區網網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

大 綱

- 資安案例分享
  - CoinMiner惡意挖礦木馬程式
  - IOT設備資安管控
  - User-agent資安事件
- TANet DDoS防禦
  - DDoS清洗機制
  - DDoS攻擊統計分析

CoinMiner惡意挖礦木馬程式(1/3)

(MALWARE-CNC Win.Trojan.CoinMiner outbound connection)

- 分析擷取封包後，發現這類事件的封包皆傳送特定 "Json" 格式內容

- 分析後發現上述封包之特徵為數位貨幣 – 門羅幣 (XMR)

CoinMiner惡意挖礦木馬程式(2/3)

(MALWARE-CNC Win.Trojan.CoinMiner outbound connection)

- 挖礦程式結合木馬後門，綁架無辜使用者的電腦，自動執行於背景，幫助「惡意軟體散播者」利用使用者主機的CPU挖礦。

  - ASOC 觀察搜集到的惡意程式，常駐於使用者電腦，且自動設定排程，

CoinMiner惡意挖礦木馬程式(3/3)

(MALWARE-CNC Win.Trojan.CoinMiner outbound connection)

➢ 建議措施

建議使用者盡快使用防毒軟體掃描並清除，或是利用以下所提供之惡意軟體清除程式掃毒：

- ✓ https://downloads.malwarebytes.com/file/mb3/
- ✓ https://security.symantec.com/nbrt/npe.aspx?&NUCLANG=zh-tw

WidgiToolbar 惡意連線事件分析(1/4)

(MALWARE-CNC User-Agent known malicious user-agent string - WidgiToolbar)

출처:北區ASOC整理

WidgiToolbar 惡意連線事件分析(2/4)

(MALWARE-CNC User-Agent known malicious user-agent string - WidgiToolbar)

- 分析發現此事件疑似因安裝 PDFcreator (一種PDF轉換程式)所致

Widgi Toolbar creates the following file(s):

