Cyber Security, Threat Hunting and Defense Challenge in Taiwan Academic Network

NCHC/TWCSIRT Research Fellow

Yi-Lang Tsai

Google Me.

- **Yi-Lang Tsai (蔡一郎)**
- **Research Fellow**, NCHC (National Center for High-performance Computing)
- **Leader**, TWCSIRT (Taiwan Computer Security Incident Response Team)
- **Leader**, Security Operation Center for NCHC (National Center for High-performance Computing)
- **Leader / Project Manager**, Security Operation Center for TANet (Taiwan Academic Network)
- **Leader**, The Honeynet Project Taiwan Chapter
- **Leader**, OWASP Taiwan Chapter
- **Leader**, Cloud Security Alliance Taiwan Chapter
- **Chairman**, Taiwan Cyber Security Alliance
- **Chairman**, **HoneyCon (Since 2009), CSA Taiwan Summit (Since 2013), IRCON (Since 2015)**
- **Director and Supervisors**, Academia-Industry Consortium For Southern Taiwan Science Park, AICSP
- **Supervisors**, Data Protection Association, CDPA
- **Director**, Digital Transformation Association, DTA
- **ISMS Auditor**, Taiwan Government annual auditing program
- **Freelance**, 35 Computer books and 80+ articles
- **Blog**, http://blog.yilang.org/
- **Facebook**, **LinkedIn**, Yi-Lang Tsai

Agenda

- About NCHC and TWCSIRT
- ISAC, CERT and SOC Framework
- Cyber Threat Hunting
- T.I.P design and development
- Case Study
  - Anti-DDoS in Academic Network
  - Malware Knowledge Database
  - Cyber Defense Exercise

About NCHC and TWCSIRT

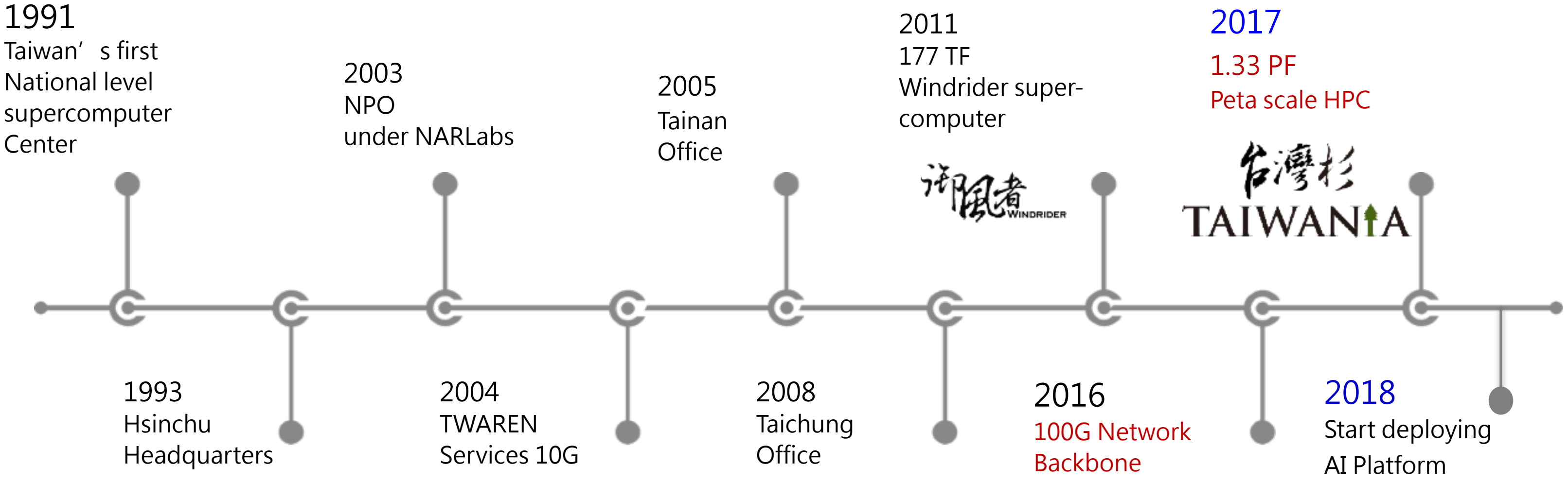
Vision and Mission for NCHC

Become a World-Class Supercomputing and Big Data Center

Enable Scientific Discoveries and Technical Innovation through prospective computing technology and platform

NCHC Milestones

A Member of NARLabs
National Center for
High-performance Computing



1991
Taiwan' s first
National level
supercomputer
Center

1993
Hsinchu
Headquarters

2003
NPO
under NARLabs

2004
TWAREN
Services 10G

2005
Tainan
Office

2008
Taichung
Office

2011
177 TF
Windrider super-computer

2016
100G Network
Backbone

2017
1.33 PF
Peta scale HPC

2018
Start deploying
AI Platform

Hsin Chu
Headquarters

Taichung Office

Tainan Office

Certifications

- ✓ ISO 9001:2015
- ✓ ISO 27001:2013
- ✓ CSA STAR Level 2 Gold Award
- ✓ BS 10012

台灣杉二號
TAIWANIA 2

台灣杉二號 TAIWANIA 2

Hardware - whole system

- 252 nodes / 9072 CPU cores /2016 GPUs
- 193.5 TB memory
- 10 PB storage
- EDR InfiniBand 100 Gbps
- 1.2 PUE (Warm Water Cooling)

Software Environment

- Slurm / Kubernetes
- Nvidia NGC Docker
- Ceph
- Spectrum Scale (GPFS)
- CentOS

Hardware - single node

- Intel Xeon Gold CPU x 2
- Nvidia Tesla V100 w/32GB x 8
- 768 GB memory
- 240 GB SSD + 4TB NVMe

AI Framework

- Tensorflow
- Caffé / Caffé 2
- PyTorch / Torch
- ……and more

Caffe2

PYTORCH

torch

NCHC NARLabs 財團法人國家實驗研究院
國家高速網路與計算中心
National Center for High-performance Computing

台灣杉二號 TAIWANIA 2

About TWCSIRT

- TWCSIRT Hosted by NCHC from 2014
- Since 2015 March become the Full Member in FIRST
- Join G-ISAC become the Full Member in Taiwan
- Locate in NCHC Tainan Business Unit.
- Vision and Mission
  - Handling information security incident in TWAREN (NCHC) and TANet (MOE)
  - Advanced information security research and framework development

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

About IRCON

- Issue analysis and information sharing to put cyber threats in control
- Establish TWCSIRT (Taiwan Computer Security Incident Response Team) to keep up with the international security organizations
- NCHC Host Taiwan Computer Security Incident Response Conference (IRCON) since 2015
- International Collaborations
  - TWCSIRT is the official member of the cyber security organization FIRST
  - Connect major organizations, CERT and CSIRT, for international cyber defense
  - Work with industry for information sharing and technology development

IRCON SUMMER CAMP 2018

27-30th AUGUST 2018

首頁
研討會
實作課程
交通資訊

08/27 CONFERENCE 研討會

08/28-29 WORKSHOP 實作課程

08/30 WARGAME

ACCESS 交通資訊

→ 前往線上報名 了解更多

→ 前往線上報名 了解更多

→ 前往線上報名 了解更多

→ 查看地圖 了解更多

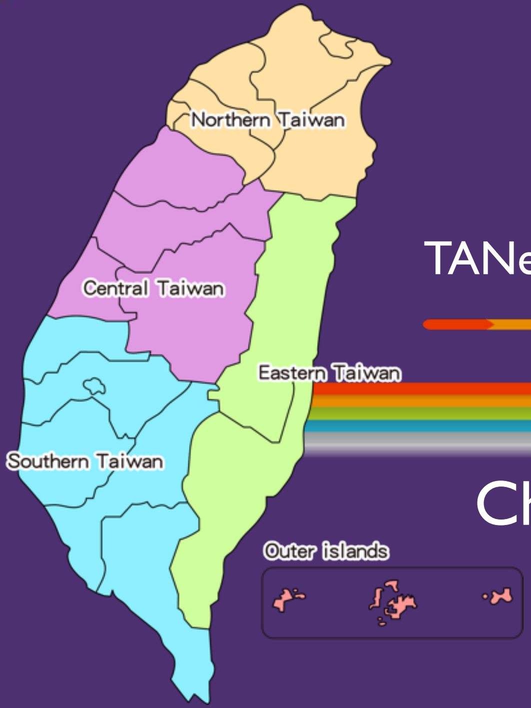
最新訊息 LATEST NEWS

Our Security Operation Center

- Operation: 7*24*365
- Scope:
  - NARLabs, National Applied Research Laboratories
    - 8 National Research Center
  - TWAREN, Taiwan Advanced Research & Education Network
    - 95 University
  - TANet, Taiwan Academic Network
    - 4000+ Schools
- Three-Tier Operation
  - 1st Line: 24 Operator
  - 2nd Line: 10 Engineer
  - 3rd Line: 3 Researcher

Cyber Threat Intelligence

Development Next Generation Network



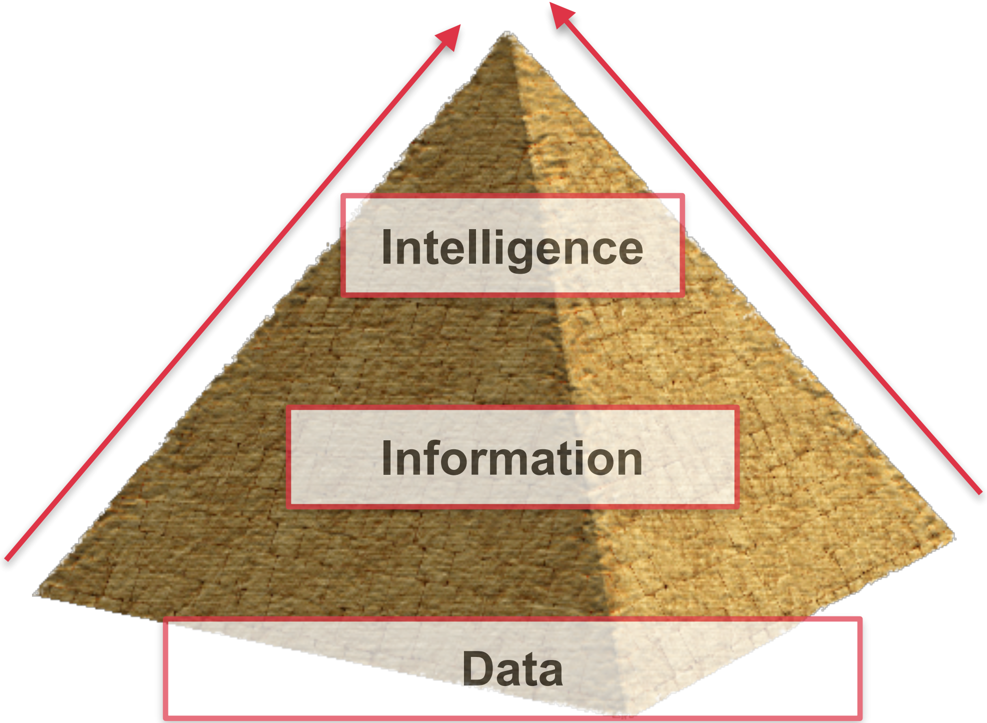
TANet & TWAREN

Challenges

- New Network Topology
- Bandwidth Upgrade 100Gbps
- Single Infrastructure and Multi Networking
- Continuous Operation
- Limited Budget

