TEAM T5
Cyber Security Research

Catching the Golden Snitch

Leveraging Threat Intelligence Platforms to Defend Against Cyber Attacks

Ashley Shen & Zha0
2016 HITCON CMT

Ashley Shen (Chi-en Shen)

Senior Threat Analyst at Team T5

- Malware analysis, malicious document detection, advanced persistence threat research
- Tracking several cyber espionage groups for years
- Tracking new operations, TTP of APT groups

✉ ashley@teamt5.org

Zha0 (zha0)

Senior Researcher at T5

- 7+ years experience on Reverse Engineering
- 5+ years experience on malware analysis
- Sandbox, Exploit research
- APT research

✉ zha0@teamt5.org

Agenda

- **Introduction**
  - What do we fear about cyber threat?
  - Why do we need Cyber Threat Intelligence?
- **Catching the Golden Snitch**
  - Main features of TIP
  - Aggregation, Analysis, Action
- **APT Research Real Case**
  - Story Begins
  - Pitfalls of Correlation
  - New activities of Menupass group
- **Products Available**
  - Available Products in each phase
  - Available TIP Products
- **Conclusion**
  - Some takeaways

INTRODUCTION

TEAM T5
Cyber Security Research

What do we fear about Cyber Threat?

State Secrete
(Political, Economic, Defense)
National Security

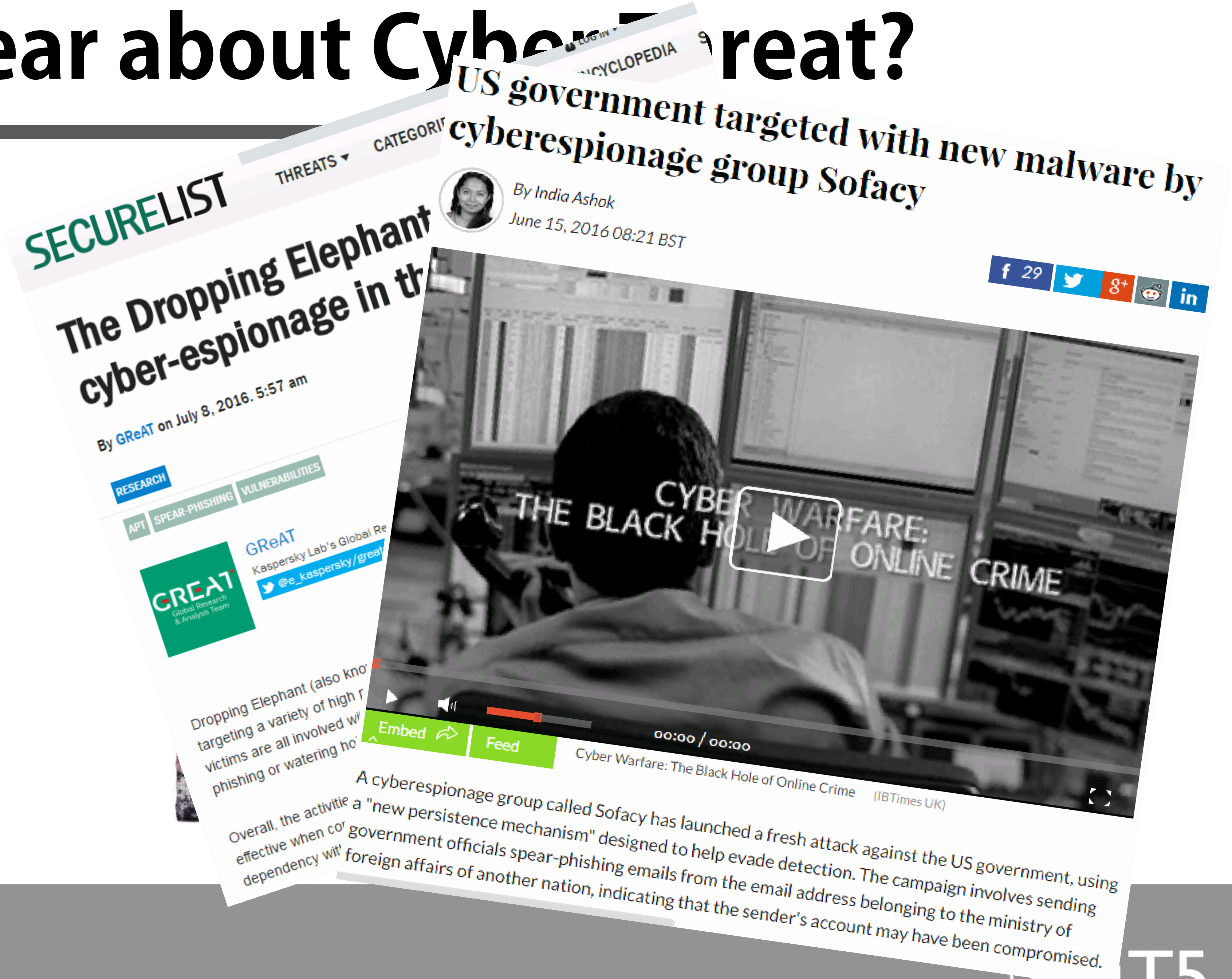
Business Intellectual Property
Customer Data

Personal identifiable Data
Privacy

What do we fear about Cyber Threat?

- However……

Cyber Espionage Attacks
Hacktivism Attacks



SECURELIST

The Dropping Elephant cyber-espionage in th

By GReAT on July 8, 2016. 5:57 am

GReAT
Kaspersky Lab's Global Re
@e_kaspersky/great

Dropping Elephant (also kno
targeting a variety of high p
victims are all involved wi
phishing or watering ho

Overall, the activitie
effective when co
dependency wit

US government targeted with new malware by cyberespionage group Sofacy

By India Ashok
June 15, 2016 08:21 BST

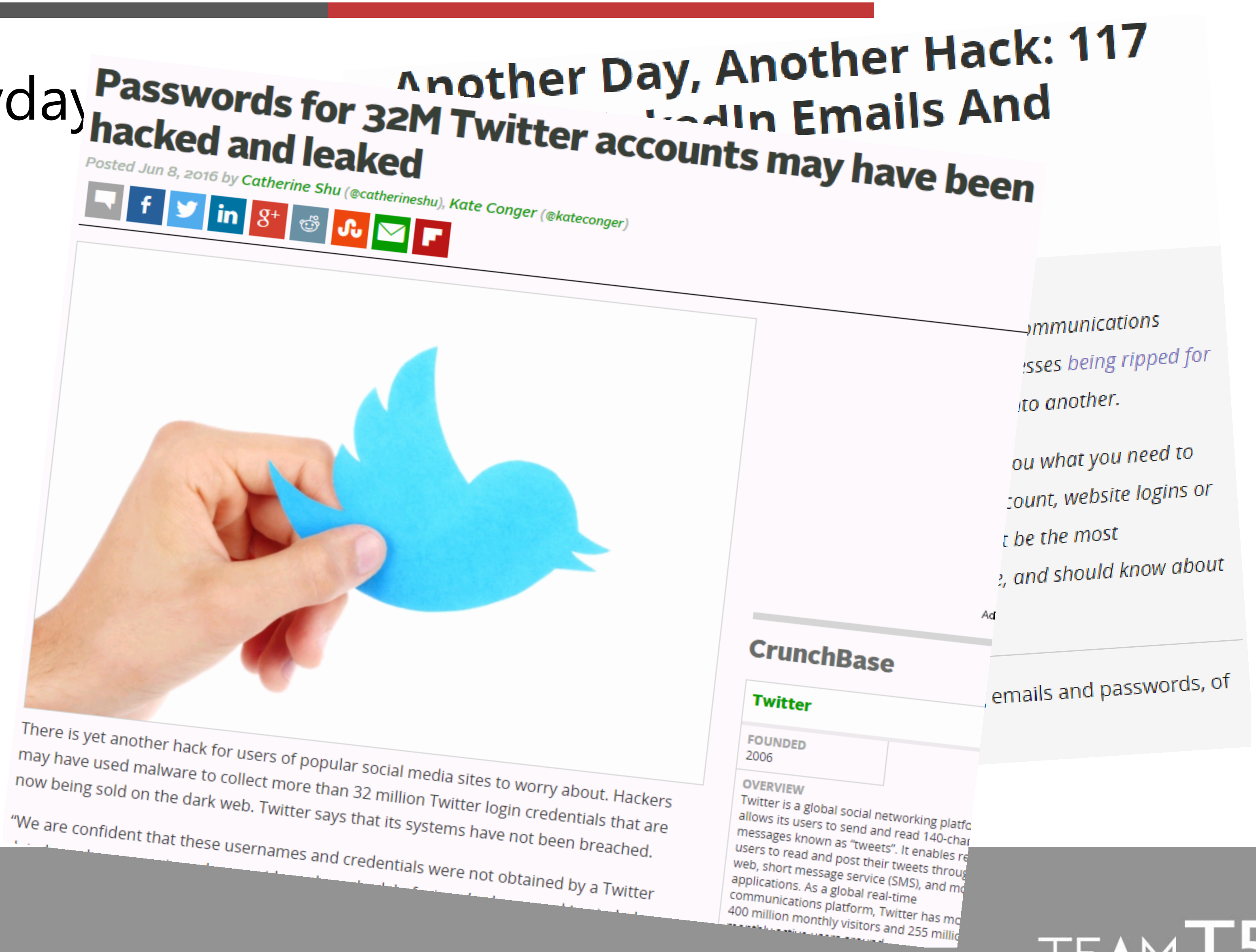
Cyber Warfare: The Black Hole of Online Crime (IBTimes UK)

A cyberespionage group called Sofacy has launched a fresh attack against the US government, using a "new persistence mechanism" designed to help evade detection. The campaign involves sending government officials spear-phishing emails from the email address belonging to the ministry of foreign affairs of another nation, indicating that the sender's account may have been compromised.

What do we fear about Cyber Threat?

- Breaches happens everyday

Cyber Espionage
Cyber Crime



Another Day, Another Hack: 117
…kedIn Emails And

…mmunications
…sses being ripped for
…to another.

…ou what you need to
…count, website logins or
…t be the most
…, and should know about

…emails and passwords, of

Passwords for 32M Twitter accounts may have been hacked and leaked

Posted Jun 8, 2016 by Catherine Shu (@catherineshu), Kate Conger (@kateconger)

There is yet another hack for users of popular social media sites to worry about. Hackers may have used malware to collect more than 32 million Twitter login credentials that are now being sold on the dark web. Twitter says that its systems have not been breached.

"We are confident that these usernames and credentials were not obtained by a Twitter

CrunchBase

Twitter

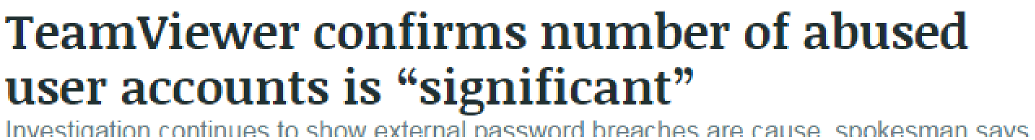
FOUNDED
2006

OVERVIEW
Twitter is a global social networking platfo… allows its users to send and read 140-char… messages known as "tweets". It enables re… users to read and post their tweets throug… web, short message service (SMS), and mo… applications. As a global real-time communications platform, Twitter has mo… 400 million monthly visitors and 255 millio…

What do we fear about Cyber Threat?

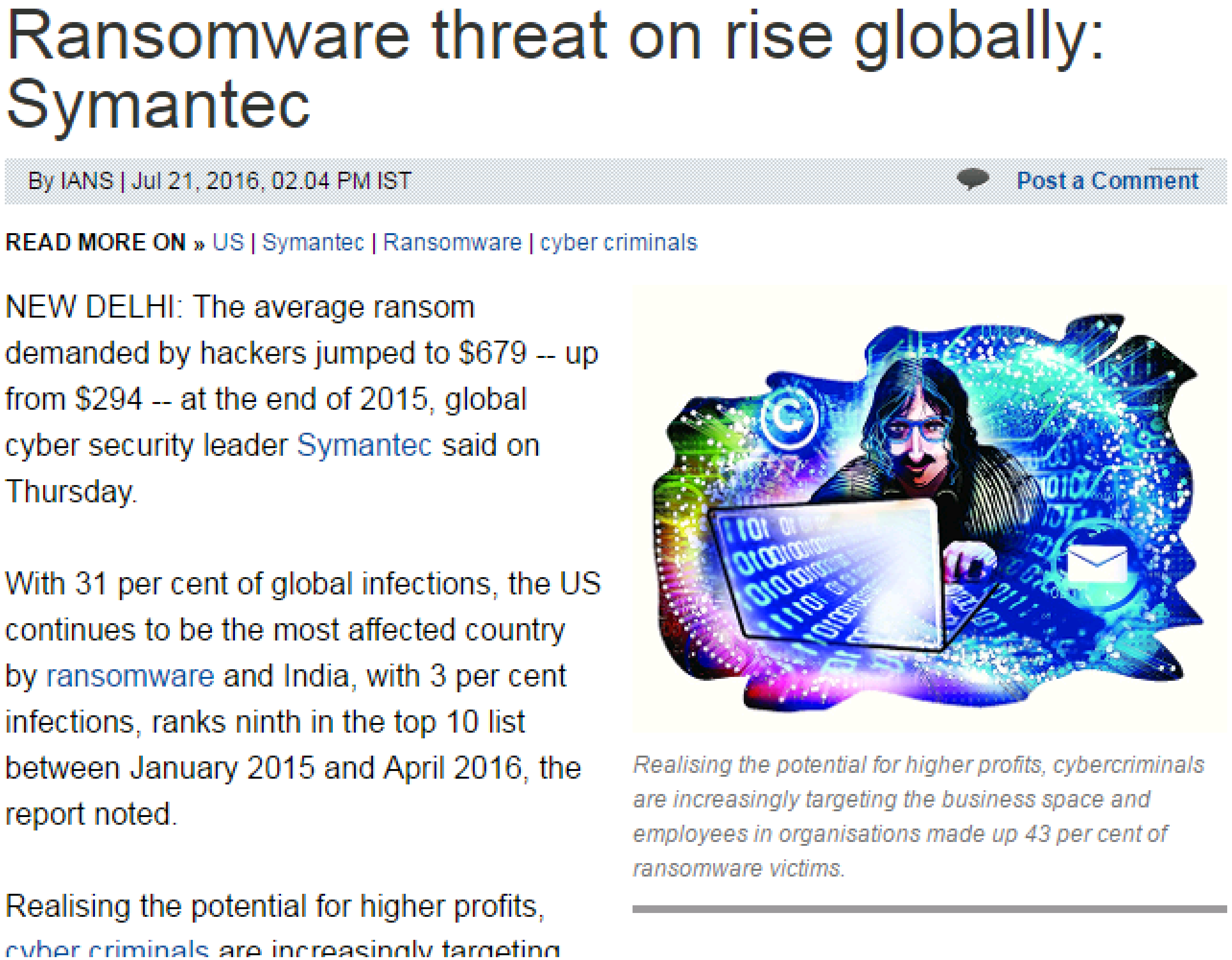
- Data leaked everyday..

Personal identifiable Data Privacy



TeamViewer confirms number of abused user accounts is “significant”

Investigation continues to show external password breaches are cause, spokesman says



Ransomware threat on rise globally: Symantec

By IANS | Jul 21, 2016, 02.04 PM IST

Post a Comment

READ MORE ON » US | Symantec | Ransomware | cyber criminals

NEW DELHI: The average ransom demanded by hackers jumped to $679 -- up from $294 -- at the end of 2015, global cyber security leader Symantec said on Thursday.

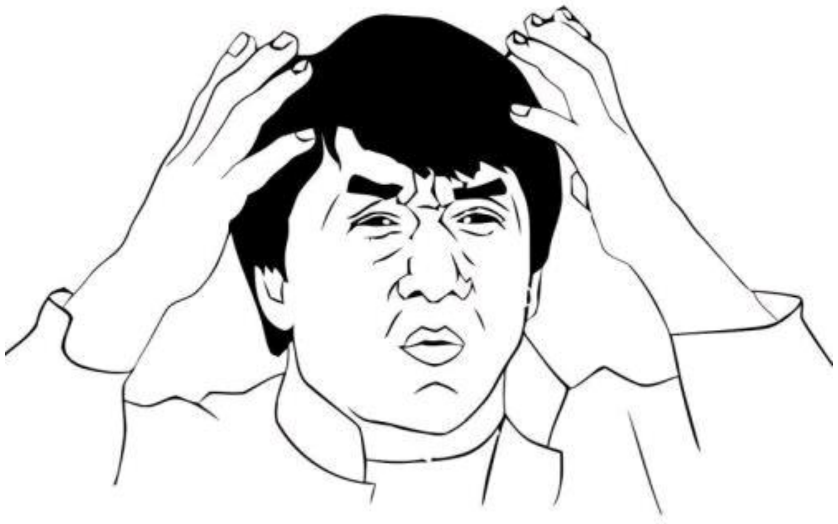
With 31 per cent of global infections, the US continues to be the most affected country by ransomware and India, with 3 per cent infections, ranks ninth in the top 10 list between January 2015 and April 2016, the report noted.

Realising the potential for higher profits, cyber criminals are increasingly targeting

Realising the potential for higher profits, cybercriminals are increasingly targeting the business space and employees in organisations made up 43 per cent of ransomware victims.

Problems..

- New breaches happens everyday
- New indicators disclosed everyday
- New vulnerabilities disclosed everyday
  - About 18 new CVE vulnerabilities disclosed everyday in 2015
  - Totally 6419 CVE vulnerabilities disclosed in 2015
- Advanced Persistent Threat
  - Targeting your Achilles' heel



Cyber Threat Intelligence

- **Knowledge about adversaries** and their **motivations**, **intentions**, and **methods** that is **collected, analyzed, and disseminated** in ways that help security and business staff at all levels **protect the critical assets of the enterprise**.

Jon Friedman et al, 2015, Definitive Guide to Cyber Threat Intelligence

iDEFENSE
THE POWER OF INTELLIGENCE

CROWDSTRIKE

Symantec

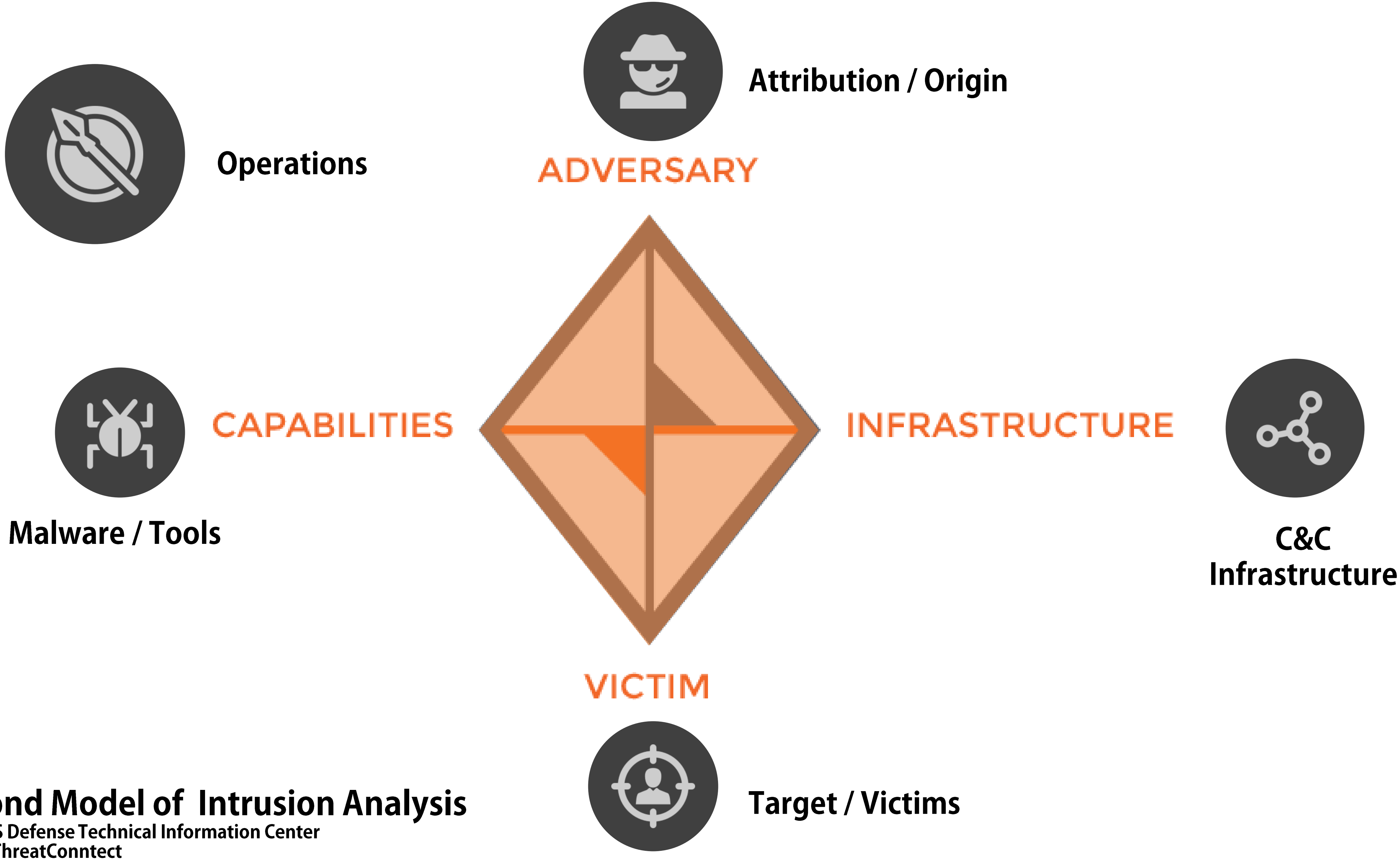
LOOKINGGLASS
Transforming the Art of Threat Intelligence