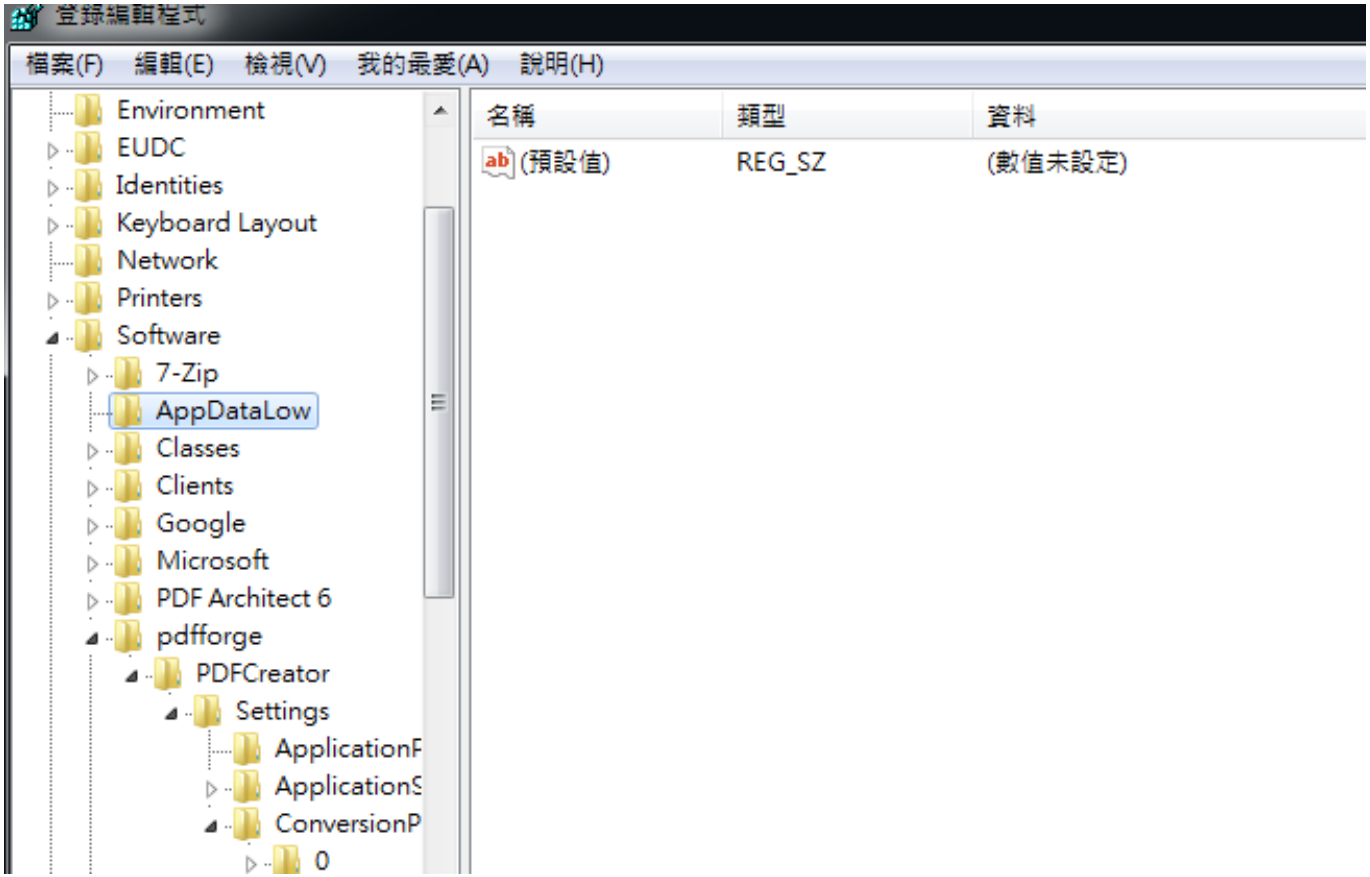
#	File Name	Size	MD5	Detection Count
1	%PROGRAMFILES%\pdfforge Toolbar\WidgiToolbarIE.dll	650,752	0369affb46aa2071d04a3fb361ee5bd0	7,546
2	%PROGRAMFILES%\pdfforge Toolbar\SearchSettings.exe	992,256	2ba55d793667eaca14437277dd472b29	4,432
3	%PROGRAMFILES%\pdfforge Toolbar\SearchSettings.dll	1,114,112	e3b00dc3e381c3e02fc34256d12168c2	2,624
4	%PROGRAMFILES%\PDFCreator Toolbar\v3.0.0.0\PDFCreator_Toolbar.dll	757,760	a9289dcc914ed8a96e6e91d9cd2babdb	128
5	%PROGRAMFILES%\pdfforge Toolbar\IE\1.1.2\pdfforgeToolbarIE.dll	20	a9a2ecd63b89704922764fc242a87053	27
6	%PROGRAMFILES%\pdfforge Toolbar\FF\chrome\TBM4A23.tmp	69,832	7d2561803908cd8a4a13098fc8499c93	26
7	%WINDIR%\TEMP\pdfforgeToolbar.exe	4,493,608	07fa90568290c3ae84db3787747940bf	8
8	%ALLUSERSPROFILE%\Application Data\pdfforge Toolbar			2
9	%ALLUSERSPROFILE%\pdfforge Toolbar			1

出處:北區ASOC整理

WidgiToolbar 惡意連線事件分析(3/4)

(MALWARE-CNC User-Agent known malicious user-agent string - WidgiToolbar)

- 從 PDFcreator 官網下載並安裝測試後，並未發現相關特徵，推測使用者疑似使用第三方網站所下載之軟體，因而遭加料



出處:北區ASOC整理

WidgiToolbar 惡意連線事件分析(4/4)

(MALWARE-CNC User-Agent known malicious user-agent string - WidgiToolbar)

➢建議事項

建議使用者先移除相關程式，並盡速使用防毒軟體掃描並清除或利用以下所提供之惡意軟體清除程式掃毒：

- ✓ https://downloads.malwarebytes.com/file/mb3/
- ✓ https://security.symantec.com/nbrt/npe.aspx?&NUCLANG=zh-tw

➢相關參考

- ✓ https://www.enigmasoftware.com/widgitoolbar-removal/

出處:北區ASOC整理

Test 惡意連線事件分析(1/2)

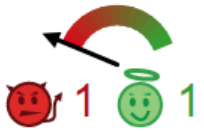
(MALWARE-CNC User-Agent known malicious user agent - test)

- 此事件是木馬偽裝成為Notepad.exe

Wireshark · Follow TCP Stream (tcp.stream eq 60) · request_1524022369

```
GET / HTTP/1.1
User-Agent: test
Host: www.baidu.com
Cache-Control: no-cache
Cookie: BAIDUID=B667597177F18B2AF4CF92BD3BF949B6:FG=1; BIDUPSID=B667597177F18B2AF4CF92BD3BF949B6;
PSTM=1523578448; H_PS_PSSID=1464_21108_18559_22075; BDSVRTM=0; BD_HOME=0
```

