How to Remediate Emails from CTR

Contents

Introduction Background Information

Components Used

Configure

Verification

Step 1. Access the CTR Portal based on the access to available servers and investigate Step 2. Investigate the delivered messages that seem to be malicious or a threat by using the supported observables. Observables can be searched by the following criteria, as shown in the image:

2.1 An example of an IP investigation and Investigation below, as shown in the images:

2.2 Here is what you get in your inbox before the message gets remediated, as shown in the image:

2.3 On clicking "Cisco Message ID", select from menu options any of the supported Remediated Actions, as shown in the image:

2.4 In this example, "Initiate Forward" is selected and a Success popup window appears in the lower right corner, as shown in the image:

2.5 In the ESA, you can see the following logs under "mail_logs" that show that the "CTR" remediation initiates, the action selected, and the final status.

2.6 The statement "[Message Remediated]" appears prepended in the subject of the message, as shown in the image:

2.7 The email address you type in when configuring the ESA/SMA module is the one that receives the remediated emails when selecting the "Forward" or "Forward/Delete" option, as shown in the image:

2.8 Finally, if you look at the message tracking details of the new interface of the ESA/SMA, you can see the same logs obtained in the "mail_logs" and the "Last State" as "Remediated", as shown in the image:

Introduction

This document describes how to remediate emails from Cisco Threat Response (CTR).

Background Information

CTR investigation has been updated to support OnDemand Mail Remediation. Admin can search specific emails from O365 and OnPrem Exchange user mailboxes and remediate them through an Email Security Appliance (ESA) or Security Management Appliance (SMA).

Components Used

The information in this document is based on these software and hardware versions:

- CTR Account
- Cisco Security Services Exchange
- 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. If your network is live, ensure that you understand the potential impact of any command.

Note: Search and Mail Remediation is supported in O365, Exchange 2016 & 2019 Hybrid Deployments, and On-Prem 2013 Exchange Deployments only.

Configure

- 1. Configure Account Settings in the ESA
- 2. Configure Chained Profile and Map the Domain(s) to the Account Profile
- 3. Integrate CTR with either ESA or SMA

Verification

You can investigate the observables in the CTR Portal and select the message for remediation using the below steps:

Step 1. Access the CTR Portal based on the access to available servers and investigate

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

Step 2. Investigate the delivered messages that seem to be malicious or a threat by using the supported observables. Observables can be searched by the following criteria, as shown in the image:

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 An example of an IP investigation and Investigation below, as shown in the images:

$\leftarrow \rightarrow \mathbf{G}$	C A #2 https://visibility.amp.cisco.com/invet	stigate		습	
dialo Threat Response	e ^{li} : Threat Response Investigate Snapshots Incidents Intelligence				🝘 ? Alan Macorra ~
ip: "15.0.0.59"					
					٢
Investigate Upload Sna	pshot What can I search for?				👀 Auto Omit
$\leftarrow \ \ \rightarrow \ \ \sigma$	O A ≠ https://visibility.amp.cisco.com/invest	igate?q=15.0.0.59		\$	☺ 👱 😞 🤤 🦉 🖷 ≡
cisco Threat Response	Investigate Snapshots Incidents Intelligence				P ? Alan Macorra ~
Add to Investigation	New Investigation Snapshots Y	1 of 1 enrichments complete 📣			
2 Targets ~	Q 1 Investigated ~	0 Omitted	م م 10 Related م	0 Indicators	2 Modules 🗸
Sightings					8 Z ···
My Environment (3) Global (3) 2021-09-11720.0126.0002 - 2021-09-14T04:26:41.0002 Malfolous Suspicious 4 3 2 1					
	2021-09-11T20.01.26.000Z	2021-09-	11720;25:51.000Z	2021-09-14T04	1.24.41.000Z
Graph Filters: Show All, Expande	ed v Showing 11 nodes	3. / ···	Results		87
		≏ \	Details		
	Core Message 0 ~ Core Details 1 ~ Core Core Core Core Core Core Core Core	No Alexed V PRE 1 Targuil final V () +	armacorra@cis_ ensi ensi ensi armacorra@cis_	Please select an Obs	ervable/Target

2.2 Here is what you get in your inbox before the message gets remediated, as shown in the image:



2.3 On clicking "Cisco Message ID", select from menu options any of the supported Remediated Actions, as shown in the image:



2.4 In this example, "Initiate Forward" is selected and a Success popup window appears in the lower right corner, as shown in the image:

