Remediación de correos electrónicos de CTR

Contenido

Introducción

Antecedentes

Componentes Utilizados

<u>Configurar</u>

Verificación

Paso 1. Acceda al portal CTR en función del acceso a los servidores disponibles e investigue Paso 2. Investigue los mensajes entregados que parecen ser maliciosos o una amenaza utilizando los observables admitidos. Se puede buscar en los objetos observables según los siguientes criterios, como se muestra en la imagen:

2.1 Ejemplo de una investigación e investigación de IP a continuación, como se muestra en las imágenes:

2.2 Esto es lo que obtiene en la bandeja de entrada antes de que se solucione el mensaje, como se muestra en la imagen:

2.3 Al hacer clic en "ID de mensaje de Cisco", seleccione entre las opciones de menú cualquiera de las acciones remediadas admitidas, como se muestra en la imagen:

2.4 En este ejemplo, se selecciona "Iniciar reenvío" y aparece una ventana emergente de éxito en la esquina inferior derecha, como se muestra en la imagen:

2.5 En el ESA, puede ver los siguientes registros en "mail logs" que muestran que se inicia la remediación "CTR", la acción seleccionada y el estado final.

2.6 La instrucción "[Message Remediated]" aparece precedida en el asunto del mensaje, como se muestra en la imagen:

2.7 La dirección de correo electrónico que escriba al configurar el módulo ESA/SMA es la que recibe los correos electrónicos corregidos al seleccionar la opción "Reenviar" o "Reenviar/Eliminar", como se muestra en la imagen:

2.8 Por último, si observa los detalles del seguimiento de mensajes de la nueva interfaz de ESA/SMA, puede ver los mismos registros obtenidos en los "mail_logs" y el "Last State" como "Remediated", como se muestra en la imagen:

Introducción

Este documento describe cómo solucionar los correos electrónicos de Cisco Threat Response (CTR).

Antecedentes

La investigación de CTR se ha actualizado para admitir OnDemand Mail Remediation. Los administradores pueden buscar correos específicos de los buzones de correo de usuario de O365 y OnPrem Exchange y remediarlos mediante un dispositivo de seguridad de correo electrónico (ESA) o un dispositivo de administración de seguridad (SMA).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cuenta CTR
- Intercambio de servicios de seguridad de Cisco
- ESA AsycnOs 14.0.1-033

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Nota: La búsqueda y la remediación de correo se admiten únicamente en implementaciones híbridas de O365, Exchange 2016 y 2019 y en implementaciones de Exchange in situ 2013.

Configurar

- 1. Configuración de la Configuración de la Cuenta en el ESA
- 2. Configure el perfil en cadena y asigne los dominios al perfil de cuenta
- 3. Integración de CTR con ESA o SMA

Verificación

Puede investigar los elementos observables en el portal CTR y seleccionar el mensaje para la remediación mediante los pasos siguientes:

Paso 1. Acceda al portal CTR en función del acceso a los servidores disponibles e investigue

- EE. UU. https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- UE https://visibility.eu.amp.cisco.com/investigate

Paso 2. Investigue los mensajes entregados que parecen ser maliciosos o una amenaza utilizando los observables admitidos. Se puede buscar en los objetos observables según los siguientes criterios, como se muestra en la imagen:

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 Ejemplo de una investigación e investigación de IP a continuación, como se muestra en las imágenes:

$\leftarrow \rightarrow \mathbf{G}$	O A 🕫 https://visibility.amp.cisco.com/investigate			ជ	
threat Response	Threat Response Investigate Snapshots Incidents Intelligence				🗭 🕐 Alan Macorra ~
ip: "15.0.0.59"					
					0
Investigate Upload Sna	pshot What can I search for?				🚾 💿 Auto Omit
$\leftarrow \ \ \rightarrow \ \ C$	O A ≠ https://visibility.amp.cisco.com/invest	tigate?q=15.0.0.59		습	☞ 生 😞 🥥 🥌 ≡
threat Response	Investigate Snapshots Incidents Intelligen				🗭 ? Alan Macorra 🗸
C Add to Investigation V 1 of 1 enrichments complete 🥔 Automatic 3 Panel La					
2 Targets V	Q 1 Investigated ~	0 Omitted	ာင္ရွိ ⁰ 10 Related 🗸	0 Indicators	2 Modules V
Sightings					8 Z ···
My Environment (3) Globa					
4-1		2021-09-11120:01:26.0002 Maticious Suspicious Comm	2 - 2021-09-14104:24:41.0002 ton ⊯ Unknown ■ Clean ■ Targets		
3 -					
2 -					
	2021-09-11170:01:26.000Z	2621-09-1	1720-25-51.000Z	2021-09-14T04	2441.0007
Graph Filters: Show All Expande	ed • Showing 11 pades	a /	Results		a /
			Details		
	⊠ - (Ż	▼ 2 TARGETS		
	Cisco Messo 0 - Ensi 640960-564D24	il Subject ⊷ test 1	@ amacorra@cis		
			ee@mexesa.c		
	Clean Dorly	Ň			
	Target Emol	<u>@</u>	15.0.0.59	Please select an Obs	ervable/Target
		Target Email 🗸	3 Sightings in My Environm		
m	Domain Cedopal-S640203 exess.com	0	> 0 OMITTED		
		+			
	test 2 remediation te	× ::: =			