SHA256:	2b5064dcf918207d31537e41c1b43b6cac2b62f9d343005c1180dde8e21790d9
File name:	Notepad.exe
Detection ratio:	40 / 41
Analysis date:	2011-04-27 18:54:54 UTC (6 years, 11 months ago) View latest



出處:北區ASOC整理

Test 惡意連線事件分析(2/2)

(MALWARE-CNC User-Agent known malicious user agent - test)

- 建議

  使用防毒軟體進行掃描

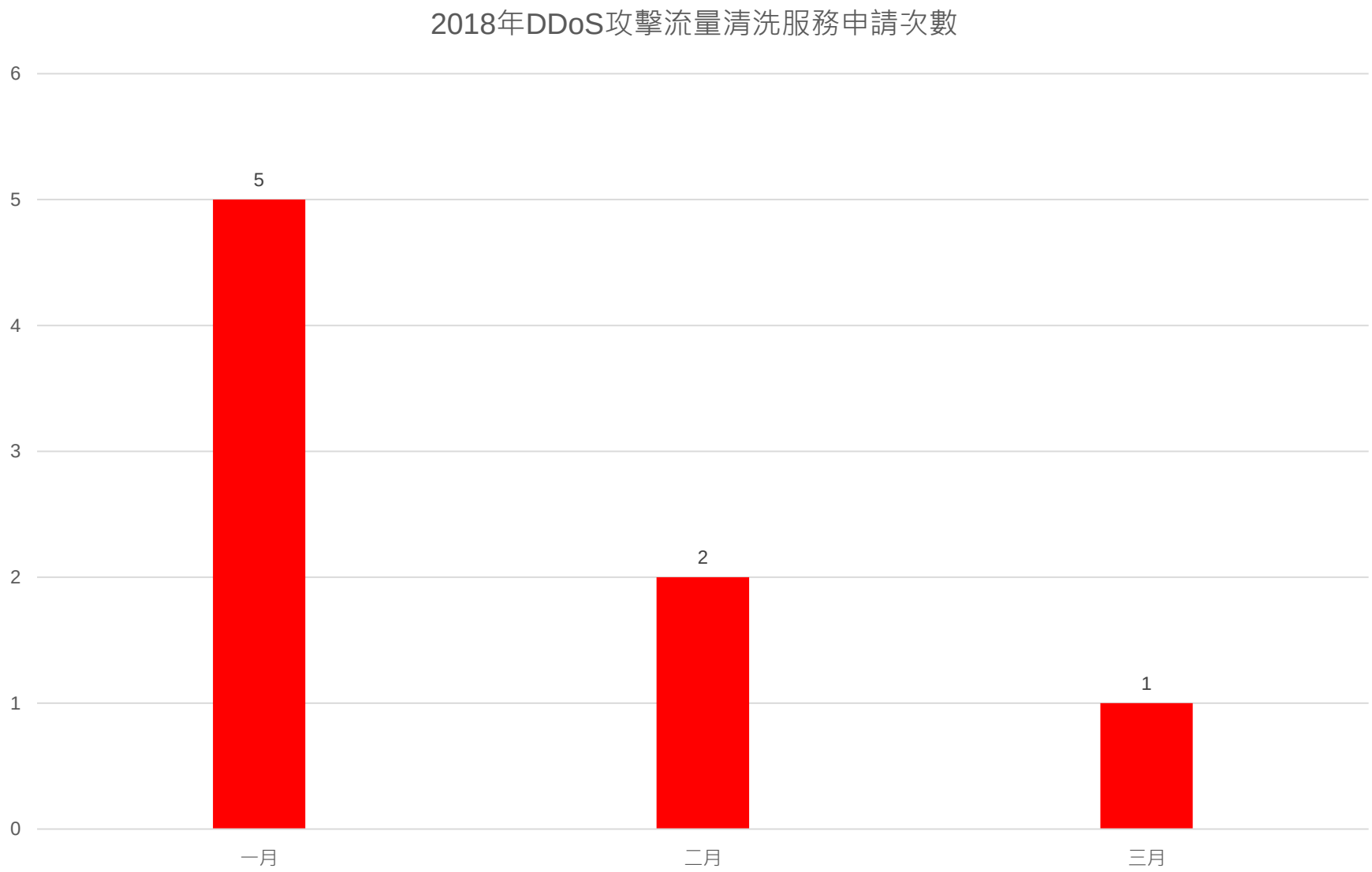
- 相關參考
  - ✓ https://baike.baidu.com/item/Notepad.exe/10684198 （此為百度網址）。
  - ✓ https://www.virustotal.com/en/file/2b5064dcf918207d31537e41c1b43b6cac2b62f9d343005c1180dde8e21790d9/analysis/1303930494/