Threat Intelligence

- Attack
- Aggregation
- Analysis
- Action
- Automatic

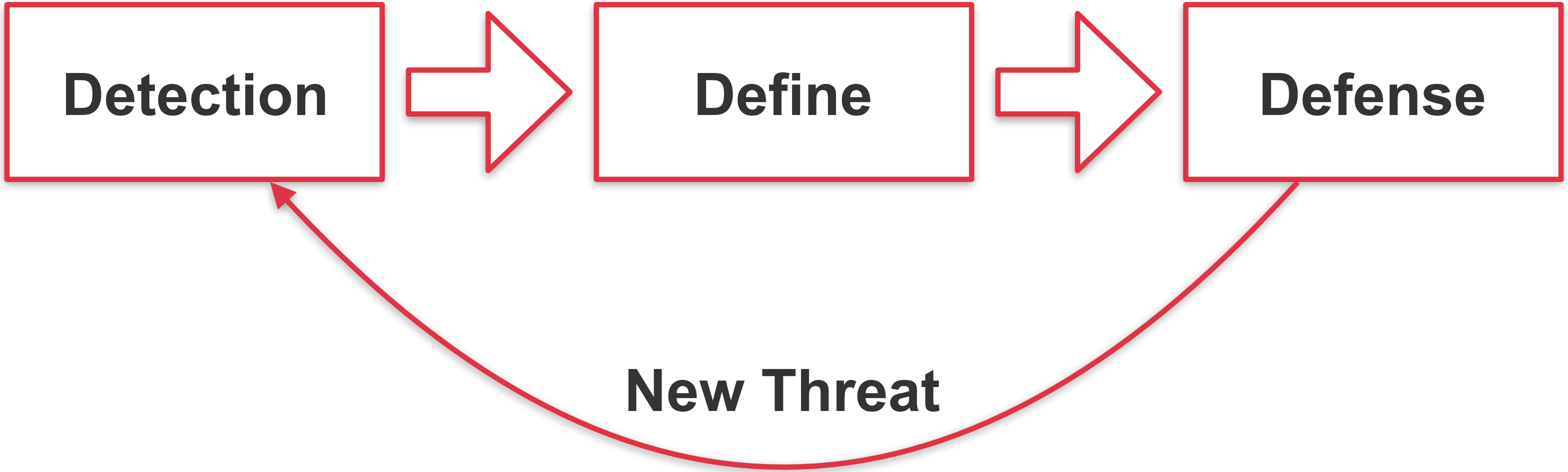


Intelligence

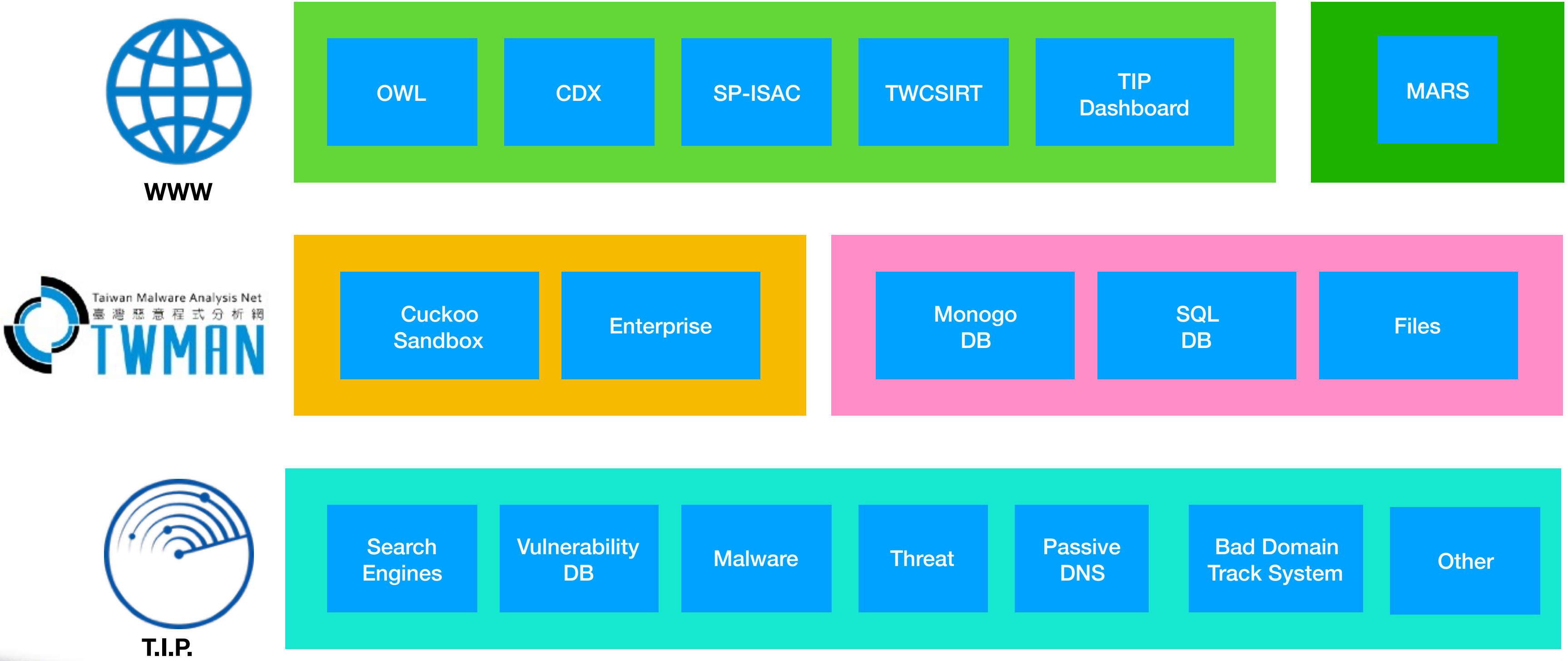
Information

Data

Eco System



Threat Intelligence Platform



WWW

- OWL
- CDX
- SP-ISAC
- TWCSIRT
- TIP Dashboard
- MARS

Taiwan Malware Analysis Net 臺灣惡意程式分析網 TWMAN

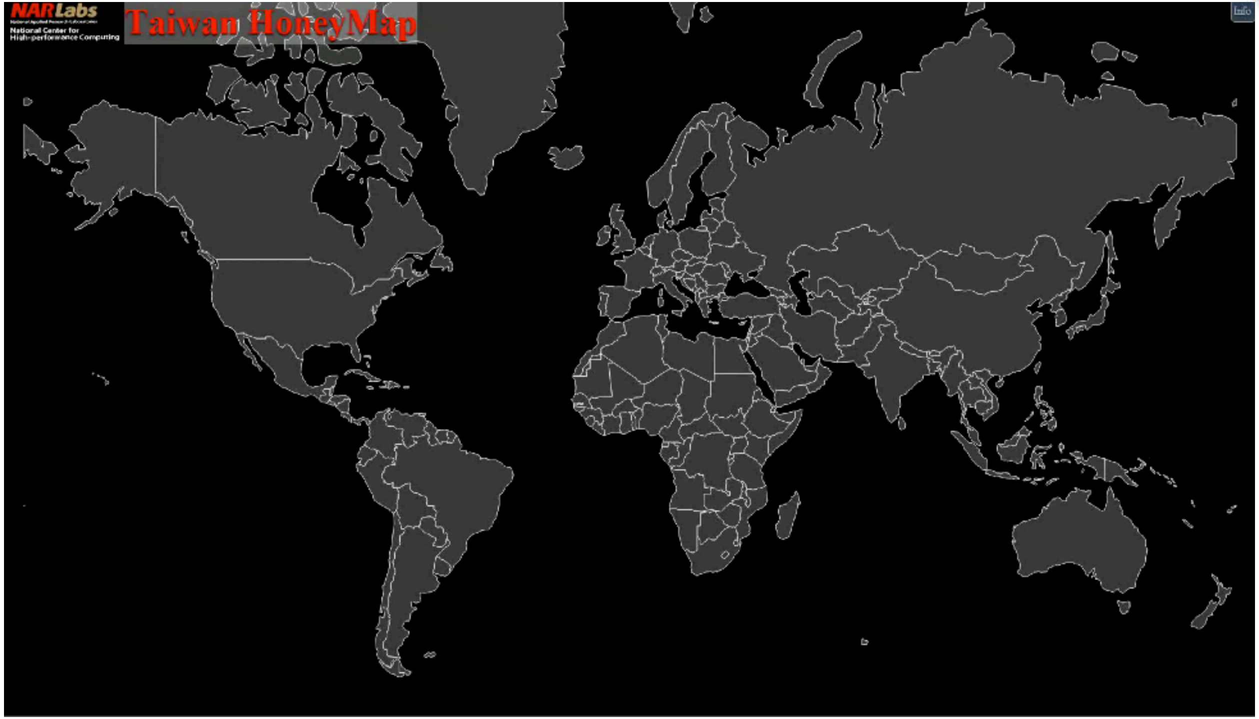
- Cuckoo Sandbox
- Enterprise
- Monogo DB
- SQL DB
- Files

T.I.P.

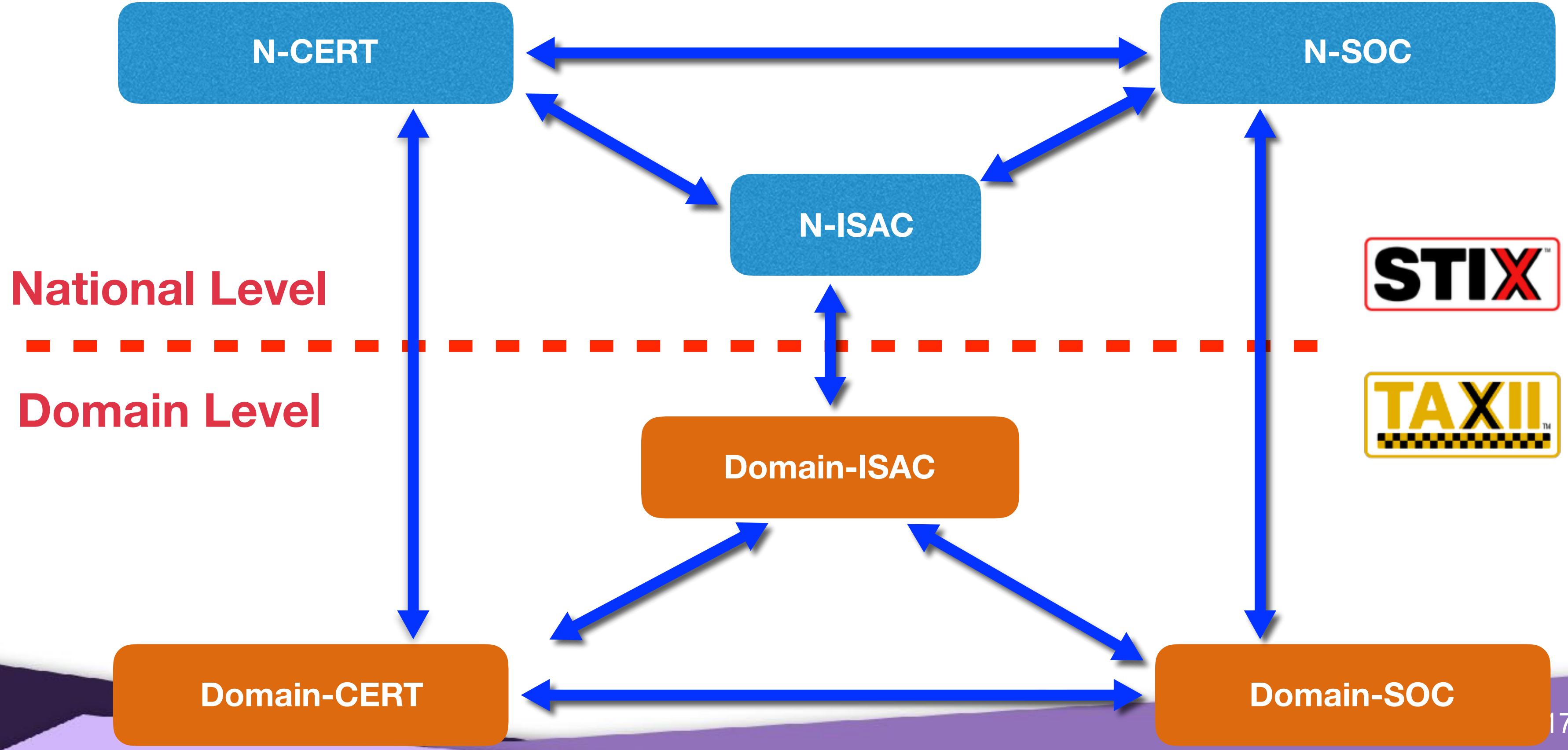
- Search Engines
- Vulnerability DB
- Malware
- Threat
- Passive DNS
- Bad Domain Track System
- Other

