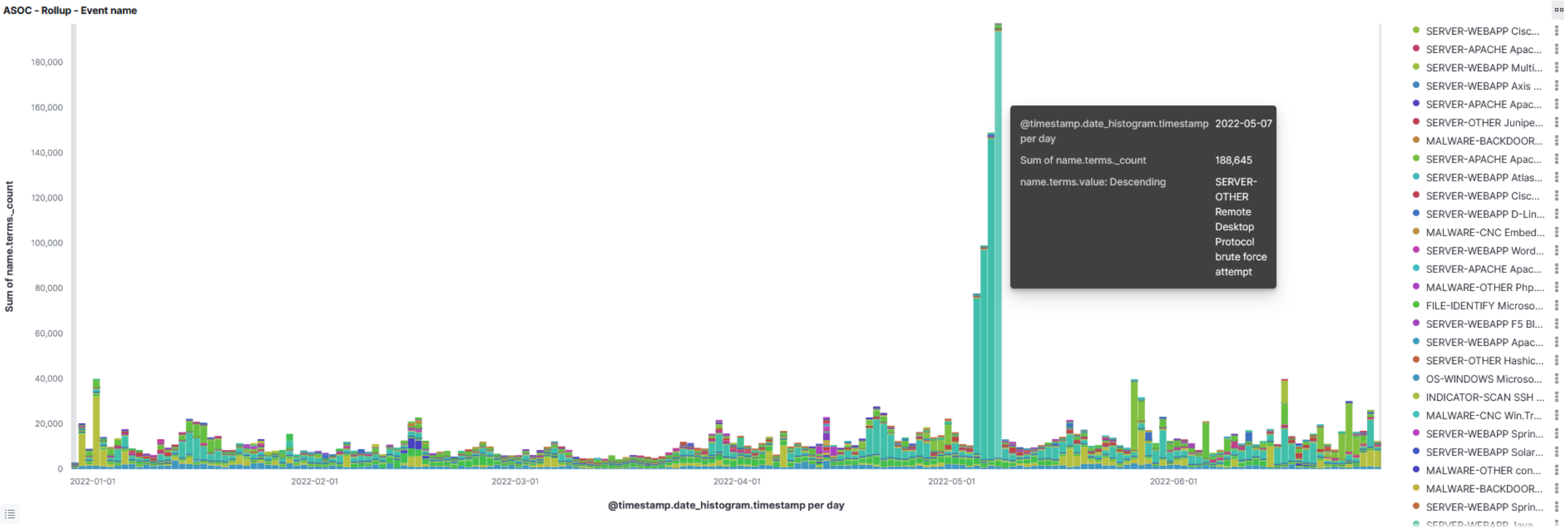
台大區網會議簡報

臺灣大學-北區ASOC 童鵬哲

2

區網事件趨勢

區網事件趨勢


ASOC - Rollup - Event name
Sum of name.terms._count
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
2022-01-01
2022-02-01
2022-03-01
2022-04-01
2022-05-01
2022-06-01
@timestamp.date_histogram.timestamp per day
@timestamp.date_histogram.timestamp per day 2022-05-07
Sum of name.terms._count 188,645
name.terms.value: Descending SERVER-OTHER Remote Desktop Protocol brute force attempt
SERVER-WEBAPP Cisc...
SERVER-APACHE Apac...
SERVER-WEBAPP Multi...
SERVER-WEBAPP Axis ...
SERVER-APACHE Apac...
SERVER-OTHER Junipe...
MALWARE-BACKDOOR...
SERVER-APACHE Apac...
SERVER-WEBAPP Atlas...
SERVER-WEBAPP Cisc...
SERVER-WEBAPP D-Lin...
MALWARE-CNC Embed...
SERVER-WEBAPP Word...
SERVER-APACHE Apac...
MALWARE-OTHER Php....
FILE-IDENTIFY Microso...
SERVER-WEBAPP F5 BI...
SERVER-WEBAPP Apac...
SERVER-OTHER Hashic...
OS-WINDOWS Microso...
INDICATOR-SCAN SSH ...
MALWARE-CNC Win.Tr...
SERVER-WEBAPP Sprin...
SERVER-WEBAPP Solar...
MALWARE-OTHER con...
MALWARE-BACKDOOR...
SERVER-WEBAPP Sprin...

提權攻擊

Event Top50 (rollup)

name.terms.value: Descending	Count
SERVER-WEBAPP MVPower DVR Shell arbitrary command execution attempt	64,929
SERVER-WEBAPP Netgear DGN1000 series routers authentication bypass attempt	63,308
SERVER-WEBAPP D-Link multiple products HNAP SOAPAction header command injection attempt	27,020
MALWARE-BACKDOOR MISC Linux rootkit attempt	24,688
SERVER-WEBAPP Drupal 8 remote code execution attempt	20,859
OS-WINDOWS Microsoft Windows SMB remote code execution attempt	20,183
MALWARE-BACKDOOR attempt	19,324
SERVER-OTHER Juniper ScreenOS unauthorized backdoor access attempt	19,211
MALWARE-BACKDOOR MISC Linux rootkit attempt lrkr0x	17,285
MALWARE-BACKDOOR MISC r00t attempt	17,074
OS-WINDOWS Microsoft Windows RDP MS_T120 channel bind attempt	15,521
MALWARE-BACKDOOR MISC rewt attempt	13,337
MALWARE-BACKDOOR MISC sm4ck attempt	12,980
SERVER-WEBAPP Java ClassLoader access attempt	11,457
SERVER-WEBAPP DD-WRT httpd cgi-bin remote command execution attempt	11,337

Application 攻撃

Event Top50 (rollup)

name.terms.value: Descending	Count
SERVER-WEBAPP GPON Router authentication bypass and command injection attempt	56,326
SERVER-WEBAPP PHPUnit PHP remote code execution attempt	51,788
SERVER-WEBAPP Apache HTTP Server httpd directory traversal attempt	30,172
SERVER-WEBAPP Zeroshell Linux Router command injection attempt	28,786
SQL 1 = 1 - possible sql injection attempt	23,317
SERVER-WEBAPP vBulletin pre-authenticated command injection attempt	17,904
SQL HTTP URI blind injection attempt	13,389
SQL url ending in comment characters - possible sql injection attempt	11,396
SERVER-WEBAPP WordPress wp-config.php access via directory traversal attempt	10,739
SQL generic sql with comments injection attempt - GET parameter	8,749
SERVER-WEBAPP Spring Cloud Gateway Spring Expression Language injection attempt	7,139
SERVER-WEBAPP Oracle WebLogic Server remote code execution attempt	4,864
SERVER-WEBAPP SolarWinds Orion authentication bypass attempt	4,825
SQL use of sleep function in HTTP header - likely SQL injection attempt	4,734
SERVER-WEBAPP Cisco ASA directory traversal attempt	4,391
SERVER-WEBAPP Citrix ADC and Gateway information disclosure attempt	4,375
SERVER-WEBAPP Pulse Secure SSL VPN arbitrary file read attempt	4,313

木馬CNC連線

Event Top50 (rollup)

name.terms.value: Descending	Count
MALWARE-CNC Win.Trojan.MirrorBlast outbound connection	31,670
MALWARE-CNC Unix.Trojan.Mirai variant post compromise echo loader attempt	12,078
INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgos...	10,440
MALWARE-BACKDOOR Arucer backdoor traffic - yes command attempt	10,097
MALWARE-CNC Unix.Trojan.Mirai variant post compromise activity	8,587
MALWARE-CNC known malicious SSL certificate - Odinaff C&C	8,193
MALWARE-CNC Win.Trojan.TorrentLocker/Teerac self-signed certificate	8,179
MALWARE-CNC Unix.Trojan.Mirai variant post compromise fingerprinting	5,793
MALWARE-CNC Win.Backdoor.Chopper web shell connection	5,355
MALWARE-CNC Torpig bot sinkhole server DNS lookup	4,229
MALWARE-CNC Win.Trojan.ZeroAccess inbound connection	3,955
MALWARE-OTHER Unix.Miner.Xbash variant dropped bash script	3,929
MALWARE-CNC Win.Trojan.Donvibs variant outbound connection	3,415
MALWARE-CNC Win.Trojan.Jadtre variant outbound connection	3,381
MALWARE-CNC User-Agent known malicious user-agent string SurfBear	2,929
MALWARE-OTHER Php.Webshell.AK74 inbound connection attempt	2,259

其他攻擊

Event Top50 (rollup)

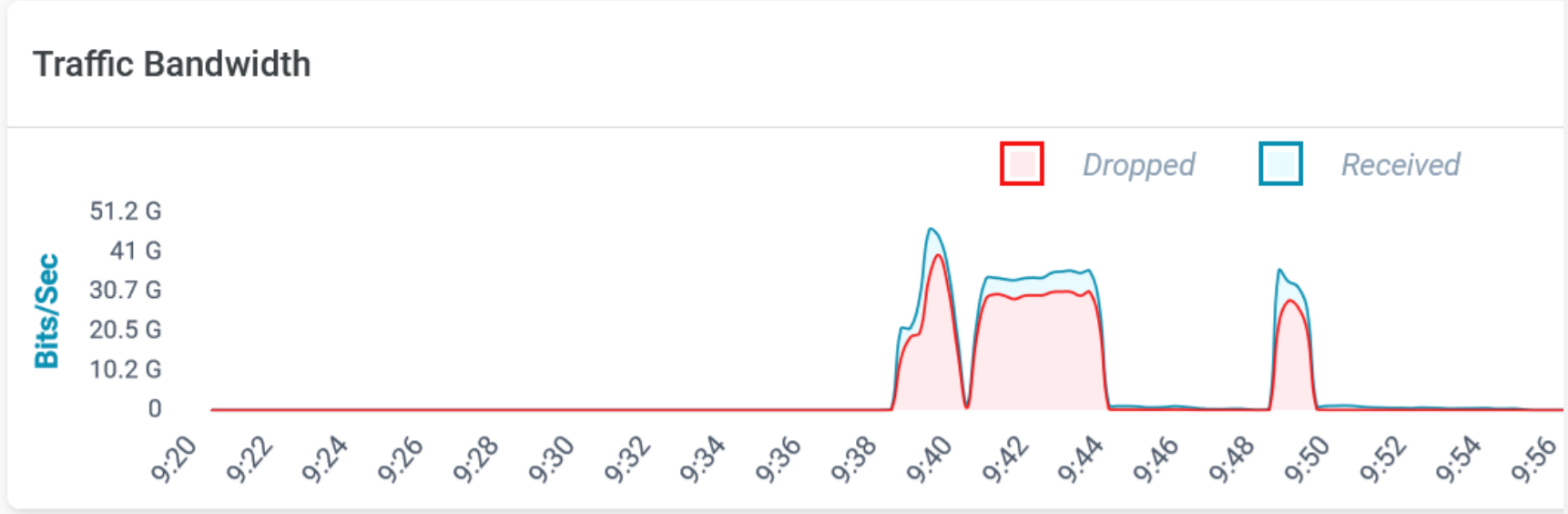
name.terms.value: Descending	Count
INDICATOR-SCAN SSH brute force login attempt	51,570
SERVER-OTHER Remote Desktop Protocol brute force attempt	43,625
MALWARE-BACKDOOR HideSource backdoor attempt	13,605
FILE-IDENTIFY Microsoft emf file download request	3,308
SERVER-OTHER Remote Desktop Protocol brute force attempt-outbound	797
INDICATOR-SCAN SSH brute force login attempt-outbound	571
POLICY-OTHER eicar test string download attempt	313
MALWARE-OTHER SimpleTDS - page redirecting to a SimpleTDS	212
MALWARE-CNC Vicepass outbound connection initial request to the CNC sending system information	52
MALWARE-BACKDOOR ReGeorg socks proxy initial connection attempt	28
MALWARE-BACKDOOR HidePak backdoor attempt	27
MALWARE-OTHER SimpleTDS - request to go.php	25
POLICY-OTHER Pulse Connect Secure vulnerable URI access attempt	25
MALWARE-BACKDOOR ReGeorg socks proxy connection attempt	21

