TANet的資安事件與因應對策

蔡一郎 研究員

NARLabs
National Applied Research Laboratories
National Center for
High-performance Computing
www.csirt.org.tw

Google Me.

- 蔡一郎 Steven
- 現任：財團法人國家實驗研究院 國家高速網路與計算中心 研究員
- 重要經歷：
  - 國立成功大學研究發展基金會 助理研究員
  - 台灣雲端安全聯盟 1st 2rd 理事長
  - 中華民國資料保護協會 1st監事
  - 中華民國南部科學園區產學協會 5th理事、6th監事
  - 台灣科技化服務協會 3rd理事
  - 台灣資訊安全聯合發展協會 1st 監事
  - **The Honeynet Project Taiwan Chapter Leader**
  - **Cloud Security Alliance Taiwan Chapter Founder**
  - **OWASP Taiwan Chapter Leader**
  - 部落客：http://blog.yilang.org
  - Facebook: Yi-Lang Tsai
  - 自由作家
    - 電腦圖書著作35本
    - Information Security(資安人)、Linux Guide、NetAdmin、網路資訊等文章，計80餘篇
- 專業證照：
  - RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC、BS10012 LAC、CSA STAR Auditing

大綱

- 資安威脅與趨勢
- 非傳統經濟的崛起
- DNS攻擊案例
- DDoS攻擊手法分析
- 全方位的防禦技術與因應對策
- 結論

資安威脅與趨勢

目前的資訊世界

- 演算法決定所能夠取得資訊
- 搜尋引擎決定資訊的優先順序
- 資訊的價值因人而異

攻擊的手法不斷翻新

- 「網紅」與「直播」
- 刻意設計的問題影片
- 吸引瀏覽者的連結

- 結果
  - 進入釣魚網站
  - 遠端植入惡意程式

網路成為資訊傳播的主要管道

- 社群網路成為人類社交的主要管道
- 網路的連結提供需求雙方資訊的交換
- 終端裝置的多樣化，提供即時的資訊
- 人是物聯網主要的使用者，並與行動裝置緊密結合
- 數位化的智慧城市時代

資安人的Exploit-DB

- 收集多種被發佈的弱點以及攻擊用的”測試”程式
- 可配合Metasploit相關工具軟體進行測試
  - 例如：Kali Linux

https://www.exploit-db.com/

Google Hacking DB

NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT

Date	Title	Category
2017-11-30	intext:"/wp-content/uploads/wpsc/"	Sensitive Directories
2017-11-29	inurl:"/address/speeddial.html?start" and intext:"Please configure the password" and intitle:"Brother"	Various Online Devices
2017-11-29	inurl:"nfs://www." "index of /"	Sensitive Directories
2017-11-28	intitle:index.of .bashrc	Sensitive Directories
2017-11-28	inurl:"ews/setting/setews.htm"	Various Online Devices
2017-11-27	intext:"index of /userfiles/file/"	Sensitive Directories
2017-11-27	intext:"softperms.txt" ext:TXT	Files Containing Juicy Info
2017-11-27	inurl:composer.json filetype:json -site:github.com	Files Containing Juicy Info
2017-11-27	"Cake\Routing\Exception\" -site:github.com -site:stackoverflow.com -site:cakephp.org"	Error Messages
2017-11-24	"Use these fields to set or change the Administrator Password. When set, the Administrator Password is.....	Various Online Devices

https://www.exploit-db.com/google-hacking-database/

NIST-NVD

- National Vulnerability Database

	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	28	11	0	0
This Week	90	108	154	1
This Month	147	212	316	1
Last Month	1122	1100	2342	107
This Year	13746	13232	61432	766

CVE Status Count

Total	98021
Received	38
Awaiting Analysis	368
Undergoing Analysis	151
Modified	61417
Deferred	2
Rejected	4349

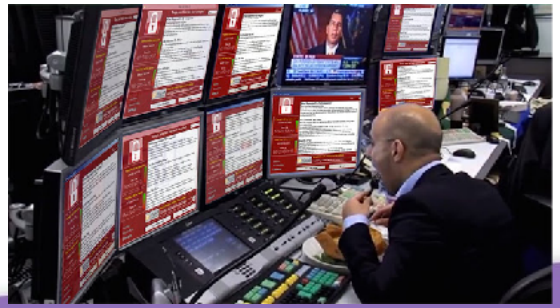
NVD Contains

CVE Vulnerabilities	98021
Checklists	485
US-CERT Alerts	249
US-CERT Vuln Notes	4468
OVAL Queries	10286
CPE Names	126016

https://nvd.nist.gov/general/nvd-dashboard

WannaCry大規模來襲

- 惡意程式加上勒索，針對系統重大弱點進行自動化攻擊與散佈



最近的新聞！

- 資安研究，有時候是一體的兩面
- 特殊的網域名稱 iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

sinkhole.tech – where the bots party hard and the researchers harder.

https://dq.yam.com/post.php?id=8002

擋下「想哭」病毒的英國資安專家 被控開發惡意軟體遭逮

2017-08-04 by：薇薇 10167

你還記得今年五月讓全球人心惶惶的電腦病毒「想哭」嗎？近日，被封為網路英雄、成功擋下「想哭」的英國資安專家遭控開發惡意勒索軟體，在美國遭到FBI的逮捕。

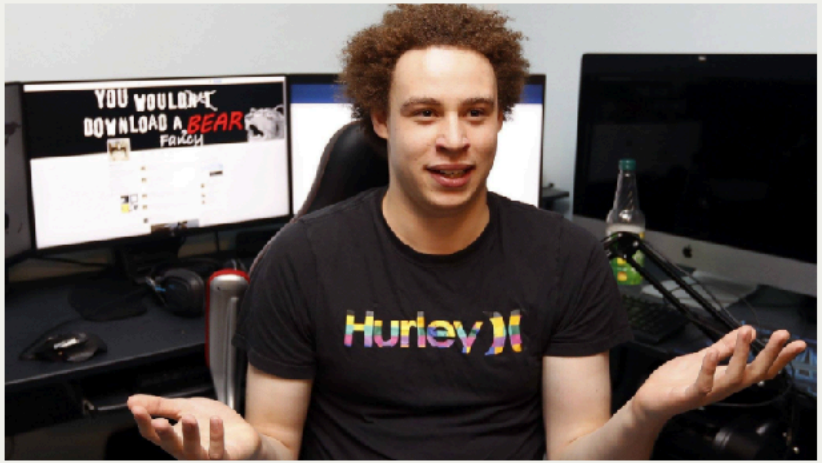


Photo: Press Today

圖為今年 23歲的英國資安專家哈欽斯，近日，他被控開發惡意軟體在美國拉斯維加斯機場遭到FBI逮捕。

擋下「想哭」聲名大噪

你還記得今年五月席捲全球 150個國家、造成超過 100萬台電腦中毒的惡意勒索軟體「想哭」(WannaCry)嗎？當時，英國 23歲的資安專家哈欽斯(Marcus Hutchins)找到了「殺手開關」，成功阻擋「想哭」的進一步蔓延而聲名大噪。

DNS記錄與WannaCry

NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT

>	17/07/05 23:14:17.000	Jul 05 15:14:17 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87026 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14323232?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.38.137 end=Jul 05 2017 23:13:47 CST externalId=14323232 proto=TCP sourceDnsDomain=78-user127.cc.ncut.edu.tw src=140.128.78.127 start=Jul 05 2017 23:13:47 CST host = 10.0.1.28 | source = udp:666 | sourcetype = syslog-for-lastline
>	17/07/05 21:26:42.000	Jul 05 13:26:42 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=86756 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312974?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:26:12 CST externalId=14312974 proto=TCP sourceDnsDomain=95-user169.lib.ncut.edu.tw src=140.128.95.169 start=Jul 05 2017 21:26:12 CST host = 10.0.1.28 | source = udp:666 | sourcetype = syslog-for-lastline
>	17/07/05 21:21:25.000	Jul 05 13:21:25 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87049 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312456?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:20:48 CST externalId=14312456 proto=TCP sourceDnsDomain=t2.ba.dep-appoint.static.012.ippool.cyut.edu.tw src=120.110.27.12 start=Jul 05 2017 21:20:48 CST host = 10.0.1.28 | source = udp:666 | sourcetype = syslog-for-lastline
>	17/07/05 21:21:13.000	Jul 05 13:21:13 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87049 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312456?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:20:48 CST externalId=14312456 proto=TCP sourceDnsDomain=t2.ba.dep-appoint.static.012.ippool.cyut.edu.tw src=120.110.27.12 start=Jul 05 2017 21:20:48 CST host = 10.0.1.28 | source = udp:666 | sourcetype = syslog-for-lastline

WannaCry統計

最高 10 個值	數量	%
163.17	467	5.285%
163.17	316	3.576%
163.17	289	3.271%
140.12 200	278	3.146%
140.12	268	3.033%
163.17	264	2.988%
163.17	241	2.727%
163.17	233	2.637%
163.17 5	224	2.535%
163.17	203	2.297%

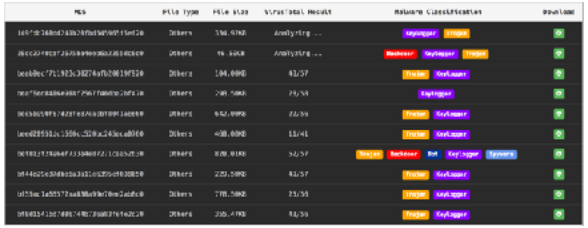
- 同網段快速蔓延，災情擴大
- 追蹤與掌握資安威脅的趨勢！

值	數量	%
May	5,105	57.775%
Jun	1,570	17.768%
Jul	1,430	16.184%
Aug	731	8.273%

惡意程式知識庫簡介

- 自2009年規劃反駭客偵測技術，並同步建置大尺度誘捕網路，2010年完成建置，「惡意程式知識庫」於2013年8月正式開放服務
- 惡意程式分析
  - 國內唯一開放服務之惡意程式知識庫
  - 收集超過1,500萬惡意程式樣本
  - 提供惡意程式樣本、分析報告、類型搜尋功能
  - 已開放下載的惡意程式樣本超過1,100萬隻(持續增加中)
- 建置誘捕平台偵測惡意攻擊
  - 6,000+誘捕系統
  - 搜集平均65GB/天巨量資料
- 全天候資安防禦
  - 7*24全天候資安維運中心(SOC)
  - 平均每月通報15,000筆資安事件
  - 擁有主動/被動偵測系統
  - 自主研發情資回饋機制，建立增強資安防禦

owl.nchc.org.tw



統計資料至2017年6月底

惡意程式知識庫-系統與服務架構

NARLabs National Applied Research Laboratories National Center for High-performance Computing