FireEye®

VERISIGN™

SecureWorks®

iSIGHTPARTNERS



Operations

ADVERSARY

Attribution / Origin

CAPABILITIES

Malware / Tools

INFRASTRUCTURE

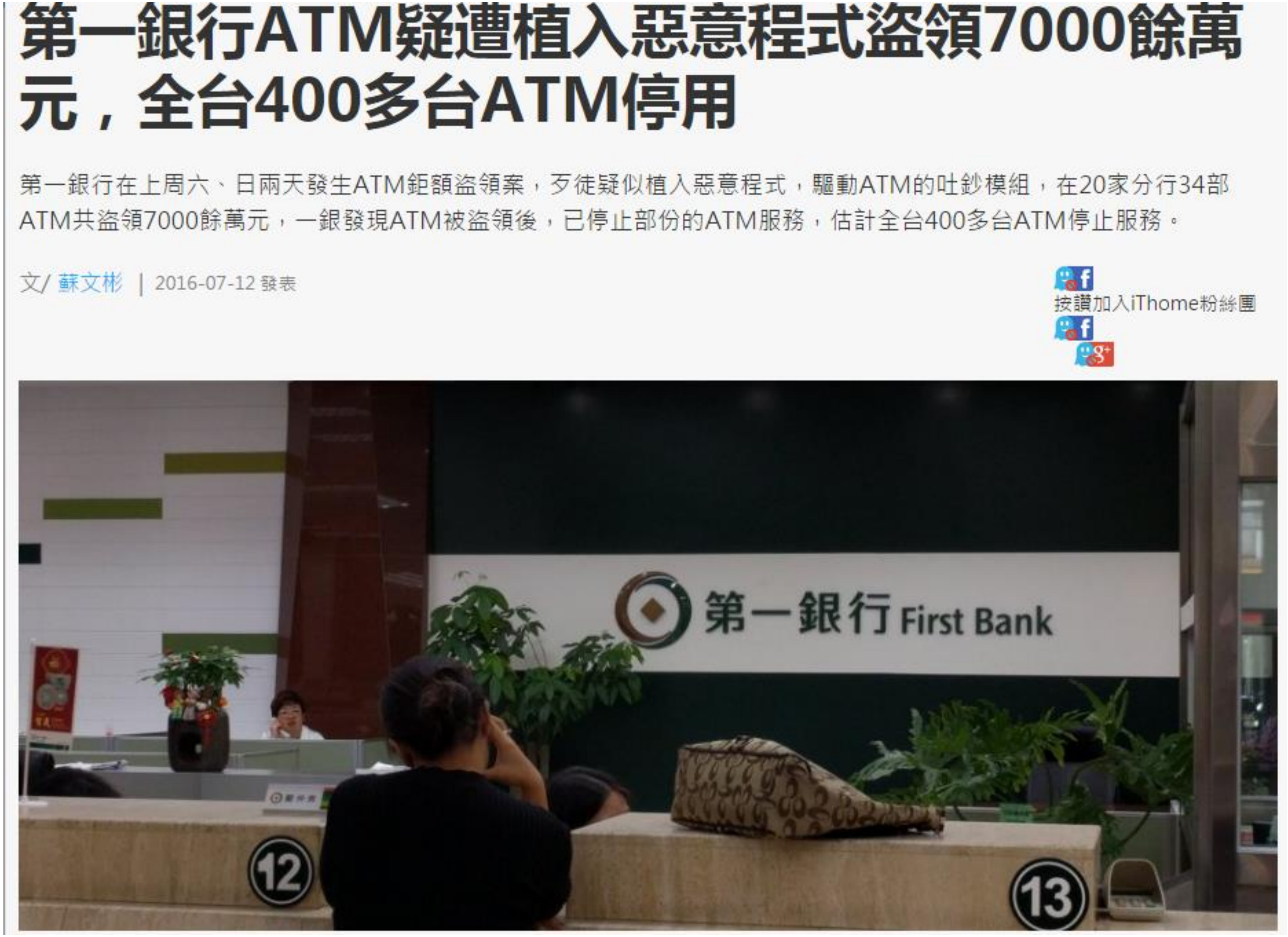
C&C
Infrastructure

VICTIM

Target / Victims

Diamond Model of Intrusion Analysis

ref: 2013 US Defense Technical Information Center
image ref: ThreatConntect



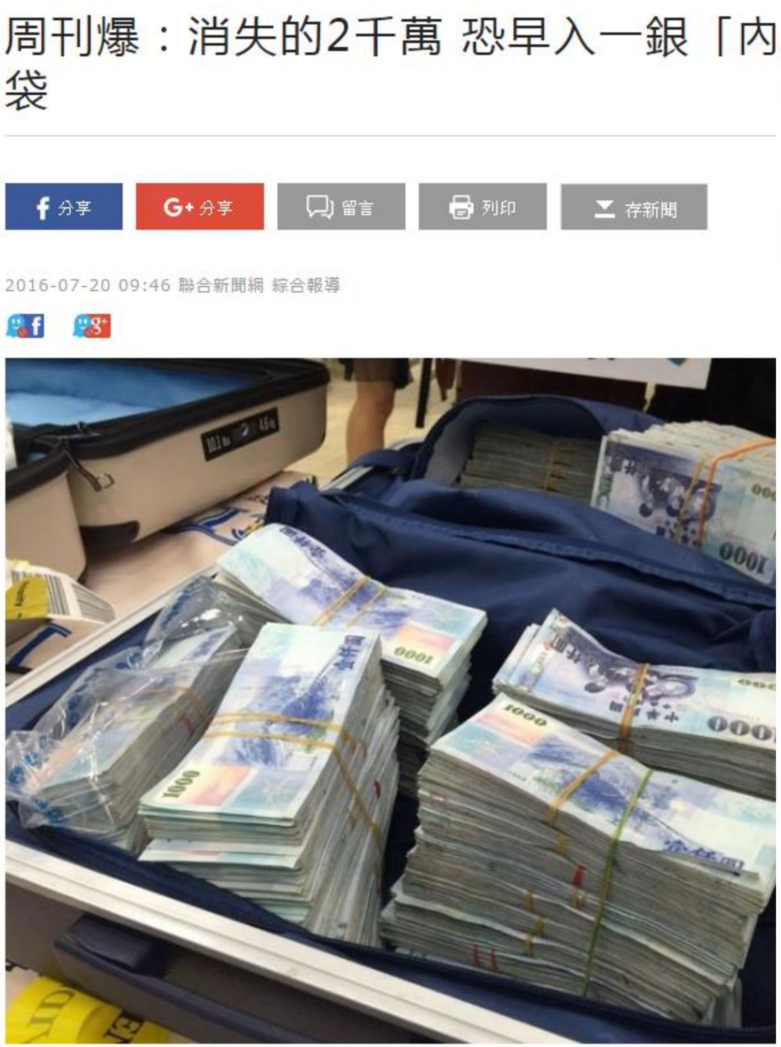
第一銀行ATM疑遭植入惡意程式盜領7000餘萬元，全台400多台ATM停用

第一銀行在上周六、日兩天發生ATM鉅額盜領案，歹徒疑似植入惡意程式，驅動ATM的吐鈔模組，在20家分行34部ATM共盜領7000餘萬元，一銀發現ATM被盜領後，已停止部份的ATM服務，估計全台400多台ATM停止服務。

文/ 蘇文彬 | 2016-07-12 發表

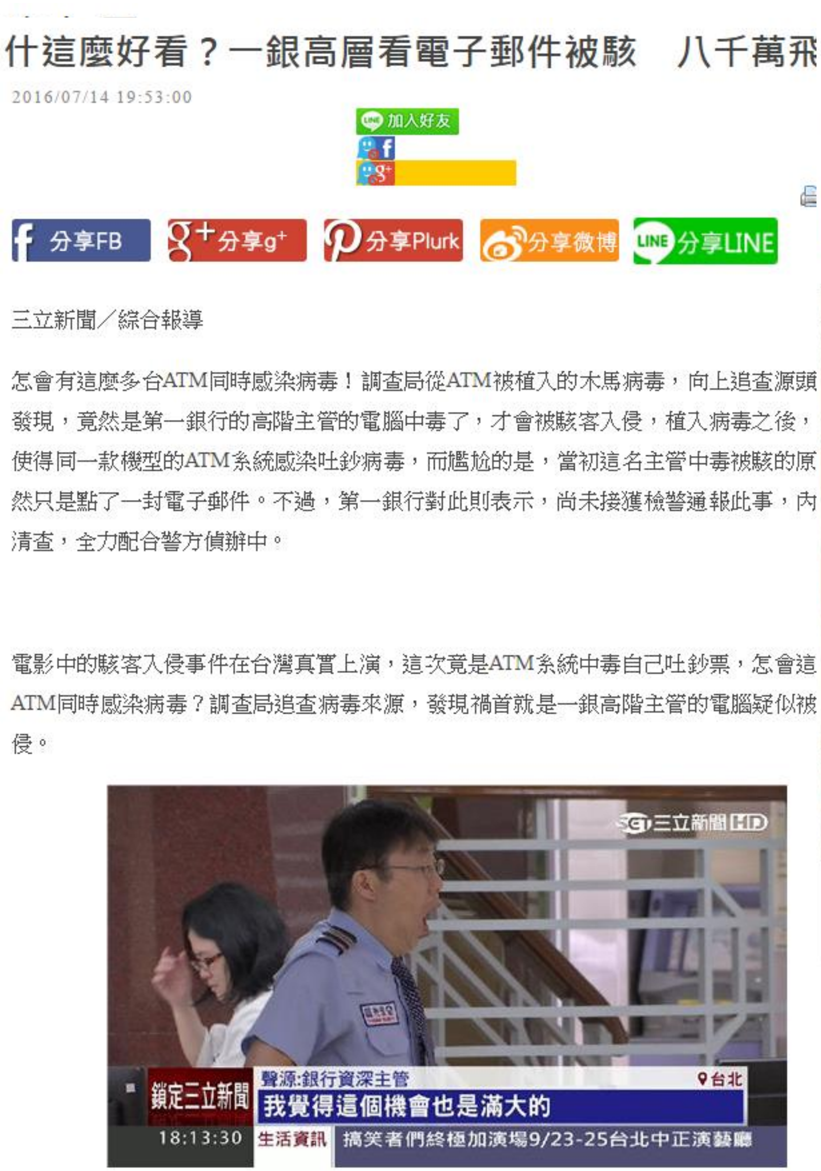
按讚加入iThome粉絲團

Ref: iThome



周刊爆：消失的2千萬 恐早入一銀「內
袋

2016-07-20 09:46 聯合新聞網 綜合報導



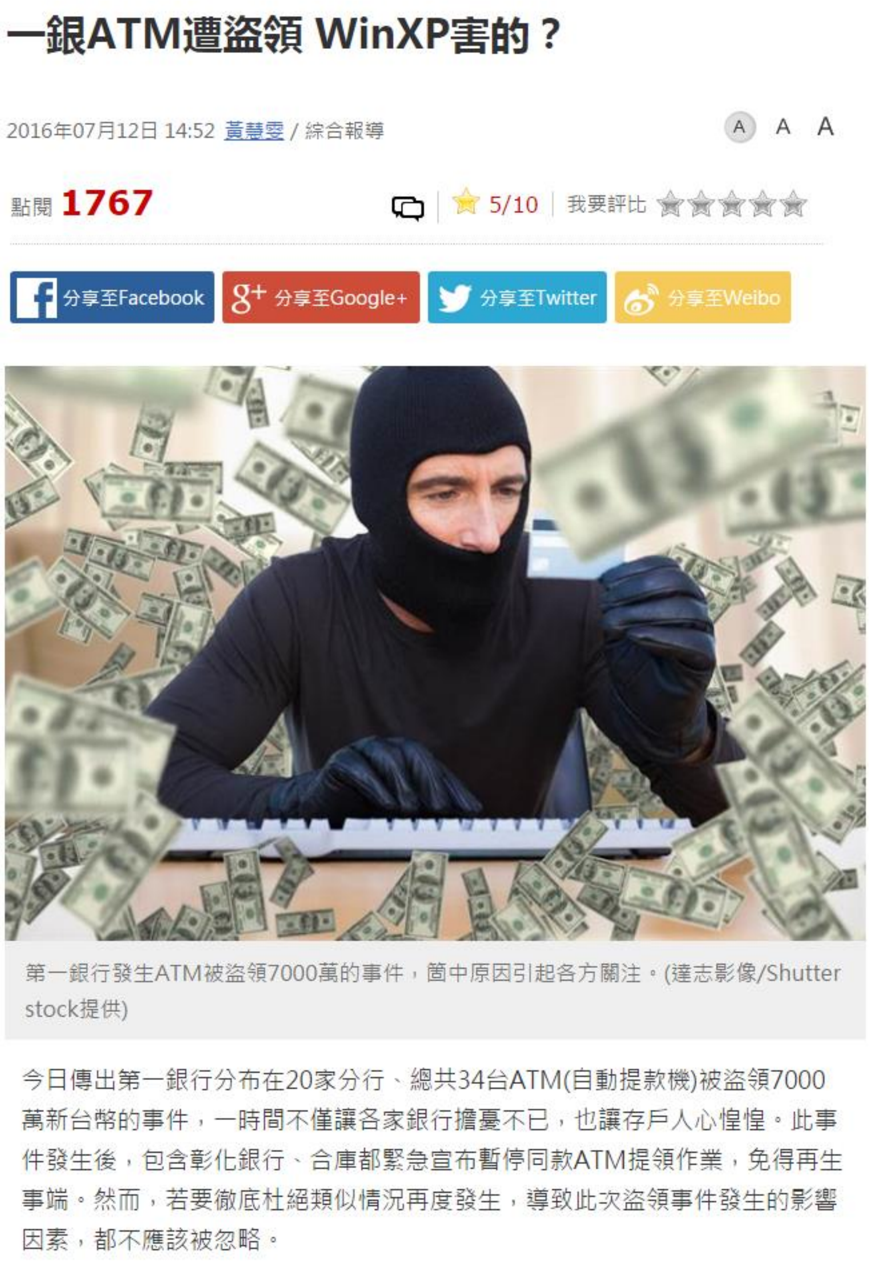
什這麼好看？一銀高層看電子郵件被駭　八千萬飛

2016/07/14 19:53:00

三立新聞／綜合報導

怎會有這麼多台ATM同時感染病毒！調查局從ATM被植入的木馬病毒，向上追查源頭
發現，竟然是第一銀行的高階主管的電腦中毒了，才會被駭客入侵，植入病毒之後，
使得同一款機型的ATM系統感染吐鈔病毒，而尷尬的是，當初這名主管中毒被駭的原
然只是點了一封電子郵件。不過，第一銀行對此則表示，尚未接獲檢警通報此事，內
清查，全力配合警方偵辦中。

電影中的駭客入侵事件在台灣真實上演，這次竟是ATM系統中毒自己吐鈔票，怎會這
ATM同時感染病毒？調查局追查病毒來源，發現禍首就是一銀高階主管的電腦疑似被
侵。



一銀ATM遭盜領 WinXP害的？

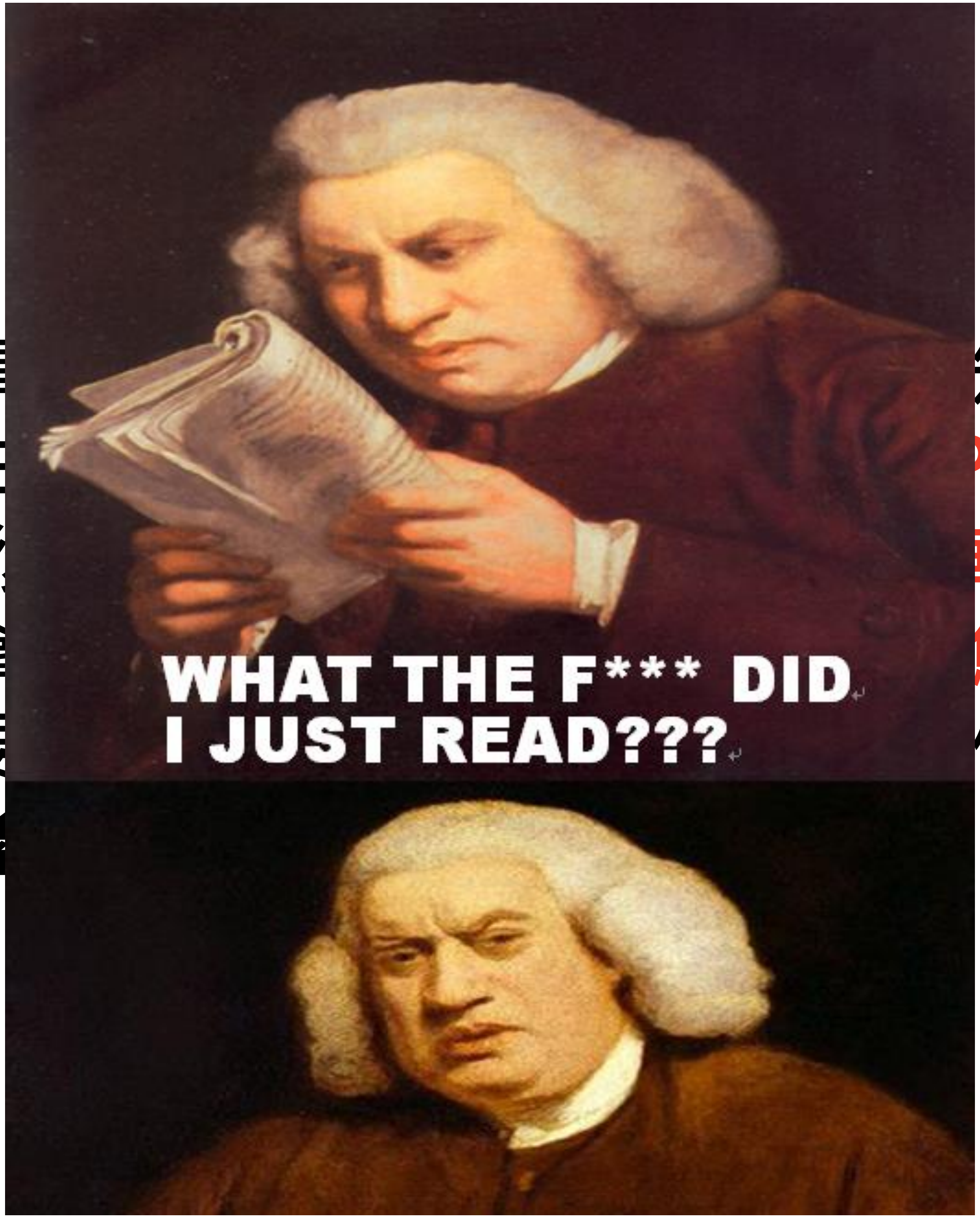
2016年07月12日 14:52 黃慧雯 / 綜合報導

第一銀行發生ATM被盜領7000萬的事件，箇中原因引起各方關注。(達志影像/Shutterstock提供)

今日傳出第一銀行分布在20家分行、總共34台ATM(自動提款機)被盜領7000萬新台幣的事件，一時間不僅讓各家銀行擔憂不已，也讓存戶人心惶惶。此事件發生後，包含彰化銀行、合庫都緊急宣布暫停同款ATM提領作業，免得再生事端。然而，若要徹底杜絕類似情況再度發生，導致此次盜領事件發生的影響因素，都不應該被忽略。

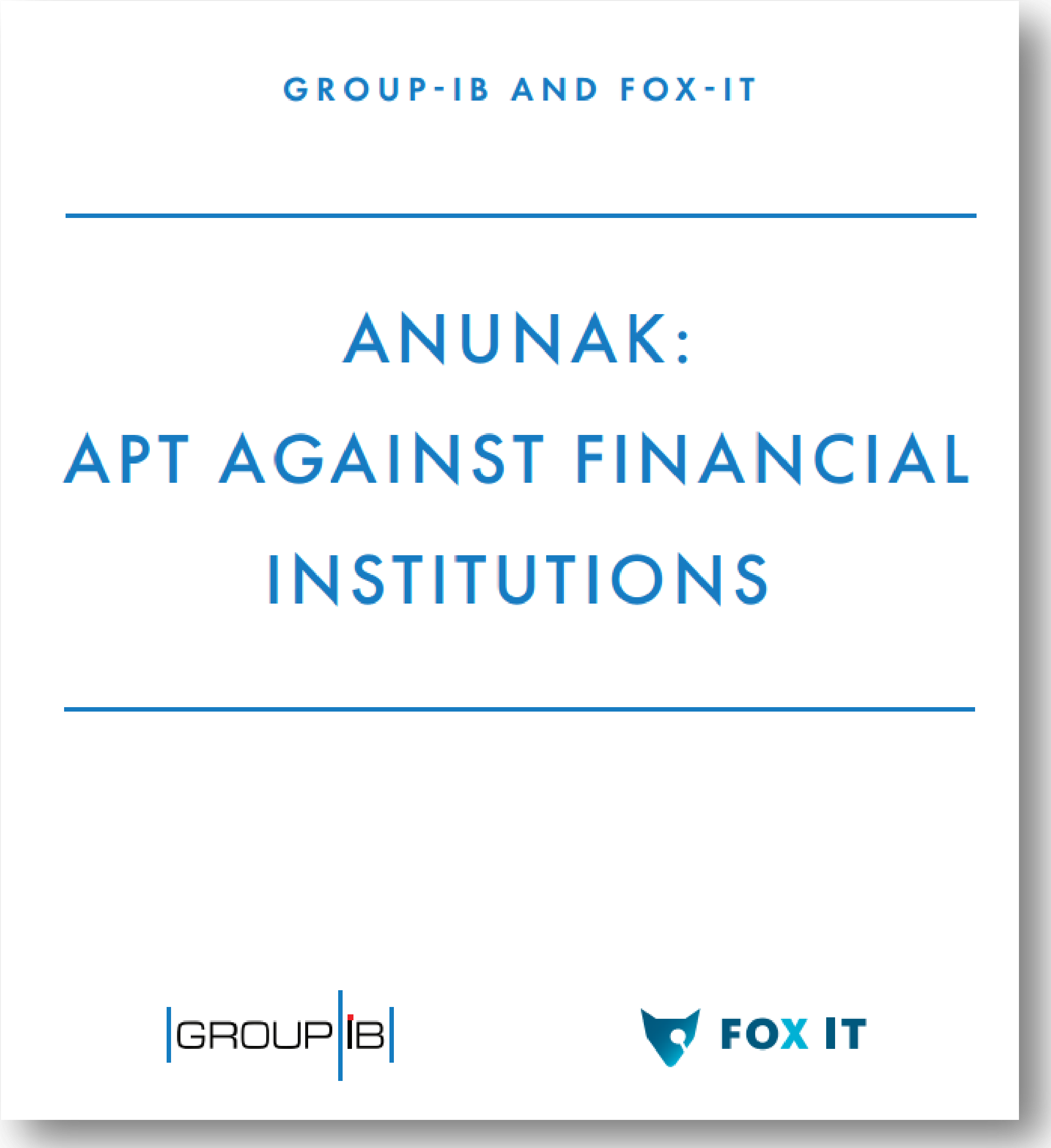
Ref: 聯合新聞網, 三立新聞

「關於一銀事 知道這
起盜領案是由 Ping
8.8.8.8 ，然 軟糖的嫌
犯可以把錢拿 鯧魚 ，
被捕之後說要 們有沒
有發現, 安德



Cyber Threat Intelligence Example

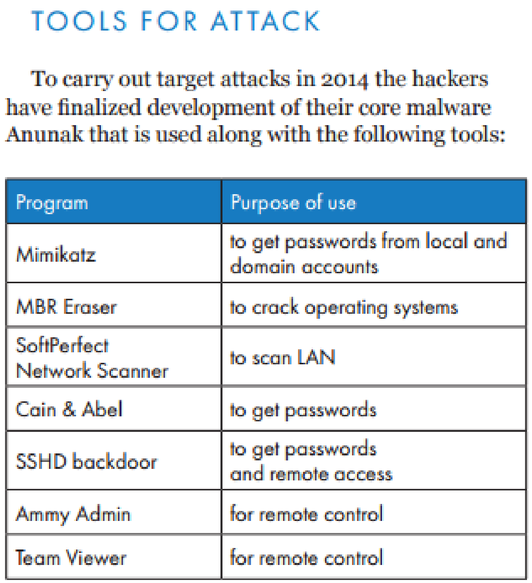
- Anunak: APT against financial institutions - Group-IB and Fox-IT
- This report describes the details and type of operations carried out by an organized criminal group from Russia that focuses on financial industry.



GROUP-IB AND FOX-IT

ANUNAK:

APT AGAINST FINANCIAL INSTITUTIONS



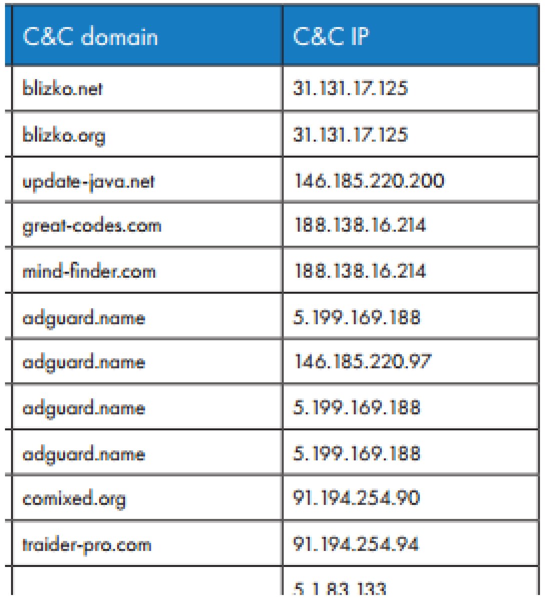
TOOLS FOR ATTACK

To carry out target attacks in 2014 the hackers have finalized development of their core malware Anunak that is used along with the following tools:

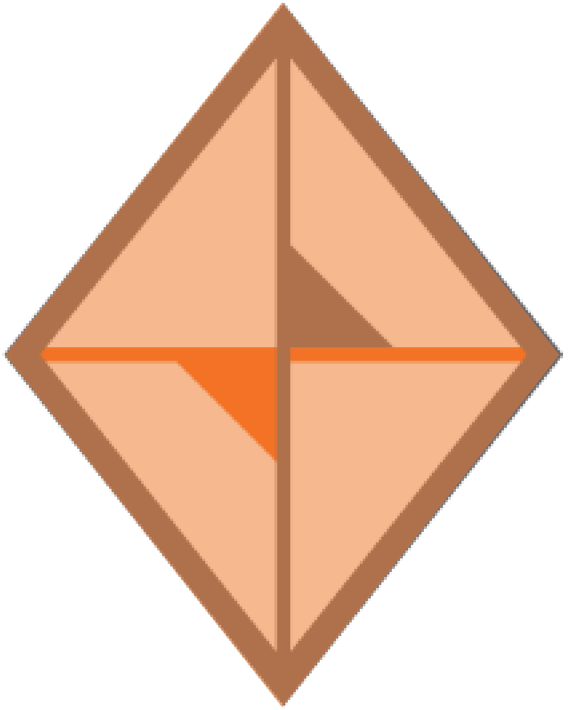
Program	Purpose of use
Mimikatz	to get passwords from local and domain accounts
MBR Eraser	to crack operating systems
SoftPerfect Network Scanner	to scan LAN
Cain & Abel	to get passwords
SSHD backdoor	to get passwords and remote access
Ammy Admin	for remote control
Team Viewer	for remote control

ADVERSARY

Citizens of both Russian and Ukrainian origin.



