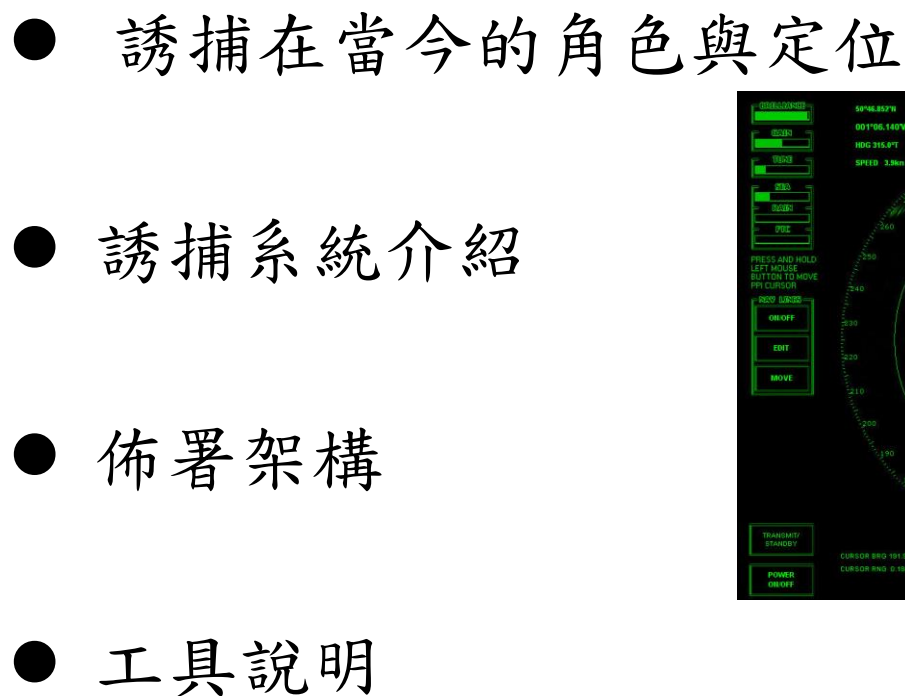




新世代誘捕系統佈署機制

國家高速網路與計算中心
許勝翔



誘捕在當今的角色與定位

- ✓ 原廠研發特徵碼不可或缺的一環
 - 沒法單純透過特徵碼判斷，需要靠行為模式確認的攻擊
- ✓ 無法裝防毒，妨害設備缺少防禦機制
- ✓ 想跟駭客學技術的您

