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 NAR Labs
National Center for High-performance Computing

1991
Taiwan’s first National level supercomputer Center

1993
Hsinchu Headquarters

2003
NPO under NAR Labs

2004
TWAREN Services 10G

2005
Tainan Office

2008
Taichung Office

2011
177 TF Windrider supercomputer

2016
100G Network Backbone

2017
1.33 PF Peta scale HPC

2018
Start deploying AI Platform

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

Hsin Chu Headquarters
Taichung Office
Tainan Office
### 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
- Caffe2
- PyTorch / Torch
- ......and more
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
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
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

Challenges

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

TANet & TWAREN
Threat Intelligence

- Attack
- Aggregation
- Analysis
- Action
- Automatic
Eco System

Detection → Define → Defense

New Threat
Threat Intelligence Platform

WWW

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

Cuckoo Sandbox, Enterprise

Monogo DB, SQL DB, Files

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

National Level

Domain Level
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 known
  - 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
Case Study:

DDoS, Distributed Denial-of-Service
## DDoS Attack IP Top 10

<table>
<thead>
<tr>
<th>IP</th>
<th>Count</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>140.128.173.213</td>
<td>14</td>
<td>UDP</td>
</tr>
<tr>
<td>210.60.208.166</td>
<td>14</td>
<td>UDP</td>
</tr>
<tr>
<td>210.59.63.250</td>
<td>11</td>
<td>UDP</td>
</tr>
<tr>
<td>192.192.100.2</td>
<td>10</td>
<td>UDP, ICMP, DNS_AMP, memcached_AMP</td>
</tr>
<tr>
<td>163.26.255.254</td>
<td>8</td>
<td>UDP</td>
</tr>
<tr>
<td>140.138.179.195</td>
<td>7</td>
<td>UDP, DNS_AMP, CLDAP_AMP</td>
</tr>
<tr>
<td>210.60.208.167</td>
<td>6</td>
<td>UDP</td>
</tr>
<tr>
<td>163.32.74.1</td>
<td>5</td>
<td>UDP, DNS_AMP, CLDAP_AMP</td>
</tr>
<tr>
<td>210.60.233.247</td>
<td>5</td>
<td>UDP, ICMP, CLDAP_AMP</td>
</tr>
<tr>
<td>120.115.60.54</td>
<td>4</td>
<td>UDP, ICMP, NTP_AMP, CLDAP_AMP</td>
</tr>
</tbody>
</table>

Data Range: 2019 April
## DDoS Attack Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP RST</td>
<td>403</td>
</tr>
<tr>
<td>UDP</td>
<td>180</td>
</tr>
<tr>
<td>IP Fragmentation</td>
<td>45</td>
</tr>
<tr>
<td>CLDAP Amplification</td>
<td>36</td>
</tr>
<tr>
<td>TCP SYN</td>
<td>18</td>
</tr>
<tr>
<td>ICMP</td>
<td>16</td>
</tr>
<tr>
<td>DNS Amplification</td>
<td>15</td>
</tr>
<tr>
<td>memcached Amplification</td>
<td>11</td>
</tr>
<tr>
<td>NTP Amplification</td>
<td>6</td>
</tr>
</tbody>
</table>

Data Range: 2019 April
Digital Attack Map

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
Hybrid Attack: SQL-Inject

Attacker

Target
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 Security site 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
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

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ip</td>
<td>IPv4 address</td>
<td>Botnet IPs</td>
</tr>
<tr>
<td>2</td>
<td>time</td>
<td>datetime</td>
<td>Time when Datafeed Generate</td>
</tr>
</tbody>
</table>
Mirai Infections

• Sample Data
  - 179.182.231.78,2019-05-09 23:59:59
  - 114.32.245.21,2019-05-09 23:59:59
  - 197.59.251.0,2019-05-09 23:59:59
  - 5.139.58.158,2019-05-09 23:59:59
  - 201.95.65.79,2019-05-09 23:59:59
  - 42.227.192.58,2019-05-09 23:59:59
Mirai Infections