HoneyMap

- **Data Source**
  - Large Scale Honeypot / Honeynet in TANet and TWARE
  - Use 6000+ IPv4 address
- **Finding**
  - Commander & Controller (C2) Serve
  - Malware sample
  - Multi-Layer malware behaviors

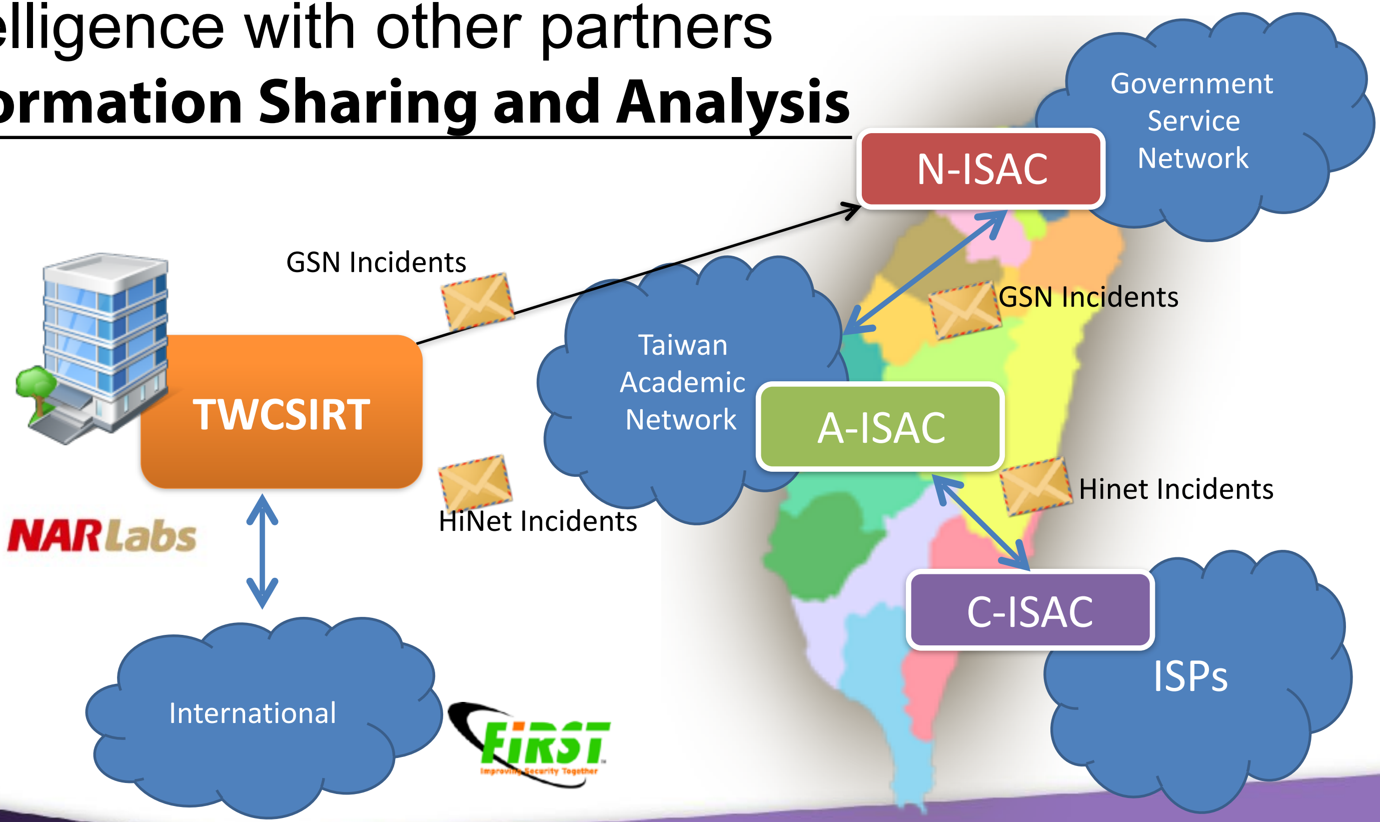


On going: ISAC、CERT、SOC



Information Sharing and Analysis

Sharing intelligence with other partners through **Information Sharing and Analysis Centers** .



Thinking

- How is addressing the issue of information sharing?

Data --> Information --> Intelligence

The Problem

- Attacks are becoming incredibly sophisticated.
- Know what happened is one thing.
- Knowing what to look for to see if it is happening to you - is key.
- ISAC's have had limited success
- ISAC model is segmented by vertical (Financial, Energy, etc.)
  - View across the sectors is critical to protecting companies
  - ISACs do not allow for a Cloud Segment

The Problem

- ISAC Model requires sending sensitive data to a trusted third party.
  - Company identity is know
  - Snowden incident has made sharing with trusted third parties undesirable
- Need is clear - a trusted method of sharing is required
  - Company identity is quick and simple
  - Incident data submission is quick and simple
  - Rapid analysis of data including correlation with other reports and open source data
  - Alerts sent in minutes, not days/weeks
  - Ability to anonymously discuss attacks with others and share solutions

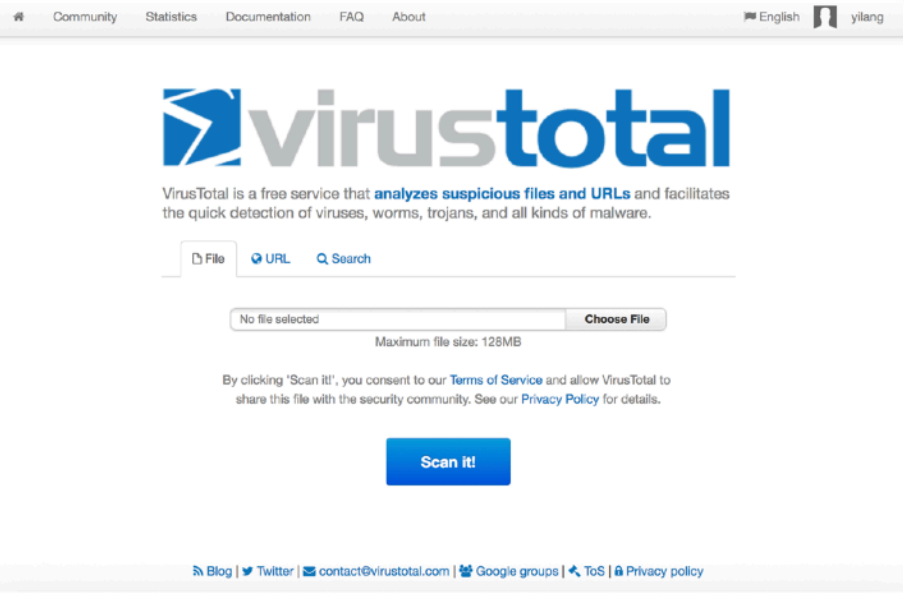
FIRST

- FIRST is the global Forum of Incident Response and Security Teams
- FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.
- FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

https://first.org/

VirusTotal

- VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google Inc. in September 2012
- VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives
- File、URL Analysis
- Threat and Risk



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Scan it!
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Case Study:

DDoS, Distributed Denial-of-Service

DDoS Attack IP Top 10

IP	Count	Protocol
140.128.173.213	14	UDP
210.60.208.166	14	UDP
210.59.63.250	11	UDP
192.192.100.2	10	UDP, ICMP, DNS_AMP, memcached_AMP
163.26.255.254	8	UDP
140.138.179.195	7	UDP, DNS_AMP, CLDAP_AMP
210.60.208.167	6	UDP
163.32.74.1	5	UDP, DNS_AMP, CLDAP_AMP
210.60.233.247	5	UDP, ICMP, CLDAP_AMP
120.115.60.54	4	UDP, ICMP, NTP_AMP, CLDAP_AMP

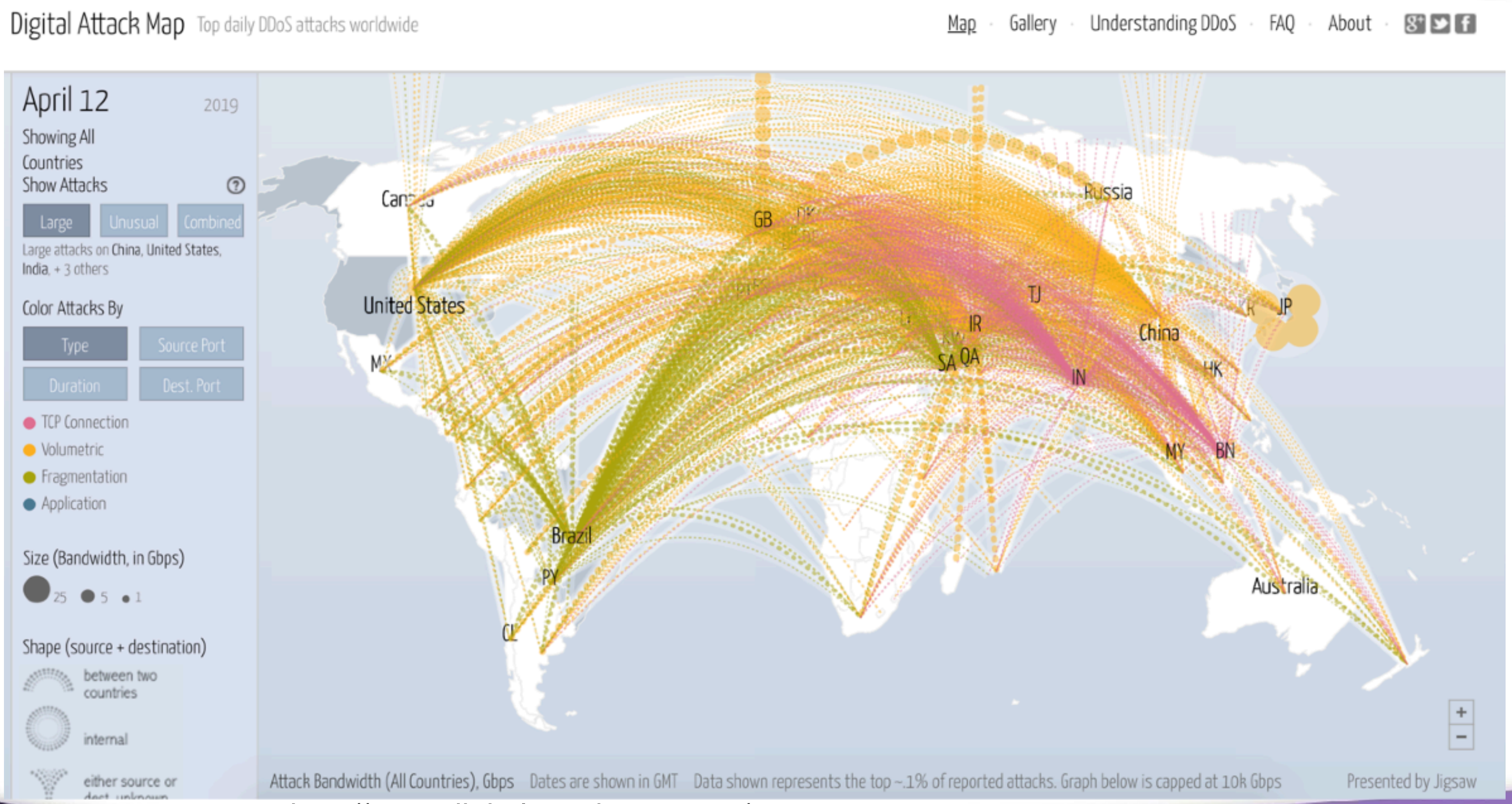
Data Range: 2019 April

DDoS Attack Protocol

Protocol	Count
TCP RST	403
UDP	180
IP Fragmentation	45
CLDAP Amplification	36
TCP SYN	18
ICMP	16
DNS Amplification	15
memcached Amplification	11
NTP Amplification	6