C&C domain	C&C IP
blizko.net	31.131.17.125
blizko.org	31.131.17.125
update-java.net	146.185.220.200
great-codes.com	188.138.16.214
mind-finder.com	188.138.16.214
adguard.name	5.199.169.188
adguard.name	146.185.220.97
adguard.name	5.199.169.188
adguard.name	5.199.169.188
comixed.org	91.194.254.90
traider-pro.com	91.194.254.94
	5.1.83.133



CAPABILITIES

INFRASTRUCTURE

Spear-phishing Emails
Access Internal Bank Network
Compromised AD servers and ATM Management Infrastructure
Malwares: Anunak, Mimikatz, MBR Eraser, SSHD, Ammy Admin

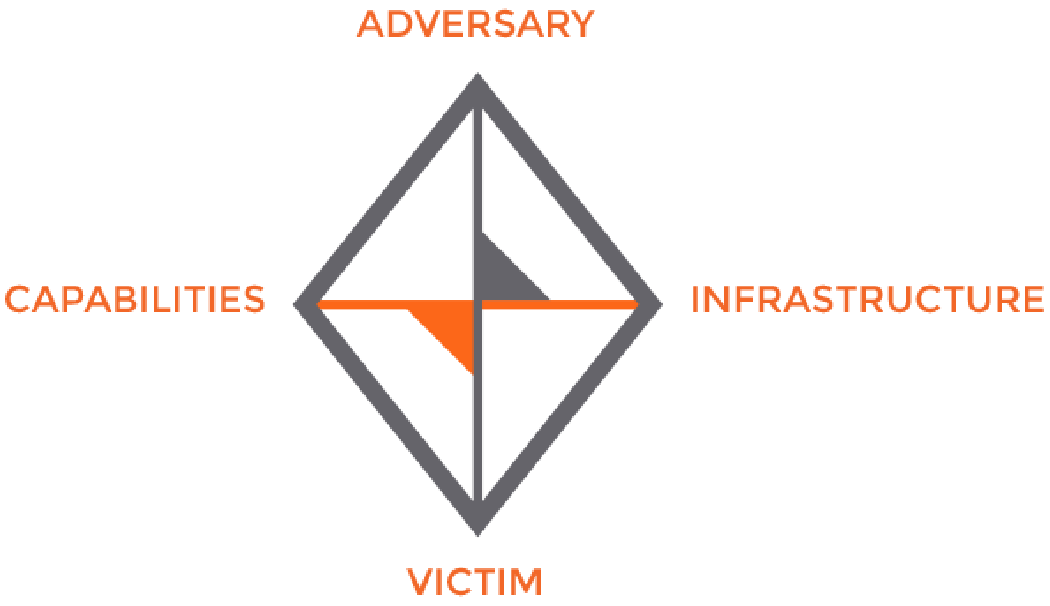
C&C servers
Internal bank networks

VICTIM

Banks, Payment providers, Retail industry, news, media and PR companies. More than 50 Russian banks and 5 payment systems was compromised.

Problems for Researchers

- How to aggregate all the data from different sources? (Open source intelligence, Incident Response, Community, Customers, Exchange Platform)
- How to manage all the information for better analysis?
- How to analysis these data, co-relate incidents to campaigns?



- What is the most significant threat to me?
- How to aggregate these cyber threat intelligence with internal data?
- How to share and do intelligence exchange?

THREAT INTELLIGENCE PLATFORM

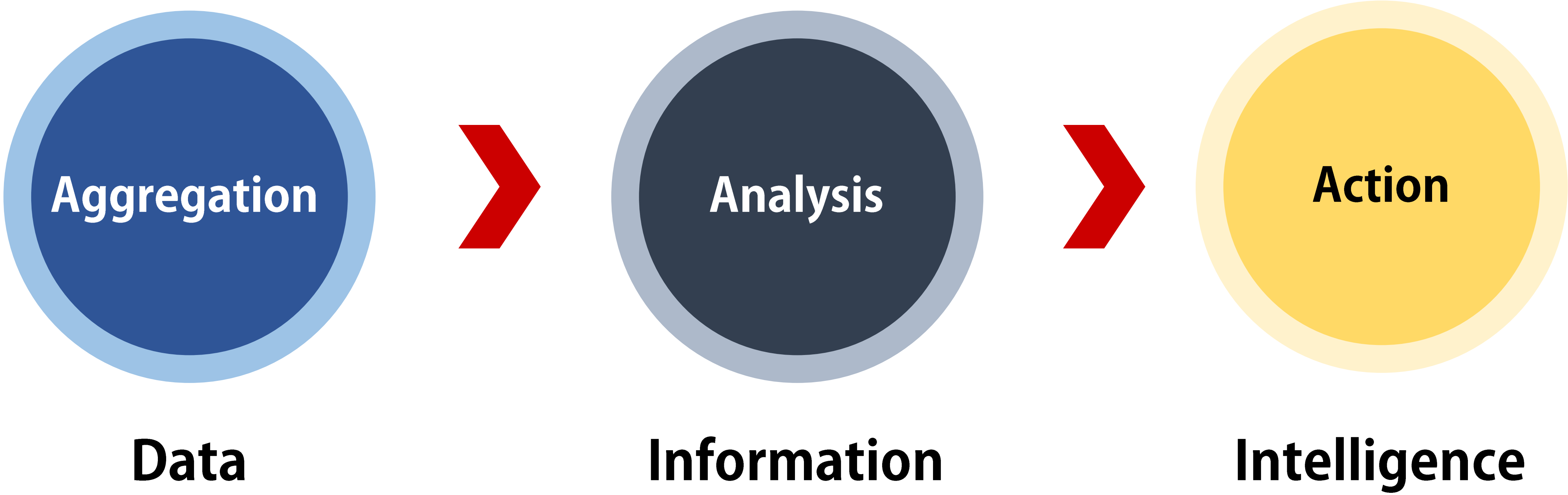
Threat Intelligence Platform

TEAM T5

Cyber Security Research

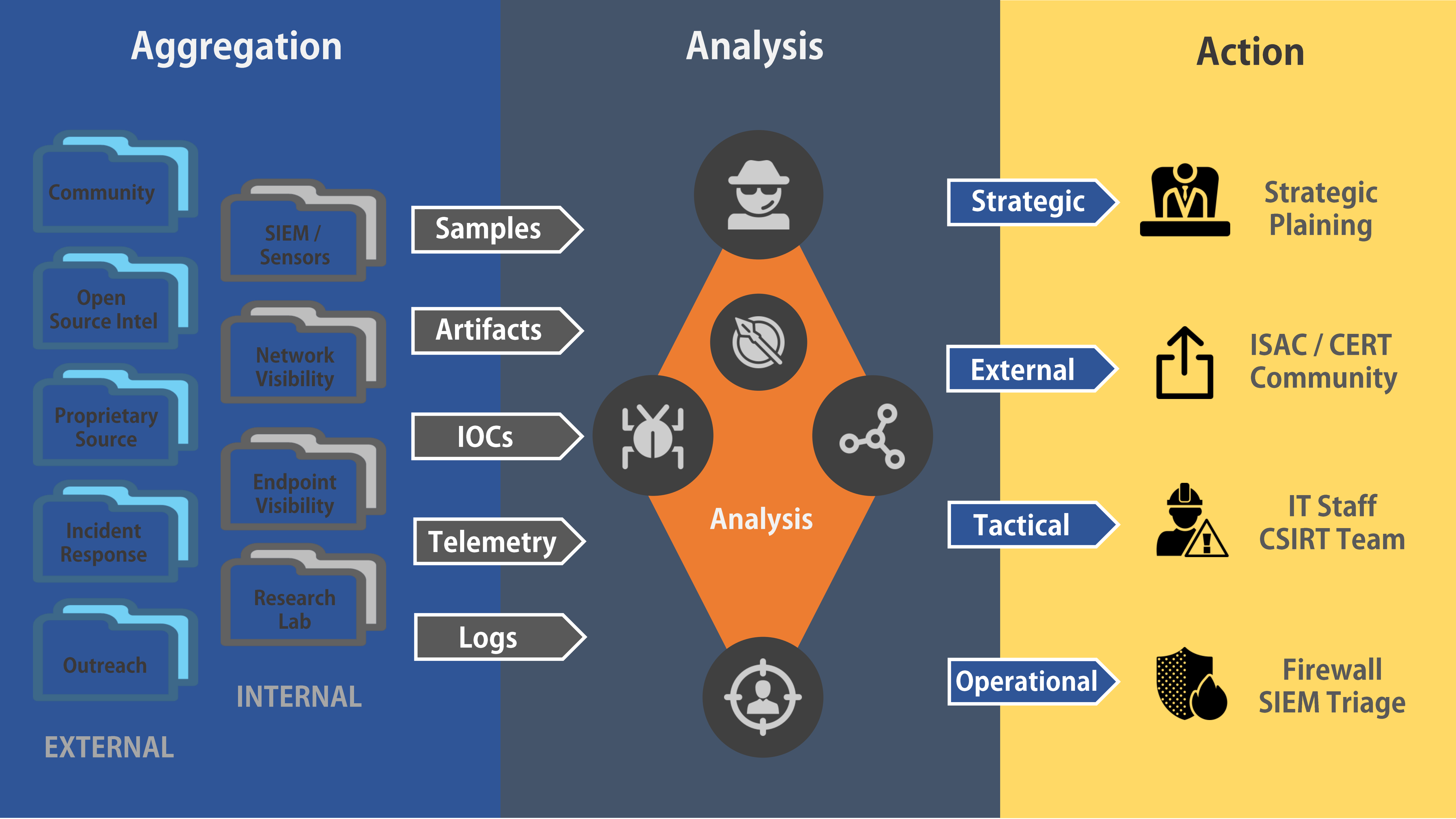
Threat Intelligence Platform

- To support research and tailored threat intelligence program
- Simply defined, TIP include three main features:



Aggregation → Analysis → Action

Data → Information → Intelligence



Aggregation

Community

Open Source Intel

Proprietary Source

Incident Response

Outreach

EXTERNAL

SIEM / Sensors

Network Visibility

Endpoint Visibility

Research Lab

INTERNAL

Samples

Artifacts

IOCs

Telemetry

Logs

Analysis

Analysis

Action

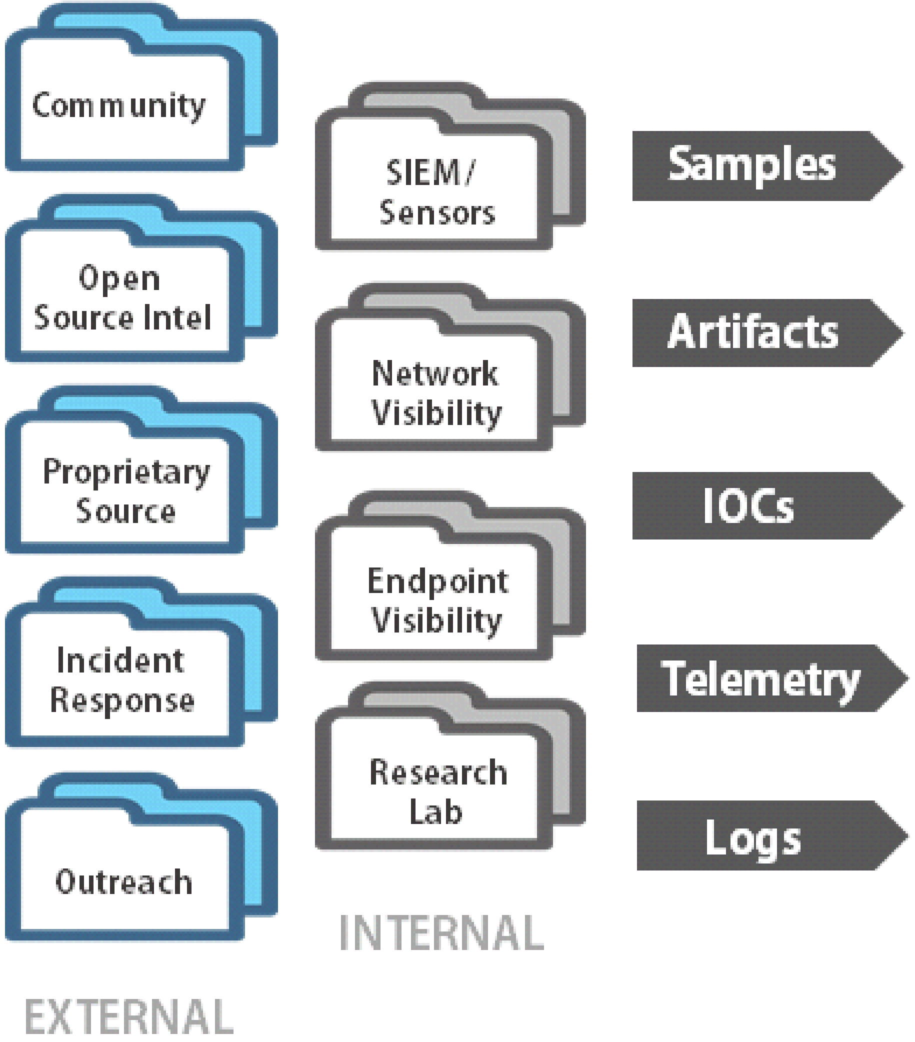
Strategic — Strategic Plaining

External — ISAC / CERT Community

Tactical — IT Staff CSIRT Team

Operational — Firewall SIEM Triage

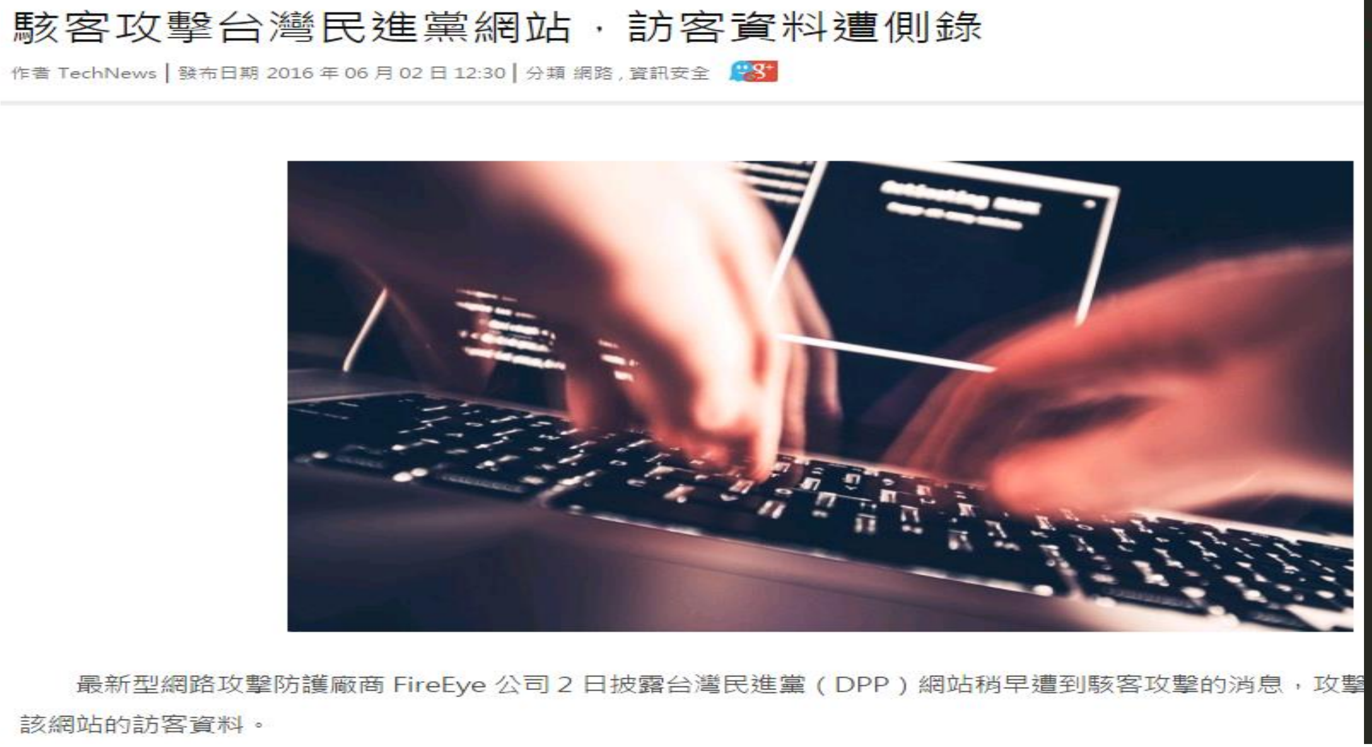
Aggregation



- Aggregating internal & external data:
  - Data from **own surface** and **external sources**
- The most important source of relevant threat data of an organization is your **own attack surface**.

APT Attack Tailored TTP Example

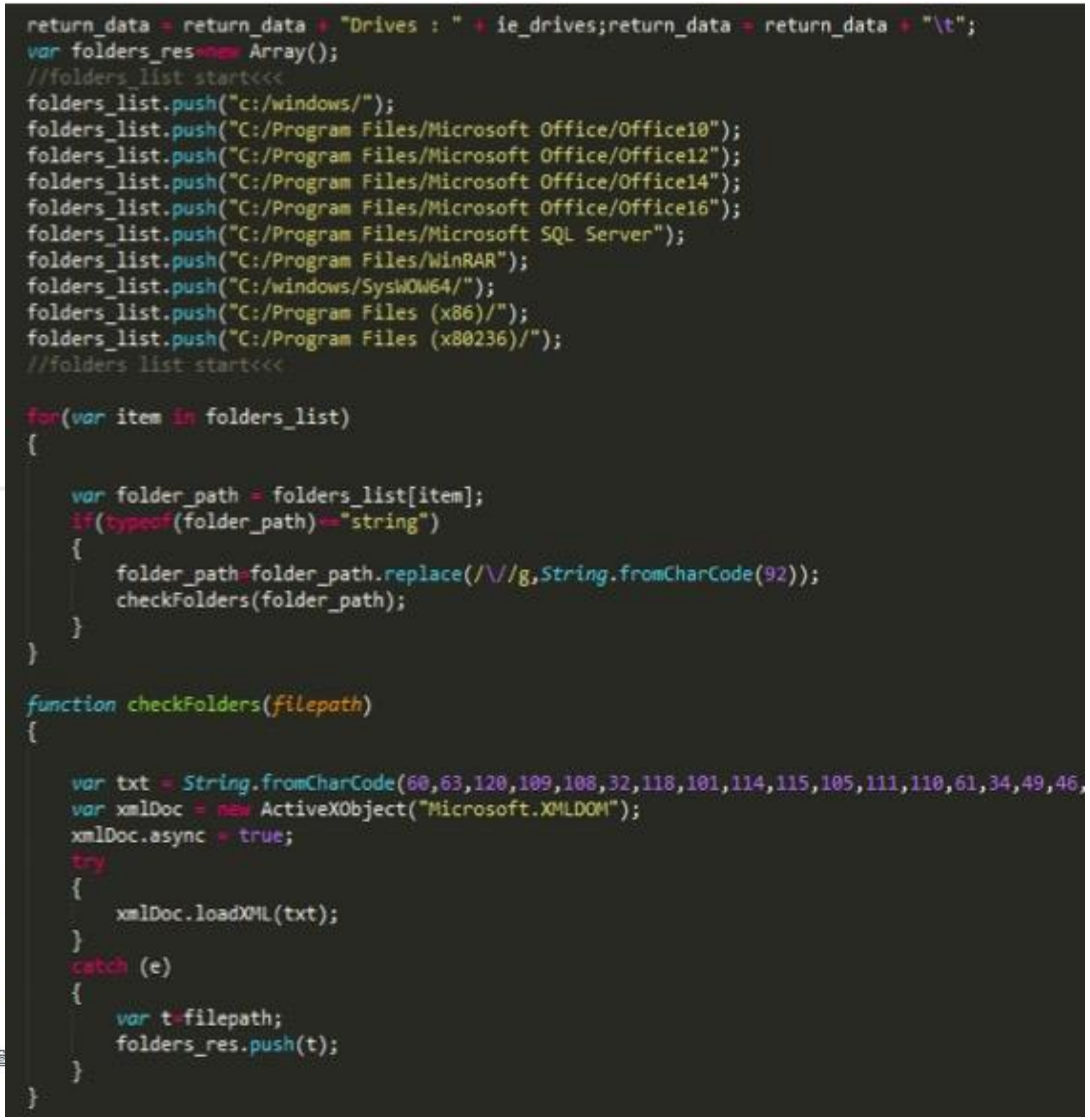
- TTP = Tactics, Techniques, and Procedures
- Targeted Attack Reconnaissance
  - Scanbox example



駭客攻擊台灣民進黨網站，訪客資料遭側錄

作者 TechNews | 發布日期 2016 年 06 月 02 日 12:30 | 分類 網路 , 資訊安全

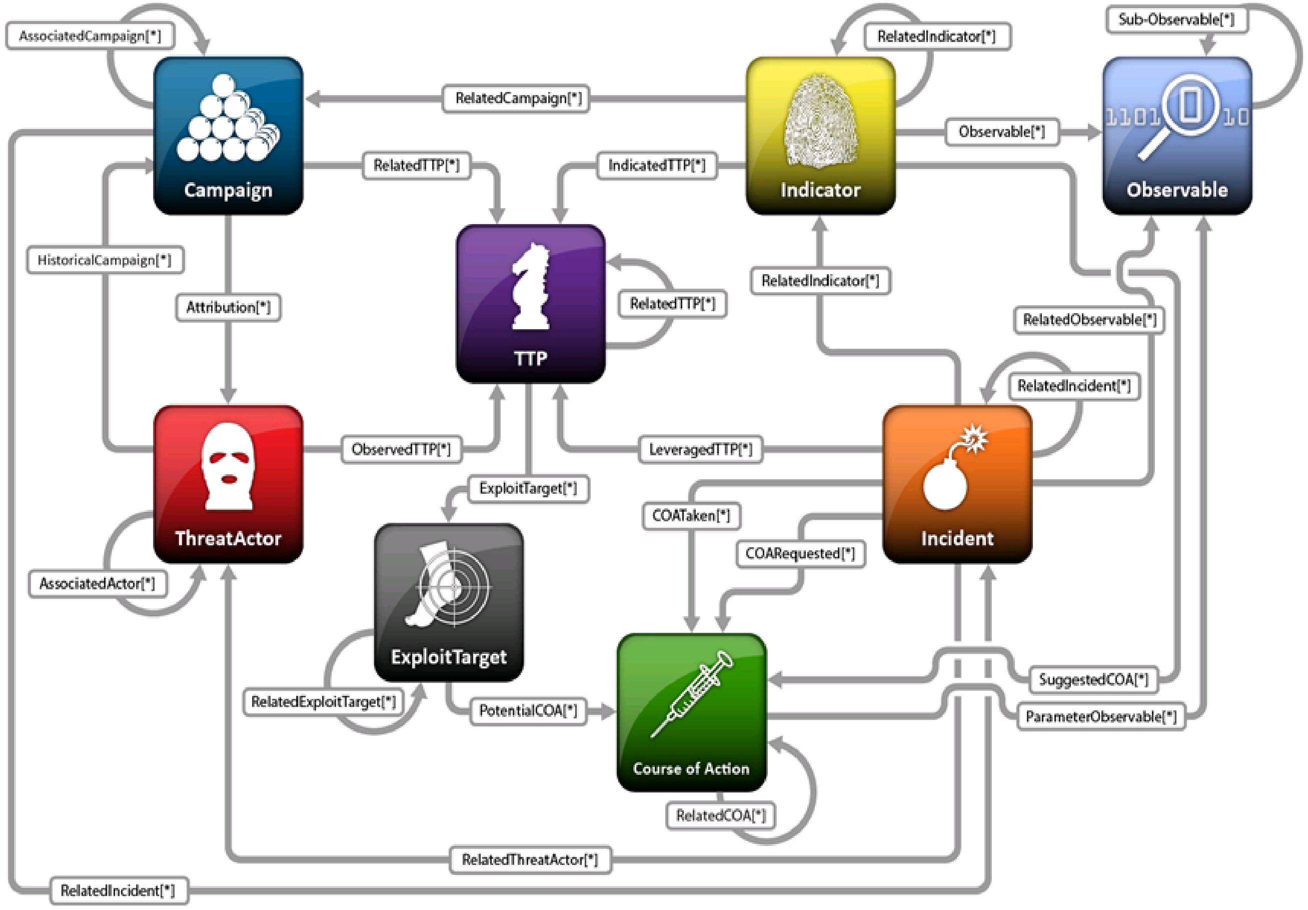
最新型網路攻擊防護廠商 FireEye 公司 2 日披露台灣民進黨（DPP）網站稍早遭到駭客攻擊的消息，攻擊
該網站的訪客資料。



