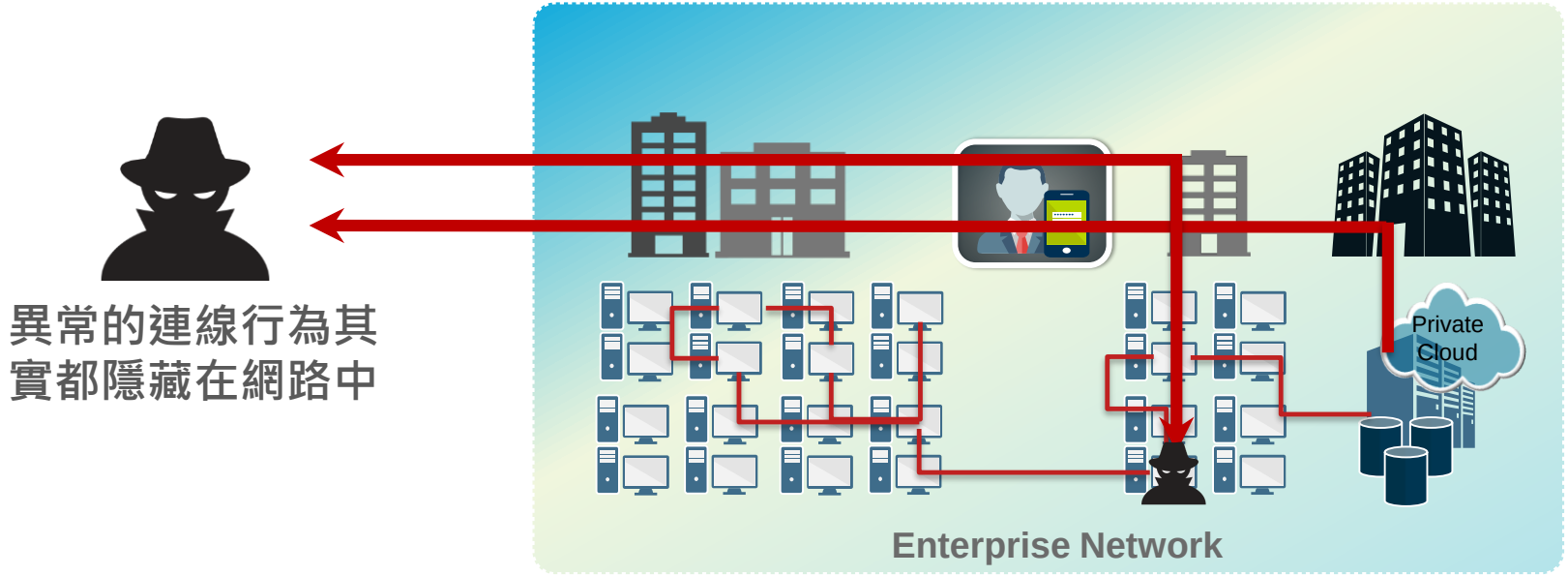
資安通報須具備的資訊

林家笙(Fungi Lin)

Security Solution consultant
Palo Alto Networks Taiwan

滲透入侵需要時間與步驟

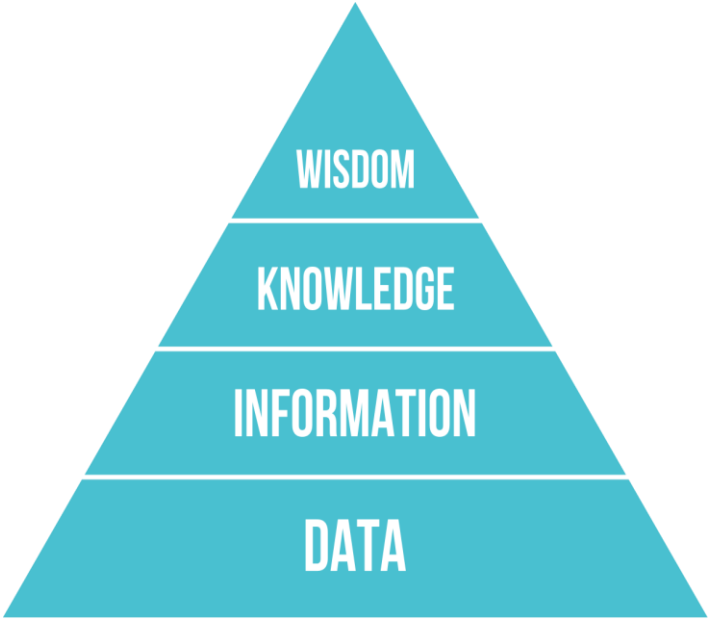


* 2016 Verizon Data Breach Investigation Report

數據粹煉的演進

過去

Signature
(Quantity)

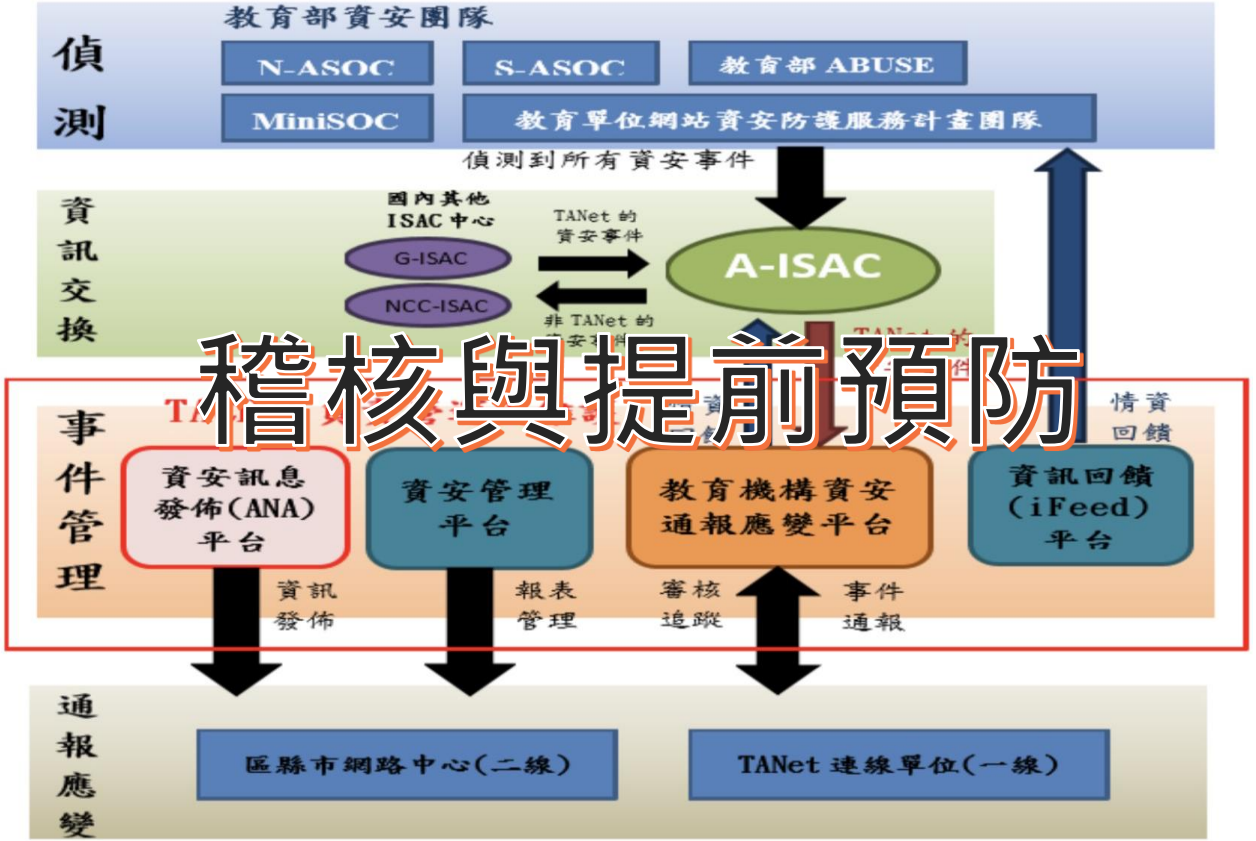


未來

Structured
Signature
(Quality)

