# Adversary Attribution Report

ICT3214 – Security Analytics | AY2025/2026 Trimester 1

Generated on: 2025-10-19 02:35:34

Detected TTPs: T1001

## 1. Analysis Summary

The detected TTP T1001 does not directly match any of the listed techniques from the matched attacker groups. However, it is essential to analyze the broader context of the techniques employed by the groups to identify potential overlaps and likely actors. The groups exhibit a range of techniques focused on credential dumping, exploitation for privilege escalation, and data exfiltration, which are common in advanced persistent threats (APTs).

## 2. Overlap Table

|  |  |
| --- | --- |
| Actor Group | Overlap Count |
| --------------------- | --------------- |
| Threat Group-3390 | 0 |
| Gamaredon Group | 0 |
| MuddyWater | 0 |
| APT28 | 0 |
| HAFNIUM | 0 |
| Moonstone Sleet | 0 |
| WIRTE | 0 |
| Windshift | 0 |
| Saint Bear | 0 |
| Ke3chang | 0 |

## 3. Most Likely Attacker

None identified – Confidence: Low  
  
---  
  
Summary of Findings:  
The analysis reveals that the detected TTP T1001 does not align with any of the techniques associated with the matched attacker groups. This absence of overlap indicates that the current incident may not be directly linked to the identified groups or that the techniques used in this incident are not fully represented in the existing threat intelligence.  
  
Justification for Likely Involvement:  
Given that T1001 (Data Obfuscation) is a technique that can be used by various threat actors, including those not listed in the matched groups, it is difficult to attribute the incident to any specific actor based solely on the provided data. The lack of overlap suggests that the techniques employed may either be novel or not yet documented in the context of these groups.

## 4. Defensive Mitigations

Error reading mitigations CSV: 'utf-8' codec can't decode byte 0xe4 in position 9990: invalid continuation byte

## 5. Analyst Suggestions

The confidence rating is low due to the absence of direct overlaps between the detected TTP and the techniques associated with the matched attacker groups. This suggests that the incident may involve either a different threat actor or a unique set of tactics not yet documented in the existing intelligence. Further investigation and data collection are necessary to clarify the situation.