思科郵件安全高級惡意軟體防護(AMP)最佳實踐 指南

目錄

<u>簡介</u>

<u>驗證功能金鑰</u> <u>啟用高級惡意軟體防護(AMP)</u> 自定義高級惡意軟體防護(AMP)全域性設定 <u>檔案分析閾值設定</u> <u>將ESA與面向終端的AMP控制檯整合</u> <u>啟用郵箱自動補救(MAR)</u> <u>在郵件策略中配置高級惡意軟體防護(AMP)</u> <u>將SMA與思科威脅響應(CTR)整合</u> <u>結論</u>

簡介

高級惡意軟體防護(AMP)是一個全面的解決方案,可實現惡意軟體檢測和攔截、持續分析和追溯性 警報。利用AMP和Cisco Email Security可實現跨攻擊過程(攻擊前、攻擊中和攻擊後)的卓越保護 ,並採用最經濟高效、部署最簡單的高級惡意軟體防禦方法。

此最佳實踐文檔將涵蓋思科郵件安全裝置(ESA)上的AMP的主要功能,如下所示:

- 檔案信譽 在檔案通過ESA時捕獲每個檔案的指紋,並將其傳送到AMP基於雲的情報網路進 行信譽鑑定。根據這些結果,您可以自動阻止惡意檔案並應用管理員定義的策略。
- 檔案分析 提供分析通過ESA的未知檔案的功能。高度安全的沙盒環境使AMP能夠收集有關 檔案行為的準確詳細資訊,並將這些資料與詳細的人力和機器分析相結合,以確定檔案的威脅 級別。然後,此配置被饋入基於AMP雲的智慧網路,並用於動態更新和擴展AMP雲資料集以增 強保護。
- 郵箱自動補救(MAR) 對於Microsoft Office 365和Exchange 2013/2016,可自動刪除包含檔案且在初始檢查點後變為惡意的電子郵件。這節省了管理員的工作時間,並有助於控制威脅的影響。
- Cisco AMP Unity -允許組織在AMP for Endpoints控制檯中註冊其啟用AMP的裝置(包括ESA和 AMP訂用)的功能。通過此類整合,思科電子郵件安全可以像面向終端的AMP控制檯已提供的 方法一樣檢視和查詢示例觀察結果,並允許在一個使用者介面中關聯所有威脅媒介中的檔案傳 播資料。
- Cisco Threat Response 是一個協調平台,將來自思科和第三方來源的安全相關資訊整合到 單個直觀的調查和響應控制檯中。它通過作為事件日誌和威脅情報整合框架的模組化設計來實 現這一點。模組通過構建關係圖快速關聯資料,從而使安全團隊能夠清楚地瞭解攻擊,並快速 做出有效的響應操作。

驗證功能金鑰

- 在ESA上,導航到System Administration> Feature Keys
- •查詢「檔案信譽」和「檔案分析」功能鍵,並確保狀態為「活動」

啟用高級惡意軟體防護(AMP)

- 在ESA上, 導航至Security Services >Advanced Malware Protection File Reputation and Analysis
- 按一下Advanced Malware Protection 全域性設定:

Advanced Halware Protection	
File Reputation:	Enabled
File Analysis:	Enabled
	Rela Clobal Sattinas

• 提交更改。

自定義高級惡意軟體防護(AMP)全域性設定

- AMP現已啟用,按一下Edit Global Settings以自定義全域性設定。
- 副檔名清單將不時自動更新,因此請始終訪問此設定並確保已選擇所有副檔名:



- 展開**檔案信譽的高級設定**
- 檔案信譽伺服器的預設選擇為AMERICA(cloud-sa.amp.cisco.com)
- 點選下拉選單,然後選擇最近的檔案信譽伺服器(特別適用於APJC和歐洲客戶):

* Advanced Bettings for File Reputation	Pile Reputation Server	AMERICAS (cloud-second clico core)	0
	ANP for Endpoints Console Integration $\langle\Xi\rangle$	AMERICALLAGEO() (Claud-salampics.com/miceo) (SURDPE (cloud-salamano.chece.com)	erso: () Deregister
	556, Communication for file Reputation	APUE (close-tenage ang class pore) Proder my visite et and Turnel Procy (Sptional): Server: Upervane: Passylvase: Petage Reservace: Petage Contribute volation for Turnel Proce (7)	Pac
	Rearbest Interval	3 erste	
	Query Times.d:	d seconds	
	Processing Timesus:	TUB seconds	
	File Reputation Claim 30:	bc?9abd0-4463-4453-668a-73a3952a0434	
	Ne Ratraspective:	Suppress the vertilet update alorts (8)	

