如何修正來自CTR的電子郵件

目錄

<u>簡介</u>

<u>背景資訊</u>

<u>採用元件</u>

<u>設定</u>

<u>驗證</u>

步驟1.根據訪問可用伺服器的情況訪問CTR門戶並進行調查

<u>步驟2.使用支援的觀察量調檢視似惡意或威脅的已傳送郵件。可觀察量可以通過以下標準進行搜尋</u> <u>,如圖所示:</u>

<u>2.1以下IP調查和調查的示例,如下圖所示:</u>

<u>2.2以下是在郵件補救之前您收件箱中獲得的內容,如下圖所示:</u>

_____2.3按一下「Cisco Message ID」(思科消息ID)後,從選單選項中選擇任何支援的修正操作 ,如下圖所示:

_____2.4在本例中,「Initiate Forward」被選中,並在右下角出現「Success」彈出視窗,如下圖 所示:

_____2.5在ESA中,您可以看到「mail logs」下的以下日誌,其中顯示「CTR」補救已啟動、已選 <u>擇的操作和最終狀態。</u>

_____2.7在配置ESA/SMA模組時鍵入的電子郵件地址是在選擇「轉發」或「轉發/刪除」選項時接 收修正電子郵件的地址,如下圖所示:

_____2.8最後,如果您檢視ESA/SMA新介面的郵件跟蹤詳細資訊,您會看到「mail_logs」和「 Last State」中獲取的日誌與「Remediated」相同,如下圖所示:

簡介

本文說明如何修正來自思科威脅回應(CTR)的電子郵件。

背景資訊

已更新CTR調查以支援按需郵件補救。管理員可以搜尋來自O365和OnPrem Exchange使用者郵箱的特定電子郵件,並通過郵件安全裝置(ESA)或安全管理裝置(SMA)對其進行補救。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- CTR帳戶
- 思科安全服務交換
- ESA AsycnOs 14.0.1-033

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

附註:僅支援O365、Exchange 2016和2019混合部署以及本地2013 Exchange部署中的搜尋 和郵件補救。

設定

- 1. <u>在ESA中配置帳戶設定</u>
- 2. 配置鏈結配置檔案並將域對映到帳戶配置檔案
- 3. <u>將CTR與ESA或SMA整合</u>

驗證

您可以調查CTR門戶中的可觀察量,並使用以下步驟選擇用於補救的消息:

步驟1.根據訪問可用伺服器的情況訪問CTR門戶並進行調查

- US <u>https://visibility.amp.cisco.com/investigate</u>
- APJC https://visibility.apjc.amp.cisco.com/investigate
- 歐盟<u>https://visibility.eu.amp.cisco.com/investigate</u>

步驟2.使用支援的觀察量調檢視似惡意或威脅的已傳送郵件。可觀察量可以通過以下 標準進行搜尋,如圖所示:

IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123- abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

2.1以下IP調查和調查的示例,如下圖所示:





2.2以下是在郵件補救之前您收件箱中獲得的內容,如下圖所示:



2.3按一下「Cisco Message ID」(思科消息ID)後,從選單選項中選擇任何支援的修正操作 ,如下圖所示:



2.4在本例中,「Initiate Forward」被選中,並在右下角出現「Success」彈出視窗,如下圖所示:

Graph Filters: Show All, Expanded • Showing 11 nodes	& / ···	Results	8.7 ···
		Details	
- 🖂	- 🛛	Cisco Message ID	
Corp Mesos No Stated 640962-564D203017654DD782E6		640962-564 Ciaco Message ID No threat objects found.	Cisco Message ID No threat objects found.
🖂 Cisco Message ID	8	mexesa.com	
Add to current Investigation	~ here a	Domain	
Investigate in Threat Response		@ amacorra@cis	
Create Judgement	sert -{ @ }	Email Address	
Email Security Appliance	Transferration of the second s	ee@mexesa.c	
 Initiate Deletion 	· initiation ·	Email Address	
 Initiate Forward 	0	remediation test	
 Initiate Forward/Delete 	+	Email Subject	Success
Threat Grid	· · · · · · · · · · · · · · · · · · ·	test 1	Initiate Forward
Search 640962-564D203017654DD782	× =	TR + E Subject	

2.5在ESA中,您可以看到「mail_logs」下的以下日誌,其中顯示「CTR」補救已啟動、已選 擇的操作和最終狀態。

Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

Mon Sep 13 23:38:06 2021 Info: Message 640962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'. Remediation status: Remediated.