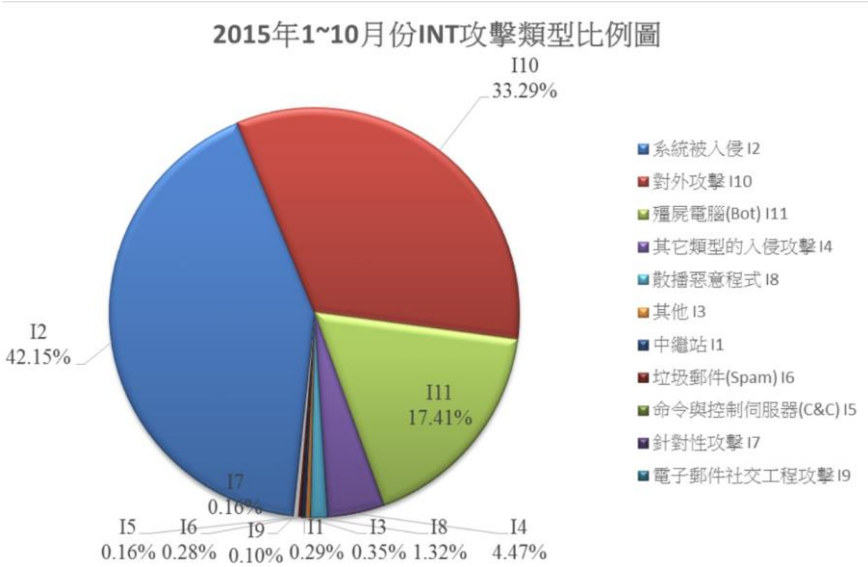
paloalto NETWORKS

教育機構資安通報機制運作



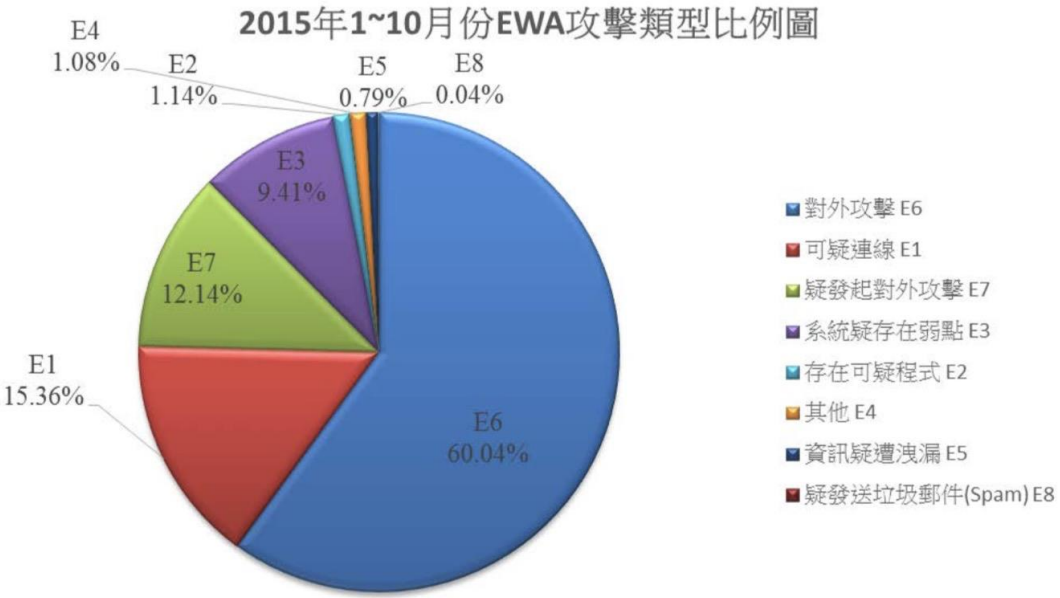
學術網路資安事件(告知通報事件)

事件子類別	數量
系統被入侵	7,520
對外攻擊	5,939
殭屍電腦(BOT)	3,106
其它類型的入侵攻擊	798
散播惡意程式	236
其他	63
中繼站	52
垃圾郵件(SPAM)	50
命令與控制伺服器(C&C)	29
針對性攻擊	28
電子郵件社交工程攻擊	18
總計	**17,839**



學術網路資安預警事件

事件子類別	數量
對外攻擊	4,708
可疑連線	1,204
疑發起對外攻擊	952
系統疑存在弱點	738
存在可疑程式	89
其他	85
資訊疑遭洩漏	62
疑發送垃圾郵件(SPAM)	3
總計	7,841



資安預警情報

- 資安預警情報(EWA)為教育部各資安計畫團隊或是其他情資來源單位，偵測到**疑似網路攻擊行為**時所發送的預警通知。
- **由一線單位進行檢查、處理及填報作業，區縣市網路中心進行追蹤作業**
- 一線單位收到資安預警通知時，請檢查該主機是否有異常網路活動跡象，並進行處理狀態回覆：
  - 確實事件：先於通報平台採『**自行通報**』取得事件單編號
  - **誤報：請詳填原因 (以利發單單位調校規則)**
  - 無法判斷：證據不足
- 處理時效：一星期內

如何強化疑似網路攻擊行為的資訊?

資安通報事件資訊

發生次數:1

開始時間	結束時間	事件名稱	來源位址	來源連接埠	來源所在國家或地區碼	目標位址	目標連接埠	目標位置國家或地區碼	彙總的事件計數
2019/07/12 09:18:44	2019/07/12 09:18:44	PUA-OTHER XMR-Stak cryptocurrency mining pool connection attempt	[redacted]	62873	TW	45.195.146.32	8888	HK	1

發生次數:1

開始時間	結束時間	事件名稱	來源位址	來源連接埠	來源所在國家或地區碼	目標位址	目標連接埠	目標位置國家或地區碼	彙總的事件計數
2019/07/10 16:51:54	2019/07/10 16:51:54	PUA-OTHER Cryptocurrency Miner outbound connection attempt	[redacted]	54547	TW	88.99.242.92	5555	DE	1

發生次數:1

開始時間	結束時間	事件名稱	來源位址	來源連接埠	來源所在國家或地區碼	目標位址	目標連接埠	目標位置國家或地區碼	彙總的事件計數
2019/07/09 08:36:24	2019/07/09 08:36:24	MALWARE-CNC Worm.Silly variant outbound connection	[redacted]	49448	TW	117.20.41.68	80	SG	1

探討案例一: 門羅幣挖礦資安通報

門羅幣挖礦資安通報

原發布編號	ASOC-INT-201811-0xxx	原發布時間	2018-11-07 08:16:45
事件類型	對外攻擊	原發現時間	2018-11-07 06:30:32
事件主旨	通報:[XXXX 大學]xxx.xxx.xxx.xxx General.Interest: Monero.Cryptocurrency.Miner,		
事件描述	ASOC 發現貴單位(XXXX 大學)所屬 xxx.xxx.xxx.xxx 疑似對外進行 General.Interest: Monero.Cryptocurrency.Miner, 攻擊		
手法研判	Monero(XMR)是一個創建於 2014 年 4 月開源加密貨幣，它可以在 Windows、Mac、Linux 和 FreeBSD 上運行。貴單位疑似對外進行非法攻擊行為，利用 Monero 挖礦惡意軟體進行採礦行為。Monero 挖礦程序會吃掉受害機器的 CPU 運算能力，進而損耗受害機器系統資源。		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.確實安裝修補程式並且更新系統。 5.攻擊名稱相關參考資料網站： https://fortiguard.com/appcontrol/44016 https://github.com/fireice-uk/xmr-stak-cpu https://en.wikipedia.org/wiki/Monero_(cryptocurrency)		

其實可以有更多資訊呈現出來

a. 存取惡意中繼站清單(C2 Domain)

b. 存取惡意網站(URL 清單)

探討案例一: 門羅幣挖礦資安通報,應具有更詳細的資訊,自動化更新黑名單

File Analysis | Network Sessions | Coverage | Indicators

WildFire AV Signature

Signature Name
Virus/Win32.WGeneric.mvmtt

C2 Domain Signatures

Domain	Signature Name
xmr.crypto-pool.fr	generic:xmr.crypto-pool.fr

URLs

URL	Category
time.windows.com	Computer and Internet Info
a3-129.akadns.net	Content Delivery Networks
a5-130.akadns.org	Content Delivery Networks
akadns.net	Content Delivery Networks
xmr.crypto-pool.fr	Insufficient Content

Domain

				Indicator
!	113	7k	2	xmr.crypto-pool.fr
!	209	8k	2	crypto-pool.fr
!	23k	0.1M	0.2M	dns200.anycast.me

Mutex

			Indicator
1	3	0	42ZhhaaBgtVLswaNNd94PaEddkpBGdjBLcUxFaxj9spRFHAk1h2BpF4Y4ztwERR3a2cw1yiQpFUij4KxukMF3yeh73Zw6qx

Connection Activity

			Parent Process	Parameters
2	5	0	sample.exe	connect , 212.129.44.156:80 , 2 , FR
67M	13M	0.5M	unknown	udp , 13.65.245.138:123 , US
546M	93M	5M	unknown	udp , 224.0.0.252:5355 , -

當收到這份資安通報時,可以使用API的方式,把相關的資訊更新到網路設備上

原發布編號	ASOC-INT-201811-0xxx	原發布時間	2018-11-07 08:16:45
事件類型	對外攻擊	原發現時間	2018-11-07 06:30:32
事件主旨	通報:[XXXX大學]xxx.xxx.xxx.xxx General.Interest: Monero.Cryptocurrency.Miner,		
事件描述	ASOC發現貴單位(XXXX大學)所屬 xxx.xxx.xxx.xxx 疑似對外進行 General.Interest: Monero.Cryptocurrency.Miner, 攻擊		
惡意中繼站	xmr.crypto-pool.fr, crypto-pool.fr, dns200.anycast.me		
惡意網站	crypto-pool.fr, xmr.crypto-pool.fr		
惡意連線的IP	212.129.44.157:80, 13.65.245.138:123		
SHA256	ea579b7d0cc1106cdb285a41bc031205240b93f438c000a7aee30cd80dc72d52		
SHA1	0902181d1b9433b5616763646a089b1bdf428262		
MD5	23a2278fae626df2e134b9d141dc59dc		
Mutex	42ZhhaaBgtVLswaNNd94PaEddkpBGdjBLcUxFaxj9spRFHAk1h2BpF4Y4ztwERR3a2cw1yiQpFUij4KxukMF3yeh73Zw6qx		
手法研判	Monero(XMR)是一個創建於2014年4月開源加密貨幣，它可以在Windows、Mac、Linux和FreeBSD上運行。貴單位疑似對外進行非法攻擊行為，利用Monero挖礦惡意軟體進行採礦行為。Monero挖礦程序會吃掉受害機器的CPU運算能力，進而損耗受害機器系統資源。		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.確實安裝修補程式並且更新系統。 5.攻擊名稱相關參考資料網站：https://fortiguard.com/appcontrol/44016 https://github.com/fireice-uk/xmr-stak-cpu https://en.wikipedia.org/wiki/Monero_(cryptocurrency)		

