Incident Analysis Report: Backdoor Confirmation and Triage Methodology

Date: 09/21/2025 **Analyst:** Amir (Drawing upon initial findings by Johny) **Focus:** Detailed analysis of anomalous activity demonstrating sophisticated investigative processes within a Security Operations Center (SOC) environment.

---

1. Executive Summary and SOC Mandate

This analysis was initiated following the observation of anomalous behaviors indicative of adversary access across several Windows hosts. The primary goal was to systematically triage logs ingested into **Splunk** to confirm the creation of a backdoor and establish the methods of persistence and remote execution.

The investigation confirmed that the adversary successfully leveraged compromised credentials (implied via the actions of Micheal.Beaven) to **remotely create the malicious user A1berto**. Furthermore, a sophisticated encoded PowerShell payload was executed on the host **james.brown**, requiring external tools for decoding and full Indicator of Compromise (IOC) identification.

2. Methodological Triage and Data Collection

To address the manager's request for a quick investigation, logs from suspected hosts were pulled and ingested into the **Splunk index main**. This preliminary step yielded a total of **12,256 events** for detailed examination.

The investigative approach prioritized mapping observed behaviors (Tactics, Techniques, and Procedures or TTPs) to specific Windows logging mechanisms:

Investigative Step (TTP)	**Required Knowledge/Triage Process**	**Key Event ID(s) Utilized**
User Creation & Account Triage	Determined the Event ID for new user creation (requiring external confirmation/Google search). Filtered logs based on this ID to identify the new username, **A1berto**.	Windows Event ID 4720 (Implied by context)
Establishing Persistence	Researched (Google search) common Event IDs related to registry modification and security descriptor updates (4657, Sysmon 12, 13, 14). Applied this filtering to locate the specific	Event ID 4657, Sysmon 12

	Sysmon Event ID 12 confirming the registry path for persistence.	
Remote Execution Analysis	Researched (Google search) the most common Windows Event ID for **process creation (4688)**. Filtered logs based on 4688 and examined the commandline field to extract the full remote command.	Windows Event ID 4688
PowerShell Payload Detection	Researched (Google search) the Event IDs associated with PowerShell script block logging and module logging. Filtered logs for these specific IDs on the infected host **james.brown**.	Event IDs 4104 and 4103
Payload Decoding	Identified the need for external tooling (a standard SOC procedure for encrypted/encoded data) and utilized **CyberChef's "From Base64" and "Decode text" features** to reconstruct the malicious URL.	N/A (External Tool)

3. Detailed Findings and Technical Analysis

3.1 Backdoor Account Creation and Origin

The analysis confirmed the adversary's initial action was to establish a dedicated persistence mechanism through a new user account:

1. **User Creation:** The new account was identified as **A1berto**. Only one event confirmed its creation.

2. **Attribution:** The account was created by the user **Micheal.Beaven**. This suggests the adversary utilized compromised credentials belonging to Micheal.Beaven to execute the action.

3. **Impersonation Tactic:** By examining user fields in Splunk, it was determined that the name **A1berto** likely attempts to impersonate a legitimate user named **Alberto** located in the cybertees department, a common tactic for maintaining covert access.

4. **Remote Command Execution:** The malicious account creation was performed remotely using **WMIC**. Filtering on Event ID 4688 revealed the exact command used: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1".

5. **Persistence Mechanism:** Application of registry-specific Event IDs (Event ID 12) confirmed an update to the path **HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto** concerning the new backdoor user.

3.2 Login Attempts and PowerShell Activity

Despite successful creation, monitoring for login attempts from A1berto (as part of standard post-creation monitoring) revealed **0 observed logins** during the investigation period.

On the infected host **james.brown**, which was confirmed to have PowerShell logging enabled, the filtering on Event IDs 4104 and 4103 yielded **79 events** related to the malicious execution.

The executed command was confirmed to be encoded. The subsequent decoding process using CyberChef yielded the following external communication Indicator of Compromise (IOC):

- **Defanged IOC:** hxxp[://]10[.]10[.]10[.]5/news[.]php
- **Original URL:** http://10.10.10.5/news.php

4. Conclusion and Remediation Recommendations

This investigation successfully utilized specialized Splunk queries and external knowledge (Event ID mapping, CyberChef) to confirm a multi-stage compromise involving user creation, remote execution, registry persistence, and execution of a hostile PowerShell payload.

The evidence points to **WORKSTATION6** (as seen in the WMIC command) and **james.brown** as primary nodes of interest.

Recommended Next Steps (Standard SOC Procedure):

1. **Isolation:** Immediately isolate james.brown and potentially WORKSTATION6.
2. **Credential Reset:** Force a password reset and full audit of the user Micheal.Beaven.
3. **Removal:** Delete the malicious user account A1berto.
4. **Network Blocking:** Implement blocks on the malicious IP address **10.10.10.5** at the firewall and perimeter devices.