安全防禦方式？

- IPS / IDS
- WAF、郵件過濾
- 防毒軟體
- Honeynet & Honeytrap

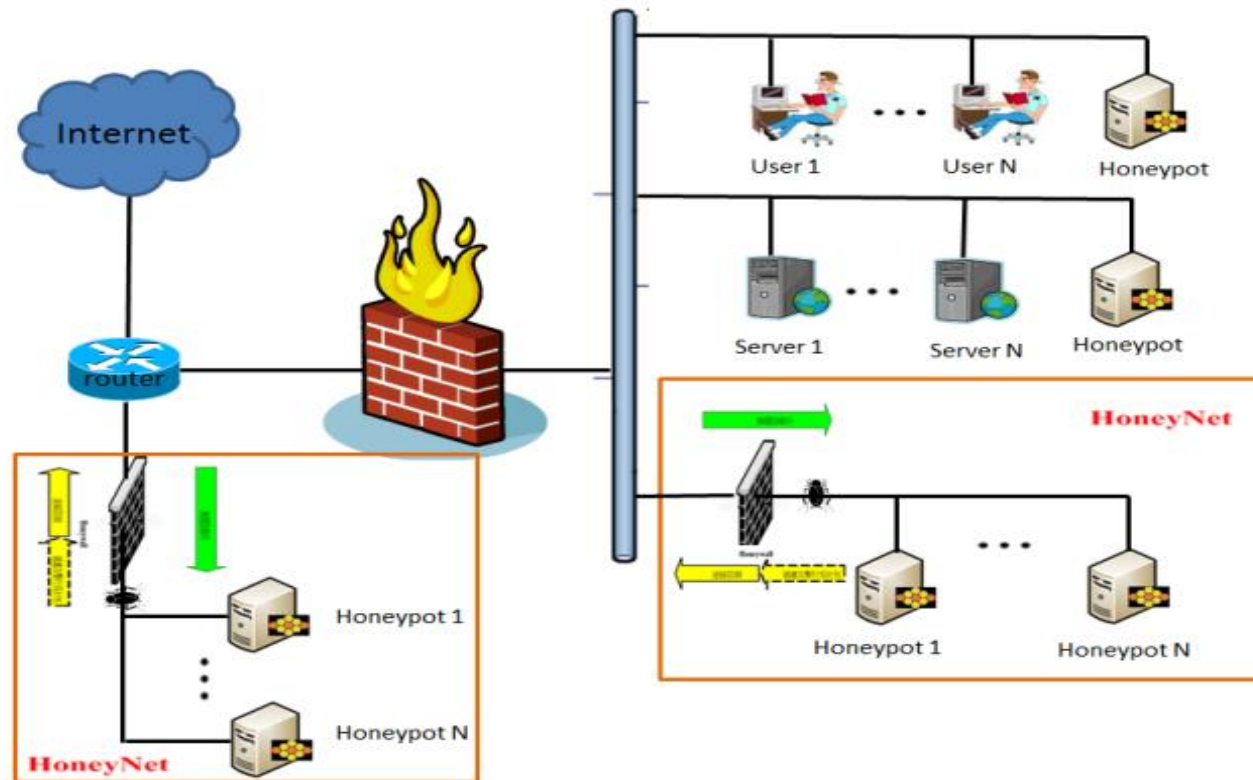
HoneyPot & HoneyNet

NARLabs

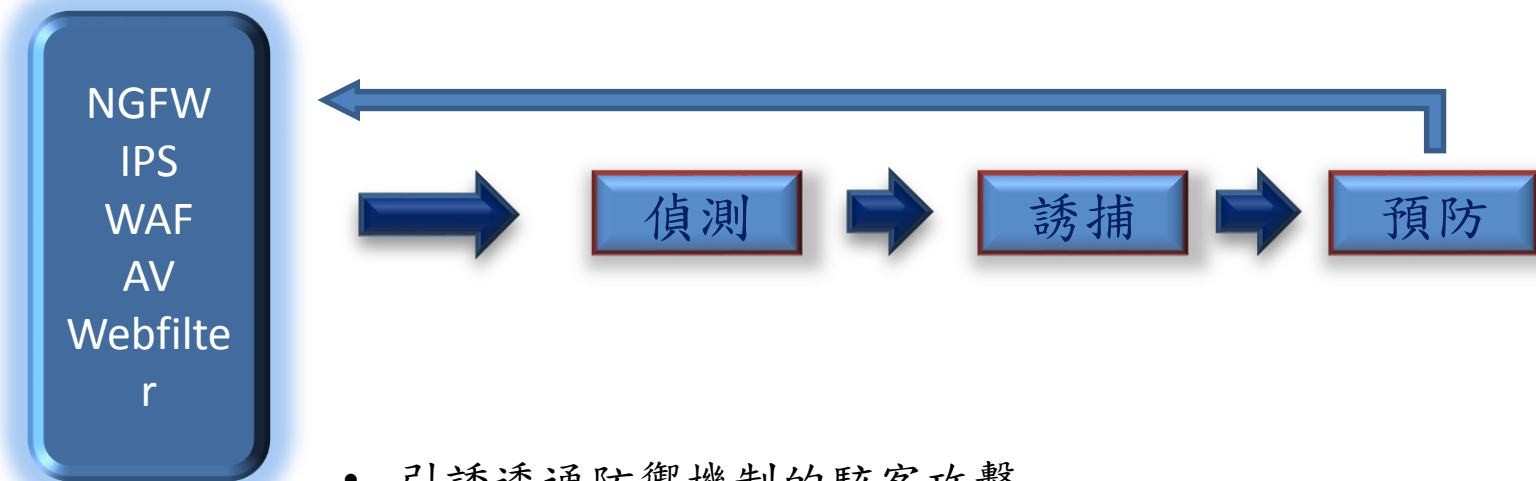
承諾 · 熱情 · 創新



佈點示意圖



部署誘捕系統的特點



- 引誘透過防禦機制的駭客攻擊
- 迷惑敵人，誘使駭客攻擊Honeypot而無暇去攻擊重要的機器
- 透過誘捕系統，完全掌握駭客手法
- 對新攻擊發出預警與防禦策略制定
- 對攻擊計劃行為週期進行深入的分析研究
- 作為對系統弱點預警及先進的監視工具
- 與入侵偵測與防火牆等防禦機制成為完整方案

誘捕網路效益

- 透過誘捕系統提供預警防禦單15萬次以上，以告知手法及解決機制
- 每周攻擊超過一萬次以上之攻擊連線 IP情資清單
- 捕捉到的惡意程式可進行後續之分析，成為知識庫典藏

owl.nchc.org.tw

Malware Samples

15,847,192

Malware Analysis Reports

3,017,179

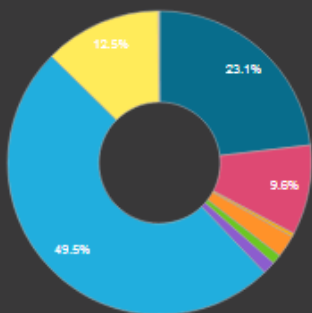
Trend



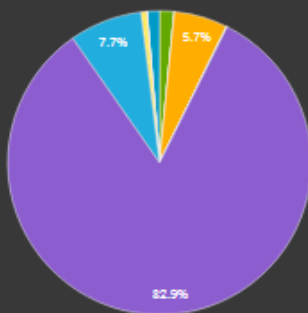
Search Top 10

Keylogger
Exploit/Root Kit
Bot
Adware
Backdoor
Ransom
Trojan
Worm

Statistics of Malware Classifications



Statistics of File Types



Malware Knowledge Base

Home Malware About

MALWARE

MD5	File Type	File Size	VirusTotal Result	Malware Name
017b7570d3488a9b114263780508310	Others	0.00KB	13/61	
012bc32e4e30a7c50a3073547477fa0	Others	84.00KB	42/57	