Data Range: 2019 April

Digital Attack Map



Digital Attack Map Top daily DDoS attacks worldwide

Map · Gallery · Understanding DDoS · FAQ · About

April 12 2019

Showing All Countries

Show Attacks

Large Unusual Combined

Large attacks on China, United States, India, + 3 others

Color Attacks By

Type Source Port Duration Dest. Port

- ● TCP Connection
- ● Volumetric
- ● Fragmentation
- ● Application

Size (Bandwidth, in Gbps)

● 25 ● 5 ● 1

Shape (source + destination)

between two countries

internal

either source or dest. unknown

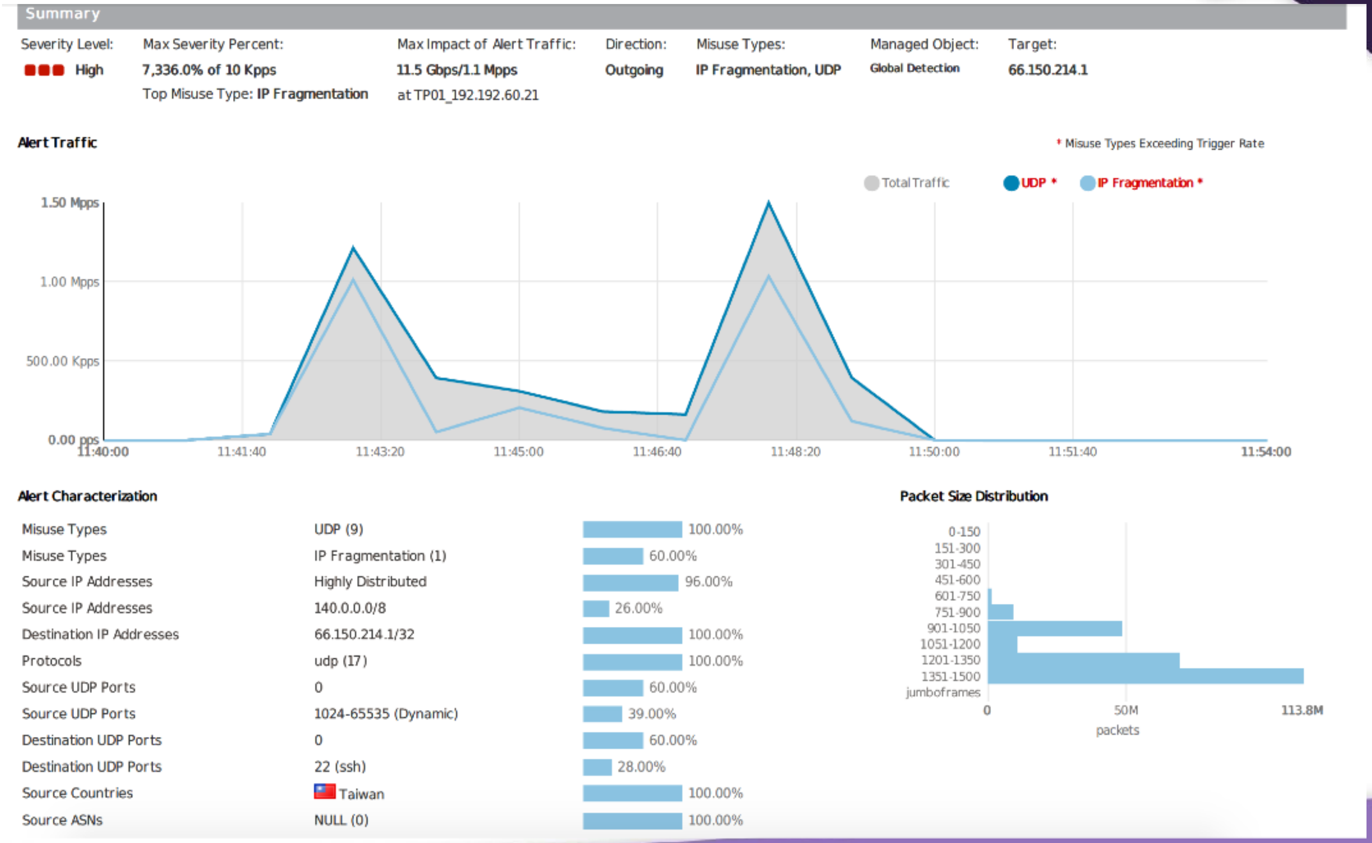
Attack Bandwidth (All Countries), Gbps Dates are shown in GMT Data shown represents the top ~.1% of reported attacks. Graph below is capped at 10k Gbps

Presented by Jigsaw

http://www.digitalattackmap.com/

DDoS Incident and Action

- Collection Netflow and learning baseline
- Normal vs. Abnormal
- Find attack model
- Do action in TMS to remove DDoS traffic
- Create incident ticket to ISAC system



Summary

Severity Level:	Max Severity Percent:	Max Impact of Alert Traffic:	Direction:	Misuse Types:	Managed Object:	Target:
■■■ High	7,336.0% of 10 Kpps Top Misuse Type: IP Fragmentation	11.5 Gbps/1.1 Mpps at TP01_192.192.60.21	Outgoing	IP Fragmentation, UDP	Global Detection	66.150.214.1

Alert Traffic

Alert Characterization

Misuse Types	UDP (9)	100.00%
Misuse Types	IP Fragmentation (1)	60.00%
Source IP Addresses	Highly Distributed	96.00%
Source IP Addresses	140.0.0.0/8	26.00%
Destination IP Addresses	66.150.214.1/32	100.00%
Protocols	udp (17)	100.00%
Source UDP Ports	0	60.00%
Source UDP Ports	1024-65535 (Dynamic)	39.00%
Destination UDP Ports	0	60.00%
Destination UDP Ports	22 (ssh)	28.00%
Source Countries	Taiwan	100.00%
Source ASNs	NULL (0)	100.00%

Packet Size Distribution

Hybrid Attack:SQL-Inject

Case Study:

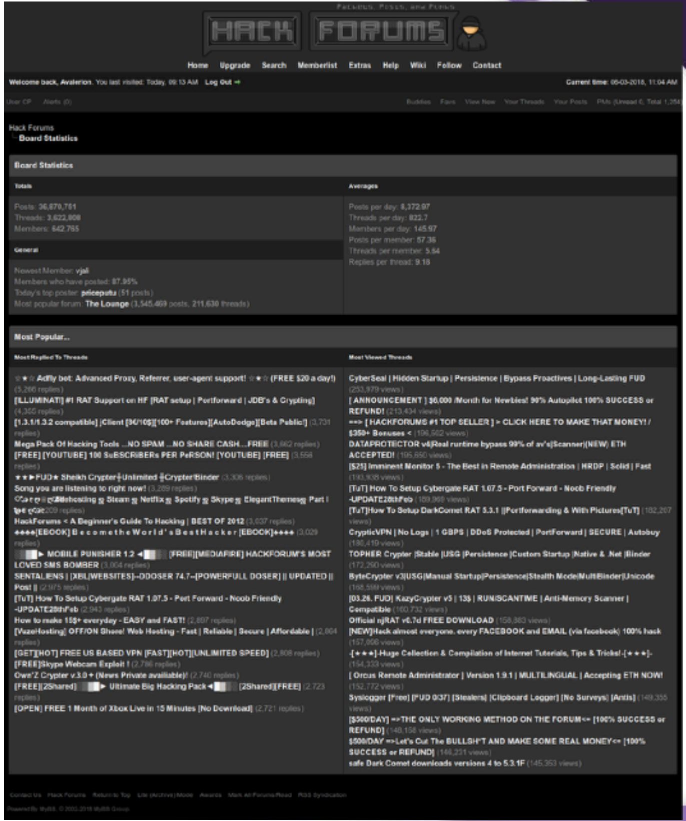
Malware KB

owl.nchc.org.tw

Example: Mirai

- Mirai (Japanese: 未來, lit. 'future') is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers.
- Mirai was used, alongside BASHLITE, in the DDoS attack on 20 September 2016 on the Krebs on Securitysite which reached **620 Gbit/s**. Ars Technica also reported a **1 Tbit/s** attack on French web host OVH. On 21 October 2016 multiple major DDoS attacks in DNS services of DNS service provider Dyn occurred using Mirai malware installed on a large number of IoT devices, resulting in the inaccessibility of several high-profile websites such as GitHub, Twitter, Reddit, Netflix, Airbnb and many others. The attribution of the Dyn attack to the Mirai botnet was originally reported by Level 3 Communications.

source: wikipedia



Welcome back, Avalerion. You last visited: Today, 09:13 AM Log Out

Current time: 05-03-2018, 11:04 AM

Hack Forums
Board Statistics

Board Statistics

Totals

Posts: 36,870,751
Threads: 3,622,808
Members: 642,765

General

Newest Member: vjali
Members who have posted: 87.95%
Today's top poster: pricepufu (51 posts)
Most popular forum: The Lounge (3,545,469 posts, 211,630 threads)

Averages

Posts per day: 8,372.97
Threads per day: 822.7
Members per day: 145.97
Posts per member: 57.36
Threads per member: 5.64
Replies per thread: 9.18

Most Popular...

Most Replied To Threads

☆★☆ Adfly bot: Advanced Proxy, Referrer, user-agent support! ☆★☆ (FREE $20 a day!) (5,266 replies)
[ILLUMINATI] #1 RAT Support on HF [RAT setup | Portforward | JDB's & Crypting] (4,355 replies)
[1.3.1/1.3.2 compatible] jClient [9€/10$][100+ Features][AutoDodge][Beta Public!] (3,731 replies)
Mega Pack Of Hacking Tools ...NO SPAM ...NO SHARE CASH....FREE (3,662 replies)
[FREE] [YOUTUBE] 100 SuBSCRIBERs PER PeRSON! [YOUTUBE] [FREE] (3,556 replies)
★★►FUD★ Sheikh Crypter╬Unlimited ╬Crypter/Binder (3,306 replies)
Song you are listening to right now! (3,289 replies)
Webhosting Steam Netflix Spotify Skype ElegantThemes Part I (3,209 replies)
HackForums < A Beginner's Guide To Hacking | BEST OF 2012 (3,037 replies)
♣♣♣♣[EBOOK] Become the World's Best Hacker [EBOOK]♣♣♣♣ (3,029 replies)
► MOBILE PUNISHER 1.2 ◄ [FREE][MEDIAFIRE] HACKFORUM'S MOST LOVED SMS BOMBER (3,004 replies)
SENTALIENS | [XBL/WEBSITES]--DDOSER 74.7--[POWERFULL DOSER] || UPDATED || Post! || (2,975 replies)
[TuT] How To Setup Cybergate RAT 1.07.5 - Port Forward - Noob Friendly -UPDATE28thFeb (2,943 replies)
How to make 15$+ everyday - EASY and FAST! (2,897 replies)
[VazeHosting] OFF/ON Shore! Web Hosting - Fast | Reliable | Secure | Affordable | (2,864 replies)
[GET][HOT] FREE US BASED VPN [FAST][HOT][UNLIMITED SPEED] (2,808 replies)
[FREE]Skype Webcam Exploit ! (2,786 replies)
Own'Z Crypter v.3.0 + (News Private available)! (2,740 replies)
[FREE][2Shared] ► Ultimate Big Hacking Pack ◄ [2Shared][FREE] (2,723 replies)
[OPEN] FREE 1 Month of Xbox Live in 15 Minutes [No Download] (2,721 replies)

