如何修复来自CTR的邮件

目录

<u>简介</u>

<u>背景信息</u>

<u>使用的组件</u>

<u>配置</u> 确认

<u>步骤2.使用支持的可观察信息来调查似乎是恶意或威胁的已传送邮件。可按以下标准搜索可观察项</u> <u>,如图所示:</u>

<u>2.1下图所示的IP调查和调查示例:</u>

<u>2.2如图所示,在修复邮件之前,您收到的收件箱内容如下:</u>

_____2.3单击"思科消息ID",从菜单选项中选择任何受支持的补救操作,如图所示:

____2.4在本例中,选择"Initiate Forward",并在右下角显示"Success"弹出窗口,如图所示:

_____2.5在ESA中,您可以在"mail_logs"下看到以下日志,这些日志显示"CTR"补救已启动、已选 操作和最终状态。

<u>2.6语句"[Message Remediated]"在消息主题中出现前置,如图所示:</u>

_____2.7在配置ESA/SMA模块时键入的电子邮件地址是在选择"转发"或"转发/删除"选项时接收修正 电子邮件的地址,如图所示:

_____2.8最后,如果您查看ESA/SMA新接口的消息跟踪详细信息,可以看到在"mail_logs"和"Last State"中获取的日志与"Remediated"相同,如图所示:

简介

本文档介绍如何从思科威胁响应(CTR)修复邮件。

背景信息

CTR调查已更新,以支持按需邮件补救。管理员可以搜索来自O365和OnPrem Exchange用户邮箱 的特定电子邮件,并通过邮件安全设备(ESA)或安全管理设备(SMA)进行补救。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- CTR帐户
- 思科安全服务交换
- ESA AsycnOs 14.0.1-033

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。 注意:O365、Exchange 2016和2019混合部署和2013内部部署仅支持搜索和邮件补救。

配置

- 1. 在ESA中配置帐户设置
- 2. 配置链接的配置文件并将域映射到帐户配置文件
- 3. <u>将CTR与ESA或SMA集成</u>

确认

您可以使用以下步骤调查CTR门户中的可观察项,并选择用于补救的消息:

步骤1.根据对可用服务器的访问权限访问CTR门户并调查

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

步骤2.使用支持的可观察信息来调查似乎是恶意或威胁的已传送邮件。可按以下标准 搜索可观察项,如图所示:

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下图所示的IP调查和调查示例:

$\leftarrow \rightarrow \mathbf{G}$	O A ≠2 https://visibility.amp.cisco.com/investigate	습 🛛 🙁 🗟 🥥 🚍 🚍				
diale Threat Response	Investigate Snapshots Incidents Intelligence	 (a) (b) (c) (c)				
ip: "15.0.0.59"						
		٩				
Investigate Upload Sn	apshot What can I search for?	Constanti Auto Omit				



2.2如图所示,在修复邮件之前,您收到的收件箱内容如下:



2.3单击"思科消息ID",从菜单选项中选择任何受支持的补救操作,如图所示:



2.4在本例中,选择"Initiate Forward",并在右下角显示"Success"弹出窗口,如图所示:



2.5在ESA中,您可以在"mail_logs"下看到以下日志,这些日志显示"CTR"补救已启动、已选操 作和最终状态。

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语句"[Message Remediated]"在消息主题中出现前置,如图所示:



2.7在配置ESA/SMA模块时键入的电子邮件地址是在选择"转发"或"转发/删除"选项时接收修正 电子邮件的地址,如图所示:



2.8最后,如果您查看ESA/SMA新接口的消息跟踪详细信息,可以看到在"mail_logs"和"Last State"中获取的日志与"Remediated"相同,如图所示:

\triangleleft	Email Gateway	Monitoring Tracking Quarantine	admin 🕹 ? 🌣 🔤 🐮 SECURE
⊜	Message Trackir	g	
	Message ID Hea	der <18fb39\$jhu2@mail.sergio.com>	< Previous Next >
	Processing Det	ils	Envelope Header and Summary
	Summary		Last State Remodiated
	23:24:41	Start message 640962 on incoming connection ((CID 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 Message 640962 or incoming Message 640962 or incoming connection (ICID 31) added recipient (w/Bmexes com)	Time 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 remediation test
	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.	Cisco Hostname
	23:25:07	Message 640/962 scanned by Advanced Malware Protection engine. Hinal verticit: SKIPPED(no attachment in message) Messane 640/962 scanned by Dirthveck Eliters. Variative Nenative	ADB1CB8ECD45)
	23:25:07	Message 640962 contains message ID header '«18fb395/bu2@mail.sergio.com»'.	Incoming Policy Match ee
	23:25:07	Message 640962 queued for delivery.	Message Size 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	Service Host Summan
	23:25:10	Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18/b39\$/bu2@mail.sergio.com> [Internald=27221502727676, 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.	(unverified) IP address
	23:38:03	Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.	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.	None
		Copyrigh 🗙 III Home 🖂 + II 1.1 PW/acy Statement	

注意:若在ESA/SMA中配置搜索和补救功能,则可以从CTR和ESA/SMA补救相同的消息。这 允许您将同一邮件转发到与集成模块中配置的邮件地址不同的<u>邮件地址</u>。