TWCSIRT

完成網站服務帳號申請，利用網站進行資料查詢與下載

利用授權金鑰(Key)或限制存取IP位址，提供遠端程式自動化查詢

網站註冊會員

開放 API

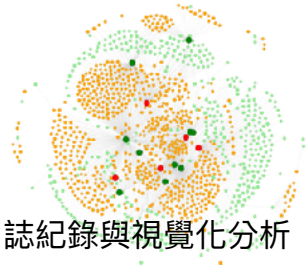
惡意程式知識庫 Malware Knowledge Base

惡意程式行為沙箱

日誌分析

檔案資料儲存於分散式資料庫

MongoDB 分散式資料庫



日誌紀錄與視覺化分析

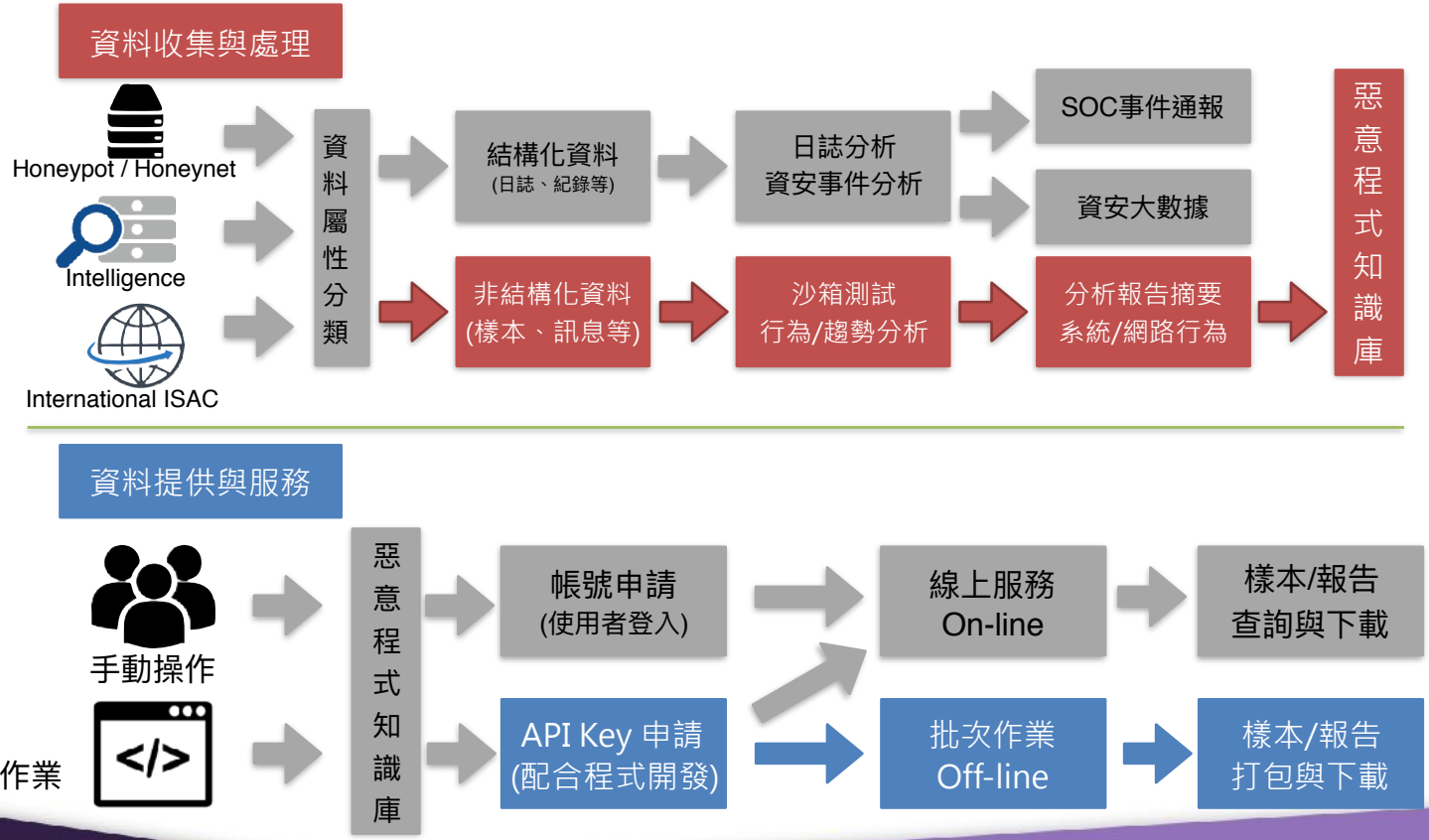
多層次資安研發平台

Honeypot / Honeynet

Intelligence

International ISAC

惡意程式知識庫-系統資料處理流程



惡意程式知識庫-Bot

NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT

MD5	File Type	File Size	VirusTotal Result	Malware Classification	Download
03851982806a7046345e344b9738e170	Others	40.27KB	32/56	Backdoor Bot Trojan	
3127af9862ad50304b4e3076568d7b10	Others	238.13KB	38/53	Backdoor Bot Trojan Worm	
be942500a467c2d9f8f2d8ea400f1970	Others	710.97KB	53/56	Backdoor Bot	
be9651c2602435c950bbae259428fb70	Others	809.42KB	53/57	Backdoor Bot	
be96c99a684dfa2c61d2b65ecbd07990	Others	852.77KB	55/58	Trojan Backdoor Bot	
be977993b7d29b2c0e4c220d45dadc40	Others	498.78KB	53/56	Backdoor Bot	
be9db2152b4f93d0d865c142007b62e0	Others	772.48KB	37/57	Adware Backdoor Bot Trojan	
be9dbef3b21f3b11c13ed3f9195a8570	Others	744.00KB	52/56	Trojan Backdoor Bot	
be9e060c70addfb3eb5fe702381c6390	Others	712.50KB	30/57	Backdoor Bot	
bea3a90e441ac6a873fa9c39a2407ab0	Others	891.08KB	52/56	Trojan Backdoor Bot	

惡意程式知識庫-Backdoor

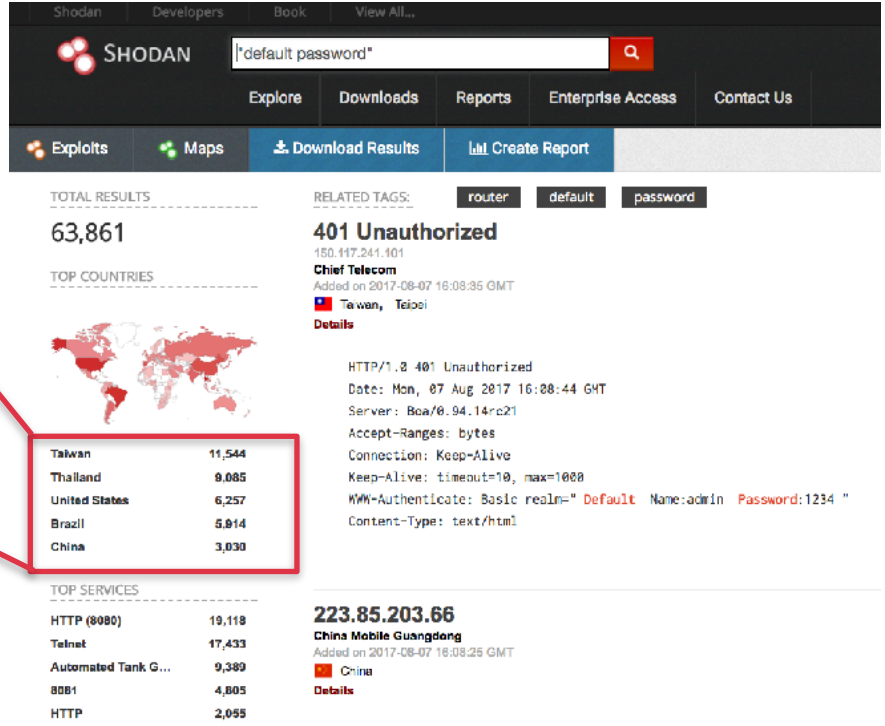
NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT

MD5	File Type	File Size	VirusTotal Result	Malware Classification	Download
0000b9d2f15bd4ea6f632a8122130e30	Others	2.43KB	46/55	Backdoor Exploit/Root Kit Trojan Worm	
010e138c1e508ccf704b1f58b96185c0	Others	1.68KB	47/56	Backdoor Exploit/Root Kit Trojan Worm	
0111754c6f6eb1d883153e132e22ca20	Others	428.48KB	9/53	Backdoor Trojan	
01126600c2c6083a37e48500d14da2f0	Others	13.92KB	43/57	Backdoor Exploit/Root Kit Trojan Worm	
011478aeeb82cb6014a30dc18b7c6220	Others	27.27KB	40/57	Backdoor Exploit/Root Kit Trojan	
011866f75079eb0ddfeb3027ab3601e0	Others	15.21KB	41/56	Backdoor Exploit/Root Kit Trojan Worm	
0128ab0d36ffa3f387d31f987b741ed0	Others	22.71KB	41/57	Backdoor Exploit/Root Kit Trojan Worm	
0140e260b902acb433eeadb0b5e05fa0	Others	5.41KB	13/57	Backdoor Trojan	
016db3974761ce35f76696596fd51620	Others	40.83KB	22/52	Backdoor Trojan	
0174eadcb9d00208fc5b83a3b5d939c0	Others	2.00KB	47/57	Backdoor Exploit/Root Kit Trojan Worm	

