The client contacted the security team after noticing unexpected activity on a key server. Since the server hosts sensitive data, the client was concerned about the possibility of unauthorized access and asked for an investigation to confirm whether the system had been compromised.

Time reported: 30/12/2025 14:30

◈ Hypothesis 1 – Legitimate Administrative Activity

The observed activity may have been caused by a legitimate system administrator performing maintenance or troubleshooting tasks outside of regular hours.

What we check

- Known admin accounts
- Normal logon patterns
- Expected PowerShell usage

How we validate / dismiss

- Logons occurred from **unfamiliar sources**
- PowerShell commands were **encoded**
- Activity did not match documented admin behavior

◈ Hypothesis 2 – Misconfiguration or Automated System Activity

The activity may have been generated by an automated system process, scheduled task, or misconfiguration.

What we check

- Scheduled tasks
- Service accounts
- Non-interactive logons

How we validate / dismiss

- PowerShell execution was **interactive**
- Commands indicated **manual reconnaissance**
- No matching scheduled tasks were identified

◈ Hypothesis 3 – External Unauthorized Access Using Valid Credentials

An external actor may have attempted to gain access to the server using credential-based techniques (such as brute-force attempts or Kerberos authentication weaknesses).

What we check

- Unusual authentication activity
- Interactive logons
- PowerShell reconnaissance

Supporting evidence

- Unusual authentication behavior
- Successful authentication followed by PowerShell execution
- Reconnaissance commands consistent with attacker behavior

◈ Hypothesis 4 – Malware or Automated Exploit

The server may have been compromised by malware or an automated exploit without direct human interaction.

What we check

- Unknown binaries
- Exploit indicators
- Non-native tools

How we validate / dismiss

- No malicious binaries observed
- Activity relied on built-in tools
- Actions suggest **hands-on-keyboard** behavior

PHASE 1

Following the client’s request, an investigation was initiated to assess whether unauthorized activity had occurred on a critical server. The scope of the investigation was limited to the Domain Controller and focused on authentication and execution activity during the timeframe in which the unexpected behavior was reported.

Phase 2

To understand the sequence of events, a timeline-based analysis was conducted using authentication and execution logs collected from the Domain Controller. Relevant events were correlated chronologically to identify patterns of activity and determine whether the observed behavior aligned with legitimate use or potential unauthorized access.

Phase 3

With the timeline established, each hypothesis was evaluated against the observed events to determine which scenario was most consistent with the activity on the Domain Controller.

◈ Hypothesis 1 – Legitimate Administrative Activity

The observed activity may have been caused by a legitimate system administrator performing maintenance or troubleshooting tasks outside of regular working hours.

What we check

- **Known administrative accounts**
- **Typical logon sources and times**
- **Expected PowerShell usage patterns**

How we validate / dismiss

- **Logons originated from unfamiliar sources**
- **PowerShell commands were encoded and obfuscated**
- **Activity did not align with documented administrative procedures**

Conclusion: ✕ Likely ruled out

💠 Hypothesis 2 – Misconfiguration or Automated System Activity

The activity may have been generated by an automated process, scheduled task, or system misconfiguration.

What we check

- Scheduled tasks
- Service or system accounts
- Non-interactive authentication events

How we validate / dismiss

- PowerShell execution was interactive
- Commands reflected manual reconnaissance behavior
- No legitimate scheduled tasks were initially associated with the activity

Conclusion: ❌ ruled out

💠 Hypothesis 3 – Unauthorized Credential-Based Access

An external actor may have attempted to gain access to the server using credential-based techniques (such as brute-force attempts or Kerberos authentication weaknesses). Following successful authentication, the attacker may have executed reconnaissance commands, established persistence, and initiated staged data exfiltration.

What we check

- Unusual authentication behavior
- Interactive logons
- PowerShell reconnaissance and obfuscation
- Persistence mechanisms
- Outbound data transfer patterns

Supporting Evidence

- **Kerberos authentication events without pre-authentication (4768 – PreAuthType = 0), consistent with AS-REP roasting attempts**
- **Successful interactive logons on the Domain Controller (4624)**
- **Encoded PowerShell execution shortly after authentication (4104)**
- **Reconnaissance commands to enumerate user privileges and locate backup files**
- **Creation of a scheduled task configured to execute every five minutes**
- **Repeated outbound connections transferring small portions of data to an external server**

Analysis

The observed activity follows a logical attack progression: credential access attempts, successful interactive authentication, post-authentication reconnaissance, persistence via scheduled tasks, and staged data exfiltration. The use of encoded PowerShell commands and living-off-the-land techniques suggests deliberate efforts to evade detection.

Conclusion: ✅ Most likely hypothesis supported

🔹 Hypothesis 4 – Malware or Automated Exploit

The server may have been compromised by malware or an automated exploit without direct human interaction.

What we check

- **Unknown or suspicious binaries**
- **Exploit artifacts**
- **Indicators of automated malware execution**

How we validate / dismiss

- **No malicious binaries were identified**
- **Activity relied primarily on native system tools**
- **Execution patterns suggest hands-on-keyboard interaction**

Conclusion: ⚠ Unlikely

Summary

Based on the correlation of multiple indicators, including Kerberos ticket anomalies, interactive logons, encoded PowerShell execution, and system reconnaissance commands, hypotheses involving legitimate administrative activity or automated processes were eliminated. The evidence strongly supports unauthorized credential-based access as the most plausible explanation for the observed behavior.