2.2 Esto es lo que obtiene en la bandeja de entrada antes de que se solucione el mensaje, como se muestra en la imagen:



2.3 Al hacer clic en "ID de mensaje de Cisco", seleccione entre las opciones de menú cualquiera de las acciones remediadas admitidas, como se muestra en la imagen:

Graph Fitters: Show All, Expanded + Showing 11 nodes	3.7	Results	0./ ···	
		Details		
⊠ <i>→</i>		Cisco Message ID	≅640962-564D203017654DD782E6-	
City Meinik Core Astatic Sector 640962-564D203017654D072826		640962-564 Cisco Message ID	Cisco Message ID No threat objects found.	
🖂 Cisco Message ID		2	mexesa.com	
Add to current Investigation Don		Comain		
Investigate in Threat Response			@ amacorra@cis	
Create Judgement Serve		Ernail Address		
Email Security Appliance	Terral Front	ee@mexesa.c		
 Initiate Deletion 		Ernail Address		
 Initiate Forward 	0			
 Initiate Forward/Delete 	+			
Threat Grid				
[3] Search 640962-564D203017654DD782		al Schinet		

2.4 En este ejemplo, se selecciona "Iniciar reenvío" y aparece una ventana emergente de éxito en la esquina inferior derecha, como se muestra en la imagen:



2.5 En el ESA, puede ver los siguientes registros en "mail_logs" que muestran que se inicia la remediación "CTR", la acción seleccionada y el estado final.

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 La instrucción "[Message Remediated]" aparece precedida en el asunto del mensaje, como se muestra en la imagen:



2.7 La dirección de correo electrónico que escriba al configurar el módulo ESA/SMA es la que recibe los correos electrónicos corregidos al seleccionar la opción "Reenviar" o "Reenviar/Eliminar", como se muestra en la imagen:

FW: [Message Remediated]remediation test		
ES	 Escalation Support <ee@mexesa.com></ee@mexesa.com> Alan Macorra Hernandez (amacorra) Monday, 13 September 2021, 23:39 Show Details 	
This message is forwarded as part of the mailbox remediation process.		
From: amacorra@cisco.com <amacorra@cisco.com> Sent: Tuesday, September 14, 2021 4:26:23 AM Subject: [Message Remediated]remediation test remediation test</amacorra@cisco.com>		

2.8 Por último, si observa los detalles del seguimiento de mensajes de la nueva interfaz de ESA/SMA, puede ver los mismos registros obtenidos en los "mail_logs" y el "Last State" como "Remediated", como se muestra en la imagen:

\triangleleft	Kemail Gateway Monitoring Tracking Quarantine admin 1 ? 🌣 🕴							
⊜	Message Tracking							
	Message ID Header <18fb39\$jhu2@mail.sergio.com>	< Previous Next >						
	Processing Details	Envelope Header and Summary						
	Summary	Last State 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						
	23:24:41 Message 640962 direction: incoming	Time						
	23:24:48 Message 640962 on incoming connection (ICID 31) added recipient (ee@mexesa.com).	13 Sep 2021 23:24:41 (GMT -05:00)						
	23:25:07 🕒 Message 640962 original subject on injection: remediation test	Sender amacorra@cisco.com						
	23:25:07 Message 640962 not evaluated for Sender Domain Reputation. Reason: Disabled at Mail Flow Policy	Recipient ee@mexesa.com						
	23:25:07 🐞 Message 640962 (145 bytes) from amacorra@cisco.com ready.	Subject						
	23:25:07 Message 640962 has sender_group: whitelist, sender_ip: 15.0.0.59 and sbrs: None	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 '<18/b39\$jhu2@mail.sergio.com>'.	ee Messace Size						
	23:25:07 Message 640962 queued for delivery.	145 (Bytes)						
	23:25:08 (DCID 6) Delivery started for message 640962 to ee@mexesa.com.	Attachments N/A						
	23:25:10 (DCID 6) Delivery details: Message 640962 sent to ee@mexesa.com							
	23:25:10 Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18/b395/bu2@mail.sergio.com> [Internalid=2722150272767/ Hostname=BY3PR19MIB5169.namprd19.prod.outlook.com] 8351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery'.	6, Sending Host Summary Reverse DNS hostname						
	23:29:50 Incoming connection (ICID 31) lost.	(unverified)						
	23:38:03 💧 Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89	IP address hc7'. 15.0.0.59						
	23:38:06 () Message 640962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327 f114fd5d89c7', Remediation status: Remediated.	- SBRS Score None						
	Copyrigh 🗙 🏭 Horne 🗔 + 🗄 L. [Privacy States	ment						

Nota: Pueden ocurrir varias soluciones, si configura en su ESA/SMA la función para buscar y remediar, puede remediar el mismo mensaje de CTR y también de ESA/SMA. Esto puede permitirle reenviar el mismo mensaje a una dirección de correo electrónico diferente a la configurada en el módulo de integración.