探討案例二: SMB攻擊資安通報

SMB 攻擊之資安通報

發佈編號	ASOC-INT-201811-0xxx	發佈時間	2018-11-16 08:10:06
事件類型	對外攻擊	發現時間	2018-11-15 14:53:19
事件主旨	通報:[XXXX 大學] xxx.xxx.xxx.xxx MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure		
事件描述	ASOC 發現貴單位(XXXX 大學)所屬 xxx.xxx.xxx.xxx 疑似對外進行 MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure 攻擊		
手法研判	貴單位疑似對外進行非法攻擊，Microsoft Server Message Block 1.0 (SMBv1) 處理特定要求的方式中存在資訊洩漏弱點。成功利用此弱點的攻擊者可能會蓄意製作封包，藉此導致伺服器資訊洩漏。如果攻擊者傳送蓄意製作的訊息到 Windows SMBv1 伺服器，最嚴重的弱點可能會允許遠端執行程式碼。 受影響產品： Microsoft Windows 7 Microsoft Windows 8.1 Microsoft Windows RT 8.1 Microsoft Windows 10 Microsoft Windows Vista Microsoft Windows Server 2016 Microsoft Windows Server 2012 R2 (Server Core) Microsoft Windows Server 2008 R2 Microsoft Windows Server 2008 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2		
處理建議	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.不要點擊來路不明的網站和檔案等。 5.檢視及執行各系統之安全修補，並將系統更新至最新版本 https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx 6.攻擊名稱相關參考資料網站： http://fortiguard.com/encyclopedia/ips/43799 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147		

探討案例二: 可以探討哪些攻擊家族使用SMB去做擴散

CoinMiner

Enabled 14,902

Owner Palo Alto Networks Unit42
 # Samples 2,283,422
Last Hit 3 days ago on 11/20/2018 6:37:43am
Tag Class Malware Family
Source Unit 42
Created 01/01/2016 12:00:00am
Updated 11/07/2018 9:01:45am
Votes 1
Aliases NeksMiner NsMiner
Groups CryptoMiner

Description:
This threat uses your PC to generate Cryptocurrencies. It installs software that can make your PC run slower than usual.

DNS Activity *is in the list*
www.multipool.us
www.bravo-mining.com
nanopool.org
moneroexplorer.com
coinhive.com
www.antpool.com
www.f2pool.com
slushpool.com
www.viabtc.com
bixin.com
bitfury.com
bcmonster.com
www.bw.com

探討案例二: SMB攻擊資安通報,應具有更詳細的資訊

Process Activity

			Parent Process	Action	Parameters
▲	0	240	0	sample.exe	CreateProcessInternalW	<null> , \\smb.com\bvb.exe
▲	0	234	0	sample.exe	\\smb.com\bvb.exe	\\smb.com\bvb.exe

URLs

URL	Category
xmr.f2pool.com	Computer and Internet Info
f2pool.com	Computer and Internet Info
vip6.alidns.com	Computer and Internet Info
vip5.alidns.com	Computer and Internet Info
teredo.ipv6.microsoft.com	Computer and Internet Info
im.qq.com	Internet Communications and Telephony
cgi.im.qq.com	Internet Communications and Telephony
dns10.hichina.com	Web Hosting
dns9.hichina.com	Web Hosting
5yyw.cn	Insufficient Content
ns-tel1.qq.com	Internet Portals
ns-os1.qq.com	Internet Portals
ns-cmn1.qq.com	Internet Portals
ns-cnc1.qq.com	Internet Portals

這些URLs有沒有可能是有問題的存取

Domain

			Indicator
▲	0	11	0	almashosting.com
▲	0	10	0	ftp.almashosting.com
!	2k	0.3M	1k	checkip.dyndns.org

Mutex

			Indicator
!	0.3M	3M	0.6M	Global\.net clr networking
			Local\c:!users!loktza!appdata!roaming!microsoft!windows!cookies!
			Local\c:!users!loktza!appdata!local!microsoft!windows!temporary internet files!content.ie5!
			Local\c:!users!loktza!appdata!local!microsoft!windows!history!history.ie5!

URL

			Indicator
▲	0	2	0	5yyw.cn/long.exe
▲	0	1	0	91.218.115.133/64.exe
▲	0	1	0	91.218.115.133/32.exe

Domain

			Indicator
▲	0	53	0	5yyw.cn
!	428	10k	1k	vip5.alidns.com
!	432	10k	1k	vip6.alidns.com

IPv4

			Indicator
▲	0	1	0	91.218.115.133

當收到這份資安通報時,可以使用API的方式,把相關的資訊更新到網路設備上

發佈編號	ASOC-INT-201811-0xxx	發佈時間	2018-11-16 08:10:06
事件類型	對外攻擊	發現時間	2018-11-15 14:53:19
事件主旨	通報:[XXXX大學] xxx.xxx.xxx.xxx MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure		
事件描述	ASOC發現貴單位(XXXX大學)所屬 xxx.xxx.xxx.xxx 疑似對外進行 MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure 攻擊		
惡意中繼站	xmr.f2pool.com, f2pool.com, 5yyw.cn		
惡意網站	5yyw.cn, f2pool.com, xmr.f2pool.com		
惡意連線的IP	91.218.115.133		
SHA256	e4c8535975d1cad358e53f5e22873a000a59b712c09d5d7e78faaaeaae0196a9		
SHA1	a6ab1b4e75cf20639d12fe63d0cdb64b6cf872a5		
MD5	a1045c302ba3d321e8ebfad64dbe6fd7		
Mutex	Local\c:!users!c1dwjr!appdata!roaming!microsoft!windows!cookies!		
手法研判	貴單位疑似對外進行非法攻擊，Microsoft Server Message Block 1.0 (SMBv1) 處理特定要求的方式中存在資訊洩漏弱點。成功利用此弱點的攻擊者可能會蓄意製作封包，藉此導致伺服器資訊洩漏。如果攻擊者傳送蓄意製作的訊息到 Windows SMBv1 伺服器，最嚴重的弱點可能會允許遠端執行程式碼。 受影響產品： Microsoft Windows 7 Microsoft Windows 8.1 Microsoft Windows RT 8.1 Microsoft Windows 10 Microsoft Windows Vista Microsoft Windows Server 2016 Microsoft Windows Server 2012 R2 (Server Core) Microsoft Windows Server 2008 R2 Microsoft Windows Server 2008 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2		
處理建議	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.不要點擊來路不明的網站和檔案等。 5.檢視及執行各系統之安全修補，並將系統更新至最新版本 https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx 6.攻擊名稱相關參考資料網站： http://fortiguard.com/encyclopedia/ips/43799 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147		

探討案例三:遠端桌面入侵攻擊之資安通報

發佈編號	ASOC-INT-201811-0xxx	發佈時間	2018-11-06 08:10:28
事件類型	對外攻擊	發現時間	2018-11-05 21:09:47
事件主旨	通報:[XXXX 大學] xxx.xxx.xxx.xxx MS.RDP.Connection.Brute.Force		
事件描述	ASOC 發現貴單位(XXXX 大學)所屬 xxx.xxx.xxx.xxx 疑似對外進行 MS.RDP.Connection.Brute.Force 攻擊		
手法研判	貴單位疑似對外進行非法攻擊行為，遠端攻擊者對 Microsoft RDP(Remote Desktop Protocol)進行暴力的密碼猜測攻擊，攻擊者在 10 秒內進行 200 次的登入請求，如成功利用將可以連入未經授權的系統，進行非法的存取。		
處理建議	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常或未經許可的連接埠，並查看記錄是否有外界對貴單位內部 IP 之異常連線。 2.如發現為非授權的連線，建議將該 IP 於防火牆阻擋。 3.建議針對被攻擊的主機做好相關主機系統服務檢查及弱點修補確認的工作，並關閉不需要的服務。 4.將所使用的密碼複雜度提高。		

探討案例三:遠端桌面入侵攻擊之資安通報,應具有更詳細的資訊,可以探討哪些攻擊家族,使用RDP去做擴散

Process Activity

				Parent Process	Action	Parameters
⚠	8	368	0	<null>	WaitForSingleObject	000002e8 , 0000000a(original:0000000a , actual:000000cb)
⚠	0	38	0	plugin-container.exe	created	Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 22 /TN "Broadcom Wireless Manager UI" /TR "\"C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\bcmntray.exe\""
⚠	0	38	0	<null>	CreateProcessInternalW	C:\Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 22 /TN "Broadcom Wireless Manager UI" /TR "\"C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\bcmntray.exe\""
⚠	0	10	0	sample.exe	created	Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 22 /TN "Broadcom Wireless Manager UI" /TR "\"C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\bcmntray.exe\""
⚠	0	10	0	sample.exe	CreateProcessInternalW	C:\Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 22 /TN "Broadcom Wireless Manager UI" /TR "\"C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\bcmntray.exe\""
⚠	0	3	0	plugin-container.exe	created	Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC ONLOGON /TN "Steam Client Bootstrapper" /TR "\"C:\Program Files\Java\jdk1.8.0_92\lib\visualvm\profiler\Steam.exe\""
⚠	0	3	0	<null>	CreateProcessInternalW	C:\Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC ONLOGON /TN "Steam Client Bootstrapper" /TR "\"C:\Program Files\Java\jdk1.8.0_92\lib\visualvm\profiler\Steam.exe\""
⚠	0	2	0	plugin-container.exe	created	Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 10 /TN "RDP Clip Monitor" /TR "\"C:\Program Files\Common Files\System\Ole DB\en-US\rdpclip.exe\""
⚠	0	2	0	plugin-container.exe	created	Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 26 /TN "ATISmart" /TR "\"C:\Program Files\Java\jdk1.8.0_92\lib\missioncontrol\features\org.eclipse.equinox.p2.core.feature_1.3.0.v20140523-0116\META-INF\ati2s9ag.exe\""
⚠	0	2	0	plugin-container.exe	created	Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 34 /TN "COMODO" /TR "\"C:\Program Files\Java\jdk1.8.0_92\lib\missioncontrol\features\org.eclipse.ecf.core.feature_1.1.0.v20140827-1444\META-INF\CLPSLA.exe\""
⚠	0	2	0	<null>	CreateProcessInternalW	C:\Windows\System32\schtasks.exe , "C:\Windows\System32\schtasks.exe" /CREATE /F /SC MINUTE /MO 10 /TN "RDP Clip Monitor" /TR "\"C:\Program Files\Common Files\System\Ole DB\en-US\rdpclip.exe\""

