Investigation and Intelligence Framework

Alan Ho, Kelvin Wong, Anthony Lai, Zetta Ke VXRL
VXRL

• Valkyire-X Security Research Lab
• Non-profit Making group in HK
• Offensive, Creative and Fun
• Only one CTF team in HK
Kelvin WONG

• Conduct digital forensics examination and investigation in HK LEA since 2002, and start research on 2010
• Speak at DEFCON, DFRWS EU, HTCIA and HITCON
• Publication on Hakin9 Magazine, Digital Forensics Magazine and Forensics Focus
Alan HO

- Worked as Application Security consultant
- Experienced developer
- Passionate over Web hacking, Application security and research
- VXRL security researcher and CTF crew member
- SANS GWAPT (Gold paper) holder
- CeCOS VIII (APWG) 2014, DFRWS EU 2014, Hack in Taiwan 2014, IFMTA 2014
Agenda

• Background
• Forensics Challenges
• Case Study
• Investigation and Intelligence Framework
• Demo
A. Someone with investigation skills and computer knowledge, but he does not have the proper tools to investigate effectively.

B. Someone with investigation skills and tools, but he does not have the computer knowledge, he may miss out important artifacts from the evidences.

C. Someone with computer knowledge and tools, but he does not have investigation skills to correlate what he finds and draw the whole picture.

Possesses investigation kills, computer knowledge, with proper tools to investigate more effectively.
Case Study

• A company director in a trading company and authorizes bank transfer up to 40,000US per day online.
• A SMS notice will be sent to the director per each transaction.
• All the online transactions are conducted on his personal computer.
Case Study

• One day, there was a transfer to Europe amounted 30,000US, he received a SMS but ignored it.

• He checked the bank statement and discovered the transaction as unauthorized. A case was reported.

• What happened?
<table>
<thead>
<tr>
<th>Botnet</th>
<th>Phishing</th>
<th>Theft by employee</th>
<th>Loss of bank card</th>
<th>Authorized transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Crime</td>
<td>Traditional Crime</td>
<td></td>
<td></td>
<td>??</td>
</tr>
</tbody>
</table>

No Crime / Misunderstanding
Traditional Crime

<table>
<thead>
<tr>
<th>Botnet</th>
<th>Phishing</th>
<th>Theft by employee</th>
<th>Loss of bank card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Crime</td>
<td></td>
<td>Traditional Crime</td>
<td></td>
</tr>
</tbody>
</table>

Locate the suspect / witness
- Where is the bank transaction?
- What kinds of the transaction?
- Any CCTV footage?
- Any Fingerprint left?
### Cyber Crime

<table>
<thead>
<tr>
<th>Botnet</th>
<th>Phishing</th>
<th>Theft by employee</th>
<th>Loss of bank card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Crime</td>
<td>Traditional Crime</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Collect evidence from director’s computer
Way Forwards

• Botnet or Phishing? Or Other?
• Which evidences should collect first?
• Does the investigator seize the director’s computer?
• Does the investigator preform a live forensics examination at the scene?
• Any help?
A. Someone with investigation skills and computer knowledge, but he does not have the proper tools to investigate effectively

B. Someone with investigation skills and tools, but he does not have the computer knowledge, he may miss out important artifacts from the evidences

C. Someone with computer knowledge and tools, but he does not have investigation skills to correlate what he finds and draw the whole picture

 possessed investigation kills, computer knowledge, with proper tools to investigate more effectively
Investigation and Intelligence Framework (IIF)

- Cybercrimes are advancing every day
- Examiners/Investigators are often too focus technically, eg reverse engineering.
- Miss out the investigation purposes
- Report and submit for court prosecution.
- IIF helps to correlate the evidences and intelligence to help the investigation more effectively.
Proof of Concept

• A tool is developed to demonstrate the framework, correlating evidence and intelligence in order to provide a big picture of the cybercrime story and help investigation more effectively.

• Extract IP addresses, Email, URLs, Social Network ID from the evidence files
# Proof of Concept

<table>
<thead>
<tr>
<th>When</th>
<th>Where</th>
<th>Who</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>When did the incident possibly happen?</td>
<td>Where did the incident possibly take place?</td>
<td>Who is the possible suspect?</td>
</tr>
<tr>
<td>Evidence</td>
<td>The timestamp extracted from the evidence</td>
<td>IP location extracted from the evidence</td>
<td>The subscriber’s information</td>
</tr>
</tbody>
</table>

- **When**
  - Concept
  - Evidence

- **Where**
  - Concept
  - Evidence

- **Who**
  - Concept
  - Evidence

- **How**
  - Concept
  - Evidence
Result of the case

- Received an email (purportedly from Fedex) with attachment
- Downloaded the attachment but Anti-virus app. can’t detect
- Visited the bank website and input the credentials on a popup windows
- Transferred the money within a minutes
- Checked the SMS on the next day but ignored it
- Discovered the illegal transaction by audit check after a few days
Fwd: Delivery Status Notification (Failure)

shaikvali547 <shaikvali547@gmail.com>

To: kohirud, kdsamir, kbbi, kkkkm

Why is this message in Spam? It's similar to

NEW ANDHRAPRadesh CAPITAL AND PLOTS

INTERNATIONAL AIR PORT OF ANDHRAPRadesh

POTTIPADU APPROVED DTCP LAYOUT @Rs.5,999/- SQYD

JUST 0.5 KM TO PROPOSED 200 FEET OUTER RING ROAD

HURRY...LIMITED PERIOD OFFER..