出處:北區ASOC整理

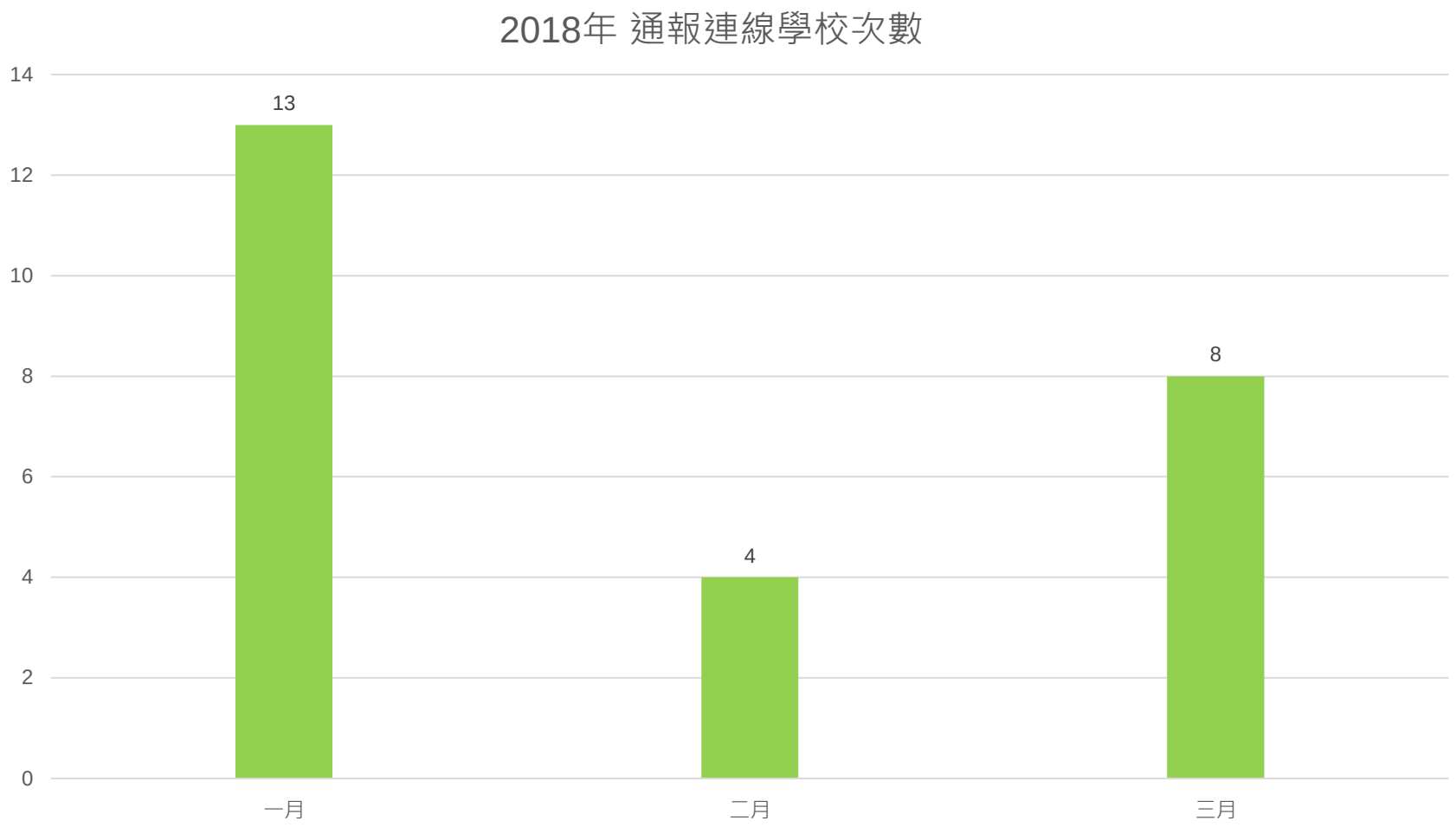
大 綱

- 資安案例分享
  - CoinMiner惡意挖礦木馬程式
  - IOT設備資安管控
  - User-agent資安事件
- TANet DDoS防禦
  - DDoS清洗機制
  - DDoS攻擊統計分析

