Account Compromise Response Playbook

This Playbook was last updated on: 4/1/2021

This incident response playbook has been developed with to coincide with Summit Partners' policies, procedures, and overall practices. This document should be treated as corporate sensitive and must not u necessarily be shared to external parties and nonrelevant internal employees.

*If this incident is being considered as a possible criminal act, then please follow all forensic policies, procedures, and standards to preserve evidence and correlate event. If you are not sure whether the incident is a criminal act, Summit Partners is going to file a complaint or submit an insurance claim, or have knowledgeable of the proper forensic approach, please **do not** proceed, and contact the cybersecurity team for guidance.*

Be sure to read and attempt to complete every step. Keep notes and save pertinent files as they will be required for the incident report. Remember to follow all policies and procedures as it pertains to the instructions and steps below.

Gathering the details of the incident

1. Document the compromised account name, account owner, computer and/or system name.

2. Describe the evidence of account compromise (log files, changes in system settings, data modifications and/or deletions, etc.).

3. Date first noticed?

4. What level access does the user have?

Further Investigation to validate account compromise and collect details

All entries that cannot be validated as authentic should be documented and reported to the IR manager. If any logs have been erased or appear to have been modified, refer to the Audit Log Compromise IR Playbook.

5. Check the user account database to ensure no new entities/ objects have been created, if the user has such permissions (e.g., administrator, power user, DBA, etc.).
    a. This can be validated by comparing with a list of authorized objects based on provisioning requests
    b. This can be validated by viewing creation and modification dates of objects