探討案例三:遠端桌面入侵攻擊之資安通報,應具有更詳細的資訊,可以探討那些攻擊家族,使用RDP去做擴散

URL	Category
edgedns-tm.info	Unknown

WildFire DNS History

Request	Response
trafficmanager.net	tm1.edgedns-tm.info

Passive DNS History

Request	Response	Count
tm1.edgedns-tm.info	13.107.247.10	118,212,041
tm1.edgedns-tm.info	13.107.252.10	79,218,627
tm1.edgedns-tm.info	204.79.195.41	240,825,263
tm1.edgedns-tm.info	none	138,643
trafficmanager.net	tm1.edgedns-tm.info	8,159,850

jhProtominer

Owner Palo Alto Networks Unit42
Samples 465,666
Last Hit 11 days ago on 11/11/2018 9:05:01pm
Tag Class Malware Family
Source Unit 42
Created 10/04/2018 6:30:20am
Updated 10/04/2018 6:30:20am
Votes 0
Groups CryptoMiner

Description:
jhProtominer is a high performance miner for Protoshares. It uses a different algorithm to allow arbitary memory usage per thread at the cost of mining speed.

Status	Hits	Last Hit	Definition
Enabled	33,679		Match all of the following conditions: **Mutex Activity** *contains* AutoProto_11 **Other API Activity** *contains* plugin-container.exe , IsDebuggerPresent

當收到這份資安通報時,可以使用API的方式,把相關的資訊更新到網路設備上

發佈編號	ASOC-INT-201811-0xxx	發佈時間	2018-11-06 08:10:28
事件類型	對外攻擊	發現時間	2018-11-05 21:09:47
事件主旨	通報:[XXXX大學] xxx.xxx.xxx.xxx MS.RDP.Connection.Brute.Force		
事件描述	ASOC發現貴單位(XXXX大學)所屬 xxx.xxx.xxx.xxx 疑似對外進行 MS.RDP.Connection.Brute.Force 攻擊		
惡意中繼站	tm1.edgedns-tm.info, trafficmanager.net		
惡意網站	edgedns-tm.info		
惡意連線的IP	13.107.247.10, 13.107.252.10, 204.79.195.41		
SHA256	12334a1da1113899c210e1a2744d8c3c88ed0241a78d2c134aeef5f8dd0aad29		
SHA1	8b137f36b447ecb0ce0c6122ec74b07ee0961af8		
MD5	85b8723471456f0f5fdf3e29b56772bb		
Mutex	Global\SyncRootManager		
手法研判	貴單位疑似對外進行非法攻擊行為，遠端攻擊者對Microsoft RDP(Remote Desktop Protocol)進行暴力的密碼猜測攻擊，攻擊者在10秒內進行200次的登入請求，如成功利用將可以連入未經授權的系統，進行非法的存取。		
處理建議	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常或未經許可的連接埠，並查看記錄是否有外界對貴單位內部IP之異常連線。 2.如發現為非授權的連線，建議將該IP於防火牆阻擋。 3.建議針對被攻擊的主機做好相關主機系統服務檢查及弱點修補確認的工作，並關閉不需要的服務。 4.將所使用的密碼複雜度提高。		

探討案例四:網頁存在任意下載漏洞之資安通報

原發布編號	TACERT-EWA-20180920-xxxxx	原發布時間	2018-09-20 14:31:17
事件類型	其他	原發現時間	2018-09-20 14:28:35
事件主旨	TACERT 接獲外部單位通知發現貴單位 XXXX 大學[xxx.xxx.xxx.xxx] 網頁程式存在任意檔案下載(Arbitrary File Download)漏洞		
事件描述	貴單位網頁程式存在任意檔案下載(Arbitrary File Download)漏洞，此漏洞可能導致貴單位機敏資料外洩，建議貴單位盡速修補該漏洞，以防止資料外洩。 漏洞注入點：http://ph.med.ncku.edu.tw/admin/download/file/down.php?filename={payload}		
手法研判	修補該程式漏洞，對輸入欄位進行惡意字元過濾作業		

這部份為WAF的保護功能之一

探討案例五:濫發電子郵件之資安通報

原發布編號	TWCERTCC-INT-201807-2980	原發布時間	2018-08-02 12:45:30
事件類型	垃圾郵件(Spam)	原發現時間	2018-07-09 07:42:00
事件主旨	教育部用戶資訊設備 IP:「xxx.xxx.xxx.xxx」疑似對外散播垃圾郵件(SPAM Mail)警訊通知		
事件描述	TWCERT/CC 於近日接獲國外 CERT 通報，發現 貴單位資訊設備在 2018/7/9 期間疑似發送垃圾郵件，建議盡速確認並解決相關問題。		
手法研判	垃圾郵件(Spam)		
建議措施	1.依事件描述所提供之資訊設備 IP，找出疑似遭入侵之資訊設備。 2.若確認該資訊設備已遭入侵，建議重新安裝作業系統，並更新至最新修補程式，亦建議更換系統使用者之相關密碼。若暫時無異常行為，建議持續觀察一個星期左右。 3.安裝防毒軟體並更新至最新版，並注意病毒碼須持續更新。 4.避免開啟來路不明的電子郵件。		

這部份為Spam Mail的功能

XX中心:近期駭客利用九合一選舉,冒用公務之名發送相關標題電子郵件,誘使使用者開啟惡意附件,植入惡意程式,目前已知相關的郵件訊息

1.冒名寄件者:「lgagl@cec[.]gov[.]tw」

2.惡意信件主旨:

(1)「107年台中選舉公告」

(2)「107年臺南選舉公告」

(3)「107年直轄市、縣市議員選舉區變更公告.doc[__空白__].exe」

3.惡意附件名稱:「107年直轄市、縣市議員選舉區變更公告.doc.exe」

4.惡意中繼站:「www[.]account_mentgooggl[.]serveuser[.]com」

當某個區網某天看到一件資安事件,能不能反饋至下轄單位設備

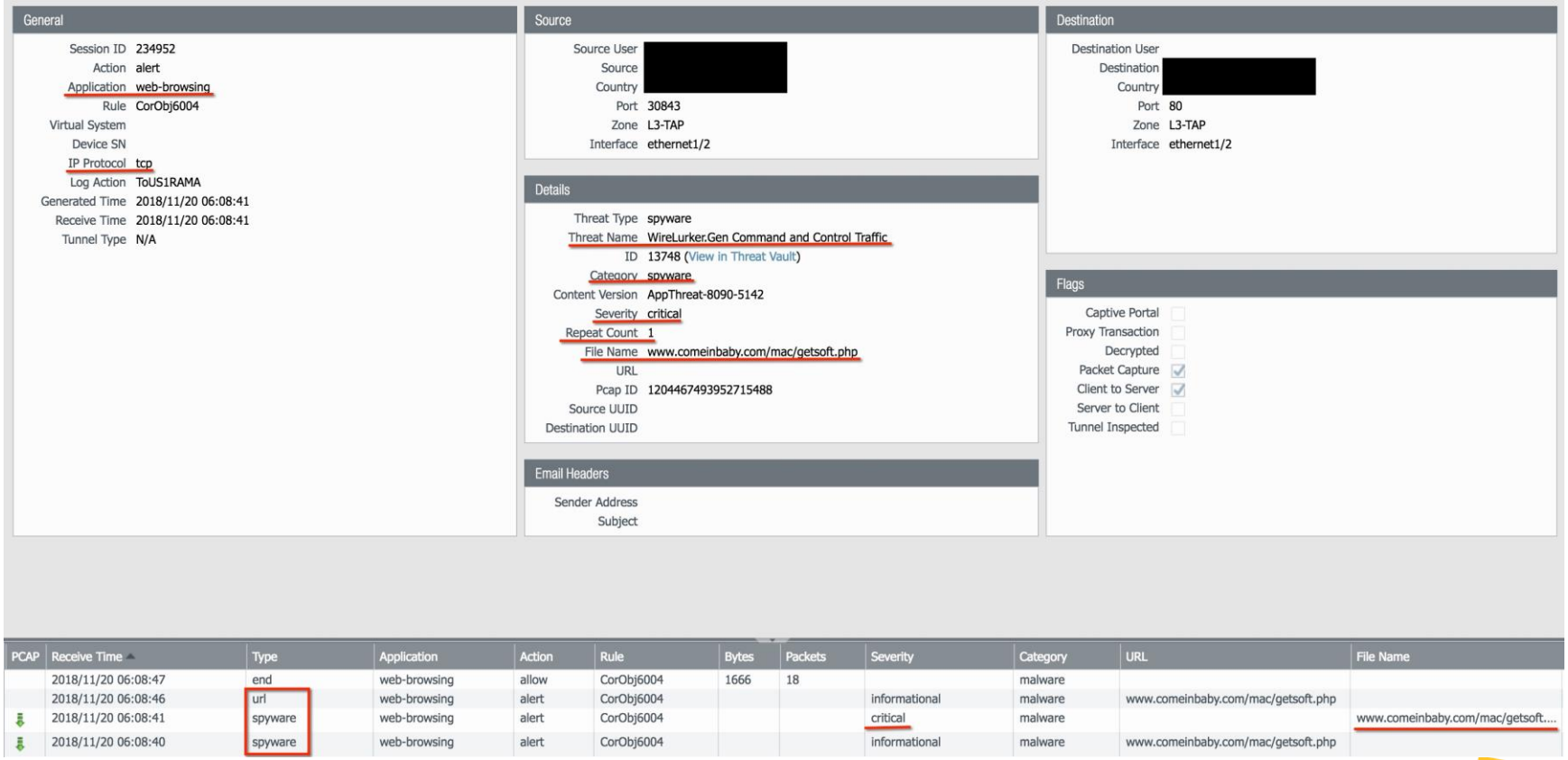
		Receive Time	Type	Name	Generate Time	Count	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity	File Name	URL
		11/20 07:27:34	spyware	WireLurker.Gen Command and Control Traffic	11/20 07:27:34	1	L3-TAP	L3-TAP	[redacted]		80	web-browsing	alert	critical	www.comeinb...	
		11/20 07:27:33	spyware	Suspicious HTTP Evasion Found	11/20 07:27:33	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		www.comeinb...
		11/20 07:05:36	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 07:05:36	1	L3-TAP	L3-TAP			16464	unknown-udp	drop	critical		
		11/20 07:01:40	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 07:01:40	1	L3-TAP	L3-TAP			16464	unknown-udp	drop	critical		
		11/20 07:01:17	spyware	Suspicious HTTP Evasion Found	11/20 07:01:17	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		networksecurit...
		11/20 07:01:16	spyware	WireLurker.Gen Command and Control Traffic	11/20 07:01:16	1	L3-TAP	L3-TAP			80	web-browsing	alert	critical	www.comeinb...	
		11/20 07:01:16	spyware	Suspicious HTTP Evasion Found	11/20 07:01:16	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		www.comeinb...
		11/20 06:34:58	spyware	WireLurker.Gen Command and Control Traffic	11/20 06:34:58	1	L3-TAP	L3-TAP			80	web-browsing	alert	critical	www.comeinb...	
		11/20 06:14:30	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 06:14:30	1	L3-TAP	L3-TAP			16471	unknown-udp	drop	critical		
		11/20 06:09:04	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 06:09:04	1	L3-TAP	L3-TAP			16464	unknown-udp	drop	critical		
		11/20 06:08:41	spyware	WireLurker.Gen Command and Control Traffic	11/20 06:08:41	1	L3-TAP	L3-TAP			80	web-browsing	alert	critical	www.comeinb...	
		11/20 06:08:40	spyware	Suspicious HTTP Evasion Found	11/20 06:08:40	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		www.comeinb...