Graph Filters: Show All, Expanded + Showing 11 nodes	8 / ···	Results	8. / ···
	•	Details	
$\bowtie \rightarrow \emptyset$		Cisco Message ID	☑640962-564D203017654DD782E6-
Caco Mession 00 →	H Sutject ↓ Nesk 1	640962-564 Cisco Message ID	Cisco Message ID No threat objects found.
🖂 Cisco Message ID		mexesa.com	
Add to current Investigation	~		
Investigate in Threat Response		amacorra@cis	
Create Judgement Som	{ @ }	Email Address	
Email Security Appliance	Turnet Freed	ee@mexesa.c	
 Initiate Deletion 	angut binar 🗸	Email Address	
 Initiate Forward 	\odot		
 Initiate Forward/Delete 	+		Success
Threat Grid	<u> </u>		Initiate Forward
Search 640962-564D203017654DD782	× = 1	J I Subject	

2.5 In the ESA, you can see the following logs under "mail_logs" that show that the "CTR" remediation initiates, the action selected, and the final status.

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 The statement "[Message Remediated]" appears prepended in the subject of the message, as shown in the image:



2.7 The email address you type in when configuring the ESA/SMA module is the one that receives the remediated emails when selecting the "Forward" or "Forward/Delete" option, as shown in the image:

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 Finally, if you look at the message tracking details of the new interface of the ESA/SMA, you can see the same logs obtained in the "mail_logs" and the "Last State" as "Remediated", as shown in the image:

\triangleleft	Email Gateway Monitoring Tracking Qui	arantine	admin 💄 ? 🌣 🔤 🖞 tesset: SECURE			
⊜	Message Tracking					
	Message ID Header <18fb39\$jhu2@mail.sergio.com>		<pre> Previous Next ></pre>			
	Processing Details		Envelope Header and Summary			
	Summary		Last State Remediated			
	23:24:41 Start message 640962 on incoming connection (K	CID 31).	Message Incoming			
	23:24:41 Message 640962 enqueued on incoming connecti	ion (ICID 31) from amacorra@cisco.com.	MID 640962			
	23:24:47 Message 640962 direction: incoming 23:24:48 Message 640962 on incoming connection (ICID 3)	1) added recipient (ee@mexesa.com).	Time 13 Sep 2021 23:24:41 (GMT -05:00)			
	23:25:07 Message 640962 original subject on injection: rem	nediation test	Sender amacorra@cisco.com			
	23:25:07 Message 640962 not evaluated for Sender Domain	n Reputation. Reason: Disabled at Mail Flow Policy	Recipient ee@mexesa.com			
	23:25:07 Message 640962 (145 bytes) from amacorra@cise	co.com ready.	Subject remediation test			
	23:25:07 Message 640962 has sender_group: whitelist, ser	nder_ip: 15.0.0.59 and sbrs: None	Sender Group whitelist			
	23:25:07 Message 640962 matched per-recipient policy ee 23:25:07 Message 640962 scanned by Advanced Malware	Protection engine. Final verdict: SKIPPED(no attachment in message)	Cisco Hostname (Name unresolved, SN:564D203017654DD782E6-			
	23:25:07 Message 640962 scanned by Outbreak Filters. Ve	rdict: Negative	ADB1CB8ECD45) Incoming Policy Match			
	23:25:07 Message 640962 contains message ID header '<1	8fb39\$jku2@mail.sergio.com>".	ee Mossage Size			
	23:25:07 Message 640962 queued for delivery.		145 (Bytes) Attachments			
	23:25:08 (DCID 6) Delivery started for message 640962 to 0 23:25:10 (DCID 6) Delivery details: Message 640962 sont to	ee@mexesa.com.	N/A			
	23:25:10 Message 640962 to ee@mexesa.com received re	mote SMTP response '2.6.0 <18fb39\$jhu2@mail.sergio.com> [internalId=27221502727676,	Sending Host Summary			
	Hostname=BY3PR19MB5169.namprd19.prod.outk 23:29:50 Incoming connection (ICID 31) lost.	ook.com] 6351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery'.	Reverse DNS hostname (unverified)			
	23:38:03 Message 640962 was initiated for "Forward" reme	dial action by 'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.	IP address 15.0.059			
	23:38:06 () Message 640962 was processed with 'Forward f114fd5d89c7'. Remediation status: Remediate	r remedial action for recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327- d.	SBRS Score None			
		Copyrigh 🗙 🏭 Home 💿 + 🗐 s. Privacy Statement				

Note: Several remediations can happen, if you configure in your ESA/SMA the feature to search and remediate, you can remediate the same message from CTR and also from ESA/SMA. This can allow you to forward the same message to a different email address than the one configured in the <u>integration module</u>.