教育體系資安檢核

臺灣大學計資中心網路組
游子興
davisyou@ntu.edu.tw
02-33665008

網路惡意活動檢視

依照技服中心每週四公布之惡意中繼名單

封包側錄
tshark

* tshark -D
  * -D 顯示網卡

```
C:\Windows\System32>cd C:\Users\user\Desktop\WiresharkPortable\App\Wireshark

C:\Users\user\Desktop\WiresharkPortable\App\Wireshark>tshark -D
1. \Device\NPF_{406BE586-DD6C-47EC-9D36-5EF6F2FF565A} (? ?   ??* 8)
2. \Device\NPF_{4BF01F85-7FE3-4069-9BE1-7018FC2A1E2B} (? ?   ??* 6)
3. \Device\NPF_{CCE5347F-35B0-4718-94C6-B136AC036A66} (Ethernet0)
4. \Device\NPF_{D220FF15-65FB-47AE-921C-F383F594EA90} (VMware Network Adapter VMnet1)
5. \Device\NPF_{AD45E842-98D5-424D-B998-E1BCC1DDC648} (? ?   ??* 7)
6. \Device\NPF_{096A257A-BD78-4D9B-BB4C-D38018A25748} (VMware Network Adapter VMnet8)
7. \Device\NPF_Loopback (Adapter for loopback traffic capture)
8. ciscodump (Cisco remote capture)
9. randpkt (Random packet generator)
10. sshdump (SSH remote capture)
11. udpdump (UDP Listener remote capture)
```

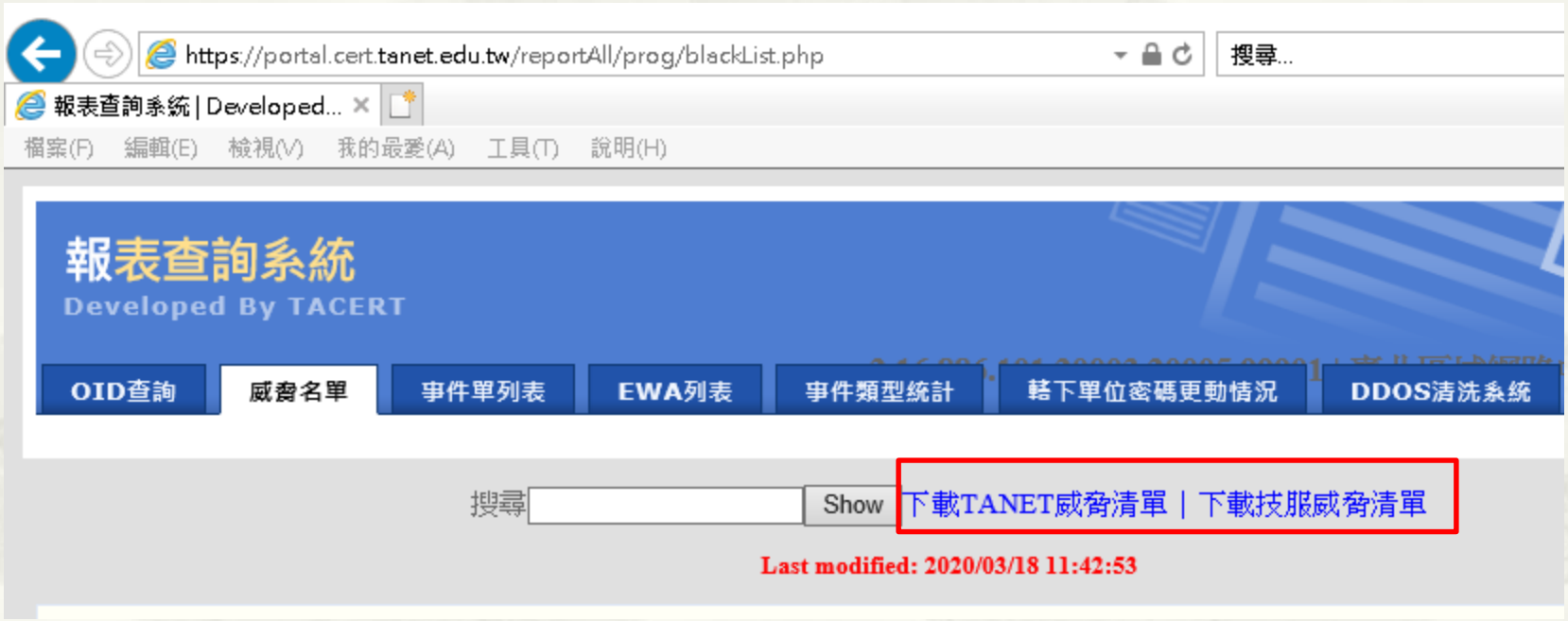
封包側錄
tshark

* tshark -i 3 -n -q -T tabs > 0826.csv
  * -i 3 -- 指定網卡 Etherneto
  * -n -- disable all name resolutions
  * -T tabs – 輸出格式
  * -q or -Q -- suppress the display of the packet summary or details;