可以看到攻擊的名稱

所使用的應用程式

檔案名稱

詳細的欄位紀錄



General

Session ID	234952
Action	alert
Application	web-browsing
Rule	CorObj6004
Virtual System	
Device SN	
IP Protocol	tcp
Log Action	ToUS1RAMA
Generated Time	2018/11/20 06:08:41
Receive Time	2018/11/20 06:08:41
Tunnel Type	N/A

Source

Source User	
Source	[redacted]
Country	
Port	30843
Zone	L3-TAP
Interface	ethernet1/2

Destination

Destination User	
Destination	[redacted]
Country	
Port	80
Zone	L3-TAP
Interface	ethernet1/2

Details

Threat Type	spyware
Threat Name	WireLurker.Gen Command and Control Traffic
ID	13748 (View in Threat Vault)
Category	spyware
Content Version	AppThreat-8090-5142
Severity	critical
Repeat Count	1
File Name	www.comeinbaby.com/mac/getsoft.php
URL	
Pcap ID	1204467493952715488
Source UUID	
Destination UUID	

Flags

Captive Portal	☐
Proxy Transaction	☐
Decrypted	☐
Packet Capture	☑
Client to Server	☑
Server to Client	☐
Tunnel Inspected	☐

Email Headers

Sender Address	
Subject	

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL	File Name
	2018/11/20 06:08:47	end	web-browsing	allow	CorObj6004	1666	18		malware		
	2018/11/20 06:08:46	url	web-browsing	alert	CorObj6004			informational	malware	www.comeinbaby.com/mac/getsoft.php	
⬇	2018/11/20 06:08:41	spyware	web-browsing	alert	CorObj6004			critical	malware		www.comeinbaby.com/mac/getsoft....
⬇	2018/11/20 06:08:40	spyware	web-browsing	alert	CorObj6004			informational	malware	www.comeinbaby.com/mac/getsoft.php	

觀察到來源IP的異常連線(問DNS,無週期性且少量連線數,最後下載檔案)

		Receive Time	Type	Name	Generate Time	Count	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity	File Name	URL
		11/20 07:27:34	spyware	WireLurker.Gen Command and Control Traffic	11/20 07:27:34	1	L3-TAP	L3-TAP	[redacted]		80	web-browsing	alert	critical	www.comeinb...	
		11/20 07:27:33	spyware	Suspicious HTTP Evasion Found	11/20 07:27:33	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		www.comeinb...
											16464	unknown-udp	drop	critical		
											16464	unknown-udp	drop	critical		
											80	web-browsing	alert	informational		networksecurit...
											80	web-browsing	alert	critical	www.comeinb...	
											80	web-browsing	alert	informational		www.comeinb...
											80	web-browsing	alert	critical	www.comeinb...	
											16471	unknown-udp	drop	critical		
											16464	unknown-udp	drop	critical		
											80	web-browsing	alert	critical	www.comeinb...	
											80	web-browsing	alert	informational		www.comeinb...

AutoFocus Intelligence Summary - 192.168.5.210 (Read Only)

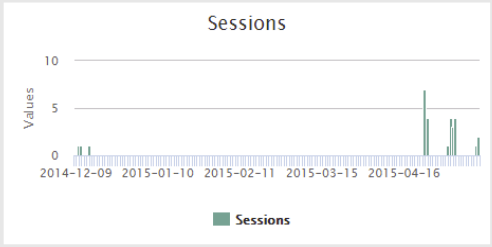
Search Autofocus for 192.168.5.210

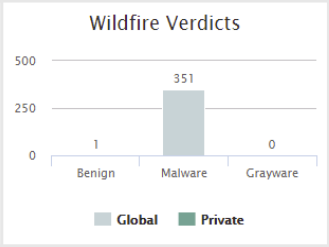
Passive DNS

Request	Type	Response	Count	First Seen	Last Seen
192-168-5-210.5c58057ea30b43cb90113751aa28b5e9.plex.direct	A	192.168.5.210	246	2015-08-03T16:28:45	2015-10-26T12:10:07
192-168-5-210.b8ca7437582c49e6baf8923d30e6da9b.plex.direct	A	192.168.5.210	36	2015-09-26T23:45:53	2015-11-15T19:26:20
chandra.okta1.com	A	192.168.5.210	6	2015-09-22T18:58:59	2015-09-22T19:07:45
device1469990-5abd317d-local.wd2go.com	A	192.168.5.210	2	2015-12-02T13:11:05	2015-12-09T12:15:13
device2699310-91f74ecc-local.wd2go.com	A	192.168.5.210	4	2015-11-08T23:54:35	2016-01-02T03:31:02