Instalment plots also available 25 kms nearer to rajadhani AMARAVATHI @Rs2,500/- sq yard.

Hurry...limited plots available..

FEEL FREE TO CONTACT SRINIVAS 9290018999 AND 8889847777..

VIJAYAWADA PLOTS ..AJITSHINGNAGAR @Rs.11,000/- SQUARE YARD ONLY..

5 Attachments
Username

Password

Login

Forgot Username or Password?

Don't have iBanking?

Register
Evidences found

• the phishing email address
• the download list
• the browsing history
• the network connect
IIF Tool - Environment

- Ubuntu 14.02 LTS
- Python 2.7
- Django
- Celery
Evidence Data

- Evidence Data
  - Memory Dump
  - Registry
  - Pcap
  - Text file

- Evidence Files are located in the “evidence pool folder”
Evidence Data

Evidence Pool
- 2015_05_08_120532_hktaxi.pcap
- winxp.vmem
- NTUSER.DAT
- websurf.pcap

Files to investigate
- sample_data.txt

Manage Evidence
Load Saved Data
Evidence Data

• Memory Dump
  – Rekall to grab the information
  – Call Rekall command from python
    • pslist
    • connscan, netscan, netstat
Evidence Data

• Registry
  —Python library
• Pcap
  —Python library
• Text files
  —String
Investigation Engine

IP Addresses
- 202.105.182.86
- 124.228.254.3
- 162.221.186.120
- 109.120.183.106
- 157.7.170.62
- 160.97.52.229

URLs
- http://www.google.com
- http://www.scid.co.za/wp-content/themes/twentytwelve/payca/88c3c07/2c0396973c394b2402
- http://027.ru
- http://baidu.com
- http://xiazhai.tuzhong.com
- http://www.qbssm.cn/a3.asp
- http://www.ubia-africard.com
- http://www.hangseongonline.com
Intelligence

• Whois
  – ipwhois package
    (https://pypi.python.org/pypi/ipwhois)

• VirusTotal
  – VirusTotal API

• CleanMX
  – CleanMX XML
    (http://support.clean-mx.de/clean-mx/xmlviruses.php?)
Intelligence

• PhishTank
  – PhishTank API
    (https://www.phishtank.com/api_info.php)
• Fake Site Database, ZeusTracker, Openphish
  – Web Request
    (http://wiki.aa419.org/index.php/Main_Page)
    (https://zeustracker.abuse.ch/monitor.php)
    (https://openphish.com/feed.txt)
"Type": "Webattack",
"Name": "CleanMX",
"APIKeys": [],
"Interface":
[
  {
    "URL": "http://support.clean-mx.de/clean-mx/xmlviruses.php?",
    "Type": "url"
  },
  "Enabled": "True",
  "Classname": "libCleanMX",
  "Rating": 1,
  "DefaultScore": 1
],

"Type": "Webattack",
"Name": "ZeusTracker",
"APIKeys": [],
"Interface":
[
  {
    "Type": "url"
  },
  {
    "Type": "url"
  },
  {
    "URL": "https://zeustracker.abuse.ch/monitor.php?search=<input_value>",
    "Type": "url",
    "Enabled": "True",
    "Classname": "libZeusTracker",
    "Rating": 1,
    "DefaultScore": 1
  },
  "DefaultScore": 1,
  "Keywords": ["Hits in Host table","Hits in ConfigURL table"]
],
"Type": "FraudWeb",
"Name": "AA419Bank",
"APIKeys": [],
"Interface":
[
  {
    "URL": "http://support.aa419bank.com",
    "Type": "url"
  },
  "Enabled": "False",
  "Classname": "libAA419Bank",
  "Rating": 1,
  "DefaultScore": 1
]
• Intelligence are categorized
  – Web Attack
  – Phishing
  – Botnet
  – Fraud
• Selected items are processed
• Details and Evaluation will be generated
After processing, the system will generate the detailed findings from the sources.
• Details
  – The details of the corresponding item is shown
  – Whether the item has records from intelligence
    • Frequency in VirusTotal and CleanMX detection
    • Appearing in ZeusTracker, Phishing Intelligence and 
      Fake Website Database
Evaluation

• The program will evaluate the case from the findings
  – In POC, evaluation is based on the frequency and existence
    • Average scores from VirusTotal and CleanMX
    • Existence in PhishTank, Openphish, ZeusTracker and Fake Website Database
Evaluation

• The result is visualized
  – Web Attack (VirusTotal and CleanMX)
  – Phishing (PhishTank and Openphish)
  – Botnet (ZeusTracker)
  – Fraud (Fake Website Database)
Export

- The result can be exported and analyzed in the future.
- Result is exported as JSON format.
Load saved data

testdata.json  Load

Evaluate  Expand All  Export Full JSON

Evidence File: #1

File name: textfile.txt
File type: ASCII text
File path: /home/iiframework/iiframework/main/iiframework/evidence_pool/textfile.txt
Evidence type: Text

IP Addresses
202.105.182.86

whois
IP: 202.105.182.86
ASN: 58543
Country: CN
Updated date: 2004-09-06T00:00:00
Expiration date: -
Extensibility

• New Intelligence can be added to the system
  – Get the API / URL of the intelligence
  – Create the new class
  – Set the configuration file

• JSON Data
  – Other systems can also load the data for analysis
Video Demonstration