8

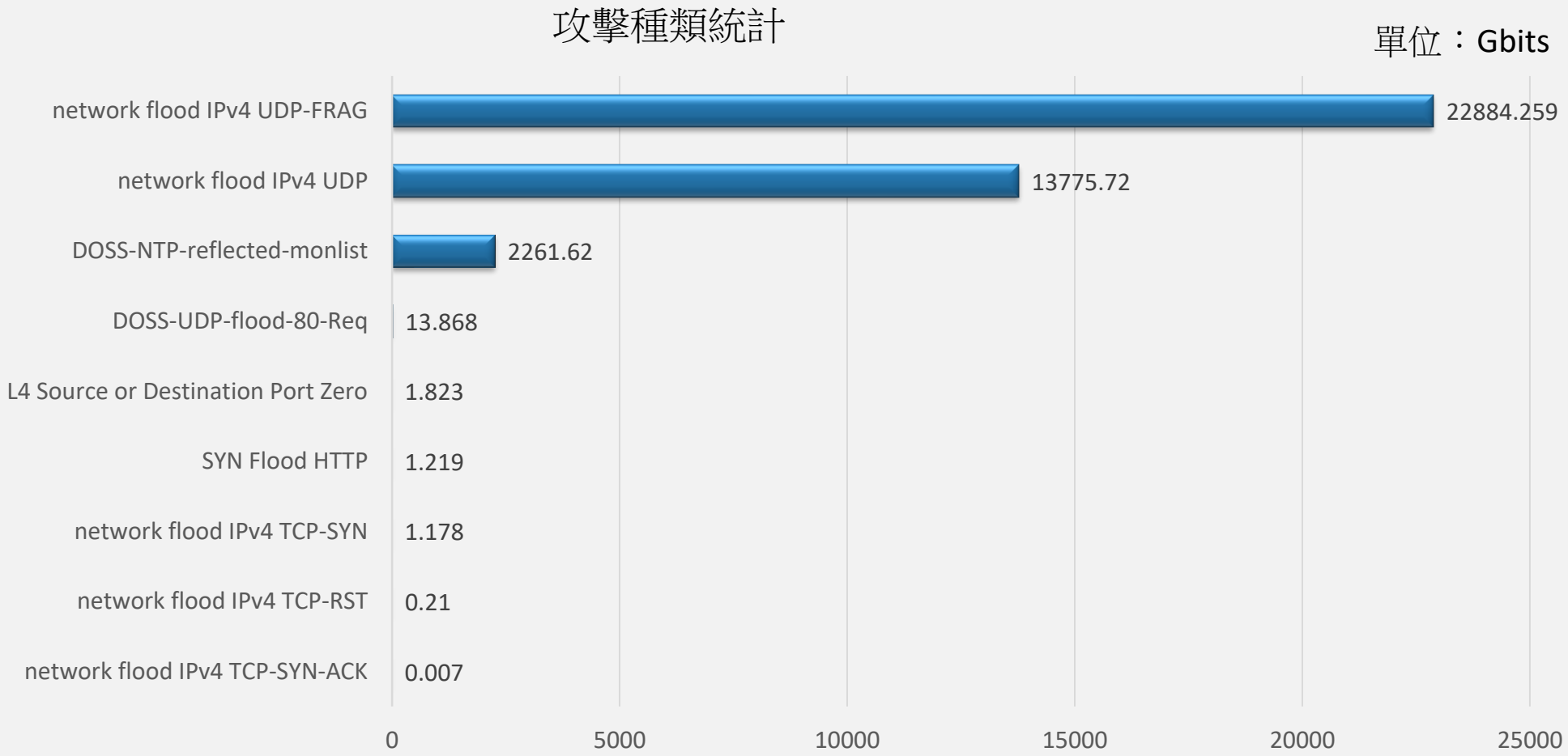
DDoS 攻擊

7x24 持續偵測與清洗服務(第二季)

單位	阻擋流量	備註
台北市教育網路中心	37,687 Gbits	



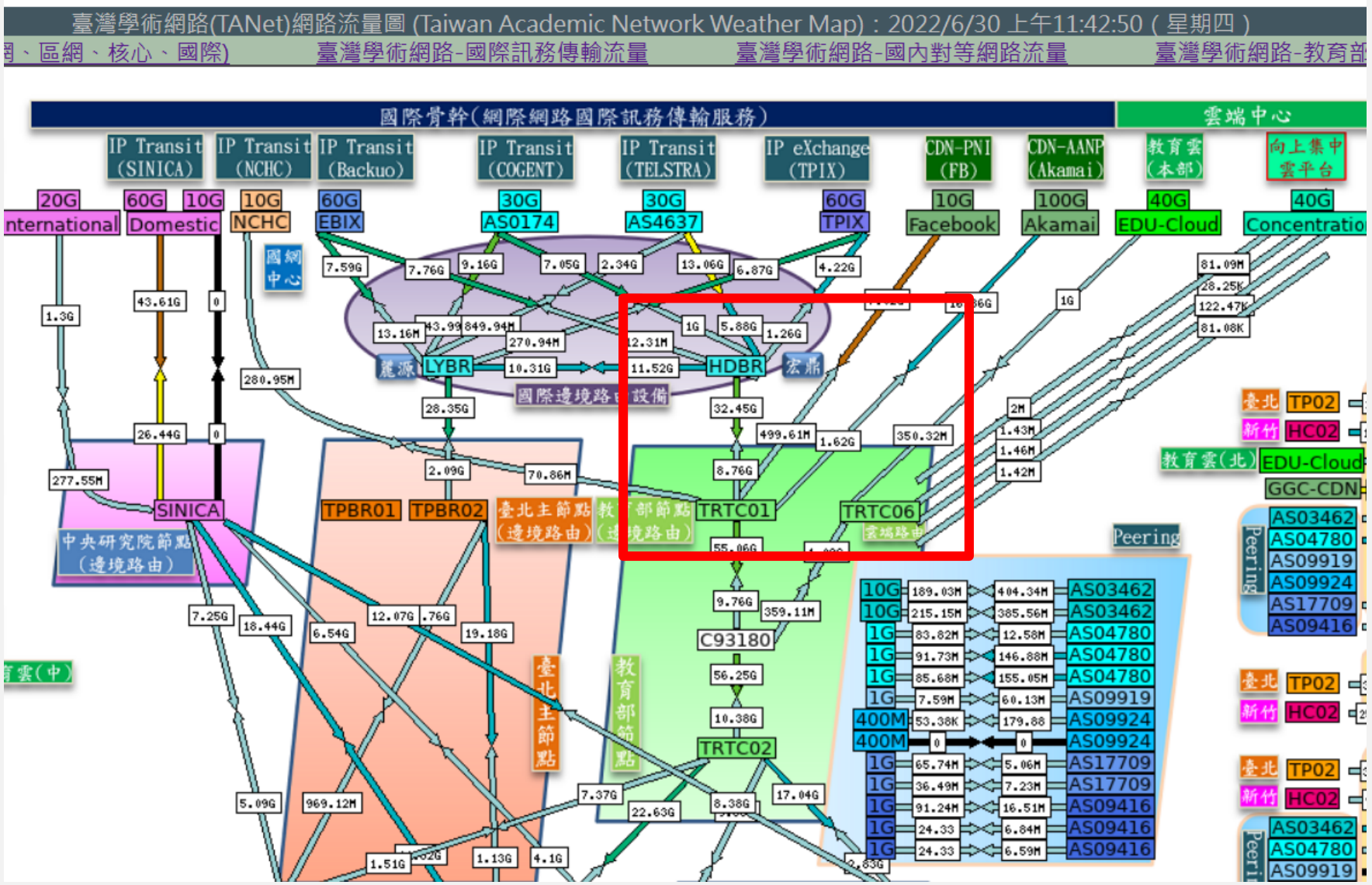
2022年第二季 DDoS攻擊總流量與攻擊類型



	network flood IPv4 TCP-SYN-ACK	network flood IPv4 TCP-RST	network flood IPv4 TCP-SYN	SYN Flood HTTP	L4 Source or Destination Port Zero	DOSS-UDP-flood-80-Req	DOSS-NTP-reflected-monlist	network flood IPv4 UDP	network flood IPv4 UDP-FRAG
數列1	0.007	0.21	1.178	1.219	1.823	13.868	2261.62	13775.72	22884.259

攻擊總流量約 38 Tbits

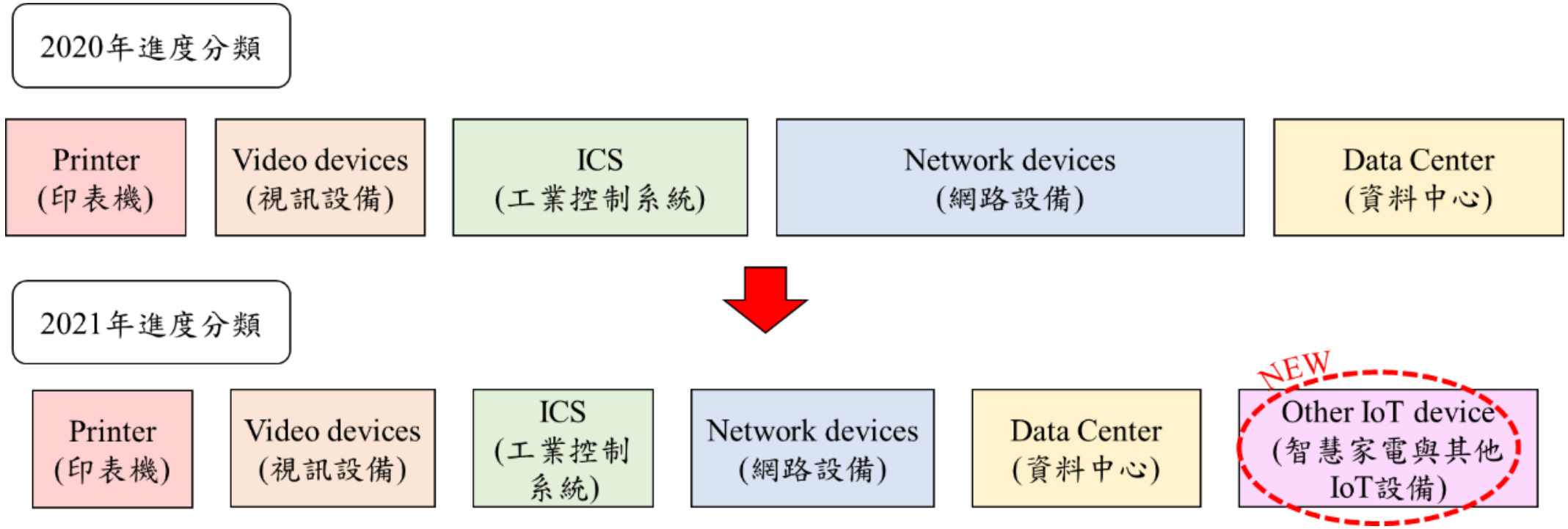
DDoS防護範圍


臺灣學術網路(TANet)網路流量圖 (Taiwan Academic Network Weather Map)：2022/6/30 上午11:42:50 (星期四)
臺灣學術網路-國際訊務傳輸流量
臺灣學術網路-國內對等網路流量
國際骨幹(網際網路國際訊務傳輸服務)
雲端中心
IP Transit (SINICA)
IP Transit (NCHC)
IP Transit (Backuo)
IP Transit (COGENT)
IP Transit (TELSTRA)
IP eXchange (TPIX)
CDN-PNI (FB)
CDN-AANP (Akamai)
教育雲 (本部)
向上集中雲平台
20G nternational
60G Domestic
10G
10G NCHC
60G EBIX
30G AS0174
30G AS4637
60G TPIX
10G Facebook
100G Akamai
40G EDU-Cloud
40G Concentratio
國網中心
LYBR
HDBR
SINICA
中央研究院節點（邊境路由）
TPBR01
TPBR02
臺北主節點（邊境路由）
TRTC01
TRTC06
C93180
TRTC02
臺北主節點
教育部節點
Peering
臺北 TP02
新竹 HC02
教育雲(北) EDU-Cloud
GGC-CDN
AS03462
AS04780
AS09919
AS09924
AS17709
AS09416