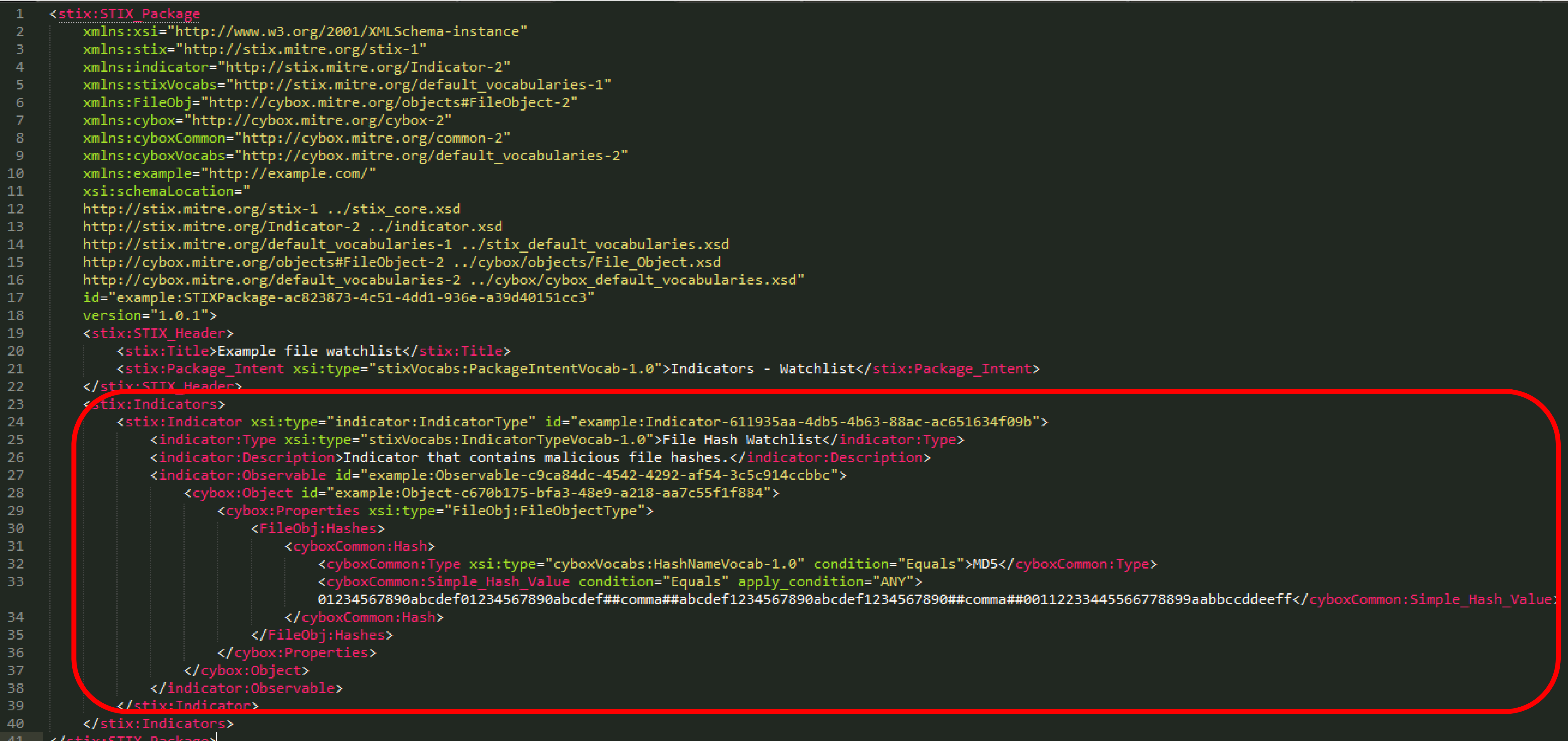
```
return_data = return_data + "Drives : " + ie_drives;return_data = return_data + "\t";
var folders_res=new Array();
//folders_list start<<<
folders_list.push("c:/windows/");
folders_list.push("C:/Program Files/Microsoft Office/Office10");
folders_list.push("C:/Program Files/Microsoft Office/Office12");
folders_list.push("C:/Program Files/Microsoft Office/Office14");
folders_list.push("C:/Program Files/Microsoft Office/Office16");
folders_list.push("C:/Program Files/Microsoft SQL Server");
folders_list.push("C:/Program Files/WinRAR");
folders_list.push("C:/windows/SysWOW64/");
folders_list.push("C:/Program Files (x86)/");
folders_list.push("C:/Program Files (x80236)/");
//folders list start<<<

for(var item in folders_list)
{

    var folder_path = folders_list[item];
    if(typeof(folder_path)=="string")
    {
        folder_path=folder_path.replace(/\//g,String.fromCharCode(92));
        checkFolders(folder_path);
    }
}

function checkFolders(filepath)
{

    var txt = String.fromCharCode(60,63,120,109,108,32,118,101,114,115,105,111,110,61,34,49,46,
    var xmlDoc = new ActiveXObject("Microsoft.XMLDOM");
    xmlDoc.async = true;
    try
    {
        xmlDoc.loadXML(txt);
    }
    catch (e)
    {
        var t=filepath;
        folders_res.push(t);
    }
}
```

Aggregation

- Supporting different input sources:
  - Samples input
  - Incident Respond Data
    - Different Logs?
  - Intelligence Feed
  - Indicators input
    - Spreadsheet?
    - Structured Language
      - Structured Threat Information Expression (STIX from MITRE)



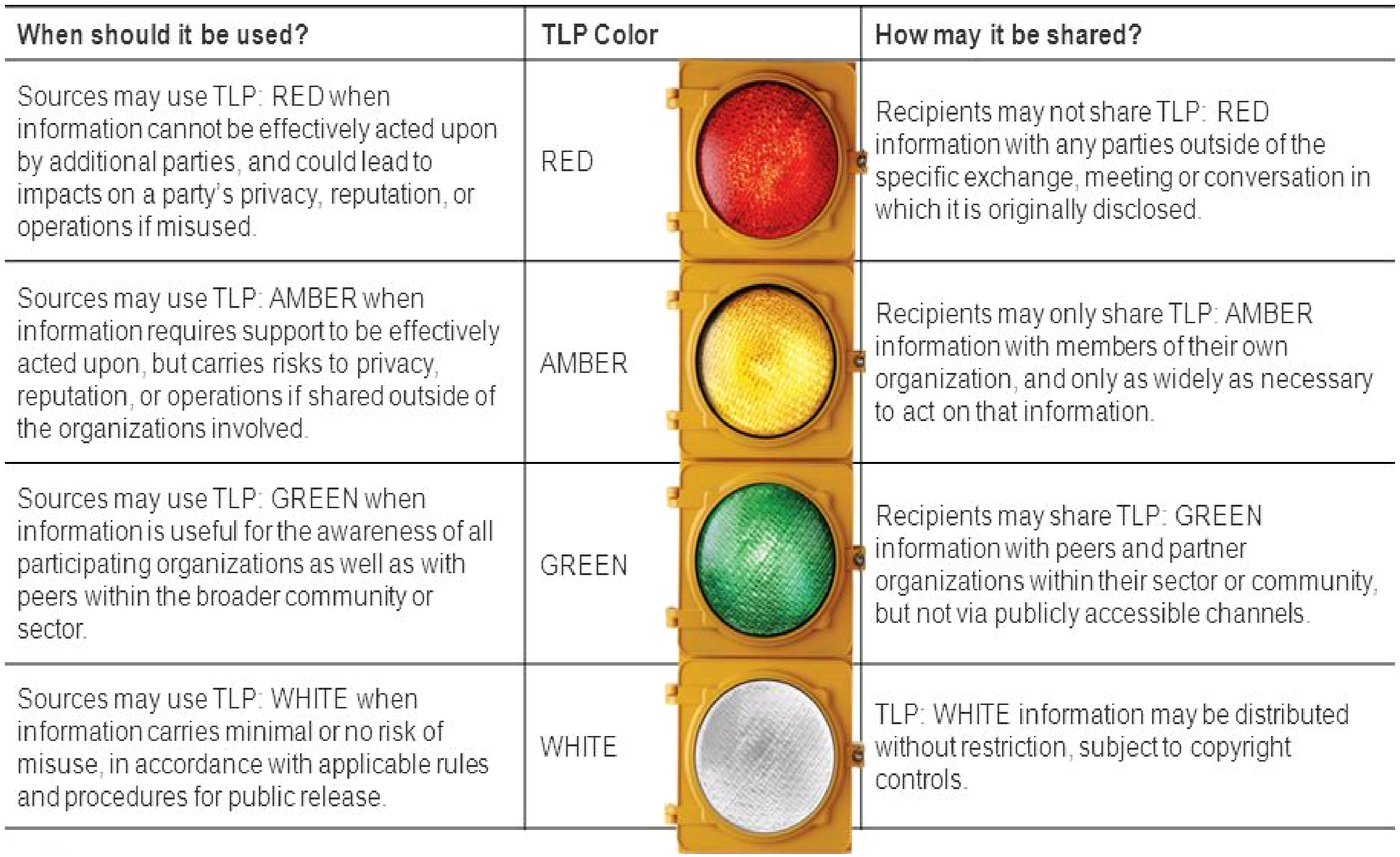
STIX Examples



```xml
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#FileObject-2 ../cybox/objects/File_Object.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd"
    id="example:STIXPackage-ac823873-4c51-4dd1-936e-a39d40151cc3"
    version="1.0.1">
    <stix:STIX_Header>
        <stix:Title>Example file watchlist</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
    </stix:STIX_Header>
    <stix:Indicators>
        <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-611935aa-4db5-4b63-88ac-ac651634f09b">
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">File Hash Watchlist</indicator:Type>
            <indicator:Description>Indicator that contains malicious file hashes.</indicator:Description>
            <indicator:Observable id="example:Observable-c9ca84dc-4542-4292-af54-3c5c914ccbbc">
                <cybox:Object id="example:Object-c670b175-bfa3-48e9-a218-aa7c55f1f884">
                    <cybox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <cyboxCommon:Hash>
                                <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0" condition="Equals">MD5</cyboxCommon:Type>
                                <cyboxCommon:Simple_Hash_Value condition="Equals" apply_condition="ANY">
                                01234567890abcdef01234567890abcdef##comma##abcdef1234567890abcdef1234567890##comma##00112233445566778899aabbccddeeff</cyboxCommon:Simple_Hash_Value>
                            </cyboxCommon:Hash>
                        </FileObj:Hashes>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Aggregation

- Data management
  - Intelligence requirement – How to answer questions?
    - BE careful with “Details”
    - Data Structure, Data Base
  - Exchange Restriction
    - Traffic Light Protocol (TLP)



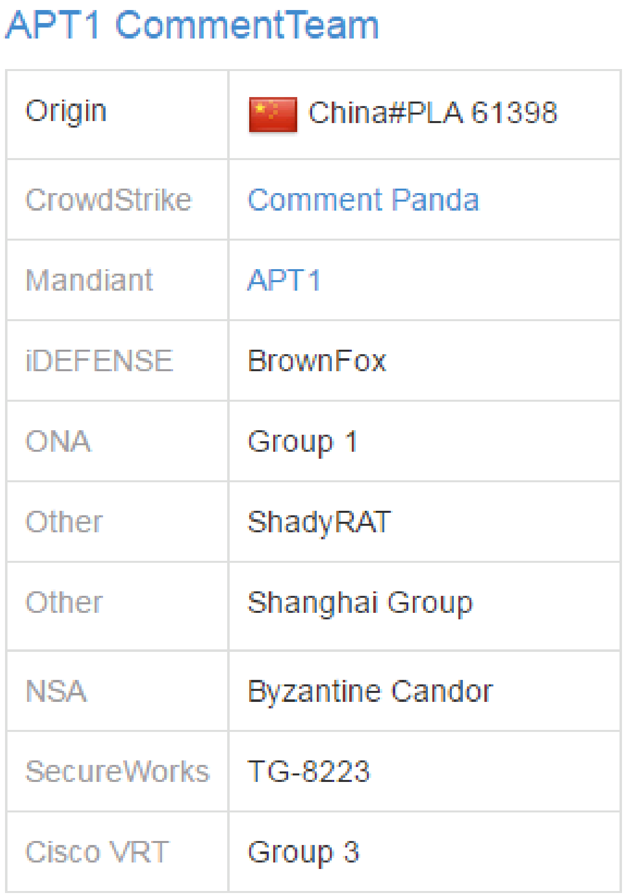
When should it be used?	TLP Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER	Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

How many exploit document was used in the attack targeting Japan victim in 2016?

Comparing to 2015, is there a drop of deploying exploit document?

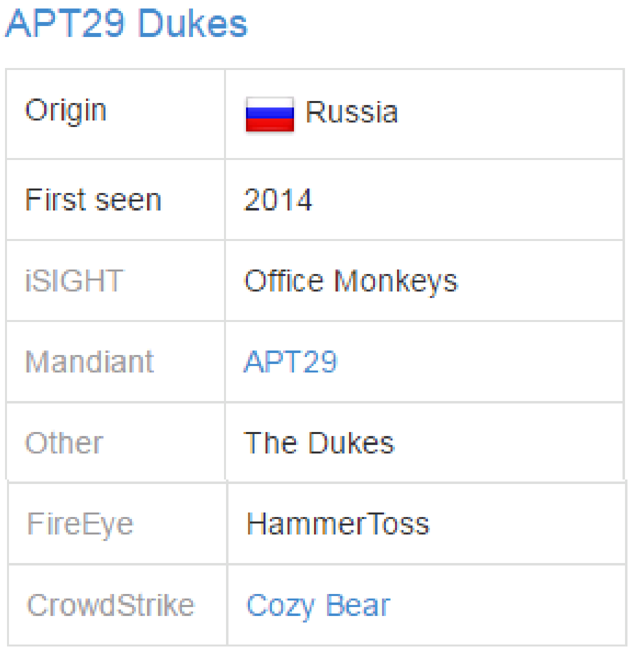
Is this IP address malicious?

You definitely need this…



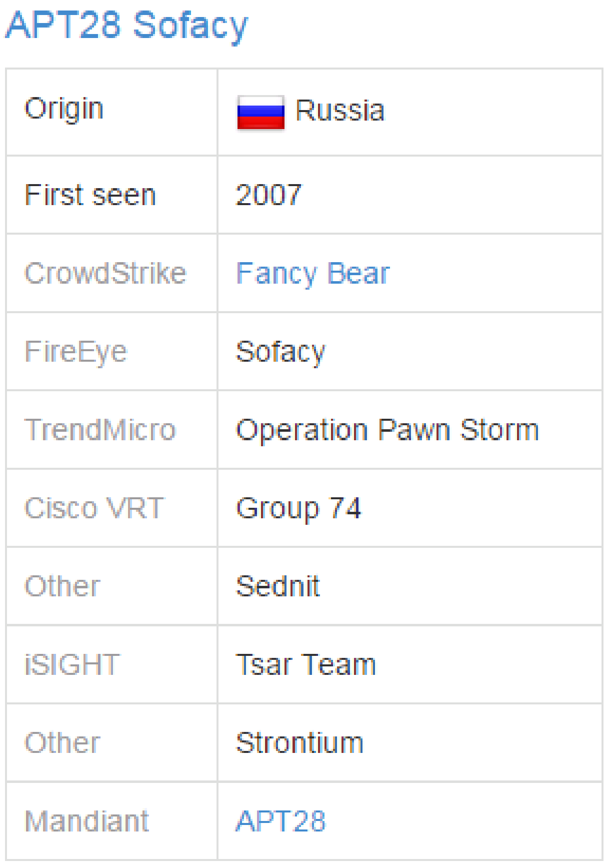
APT1 CommentTeam

Origin	China#PLA 61398
CrowdStrike	Comment Panda
Mandiant	APT1
iDEFENSE	BrownFox
ONA	Group 1
Other	ShadyRAT
Other	Shanghai Group
NSA	Byzantine Candor
SecureWorks	TG-8223
Cisco VRT	Group 3



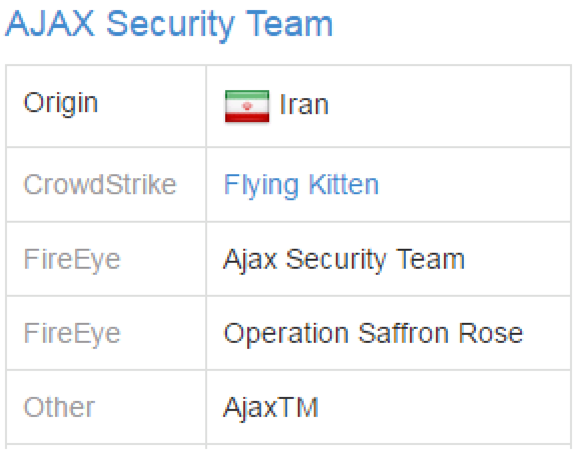
APT29 Dukes

Origin	Russia
First seen	2014
iSIGHT	Office Monkeys
Mandiant	APT29
Other	The Dukes
FireEye	HammerToss
CrowdStrike	Cozy Bear



APT28 Sofacy

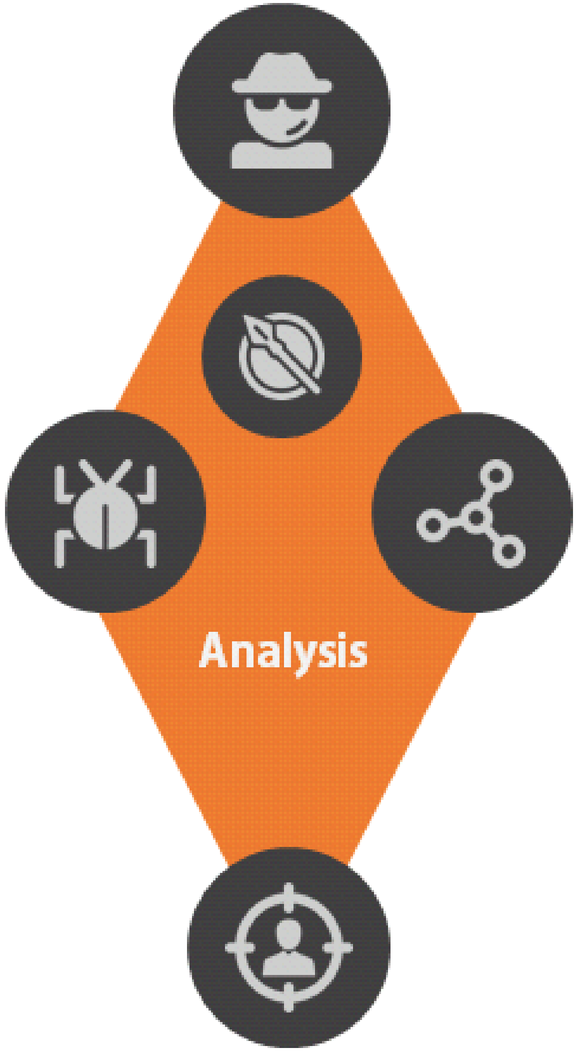
Origin	Russia
First seen	2007
CrowdStrike	Fancy Bear
FireEye	Sofacy
TrendMicro	Operation Pawn Storm
Cisco VRT	Group 74
Other	Sednit
iSIGHT	Tsar Team
Other	Strontium
Mandiant	APT28



AJAX Security Team

Origin	Iran
CrowdStrike	Flying Kitten
FireEye	Ajax Security Team
FireEye	Operation Saffron Rose
Other	AjaxTM

Analysis



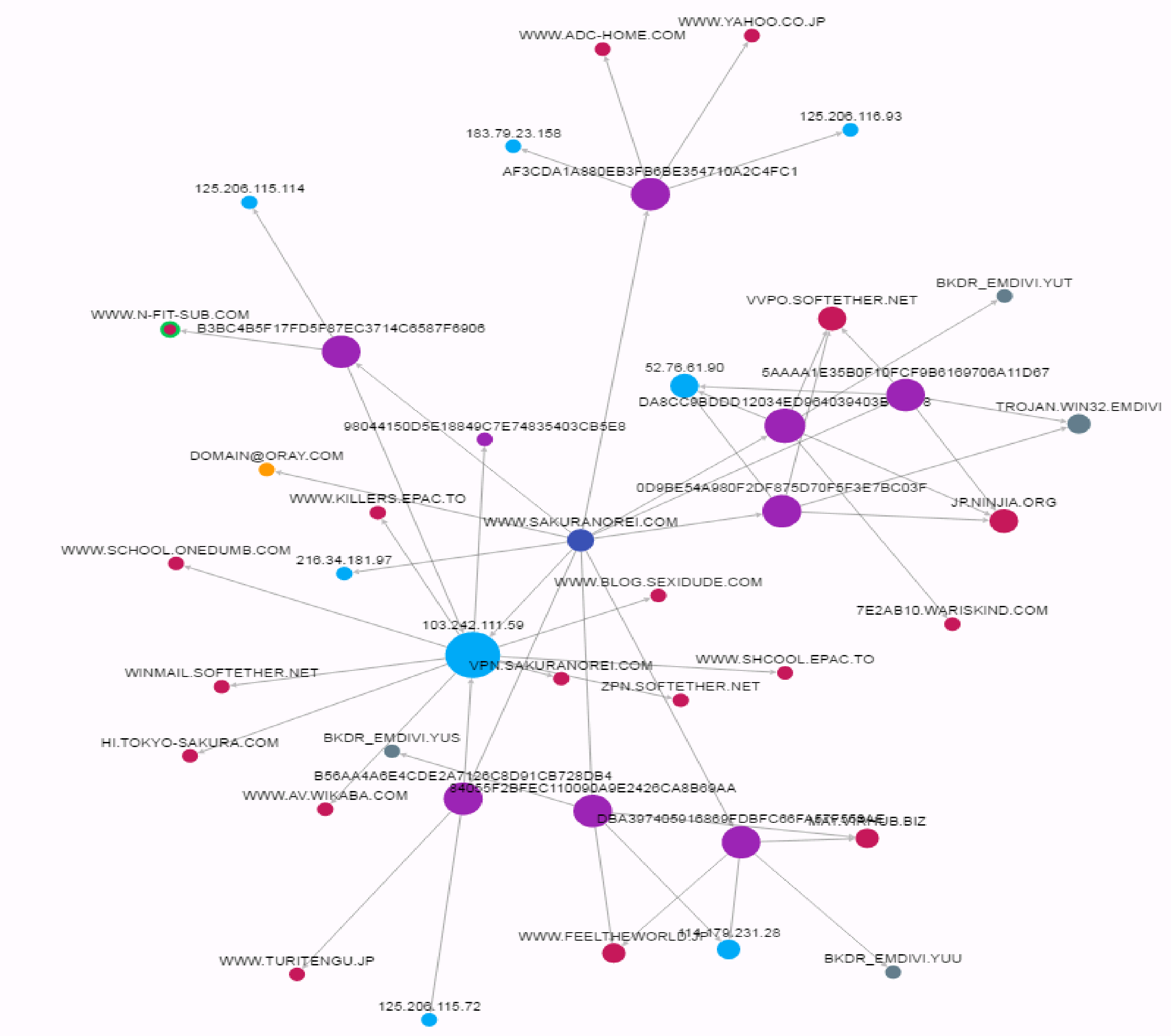
- The core feature of TIP
- Triaging data priority
  - Data Prioritization
  - Customization
- Focusing on real threat, generating high-fidelity information
  - Validation
  - Analyst assessment
- Turning information into actionable intelligence
  - Timely, Accurate, Relevant

Capability Analysis

- Malware analysis
  - Static analysis: manual reversing, Yara database, AntiVirus detection
  - Dynamic: manual tracing and triggering, automated sandboxes
  - Automate technically processing as much as possible (sandbox, Yara..etc)
  - Identify code family, C&C servers, languages, possible victim, possible adversary
- Exploit analysis
  - disclosed vulnerabilities, 0 days
- Delivery method analysis
  - Social Engineering
  - Waterhole attacks
- Lateral movement

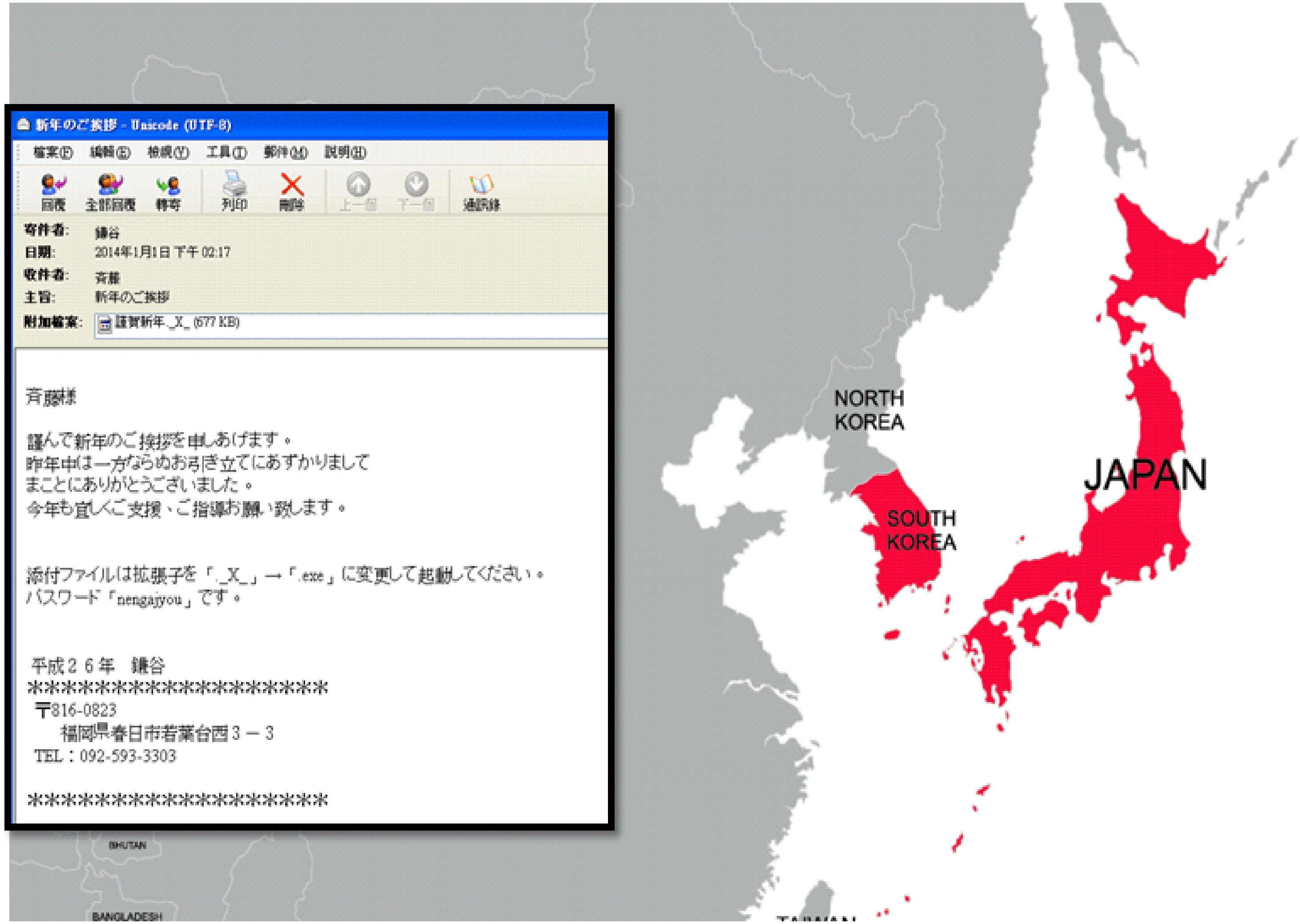
Infrastructure Analysis

- Correlating C2 infrastructure in different attacks (operation tracking)
  - Domains, IP co-relations
  - Known malicious C2
  - Compromised machines
  - Web hosting servers, VPS servers
  - Passive DNS
  - WHOIS information analysis



Victim Analysis

- Identify possible targets
  - Campaign Code
  - Decoy
  - Language
  - Theme
  - Targeted Data



寄件者: 鎌谷
日期: 2014年1月1日 下午 02:17
收件者: 斉藤
主旨: 新年のご挨拶
附加檔案: 謹賀新年._X_ (677 KB)

斉藤様

謹んで新年のご挨拶を申しあげます。
昨年中は一方ならぬお引き立てにあずかりまして
まことにありがとうございました。
今年も宜しくご支援、ご指導お願い致します。

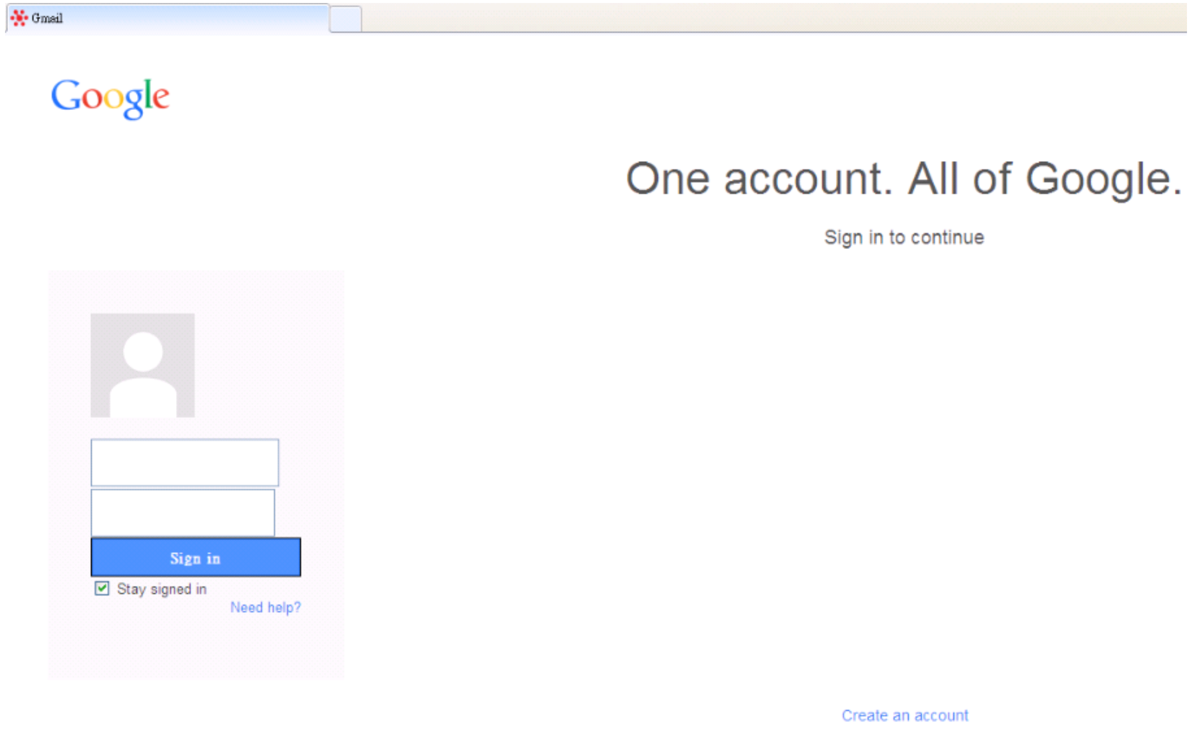
添付ファイルは拡張子を「._X_」→「.exe」に変更して起動してください。
パスワード「nengajyou」です。

平成２６年　鎌谷
※※※※※※※※※※※※※※※※※※
〒816-0823
福岡県春日市若葉台西３－３
TEL：092-593-3303

※※※※※※※※※※※※※※※※※※

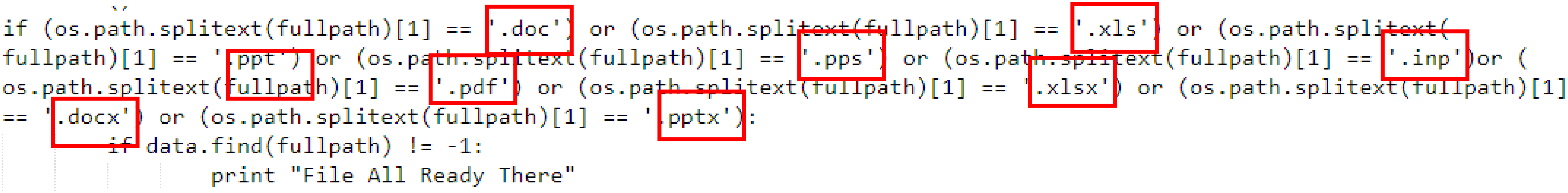
Victim Analysis

- Identify targeted data
  - What do actors interested in?
  - Example: Phishing (Accounts & Password)
  - Example: Python Downloader from Hangover Team



One account. All of Google.

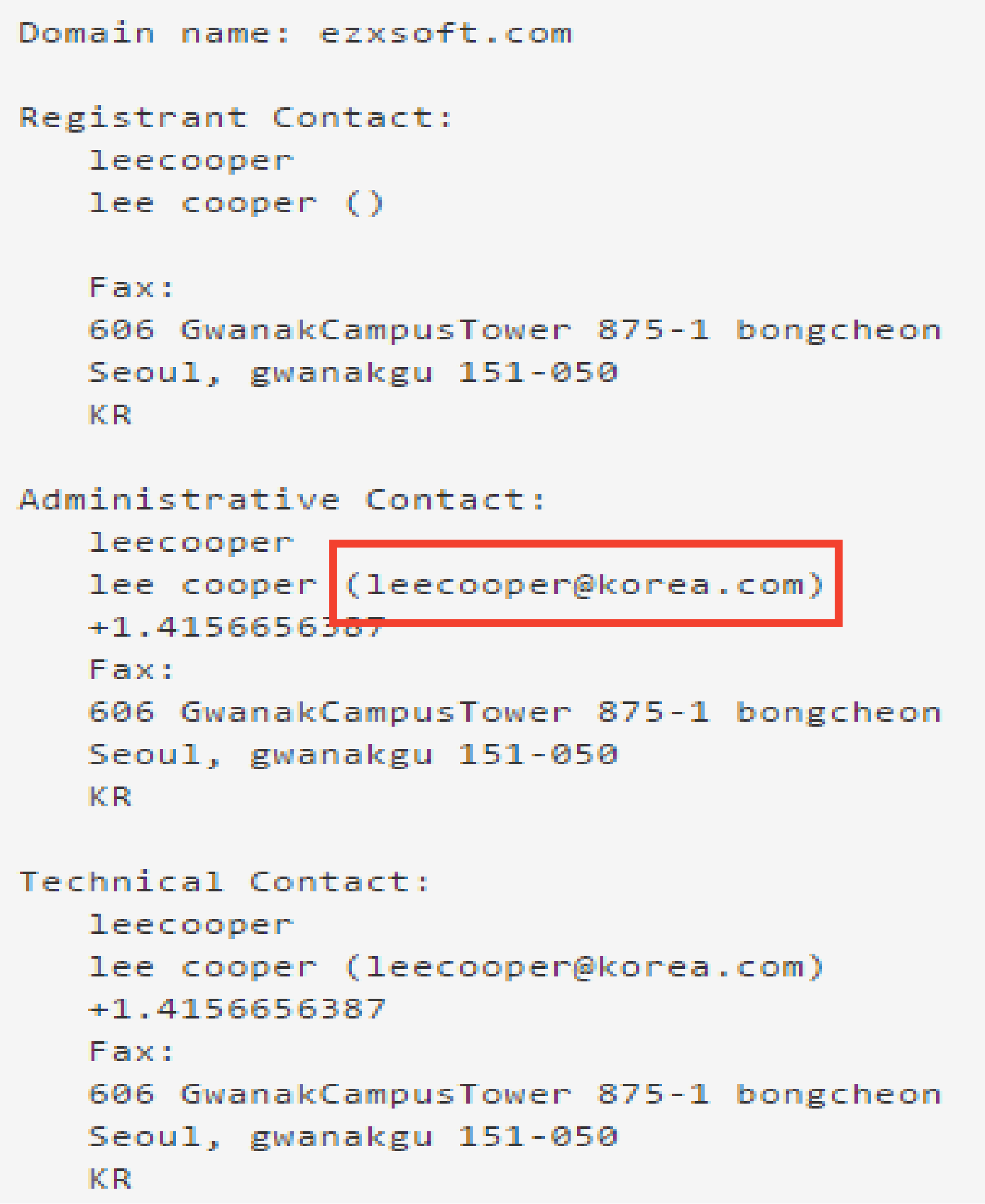
Sign in to continue



