使用API從AMP門戶匯出應用阻止清單

目錄

<u>簡介</u> <u>必要求</u> <u>採用景程 證難</u> 算程 難 算 相 別 資 記

簡介

本文檔介紹使用API從面向終端的高級惡意軟體防護(AMP)應用阻止清單匯出資訊的過程。

作者:Uriel Montero和Yeraldin Sánchez,思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題:

- •訪問面向終端的思科AMP控制面板
- 來自AMP門戶的API憑證:第三方API客戶端ID和API金鑰,此連結顯示獲取這些證書的步驟:<u>如何從AMP門戶生成API憑據</u>
- 本文檔中的API處理程式使用Postman工具

採用元件

本檔案中的資訊是根據以下軟體:

- 適用於終端的思科AMP終端控制檯版本5.4.20190709
- 郵遞員工具

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。

相關產品

本檔案也適用於以下API版本:

• api.amp.cisco.com,v1

背景資訊

思科不支援Postman工具,如果您對此有疑問,請與Postman支援部門聯絡。

流程

這是使用API和Postman工具從選定清單中收集AMP應用程式阻止清單和SHA-256清單的過程。

步驟1。在Postman工具上,導覽至Authorization > Basic Auth,如下圖所示。

Params 🛛	Authorization 🔵
TYPE	
Basic Auth	v

步驟2.在「Username」部分新增第三方API客戶端ID,並在「Password」選項上新增API金鑰,如下圖所示。

Username	3rd Party API Client ID
Password	API key
	Show Password

步驟3.在API處理程式中,選擇GET請求並貼上命令:<u>https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0</u>。

- 限制:工具顯示的項數
- Offset:資訊開始顯示專案的位置
- 在此示例中,限制值為20,偏移量為60,資訊開始顯示清單61,限制值為80,如圖所示。

GE	r	*	https://api.a	amp.cisco.com/v1	/file_lists/ap	plication_blocking?limi	it=20&offset	-60	
Para	ms 🔵	Auth	orization 🖲	Headers (8)	Body	Pre-request Script	Tests		
Que	ry Param	s							
	KEY							VALUE	
\checkmark	limit							20	
~	offset							60	
	Key							Value	
Body	Cookies	; He	aders (20)	Test Results					
Pre	etty R	law	Preview	JSON 🔻	₽				

步驟4.在先前選定的應用程式阻止清單中,複製**guid**,然後運行命令:<u>https://api.amp.cisco.com/v1/file_lists/guid/files</u>,在此示例中,清單leisanch_blocking2的 guid為221f6ebd-1245-4d56-ab31-e6997f5779ea,如下圖所示。

543 - {	
544	"name": "leisanch blocking?".
545	"guid": "221f6ebd-1245-4d56-ab31-e6997f5779ea",
546	"type": "application_blocking",
547 🔻	"links": {
548	"file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
549	}

在AMP門戶上,應用阻止清單顯示新增的8個SHA-256代碼,如下圖所示。

leisanch_blocking2		
8 files	Created by Yeraldin Sanchez Mendo	za • 2019-03-26 18:48:02 CST
Used in policies: 🗮 WIN POLICY LEISANCH		
Used in groups: leisanch_gr	roup2, leisanch_RE-renamed_1	
 View Changes 		Edit Delete

使用命令<u>https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea</u>時,清單必須顯示8個SHA-256代碼,如下圖所示。

1 -	{			
2		"ver	'sion'	': "v1.2.0",
3 🔻		"met	adata	»": {
4 -			"link	<pre><s": pre="" {<=""></s":></pre>
5				<pre>'self": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea/files"</pre>
6			}.	
7 -			"resu	ults": {
8				'total": 8.
9				'current item count": 8.
10				'index": 0.
11				'items per page": 500
12			3	
13		1	,	
14 -		1) "dat		r
10		: uau	.a.) "nome	L M. "loiseach blocking?"
10			name	· · · · · · · · · · · · · · · · · · ·
10			guid	1 : 221T0eD0-1245-4050-aD51-e099/T5//9ea,
1/ -			boti	Icles": [
18 -			1	
19				"name": "WIN POLICY LEISANCH",
20				"guid": "768cdd65-dc8b-4301-82ae-60cb9bcbc57f",
21 🔻				"links": {
22				"policy": "https://api.amp.cisco.com/v1/policies/768cdd65-dc8b-4301-82ae-60cb9bcbc57f"
23				}
24]	
25],	
26 🔻			"iten	ns": [
27 🕶			{	
28				"sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c5",
29				"description": "first sha".
30				"source": "Created from SHAs in shasyeral.txt from
31 -				"links": {
32				"file list": "https://api.amp.cisco.com/v1/file lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
33				
34			1	
35 -			1	
36				"sha256"• "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c2"
37				"decription": "First sha"
38				"source": "[rested from SHAs in sharveral tyt from "
20 -				"Source: Created from Shas In Shasyeral.cxt from
10				IIIKS : {
40				"TILE_IIST": "nttps://api.amp.cisco.com/vi/Tile_Iists/221T0ebd-1245-4050-ab51-e099/T5//96a"
41				3
42			1	
43 -			{	
44				"sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c3"
45				"description": "first sha",
46				"source": "Created from SHAs in shasyeral.txt from ", ",
47 🔻				"links": {
48				"file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- <u>思科終端進階惡意軟體防護API</u>
- <u>面向終端的思科AMP 使用手册</u>
- 技術支援與文件 Cisco Systems