Matching Tags

APT-Watch



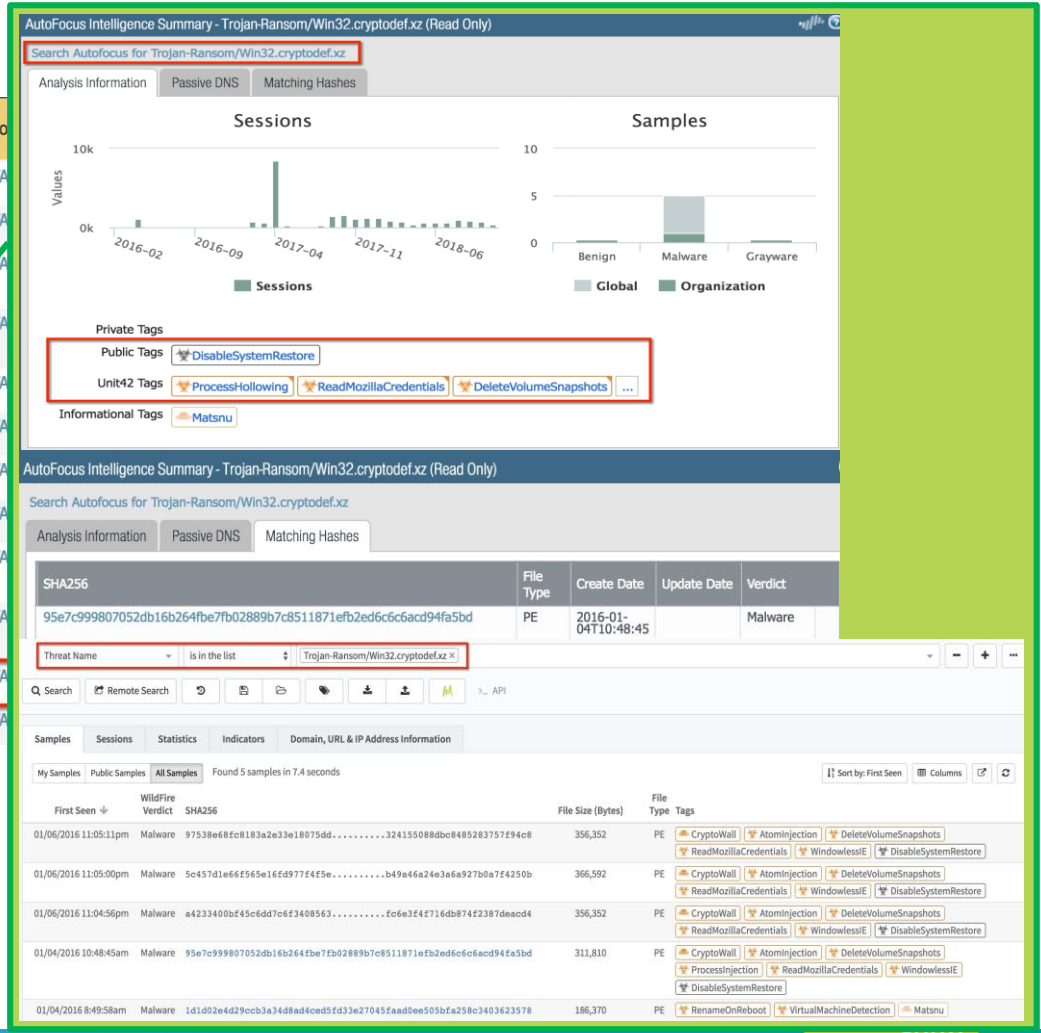


Recent WildFire Results

SHA256	File Type	Create Date	Update Date	Verdict
f33bd466dd97f846308eb78551063a561f647763d8370f8e359dc25f6ab3b71e	PE	2015-04-24T20:32:51		Malware
604cf2481e9f3c4423ee836941cbffb2f914cc6ce42ce980e391eea3d98fa48e	JAVA JAR	2014-11-23T02:46:04		Benign

Close

		Receive Time	Type	Name	Generate Time	Count	From Zone	To Zo
		11/20 07:27:34	spyware	WireLurker.Gen Command and Control Traffic	11/20 07:27:34	1	L3-TAP	L3-TA
		11/20 07:27:33	spyware	Suspicious HTTP Evasion Found	11/20 07:27:33	1	L3-TAP	L3-TA
		11/20 07:05:36	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 07:05:36	1	L3-TAP	L3-TA
		11/20 07:01:40	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 07:01:40	1	L3-TAP	L3-TA
		11/20 07:01:17	spyware	Suspicious HTTP Evasion Found	11/20 07:01:17	1	L3-TAP	L3-TA
		11/20 07:01:16	spyware	WireLurker.Gen Command and Control Traffic	11/20 07:01:16	1	L3-TAP	L3-TA
		11/20 07:01:16	spyware	Suspicious HTTP Evasion Found	11/20 07:01:16	1	L3-TAP	L3-TA
		11/20 06:34:58	spyware	WireLurker.Gen Command and Control Traffic	11/20 06:34:58	1	L3-TAP	L3-TA
		11/20 06:14:30	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 06:14:30	1	L3-TAP	L3-TA
		11/20 06:09:04	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 06:09:04	1	L3-TAP	L3-TA
		11/20 06:08:41	spyware	WireLurker.Gen Command and Control Traffic	11/20 06:08:41	1	L3-TAP	L3-TA
		11/20 06:08:40	spyware	Suspicious HTTP Evasion Found	11/20 06:08:40	1	L3-TAP	L3-TA



從攻擊事件名稱中,看到是哪種具有破壞程度的攻擊,這時如果可以通報,以API的方式回饋到不同平行單位或是下轄不同設備中,進行聯防的機制

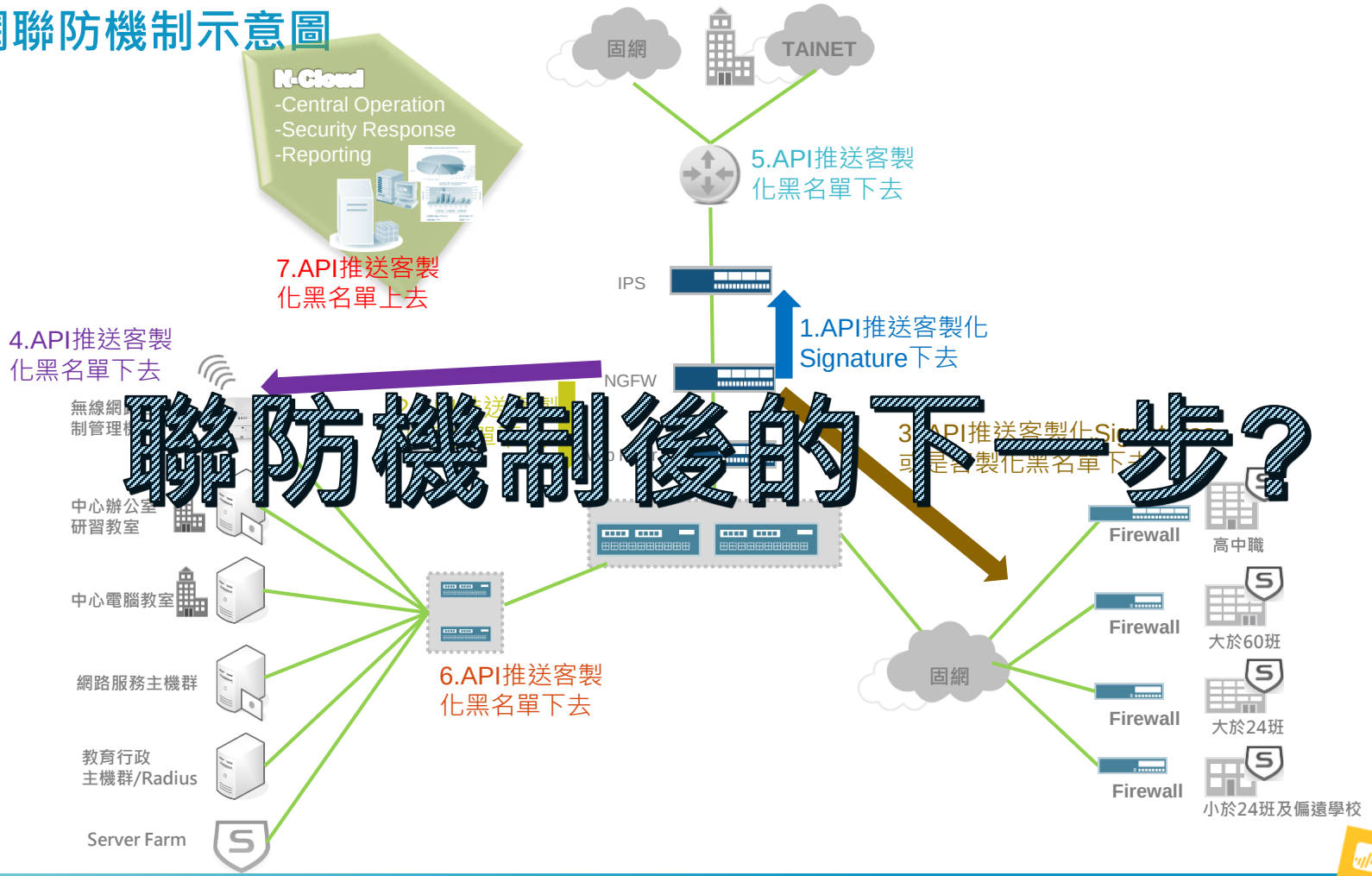
記錄到的封包,可以回饋給其他設備做聯防使用

		Receive Time	Type	Name	Generate Time	Count	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity	File Name	URL
		11/20 07:27:34	spyware	WireLurker.Gen Command and Control Traffic	11/20 07:27:34	1	L3-TAP	L3-TAP	[redacted]		80	web-browsing	alert	critical	www.comeinb...	
		11/20 07:27:33	spyware	Suspicious HTTP Evasion Found	11/20 07:27:33	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		www.comeinb...
		11/20 07:05:36	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 07:05:36	1	L3-TAP	L3-TAP			16464	unknown-udp	drop	critical		
		11/20 07:01:40	spyware	ZeroAccess.Gen Command and Control Traffic	11/20 07:01:40	1	L3-TAP	L3-TAP			16464	unknown-udp	drop	critical		
		11/20 07:01:17	spyware	Suspicious HTTP Evasion Found	11/20 07:01:17	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		networksecurit...
		11/20 07:01:16	spyware	WireLurker.Gen Command and Control Traffic	11/20 07:01:16	1	L3-TAP	L3-TAP			80	web-browsing	alert	critical	www.comeinb...	
		11/20 07:01:16	spyware	Suspicious HTTP Evasion Found	11/20 07:01:16	1	L3-TAP	L3-TAP			80	web-browsing	alert	informational		www.comeinb...
		11/20 06:34:58	spyware	WireLurker.Gen Command and Control Traffic								web-browsing	alert	critical	www.comeinb...	
		11/20 06:14:30	spyware	ZeroAccess.Gen Command and Control Traffic								unknown-udp	drop	critical		
		11/20 06:09:04	spyware	ZeroAccess.Gen Command and Control Traffic								unknown-udp	drop	critical		
		11/20 06:08:41	spyware	WireLurker.Gen Command and Control Traffic								web-browsing	alert	critical	www.comeinb...	
		11/20 06:08:40	spyware	Suspicious HTTP Evasion Found								web-browsing	alert	informational		www.comeinb...