12

IoT分類統計

IoT pattern


2020年進度分類
Printer (印表機)
Video devices (視訊設備)
ICS (工業控制系統)
Network devices (網路設備)
Data Center (資料中心)
2021年進度分類
Printer (印表機)
Video devices (視訊設備)
ICS (工業控制系統)
Network devices (網路設備)
Data Center (資料中心)
NEW
Other IoT device (智慧家電與其他IoT設備)

資料分類

A	B	C	D	E	F	G	H
IP	Port	Transpo	Shodan_Timestamp	IoT_service_type	Annotation	Rule	Vender
120. .33	443	tcp	2021/9/18	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
120. .34	443	tcp	2021/9/16	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽	Synology
120. .143	443	tcp	2021/9/16	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽	Synology
140. 85	443	tcp	2021/9/19	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽	Synology
140. .253	443	tcp	2021/9/19	網路設備	交換器	網路設備規則三：product欄位出現網路設備相關關鍵字	CISCO
140. 249	80	tcp	2021/9/19	網路設備	交換器	網路設備規則三：product欄位出現網路設備相關關鍵字	CISCO
140. 249	80	tcp	2021/9/19	網路設備	交換器	網路設備規則三：product欄位出現網路設備相關關鍵字	CISCO
140. .187	143	tcp	2021/9/19	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
140. 113	1900	udp	2021/9/19	資料中心	伺服器/工作站	資料中心規則六：在data、product、cpe、ssl.cert欄位找到hp server遠端port的特徵	HP
140. 251	80	tcp	2021/9/19	網路設備	交換器	網路設備規則三：product欄位出現網路設備相關關鍵字	CISCO
140. .1	161	udp	2021/9/19				HP
140. 201	443	tcp	2021/9/19	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
140. .245	5001	tcp	2021/9/19	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
140. .43	443	tcp	2021/9/19	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
140. 162	5001	tcp	2021/9/19	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
140. 248	80	tcp	2021/9/19	網路設備	交換器	網路設備規則三：product欄位出現網路設備相關關鍵字	CISCO
140. 172	443	tcp	2021/9/19	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
140. 249	80	tcp	2021/9/19	網路設備	交換器	網路設備規則三：product欄位出現網路設備相關關鍵字	CISCO
140. 26	4800	udp	2021/9/19	網路設備		網路設備規則五：出現網路設備廠商的名稱	MOXA
140. 133	443	tcp	2021/9/18	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology
140. .121	21	tcp	2021/9/18	印表機		印表機規則一：devicetype欄位出現印表機的關鍵字	KONICA
140. 40	520	udp	2021/9/18	網路設備	無線路由器	網路設備規則二：_shodan.module欄位出現網路設備相關關鍵字	Apple
140. 251	80	tcp	2021/9/18	網路設備	交換器	網路設備規則三：product欄位出現網路設備相關關鍵字	CISCO
140. 4	5001	tcp	2021/9/18	資料中心	網路儲存系統	資料中心規則二：ssl.cert欄位出現網路儲存系統(NAS)廠商自簽憑證的資訊	Synology

新欄位

重點資安事件研究與分析案例

01 CVE-2022-1388 漏洞分析

F5在五月初公開此漏洞資訊(繞過身分驗證)，同時也提供修補更新檔案。而後資安業者成功開發PoC程式後，呼籲管理者應立即修補此重大漏洞。

02 Spring4Shell 漏洞說明

國外資安人員在三月底公開這個漏洞資訊(RCE漏洞)，不久就出現相關PoC程式，並且在四月初就偵測到利用此漏洞的攻擊事件。

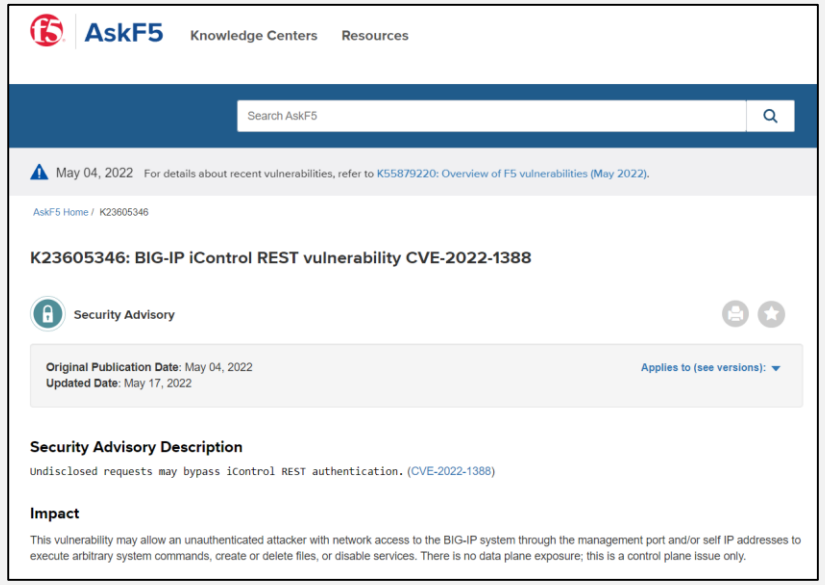
03 MALWARE-CNC 種類介紹: Redline、Vidar

北區ASOC發現有兩個規則，在第二季中有明顯的事件量。基於好奇，而進行初步的研究分析。

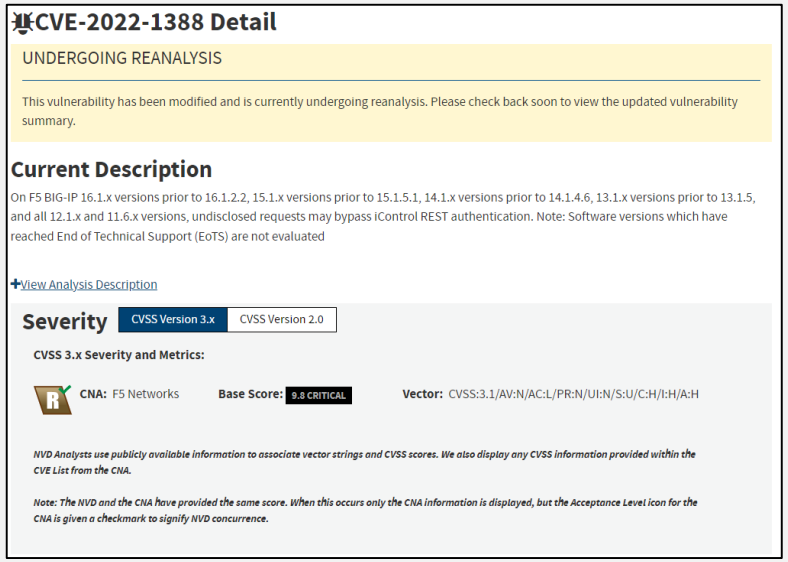
CVE-2022-1388 漏洞分析
F5 BIG-IP iControl

漏洞描述

- CVE-2022-1388 是 F5 Networks 的 BIG-IP 解決方案管理界面中的一個嚴重漏洞 (CVSS 9.8)，該漏洞由 F5 官方在 2022 年 5 月 4 日對外發布
- 此漏洞可讓未經身份驗證的攻擊者，繞過 F5 的 iControl REST 身份驗證，進而存取 BIG-IP 系統
- iControl REST 是一個 Web-based 程式介面，可執行 BIG-IP 硬體設備組態配置與管理



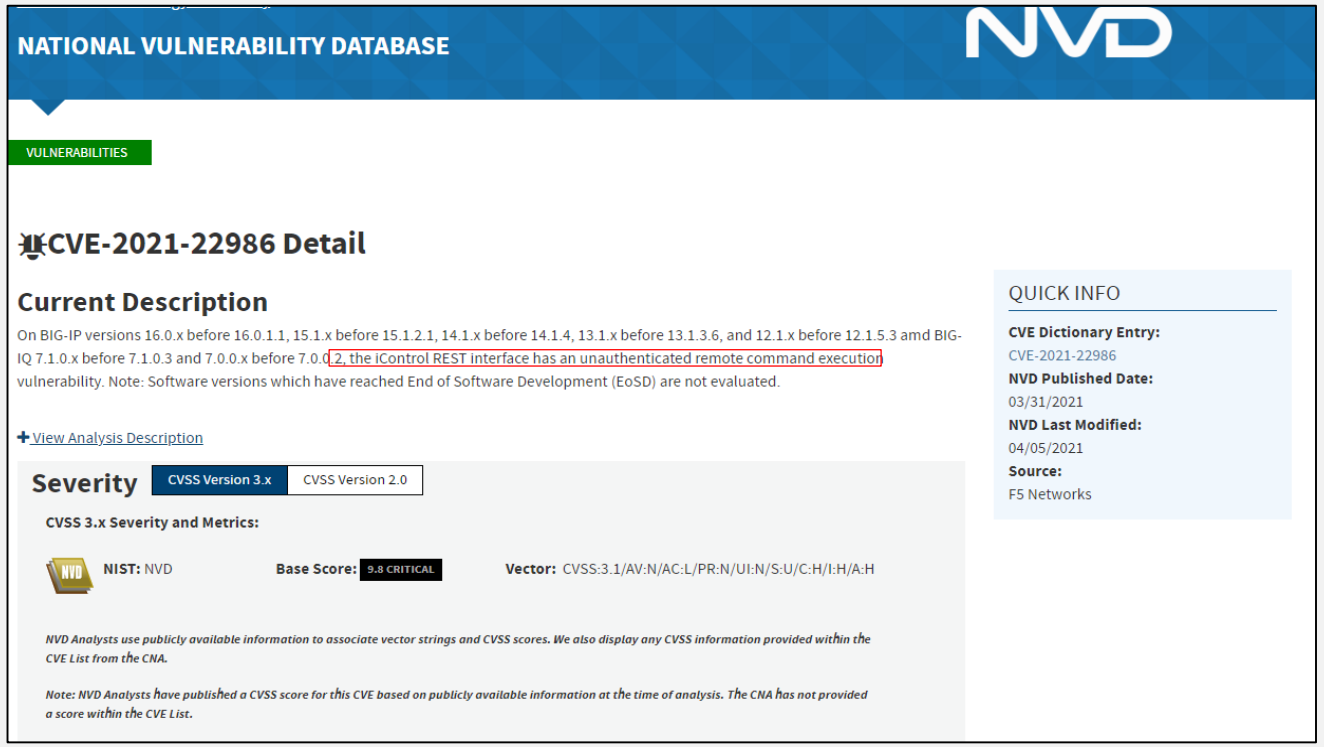
資料來源： https://support.f5.com/csp/article/K23605346