- 展開檔案分析的高級設置
- 檔案分析伺服器URL的預設選擇為AMERICAS(<u>https://panacea.threatgrid.com</u>)
- 點選下拉選單,然後選擇最近的檔案信譽伺服器(尤其適用於歐洲客戶):

File Analysis Server URL:

a fattings Advanced settings for Caulo

檔案分析閾值設定

(可選) 允許設定可接受的檔案分析得分的上限。根據閾值設定阻止的檔案在「高級惡意軟體防護

RIPS (https://peracos.fvestgrit.e.c

」報告的「傳入惡意軟體威脅檔案」部分中顯示為自定義閾值。

- •在AMP全域性設定頁面中,展開Threshold Settings。
- 雲服務的預設值為95。
- 選擇**輸入自定義值**的單選按鈕並更改值(例如70):
- 按一下Submit並提交更改

將ESA與面向終端的AMP控制檯整合

(<mark>僅適用於面向終端的AMP客戶)可通過面向終端的AMP控制檯建立統一的自定義檔案阻止列表</mark> (或檔案允許清單),並可跨安全架構(包括ESA)無縫分發包含策略。

Bee Nalue From Clead Service (M
 Deter Custom Value: 50

- 在AMP全域性設定頁面中,展開檔案信譽的高級設定
- 點選按鈕 Register Appliance with AMP for Endpoints:
- 按一下OK重定向到面向終端的AMP控制檯站點以完成註冊。
- 使用您的使用者憑據登入到AMP for Endpoints控制檯
- 按一下Allow授權ESA註冊:



ANY for Endpoints Canada 1 Tempistan (8) Jugistan Appliance with ANE for Endpoint

- 面向終端的AMP控制檯會自動將頁面切換回ESA。
- •確保註冊狀態顯示為SUCCESS:

AHP for Endpoints Conscie Integration (?) VLNESA000181_564D58189584A76C416D-4F8AA6579018 (?) Deregister 🗸 SUCCESS

• 按一下「Submit」,然後「Commit your changes」

啟用郵箱自動補救(MAR)

如果您有O365郵箱或Microsoft Exchange 2013/2016,則郵箱自動補救(MAR)功能將允許檔案信譽 判定從「清除/未知」更改為「惡意」時執行操作。

- 導覽至系統管理> 帳戶設定
- 在Account Profile下,按一下Create Account Profile以建立與您的Office 365和/或Microsoft Exchange郵箱的API連線配置檔案:

Account Profiles 😨			
Create Account Profile			
Account Profile Name	Profile Type	Description	Delete
exchange	Exchange On Premise		8

- 按一下「Submit」,然後「Commit your changes」
- (可選)鏈接配置檔案是配置檔案的集合,只有當要訪問的帳戶位於不同型別的部署的不同租 戶時,才配置連結配置檔案。
- 按一下Create Domain Mapping按鈕將您的帳戶配置檔案對映到收件人域。建議的設定如下所示:

Domain Mapping 🖸		
Domain Mapping configuration is not available since all profiles are already in	mapped	
Mailbox Profile/Chained Profile	Recipient Domain(s)	Delete
exchange	damein.com	

• 按一下「Submit」,然後「Commit your changes」

在郵件策略中配置高級惡意軟體防護(AMP)

在全域性配置了AMP和MAR後,您現在可以啟用服務以郵件策略。

- 導航到郵件策略 > 傳入郵件策略
- •通過按一下要自定義的策略的**高級惡意軟體防護**下的藍色連結,為傳入郵件策略自定義**高級惡** 意軟體防護設定。
- •出於此最佳實踐文檔的目的,按一下Enable File Reputation旁邊的單選按鈕,然後選擇Enable File Analysis:

Advanced Malware Protection Settings	
Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	

- •建議在消息中包含AMP結果的X報頭。
- 接下來的三節允許您選擇附件因郵件錯誤、速率限制或AMP服務不可用而被視為不可掃描時, ESA必須執行的操作。建議的操作是按原樣傳送,並在郵件主題上新增警告文本:

Unscannable Actions on Message Errors		
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No Yes
	Modify Message Subject:	No Prepend Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination	No Yes
	HOSE.	Host:
Unscannable Actions on Rate Limit		
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No Yes
	Modify Message Subject:	No Prepend Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination	No Yes
	HUSL.	Host:
Unscannable Actions on AMP Service Not Av	ailable	
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No 🖲 Yes
	Modify Message Subject:	No Prepend Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination	🖲 No 💿 Yes
	Host:	Host:

• 下一節將配置ESA在附件被視為惡意時丟棄該郵件:

Messages with Malware Attachments:	
Action Applied to Message:	Drop Hessage *
Archive Original Message:	© No
Drop Malware Attachments:	® No 0 Yes
Hodily Hessage Subject:	No. * Prepend Append
	WARNING: MALWARE DETECTED)
> Advanced	Optional sattings.