* 文字編輯器
  * “→” 取代成 “to”

威脅清單下載

* https://portal.cert.tanet.edu.tw/index.html



TANet/技服 威脅清單

TANet威脅清單

惡意威脅來源清單列表

更新日期：2020年03月18日
情資來源：S-ASOC, N-ASOC, N-ISAC
清單編號：v2020.10

IP List only

■為本次新增之內容
*本清單為機敏文件，限TANet內部人員使用

資料來源	通報時間	IP位置	惡意網址	攻擊型態	國家
N-ASOC	2020/3/16	103.27.111.66		SERVER-WEBAPP /etc/pass	Hong Kong
N-ASOC	2020/3/16	137.59.19.212		SERVER-WEBAPP /etc/pass	Hong Kong
N-ASOC	2020/3/16	180.131.52.131		SERVER-OTHER Remote Desk	Korea
N-ASOC	2020/3/16	185.153.199.91	server-185-153-199-91.cloudedic.net	SERVER-OTHER Remote Desk	Russian
N-ASOC	2020/3/16	185.202.2.112		SERVER-OTHER Remote Desk	France
N-ASOC	2020/3/16	185.202.2.137		SERVER-OTHER Remote Desk	France
N-ASOC	2020/3/16	69.10.62.71		MALWARE-CNC User-Agent k	United States
N-ASOC	2020/3/16	93.174.93.216	no-reverse-dns-configured.com	SERVER-WEBAPP MVPower DV	Netherlands
S-ASOC	2020/3/14	103.21.206.230		網路攻擊	Indonesia
S-ASOC	2020/3/14	104.218.50.88		網路攻擊	United States
S-ASOC	2020/3/14	104.244.73.31		網路攻擊	Luxembourg

技服威脅清單

SN	Domain-List	FirstDate	LastDate
1	openssl3.csproject.org	2019-08-15	2019-08-15
2	carsails.allowed.org	2019-08-15	2019-08-15
3	ap21.ilvsmail.com	2019-04-25	2019-07-16
4	homepage.neithey.com	2019-04-30	2019-07-16
5	eclient.cybertw.com	2019-04-30	2019-07-01
6	broadweb.cybertw.com	2019-04-30	2019-07-01
7	cloud105.iworksme.com	2019-04-30	2019-06-24
8	tc379.ilvsmail.com	2019-04-25	2019-05-20
9	ad03.eynyforum.com	2019-04-30	2019-05-15
10	update.asuswebstorage.com.ssmailer.com	2019-05-06	2019-05-06
11	www.google.com.dns-report.com	2019-05-06	2019-05-06
12	cksogo.com	2019-05-02	2019-05-02
13	fs53.eynyforum.com	2019-05-02	2019-05-02
14	eynyforum.com	2019-05-02	2019-05-02

Domain + IP List

DnList(order_by_Priority) | DnList(order_by_sn) | IpList(order_by_Priority) | IpList(order_by_sn)

使用Excel VLOOKUP() 進行比對

- VLOOKUP(A1,Sheet2!A:B,2,FALSE)
  - Lookup_value
    - A1 -- 選擇 Sheet1, A1
    - 比對之欄位, 僅能有一個. (若有多個欄位需求, 可先合併欄位產生新欄位)
    - 也可用範圍 A1:A10
  - Table_array
    - Sheet2!A:B -- 選擇 Sheet2, A and B 全部
    - 僅能比對第一個欄位.
    - ※1.建議此 Sheet 在同一個 Excel 檔案, 否則會有問題.
    - 2.建議選擇整個 Column, 不要用範圍.
  - Col_index_num= 2 -- 傳回 Sheet2!B 的值
  - Range_lookup
    - FALSE -- Sheet1!A, Sheet2!A 兩者值比對需完全符合, 若找不到傳回 #N/A
    - TRUE/NULL -- Sheet1!A, Sheet2!A 傳回最接近的值
    - TRUE -- 也可用 1
    - FALSE -- 也可用 0
- =VLOOKUP(C25,三個月內清單!C:C,1,FALSE)

簡報完畢
謝謝