Packet Capture

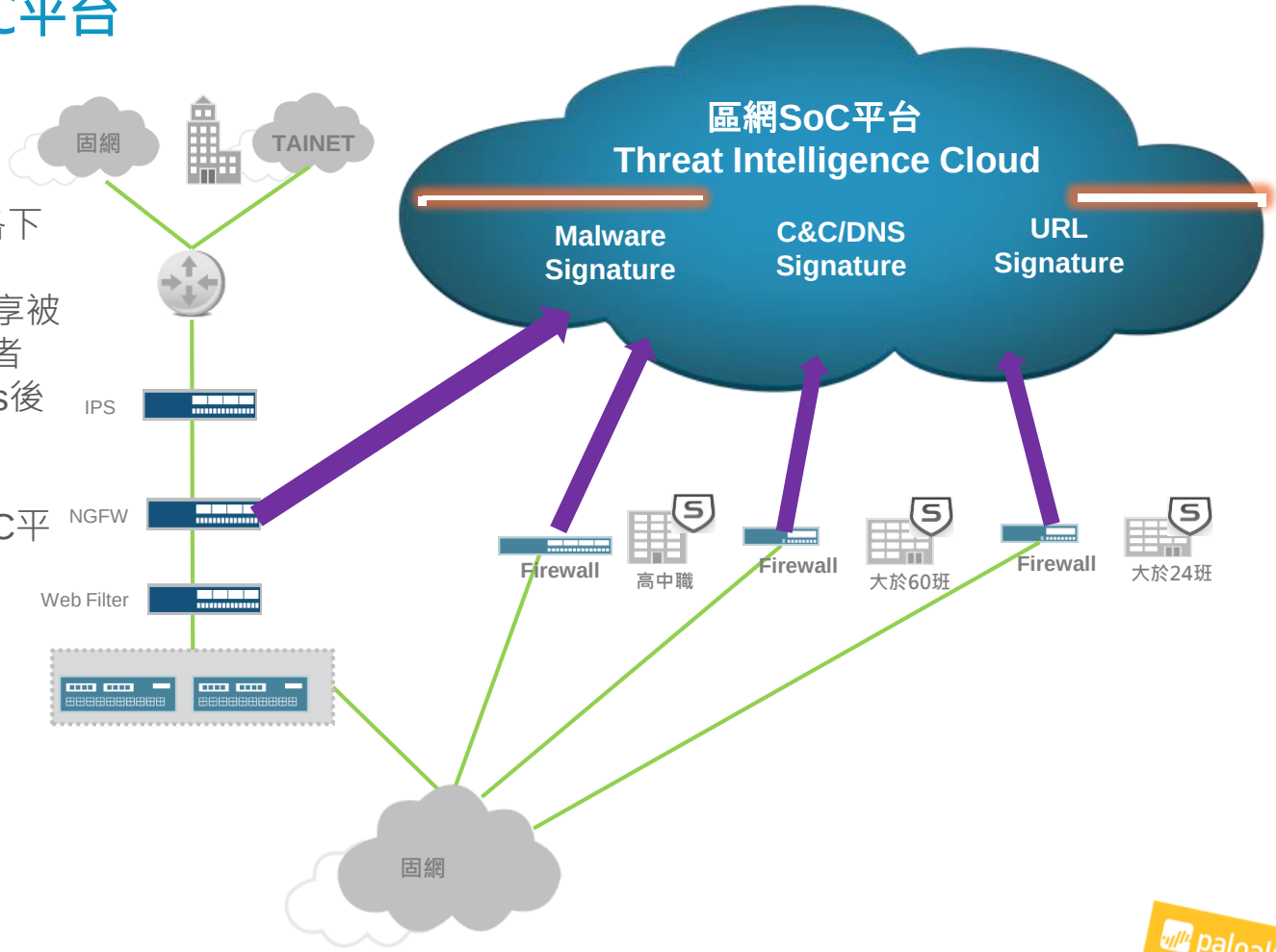
```
06:08:41.000000 0a:35:ea:12:ac:57 > 0a:11:c1:a6:fe:b4, ethertype IPv4 (0x0800),
        0x0000:  0a11 c1a6 feb4 0a35 ea12 ac57 0800 4500  .......5...W..E.
        0x0010:  0183 885b 4000 8006 4e3d 0a9a 0a3a 0a01  ...[@...N=...:..
        0x0020:  0408 787b 0050 4cd3 168b 61be c0e7 5018  ..x{.PL...a...P.
        0x0030:  ffff ae9e 0000 4745 5420 2f6d 6163 2f67  ......GET./mac/g
        0x0040:  6574 736f 6674 2e70 6870 2048 5454 502f  etsoft.php.HTTP/
        0x0050:  312e 310d 0a48 6f73 743a 2077 7777 2e63  1.1..Host:.www.c
        0x0060:  6f6d 6569 6e62 6162 792e 636f 6d0d 0a55  omeinbaby.com..U
        0x0070:  7365 722d 4167 656e 743a 2067 6c6f 6261  ser-Agent:.globa
        0x0080:  6c75 7064 6174 6520 2875 6e6b 6e6f 776e  lupdate.(unknown
        0x0090:  2076 6572 7369 6f6e 2920 4346 4e65 7477  .version).CFNetw
        0x00a0:  6f72 6b2f 3539 362e 3520 4461 7277 696e  ork/596.5.Darwin
        0x00b0:  2f31 322e 352e 3020 2878 3836 5f36 3429  /12.5.0.(x86_64)
        0x00c0:  2028 4d61 6342 6f6f 6b50 726f 3130 2532  .(MacBookPro10%2
        0x00d0:  4331 290d 0a41 6363 6570 742d 4c61 6e67  C1)..Accept-Lang
        0x00e0:  7561 6765 3a20 656e 2c20 6a61 2c20 6672  uage:.en,.ja,.fr
        0x00f0:  2c20 6465 2c20 6573 2c20 6974 2c20 7074  ,.de,.es,.it,.pt
        0x0100:  2c20 7074 2d50 542c 206e 6c2c 2073 762c  ,.pt-PT,.nl,.sv,
        0x0110:  206e 622c 2064 612c 2066 692c 2072 752c  .nb,.da,.fi,.ru,
        0x0120:  2070 6c2c 207a 682d 4861 6e73 2c20 7a68  .pl,.zh-Hans,.zh
        0x0130:  2d48 616e 742c 206b 6f2c 2061 722c 2063  -Hant,.ko,.ar,.c
        0x0140:  732c 2068 752c 2074 722c 2074 682c 2063  s,.hu,.tr,.th,.c
        0x0150:  612c 2068 722c 2065 6c2c 2068 652c 2072  a,.hr,.el,.he,.r
        0x0160:  6f2c 2073 6b2c 2075 6b2c 2065 6e2d 7573  o,.sk,.uk,.en-us
        0x0170:  0d0a 436f 6e6e 6563 7469 6f6e 3a20 6b65  ..Connection:.ke
        0x0180:  6570 2d61 6c69 7665 0d0a 3064 2030 610d  ep-alive..0d.0a.
        0x0190:  0a                                       .
```

區網聯防機制示意圖


N-Cloud
-Central Operation
-Security Response
-Reporting
固網
TAINET
5.API推送客製化黑名單下去
7.API推送客製化黑名單上去
IPS
1.API推送客製化Signature下去
4.API推送客製化黑名單下去
NGFW
聯防機制後的下一步?
中心辦公室
研習教室
中心電腦教室
網路服務主機群
教育行政
主機群/Radius
Server Farm
6.API推送客製化黑名單下去
固網
Firewall
Firewall
Firewall
Firewall
高中職
大於60班
大於24班
小於24班及偏遠學校