018c4f3f8ec108f02393ef975043c440	Others	210.00KB	27/56	
013e11c22e8b2479402c0a4c4f35c9	Others	40.94KB	22/56	
010e097930c42c3724cc052c0850	Others	209.88KB	49/56	
018c107090ec337108f0b13c2c0c00	Others	12.50KB	18/55	
01053227c7729ce02084719750e9050	Others	132.79KB	31/52	
0170a7705c070f1f051e0c051122070	Others	12.50KB	9/56	
017797c010515451c0990cc747c300	Others	0.00KB	0/57	
01402450e9710a23f00b97724377410	Others	650.50KB	47/57	
012b017381ae3880c270d307730700	Others	93.27KB	20/57	
0137a70a700009140030a02330e000	Others	40.81KB	15/56	
01400022a4370030a0000000000000	Others	291.50KB	37/55	
01220b92b2790ca74000c0a000120	Others	105.29KB	42/57	
0174100373970337440053371105470	Others	12.50KB	8/55	
0142c451a0310a040005736f0707100	Others	1.13KB	38/55	
011d70a09c10a030c330010c5c010	Others	12.50KB	8/54	
0144e070a07010a2f900e13ca707070	Others	31.00KB	50/56	
010200a700a07c700700f0c09f930000	Others	795.82KB	27/51	
012b000c0c0700170700a07000070	Others	32.00KB	50/57	

