f044	
Hash	846dc77c1246db20d976346e0e359502	Gentlemen
Hash	adac9984b3cc43d66a0d33079bbec299	Gentlemen
Hash	ae0e536766788478263bf448a9381641	Gentlemen
Hash	b3e418d30312c1b2c58a791286868f42	Gentlemen
Hash	b9986a0f1f1f1a798dc3f0c59a80a1a3	

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