shodan.io-Default Password

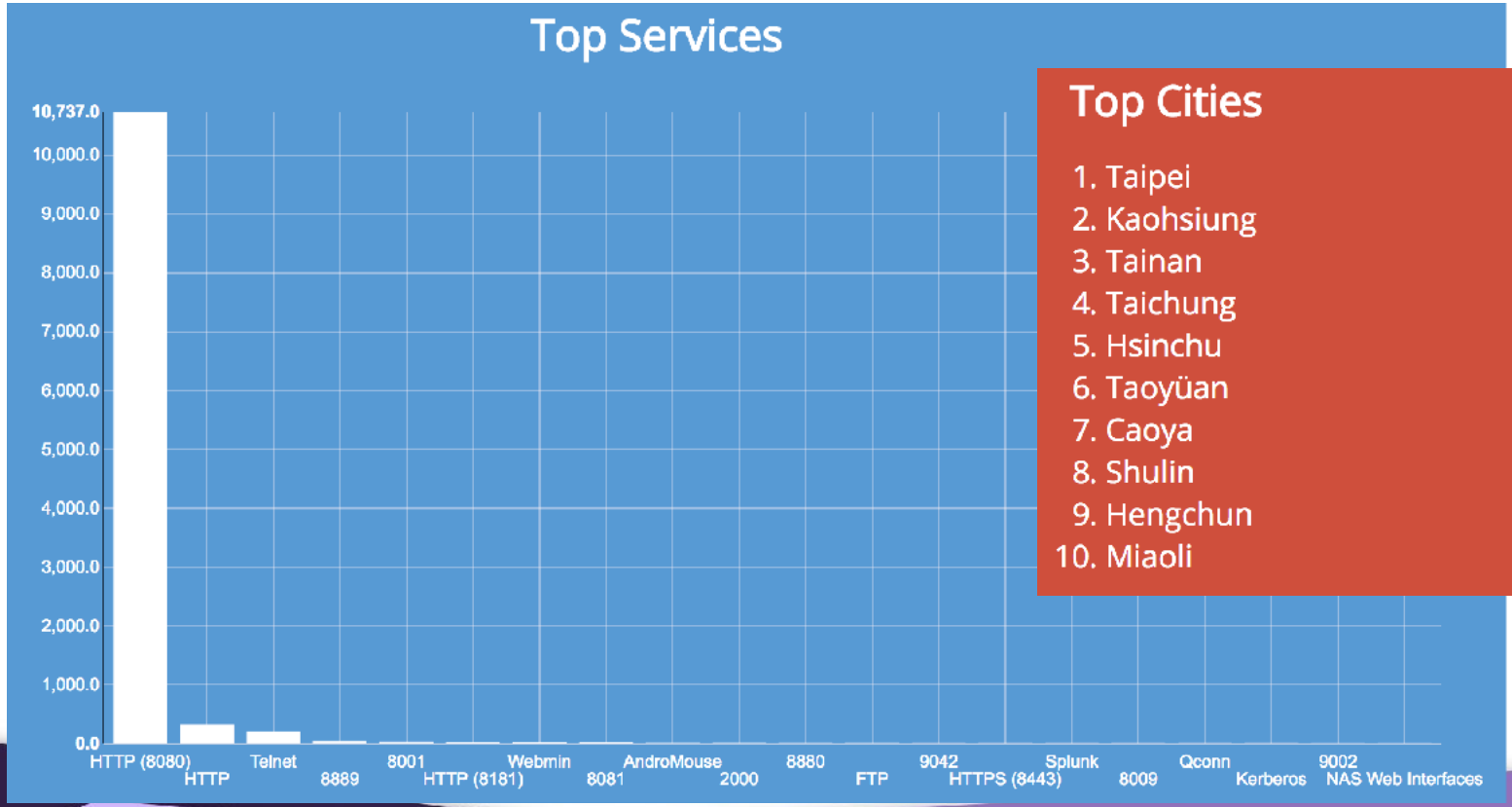
Taiwan	11,544
Thailand	9,085
United States	6,257
Brazil	5,914
China	3,030

Taiwan No.1



shodan.io-Default Password

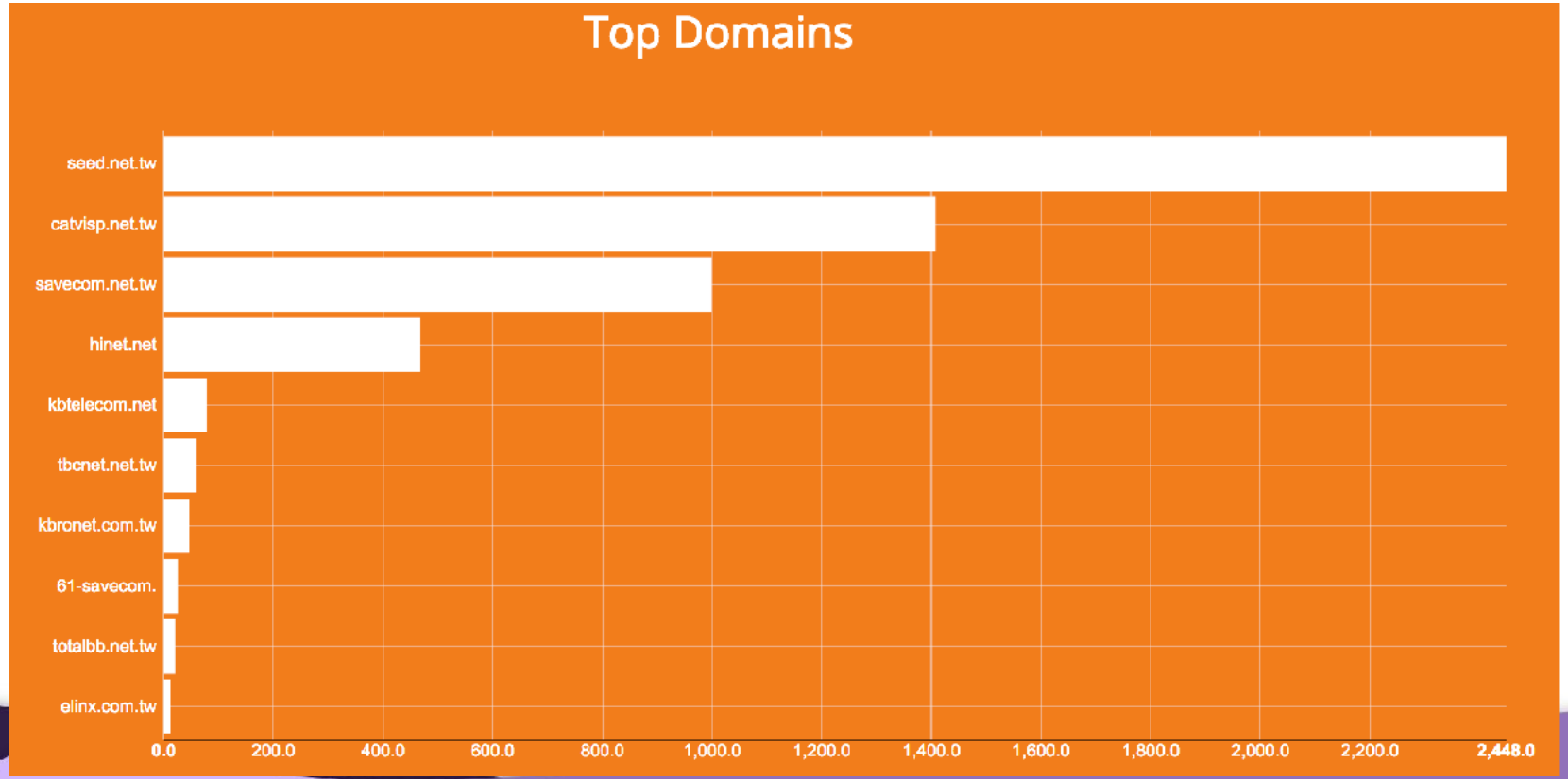
NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT



Top Cities

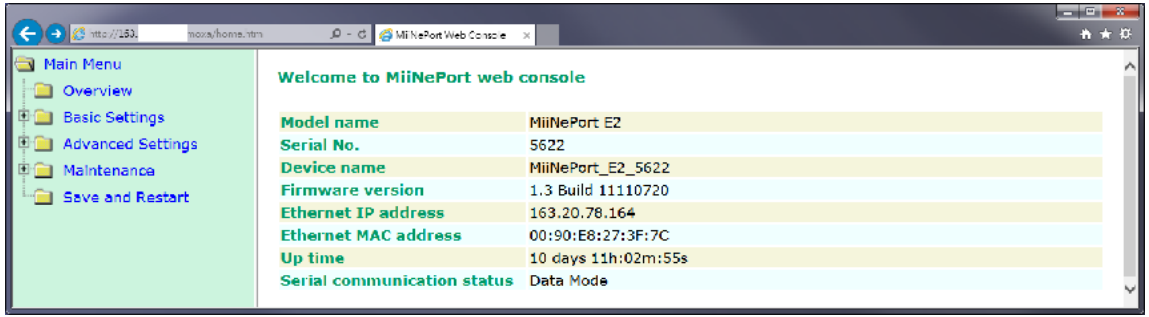
1.	Taipei	10,428
2.	Kaohsiung	422
3.	Tainan	131
4.	Taichung	44
5.	Hsinchu	20
6.	Taoyüan	7
7.	Caoya	6
8.	Shulin	3
9.	Hengchun	3
10.	Miaoli	2