Most Viewed Threads

CyberSeal | Hidden Startup | Persistence | Bypass Proactives | Long-Lasting FUD (253,979 views)
[ANNOUNCEMENT] $6,000 /Month for Newbies! 90% Autopilot 100% SUCCESS or REFUND! (213,434 views)
==> [HACKFORUMS #1 TOP SELLER] > CLICK HERE TO MAKE THAT MONEY! / $350+ Bonuses < (196,502 views)
DATAPROTECTOR v4|Real runtime bypass 99% of av's|Scanner|(NEW) ETH ACCEPTED! (195,850 views)
[$25] Imminent Monitor 5 - The Best in Remote Administration | HRDP | Solid | Fast (193,938 views)
[TuT] How To Setup Cybergate RAT 1.07.5 - Port Forward - Noob Friendly -UPDATE28thFeb (189,969 views)
[TuT]How To Setup DarkComet RAT 5.3.1 ||Portforwarding & With Pictures[TuT] (182,207 views)
CrypticVPN | No Logs | 1 GBPS | DDoS Protected | PortForward | SECURE | Autobuy (186,419 views)
TOPHER Crypter |Stable |USG |Persistence |Custom Startup |Native & .Net |Binder (172,290 views)
ByteCrypter v3|USG|Manual Startup|Persistence|Stealth Mode|MultiBinder|Unicode (168,598 views)
[03.26. FUD] KazyCrypter v5 | 13$ | RUN/SCANTIME | Anti-Memory Scanner | Compatible (160,732 views)
Official njRAT v0.7d FREE DOWNLOAD (158,383 views)
[NEW]Hack almost everyone. every FACEBOOK and EMAIL (via facebook) 100% hack (157,096 views)
-[★★★]-Huge Collection & Compilation of Internet Tutorials, Tips & Tricks!-[★★★]- (154,333 views)
[Orcus Remote Administrator | Version 1.9.1 | MULTILINGUAL | Accepting ETH NOW! (152,772 views)
Syslogger [Free] [FUD 0/37] [Stealers] [Clipboard Logger] [No Surveys] [Antis] (149,355 views)
[$500/DAY] =>THE ONLY WORKING METHOD ON THE FORUM<= [100% SUCCESS or REFUND] (148,158 views)
$500/DAY =>Let's Cut The BULLSH*T AND MAKE SOME REAL MONEY<= [100% SUCCESS or REFUND] (146,231 views)
safe Dark Comet downloads versions 4 to 5.3.1F (145,353 views)

Mirai Infections

- Average Volume :
  - 100,000 - 200,000 IPv4 addresses per day
- Update Frequency : Daily
  - for the previous day generation at 12:00 (UTC time)
  - provided as a gzip-encoded text file in CSV format

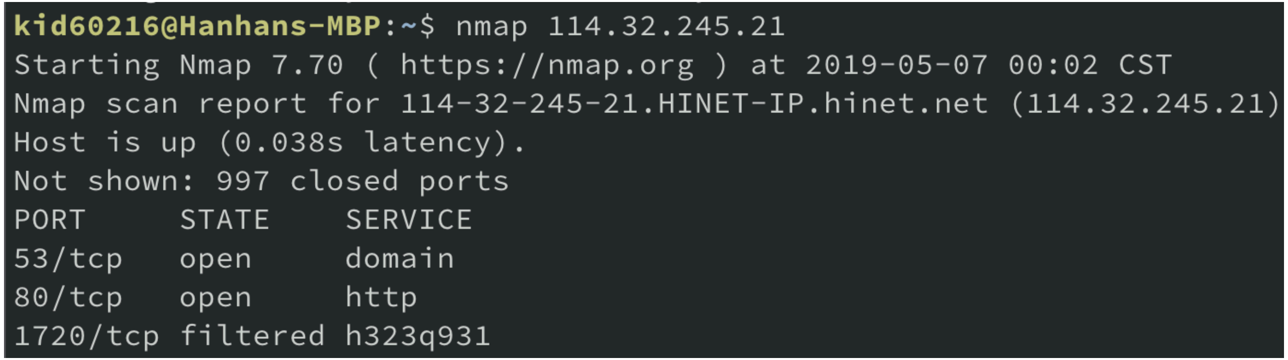
#	Field Name	Data Type	Description
1	ip	IPv4 address	Botnet IPs
2	time	datetime	Time when Datafeed Generate

Mirai Infections

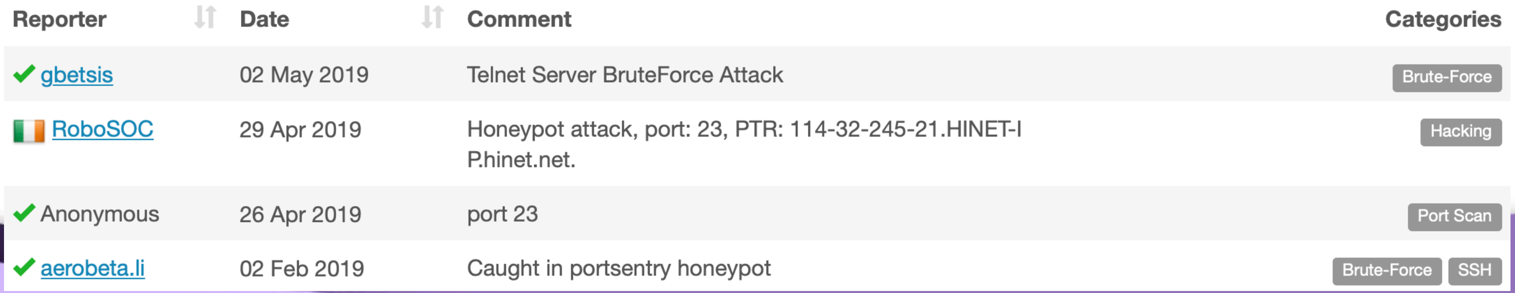
- Sample Data
  - 179.182.231.78,2019-05-09 23:59:59
  - 181.110.164.140,2019-05-09 23:59:59
  - 114.32.245.21,2019-05-09 23:59:59
  - 197.59.251.0,2019-05-09 23:59:59
  - 197.53.124.140,2019-05-09 23:59:59
  - 183.193.234.190,2019-05-09 23:59:59
  - 197.39.200.103,2019-05-09 23:59:59
  - 5.139.58.158,2019-05-09 23:59:59
  - 201.95.65.79,2019-05-09 23:59:59
  - 156.210.142.162,2019-05-09 23:59:59
  - 42.227.192.58,2019-05-09 23:59:59

Mirai Infections

- 114.32.245.21,TW,,TAIPEI,3462



```
kid60216@Hanhans-MBP:~$ nmap 114.32.245.21
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-07 00:02 CST
Nmap scan report for 114-32-245-21.HINET-IP.hinet.net (114.32.245.21)
Host is up (0.038s latency).
Not shown: 997 closed ports
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   open     http
1720/tcp filtered h323q931
```



Reporter	Date	Comment	Categories
✓ gbetsis	02 May 2019	Telnet Server BruteForce Attack	Brute-Force
🇮🇪 RoboSOC	29 Apr 2019	Honeypot attack, port: 23, PTR: 114-32-245-21.HINET-IP.hinet.net.	Hacking
✓ Anonymous	26 Apr 2019	port 23	Port Scan
✓ aerobeta.li	02 Feb 2019	Caught in portsentry honeypot	Brute-Force SSH

Malware Knowledge Base in Taiwan

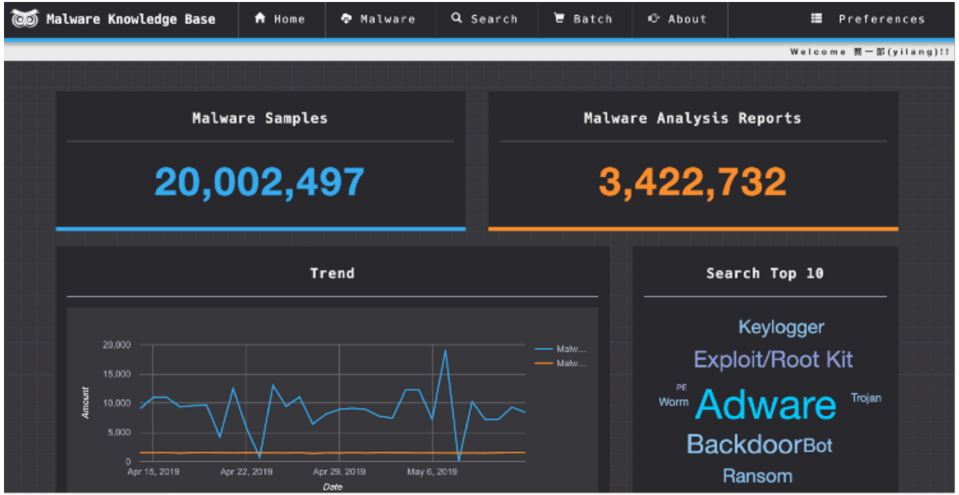
Malware Knowledge Base, hosted by the National Center for High-performance Computing, is a malware analysis platform that observes and records system behaviors conducted by analysis objects in a controlled environment with various types of dynamic analysis tools.

The mission of Malware Knowledge Base is to strengthen malware research and promote security innovations in both academia and industry.

By providing malware-related resources, Malware Knowledge Base can contribute to security research and make the Internet a safer place.

Malware Knowledge Base

- Build the behavior analysis of the network threat and malware
- Only malware behavior database in Taiwan
  - Collect 20+ M malware samples
  - Provide malware samples, analysis reports, and search functions
- Build entrapment platform to detect attacks
  - 6,000+ entrapment systems
  - Collect about 65GB/day data
- Around the clock cyber security defense
  - 7*24*365 security operation center(SOC)
  - Average 15,000/mo. security issues
  - Hold active/passive detect system
  - Self developed information feedback mechanism, enhance cyber security defense



Welcome 葉一郎(yilang)!!