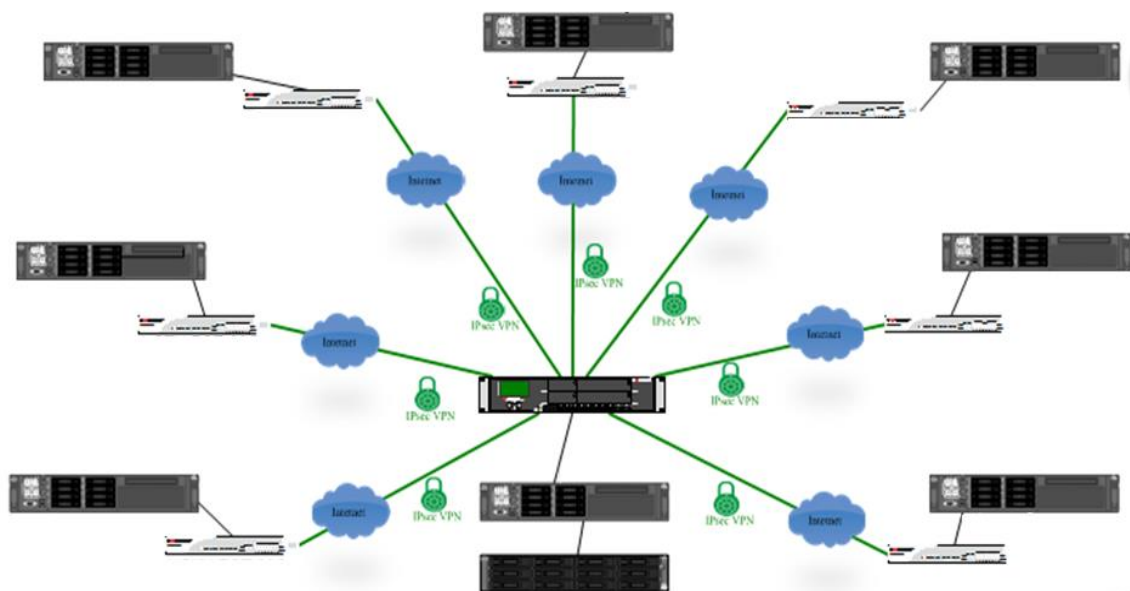
佈 署 架 構

佈署範圍

目前使用圖示各區網使用當地IP進行偵測，
約可產生6,000個預警分析來源。



過去：分散式架構



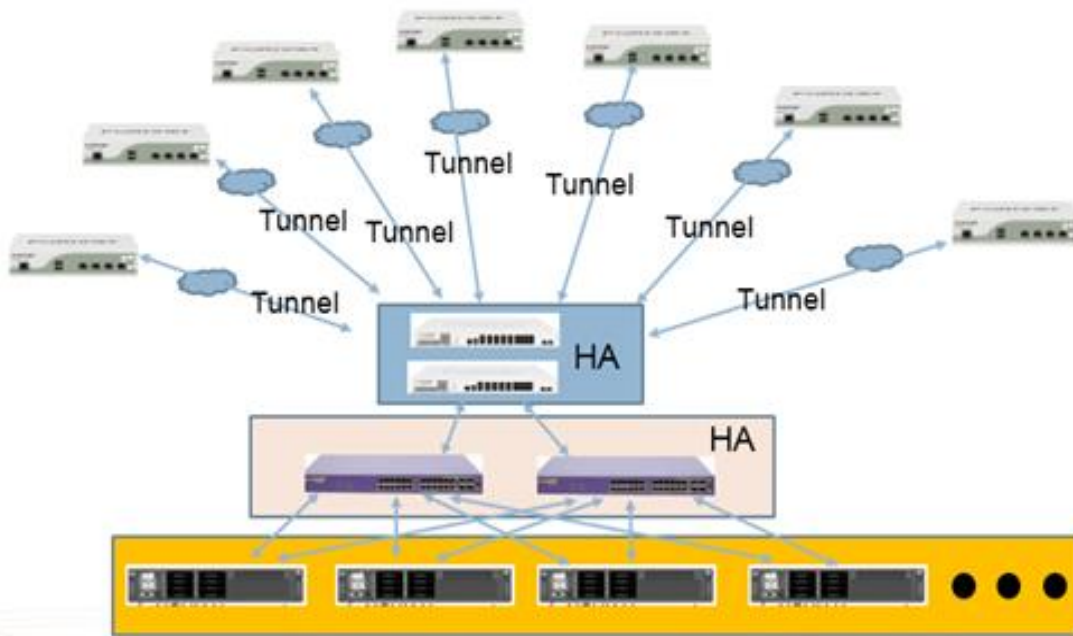
控管不易

資源浪費

單一主機，單一網段

日誌分散

現在：SinkHole架構



中央控管彈性調整部署

資源分配

單一主機，多網段