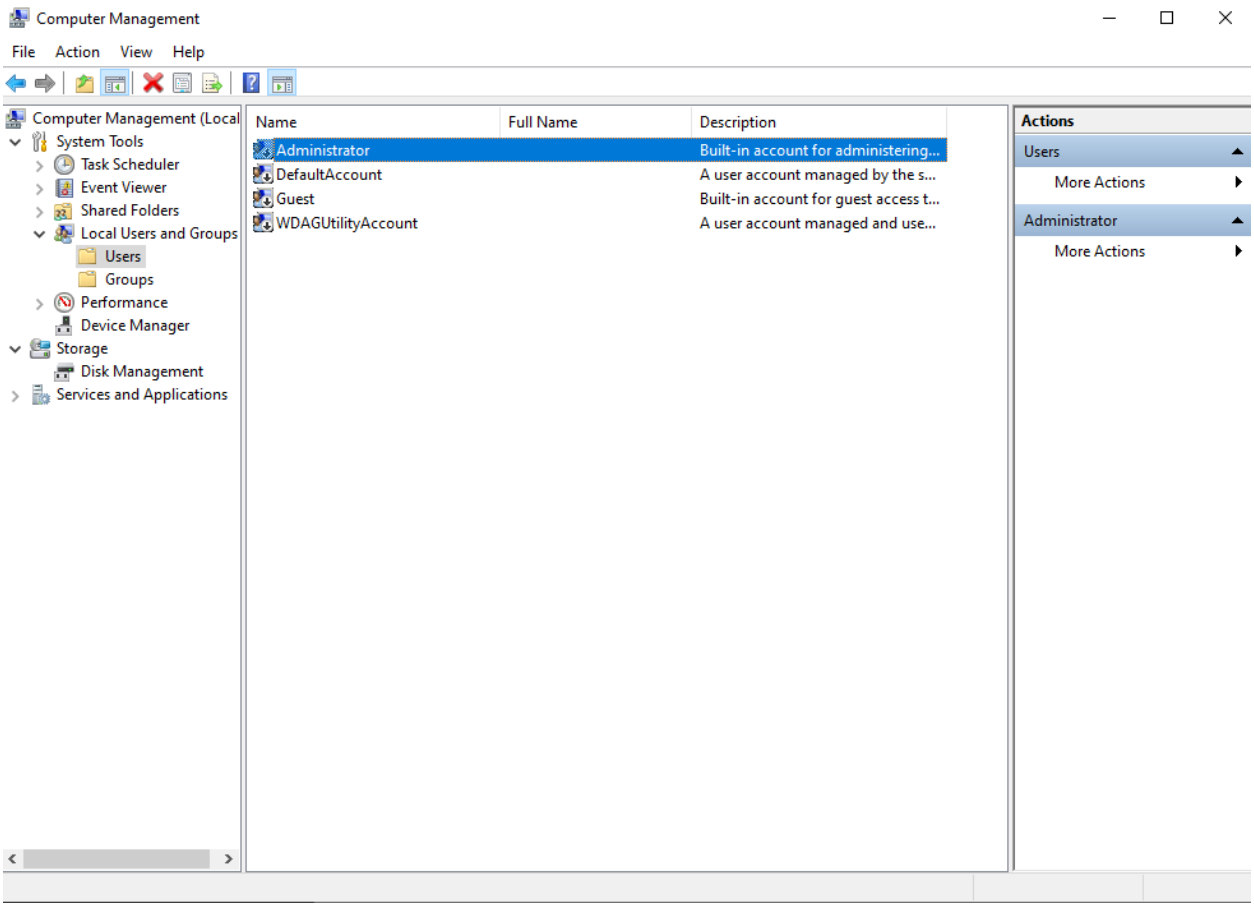

Figure 1- Accessing the Windows User DB

6. Check system logs that track authentication attempts (48 hours prior to the reported incident through the current time). Search for the account entries:
    a. Verify the authenticity of successful logins with the user
    b. Verify the authenticity of failed attempts with the user

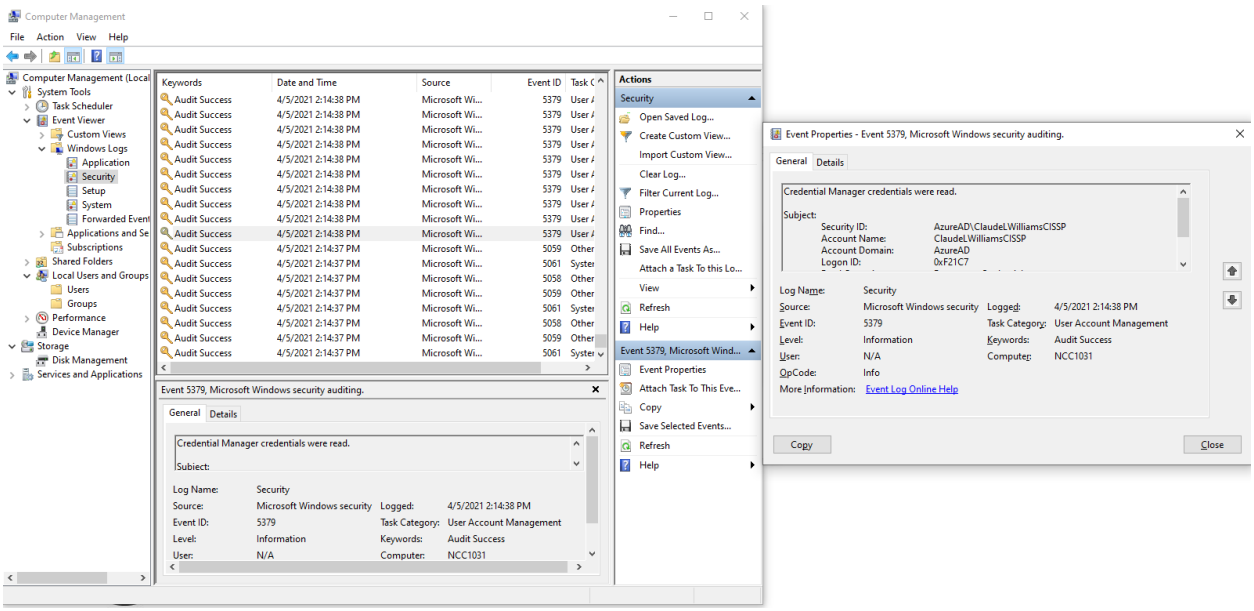

Figure 2 - Windows Security Log

7. Check logs that capture system and/ or application changes, if the user has such permissions (e.g., administrator, power user, DBA, etc.). Search for the account entries to verify the authenticity of changes and attempts at changes.

8. Check logs that capture system changes, if the user has such permissions (e.g., administrator, power user, DBA, etc.). Search for the account entries to verify the authenticity of changes and attempts at changes

9. Check logs that capture file system changes. Search for the account entries to verify the authenticity of file system changes and attempts at changes (e.g., additional files, deleted files, and modified files, etc.).

