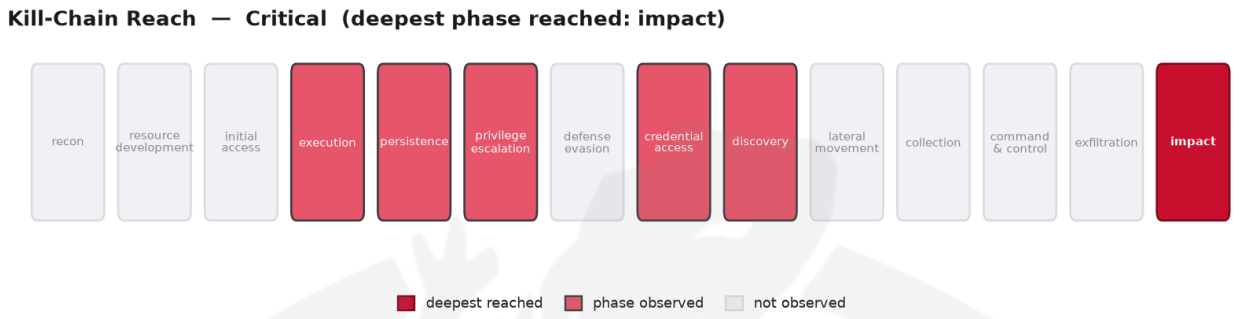
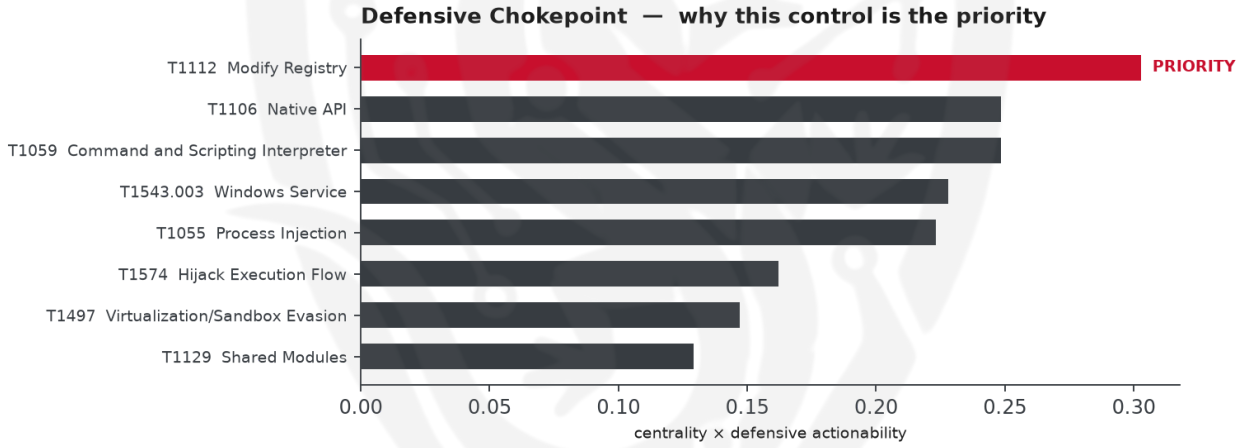
THREAT REPORT: THE GENTLEMEN

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 techniques to impair defenses and disable targets' Endpoint Detection and Response (EDR) systems. The priority defensive action should be given to monitoring sensitive registry keys for modification and restricting registry-edit tools for unprivileged users. The targeted country and sectors are currently unknown, but the threat actor's techniques pose a critical operational risk. It is essential to focus on the technical mechanics of the attack to mitigate potential damage.

Threat Overview

The Gentlemen threat actor is employing a range of techniques, including Windows Management Instrumentation, OS Credential Dumping, and Service Stop, to achieve their goals. Although the central CVE and malware families used are currently unknown, the threat actor's tactics pose a significant threat

to targeted systems. The victimology of this campaign is also unclear, but the techniques used suggest a high level of sophistication.

Attack Chain and Priority Control

The observed techniques used by The Gentlemen threat actor form a complex attack chain, involving multiple steps to impair defenses and gain control over targeted systems. The priority technique, T1112 Modify Registry, is a critical chokepoint in this 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

There is currently no available information on the hosting providers or ASNs used by The Gentlemen threat actor, and no malware families have been corroborated by abuse.ch. Additionally, AbuseIPDB has not flagged any 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
- T1003 OS Credential Dumping
- T1129 Shared Modules
- T1489 Service Stop
- T1543.003 Windows Service
- T1007 System Service Discovery
- T1082 System Information Discovery
- T1106 Native API
- T1055 Process Injection
- T1112 Modify Registry
- T1059 Command and Scripting Interpreter
- T1497 Virtualization/Sandbox Evasion
- T1057 Process Discovery
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1574 Hijack Execution Flow
- T1068 Exploitation for Privilege Escalation
- T1055.001 Dynamic-link Library Injection
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3187).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3187; 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
Blue Mockingbird	0.3187
Aquatic Panda	0.303
BlackByte	0.2901
Medusa Group	0.2863
Poseidon Group	0.2843

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
Hash	7ee17efef04bb7c9de90d5210263ed6993f867e5a11f86e65e3bb1362c7de237
Hash	9ca9432b0d29204cb5420a1a6b01533d4552130c2a8a5ecd7837efadefb4a046
Hash	c277ae5a4dd62f51de5278790796cd2700de7f77ea17762e97729f27872d076b

---

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.k@3sdragon.eu

- **Control applied:** T1112 Modify Registry (persistence)
- **Observed here:** The Gentlemen used T1543.003 Windows Service here as an alternative persistence technique.
- **Projected pivot:** T1543.003 Windows Service (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The Gentlemen could pivot to utilizing Windows Service (T1543.003) to maintain persistence and evade detection, potentially leveraging this technique to execute malicious code or establish a backdoor. They may attempt to create a new service that appears legitimate, but would likely be thwarted by robust monitoring and access controls. To counter this potential move, the defensive control of Restrict service/daemon creation to admins; monitor service and driver installs should be implemented.

Detection and hardening for the pivot (T1543.003 Create or Modify System Process)

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process