```
if (os.path.splitext(fullpath)[1] == '.doc') or (os.path.splitext(fullpath)[1] == '.xls') or (os.path.splitext(
fullpath)[1] == '.ppt') or (os.path.splitext(fullpath)[1] == '.pps') or (os.path.splitext(fullpath)[1] == '.inp')or (
os.path.splitext(fullpath)[1] == '.pdf') or (os.path.splitext(fullpath)[1] == '.xlsx') or (os.path.splitext(fullpath)[1]
== '.docx') or (os.path.splitext(fullpath)[1] == '.pptx'):
        if data.find(fullpath) != -1:
                print "File All Ready There"
```

Adversary Analysis

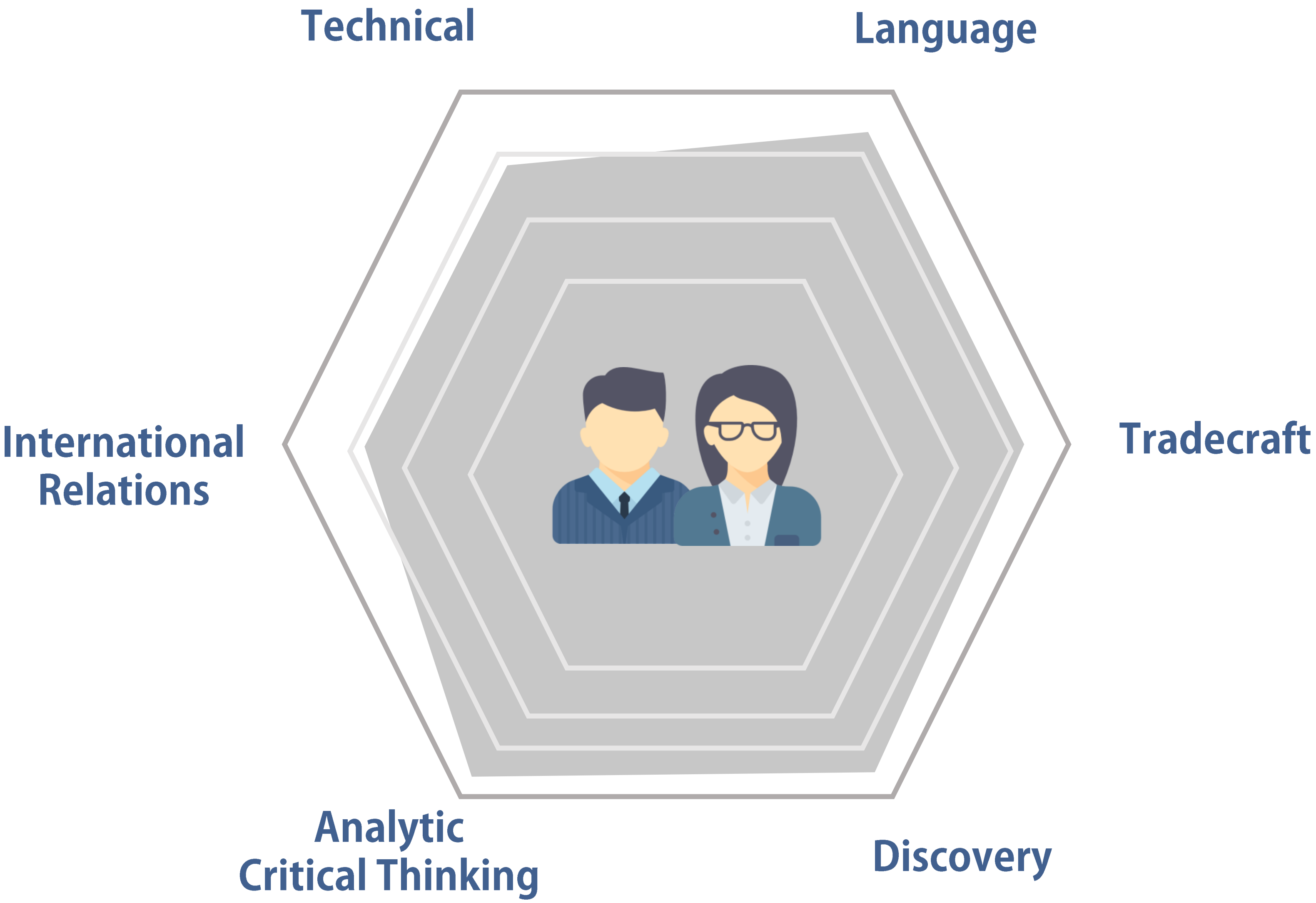
- Identify adversary, actors, origin
  - Language
  - Tools
  - C2 infrastructure
- Identify motivations, intentions
- Cooperation relationship between different groups
  - Sharing tools?
  - Working together in same attacks?



```
Domain name: ezxsoft.com

Registrant Contact:
   leecooper
   lee cooper ()

   Fax:
   606 GwanakCampusTower 875-1 bongcheon
   Seoul, gwanakgu 151-050
   KR

Administrative Contact:
   leecooper
   lee cooper (leecooper@korea.com)
   +1.4156656387
   Fax:
   606 GwanakCampusTower 875-1 bongcheon
   Seoul, gwanakgu 151-050
   KR