2.6語句「[Message Remediated]」顯示在消息主題的前面,如下圖所示:

[Message Remediated]remediation test		
ES	Escalation Support This message is forwarded as part of the mailbox remediation process.	
0	You forwarded this message on Mon 9/13/2021 11:39 PM	
-th-th- cisco	amacorra@cisco.com Mon 9/13/2021 11:26 PM	
	remediation test	

2.7在配置ESA/SMA模組時鍵入的電子郵件地址是在選擇「轉發」或「轉發/刪除」選項時接 收修正電子郵件的地址,如下圖所示:



2.8最後,如果您檢視ESA/SMA新介面的郵件跟蹤詳細資訊,您會看到「mail_logs」和「Last State」中獲取的日誌與「Remediated」相同,如下圖所示:

\checkmark	Email Gateway	Monitoring Tracking Quarantine	admin 🛓 ? 🌣 🔤 🕼 SECURE
⊜	Message Tracki	ng	
	Message ID Hea	der <18fb39\$jhu2@mail.sergio.com>	< Previous Next >
	Processing Det	ails	Envelope Header and Summary Last State
	Summary		Remediated
	23:24:41	Start message 640962 on incoming connection (ICID 31).	Message Incoming
	23:24:41	Message 640962 enqueued on incoming connection (ICID 31) from amacorra@cisco.com.	MID 640962
	23:24:41	Message 640962 direction: incoming	Time 13 Sec 2021 23:24:41 (GMT +05:00)
	23:24:48	Message 640962 on incoming connection (ICID 31) added recipient (ee@mexesa.com).	Sender
	23:25:07	Message 64/09/2 onginal subject on injection: remediation test	amacorraepoisco.com Recipient
	23:25:07	Message 640962 (145 bytes) from amacorra@cisco.com ready.	ee@mexesa.com Subject
	23:25:07	Message 640962 has sender_group: whitelist, sender_ip: 15.0.0.59 and sbrs: None	remediation test Sender Group
	23:25:07	Message 640962 matched per-recipient policy ee for inbound mail policies.	whitelist
	23:25:07	Message 640962 scanned by Advanced Malware Protection engine. Final verdict: SKIPPED(no attachment in message)	(Name unresolved, SN:564D203017654DD782E6- ADB1CB8ECD45)
	23:25:07	Message 640962 scanned by Outbreak Filters. Verdict: Negative	Incoming Policy Match
	23:25:07	Message 640962 contains message ID header '<18fb39\$jhu2@mail.sergio.com>'.	ee Message Size
	23:25:07	Message 640962 queued for delivery.	145 (Bytes) Attachments
	23:25:08	(DCID 6) Delivery started for message 640962 to ee@mexesa.com.	N/A
	23:25:10	UC-RU b) Univery details: Message 040962 sent to de@mexesa.com	Sending Host Summary
	23.23:10	Hostname=BY3PR19MB5169.namprd19.prod.outlook.com] 8351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery.	Reverse DNS hostname
	23:29:50	Incoming connection (ICID 31) lost.	IP address
	23:38:03	nessage o4usez was instated for informedial action by "admin" from source "CTR" in batch "2546dcal-953d-404c-9327-1114(d5d85c2".	15.0.0.59 SBRS Score
	23:38:06	j messenge vervarez mes processes min normana remedial action for recipient elegimexess.com in patch 2040dC8F-9030-4046-9327- f114fd5d89c7', Remediation status: Remediated.	None
		X III Home	
		Copyright Control Control and Annual An	

附註:可能會發生多個補救,如果您在ESA/SMA中配置搜尋和補救功能,則可以從CTR和 ESA/SMA補救同一消息。這允許您將同一郵件轉發到與整合模組中配置的郵件地址不同的<u>郵</u> 件地址。