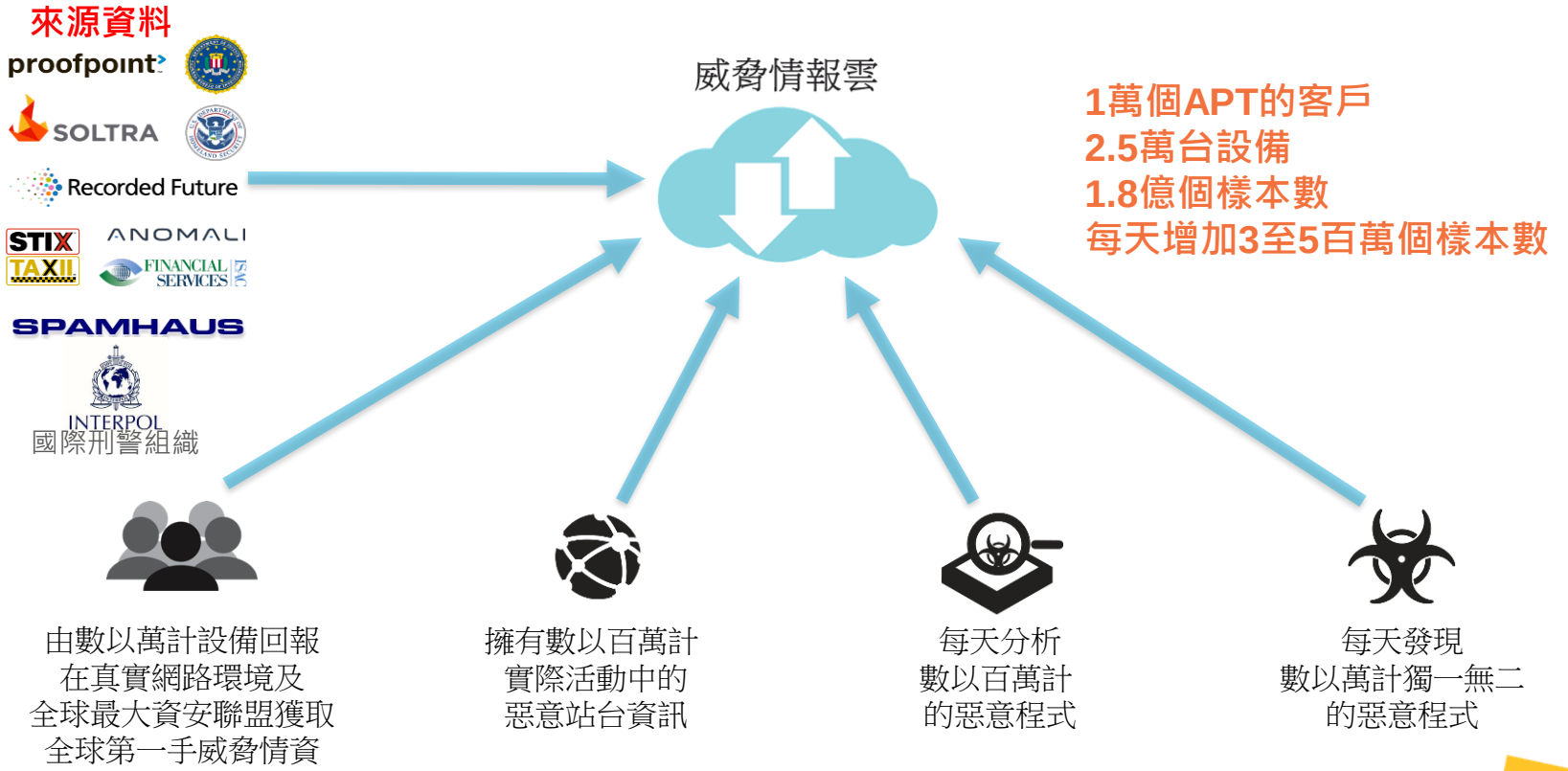
打造區網的小型SoC平台

1.區網管理者可以看到目前各下轄學校的威脅資安事件
2. 在區網SoC平台上,可以共享被攻擊的資源,發告警通知管理者
3. 可以自動化生成Signatures後自動佈署到其他管轄學校
4. 自動達到預警事件的通知
5. 可以集結各區網的小型SoC平台,讓各教育單位共享資源

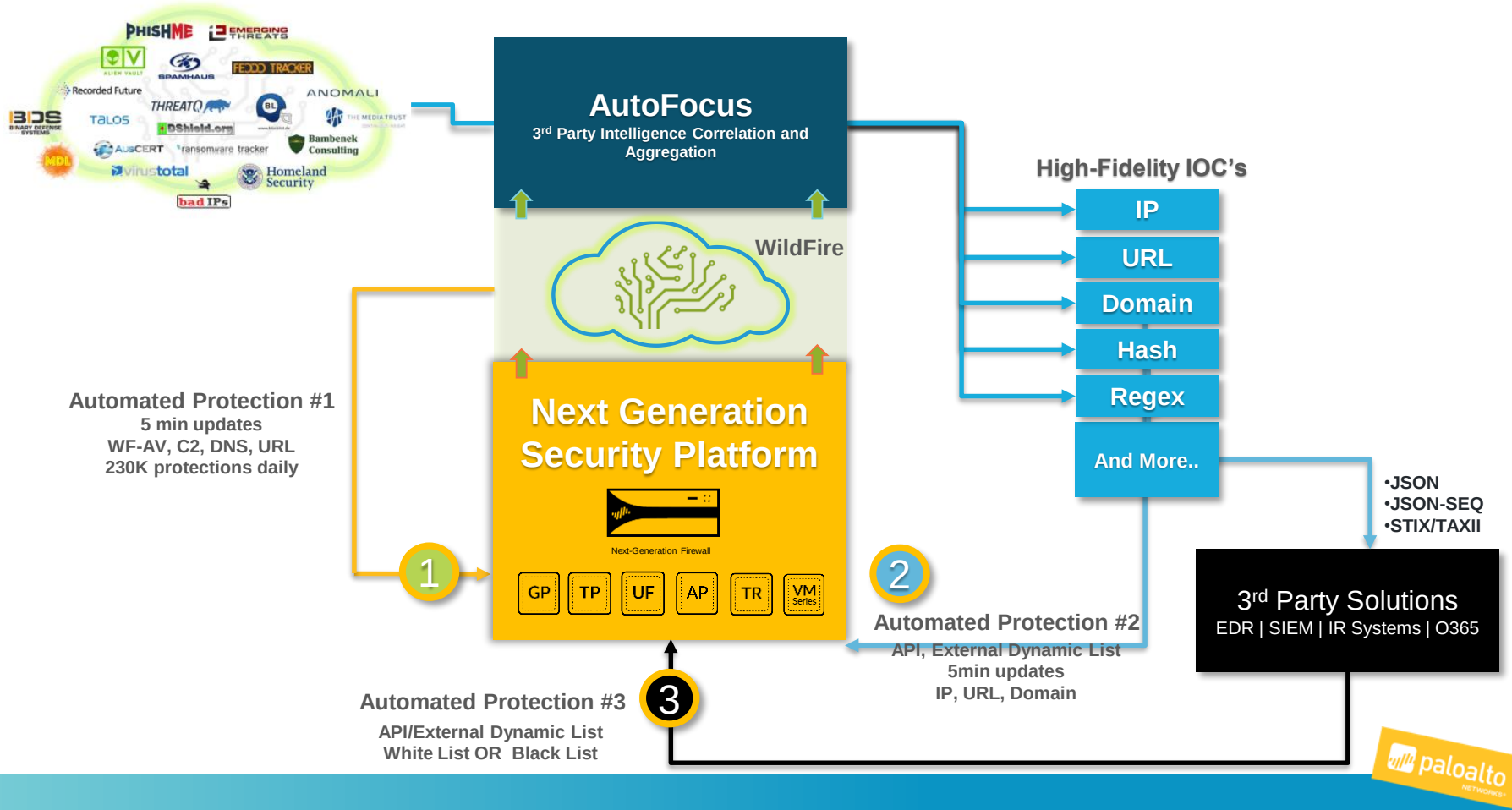


打造北、中、南各區網的威脅情資雲

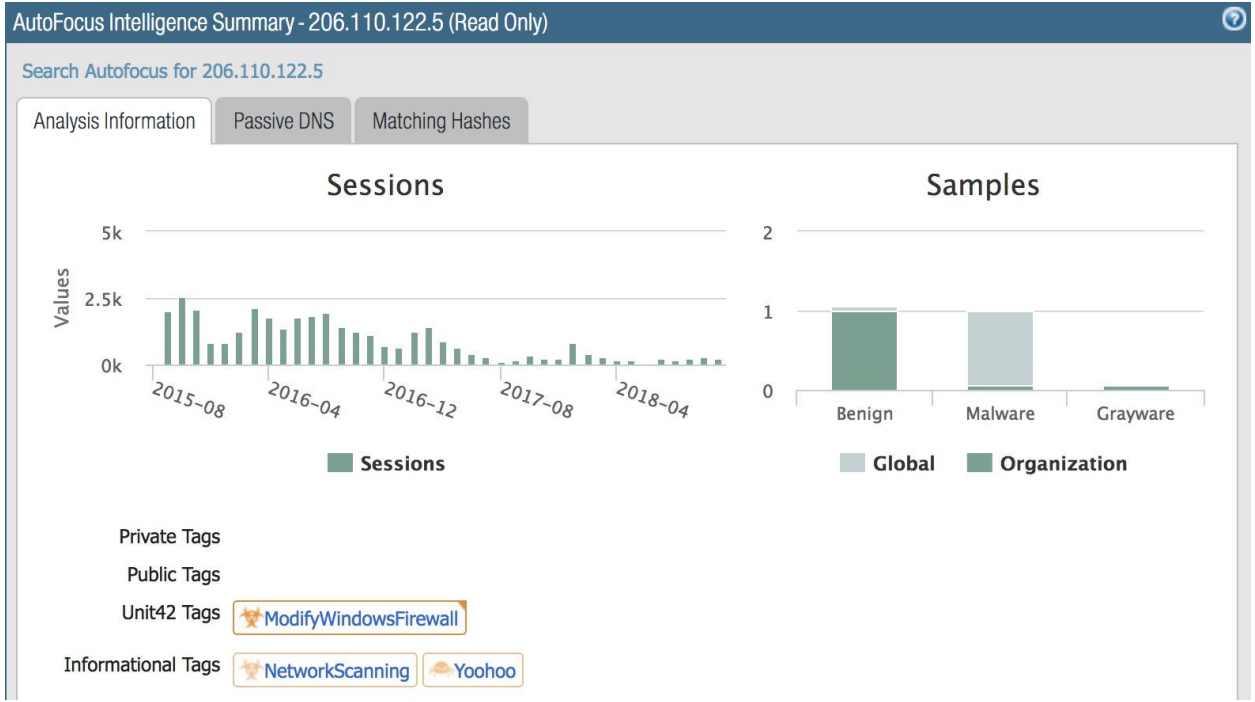
全球樣本數最多且已被分析的威脅情資



自動化的分析與提供每五分鐘更新防禦



XX中心疑似假冒公務之名做社交工程攻擊
冒名寄件者xx@ test.edu.tw



AutoFocus Intelligence Summary - 206.110.122.5 (Read Only)

Search Autofocus for 206.110.122.5

Analysis Information | Passive DNS | Matching Hashes

Request	Type	Response	Count	First Seen	Last Seen
exchange.emeryusd.k12.ca.us	A	206.110.122.5	13779	2014-01-09T18:41:58	2018-07-18T20:00:24
mail.emeryusd.k12.ca.us	A	206.110.122.5	13259	2013-12-21T00:13:16	2018-07-18T16:03:28
mail.emeryusd.org	A	206.110.122.5	13425	2014-01-12T19:14:02	2018-09-08T14:23:00

AutoFocus Intelligence Summary - 206.110.122.5 (Read Only)

Search Autofocus for 206.110.122.5

Analysis Information | Passive DNS | Matching Hashes

SHA256	File Type	Create Date	Update Date	Verdict
ed605512437865342c7b735d32c08667c90dc53cd417940effbb3eb9f6c83ca5	PDF	2014-02-04T17:26:26		Benign


paloalto
NETWORKS®