10. Check the Task Scheduler for any new automated tasks and examine previously run tasks.

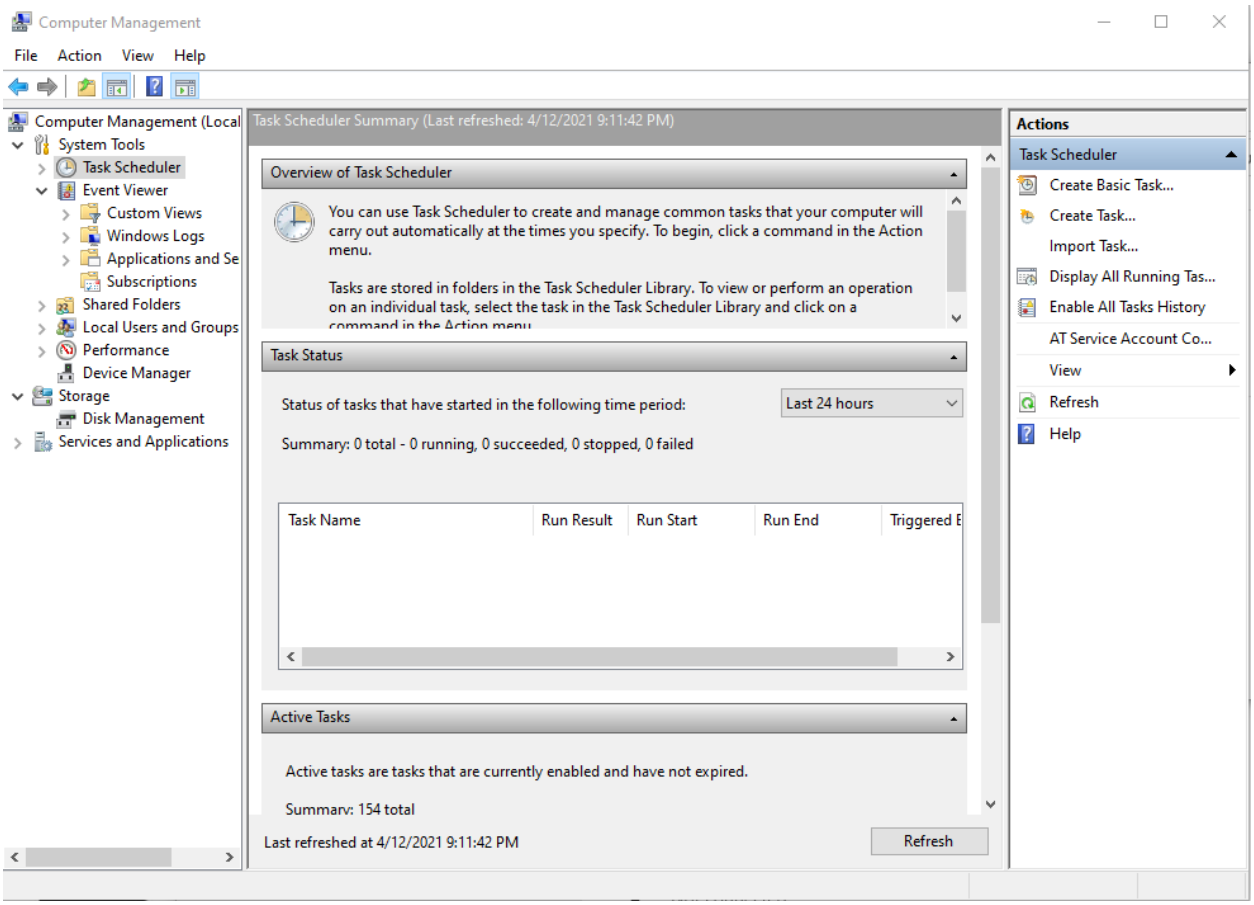

Figure 3 - Windows Task Scheduler

Addressing the incident

11. Temporarily disable the compromised account
12. Rename of the compromised account
13. Change the password of the compromised account
14. Monitor the compromised account for further issues
15. Generate an incident report at http://www.CyNtell.com/Summit.