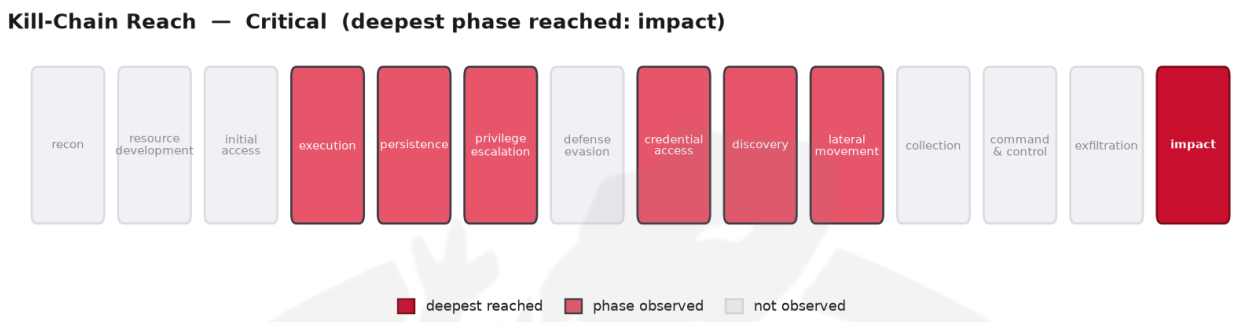
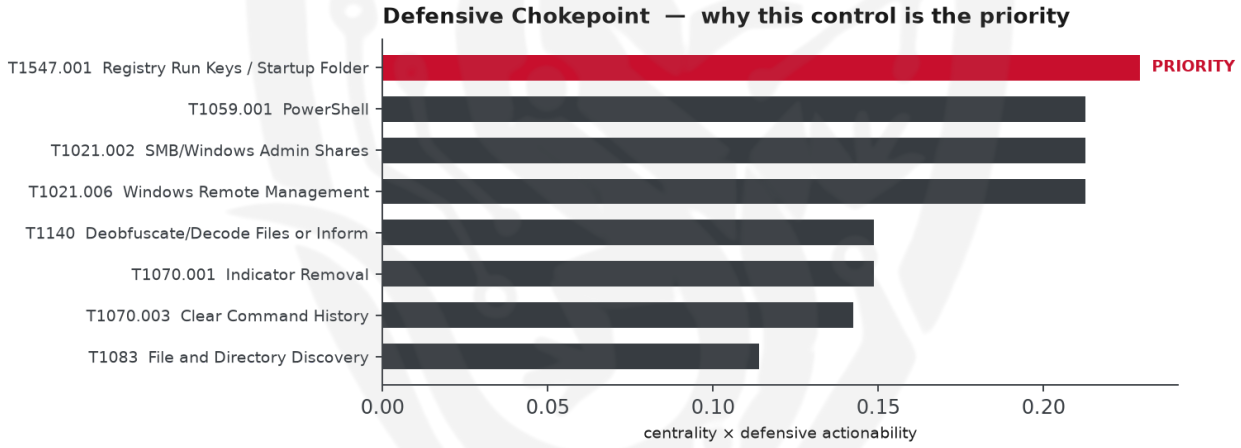
THREAT REPORT: THE GENTLEMEN

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 source attributes this activity to The Gentlemen, who have been observed utilizing the Gentlemen, SystemBC, Cobalt Strike, and AnyDesk malware families to target organizations in the United States, Brazil, Germany, and the United Kingdom, primarily in the manufacturing, technology, healthcare, finance, and government sectors. The threat actor is exploiting CVE-2024-55591 to gain access to systems. Priority should be given to patching this vulnerability and auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The observed attacks have reached a critical operational risk band, indicating a high potential for impact.

Threat Overview

The Gentlemen threat actor is using a combination of malware families, including Gentlemen, SystemBC, Cobalt Strike, and AnyDesk, to exploit the CVE-2024-55591 vulnerability. The targeted sectors include manufacturing, technology, healthcare, finance, and government, with a focus on the United States, Brazil,

Germany, and the United Kingdom. The malware is designed to encrypt data, making it a significant threat to the targeted organizations.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, Windows Management Instrumentation, OS credential dumping, and service stop, among others. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which is the graph chokepoint. To mitigate this threat, the priority control is to: Patch CVE-2024-55591 on all affected systems as the top priority, then: 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 observed hosting provider or ASN, abuse.ch has corroborated the Gentlemen malware family. However, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These corroboration efforts provide additional context to the threat, but do not override the source assessment.

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
- T1047 Windows Management Instrumentation
- T1003 OS Credential Dumping
- T1489 Service Stop
- T1069.002 Domain Groups
- T1135 Network Share Discovery
- T1082 System Information Discovery
- T1070.003 Clear Command History
- T1140 Deobfuscate/Decode Files or Information
- T1021.002 SMB/Windows Admin Shares
- T1021.006 Windows Remote Management
- T1070.001 Indicator Removal
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1018 Remote System Discovery

- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2413).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4271; 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	0.4271
FIN10	0.3961
APT18	0.3849
Medusa Group	0.3832
Wizard Spider	0.3831

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
Domain	tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion	
URL	hxxp://tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion/	
Hash	3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235	Gentlemen

Type	Indicator	Context
Hash	4200b46a93c6ab059e2b34ce200c4a5b	Unknown malware
Hash	42bcc743c71a9ea083c1c750a398110582796762	
Hash	ead0d7a8ae0a6ffb7f0a5873fec4ff5e	
Hash	39bd9c888d3e8110c127ba60cc727d2538bf7da2	

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