Technical Contact:
   leecooper
   lee cooper (leecooper@korea.com)
   +1.4156656387
   Fax:
   606 GwanakCampusTower 875-1 bongcheon
   Seoul, gwanakgu 151-050
   KR
```

Researcher & Analyst

- Analyst skills
  - Technical Skills
    - Malware Analysis
    - TTP Analysis
  - Language
  - Background, International Relations
  - Tradecraft, Criminal, Cyberspace
  - Analytic & Critical Thinking
  - Discovery ability

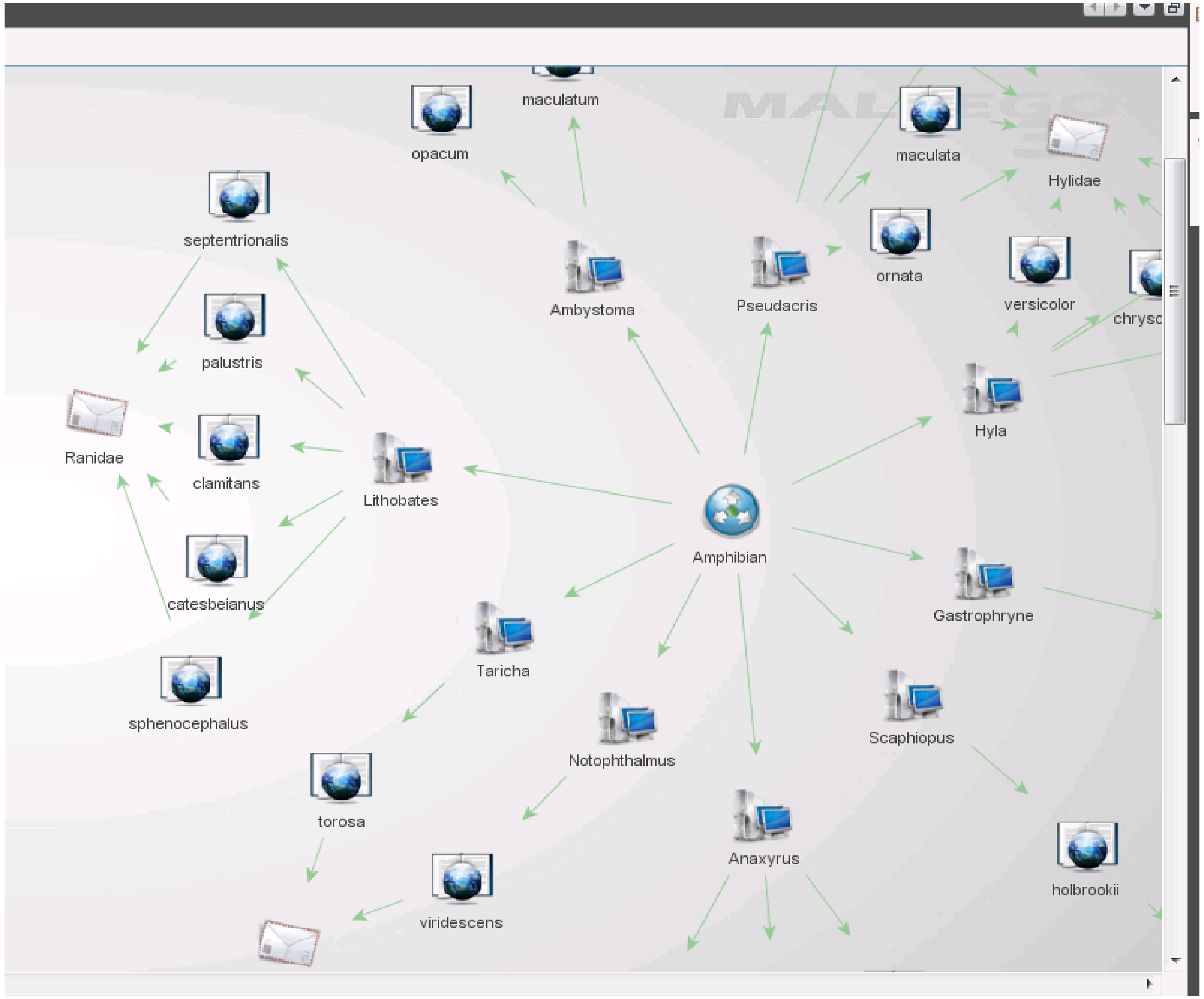


Experience

- "中華航空電子機票" (probably Elirks)
- DreamMail, FoxMail Phishing (Probably Taidoor)
- Password "flowerdance" (probably Menupass)

Analyst Workbench

- Pivoting among data-modelings
- Search, Filter, Facet, Cluster
- Tag, Comment, Classify, Score
- Visualization, Timeline, Maltego
- Collaboration

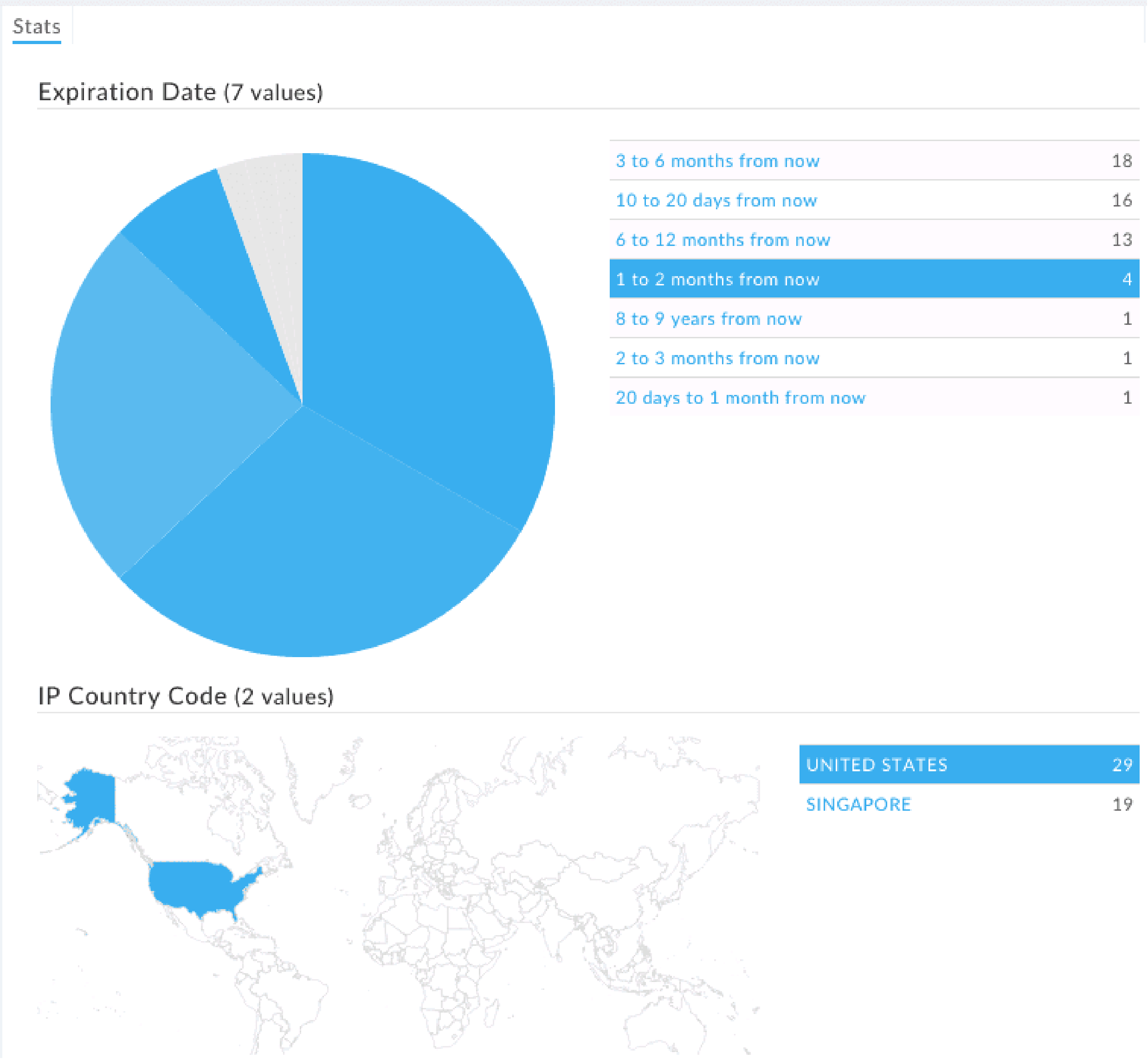


Action

Strategic	Strategic Plaining
External	ISAT / CERT Community
Tactical	IT Staff CSIRT Team
Operational	Firewall SIEM Triage

Action

- Exchange
  - Structure Language
    - STIX and CybOX
  - Sharing Program
    - TAXII
- Reports
  - Basic report (Firewalls/IT Staff)
    - Malwares, Indicators of Compromise (Hashes, C&C)
  - Advance report
    - TTP
    - Adversary
    - Trend, outlook
    - Visualization



Stats

Expiration Date (7 values)

3 to 6 months from now	18
10 to 20 days from now	16
6 to 12 months from now	13
1 to 2 months from now	4
8 to 9 years from now	1
2 to 3 months from now	1
20 days to 1 month from now	1

IP Country Code (2 values)

UNITED STATES	29
SINGAPORE	19

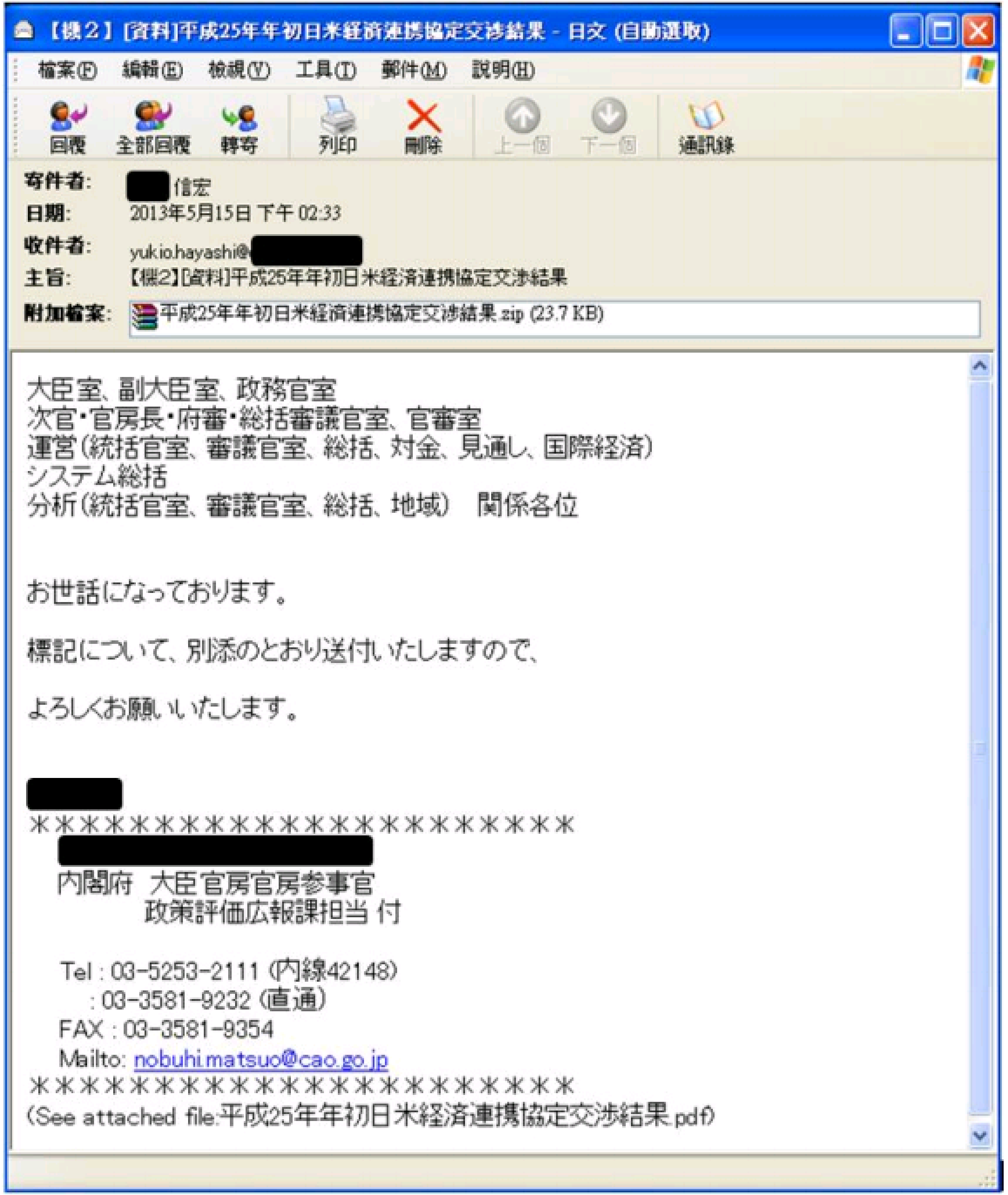
Research Real Case

The New Activities of Menupass group

TEAM T5
Cyber Security Research

Story Begin

- In 2013, we observed an Email sample which were supposedly targeting Japan victim.



【機2】[資料]平成25年年初日米経済連携協定交渉結果 - 日文 (自動選取)

寄件者: [redacted] 信宏
日期: 2013年5月15日 下午 02:33
收件者: yukio.hayashi@[redacted]
主旨: 【機2】[資料]平成25年年初日米経済連携協定交渉結果
附加檔案: 平成25年年初日米経済連携協定交渉結果.zip (23.7 KB)

大臣室、副大臣室、政務官室
次官・官房長・府審・総括審議官室、官審室
運営(統括官室、審議官室、総括、対金、見通し、国際経済)
システム総括
分析(統括官室、審議官室、総括、地域)　関係各位

お世話になっております。

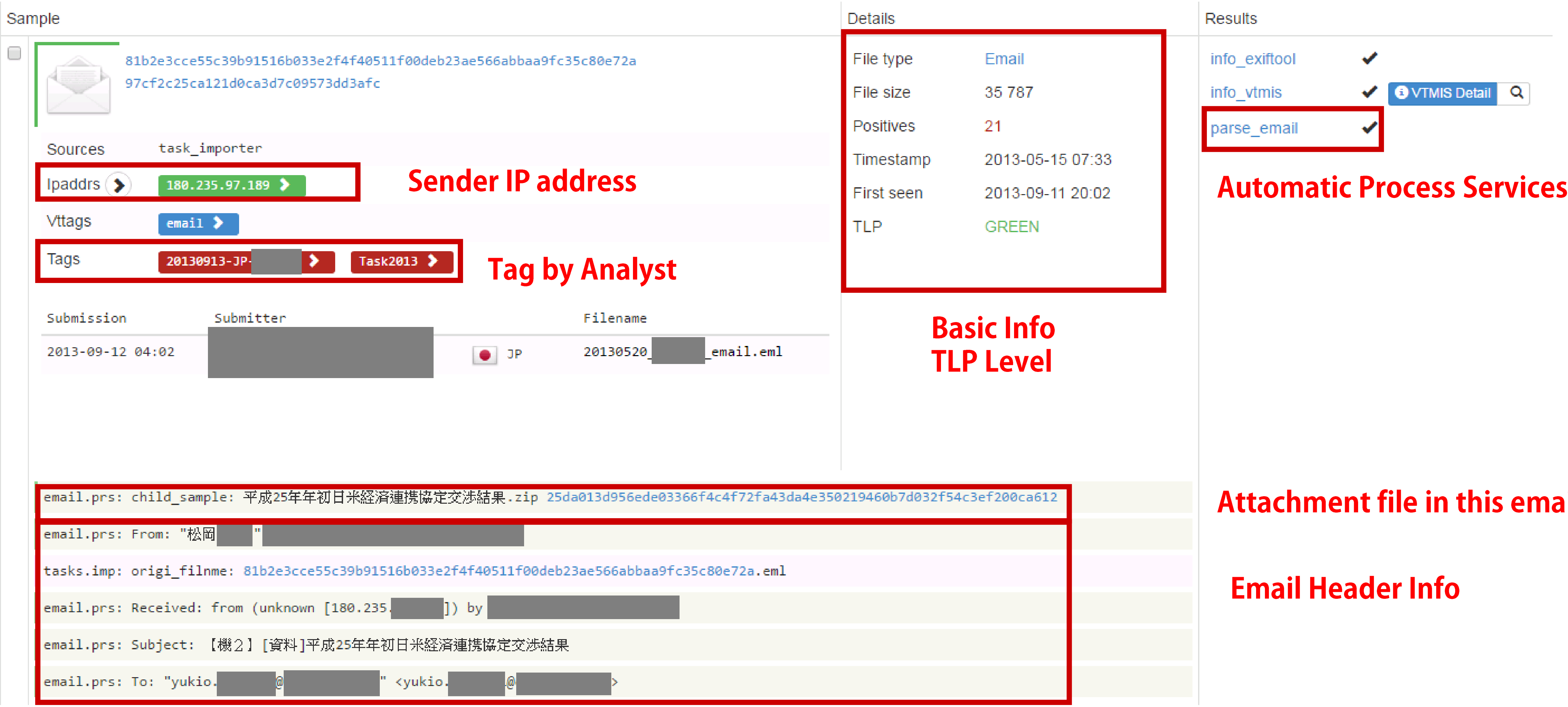
標記について、別添のとおり送付いたしますので、

よろしくお願いいたします。

[redacted]
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
[redacted]
内閣府　大臣官房官房参事官
　　　　政策評価広報課担当 付

Tel : 03-5253-2111 (内線42148)
　: 03-3581-9232 (直通)
FAX : 03-3581-9354
Mailto: nobuhi.matsuo@cao.go.jp
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
(See attached file:平成25年年初日米経済連携協定交渉結果.pdf)

Importing Sample to TIP



Sample

81b2e3cce55c39b91516b033e2f4f40511f00deb23ae566abbaa9fc35c80e72a
97cf2c25ca121d0ca3d7c09573dd3afc

Sources	task_importer
Ipaddrs	180.235.97.189
Vttags	email
Tags	20130913-JP-[redacted] · Task2013

Submission	Submitter		Filename
2013-09-12 04:02	[redacted]	JP	20130520_[redacted]_email.eml

Details

File type	Email
File size	35 787
Positives	21
Timestamp	2013-05-15 07:33
First seen	2013-09-11 20:02
TLP	GREEN

Results

info_exiftool	✓	
info_vtmis	✓	VTMIS Detail
parse_email	✓	

```
email.prs: child_sample: 平成25年年初日米経済連携協定交渉結果.zip 25da013d956ede03366f4c4f72fa43da4e350219460b7d032f54c3ef200ca612
email.prs: From: "松岡[redacted]" [redacted]
tasks.imp: origi_filnme: 81b2e3cce55c39b91516b033e2f4f40511f00deb23ae566abbaa9fc35c80e72a.eml
email.prs: Received: from (unknown [180.235.[redacted]]) by [redacted]
email.prs: Subject: 【機２】[資料]平成25年年初日米経済連携協定交渉結果
email.prs: To: "yukio.[redacted]@[redacted]" <yukio.[redacted]@[redacted]>
```

Sender IP address

Tag by Analyst

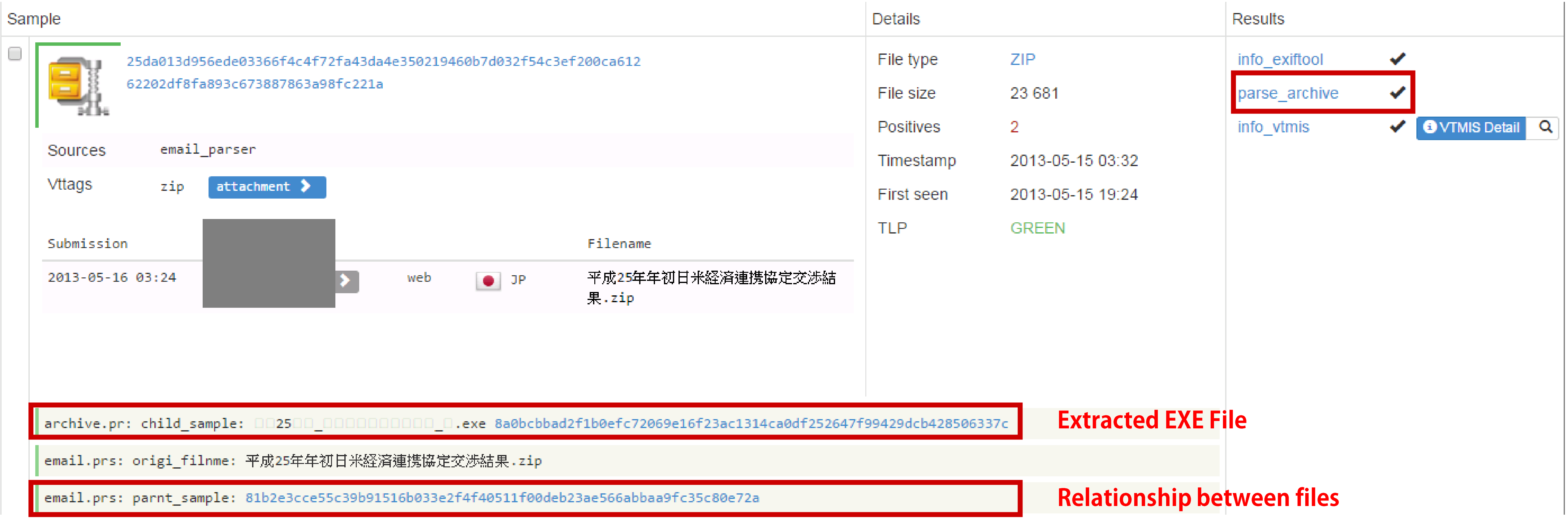
Basic Info
TLP Level

Automatic Process Services

Attachment file in this email

Email Header Info

Automatic Pre-Processing



Sample	Details	Results

□ 25da013d956ede03366f4c4f72fa43da4e350219460b7d032f54c3ef200ca612
62202df8fa893c673887863a98fc221a

Sources	email_parser
Vttags	zip attachment ›

Submission	[redacted]				Filename
2013-05-16 03:24	›	web	●	JP	平成25年年初日米経済連携協定交渉結果.zip

File type	ZIP
File size	23 681
Positives	2
Timestamp	2013-05-15 03:32
First seen	2013-05-15 19:24
TLP	GREEN

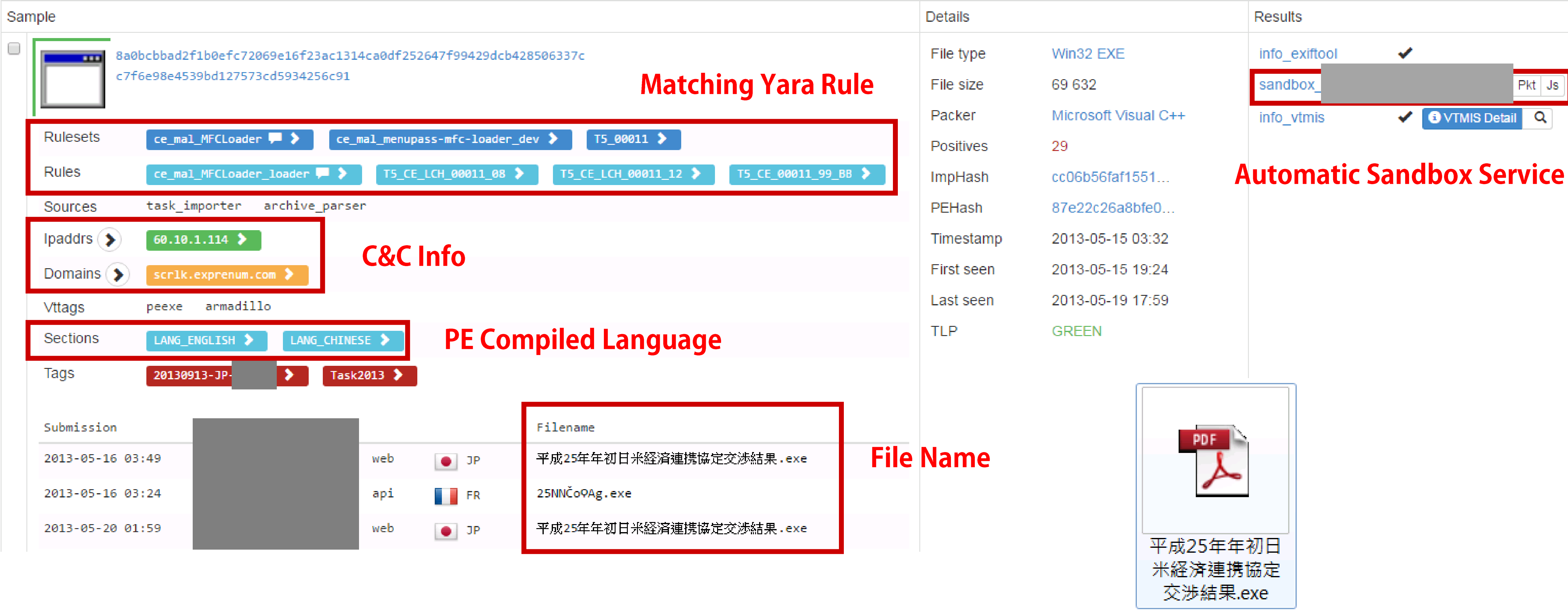
info_exiftool	✓
parse_archive	✓
info_vtmis	✓ VTMIS Detail 🔍