日誌集中

運用技術（Layer 2透通）

VXLAN



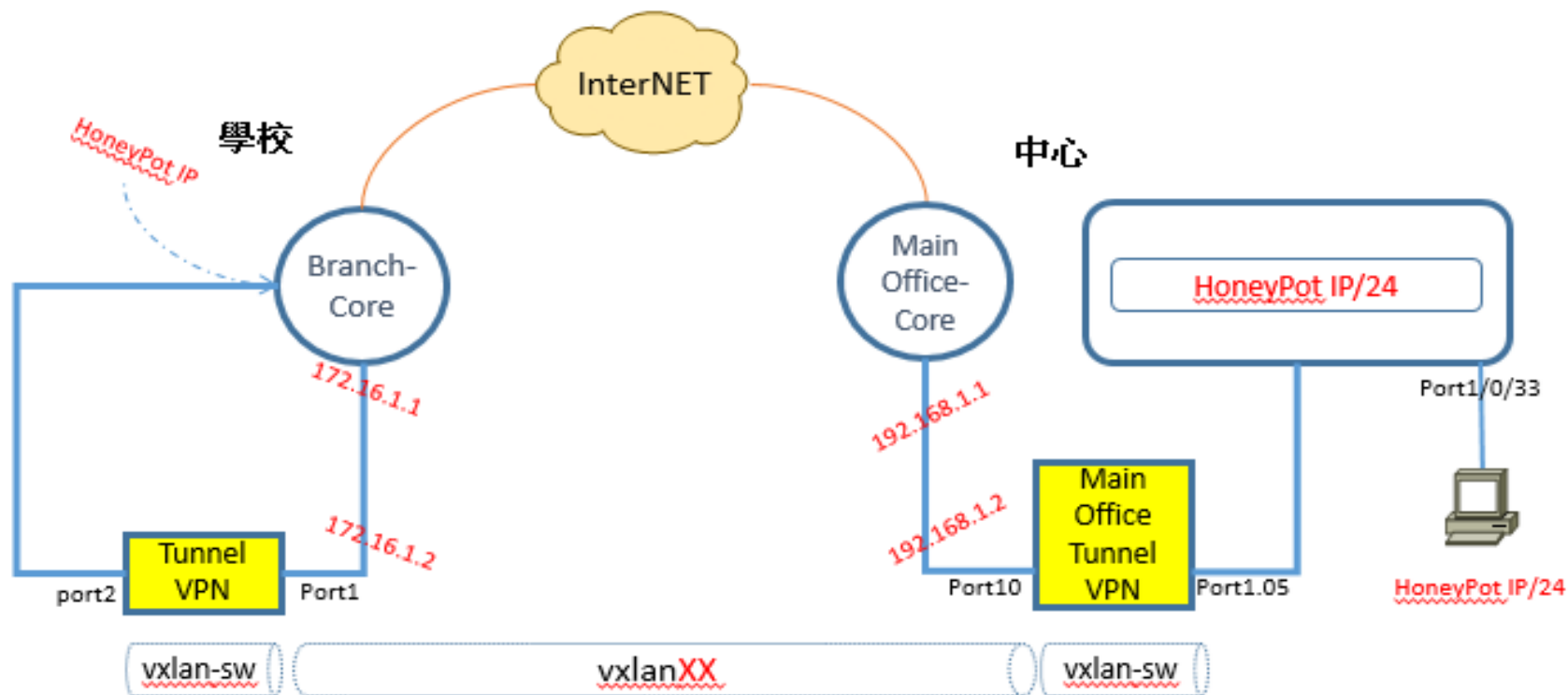
- ☐ 應用靈活部署
- ☐ 更好的擴展性
- ☐ 提高網路使用率

FortiOS



- ☐ Version 5.6
- ☐ 支援多個Vlan在同Tunnel

運作示意



誘捕平台

NAR Labs

承諾·熱情·創新

Left sidebar (File Explorer):