Malware Samples

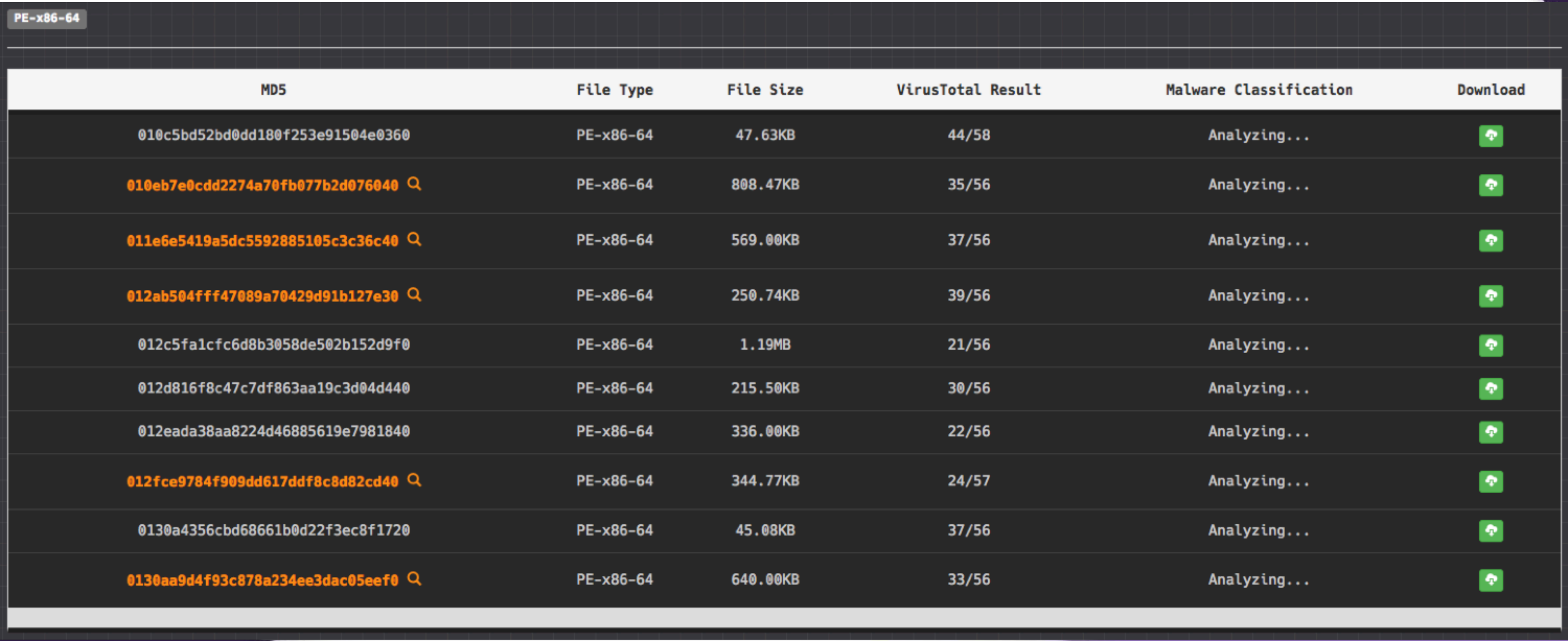
20,002,497

Malware Analysis Reports

3,422,732

https://owl.nchc.org.tw

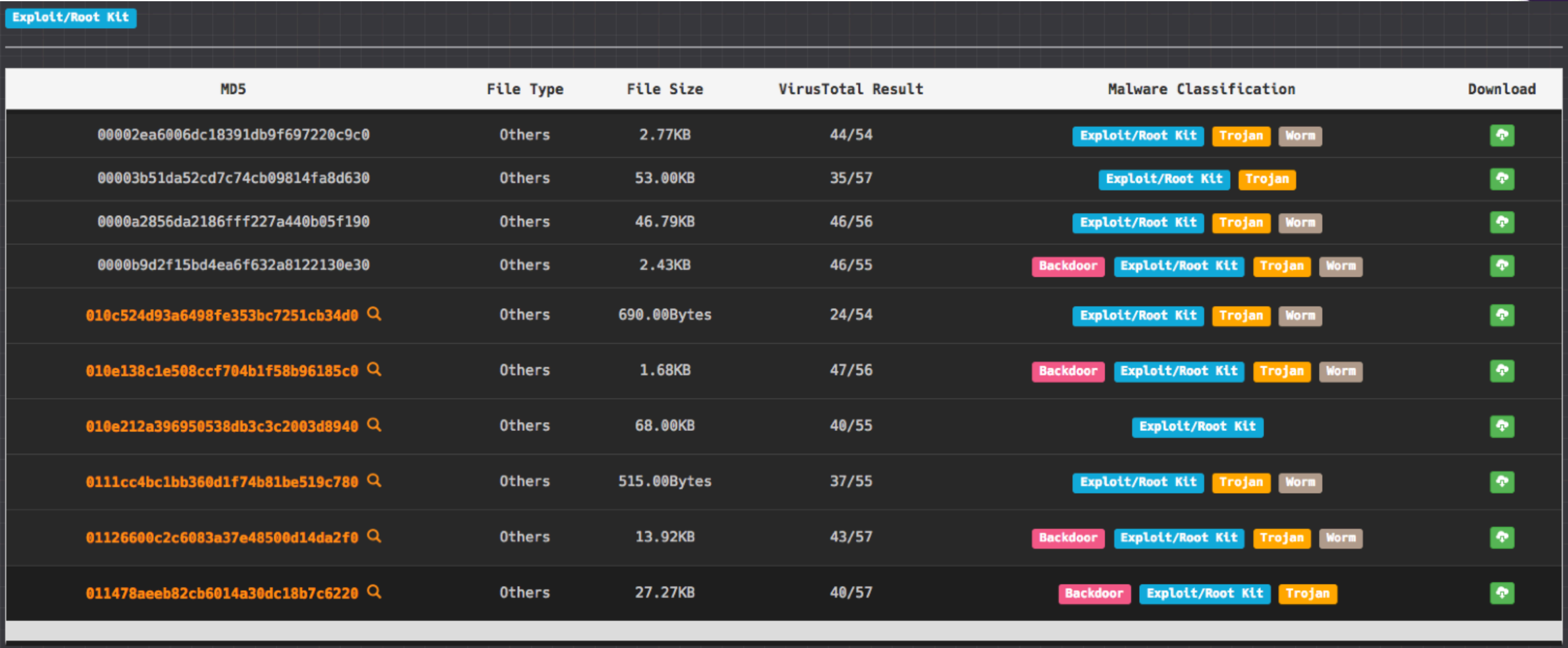
Malware KB: PE-x86-64



PE-x86-64

MD5	File Type	File Size	VirusTotal Result	Malware Classification	Download
010c5bd52bd0dd180f253e91504e0360	PE-x86-64	47.63KB	44/58	Analyzing...	⬇
010eb7e0cdd2274a70fb077b2d076040 🔍	PE-x86-64	808.47KB	35/56	Analyzing...	⬇
011e6e5419a5dc5592885105c3c36c40 🔍	PE-x86-64	569.00KB	37/56	Analyzing...	⬇
012ab504fff47089a70429d91b127e30 🔍	PE-x86-64	250.74KB	39/56	Analyzing...	⬇
012c5fa1cfc6d8b3058de502b152d9f0	PE-x86-64	1.19MB	21/56	Analyzing...	⬇
012d816f8c47c7df863aa19c3d04d440	PE-x86-64	215.50KB	30/56	Analyzing...	⬇
012eada38aa8224d46885619e7981840	PE-x86-64	336.00KB	22/56	Analyzing...	⬇
012fce9784f909dd617ddf8c8d82cd40 🔍	PE-x86-64	344.77KB	24/57	Analyzing...	⬇
0130a4356cbd68661b0d22f3ec8f1720	PE-x86-64	45.08KB	37/56	Analyzing...	⬇
0130aa9d4f93c878a234ee3dac05eef0 🔍	PE-x86-64	640.00KB	33/56	Analyzing...	⬇

Malware KB: Exploit/Root Kit



Exploit/Root Kit

MD5	File Type	File Size	VirusTotal Result	Malware Classification	Download
00002ea6006dc18391db9f697220c9c0	Others	2.77KB	44/54	Exploit/Root Kit Trojan Worm	☁
00003b51da52cd7c74cb09814fa8d630	Others	53.00KB	35/57	Exploit/Root Kit Trojan	☁
0000a2856da2186fff227a440b05f190	Others	46.79KB	46/56	Exploit/Root Kit Trojan Worm	☁
0000b9d2f15bd4ea6f632a8122130e30	Others	2.43KB	46/55	Backdoor Exploit/Root Kit Trojan Worm	☁
010c524d93a6498fe353bc7251cb34d0 🔍	Others	690.00Bytes	24/54	Exploit/Root Kit Trojan Worm	☁
010e138c1e508ccf704b1f58b96185c0 🔍	Others	1.68KB	47/56	Backdoor Exploit/Root Kit Trojan Worm	☁
010e212a396950538db3c3c2003d8940 🔍	Others	68.00KB	40/55	Exploit/Root Kit	☁
0111cc4bc1bb360d1f74b81be519c780 🔍	Others	515.00Bytes	37/55	Exploit/Root Kit Trojan Worm	☁
01126600c2c6083a37e48500d14da2f0 🔍	Others	13.92KB	43/57	Backdoor Exploit/Root Kit Trojan Worm	☁
011478aeeb82cb6014a30dc18b7c6220 🔍	Others	27.27KB	40/57	Backdoor Exploit/Root Kit Trojan	☁

Case Study:

Cyber Defense eXercise

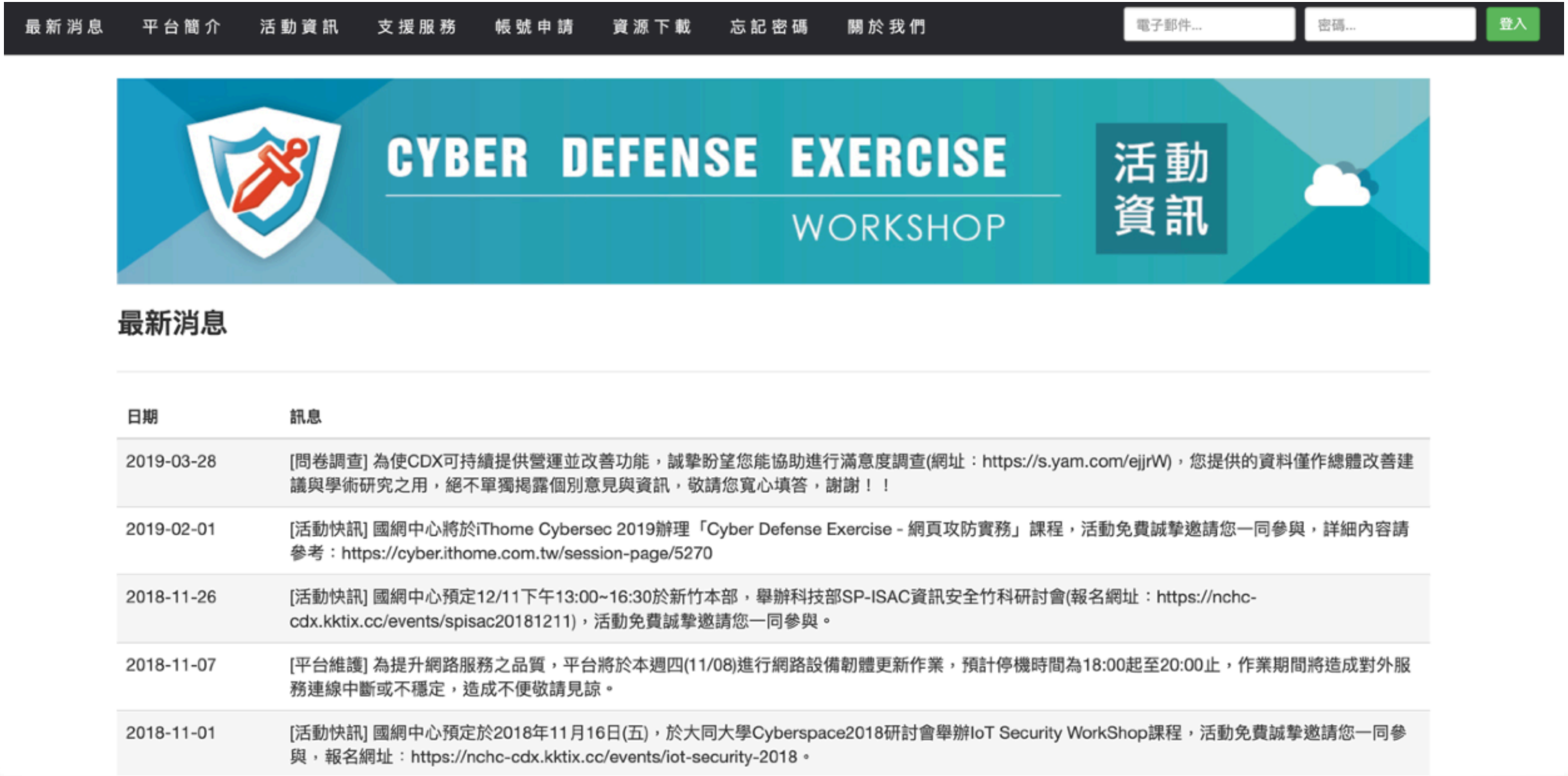
cdx.nchc.org.tw

Cyber Defense eXercise

- **Training**
  - Cloud-based training and challenge platform for cyber security
  - Start and Setup training course environment in 90 seconds
  - On-Demond to chose different template for learning
  - Over 150+ vulnerability virtual machine
  - Design and Deployment very easy
  - Full time services for on-line learning
- **Challenge**
  - CTF and King of the Hill
  - Cross multi-domain to setup the environment
    - Red Team Testing
    - Blue Team Defense
    - Internet of Things
    - Cyber Physics System for Industry IoT