shodan.io-Default Password



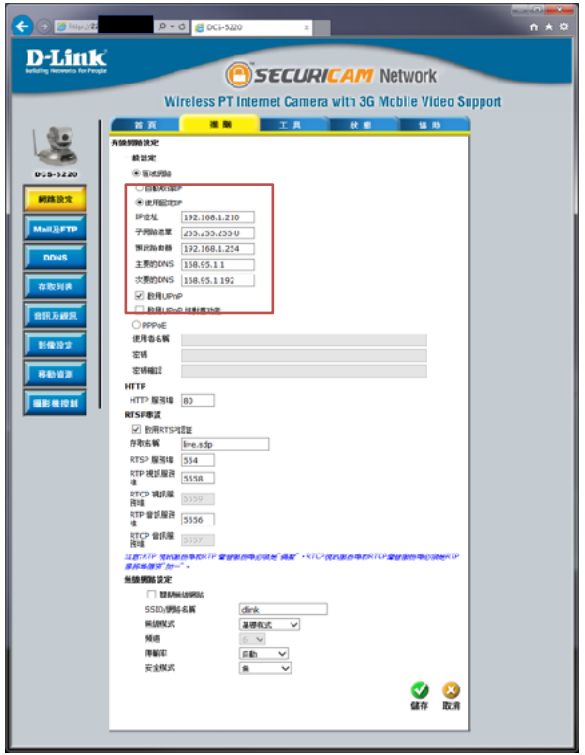
網路已成為主要的通訊趨勢

- ICT / SCADA
- Serial to Ethernet
- Printer Server

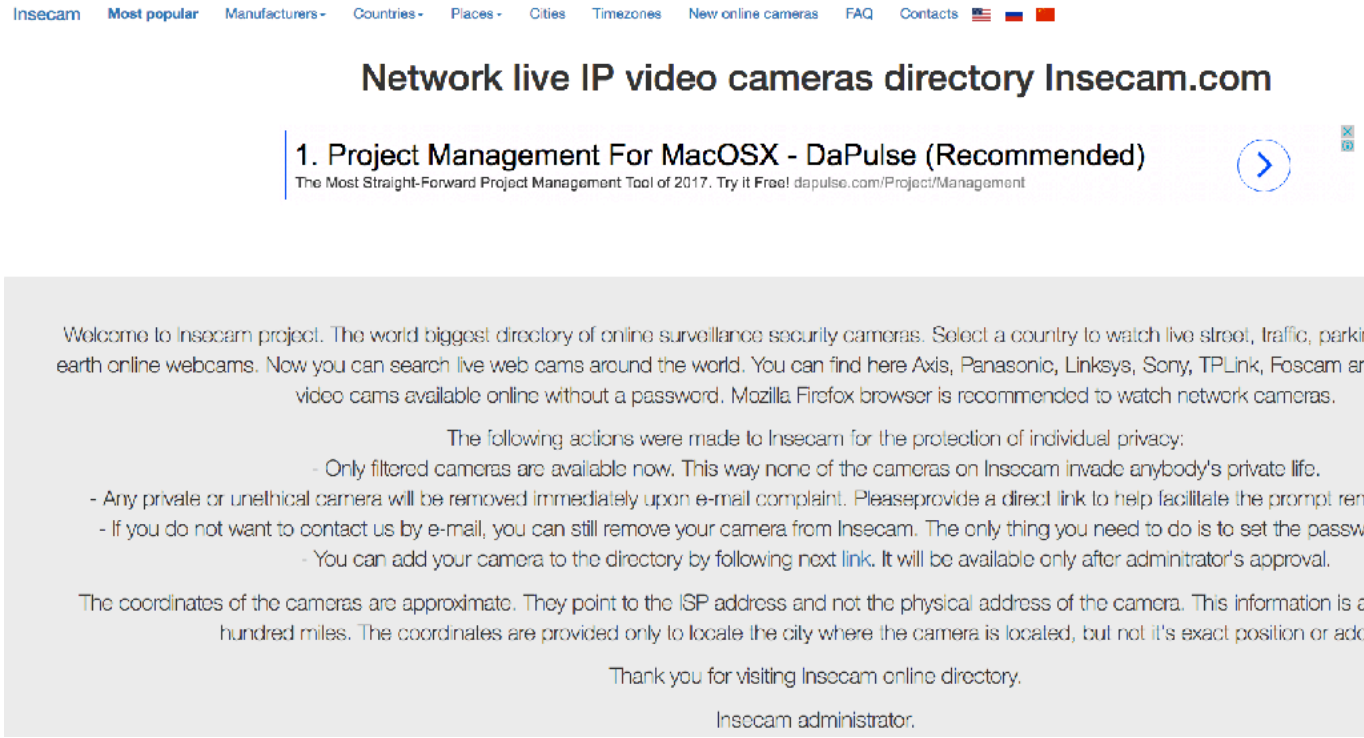


開放的資訊？


D-Link
SECURICAM Network
Wireless PT Internet Camera with 3G Mobile Video Support
DCS-5220

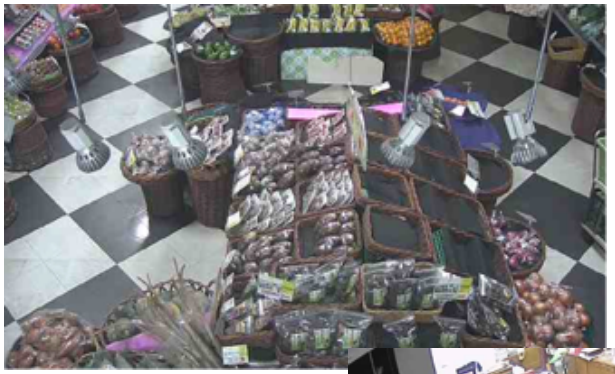

D-Link
SECURICAM Network
Wireless PT Internet Camera with 3G Mobile Video Support

攝影機直播網站



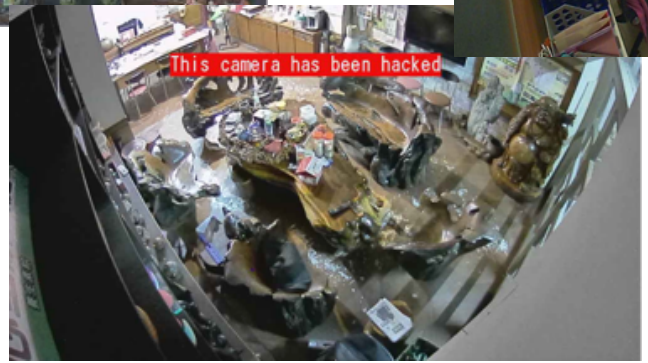
http://www.insecam.org/

無設防的網路攝影機



超級市場

醫療診所



工藝品店

資料來源 http://insecam.org/

非傳統經濟的崛起

暗網中的駭客交易

IOT Botnet Setup for DDOS (Working)

Vendor	[redacted] (4.60⭐) (ⓐ 1/0/2)
Price	฿0.072 (€200)
Ships to	Worldwide, Worldwide
Ships from	WW
Escrow	Yes

Product description

I will setup IOT botnet for you:
yes this is a working IOT botnet edited by me.

You will need :
2 or more VPS servers min 1GB ram

What i will do :
I will setup the Command server and install scanners on VPS for you.
This listing comes with bots connected

Do not ask me stupid shit this service is for DDOS only.

DDOS ATTACK - Website takedown - 1 week

Vendor	[redacted] ⭐) (ⓐ 344/9/31) (13/1/1)
Price	฿0.0912 ($300)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	No

Product description

DDOS ANY WEBSITE FOR ONE WEEK . 100% Fucking Awesome

WE CRACK FACEBOOK AND GMAIL PASSWORDS UPTO 15 CHARACTERS LONG INCLUDING SPECIAL AND NUMBERS IN 48 hours !!

boom

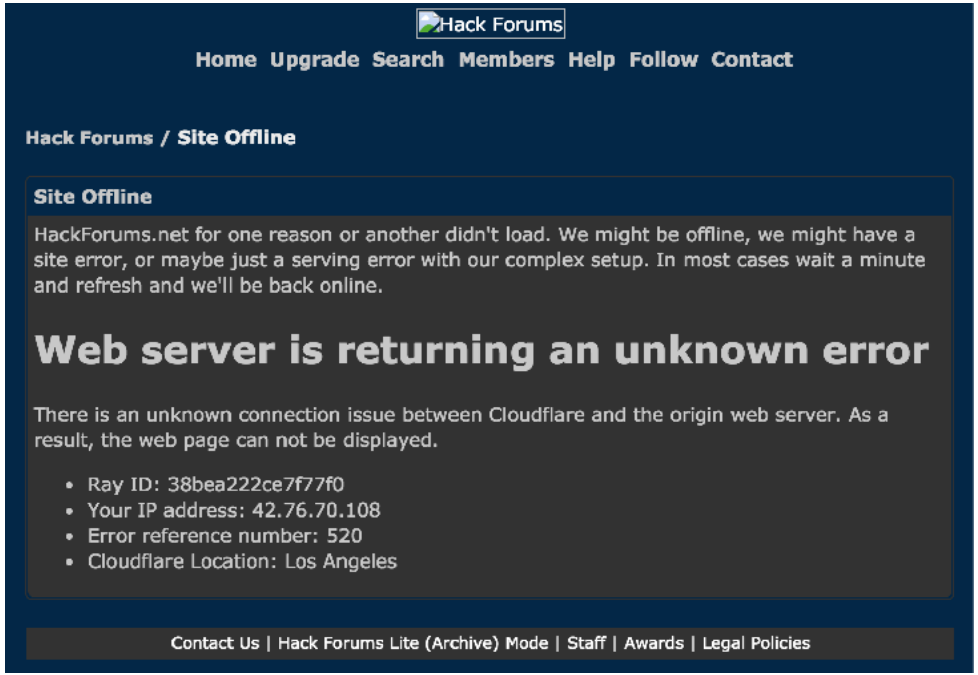
I use various hacking techniques based on the job requiwhite ,First stage is mostly a phising attack - these attack are simple and leads to success more times than you would think.
Second stage of the attack is normally a brute force crack with my botnet. I can crack facebook,gmail and other email passwords upto 15 characters long including special and numbers in less that 4 days.
Most of this work is done with a custom written version of hydra. For Servers and PC's an IP address or hostname is needed.For phones any info you have will do,number is important/email
DDOS attack start with basic stuff, buffer overflows & resource consuming techniques.Followed by upto a 5GBPS second attack from our BOTNET.We been in this is blackhat game along time , we know our shit , Dont let the fact we made our webiste in notepad fool you.
We do amazing phone hacking.Our team has some serious skills. We need details , phone model , number , network provider , Do you have physical access to the handset ? Does the phone connect to your wifi ? any other information you have , no information is irreleverent.
XMPP : plaxis@jabb3r.org

不可不知的TOR

- Tor（The Onion Router，洋蔥路由器）是實現匿名通訊的自由軟體。
- Tor是第二代洋蔥路由的一種實現，用戶通過Tor可以在網際網路上進行匿名交流。
- 最初該專案由美國海軍研究實驗室贊助。2004年後期，Tor成為電子前哨基金會（EFF）的一個專案。

https://www.torproject.org/

兩個世界


Hack Forums
Home Upgrade Search Members Help Follow Contact
Hack Forums / Site Offline
Site Offline
HackForums.net for one reason or another didn't load. We might be offline, we might have a site error, or maybe just a serving error with our complex setup. In most cases wait a minute and refresh and we'll be back online.
Web server is returning an unknown error
There is an unknown connection issue between Cloudflare and the origin web server. As a result, the web page can not be displayed.
Ray ID: 38bea222ce7f77f0
Your IP address: 42.76.70.108
Error reference number: 520
Cloudflare Location: Los Angeles
Contact Us | Hack Forums Lite (Archive) Mode | Staff | Awards | Legal Policies


Welcome to HackForums.net
Current time: 08-09-2017, 03:55 PM
Packets, Posts, and Punks
HACK FORUMS
Home Upgrade Search Members Extras Wiki Help Follow Contact
Hello There, Guest! (Login — Register)
Hack Forums
$100 Gift Card for $40
Uber & Uber Eats
THE CRYPTO
Common Hack Tech Code Game Groups Web GFX Market Money
Hack Forums Official Information
Forum
Threads/Posts
Last Post
Rules, Announcements, News, and Feedback
This is where site rules and important announcements about the site are made. Please read carefully before you join. Also you can leave us feedback or ask site questions here.
Moderated By: Mentors
65,291
1,074,821
Closing my account.
Today 03:45 PM
by temp_Obli
Suggestions and
HF News

虛擬貨幣

- 虛擬貨幣成為地下市場的主流貨幣
- 以比特幣為例，今年成長了將近120倍

https://www.bitoex.com/charts?locale=zh-tw

比特幣接軌真實世界

- 比特幣是一種使用者自治且全球通用的加密電子貨幣
- 不受任何國家的央行控制
- 大部分的比特幣兌換都屬於私人交易，或是通過網路交易而獲得
- 在日本等國家已開放比特幣可在市場上使用
- 設立比特幣提款機