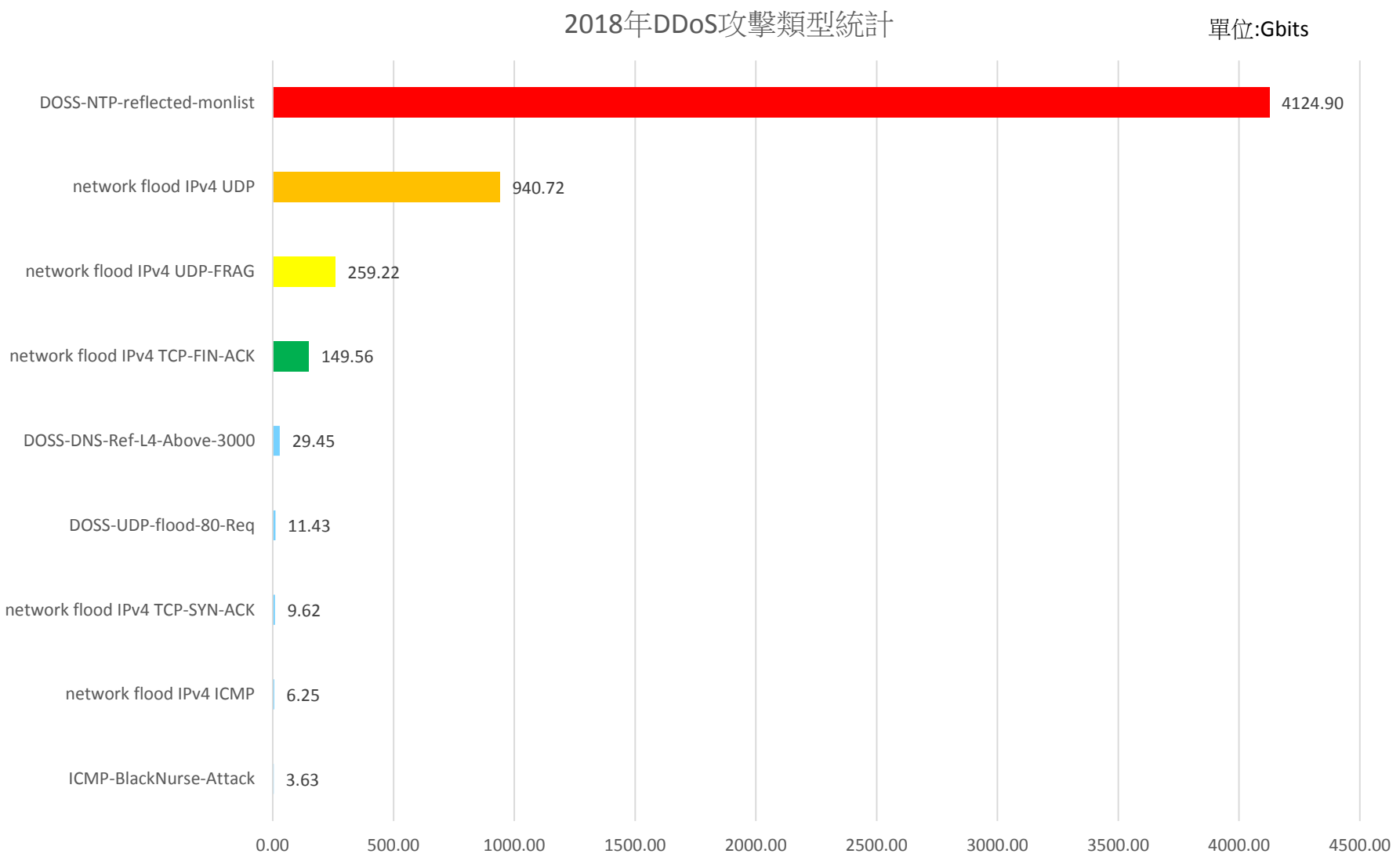
連線單位申請DDoS清洗服務次數統計



通知連線學校次數統計



DDoS攻擊類型統計


2018年DDoS攻擊類型統計
單位:Gbits
DOSS-NTP-reflected-monlist
4124.90
network flood IPv4 UDP
940.72
network flood IPv4 UDP-FRAG
259.22
network flood IPv4 TCP-FIN-ACK
149.56
DOSS-DNS-Ref-L4-Above-3000
29.45
DOSS-UDP-flood-80-Req
11.43
network flood IPv4 TCP-SYN-ACK
9.62
network flood IPv4 ICMP
6.25
ICMP-BlackNurse-Attack
3.63
0.00
500.00
1000.00
1500.00
2000.00
2500.00
3000.00
3500.00
4000.00
4500.00

Q & A