- NCHC_honeypot
 - nchc_honeypot
 - 10.0.14.1
 - 10.0.14.2
 - 10.0.14.3
 - 10.0.14.4
 - honeypot_cowrie_ntu
 - honeypot_dionaea_3
 - honeypot_amun
 - honeypot_amun_1
 - honeypot_amun_2
 - honeypot_amun_3
 - honeypot_conpot
 - honeypot_conpot_1
 - honeypot_conpot_2
 - honeypot_cowrie
 - honeypot_cowrie_nchu
 - honeypot_cowrie_nchu_1
 - honeypot_cowrie_ncku
 - honeypot_cowrie_ncnu
 - honeypot_cowrie_niu
 - honeypot_cowrie_ntu_1
 - honeypot_cowrie_ntu_2
 - honeypot_dionaea
 - honeypot_dionaea_1
 - honeypot_dionaea_2
 - honeypot_forward
 - honeypot_glstopf

Main Panel (vSphere Web Client):

Navigation: 入門 | 摘要 | 虛擬機器 | 效能 | 組態 | 工作與事件 | 警示 | 權限 | 對應 | 儲存區視圖 | 硬體狀況

Hardware (硬體):

- 處理器
- 記憶體
- 儲存區
- 網路功能
- 儲存裝置介面卡
- 網路介面卡
- 進階設定
- 電源管理

Software (軟體):

- 授權的功能
- 時間組態
- DNS 和路由
- 驗證服務
- 電源管理
- 虛擬機器啟動/關閉
- 虛擬機器分頁檔位置
- 安全性設定檔
- 主機快取組態
- 系統資源配置

Network Function (網路功能):

檢視: vSphere Standard Switch | vSphere Distributed Switch

標準交換器: vSwitch1

虛擬機器連接埠群組:

- ncnu_2
 - 1 台虛擬機器 | VLAN 識別碼: 1102
 - honeypot_telnet_ncnu
- ncnu_4
 - VLAN ID: 1104
- ncnu_12
 - VLAN ID: 1112
- ncnu_9
 - 2 台虛擬機器 | VLAN 識別碼: 1109
 - honeypot_glstopf_nctu
 - honeypot_glstopf_ncnu
- ncnu_3

實體介面卡:

- vmnic1 1000 完整
- vmnic2 待命



情資分析平台

NAR Labs

承諾 · 熱情 · 創新

惡意訪問次數統計

25,756

惡意程式下載次數統計

74

惡意程式數量統計

37

惡意樣本下載連結統計

38

惡意程式 TOP 10

惡意程式MD5

次數

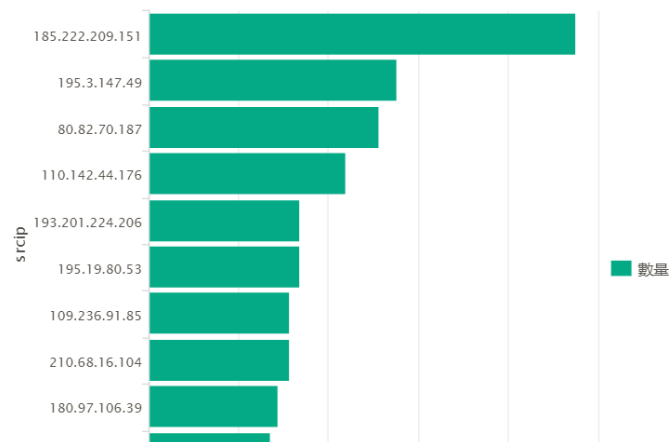
b781bda46294650eac0a82d2da70ee45
44db31c1238b00cd4ddf857f27ee6d7e0116fba
5142a66aeb9423066e8d53dc5f78294
87136c488903474630369e232704fa4d
e2c2715c9bc248fb844bdf2885343153
ee50541a5d92a8c6deb2e7e4bb35e2d0
5132e7f4b96d64c33aa1574d46321b2b
595673fac780251f8083e688c7c381cd
5d150f55f782e50ab64451aea3591ae9
61ddb216aea513c941b4e0ab7e7165b6

