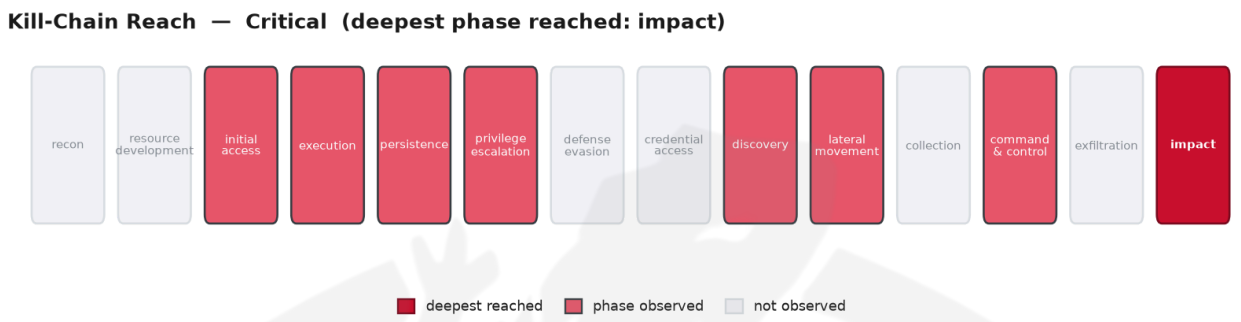
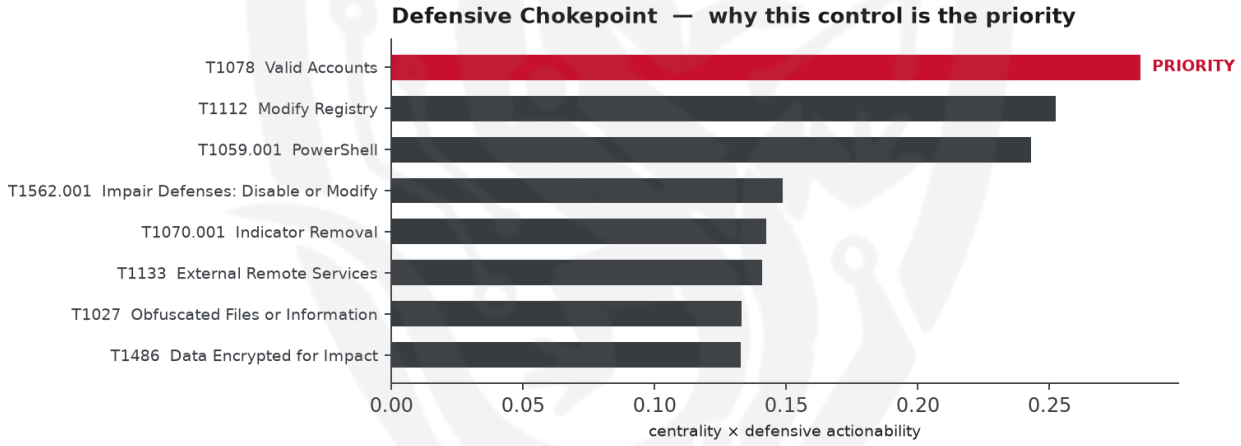
THREAT REPORT: THE GENTLEMEN

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, a threat actor utilizing the Gentlemen and Qilin malware families, as well as Trojan:Win32/MpTamperBulkExcl.H, to target the Transportation and Construction sectors. The actor is exploiting CVE-2024-55591, and priority should be given to patching this vulnerability on all affected systems. The threat actor's use of valid accounts is a key technique in their attack chain, emphasizing the need for swift defensive action.

Threat Overview

The Gentlemen threat actor is using a combination of malware families, including the Gentlemen, Qilin, and Trojan:Win32/MpTamperBulkExcl.H, to exploit the CVE-2024-55591 vulnerability. The actor is targeting organizations in the Transportation and Construction sectors, although the specific countries targeted are not specified. The malware is used to gain access to systems, where the actor can then use various techniques to evade detection and achieve their goals.

Attack Chain and Priority Control

The observed attack chain involves a range of techniques, including scheduled tasks, system owner/user discovery, and external remote services. However, the priority technique is T1078 Valid Accounts, which is used to gain access to systems and maintain persistence. To mitigate this threat, the priority control is to: Patch CVE-2024-55591 on all affected systems as the top priority, then: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no corroboration from third-party sources regarding the hosting providers or ASNs used by the threat actor, as no such information is available. Similarly, there are no malware families corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB.

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
- T1033 System Owner/User Discovery
- T1133 External Remote Services
- T1548.002 Bypass User Account Control
- T1036.005 Match Legitimate Resource Name or Location
- T1082 System Information Discovery
- T1112 Modify Registry
- T1070.001 Indicator Removal
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1071.001 Web Protocols
- T1018 Remote System Discovery
- T1105 Ingress Tool Transfer
- T1021.001 Remote Desktop Protocol
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2846).

- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5085; 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
APT18	0.5085
Silence	0.4486
FIN8	0.4455
Akira	0.4404
APT39	0.4391

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	f918535f974591ef031bd0f30a8171e3da27a6754e6426a8ba095f83195661c8