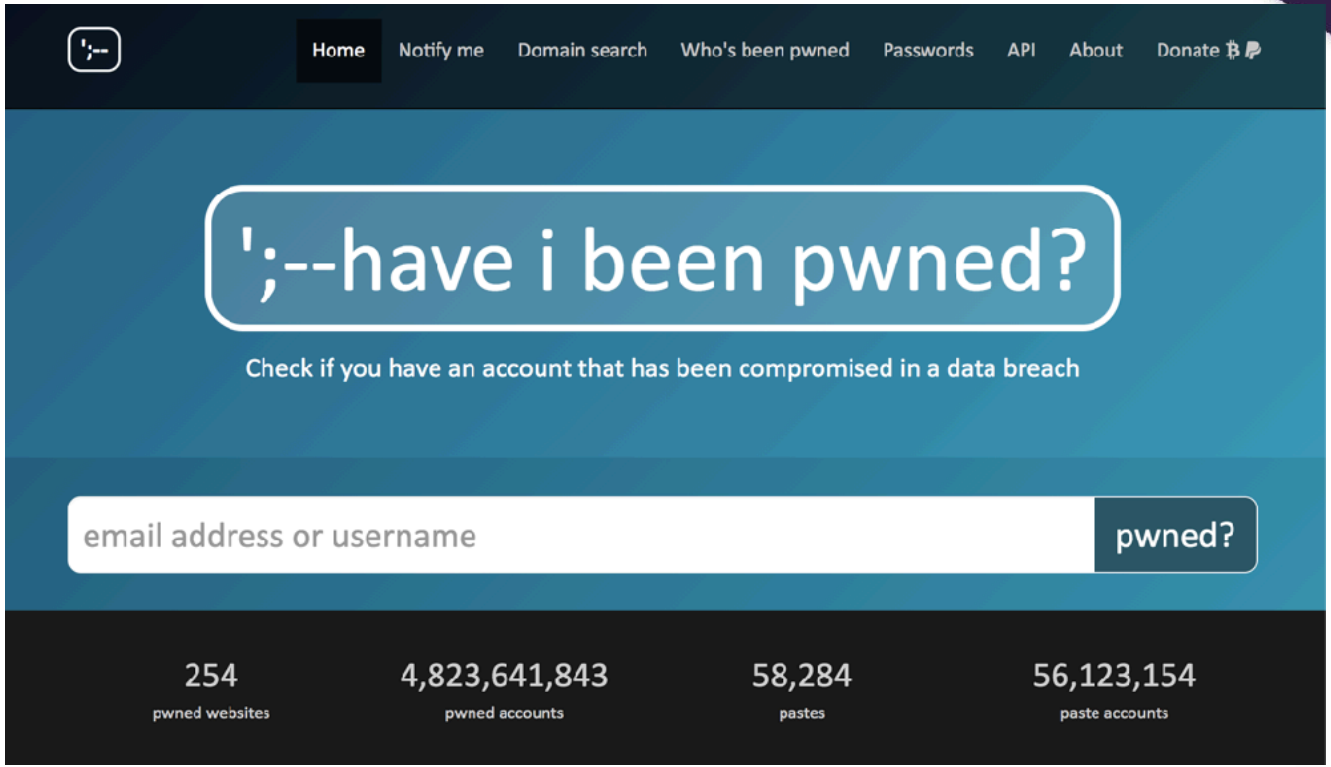
匿名便利貼

- 可以匿名張貼內容
- 成為另類駭客文化的集中地
- 販售個人隱私資料、信用卡、網站帳號等

https://pastebin.com/

Have I been pwned?

- pwn，是網路文化下的產物，一個駭客語法的俚語詞，自”own”這個字引申出來的
- 玩家在整個遊戲對戰中處在勝利的優勢，或是說明競爭對手處在完全慘敗的情形

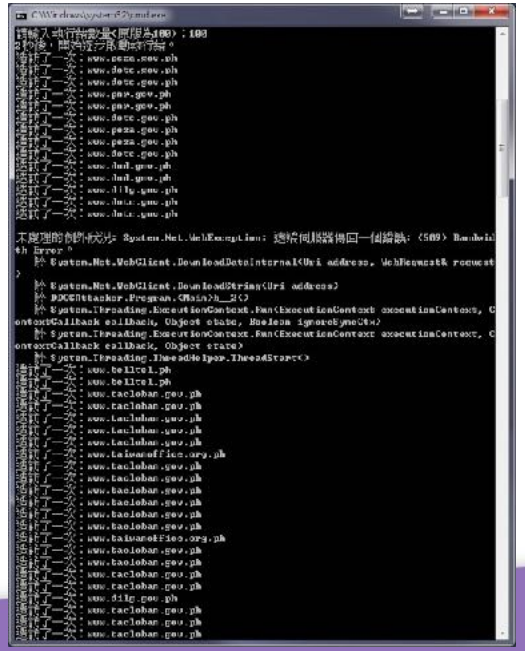


https://haveibeenpwned.com/

DNS攻擊案例

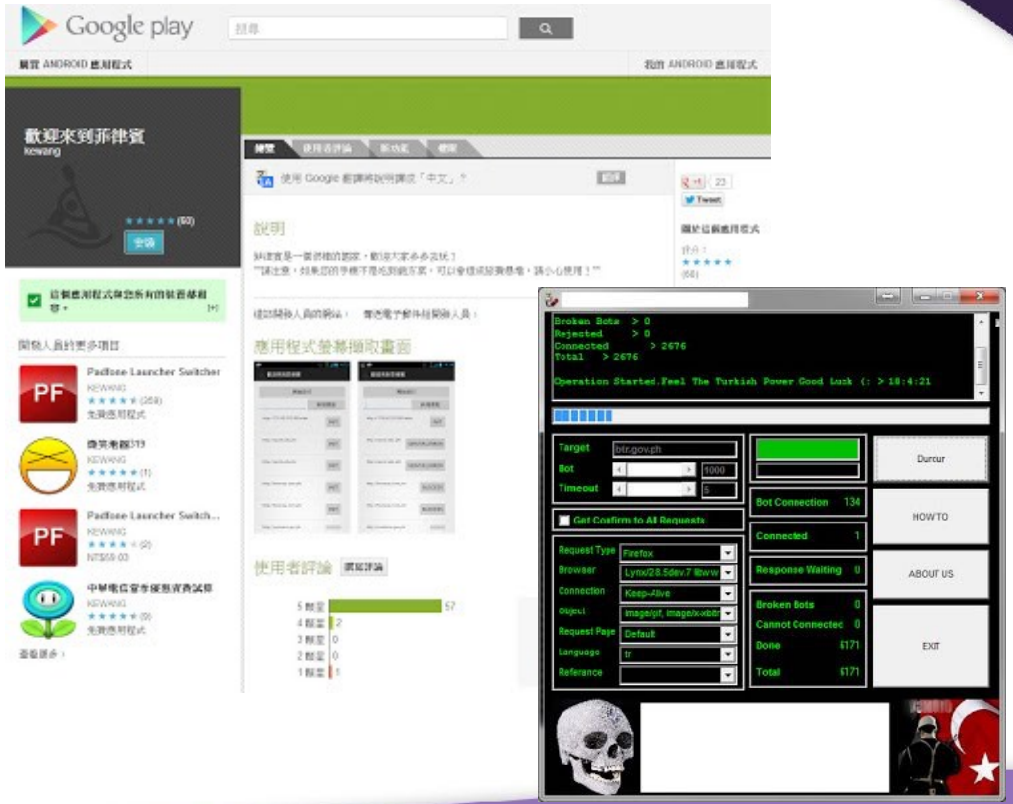
回顧台菲網路攻擊事件

- 因真實世界的國際問題而引起
- 真實世界仍在處理程序問題時，虛擬世界早就戰火遍野



台菲網路攻擊的技術分析

- DDoS分散式阻斷服務攻擊
  - 進行高頻率的網頁更新要求
    - 網頁版、手機版
  - 利用DDoS工具進行特定目標攻擊
- SQL Injection資料隱碼植入攻擊
  - 網站未檢查使用者輸入字串
  - 配合Google Hacking搜尋對象
  - 使用網站爬蟲程式進行網站結構分析
- 系統與應用程式漏洞
  - 古老的問題，但是最有效
  - 配合Malicious Exploit Code