CDX
Cyber Defense Exercise

CDX Website v1

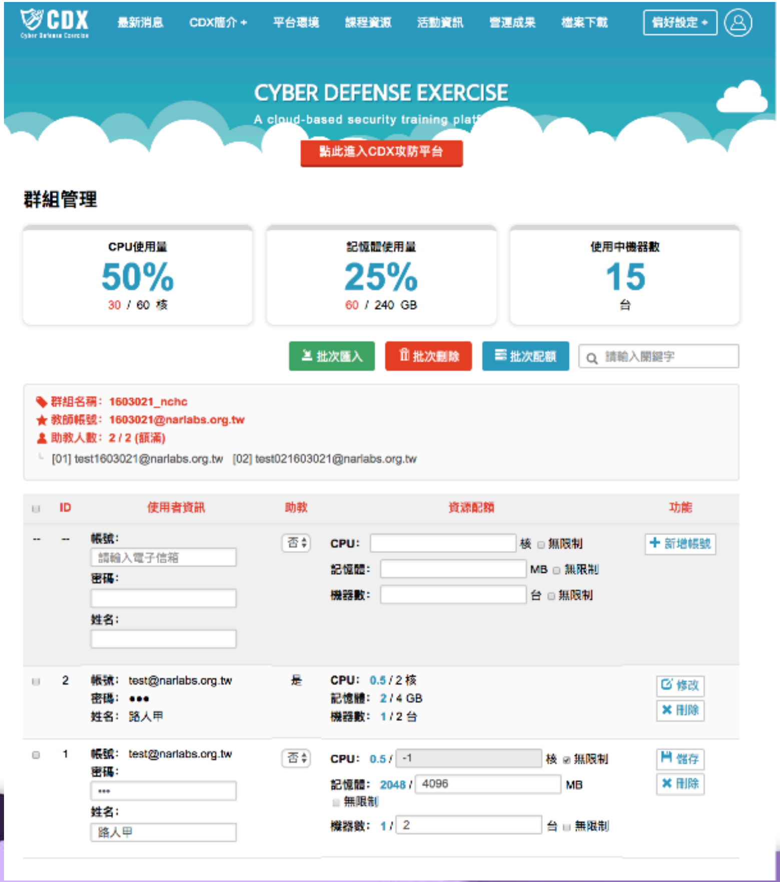


最新消息

日期	訊息
2019-03-28	[問卷調查] 為使CDX可持續提供營運並改善功能，誠摯盼望您能協助進行滿意度調查(網址：https://s.yam.com/ejjrW)，您提供的資料僅作總體改善建議與學術研究之用，絕不單獨揭露個別意見與資訊，敬請您寬心填答，謝謝！！
2019-02-01	[活動快訊] 國網中心將於iThome Cybersec 2019辦理「Cyber Defense Exercise - 網頁攻防實務」課程，活動免費誠摯邀請您一同參與，詳細內容請參考：https://cyber.ithome.com.tw/session-page/5270
2018-11-26	[活動快訊] 國網中心預定12/11下午13:00~16:30於新竹本部，舉辦科技部SP-ISAC資訊安全竹科研討會(報名網址：https://nchc-cdx.kktix.cc/events/spisac20181211)，活動免費誠摯邀請您一同參與。
2018-11-07	[平台維護] 為提升網路服務之品質，平台將於本週四(11/08)進行網路設備韌體更新作業，預計停機時間為18:00起至20:00止，作業期間將造成對外服務連線中斷或不穩定，造成不便敬請見諒。
2018-11-01	[活動快訊] 國網中心預定於2018年11月16日(五)，於大同大學Cyberspace2018研討會舉辦IoT Security WorkShop課程，活動免費誠摯邀請您一同參與，報名網址：https://nchc-cdx.kktix.cc/events/iot-security-2018。

https://cdx.nchc.org.tw/

CDX Website v2

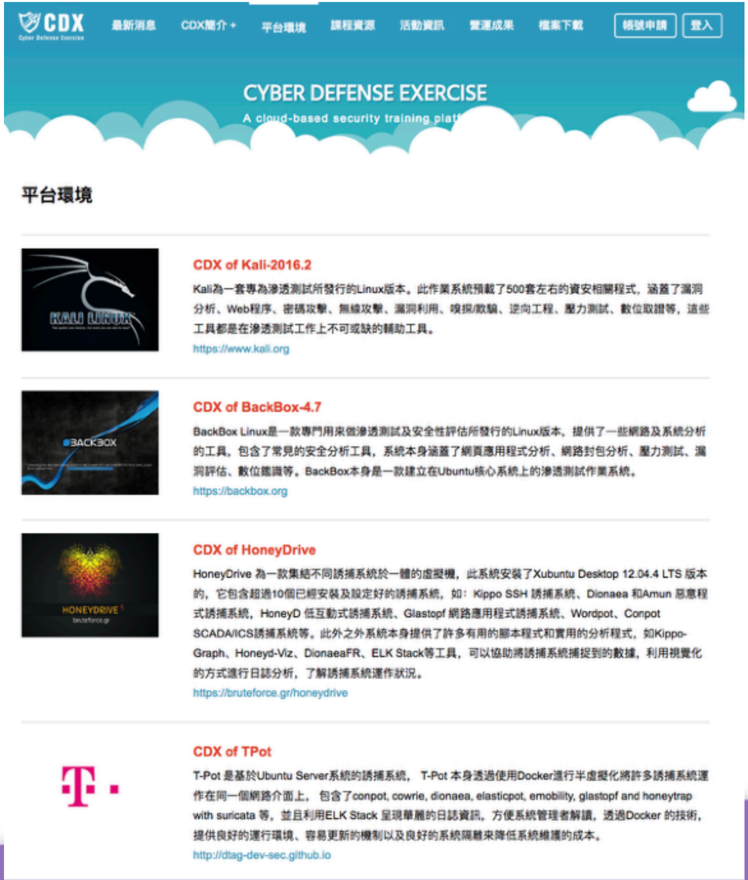


群組管理

CPU使用量	記憶體使用量	使用中機器數
50%	25%	15
30 / 60 核	60 / 240 GB	台

群組名稱：1603021_nchc
教師帳號：1603021@narlabs.org.tw
助教人數：2 / 2 (額滿)
[01] test1603021@narlabs.org.tw [02] test021603021@narlabs.org.tw

□	ID	使用者資訊	助教	資源配額	功能
--	--	帳號：請輸入電子信箱 密碼： 姓名：	否	CPU： 核 □ 無限制 記憶體： MB □ 無限制 機器數： 台 □ 無限制	+ 新增帳號
□	2	帳號：test@narlabs.org.tw 密碼：●●● 姓名：路人甲	是	CPU：0.5 / 2 核 記憶體：2 / 4 GB 機器數：1 / 2 台	修改 刪除
□	1	帳號：test@narlabs.org.tw 密碼：••• 姓名：路人甲	否	CPU：0.5 / -1 核 ☑ 無限制 記憶體：2048 / 4096 MB □ 無限制 機器數：1 / 2 台 □ 無限制	儲存 刪除



平台環境

CDX of Kali-2016.2

Kali為一套專為滲透測試所發行的Linux版本。此作業系統預載了500套左右的資安相關程式，涵蓋了漏洞分析、Web程序、密碼攻擊、無線攻擊、漏洞利用、嗅探/欺騙、逆向工程、壓力測試、數位取證等，這些工具都是在滲透測試工作上不可或缺的輔助工具。

https://www.kali.org

CDX of BackBox-4.7

BackBox Linux是一款專門用來做滲透測試及安全性評估所發行的Linux版本，提供了一些網路及系統分析的工具，包含了常見的安全分析工具，系統本身涵蓋了網頁應用程式分析、網路封包分析、壓力測試、漏洞評估、數位鑑識等。BackBox本身是一款建立在Ubuntu核心系統上的滲透測試作業系統。

https://backbox.org

CDX of HoneyDrive

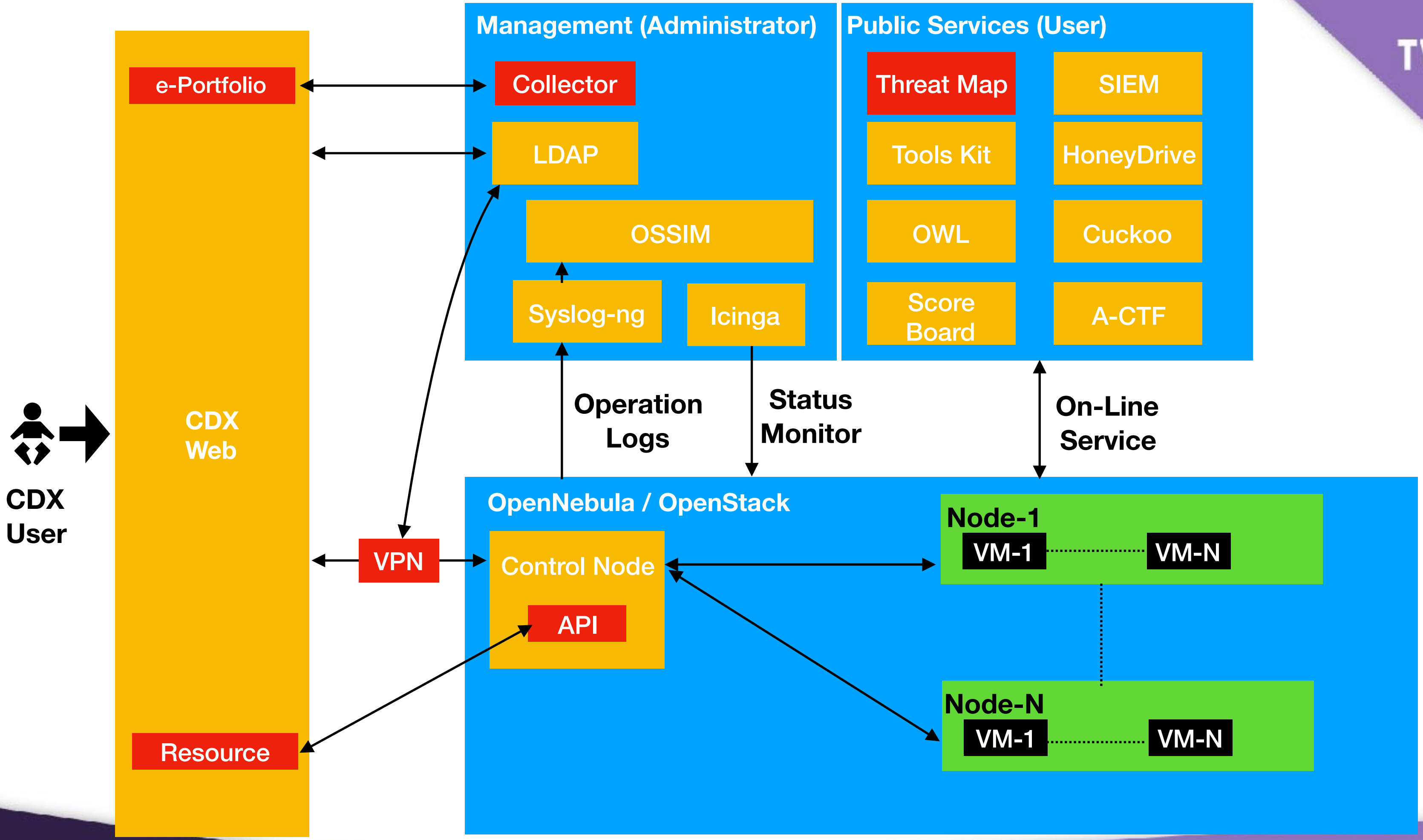
HoneyDrive 為一款集結不同誘捕系統於一體的虛擬機，此系統安裝了Xubuntu Desktop 12.04.4 LTS 版本的，它包含超過10個已經安裝及設定好的誘捕系統，如：Kippo SSH 誘捕系統、Dionaea 和Amun 惡意程式誘捕系統，HoneyD 低互動式誘捕系統、Glastopf 網路應用程式誘捕系統、Wordpot、Conpot SCADA/ICS誘捕系統等。此外之外系統本身提供了許多有用的腳本程式和實用的分析程式，如Kippo-Graph、Honeyd-Viz、DionaeaFR、ELK Stack等工具，可以協助將誘捕系統捕捉到的數據，利用視覺化的方式進行日誌分析，了解誘捕系統運作狀況。

https://bruteforce.gr/honeydrive

CDX of TPot

T-Pot 是基於Ubuntu Server系統的誘捕系統， T-Pot 本身透過使用Docker進行半虛擬化將許多誘捕系統運作在同一個網路介面上， 包含了conpot, cowrie, dionaea, elasticpot, emobility, glastopf and honeytrap with suricata 等，並且利用ELK Stack 呈現華麗的日誌資訊，方便系統管理者解讀，透過Docker 的技術，提供良好的運行環境、容易更新的機制以及良好的系統隔離來降低系統維護的成本。