• 114.32.245.21,TW,,TAIPEI,3462

```
$ 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
```
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

https://owl.nchc.org.tw
### Malware KB: PE-x86-64

<table>
<thead>
<tr>
<th>MD5</th>
<th>File Type</th>
<th>File Size</th>
<th>VirusTotal Result</th>
<th>Malware Classification</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>010c5bd52bd0dd1dd0f25e91594e0360</td>
<td>PE-x86-64</td>
<td>47.63KB</td>
<td>44/58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>010eb7e0cdd2274a70fb077b2d076040</td>
<td>PE-x86-64</td>
<td>888.47KB</td>
<td>35/56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>011e6e5419a5dc5592885105c3c36c40</td>
<td>PE-x86-64</td>
<td>569.00KB</td>
<td>37/56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>012ab504ff47809a70423d91b127c30</td>
<td>PE-x86-64</td>
<td>250.74KB</td>
<td>39/56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>012e5fa1cfc6d8b30506e502b152d9f0</td>
<td>PE-x86-64</td>
<td>1.19MB</td>
<td>21/56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>012d816f8c47c7d7f063aa19c3d04d440</td>
<td>PE-x86-64</td>
<td>215.50KB</td>
<td>30/56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>012eada38aa8224d46885619e7981840</td>
<td>PE-x86-64</td>
<td>336.00KB</td>
<td>22/56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>012fcee9784f9c9999d617ddf8c8bd2cd40</td>
<td>PE-x86-64</td>
<td>344.77KB</td>
<td>24/57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0138a4356cbda66661bd22f3ec8f1720</td>
<td>PE-x86-64</td>
<td>45.08KB</td>
<td>37/56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0138aa9d4f93c878a234ee3dacb05ee0f0</td>
<td>PE-x86-64</td>
<td>640.00KB</td>
<td>33/56</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Malware KB: Exploit/Root Kit

<table>
<thead>
<tr>
<th>MD5</th>
<th>File Type</th>
<th>File Size</th>
<th>VirusTotal Result</th>
<th>Malware Classification</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>00002ea6066dc18391db9f697220c9c0</td>
<td>Others</td>
<td>2.77KB</td>
<td>44/54</td>
<td>Exploit/Root Kit</td>
<td></td>
</tr>
<tr>
<td>00003b51da52cd7c74cb89814fa8d630</td>
<td>Others</td>
<td>53.00KB</td>
<td>35/57</td>
<td>Exploit/Root Kit</td>
<td></td>
</tr>
<tr>
<td>0000da2856da2186ff227a440b05f190</td>
<td>Others</td>
<td>46.79KB</td>
<td>46/56</td>
<td>Exploit/Root Kit</td>
<td></td>
</tr>
<tr>
<td>00009d2f15bd44e6f632a822130e30</td>
<td>Others</td>
<td>2.43KB</td>
<td>46/55</td>
<td>Backdoor, Exploit/Root Kit, Trojan, Worm</td>
<td></td>
</tr>
<tr>
<td>010c524d93a6498fe353bc7251cb34d0</td>
<td>Others</td>
<td>690.00Bytes</td>
<td>24/54</td>
<td>Exploit/Root Kit</td>
<td></td>
</tr>
<tr>
<td>010e138c1e508ccf704b1f58b96185c8</td>
<td>Others</td>
<td>1.60KB</td>
<td>47/56</td>
<td>Backdoor, Exploit/Root Kit, Trojan, Worm</td>
<td></td>
</tr>
<tr>
<td>010e212a396950538db3c3c2003d9840</td>
<td>Others</td>
<td>68.00KB</td>
<td>40/55</td>
<td>Exploit/Root Kit</td>
<td></td>
</tr>
<tr>
<td>011cc4bcb1bb360d1f74b81be519c780</td>
<td>Others</td>
<td>515.00Bytes</td>
<td>37/55</td>
<td>Exploit/Root Kit</td>
<td></td>
</tr>
<tr>
<td>0112600c2c6f03a37e40500d14a2f0</td>
<td>Others</td>
<td>13.92KB</td>
<td>43/57</td>
<td>Backdoor, Exploit/Root Kit, Trojan, Worm</td>
<td></td>
</tr>
<tr>
<td>011478ae082cb6014a30dc18b7c6220</td>
<td>Others</td>
<td>27.27KB</td>
<td>40/57</td>
<td>Backdoor, Exploit/Root Kit, Trojan</td>
<td></td>
</tr>
</tbody>
</table>
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-Demand 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 Website v1

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

System Dashboard

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!