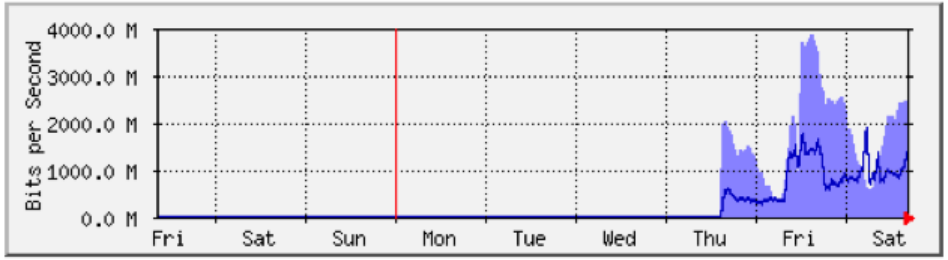
台菲網路攻擊的技術分析

- 一攻一防之間，運用匿蹤的技術
  - 開放服務的Proxy
  - 網路上的隱匿服務
    - SafeIP

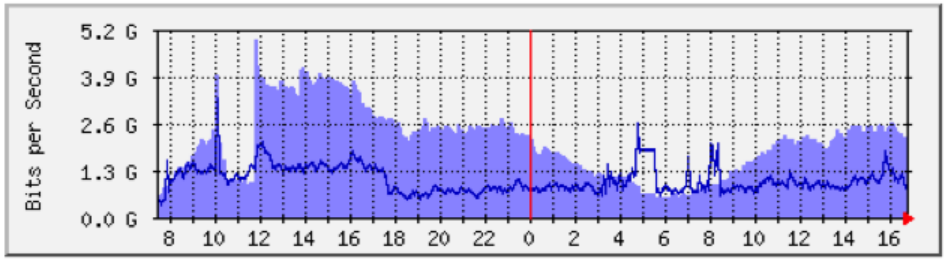
當反課綱事件發生時

NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT

```
64 bytes from 168.95.1.1: icmp_seq=1033 ttl=248 time=26930.619 ms
64 bytes from 168.95.1.1: icmp_seq=1034 ttl=248 time=25946.567 ms
64 bytes from 168.95.1.1: icmp_seq=1035 ttl=248 time=24971.575 ms
64 bytes from 168.95.1.1: icmp_seq=1036 ttl=248 time=24150.163 ms
64 bytes from 168.95.1.1: icmp_seq=1037 ttl=248 time=23149.629 ms
64 bytes from 168.95.1.1: icmp_seq=1038 ttl=248 time=22155.844 ms
64 bytes from 168.95.1.1: icmp_seq=1039 ttl=248 time=21312.961 ms
64 bytes from 168.95.1.1: icmp_seq=1065 ttl=248 time=9879.083 ms
64 bytes from 168.95.1.1: icmp_seq=1066 ttl=248 time=9978.448 ms
64 bytes from 168.95.1.1: icmp_seq=1067 ttl=248 time=9014.878 ms
64 bytes from 168.95.1.1: icmp_seq=1068 ttl=248 time=8081.845 ms
64 bytes from 168.95.1.1: icmp_seq=1069 ttl=248 time=7529.564 ms
64 bytes from 168.95.1.1: icmp_seq=1070 ttl=248 time=6528.702 ms
64 bytes from 168.95.1.1: icmp_seq=1071 ttl=248 time=5869.735 ms
64 bytes from 168.95.1.1: icmp_seq=1072 ttl=248 time=4865.237 ms
64 bytes from 168.95.1.1: icmp_seq=1073 ttl=248 time=3860.678 ms
64 bytes from 168.95.1.1: icmp_seq=1074 ttl=248 time=4475.868 ms
64 bytes from 168.95.1.1: icmp_seq=1075 ttl=248 time=7214.598 ms
64 bytes from 168.95.1.1: icmp_seq=1076 ttl=248 time=6318.742 ms
64 bytes from 168.95.1.1: icmp_seq=1077 ttl=248 time=5315.454 ms
64 bytes from 168.95.1.1: icmp_seq=1078 ttl=248 time=4326.050 ms
64 bytes from 168.95.1.1: icmp_seq=1079 ttl=248 time=3662.656 ms
64 bytes from 168.95.1.1: icmp_seq=1080 ttl=248 time=3185.146 ms
64 bytes from 168.95.1.1: icmp_seq=1081 ttl=248 time=2217.305 ms
64 bytes from 168.95.1.1: icmp_seq=1082 ttl=248 time=1259.081 ms
64 bytes from 168.95.1.1: icmp_seq=1083 ttl=248 time=650.141 ms
64 bytes from 168.95.1.1: icmp_seq=1084 ttl=248 time=87.073 ms
64 bytes from 168.95.1.1: icmp_seq=1085 ttl=248 time=3304.383 ms
64 bytes from 168.95.1.1: icmp_seq=1086 ttl=248 time=4042.994 ms
64 bytes from 168.95.1.1: icmp_seq=1087 ttl=248 time=3360.810 ms
64 bytes from 168.95.1.1: icmp_seq=1088 ttl=248 time=2401.968 ms
64 bytes from 168.95.1.1: icmp_seq=1089 ttl=248 time=1407.464 ms
```



	最大	平均	目前
Internet ==> TANet	3847.0 Mb/秒 (38.5%)	1718.6 Mb/秒 (17.2%)	2424.6 Mb/秒 (24.2%)
TANet ==> Internet	1855.8 Mb/秒 (18.6%)	802.8 Mb/秒 (8.0%)	1108.0 Mb/秒 (11.1%)



	最大	平均	目前
Internet ==> TANet	4892.4 Mb/秒 (48.9%)	2040.6 Mb/秒 (20.4%)	2136.5 Mb/秒 (21.4%)
TANet ==> Internet	3265.7 Mb/秒 (32.7%)	1024.1 Mb/秒 (10.2%)	811.5 Mb/秒 (8.1%)

Github DDoS Attack

NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT

Large Scale DDoS Attack on github.com

March 27, 2015 jnewland Engineering

We are currently experiencing the largest DDoS (distributed denial of service) attack in github.com's history. The attack began around 2AM UTC on Thursday, March 26, and involves a wide combination of attack vectors. These include every vector we've seen in previous attacks as well as some sophisticated new techniques that use the web browsers of unsuspecting, uninvolved people to flood github.com with high levels of traffic. Based on reports we've received, we believe the intent of this attack is to convince us to remove a specific class of content.

We are completely focused on mitigating this attack. Our top priority is making sure github.com is available to all our users while deflecting malicious traffic. Please watch our status site or follow @githubstatus on Twitter for real-time updates.

https://status.github.com/

Github DDoS Attack

March 27, 2015

23:49 CST	We're aware that GitHub.com is intermittently unavailable for some users during the ongoing DDoS. Restoring service for all users while deflecting attack traffic is our number one priority.
23:04 CST	We've deployed our volumetric attack defenses against an extremely large amount of traffic. Performance is stabilizing.
22:45 CST	The attack has ramped up again, and we're evolving our mitigation strategies to match.
20:33 CST	The DDoS attack is still ongoing, but connectivity is back to normal as we continue mitigation. We're keeping a close eye on our traffic for any abnormalities.
18:00 CST	We continue to respond to an ongoing DDoS attack. Some users may experience intermittent connectivity with git operations as we mitigate the problem.
16:31 CST	At this time we're fully operational but we're still mitigating the ongoing DDoS attack and there may be intermittent connectivity issues as we continue working on the problem

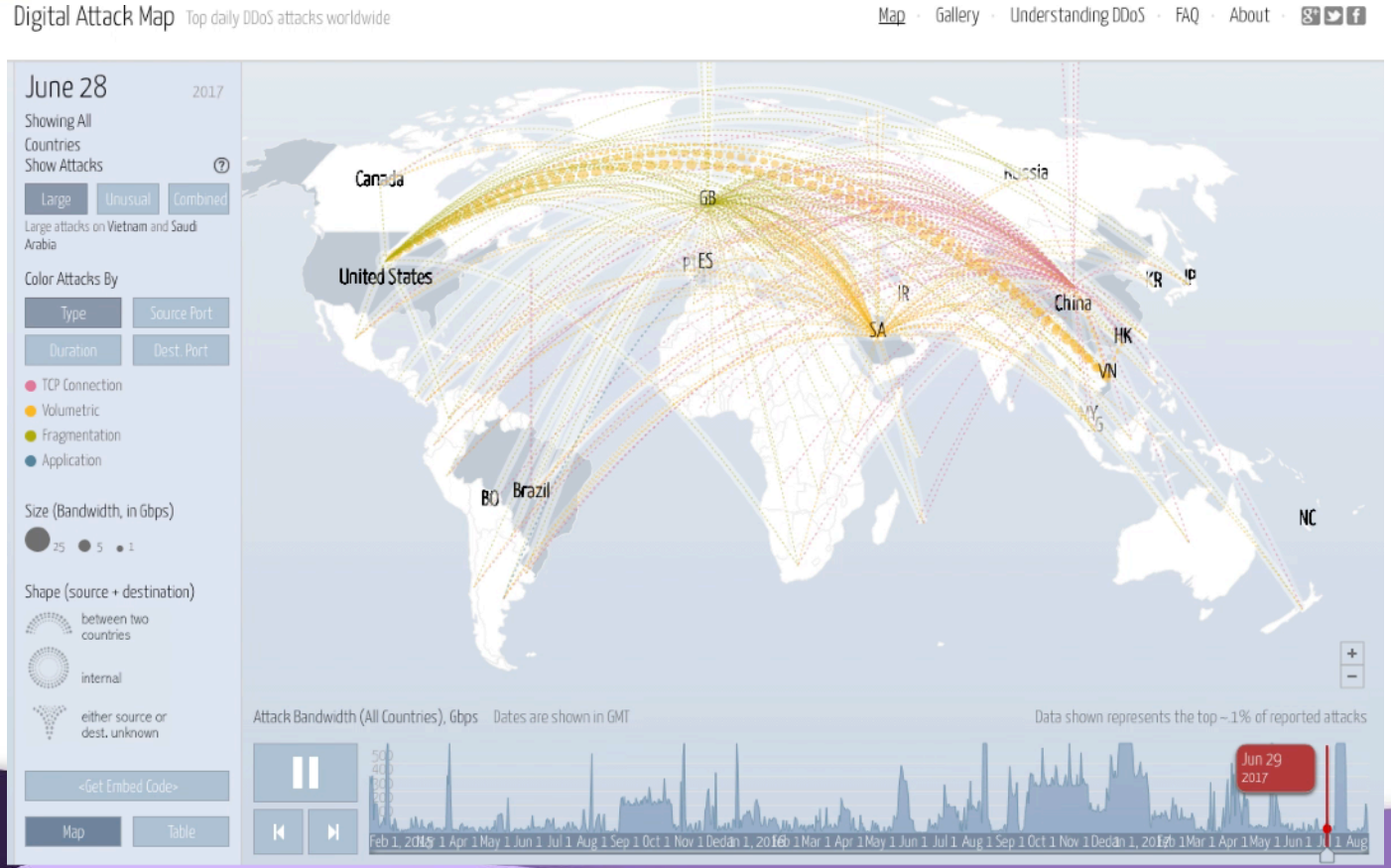
- DDoS attack is still ongoing

DDoS攻擊手法分析

常見的偵測方法

- Invalid Packets
- IPv4 Address Filter Lists
- IPv4 Black/White Lists
- Packet Header Filtering
- IP Location Filter Lists
- Zombie Detection
- UDP Reflection/Amplification Protection
- Per Connection Flood Protection
- TCP SYN Authentication
- DNS Scoping
- DNS Authentication
- TCP Connection Limiting
- TCP Connection Reset
- Payload Regular Expression
- Protocol Baselines
- DNS Malformed
- DNS Rate Limiting
- DNS NXDomain Rate Limiting
- DNS Regular Expression
- HTTP Malformed
- HTTP Scoping
- HTTP Rate Limiting
- AIF and HTTP/URL Regular Expression
- SSL Negotiation
- SIP Malformed
- SIP Request Limiting
- Shaping
- IP Location Policing

Digital Attack Map



- 全球DDoS攻擊威脅監測

資料來源：
http://www.digitalattackmap.com/

DDoS事件簿

- 當行動裝置與物聯網裝置總數超過傳統個人電腦總數時
- 裝置的弱點成為駭客有興趣的目標

2.5萬監視器成DDoS殭屍網路大軍，多數來自台灣！

美國資安公司Sucuri指出，在調查珠寶商網站遭DDoS攻擊時發現，攻擊來自駭客掌握的2.5萬個監控攝影機組成的殭屍網路大軍，其中24%來自台灣，其次是美國(12%)及印尼(9%)等其他地區。

文/ 陳文義 | 2016-06-28 發表

讚 4.3 萬 按讚加入iThome粉絲團 讚 1,782 分享

示意圖

資料來源 http://www.ithome.com.tw/news/106745

Mirai Botnet

- Mirai可以讓執行Linux的計算系統成為被遠端操控的「殭屍」，以達到通過殭屍網路進行大規模網路攻擊的目的
- Mirai的主要感染物件是可存取網路的消費級電子裝置，例如網路監控攝錄影機和家庭路由器等。
- Mirai構建的殭屍網路已經參與了幾次影響廣泛的大型分散式阻斷服務攻擊，包括2016年9月20日針對電腦保安撰稿人布萊恩·克萊布斯個人網站的攻擊、對法國網站代管商OVH的攻擊，以及2016年10月Dyn公司網路攻擊事件
- Mirai的原始碼已經以開源的形式發布，其中的技術也已被其他一些惡意軟體採用

Mirai Botnet

- 當軍火庫被打開時
- 開發攻擊用的惡意程式變得更加容易

jgamblin committed on GitHub Merge pull request #38 from Red64/patch-1 ... Latest commit 3273043 24 days ago