資料來源： https://nvd.nist.gov/vuln/detail/CVE-2022-1388

漏洞說明

- CVE-2022-1388 是存在於 F5 的 BIG-IP (All Modules) 所使用的 iControl REST 元件中
- 該元件的功能是為了讓使用者或自動化(腳本)程式能與F5設備執行輕量且快速的互動
- 漏洞發生的原因跟去年發生的 CVE-2021-22986 漏洞太過相似，推測是上次漏洞修補方式並不完善。



資料來源： https://nvd.nist.gov/vuln/detail/CVE-2021-22986#vulnCurrentDescriptionTitle

影響範圍

- 受影響之 BIG-IP (All modules) 版本如下：
  - 16.1.0 - 16.1.2
  - 15.1.0 - 15.1.5
  - 14.1.0 - 14.1.4
  - 13.1.0 - 13.1.4
  - 12.1.0 - 12.1.6 (End of Support)
  - 11.6.1 - 11.6.5 (End of Support)

Product	Branch	Versions known to be vulnerable[1]	Fixes introduced in[3]	Severity	CVSSv3 score[2]	Vulnerable component or feature
BIG-IP (all modules)	17.x	None	17.0.0	Critical	9.8	iControl REST
	16.x	16.1.0 - 16.1.2	16.1.2.2			
	15.x	15.1.0 - 15.1.5	15.1.5.1			
	14.x	14.1.0 - 14.1.4	14.1.4.6			
	13.x	13.1.0 - 13.1.4	13.1.5			
	12.x	12.1.0 - 12.1.6	Will not fix			
	11.x	11.6.1 - 11.6.5	Will not fix			
BIG-IQ Centralized Management	8.x	None	Not applicable	Not vulnerable	None	None
	7.x	None	Not applicable			
F5OS-A	1.x	None	Not applicable	Not vulnerable	None	None
F5OS-C	1.x	None	Not applicable	Not vulnerable	None	None
Traffix SDC	5.x	None	Not applicable	Not vulnerable	None	None

資料來源：https://support.f5.com/csp/article/K23605346

建議措施

- 目前 F5 官方已針對此漏洞釋出修復版本，請根據使用的版本做更新 ：
  - BIG-IP 16.x ：16.1.2.2
  - BIG-IP 15.x ：15.1.5.1
  - BIG-IP 14.x ：14.1.4.6
  - BIG-IP 13.x ：13.1.3.5
  - BIG-IP 12.x ：停止支援(EoS)，不會有修補版本
  - BIG-IP 11.x ：停止支援(EoS)，不會有修補版本
- 若目前所使用之版本因已停止支援而未釋出修補程式，建議升級至仍有支援且已推出修補程式之版本。

Recommended Actions

If you are running a version listed in the **Versions known to be vulnerable** column, you can eliminate this vulnerability by installing a version listed in the **Fixes introduced in** column. If the **Fixes introduced in** column does not list a version for your branch, then no update candidate currently exists for that branch and F5 recommends upgrading to a version with the fix (refer to the table).

If the **Fixes introduced in** column lists a version prior to the one you are running, in the same branch, then your version should have the fix.

資料來源：https://support.f5.com/csp/article/K23605346

緩解措施

- 若無法更新至最新版本，可參考 F5 官方提供之緩解措施(詳細細節請至官網查詢)：
  - 禁止透過設備之 self IP 位址存取 iControl REST 介面
  - 僅允許受信任之使用者與設備可透過 BIG-IP 設備管理頁面存取 iControl REST 介面
  - 調整 BIG-IP 設備之 httpd 設定檔

Mitigation

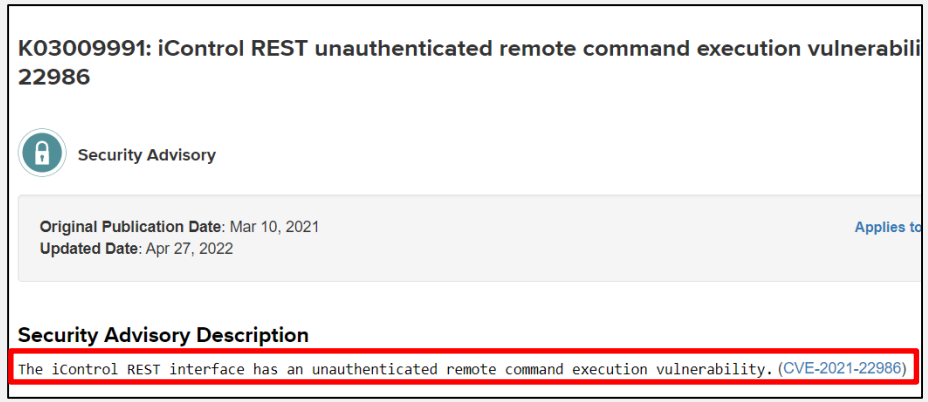
Until it is possible to install a fixed version, you can use the following sections as temporary mitigations. These mitigations restrict access to iControl REST to only trusted networks or devices, thereby limiting the attack surface.

- Block iControl REST access through the self IP address
- Block iControl REST access through the management interface
- Modify the BIG-IP httpd configuration

資料來源：https://support.f5.com/csp/article/K23605346

漏洞原理-1

- 此漏洞發生在 iControl REST 進行身分驗證時，攻擊者可透過特殊的 HTTP request header 就可繞過身分驗證
- 本次漏洞原理跟CVE-2021-22986漏洞一樣，故後續原理、分析章節會一併一起說明
- 兩者漏洞的差異：
  - CVE-2021-22986漏洞是未經授權(意思可等於繞過身分驗證)的遠端任意執行程式碼(RCE)
  - CVE-2022-1388漏洞是只有繞過身分驗證



資料來源： https://support.f5.com/csp/article/K03009991

資料來源： https://support.f5.com/csp/article/K23605346

漏洞分析-2

- 需要滿足四個條件才會成功的繞過身分驗證
- 條件說明如下：
  1. Connection header必須包含X-F5-Auth-Token
  2. X-F5-Auth-Token 必須存在
  3. 在host header中，一定要是 localhost(也可以寫成127.0.0.1)，或Connection header務必包含X-Forwarded-Host
  4. Auth header務必把帳號設定成admin，而密碼為任意(代表密碼可以為空)

➢ 其他深入分析內容請參考補充資料章節

Summary

Necessary conditions of a request for exploiting this vulnerability:

1. Connection header must include X-F5-Auth-Token
2. X-F5-Auth-Token header must be present
3. Host header must be localhost / 127.0.0.1 or the Connection header must include X-Forwarded-Host
4. Auth header must be set with the admin username and any password

資料來源：https://github.com/horizon3ai/CVE-2022-1388

HTTP/1.1 header 字串一覽

HTTP/1.1 規範了 47 種字串。

通用 header

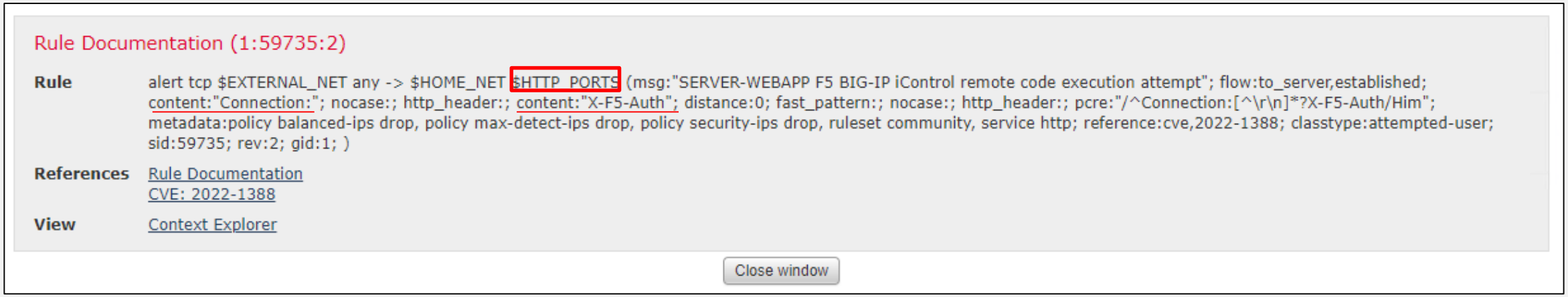
- Cache-Control：控制緩存行為
- Connetion：逐跳 header、連接的管理
- Date：創建日期
- Pragma：訊息指令
- Trailer：訊息尾端的 header 一覽
- Transfer-Encoding：指定訊息主體的傳輸編碼方式
- Upgrade：升級為其他協議
- Via：代理伺服器相關訊息
- Warning：錯誤通知

請求 header

- Accept：用戶代理可處理的媒體類型
- Accept-Charset：優先的字串集
- Accept-Encoding：優先的內容編碼
- Accept-Language：優先的自然語言
- Authorization：網頁認證訊息
- Expect：期待伺服器的特定行為
- Form：用戶的電子信箱地址
- Host：請求資料的伺服器位置
- If-Match：比較實體標記（ETag）
- If-Modified-Since：比較資料更新時間

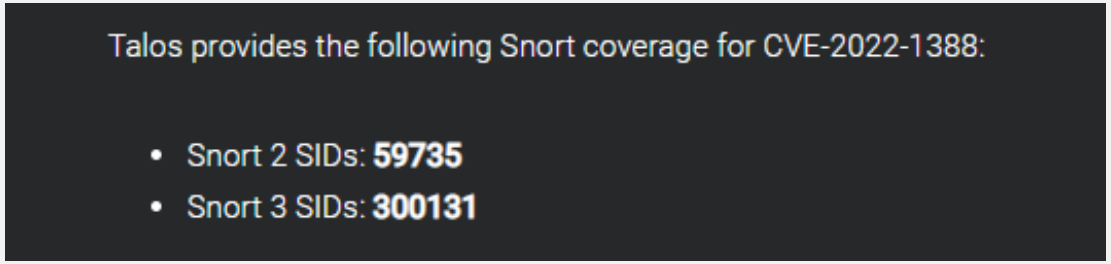
資料來源：https://ithelp.ithome.com.tw/articles/10204743

IPS偵測規則說明



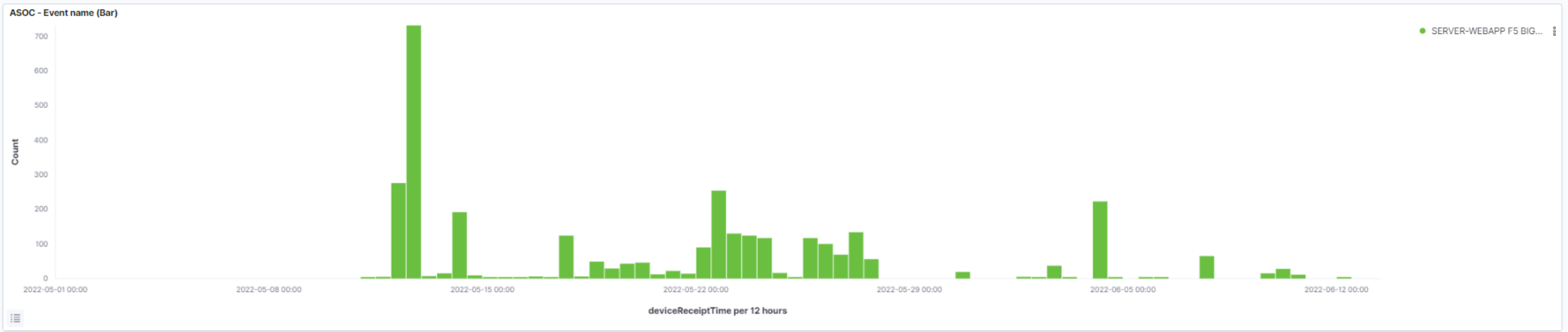
此規則偵測條件為：

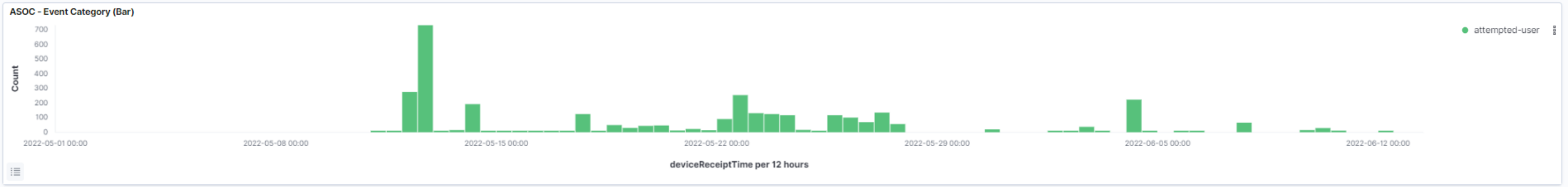
1. 外對內的tcp連線；來源埠不限；目標埠為網站常用的連線埠(80、81、8080....等)
2. 封包內容包含下列關鍵字
   ① Connection:
   ② X-F5-Auth