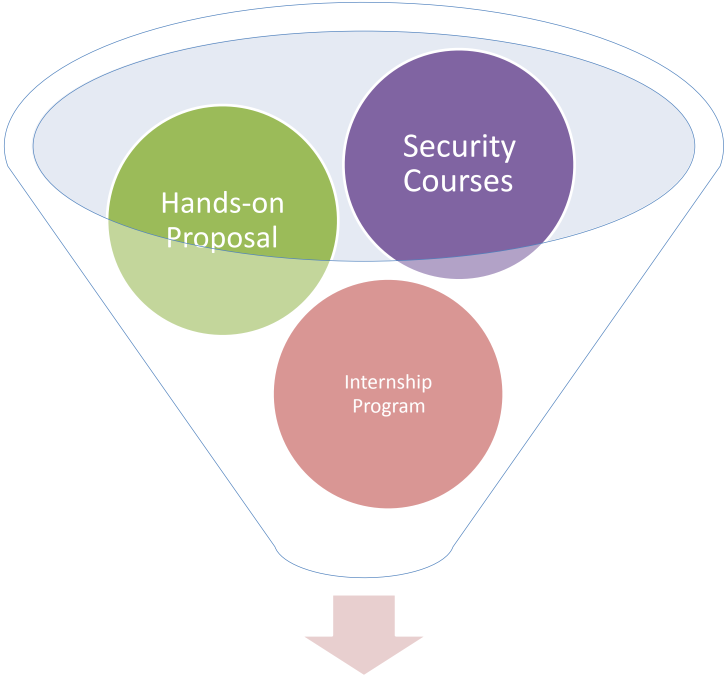
http://dtag-dev-sec.github.io


Management (Administrator)
Collector
LDAP
OSSIM
Syslog-ng
Icinga
Public Services (User)
Threat Map
SIEM
Tools Kit
HoneyDrive
OWL
Cuckoo
Score Board
A-CTF
e-Portfolio
CDX Web
Resource
CDX User
VPN
Operation Logs
Status Monitor
On-Line Service
OpenNebula / OpenStack
Control Node
API
Node-1
VM-1
VM-N
Node-N
VM-1
VM-N

TWCSIRT

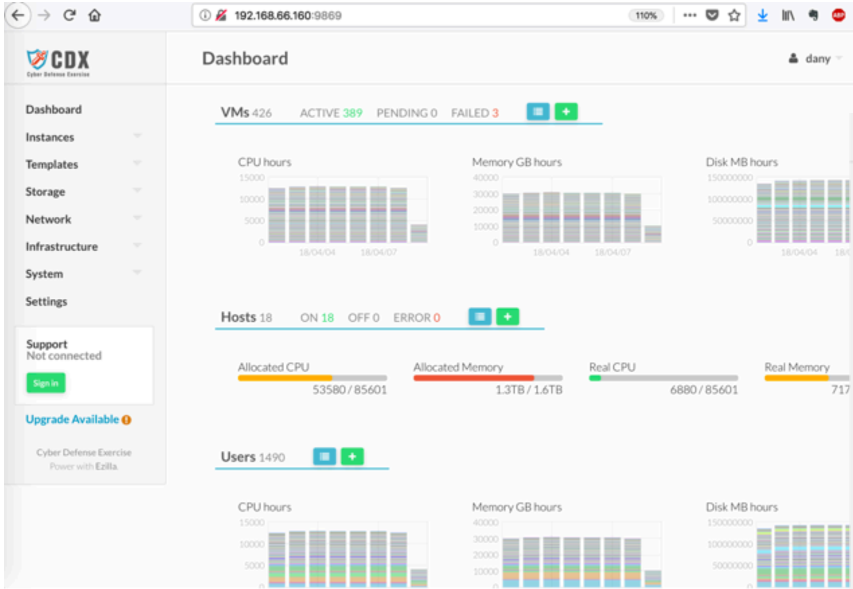
InfoSec Education Program

- Working with academic institutes, regional network centers and universities to provide opportunities for students to learn information security skills and get involved with security projects.



InfoSec Education

Management / Operation



Dashboard

VMs 426 ACTIVE 389 PENDING 0 FAILED 3

Hosts 18 ON 18 OFF 0 ERROR 0

Allocated CPU 53580 / 85601

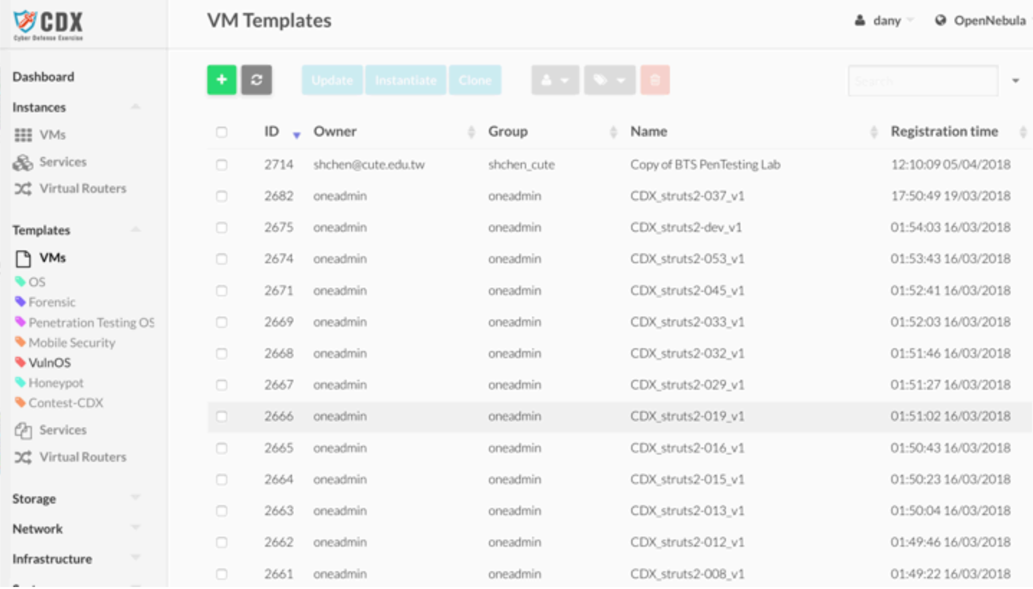
Allocated Memory 1.3TB / 1.6TB

Real CPU 6880 / 85601

Real Memory 717

Users 1490

System Dashboard



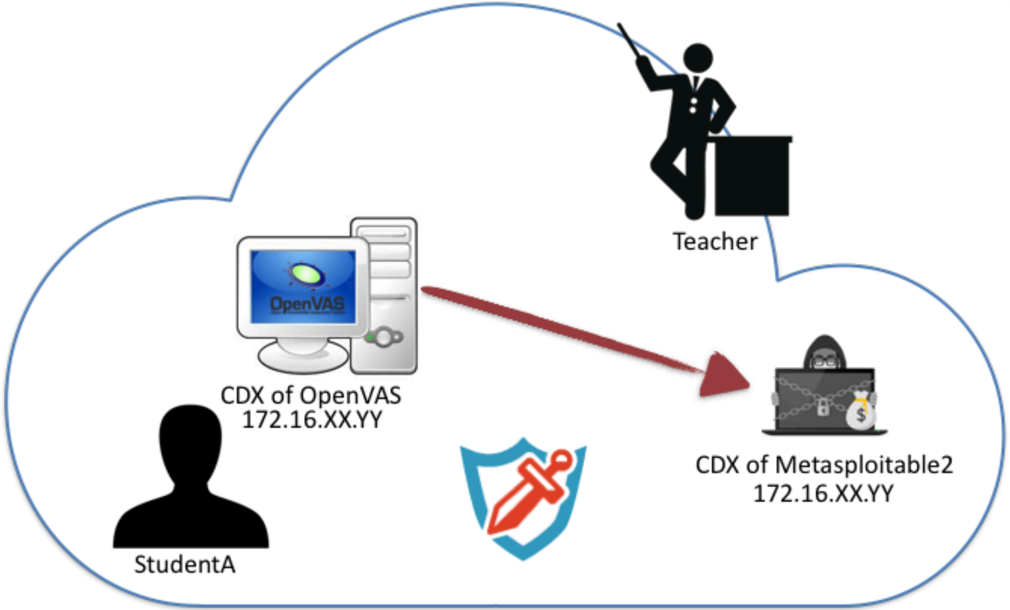
VM Templates

	ID	Owner	Group	Name	Registration time
□	2714	shchen@cute.edu.tw	shchen_cute	Copy of BTS PenTesting Lab	12:10:09 05/04/2018
□	2682	oneadmin	oneadmin	CDX_struts2-037_v1	17:50:49 19/03/2018
□	2675	oneadmin	oneadmin	CDX_struts2-dev_v1	01:54:03 16/03/2018
□	2674	oneadmin	oneadmin	CDX_struts2-053_v1	01:53:43 16/03/2018
□	2671	oneadmin	oneadmin	CDX_struts2-045_v1	01:52:41 16/03/2018
□	2669	oneadmin	oneadmin	CDX_struts2-033_v1	01:52:03 16/03/2018
□	2668	oneadmin	oneadmin	CDX_struts2-032_v1	01:51:46 16/03/2018
□	2667	oneadmin	oneadmin	CDX_struts2-029_v1	01:51:27 16/03/2018
□	2666	oneadmin	oneadmin	CDX_struts2-019_v1	01:51:02 16/03/2018
□	2665	oneadmin	oneadmin	CDX_struts2-016_v1	01:50:43 16/03/2018
□	2664	oneadmin	oneadmin	CDX_struts2-015_v1	01:50:23 16/03/2018
□	2663	oneadmin	oneadmin	CDX_struts2-013_v1	01:50:04 16/03/2018
□	2662	oneadmin	oneadmin	CDX_struts2-012_v1	01:49:46 16/03/2018
□	2661	oneadmin	oneadmin	CDX_struts2-008_v1	01:49:22 16/03/2018

VM Templates

Training Course-Vulnerability Scan

- Step 1: Open Tools VM and Target VM
- Step 2: Login Tools VM to learning OpenVAS
- Step 3:Waiting the scan result
- Step 4:Reading report and do some action for the risk



Conclusions

Conclusions

- Next generation application based on more and more network bandwidth
- How to remove DDoS attack from network operation is the key issue in the future
- Cybersecurity Intelligence sharing and exchange
- Co-work with the other operation center to exchange and sharing information
- Analysis and Handling malware behavior
- Collect and Analysis CDX training and challenge data
- Use AI Computing power for cyber security intelligence analysis

Thank you
for your attention!

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