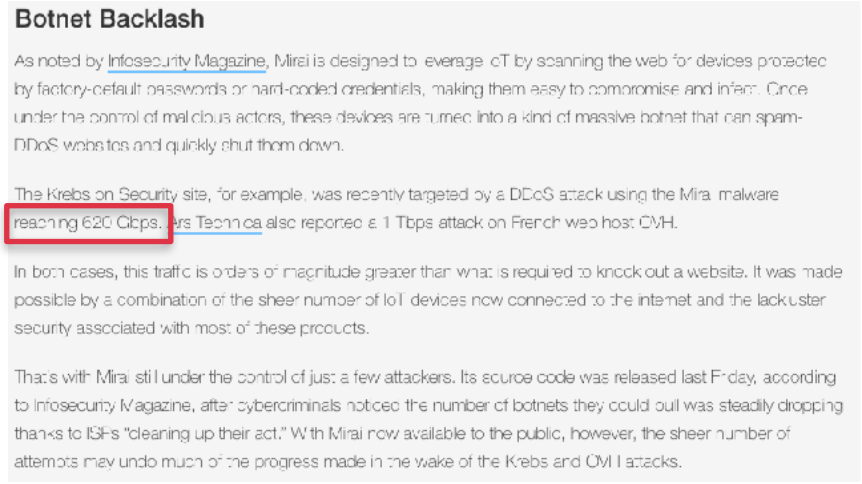
dlr	Trying to Shrink Size	10 months ago
loader	Trying to Shrink Size	10 months ago
mirai	Trying to Shrink Size	10 months ago
scripts	Transcribe post to markdown while preserving	10 months ago
ForumPost.md	Transcribe post to markdown while preserving	10 months ago
ForumPost.txt	Update ForumPost.txt	9 months ago
LICENSE.md	Trying to Shrink Size	10 months ago
README.md	Fix a typo in README.md	24 days ago

jgamblin Trying to Shrink Size Latest commit 9779d43 on 25 Oct 2016

..		
bot	Trying to Shrink Size	10 months ago
cnc	Trying to Shrink Size	10 months ago
tools	Trying to Shrink Size	10 months ago
build.sh	Trying to Shrink Size	10 months ago
prompt.txt	Trying to Shrink Size	10 months ago

https://github.com/jgamblin/Mirai-Source-Code

620Gbps或1Tbps的攻擊



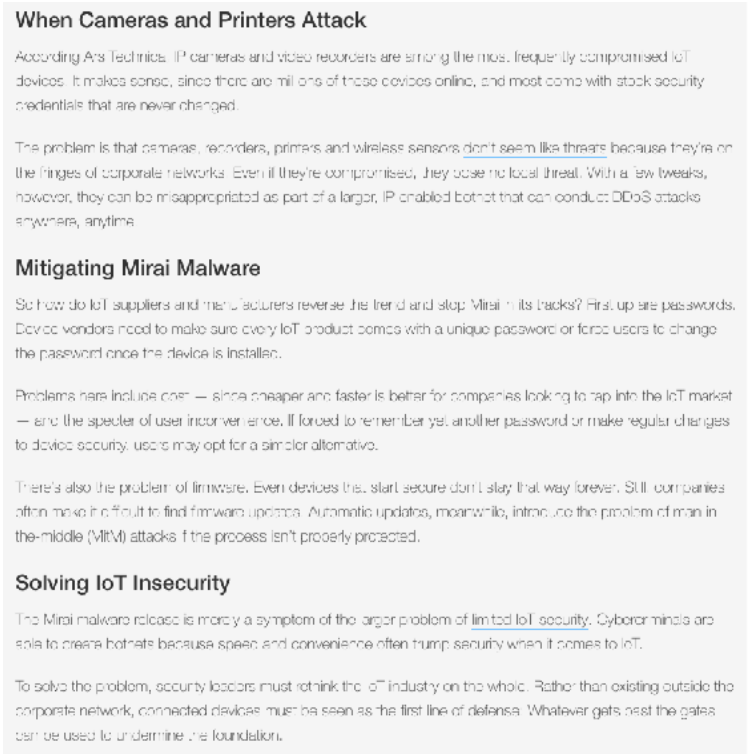
Botnet Backlash

As noted by Infosecurity Magazine, Mirai is designed to leverage IoT by scanning the web for devices protected by factory-default passwords or hard-coded credentials, making them easy to compromise and infect. Once under the control of malicious actors, these devices are turned into a kind of massive botnet that can spam-DDoS websites and quickly shut them down.

The Krebs on Security site, for example, was recently targeted by a DDoS attack using the Mirai malware reaching 620 Gbps. Ars Technica also reported a 1 Tbps attack on French web host OVH.

In both cases, this traffic is orders of magnitude greater than what is required to knock out a website. It was made possible by a combination of the sheer number of IoT devices now connected to the internet and the lackluster security associated with most of these products.

That's with Mirai still under the control of just a few attackers. Its source code was released last Friday, according to Infosecurity Magazine, after cybercriminals noticed the number of botnets they could pull was steadily dropping thanks to ISPs "cleaning up their act." With Mirai now available to the public, however, the sheer number of attempts may undo much of the progress made in the wake of the Krebs and OVH attacks.



When Cameras and Printers Attack

According Ars Technica, IP cameras and video recorders are among the most frequently compromised IoT devices. It makes sense, since there are millions of these devices online, and most come with stock security credentials that are never changed.

The problem is that cameras, recorders, printers and wireless sensors don't seem like threats because they're on the fringes of corporate networks. Even if they're compromised, they pose no local threat. With a few tweaks, however, they can be misappropriated as part of a larger, IP enabled botnet that can conduct DDoS attacks anywhere, anytime.

Mitigating Mirai Malware

So how do IoT suppliers and manufacturers reverse the trend and stop Mirai in its tracks? First up are passwords. Device vendors need to make sure every IoT product comes with a unique password or force users to change the password once the device is installed.

Problems here include cost — since cheaper and faster is better for companies looking to tap into the IoT market — and the specter of user inconvenience. If forced to remember yet another password or make regular changes to device security, users may opt for a simpler alternative.

There's also the problem of firmware. Even devices that start secure don't stay that way forever. Still, companies often make it difficult to find firmware updates. Automatic updates, meanwhile, introduce the problem of man in the-middle (MitM) attacks if the process isn't properly protected.

Solving IoT Insecurity

The Mirai malware release is merely a symptom of the larger problem of limited IoT security. Cybercriminals are able to create botnets because speed and convenience often trump security when it comes to IoT.

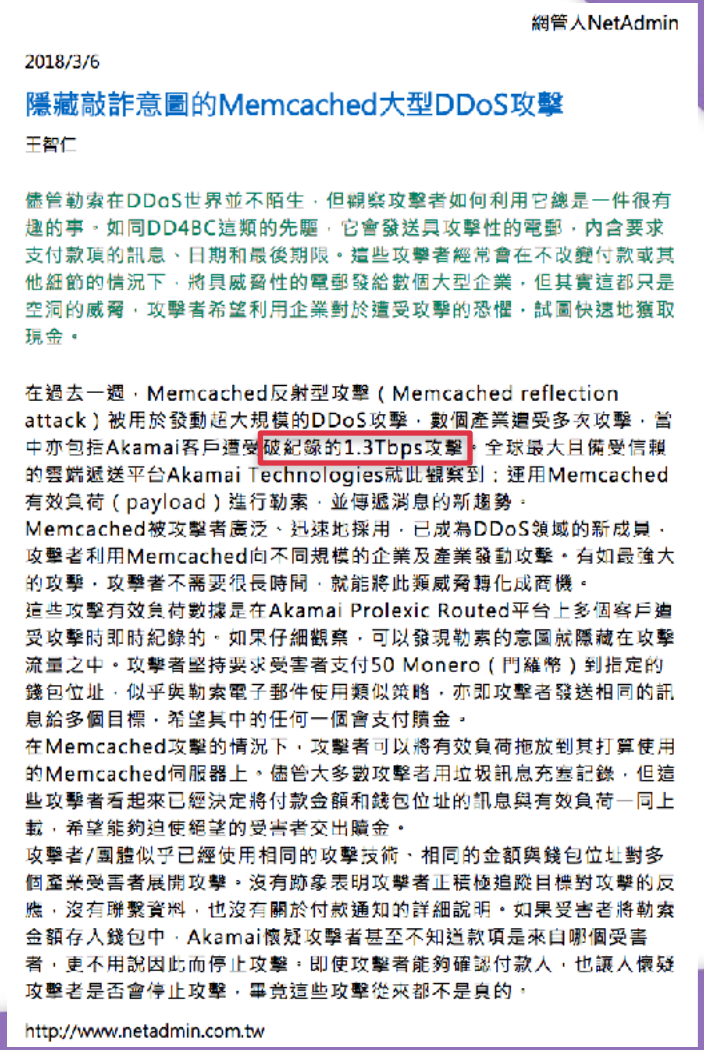
To solve the problem, security leaders must rethink the IoT industry on the whole. Rather than existing outside the corporate network, connected devices must be seen as the first line of defense. Whatever gets past the gates can be used to undermine the foundation.

2016年9月20日，攻擊者通過Mirai和BASHLITE對Krebs on Security網站發動了DDoS攻擊，攻擊流量達到了620 Gbp。Ars Technica報導稱在對法國網站代管商OVH的攻擊中發現了1 Tbps的攻擊流量

https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/

更大的攻擊流量

- 攻擊行動背後的真相
- 更多樣化的攻擊手法被應用
- DDoS攻擊帶來大量的威脅



網管人NetAdmin

2018/3/6

隱藏敲詐意圖的Memcached大型DDoS攻擊

王智仁

儘管勒索在DDoS世界並不陌生，但觀察攻擊者如何利用它總是一件很有趣的事。如同DD4BC這類的先驅，它會發送具攻擊性的電郵，內含要求支付款項的訊息、日期和最後期限。這些攻擊者經常會在不改變付款或其他細節的情況下，將具威脅性的電郵發給數個大型企業，但其實這都只是空洞的威脅，攻擊者希望利用企業對於遭受攻擊的恐懼，試圖快速地獲取現金。

在過去一週，Memcached反射型攻擊（Memcached reflection attack）被用於發動起大規模的DDoS攻擊，數個產業遭受多次攻擊，當中亦包括Akamai客戶遭受破紀錄的1.3Tbps攻擊，全球最大且備受信賴的雲端遞送平台Akamai Technologies就此觀察到；運用Memcached有效負荷（payload）進行勒索，並傳遞消息的新趨勢。

Memcached被攻擊者廣泛、迅速地採用，已成為DDoS領域的新成員，攻擊者利用Memcached向不同規模的企業及產業發動攻擊。有如最強大的攻擊，攻擊者不需要很長時間，就能將此類威脅轉化成商機。

這些攻擊有效負荷數據是在Akamai Prolexic Routed平台上多個客戶遭受攻擊時即時紀錄的，如果仔細觀察，可以發現勒索的意圖就隱藏在攻擊流量之中。攻擊者堅持要求受害者支付50 Monero（門羅幣）到指定的錢包位址，似乎與勒索電子郵件使用類似策略，亦即攻擊者發送相同的訊息給多個目標，希望其中的任何一個會支付贖金。