資料來源：https://blog.talosintelligence.com/2022/05/threat-advisory-critical-f5-big-ip-vuln.html

學術網路偵測狀態-2

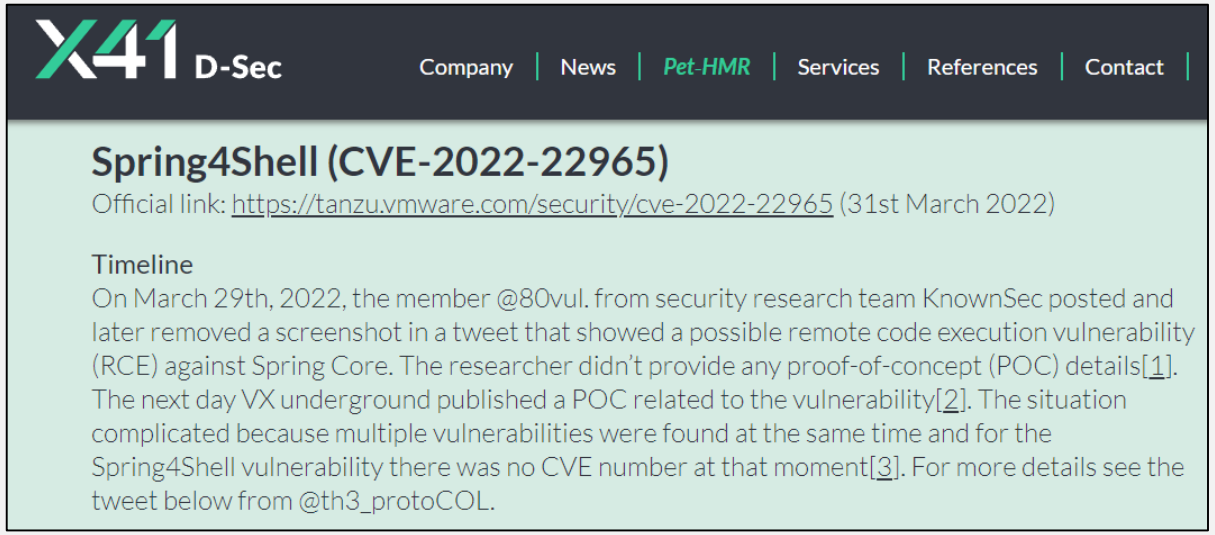

ASOC - Event name (Bar)
SERVER-WEBAPP F5 BIG...
Count
700
600
500
400
300
200
100
0
2022-05-01 00:00
2022-05-08 00:00
2022-05-15 00:00
2022-05-22 00:00
2022-05-29 00:00
2022-06-05 00:00
2022-06-12 00:00
deviceReceiptTime per 12 hours


ASOC - Event Category (Bar)
attempted-user
Count
700
600
500
400
300
200
100
0
2022-05-01 00:00
2022-05-08 00:00
2022-05-15 00:00
2022-05-22 00:00
2022-05-29 00:00
2022-06-05 00:00
2022-06-12 00:00
deviceReceiptTime per 12 hours

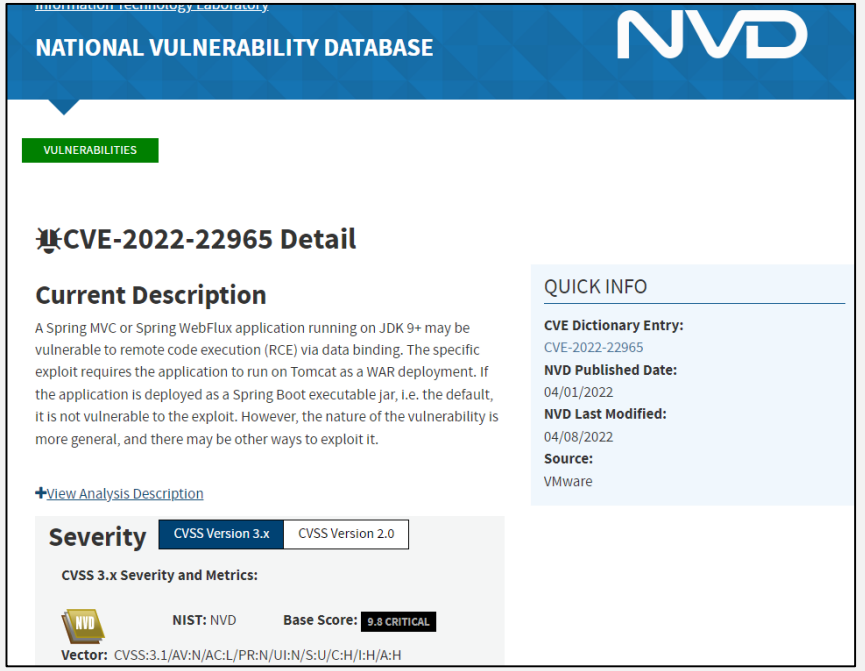
Spring4Shell漏洞說明

漏洞介紹

- Spring4Shell是一個遠端執行程式碼(RCE)漏洞。漏洞編號為CVE-2022-22965，該漏洞風險等級為最高(9.8分)
- 此漏洞由國外資安研究人員在三月底，於推特上發布漏洞資訊(但已被刪除)
- 漏洞資訊公開後，相關PoC程式就出現在Github上
- 四月初就陸續傳出相關的漏洞攻擊資訊



資料來源：https://x41-dsec.de/pethmr/springshell/



資料來源：https://nvd.nist.gov/vuln/detail/CVE-2022-22965

影響範圍

- 根據Spring官方漏洞說明：
  - 執行JDK版本為9(含)以上
  - 使用Apache Tomcat做為Servlet容器
  - 程式專案封裝成Java web archive(WAR)，並部署於獨立之Tomcat實體
  - 程式專案與Spring-webmvc或spring-webflux有相依性
  - Spring Framework 5.3.0至5.3.17、5.2.0至5.2.19，以及之前舊的版本

Am I Impacted?

These are the requirements for the specific scenario from the report:

- Running on JDK 9 or higher
- Apache Tomcat as the Servlet container.
- Packaged as a traditional WAR and deployed in a standalone Tomcat instance. Typical Spring Boot deployments using an embedded Servlet container or reactive web server are not impacted.
- `spring-webmvc` or `spring-webflux` dependency.
- Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older versions.

資料來源：https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

Spring Framework Spring4Shell (CVE-2022-22965)

CRITICAL Nessus Plugin ID 159542

信息 依賴項 家屬

Synopsis

遠端主機上的 Web 應用程式架構程式庫受到遠端程式碼執行弱點的影響。

描述

遠端主機上的 Spring Framework 程式庫版本為 5.2.20 之前的版本或 5.3.18 之前的 5.3.x。因此，該主機受到遠端程式碼執行弱點影響：

- 透過資料系結，JDK 9+ 上執行的 Spring MVC 或 Spring WebFlux 應用程式可能很容易受到遠端程式碼執行 (RCE) 弱點影響。特定的惡意利用需要應用程式在 Tomcat 上作為 WAR 部署執行。如果應用程式部署為 Spring Boot 可執行檔 jar (即預設值)，則不會受此弱點影響。不過，這個弱點更具普遍性，可能還有其他利用方式。
- 如要利用這個弱點，需滿足以下先決條件：
- JDK 9 或更高版本

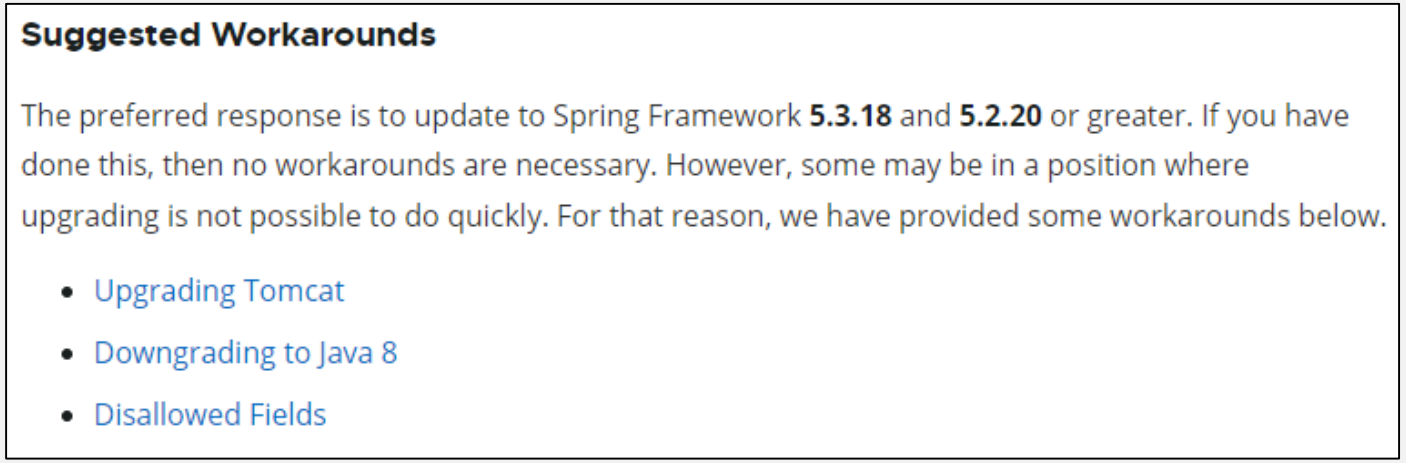
Apache Tomcat 是一個 Servlet 容器

- 封裝為 WAR
- spring-webmvc 或 spring-webflux 依附元件

資料來源： https://zh-tw.tenable.com/plugins/nessus/159542

建議措施和暫時緩解方法

- Spring官方建議應升級到最新版本(資料截至4/15)
  - Spring Framework 5.3.19、5.2.21或之後更新的版本
  - Spring Boot 2.6.7、2.5.13或之後更新的版本
- 官方提供暫時緩解方法有：
  - 升級Apache Tomcat版本(10.0.20, 9.0.62, 8.5.78或之後更新的版本)
  - 降級Java版本到Java 8
  - 不允許特定Java類別(class)中的屬性(Fields)的使用



Suggested Workarounds

The preferred response is to update to Spring Framework **5.3.18** and **5.2.20** or greater. If you have done this, then no workarounds are necessary. However, some may be in a position where upgrading is not possible to do quickly. For that reason, we have provided some workarounds below.