惡意程式下載點統計 TOP 10

下載點

次數

前十名IP



攻擊來源詳細資訊

攻擊來源IP	攻擊單位	攻擊者國家	受攻擊單位	數量
185.222.209.151	ISP業者 OR 國外IP	NONE	中山大學 中興大學 台東大學 成功大學 暨南大學 東華大學	119
195.3.147.49	ISP業者 OR 國外IP	Latvia	中興大學 台東大學 台灣大學 宜蘭大學 成功大學 暨南大學 東華大學	69
80.82.70.187	ISP業者 OR 國外IP	Seychelles	中山大學 中正大學 中興大學 台灣大學 宜蘭大學 教育部	64

Dashboard

Shinkhole 帶來 效率提升

- 提昇硬體效能使用，以提供更多種類的誘捕系統偵測，以收集到更多不同攻擊類型資料。

管理方便

- 設備放置各偵控點時，除了在維護時需耗費較多時間處理外，也無法達到硬體7*24小時全天候的監控，中心有專職的值班人員以7*24小時巡檢，以避免設備停機。

成本大幅降低

- 由於原先每個誘捕監控點，是透過各自硬體與軟體VMware vShpere Infrastructure來完成佈署，日後每增加一個擴充點需增加硬體與軟體的費用，其增加之費用也高昂，透過此架構後，只需在學校增加一台端點設備即可。

可靠度增加

- 為了提高網路的穩定性與可用性，以備援架構做為保護服務不中斷，消除單點故障來提升網路的可靠性，確保Botnet偵測惡意攻擊連線資訊服務。

擴展性方便

- 原架構下不需變更任何設定下，能更廣泛的深入學術網路內部研究，對未來持續擴充到學術網路末端的相關研究需求，有十分正面的推動影響力。

誘捕工具說明

誘捕系統類型

- 誘捕功能

- Network
- Connection
- Web App
- Malware
- Client-Side

- 分析功能

- 資料視覺化

誘捕功能

High-Interaction	
優點	劣點
1. 採用真實的作業系統提供所需之服務。 2. 可收集較新型的攻擊資訊	1. 佈署與管理較困難。 2. 高風險容易成為跳板。
Low-Interaction	
優點	劣點
1. 所有弱點服務皆為模擬。 2. 易於佈署與管理 3. 低風險不容易成為跳板。	1. 模擬的弱點皆為已知型。 2. 無法收集新型的攻擊資訊。

Honeypots

• Database Honeypots

- [Delilah](#) - An Elasticsearch Honeypot written in Python.
- [ESPot](#) - An Elasticsearch honeypot written in NodeJS, to capture every attempts to exploit CVE-2014-3120.
- [Elastic honey](#) - A Simple Elasticsearch Honeypot.
- [MongoDB-HoneyProxy](#) - A MongoDB honeypot proxy.
- [NoSQLpot](#) - The NoSQL Honeypot Framework.
- [mysql-honeypotd](#) - Low interaction MySQL honeypot written in C.
- [mysql](#) - A mysql honeypot, still very very early stage.