在Memcached攻擊的情況下，攻擊者可以將有效負荷拖放到其打算使用的Memcached伺服器上，儘管大多數攻擊者用垃圾訊息充塞記錄，但這些攻擊者看起來已經決定將付款金額和錢包位址的訊息與有效負荷一同上載，希望能夠迫使絕望的受害者交出贖金。

攻擊者/團體似乎已經使用相同的攻擊技術、相同的金額與錢包位址對多個產業受害者展開攻擊。沒有跡象表明攻擊者正積極追蹤目標對攻擊的反應，沒有聯繫資料，也沒有關於付款通知的詳細說明。如果受害者將勒索金額存入錢包中，Akamai懷疑攻擊者甚至不知道款項是來自哪個受害者，更不用說因此而停止攻擊。即使攻擊者能夠確認付款人，也讓人懷疑攻擊者是否會停止攻擊，畢竟這些攻擊從來都不是真的。

http://www.netadmin.com.tw

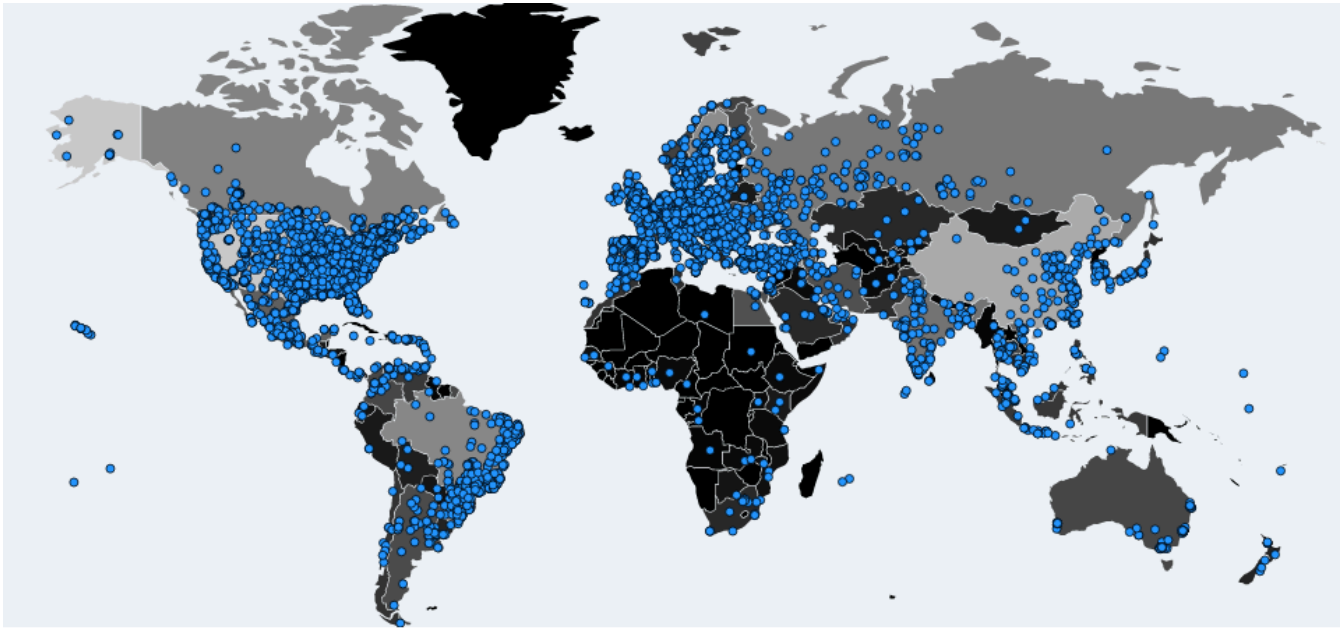
Mirai Botnet追蹤

23,276
ONLINE

20,071
OFFLINE

43,347
TOTAL

時間週期：24H



https://intel.malwaretech.com/botnet/mirai

資安事件的因應對策

資安事件的因應對策

當資安事件發生時

- 自主通報
  - 從所管理的系統與設備上，發現可能存在的資安威脅，多數以通報外部攻擊為主
- 接獲通報
  - 由ASOC(南/北)或其它資安團隊偵測到的資安事件，收集資料後，進行通報與應變處理
  - TACERT為主要的服務窗口
  - ASOC與資安團隊提供技術協助

APT攻擊偵測

- 惡意網域名稱資料庫
- 惡意程式下載偵測，可支援多種不同檔案格式
  - Windows PE32或64位元之執行檔。
  - Windows DLL動態連結函式庫。
  - MicroSoft Office文件格式PDF文件格式。
  - 壓縮檔，包含zip與rar檔案格式。
  - Java壓縮檔。
  - Java Script檔案格式。
  - Android檔案格式。
- 及時流量分析，可支援多種網路協定
  - HTTP, DNS, FTP, SMB, SMTP

全方位的防禦技術與因應對策

掌握本身的資安問題

- 從資安的角度
  - 沒事，不代表真的沒事
    - 需要從系統、網路的架構思考起
  - 系統正常，不代表系統真的正常
    - 系統狀態的掌握，是目前許多系統管理人員的痛
  - 存在弱點，不代表沒人來用
    - 系統弱點掃瞄，看不懂的人多的是，需要專業的資安分協協助
  - 網路流量，只是參考的指標之一
    - 看流量大小的時代已過去，目前只能是受害指標的數據

管理層面

- 資訊安全與網路管理政策
- 導入資訊安全管理制度
  - ISO 27001
  - CSA STAR
- 建立資安管理生態系統

雲端安全控制矩陣(CCM)

NARLabs National Applied Research Laboratories
National Center for High-performance Computing
TWCSIRT

AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DSC	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management
HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management

136 CONTROLS
Cloud Controls Matrix v3.0

//

133 CONTROLS
Cloud Controls Matrix v3.0.1

https://downloads.cloudsecurityalliance.org/assets/research/cloud-controls-matrix/CSA_CCM_v.3.0.1_-_12-10-15.zip

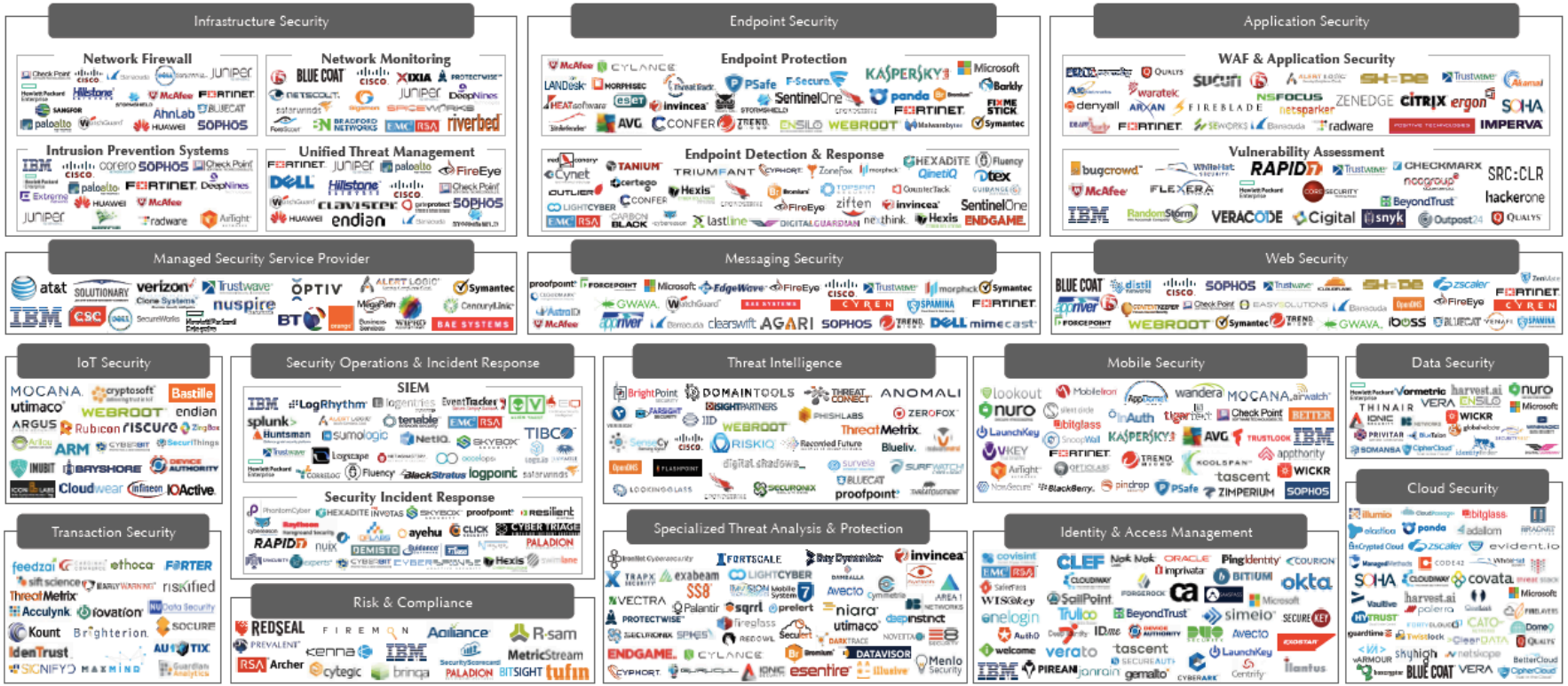
CSA Security Guidance V4

- **Domain 1**:Cloud Computing Concepts and Architectures
- **Domain 2**:Governance and Enterprise Risk Management
- **Domain 3**:Legal Issues, Contracts and Electronic Discovery
- **Domain 4**:Compliance and Audit Management
- **Domain 5**:Information Governance
- **Domain 6**:Management Plane and Business Continuity
- **Domain 7**:Infrastructure Security
- **Domain 8**:Virtualization and Containers
- **Domain 9**:Incident Response
- **Domain 10**:Application Security
- **Domain 11**:Data Security and Encryption
- **Domain 12**:Identity, Entitlement and Access Management
- **Domain 13**:Security as a Service
- **Domain 14**:Related Technology

資安從來就不是技術問題

NARLabs
National Applied Research Laboratories
National Center for High-performance Computing

TWCSIRT



結論

重點摘要

- 關鍵基礎服務已成為駭客利用的目標
- 更新系統與應用服務，降低弱點被運用的機會
- 物聯網與新興應用帶來新的資安問題
- 赤手空拳無法面對隨時可能來臨的網路攻擊
- 資安問題從來就不是技術問題

Thank you for your attention!

Any questions?

TWCSIRT
臺灣電腦安全事件應變中心
Taiwan Computer Security Incident Response Team