- Upgrading Tomcat
- Downgrading to Java 8
- Disallowed Fields

資料來源：https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

其他緩解措施

緩解措施

若無法採用官方建議的解決方式的話，可以採用以下的做法：

1.確認 JDK 版本代號

如要確認 JDK 版本代號，請於貴組織系統的伺服器上執行 java -version 指令以確認運行中的版本代號。

```
user@ubuntu:~$ java -version
openjdk version "11.0.14.1" 2022-02-08
OpenJDK Runtime Environment (build 11.0.14.1+1-Ubuntu-0ubuntu1.20.04)
OpenJDK 64-Bit Server VM (build 11.0.14.1+1-Ubuntu-0ubuntu1.20.04, mixed mode, sharing)
user@ubuntu:~$ find ./apache-tomcat-8.5.77/ -name "spring-beans*"
./apache-tomcat-8.5.77/webapps/vulnerable-1.0.0.0/WEB-INF/lib/spring-beans-5.3.15.jar
user@ubuntu:~$
```

- 如果版本代號低於或等於 8，將不會受此漏洞影響。
- 如果版本代號高於或等於 9，則漏洞存在。請參照以下臨時方案抵禦潛在的攻擊。

2. 臨時方案：WAF 阻擋

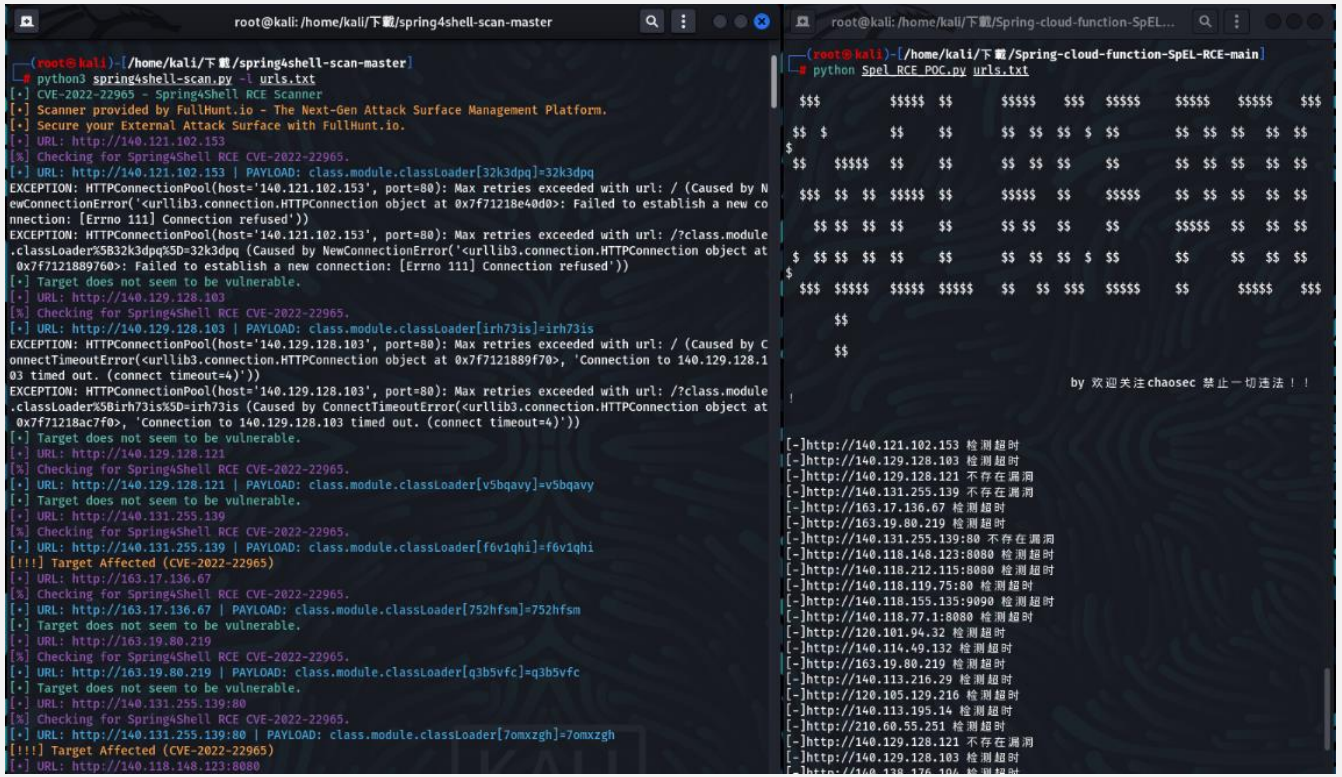
在網頁應用防火牆（WAF）中置入規則過濾以下字串

- `class.*`, `Class.*`, `*.class.*`, `*.Class.*`

資料來源： https://teamt5.org/tw/posts/spring-rce-zeroday-vulnerability/

POC程式測試結果紀錄

- 北區ASOC查詢過去近兩年Shodan資料，找出曾經有出現Spring特徵的資料共48筆
- 經過三個PoC程式測試後，確認名單上的IP都沒有CVE-2022-22965的漏洞



區網中心	Spring4Shell
TP1RC	6
ILRC	1
NTHU	1
HCRC	5
TP2RC	2
TYRC	5
YCRC	1
TTRC	3
TNRC	2
KPPRC	8
HDRC	1
TCRC	5
SINICA	6
other	2
Total	48

備註：測試時間為06/07

自我檢測方式

如何檢測我的服務是否受到影響？

1.可以參考以下檢測方式，快速確認是否受到此弱點影響：
在 Spring 的網站程式，對 Spring 對應的路徑，送入特定的 Query，能測試網站是否存在弱點。

檢測 Query 如下：

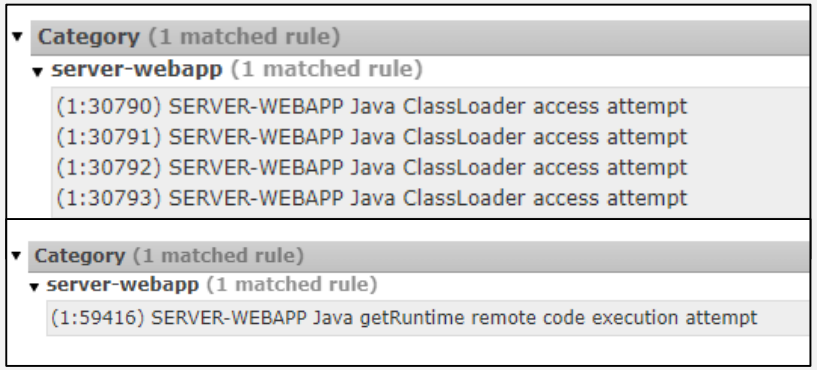
```
curl -v host:port/path?class.module.classLoader.URLs%5B0%5D=0
```

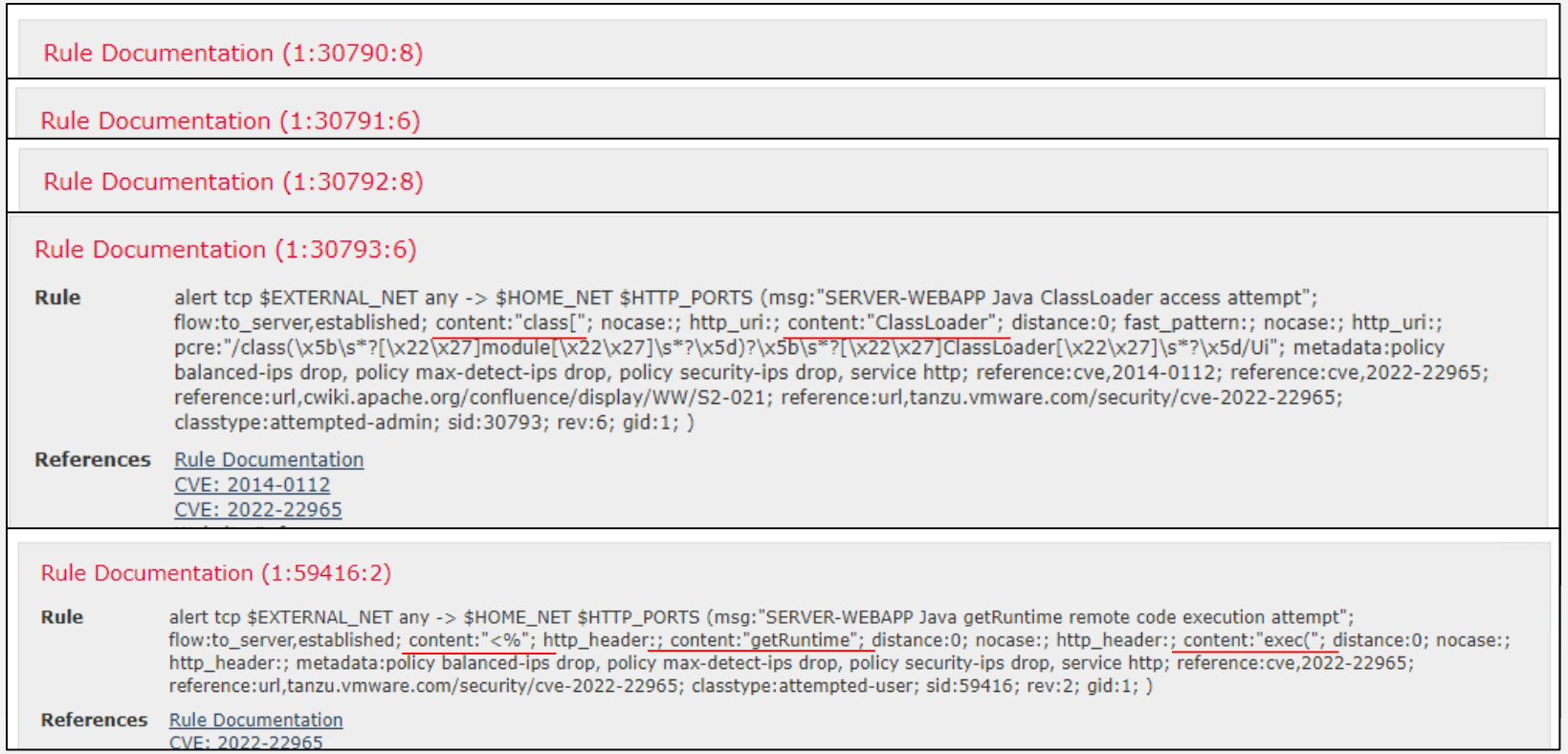
下圖為執行 Query 後，如果回應 HTTP Status 400，很可能是有弱點的。