• Web honeypots

- [Bukkit Honeypot](#) Honeypot - A honeypot plugin for Bukkit.
- [EoHoneypotBundle](#) - Honeypot type for Symfony2 forms.
- [Glastopf](#) - Web Application Honeypot.
- [Google Hack Honeypot](#) - designed to provide reconnaissance against attackers that use search engines as tool against your resources.
- [Laravel Application Honeypot](#) - Honeypot - Simple spam prevention package for Laravel applications.
- [Nodepot](#) - A nodejs web application honeypot.
- [Servletpot](#) - Web application Honeypot.
- [Shadow Daemon](#) - A modular Web Application Firewall / High-Interaction Honeypot for PHP, Perl & Python
- [WebTrap](#) - Designed to create deceptive webpages to deceive and redirect attackers away from real website
- [basic-auth-pot](#) bap - http Basic Authentication honeyPot.
- [django-admin-honeypot](#) - A fake Django admin login screen to notify admins of attempted unauthorized a
- [honeyhttpd](#) - a Python-based web server honeypot builder.
- [phpmyadmin_honeypot](#) - - A simple and effective phpMyAdmin honeypot.
- [shockpot](#) - WebApp Honeypot for detecting Shell Shock exploit attempts.
- [smart-honeypot](#) - PHP Script demonstrating a smart honey pot.
- [Snare/Tanner](#) - successors to Glastopf
 - [Snare](#) - Super Next generation Advanced Reactive honEypot
 - [Tanner](#) - Evaluating SNARE events
- [stack-honeypot](#) - Inserts a trap for spam bots into responses.



Modern Honey Network

883 commits		45 branches		0 releases		28 contributors	
Branch: master		New pull request		Find file		Clone or download	
d1str0 Merge pull request #561 from synmacs/master				Latest commit dd5c57b 11 days ago			
scripts	Fixed address for pyev repo					a month ago	
server	Fixed api information leak issue #473					8 months ago	
.gitignore	elastichoney ...					3 years ago	
.travis.yml	fix travis?					11 months ago	
LICENSE	initial commit					4 years ago	
README.md	updated dead hyperlink for Dionaea					2 months ago	
Vagrantfile	Update Vagrantfile					4 years ago	
Vagrantfile.multiple-platforms	added another vagrant file to enable cross platform testing; added su...					4 years ago	
flags-LICENSE.txt	initial commit					4 years ago	
install.sh	not on master					11 months ago	

<https://github.com/paralax/awesome-honeypots>

指令後續研究 - 6月

六月份			
類型	DDOS	挖礦	後門程式
次數	795	16	172

1	來源IP	最早觸發時間	最後觸發時間	國家	觸發次數
2	111. [REDACTED] 39	2018/6/7 01:14	2018/6/7 04:41	Taiwan	154
3	118. [REDACTED] 22	2018/6/6 01:56	2018/6/7 09:20	Taiwan	81
4	125. [REDACTED] 189	2018/6/1 04:07	2018/6/1 04:13	Taiwan	73
5	36.2 [REDACTED] 0	2018/6/13 04:13	2018/6/13 04:17	Taiwan	68
6	1.17 [REDACTED]	2018/6/25 19:19	2018/6/25 21:30	Taiwan	48
7	61.2 [REDACTED] 08	2018/6/22 04:46	2018/6/22 05:41	Taiwan	47
8	1.16 [REDACTED] 2	2018/6/20 14:37	2018/6/22 07:10	Taiwan	45
9	114. [REDACTED] 84	2018/6/1 04:08	2018/6/1 05:03	Taiwan	41
10	36.2 [REDACTED] 3	2018/6/4 04:47	2018/6/5 22:04	Taiwan	35
11	36.2 [REDACTED] 4	2018/6/10 21:52	2018/6/10 23:23	Taiwan	34
12	36.2 [REDACTED] 1	2018/6/4 02:51	2018/6/4 06:47	Taiwan	33
13	1.16 [REDACTED] 8	2018/6/27 18:23	2018/6/27 18:44	Taiwan	28
14	114. [REDACTED] 28	2018/6/17 05:42	2018/6/17 07:30	Taiwan	26
15	36.2 [REDACTED] 46	2018/6/5 20:15	2018/6/6 06:38	Taiwan	18
16	36.2 [REDACTED] 1	2018/6/23 09:52	2018/6/23 09:56	Taiwan	7
17	1.16 [REDACTED] 5	2018/6/28 20:47	2018/6/28 20:47	Taiwan	1

Q & A