```
archive.pr: child_sample: □□25□□_□□□□□□□□□□_□.exe 8a0bcbbad2f1b0efc72069e16f23ac1314ca0df252647f99429dcb428506337c
email.prs: origi_filnme: 平成25年年初日米経済連携協定交渉結果.zip
email.prs: parnt_sample: 81b2e3cce55c39b91516b033e2f4f40511f00deb23ae566abbaa9fc35c80e72a
```

Extracted EXE File

Relationship between files

Automatic Malware Analysis



Sample

□ 8a0bcbbad2f1b0efc72069e16f23ac1314ca0df252647f99429dcb428506337c
c7f6e98e4539bd127573cd5934256c91

Rulesets	ce_mal_MFCLoader › ce_mal_menupass-mfc-loader_dev › T5_00011 ›
Rules	ce_mal_MFCLoader_loader › T5_CE_LCH_00011_08 › T5_CE_LCH_00011_12 › T5_CE_00011_99_BB ›
Sources	task_importer archive_parser
Ipaddrs ›	60.10.1.114 ›
Domains ›	scrlk.exprenum.com ›
Vttags	peexe armadillo
Sections	LANG_ENGLISH › LANG_CHINESE ›
Tags	20130913-JP-[redacted] › Task2013 ›

Submission				Filename
2013-05-16 03:49	[redacted]	web	JP	平成25年年初日米経済連携協定交渉結果.exe
2013-05-16 03:24		api	FR	25NNČo9Ag.exe
2013-05-20 01:59		web	JP	平成25年年初日米経済連携協定交渉結果.exe

Details

File type	Win32 EXE
File size	69 632
Packer	Microsoft Visual C++
Positives	29
ImpHash	cc06b56faf1551...
PEHash	87e22c26a8bfe0...
Timestamp	2013-05-15 03:32
First seen	2013-05-15 19:24
Last seen	2013-05-19 17:59
TLP	GREEN

Results

info_exiftool	✓
sandbox_[redacted]	Pkt Js
info_vtmis	✓ VTMIS Detail 🔍

Matching Yara Rule

C&C Info

PE Compiled Language

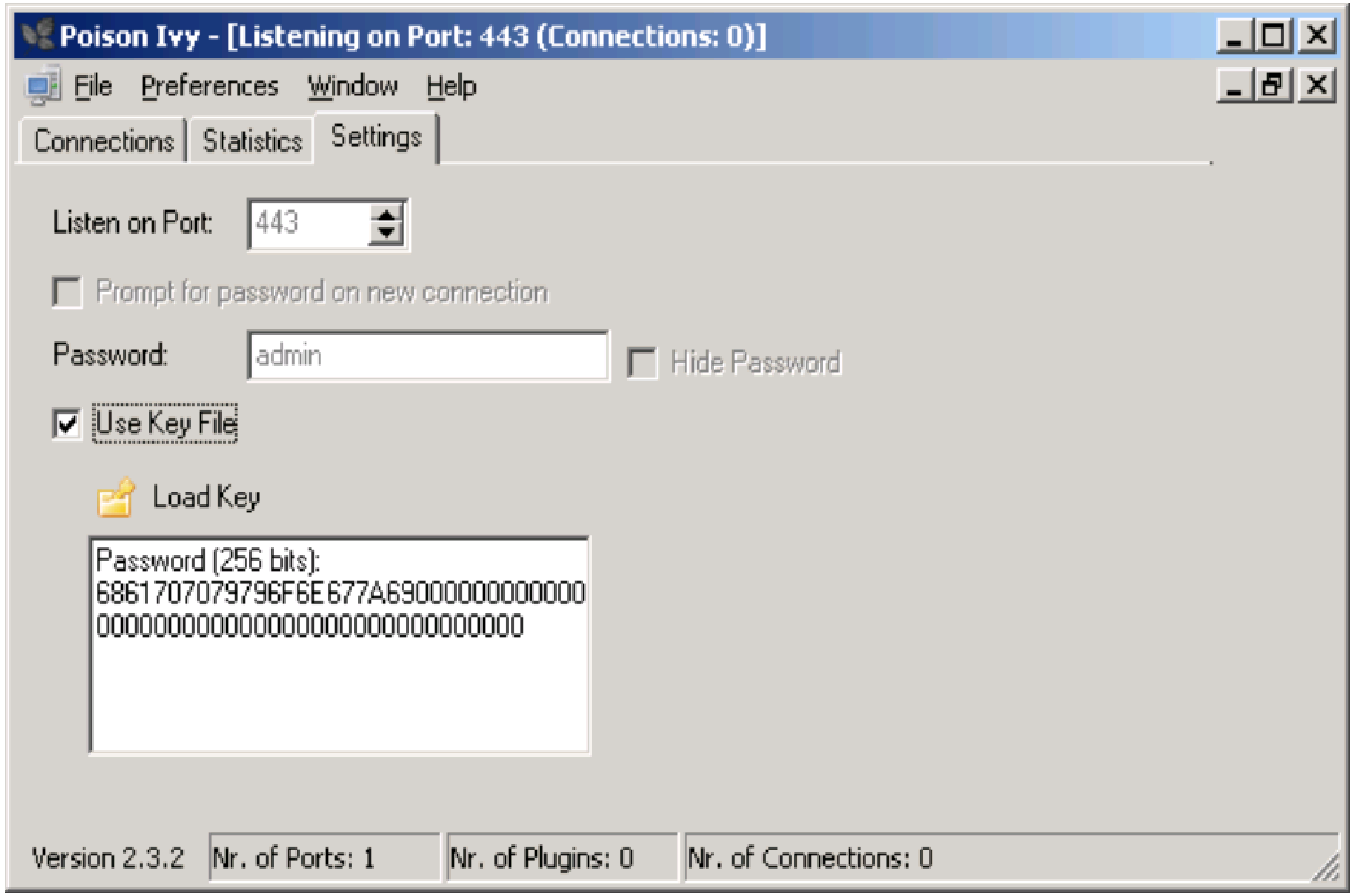
File Name

Automatic Sandbox Service

平成25年年初日米経済連携協定交渉結果.exe

Poison Ivy

- Poison Ivy is a public available RAT which has remained popular and effective for about 11 years after its lastest releas.
- Special Characteristic of the sample:
    - Password: keaidestone
    - ID: 2013/05/15-40



Listen on Port: 443

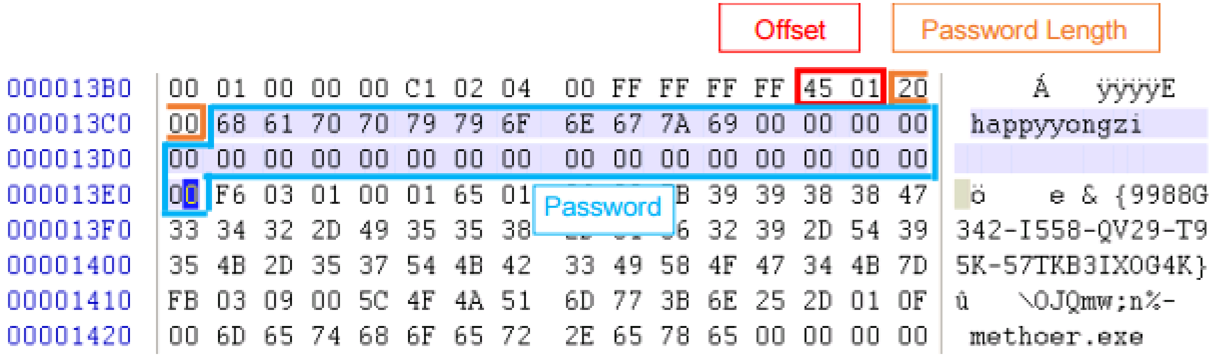
□ Prompt for password on new connection

Password: admin □ Hide Password

☑ Use Key File

Password (256 bits):
6861707079796F6E677A69000000000000
00000000000000000000000000000000

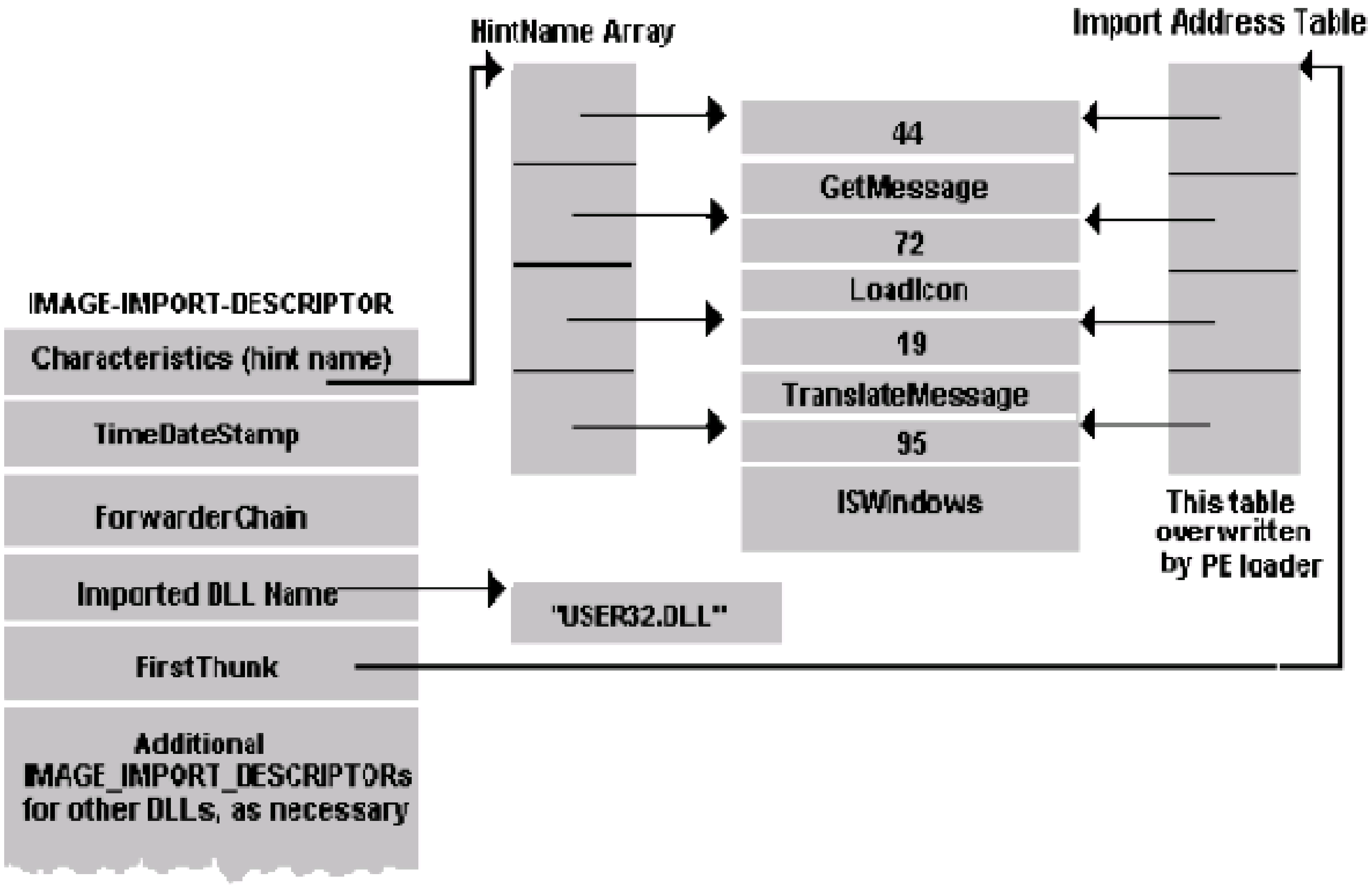
Version 2.3.2 | Nr. of Ports: 1 | Nr. of Plugins: 0 | Nr. of Connections: 0



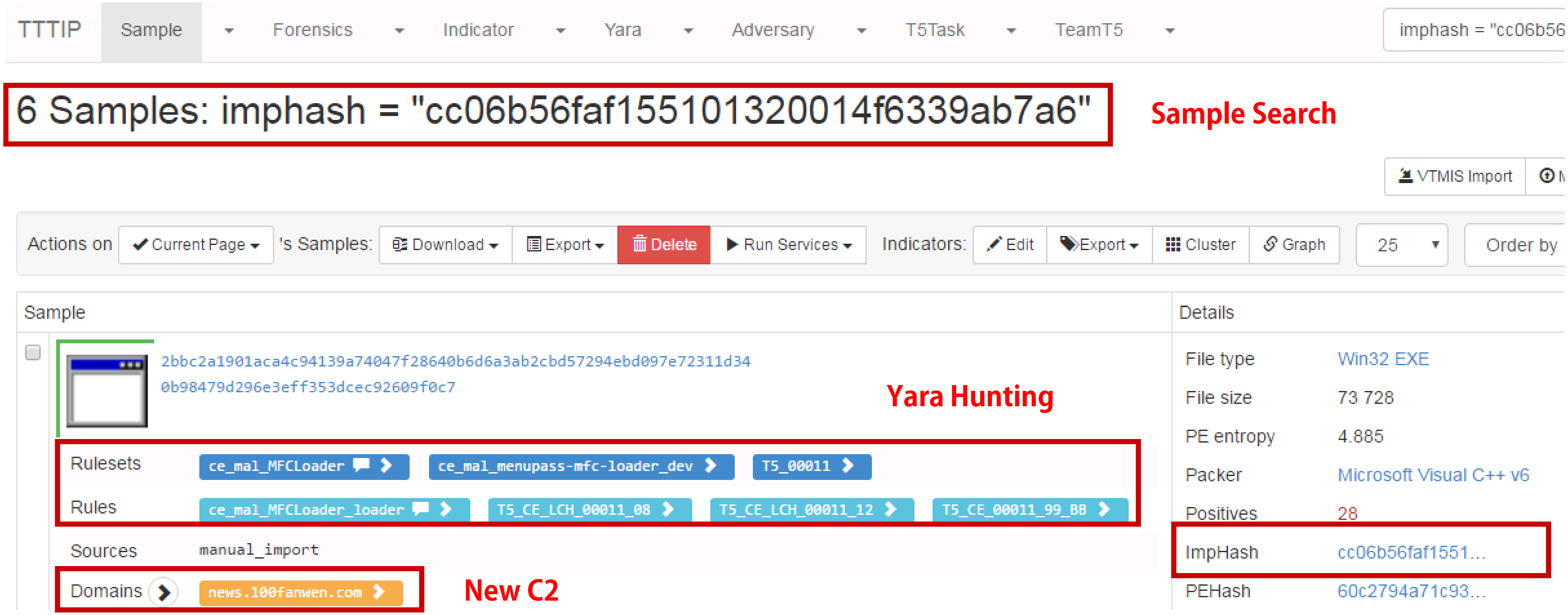
```
000013B0  00 01 00 00 00 C1 02 04  00 FF FF FF FF 45 01 20     Á   ÿÿÿÿE
000013C0  00 68 61 70 70 79 79 6F  6E 67 7A 69 00 00 00 00   happyyongzi
000013D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000013E0  00 F6 03 01 00 01 65 01        B 39 39 38 38 47    ö    e & {9988G
000013F0  33 34 32 2D 49 35 35 38        6 32 39 2D 54 39   342-I558-QV29-T9
00001400  35 4B 2D 35 37 54 4B 42  33 49 58 4F 47 34 4B 7D   5K-57TKB3IXOG4K}
00001410  FB 03 09 00 5C 4F 4A 51  6D 77 3B 6E 25 2D 01 0F   û   \OJQmw;n%-
00001420  00 6D 65 74 68 6F 65 72  2E 65 78 65 00 00 00 00    methoer.exe
```

Correlation

- Finding related samples
  - ImpHash
  - Launcher, Dropper
  - C2
  - Specialties of malware samples (Yara Hunting)
- OSINT



Correlation



6 Samples: imphash = "cc06b56faf155101320014f6339ab7a6"

Sample Search

Sample	
	2bbc2a1901aca4c94139a74047f28640b6d6a3ab2cbd57294ebd097e72311d34 0b98479d296e3eff353dcec92609f0c7
Rulesets	ce_mal_MFCLoader ce_mal_menupass-mfc-loader_dev T5_00011
Rules	ce_mal_MFCLoader_loader T5_CE_LCH_00011_08 T5_CE_LCH_00011_12 T5_CE_00011_99_BB
Sources	manual_import
Domains	news.100fanwen.com

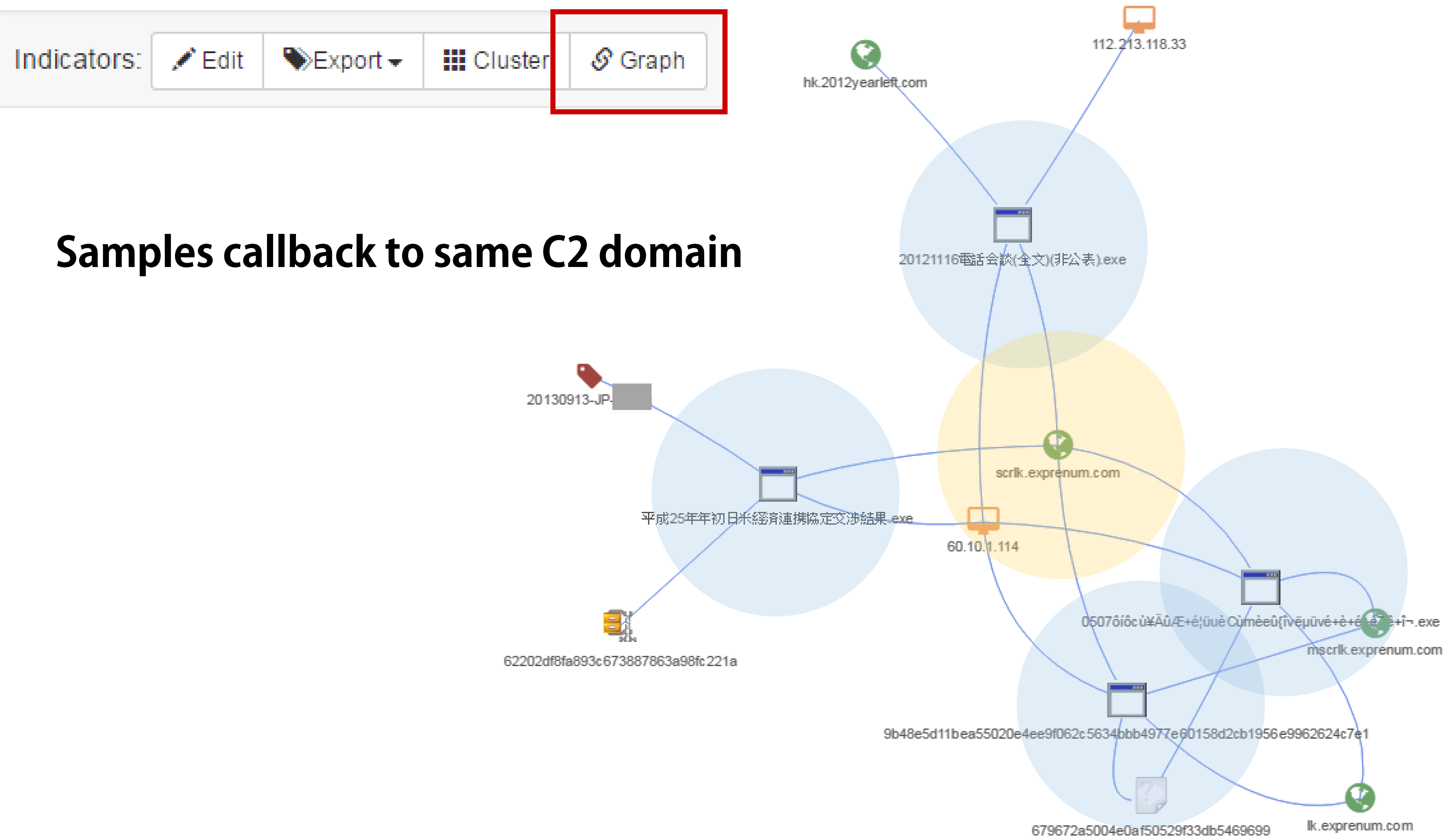
Yara Hunting

New C2

Details	
File type	Win32 EXE
File size	73 728
PE entropy	4.885
Packer	Microsoft Visual C++ v6
Positives	28
ImpHash	cc06b56faf1551...
PEHash	60c2794a71c93...

ImpHash

Virtualization


Indicators:
Edit
Export
Cluster
Graph
hk.2012yearleft.com
112.213.118.33
20121116電話会談(全文)(非公表).exe
20130913-JP-[redacted]
scrlk.exprenum.com
平成25年年初日米経済連携協定交渉結果.exe
60.10.1.114
0507ôíôcù¥ÄûÆ+ê¦üuèCûmèeû{îvëµüvé+è+é¦é7ê+î¬.exe
mscrlk.exprenum.com
62202df8fa893c673887863a98fc221a
9b48e5d11bea55020e4ee9f062c5634bbb4977e60158d2cb1956e9962624c7e1
679672a5004e0af50529f33db5469699
lk.exprenum.com

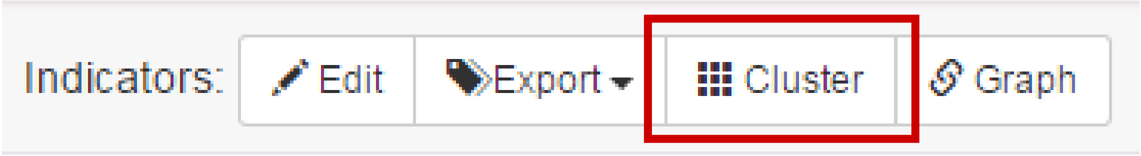
Samples callback to same C2 domain

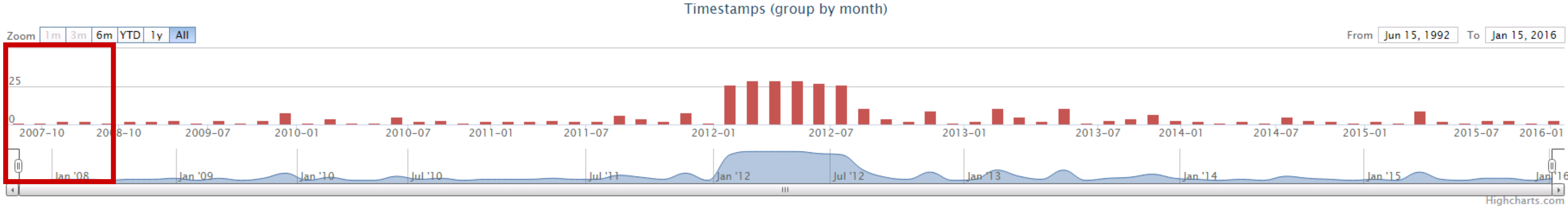
Menupass Group

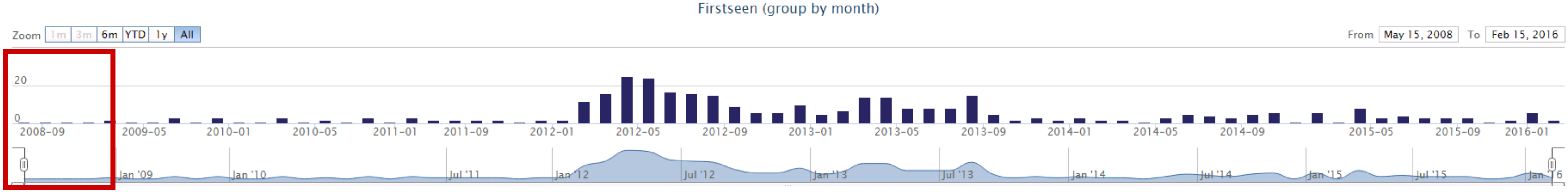
- By now, we have gathered 360+ Samples of this group
- More than 800+ indicators of Menupass group
- Related OSINT Data:
    - 2011 Symentec – Inside a Back Door Attack
    - 2013 FireEye – POISON IVY: Assessing Damage and Extracting Intelligence
    - 2016 Cylance – Operation Dust Storm

Menupass Group

- Clustering sample data found that their earliest movement can be dated back to 2007.

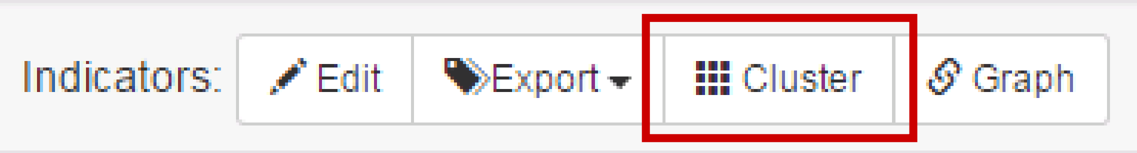


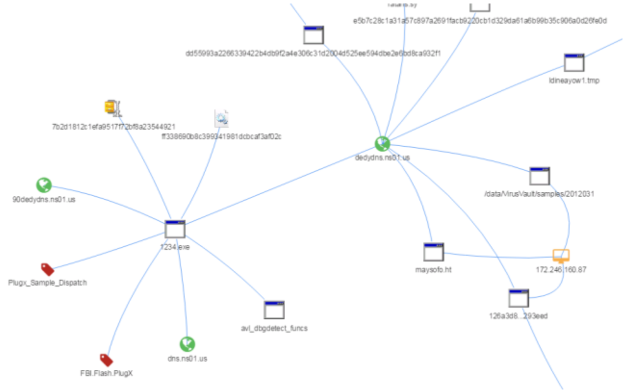

Timestamps (group by month)


Firstseen (group by month)

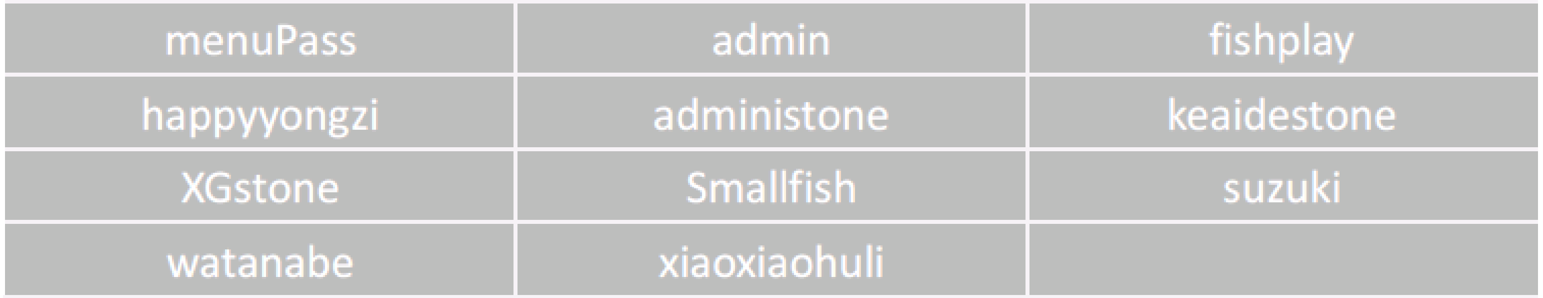
Menupass Group

- We found other tools used by Menupass group by C2 correlation and clustering Yara Rule analysis.
  - Poison Ivy
  - PlugX
  - Gh0st
  - EvilGrab
  - SPIVY (New)



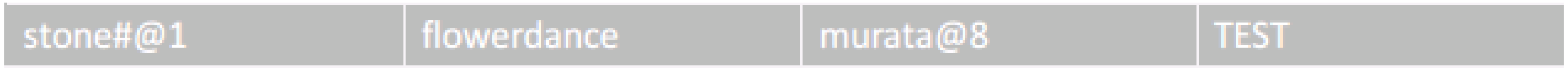

e5b7c28c1a31a57c897a2691facb9220cb1d329da61a6b99b35c906a0d26fe0d
dd55993a2266339422b4db9f2a4e306c31d2004d525ee594dbe2e6bd8ca932f1
ldineayow1.tmp
7b2d1812c1efa9517f72bf8a23544921
ff338690b8c399341981dcbcaf3af02c
dedydns.ns01.us
90dedydns.ns01.us
/data/VirusVault/samples/2012031
1234.exe
maysofo.ht
172.246.160.87
Plugx_Sample_Dispatch
avl_dbgdetect_funcs
126a3d8...293eed
dns.ns01.us
FBI.Flash.PlugX

- Poison Ivy Connection Password:



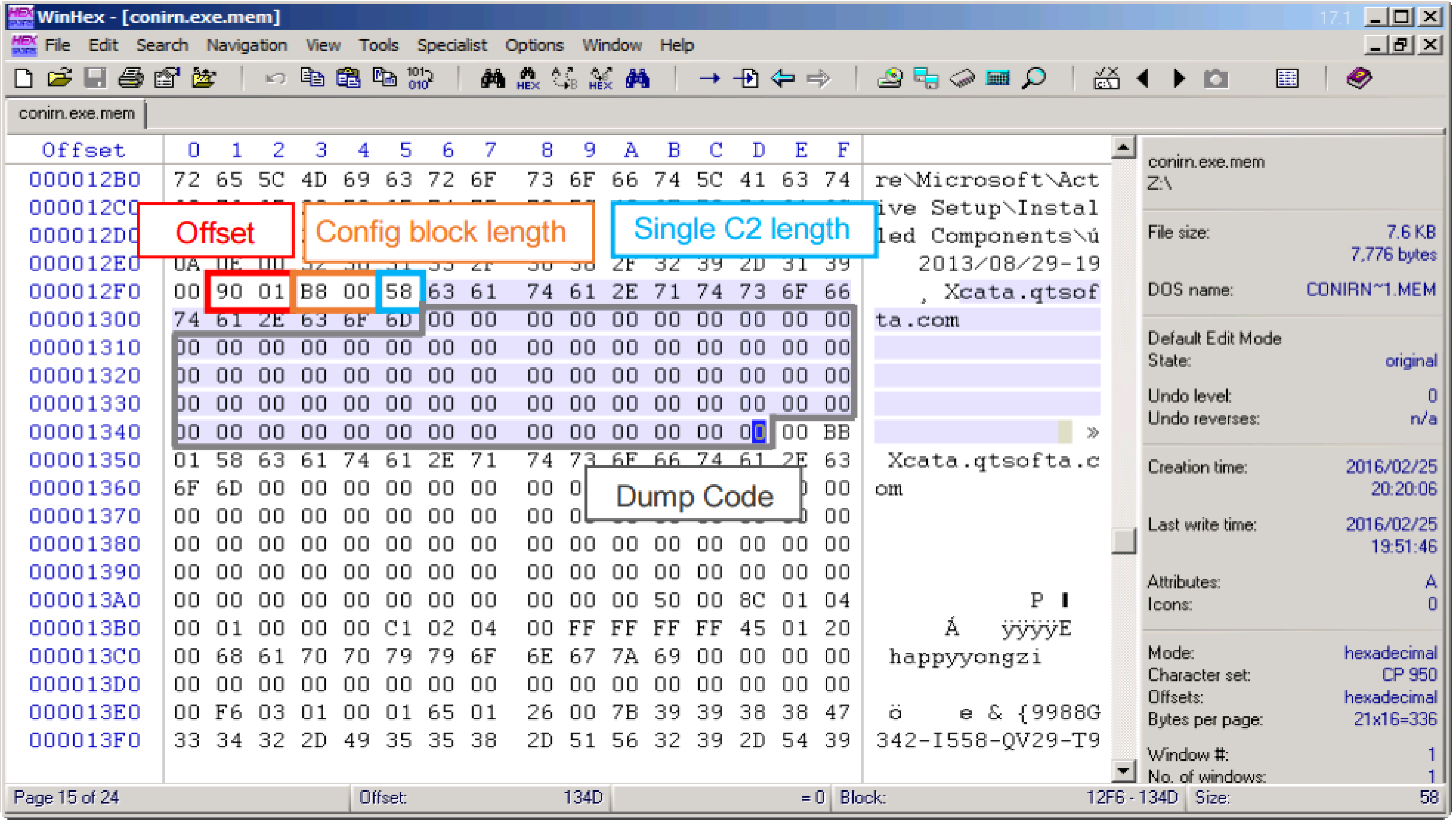
menuPass	admin	fishplay
happyyongzi	administone	keaidestone
XGstone	Smallfish	suzuki
watanabe	xiaoxiaohuli	

- PlugX Connection Password:



stone#@1	flowerdance	murata@8	TEST

Special Config Block in Poison Ivy



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000012B0   72 65 5C 4D 69 63 72 6F  73 6F 66 74 5C 41 63 74   re\Microsoft\Act
000012C0   [illegible]                                        ive Setup\Instal
000012D0   [illegible]                                        led Components\ú
000012E0   0A 0E 00 32 30 31 33 2F  30 38 2F 32 39 2D 31 39      2013/08/29-19
000012F0   00 90 01 B8 00 58 63 61  74 61 2E 71 74 73 6F 66     ¸ Xcata.qtsof
00001300   74 61 2E 63 6F 6D 00 00  00 00 00 00 00 00 00 00   ta.com
00001310   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00001320   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00001330   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00001340   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 BB                 »
00001350   01 58 63 61 74 61 2E 71  74 73 6F 66 74 61 2E 63    Xcata.qtsofta.c
00001360   6F 6D 00 00 00 00 00 00  00 0[illegible]         00   om
00001370   00 00 00 00 00 00 00 00  00 0[illegible]         00
00001380   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00001390   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000013A0   00 00 00 00 00 00 00 00  00 00 00 50 00 8C 01 04               P ▮
000013B0   00 01 00 00 00 C1 02 04  00 FF FF FF FF 45 01 20         Á    ÿÿÿÿE
000013C0   00 68 61 70 70 79 79 6F  6E 67 7A 69 00 00 00 00    happyyongzi
000013D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000013E0   00 F6 03 01 00 01 65 01  26 00 7B 39 39 38 38 47    ö     e & {9988G
000013F0   33 34 32 2D 49 35 35 38  2D 51 56 32 39 2D 54 39   342-I558-QV29-T9
```

