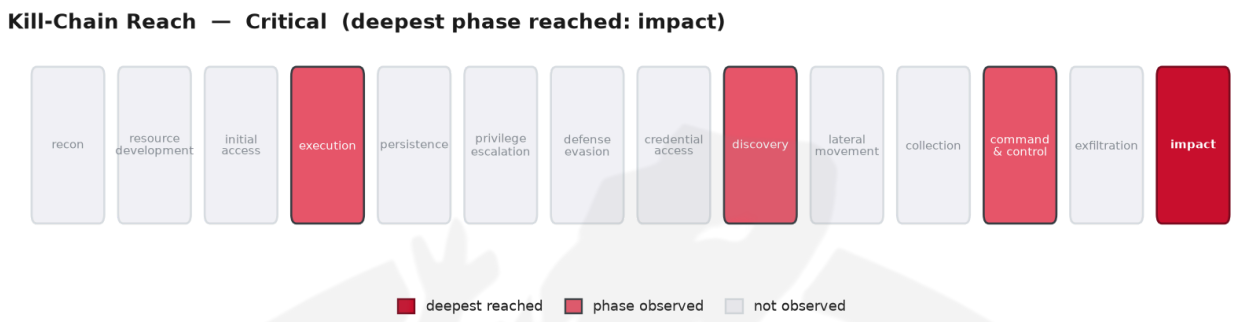
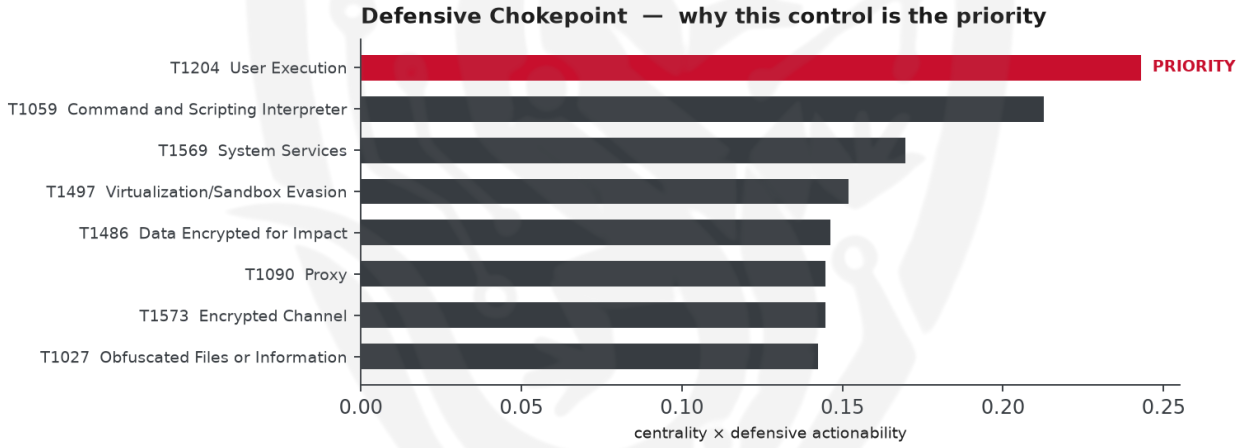
THREAT REPORT: THE GENTLEMEN

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 utilizing various malware families, including The Gentlemen, SystemBC, KillAV, and PowerRun, to target unknown sectors and countries. The priority defensive action should be to block execution of downloaded files and enforce user awareness on lures. The threat actor's techniques have been assessed as critical, reaching the impact stage. Priority should be given to defending against user execution techniques.

Threat Overview

The Gentlemen threat actor is utilizing a range of malware families, including The Gentlemen, SystemBC, KillAV, and PowerRun. The central vulnerability exploited is currently unknown. The victimology of this campaign is also unknown, with insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques used by The Gentlemen threat actor form a complex chain, including Windows Management Instrumentation, Service Stop, System Information Discovery, and others. The priority technique is T1204 User Execution, which is the graph chokepoint. To defend against this, the priority control is to "Block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures."

Infrastructure and Corroboration

The Gentlemen's malicious infrastructure has no observed hosting providers or ASNs. However, abuse.ch has corroborated the presence of Gentlemen malware, as well as unknown malware. AbuseIPDB has not flagged any indicators with high confidence, 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
- T1489 Service Stop
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1016 System Network Configuration Discovery
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1049 System Network Connections Discovery
- T1497 Virtualization/Sandbox Evasion
- T1204 User Execution
- T1057 Process Discovery
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1573 Encrypted Channel
- T1569 System Services
- T1018 Remote System Discovery
- T1105 Ingress Tool Transfer
- T1490 Inhibit System Recovery
- T1529 System Shutdown/Reboot

Analytical Scores

- Priority technique (graph chokepoint): T1204 User Execution (centrality 0.3037).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4198; 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
Medusa Group	0.4198
Darkhotel	0.3835
Windshift	0.3651
Stealth Falcon	0.3591
Inception	0.3451

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Gentlemen, Unknown malware.
- 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
Hash	a88daa62751c212b7579a57f1f4ae8f8	
Hash	c0979ec20b87084317d1bfa50405f7149c3b5c5f	
Hash	7a311b584497e8133cd85950fec6132904dd5b02388a9feed3f5e057fb891d09	
Hash	408dd6ade80f2ebbc2e5470a1fb506f1	
Hash	e00293ce0eb534874efd615ae590cf6aa3858ba4	
Hash	4c82fbafef9bab484a2fbe23e4ec8aac06e8e296d6c9e496f4a589f97fd4ab71	
Hash	3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235	Gentlemen
Hash	4200b46a93c6ab059e2b34ce200c4a5b	Unknown malware

Type	Indicator	Context
Hash	42bcc743c71a9ea083c1c750a398110582796762	
Hash	de1a114a2c5552387a1bbb61501bf129	
Hash	d6aaed67606d6dab0f652c755d3d363025f60adb	
Hash	62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8	Gentlemen
Hash	0b33a1a23b044beb5c9a63aafd35595c	
Hash	00ff099e3cf7b548a7a0260cde8ac2f24a746da2	
Hash	860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923	Gentlemen
Hash	f4ae5b89db5a6a36dbd98287ab7c860a	
Hash	36d968425629b10f38be17787f8afe4b8afa131e	
Hash	992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5	
Hash	30b49ae2f685d4403d3013410f80c2e2	
Hash	5f5bf7fc7a9ac89ce0bbb07bd1160078	
Hash	6ae7c9a7ea0b8c40a64225734f6bd01d	Gentlemen
Hash	5264a94271d875675336a503c94ece0baceb58c5	
Hash	68225c5613afe2174ed46e074147676b0f9a3915	
Hash	8468cb5888fb383d25f9144c2b2f61c414cea3f8	
Hash	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a	Gentlemen
Hash	2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d	Gentlemen
Hash	48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd	Gentlemen
Hash	5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca	Gentlemen
Hash	87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c	Gentlemen
Hash	8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db	Gentlemen
Hash	91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1	Gentlemen
Hash	994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3	Gentlemen
Hash	9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454	Gentlemen

Type	Indicator	Context
Hash	a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad	Gentlemen
Hash	b67958afc982cafbe1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6	Gentlemen
Hash	c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8	Gentlemen
Hash	c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73	Gentlemen
Hash	ec368ae0b4369b6ef0da244774995c819c63cffb7fd2132379963b9c1640ccd2	Gentlemen
Hash	efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f	Gentlemen
Hash	f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12	Gentlemen

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