• 建議的操作是在為檔案分析傳送附件時隔離郵件:

Hessages with File Analysis Pending:	
Action Applied to Message:	Quarantine *
Archive Original Message:	O No 🕷 Yes
Modify Message Subject:	© No * Preparal © Apparal
	WARNING: ATTACHMENT(S) HAY CONTAIN
F Advanced	Optional settings.

 (僅適用於傳入郵件策略)配置在威脅判定變為惡意時要對傳送給終端使用者的郵件執行的補 救操作。建議的設定如下所示:

Enable Mailbox Auto Remediation (MAR))
Mailton Auto Remediation Actions apply only if Ac	count Settings are configured. See System Administration > Account Settings .
Action to be taken on message(s) in user's mailbox:	Forward to: Oelette Forward to: and Delete

• 按一下「Submit」,然後「Commit your changes」

將SMA與思科威脅響應(CTR)整合

SMA電子郵件模組的整合要求通過CTR使用安全服務交換(SSE)。SSE允許SMA向Exchange註冊 ,並且您為Cisco Threat Response提供訪問註冊裝置的明確許可權。該過程包括通過準備連結時生 成的令牌將SMA連結到SSE。

- •在CTR門戶(<u>https://visibility.amp.cisco.com</u>)上,使用您的使用者憑據登入。
- CTR使用模組與其他思科安全產品(包括ESA)整合。按一下Modules頁籤。
- 選擇Devices,然後按一下Manage Devices:

cisco Threat Response	Investigate Snapshots Incidents Beta Intelligence Modules
Settings > Devices	
Settings Your Account	Devices
Devices API Clients	Manage Devices Reload Devices
 CTR會將頁面透視到SSE。 按一下+圖示生成新標籤, 在關閉框之前複製新令牌: Add Devices and Gene 	然後按一下Continue。 rate Tokens ❹ ×
The following tokens have be	en generated and will be valid for 1 hour(s):
Tokens	
0ac7c30df02c0abfbe4869b8	085445c8
	Close Copy to Clipboard Save To File

- 在SMA上, 導航到Management Appliances頁籤> Network > Cloud Service Settings
- 按一下Edit Setting,確保Threat Response選項為Enable。
- 威脅響應伺服器URL的預設選擇為AMERICAS(api-sse.cisco.com)。對於EUROPE客戶,請按 一下下拉選單並選擇EUROPE(api.eu.sse.itd.cisco.com):

Cloud Service Settings		
Edit Cloud Services		
Threat Response:	i € Enable	
Threat Response Server:	AMERICAS (api-see.cisco.com)	
Cancel	EUROPE (spi.ev.sse.Rd.cisco.com)	Submit

- 按一下「Submit」,然後「Commit your changes」
- 將令牌金鑰(您從CTR門戶生成)貼上到雲服務設定中,然後按一下Register:

Registration Token: () Dec7:350493243e4565836055445c5 Register

- •完成註冊過程將需要一些時間,請在幾分鐘後導航回此頁以再次檢查狀態。
- 返回CTR > Modules > Device, 然後按一下Reload Device按鈕以確保SMA出現在清單中:

Threat Response	ivestigate Snapshots Incidents Beta Intelligence Modules					? 🔅
Settings > Devices						
Settings	Devices					
Your Account						
Devices	Managa Devices Rel	Manage Devices Dalaad Devices				
API Clients	Hanaye bevices					
> Modules	Name	Туре	Version	Description	ID	IP Address
Users	sma1	SMA	13.0.0-187	SMA	1	127.0.0.1

結論

本文檔旨在描述郵件安全裝置中的思科高級惡意軟體防護(AMP)的預設或最佳實踐配置。這些設定 大多數在入站和出站電子郵件策略上均可用,建議在兩個方向上都進行配置和過濾。