# 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



Protect. Comply. Relax. Page | 1



\_

Х

🜆 Computer Management

Computer Management (Local	Name	Full Name	Description	Actions			
🙀 System Tools	Administrator		Built-in account for administering	Users			
> 🕑 Task Scheduler	🛃 DefaultAccount		A user account managed by the s	More Actions			
Shared Folders	🛃 Guest		Built-in account for guest access t				
<ul> <li>Marcur orders</li> <li>Local Users and Groups</li> </ul>	🛃 WDAGUtilityAccount		A user account managed and use	Administrator			
<ul> <li>Users</li> <li>Groups</li> <li>Performance</li> <li>Device Manager</li> <li>Storage</li> <li>Disk Management</li> <li>Services and Applications</li> </ul>				More Actions			
>							

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



Protect. Comply. Relax. P a g e | 2



Computer Management (Local						Actions	_						
System Tools	Keywords	Date and Time	Source	Event ID									
Task Scheduler	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	Security	<b>^</b>						
Event Viewer	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	👩 Open Saved Log							_
> 📑 Custom Views	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	View		Event Properties -	Event 5379, M	licrosoft Windo	ws security auditing.		
🗸 📫 Windows Logs	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	Import Custom View							
Application	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	· ·		General Details					
💽 Security	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	Clear Log							
Setup	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	Filter Current Log		Credential Manag	er credentials v	vere read.			^
🛃 System	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	Properties		Cublicate					
Forwarded Event	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /			Subject: Security	ID:	AzureAD\C	laudeLWilliamsCISSP		
> 📇 Applications and Se	Audit Success	4/5/2021 2:14:38 PM	Microsoft Wi		User /	🔐 Find		Account		ClaudeLWil			
5 Subscriptions	Audit Success	4/5/2021 2:14:37 PM	Microsoft Wi		Other	Save All Events As		Account		AzureAD			
8 Shared Folders	Audit Success	4/5/2021 2:14:37 PM	Microsoft Wi		Syster	Attach a Task To this Lo		Logon ID	e .	0xF21C7			~
Local Users and Groups Users	Audit Success	4/5/2021 2:14:37 PM	Microsoft Wi		Other	View							
Groups	Audit Success	4/5/2021 2:14:37 PM	Microsoft Wi		Other		·	Log Na <u>m</u> e:	Security				
Groups     Performance	Audit Success	4/5/2021 2:14:37 PM	Microsoft Wi	5061	Syster	Q Refresh		Source:	Microsoft Wi	ndows security	Logge <u>d</u> : 4/5/	2021 2:14:38 PM	
Performance     Device Manager	Audit Success	4/5/2021 2:14:37 PM	Microsoft Wi		Other	Help	•	Event ID:	5379		Task Category: Use	r Account Management	
Storage	audit Success	4/5/2021 2:14:37 PM	Microsoft Wi		Other		- 11	Level:	Information		Keywords: Aud	lit Success	
T Disk Management	Audit Success	4/5/2021 2:14:37 PM	Microsoft Wi	5061	Syster 🗸	Event 5379, Microsoft Wind	•	User:	N/A		Computer: NCC	01031	
Services and Applications	<				>	Event Properties		OpCode:	Info				
Services and Applications	Event 5270 Microsoft	t Windows security auditing.			×	3 Attach Task To This Eve		More Information:		oline Helo			
		e windows security additing.				-		more information.	<u>event tog of</u>	interies			
	General Details					- copy	•						
					^	Save Selected Events							
	Credential Manager credentials were read.				Refresh		Cogy					C	
	Subject:				~	👔 Help	•						_
	Log Name:	Security											
	Source:	Microsoft Windows security	Logged: 4/5/2021 2:14	38 PM									
	Event ID:	5379	Task Category: User Account										
	Level:	Information	Keywords: Audit Succes										
	User:	N/A	Computer: NCC1031		×	1							

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.



Protect. Comply. Relax. Page | 3



🜆 Computer Management × File Action View Help 🗢 🄿 🖄 📷 🚺 🜆 Computer Management (Local Actions 🗸 🎁 System Tools Task Scheduler Task Scheduler Overview of Task Scheduler Oreate Basic Task... ✓ I Event Viewer 📑 Custom Views You can use Task Scheduler to create and manage common tasks that your computer will 🎨 Create Task... 📫 Windows Logs carry out automatically at the times you specify. To begin, click a command in the Action Import Task... > 💾 Applications and Se menu. Display All Running Tas... Subscriptions Tasks are stored in folders in the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a > 👸 Shared Folders Enable All Tasks History and in the Action menu 🜆 Local Users and Groups AT Service Account Co... > 🔕 Performance Task Status 🛔 Device Manager View 🗸 🚰 Storage Refresh Status of tasks that have started in the following time period: Last 24 hours 📅 Disk Management ? Help > 🚠 Services and Applications Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed Task Name Run Result Run Start Run End Triggered E < Active Tasks Active tasks are tasks that are currently enabled and have not expired. Summary: 154 total Refresh Last refreshed at 4/12/2021 9:11:42 PM <

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.



Protect. Comply. Relax. P a g e | 4