資料來源： https://teamt5.org/tw/posts/spring-rce-zeroday-vulnerability/

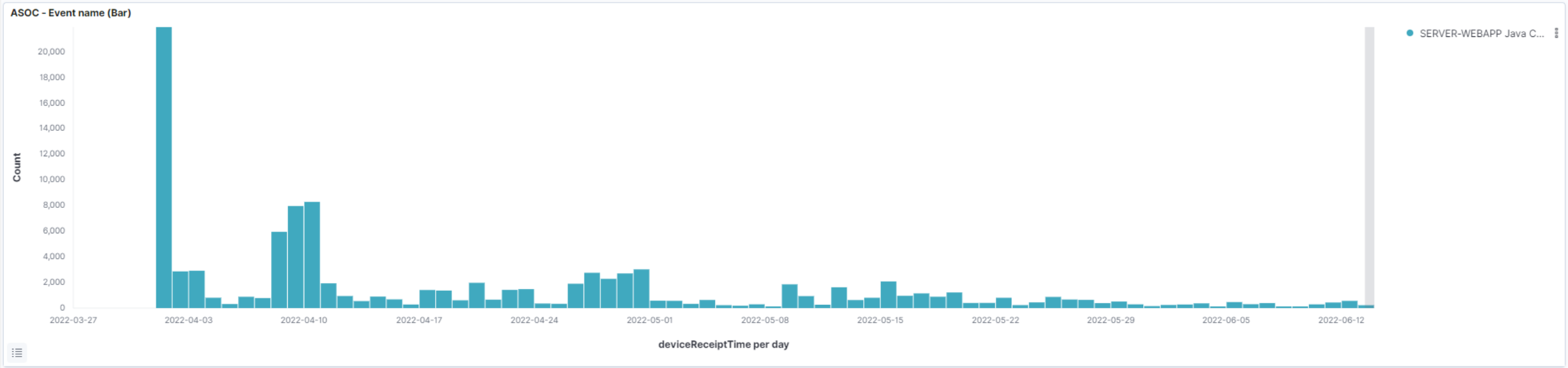
IPS相關規則列表

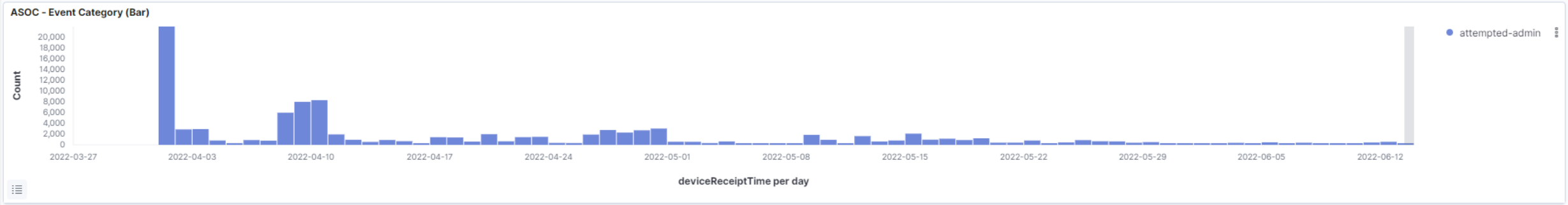
- 目前IPS上的偵測Spring4Shell規則總共有5條
- 規則判斷內容和PoC程式內出現的特徵片段相符合





學術網路偵測情況-2


ASOC - Event name (Bar)
SERVER-WEBAPP Java C...
Count
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2022-03-27
2022-04-03
2022-04-10
2022-04-17
2022-04-24
2022-05-01
2022-05-08
2022-05-15
2022-05-22
2022-05-29
2022-06-05
2022-06-12
deviceReceiptTime per day


ASOC - Event Category (Bar)
attempted-admin
Count
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2022-03-27
2022-04-03
2022-04-10
2022-04-17
2022-04-24
2022-05-01
2022-05-08
2022-05-15
2022-05-22
2022-05-29
2022-06-05
2022-06-12
deviceReceiptTime per day

MALWARE-CNC 種類介紹：Redline、Vidar

Snort 規則說明

Talos Rules 2022-03-04

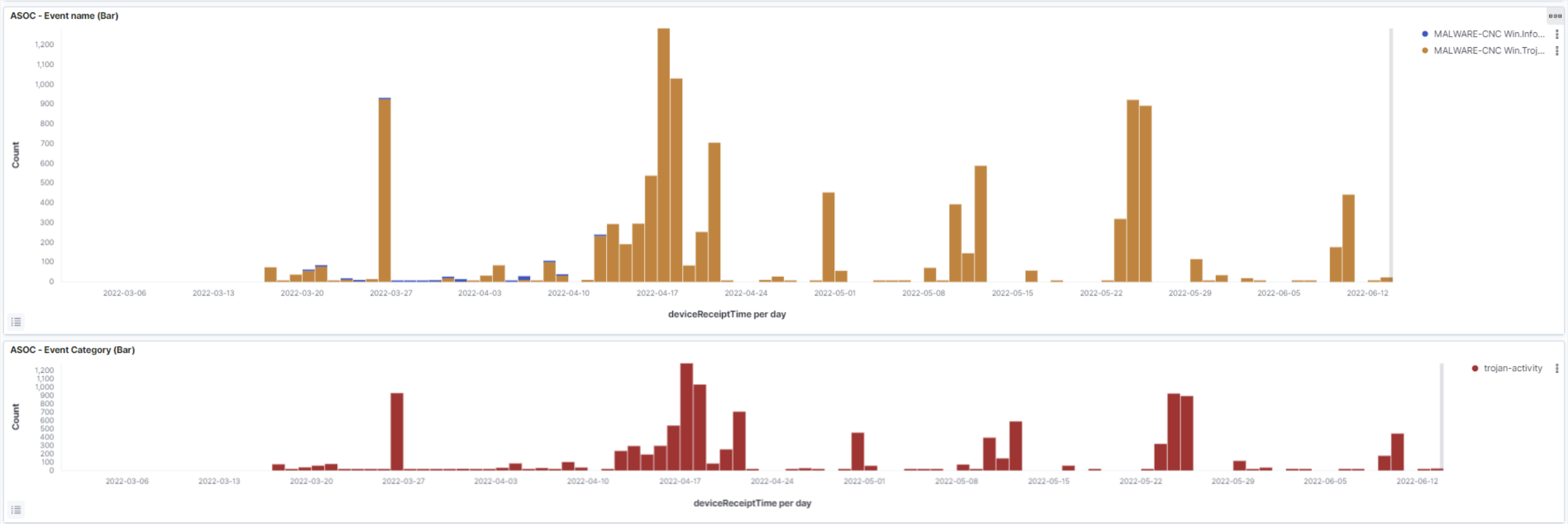
This release adds and modifies rules in several categories.

Talos is releasing Snort coverage to protect against ongoing cyber operations against Ukraine. These new Snort rules provide protection against the following malware families: Redline (SID 59160), IsaacWiper (SIDs 59163-59164), SunSeed Lua (SIDs 59165-59173), HermeticRansom (SIDs 59154-59159), Vidar (SIDs 59200-59203), and WhiteBlackCrypt (SIDs 59161-59162).

Talos has added and modified multiple rules in the deleted, malware-cnc, malware-other and os-windows rule sets to provide coverage for emerging threats from these technologies.

For information about Snort Subscriber Rulesets available for purchase, please visit the Snort product page.

學術網路偵測情況-2

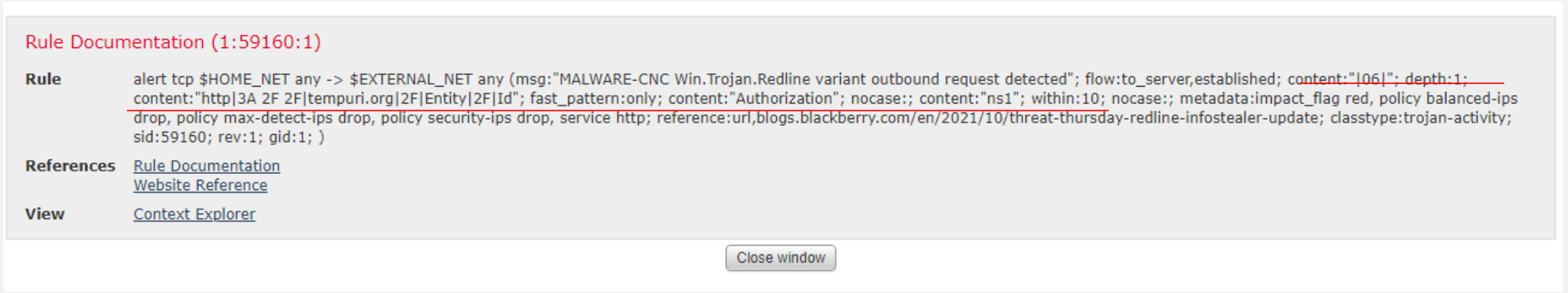

ASOC - Event name (Bar)
MALWARE-CNC Win.Info...
MALWARE-CNC Win.Troj...
Count
1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
2022-03-06
2022-03-13
2022-03-20
2022-03-27
2022-04-03
2022-04-10
2022-04-17
2022-04-24
2022-05-01
2022-05-08
2022-05-15
2022-05-22
2022-05-29
2022-06-05
2022-06-12
deviceReceiptTime per day
ASOC - Event Category (Bar)
trojan-activity
Count
deviceReceiptTime per day

RedLine Infostealer

- IPS共有五條規則(SID:58007、58009、59149、59150、59160)，而目前各大區網僅觸發59160這條(相關規則於2022/03/04更新至IPS上)
- Redline暫時都以Windows用戶為主要受害者
- 主要以竊取電腦中敏感資訊為主，例如 login credentials, browser cookies, auto-fill information, and credit card details
- 就韓國資安公司Asec調查，主要以釣魚方式散播，但有一部分是在Youtube廣告上，假借放在外掛影片中，引誘受害者下載

RedLine Infostealer

- Sid:59160 觸發規則如下：

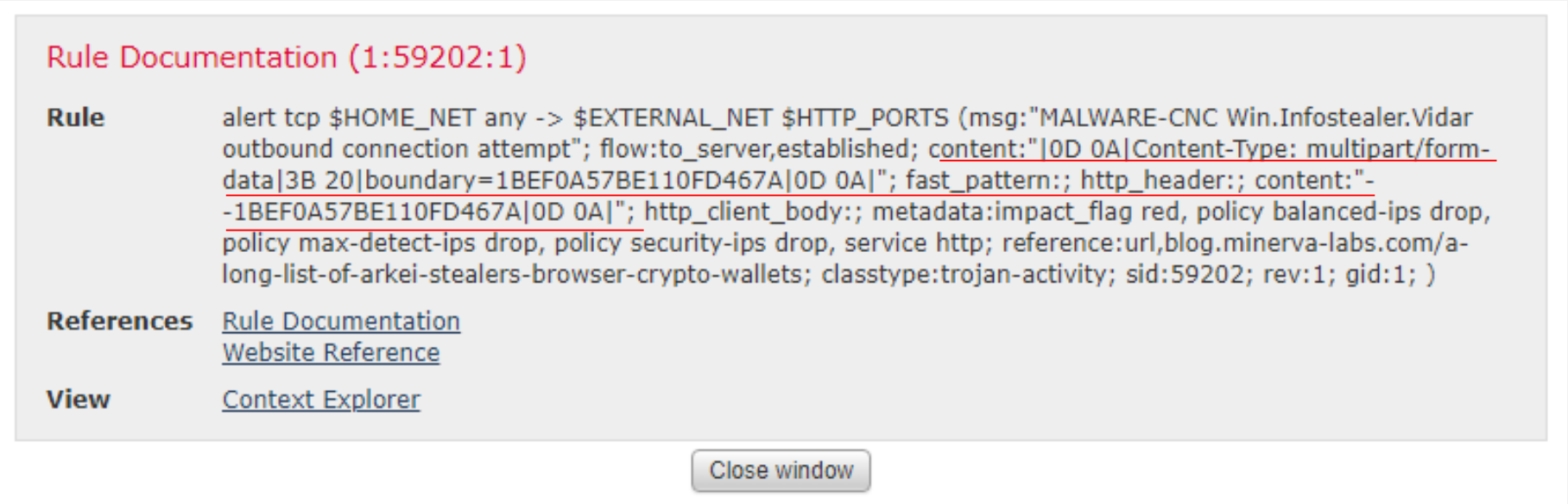


- 觸發範例封包：

```
...S.http://tempuri.org/Entity/Id1.net.tcp://185.200.191.18:80/.Id1.http://tempuri.org/V...s...a.V.D
.....@
Authorization..ns1. 4886fc967f40fd409a88dd6ae5830a80D.....e...D.1....."D,D*...D.......V.B.
....
```

A Long List Of Arkei Stealer's Crypto Browser Wallets

- IPS 針對該事件有佈署兩條規則(sid:59202、59203，於3/4更新)
- 以59202觸發最多，但59203仍有少數
- 主要以竊取電腦中敏感資訊，例如虛擬貨幣錢包或瀏覽器中的敏感資訊，外傳到CNC伺服器
- 59202偵測規則：



A Long List Of Arkei Stealer's Crypto Browser Wallets

可被竊瀏覽器										
Google Chrome	Chromium	Orbitum	Comodo Dragon	CocCoc	Uran	CryptoTab	Brave	SlimBrowser	PaleMoon	KMeleon
Microsoft Edge	Kometa	Nichrome	Maxthon 5	QIP Surf	CentBrowser	Opera	OperaGX	Waterfox	Cyberfox	Thunderbird
Amigo	Torch	Sputnik	Vivaldi	Elements	Tor	OperaNeon	Firefox	BlackHawk	IceCat	

可被竊錢包						
TronLink	Coinbase Wallet	Wombat	Clover Wallet	Polymesh Wallet	Cyano Wallet	Steem Keychain
MetaMask	Guarda	MEW CX	Liquality Wallet	ICONex	Byone	Nash Extension
Binance Chain Wallet	EQUA Wallet	GuildWallet	Terra Station	Nabox Wallet	OneKey	Hycon Lite Client
Yoroi	Jaxx Liberty	Saturn Wallet	Keplr	KHC	LeafWallet	ZilPay
Nifty Wallet	BitApp Wallet	Ronin Wallet	Sollet	Temple	DAppPlay	Coin98 Wallet
Math Wallet	iWallet	NeoLine	Auro Wallet	TezBox	BitClip	

受害電腦會對外傳送敏感資訊

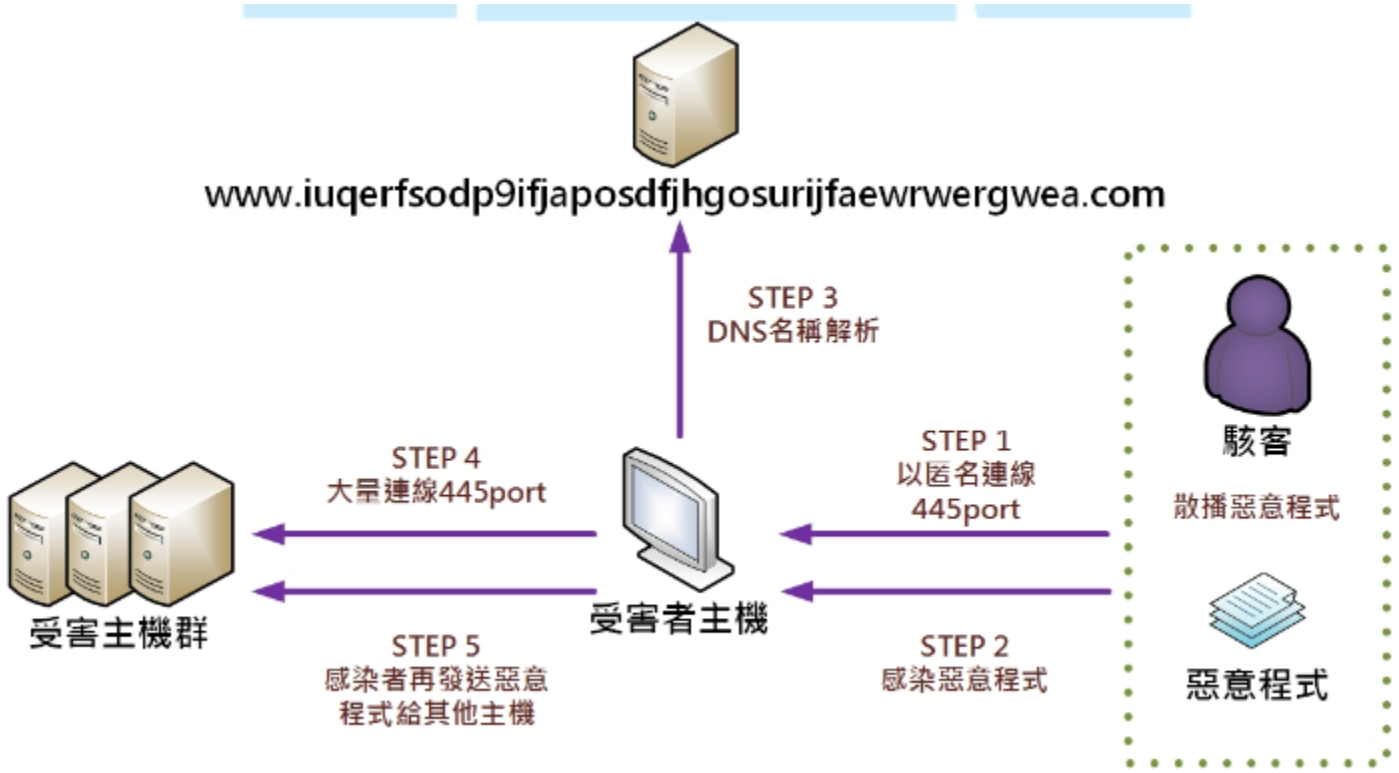
```
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

c51bc879-89e0-44cf-9e4a-9360-806e6f6e6963
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 10 Home
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

x64
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"

1191
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="user"

User
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="cccount"

0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="fcount"

0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="ver"

51.5
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile_id"

679
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="ccount"

0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="logs"; filename="c51bc879-89e0-44cf-9e4a-e1b9b1bf68601449826878.zip"
Content-Type: zip
```

43

開單宣導

Malware and DNS

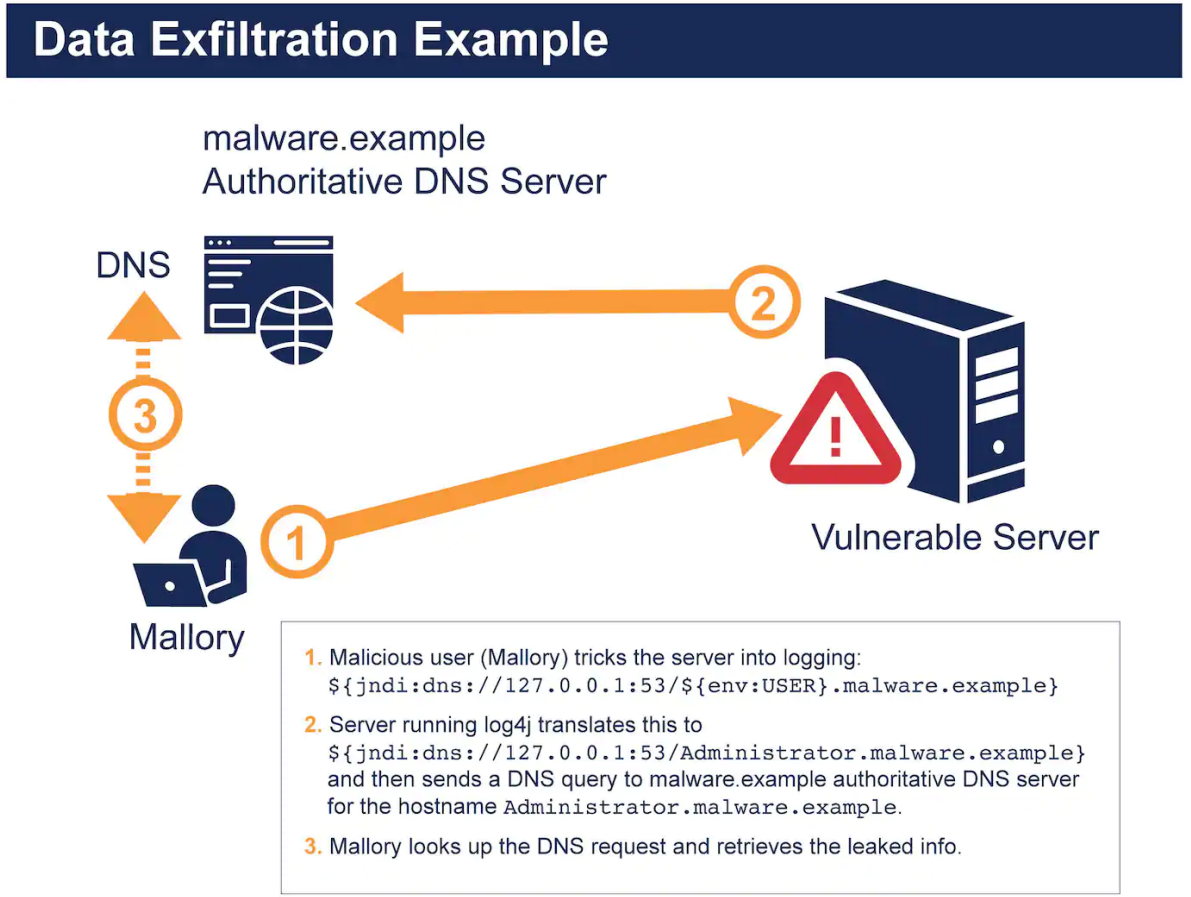
- Wannacry 勒索病毒 透過詢問 DNS 亂數 domain，用以確認是否在在真實環境而非沙箱環境。



圖片來源出處：
https://portal.cert.tanet.edu.tw/docs/pdf/2017062004063434305283221149085.pdf

Malware and DNS (conti.)

- Log4j 漏洞，駭客利用 DNS domain 的查詢，使得受害 server 向惡意 DNS server 回報受害主機之相關漏洞訊息。



圖片來源出處：
https://www.akamai.com/blog/security/a-log4j-retrospective-part-2-data-exfiltration-and-remote-code-execution-exploits

EWA 與 DNS

- 惡意 DNS domain 查詢，依目前學術網路政策都是開 EWA 情資。
- 依目前的偵測方式，骨幹僅能看到 DNS server 詢問之紀錄，並開單給 DNS server。
- 但學校老師應繼續追蹤校內環境內是哪台電腦來詢問該惡意 domain，進而查找真正問題，而徑直接誤判處理。

事件單編號	確認情形	原因	事件名稱
NTUSOC-EWA-202105-06	誤報	合法DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-05	誤報		MALWARE-CNC Win.Trojan.Zeus v3 DGA DNS query detected)
NTUSOC-EWA-202105-05	誤報	合法DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-04	誤報	合法DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-03	誤報	查校內NAT對映ip 電腦群，目	MALWARE-CNC Possible host infection - excessive DNS queries for .cn)
NTUSOC-EWA-202105-03	誤報	合法DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-03	誤報		MALWARE-CNC Torpig bot sinkhole server DNS lookup)
NTUSOC-EWA-202105-03	誤報		INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry)
NTUSOC-EWA-202105-03	誤報	該IP為合法的DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-02	誤報		MALWARE-CNC Torpig bot sinkhole server DNS lookup)
NTUSOC-EWA-202105-03	誤報	合法的DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-02	誤報		INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry)
NTUSOC-EWA-202105-02	誤報	合法DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-01	誤報	此台主機為本校DNS主機，經	MALWARE-CNC Torpig bot sinkhole server DNS lookup)
NTUSOC-EWA-202105-01	誤報	合法DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)
NTUSOC-EWA-202105-00	誤報	經查校內NAT對映ip 電腦群，	MALWARE-CNC Possible host infection - excessive DNS queries for .cn)
NTUSOC-EWA-202105-00	誤報		MALWARE-CNC Torpig bot sinkhole server DNS lookup)
NTUSOC-EWA-202105-00	誤報	合法DNS主機	MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter)

謝謝聆聽