Offset

Config block length

Single C2 length

Dump Code

conirn.exe.mem
Z:\

File size: 7.6 KB
7,776 bytes

DOS name: CONIRN~1.MEM

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Creation time: 2016/02/25
20:20:06

Last write time: 2016/02/25
19:51:46

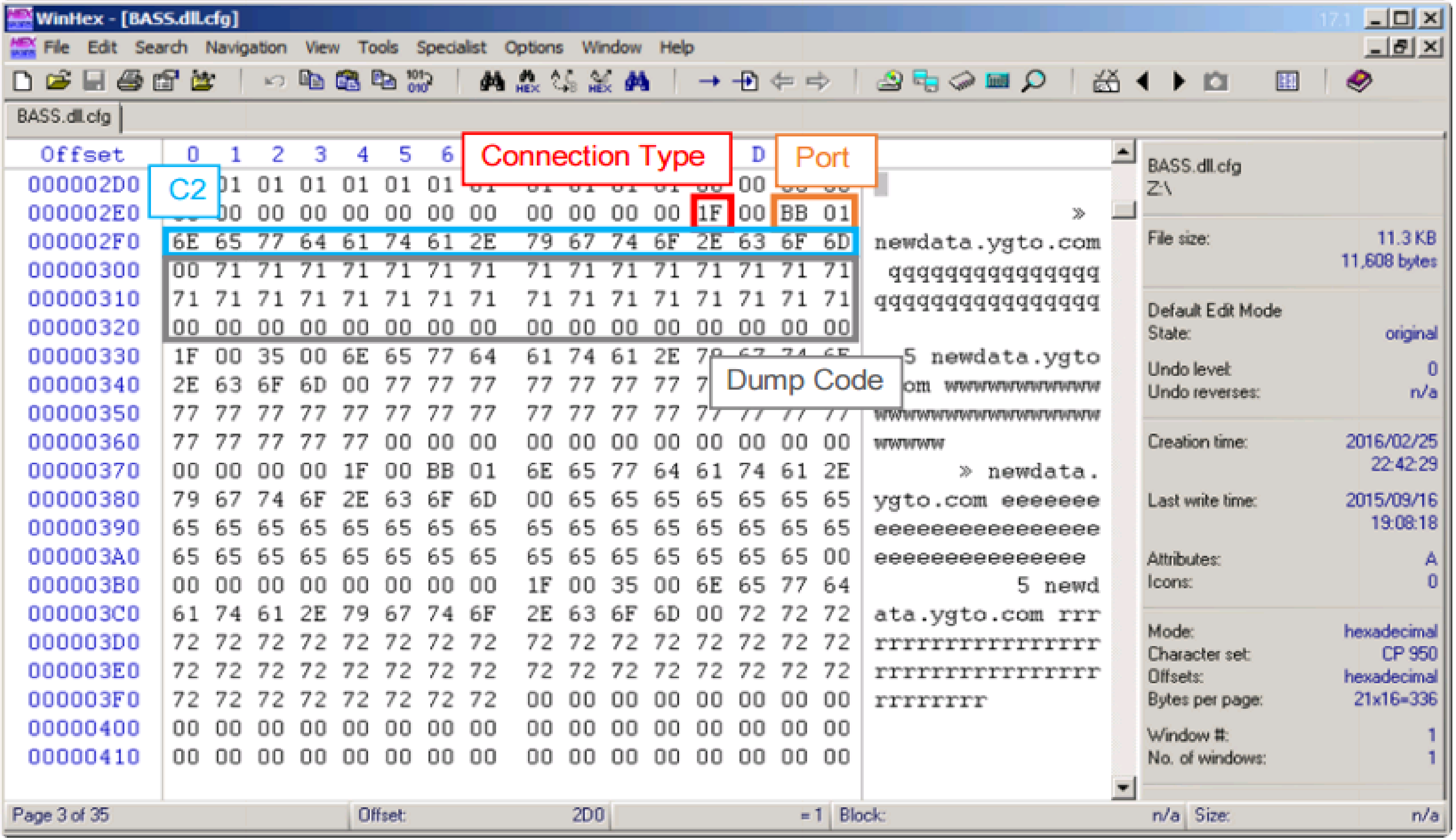
Attributes: A
Icons: 0

Mode: hexadecimal
Character set: CP 950
Offsets: hexadecimal
Bytes per page: 21x16=336

Window #: 1
No. of windows: 1

Page 15 of 24 | Offset: 134D | = 0 | Block: 12F6 - 134D | Size: 58

Special Config Block in PlugX



```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000002D0      01 01 01 01 01 01 01  01 01 01 01 00 00 00 00
000002E0   00 00 00 00 00 00 00 00  00 00 00 00 1F 00 BB 01                  »
000002F0   6E 65 77 64 61 74 61 2E  79 67 74 6F 2E 63 6F 6D   newdata.ygto.com
00000300   00 71 71 71 71 71 71 71  71 71 71 71 71 71 71 71    qqqqqqqqqqqqqqq
00000310   71 71 71 71 71 71 71 71  71 71 71 71 71 71 71 71   qqqqqqqqqqqqqqqq
00000320   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000330   1F 00 35 00 6E 65 77 64  61 74 61 2E 79 67 74 6F     5 newdata.ygto
00000340   2E 63 6F 6D 00 77 77 77  77 77 77 77 7             om wwwwwwwwwww
00000350   77 77 77 77 77 77 77 77  77 77 77 77 77 77 77 77   wwwwwwwwwwwwwwww
00000360   77 77 77 77 77 00 00 00  00 00 00 00 00 00 00 00   wwwww
00000370   00 00 00 00 1F 00 BB 01  6E 65 77 64 61 74 61 2E          » newdata.
00000380   79 67 74 6F 2E 63 6F 6D  00 65 65 65 65 65 65 65   ygto.com eeeeeee
00000390   65 65 65 65 65 65 65 65  65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
000003A0   65 65 65 65 65 65 65 65  65 65 65 65 65 65 65 00   eeeeeeeeeeeeeee
000003B0   00 00 00 00 00 00 00 00  1F 00 35 00 6E 65 77 64            5 newd
000003C0   61 74 61 2E 79 67 74 6F  2E 63 6F 6D 00 72 72 72   ata.ygto.com rrr
000003D0   72 72 72 72 72 72 72 72  72 72 72 72 72 72 72 72   rrrrrrrrrrrrrrrr
000003E0   72 72 72 72 72 72 72 72  72 72 72 72 72 72 72 72   rrrrrrrrrrrrrrrr
000003F0   72 72 72 72 72 72 72 72  00 00 00 00 00 00 00 00   rrrrrrrr
00000400   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000410   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

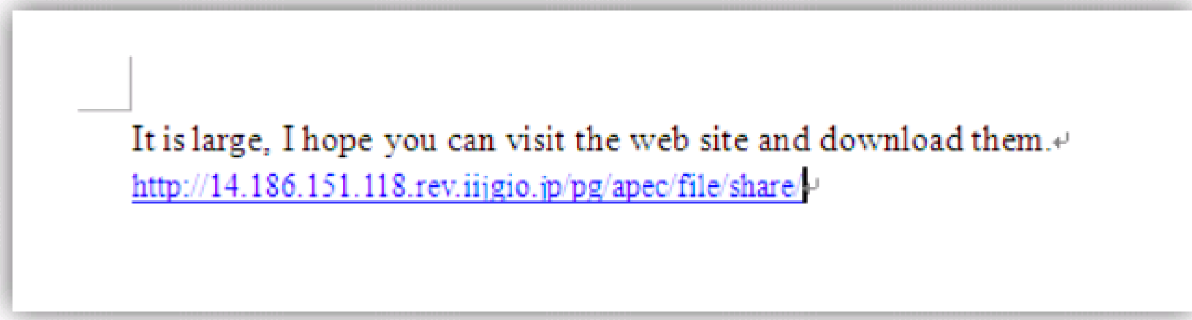
BASS.dll.cfg
Z:\

File size:	11.3 KB 11,608 bytes
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Creation time:	2016/02/25 22:42:29
Last write time:	2015/09/16 19:08:18
Attributes:	A
Icons:	0
Mode:	hexadecimal
Character set:	CP 950
Offsets:	hexadecimal
Bytes per page:	21x16=336
Window #:	1
No. of windows:	1

Page 3 of 35 | Offset: 2D0 | = 1 | Block: n/a | Size: n/a

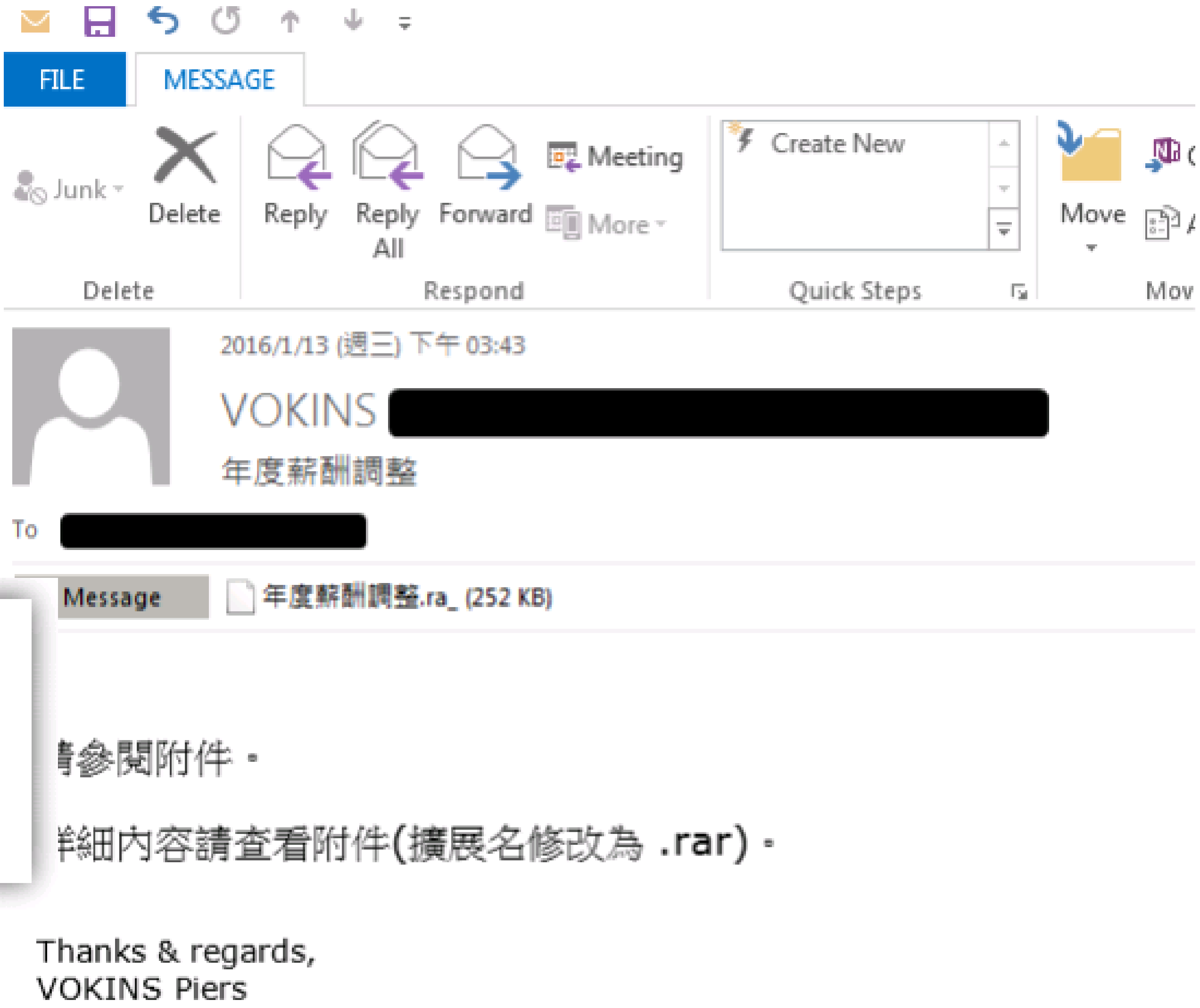
Capability Analysis

- Delivery
  - Spear-phishing Email with fabricated document file
  - Attachment file with download link



It is large, I hope you can visit the web site and download them.

http://14.186.151.118.rev.iijgio.jp/pg/apec/file/share/



2016/1/13 (週三) 下午 03:43

VOKINS [redacted]

年度薪酬調整

To [redacted]

Message 年度薪酬調整.ra_ (252 KB)

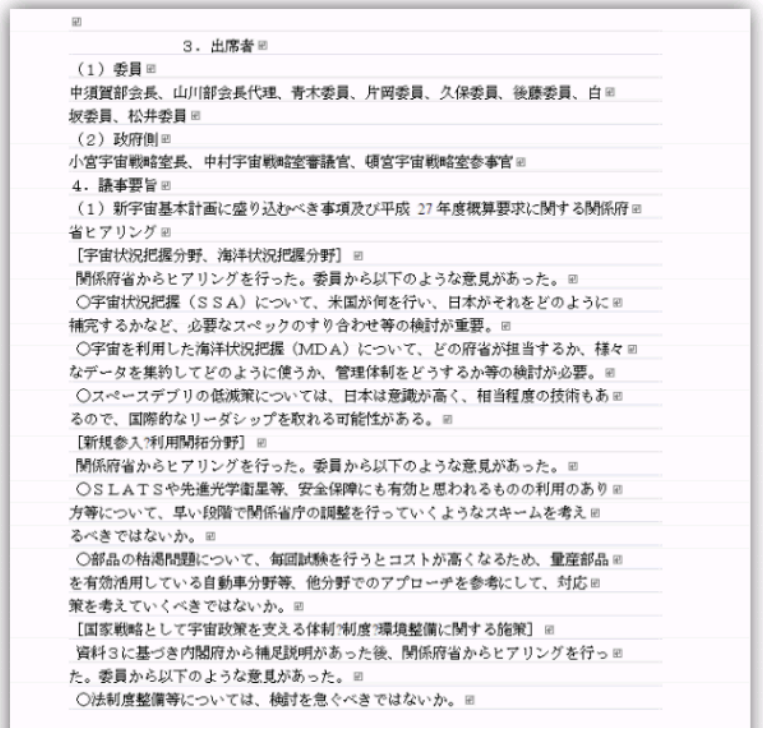
參閱附件。

細內容請查看附件(擴展名修改為 .rar)。

Thanks & regards,
VOKINS Piers

Capability Analysis

- Decoy document
  - Tailored content in decoy document



３．出席者

（１）委員

中須賀部会長、山川部会長代理、青木委員、片岡委員、久保委員、後藤委員、白坂委員、松井委員

（２）政府側

小宮宇宙戦略室長、中村宇宙戦略室審議官、頓宮宇宙戦略室参事官

４．議事要旨

（１）新宇宙基本計画に盛り込むべき事項及び平成 27 年度概算要求に関する関係府省ヒアリング

［宇宙状況把握分野、海洋状況把握分野］

関係府省からヒアリングを行った。委員から以下のような意見があった。

○宇宙状況把握（ＳＳＡ）について、米国が何を行い、日本がそれをどのように補完するかなど、必要なスペックのすり合わせ等の検討が重要。

○宇宙を利用した海洋状況把握（ＭＤＡ）について、どの府省が担当するか、様々なデータを集約してどのように使うか、管理体制をどうするか等の検討が必要。

○スペースデブリの低減策については、日本は意識が高く、相当程度の技術もあるので、国際的なリーダシップを取れる可能性がある。

［新規参入?利用開拓分野］

関係府省からヒアリングを行った。委員から以下のような意見があった。

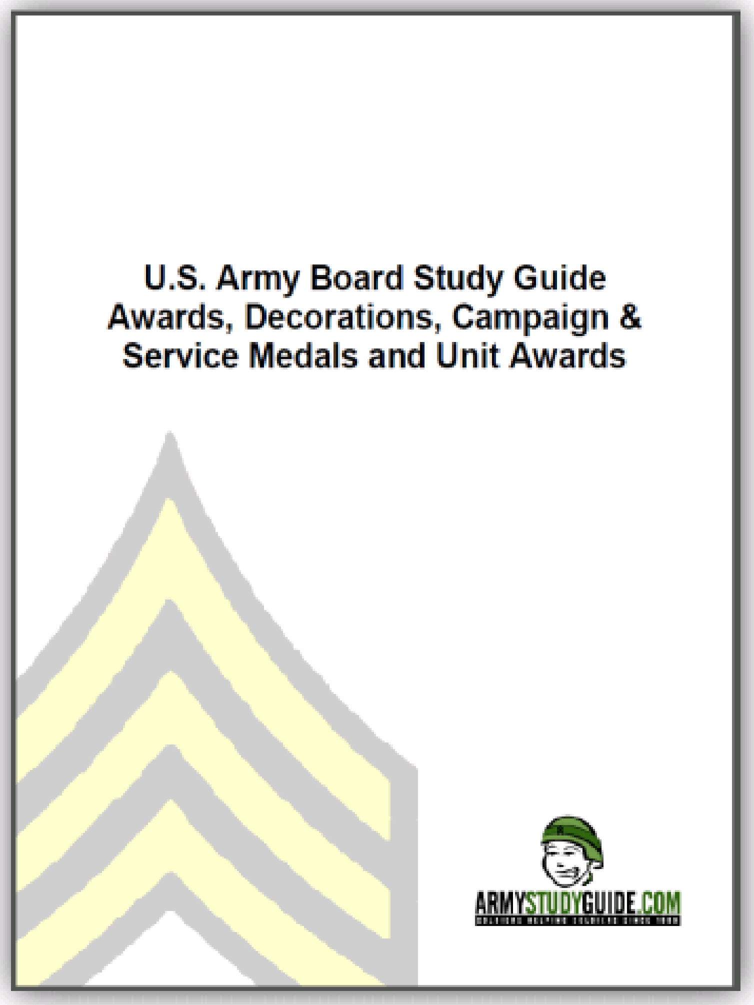
○ＳＬＡＴＳや先進光学衛星等、安全保障にも有効と思われるものの利用のあり方等について、早い段階で関係省庁の調整を行っていくようなスキームを考えるべきではないか。

○部品の枯渇問題について、毎回試験を行うとコストが高くなるため、量産部品を有効活用している自動車分野等、他分野でのアプローチを参考にして、対応策を考えていくべきではないか。

［国家戦略として宇宙政策を支える体制?制度?環境整備に関する施策］

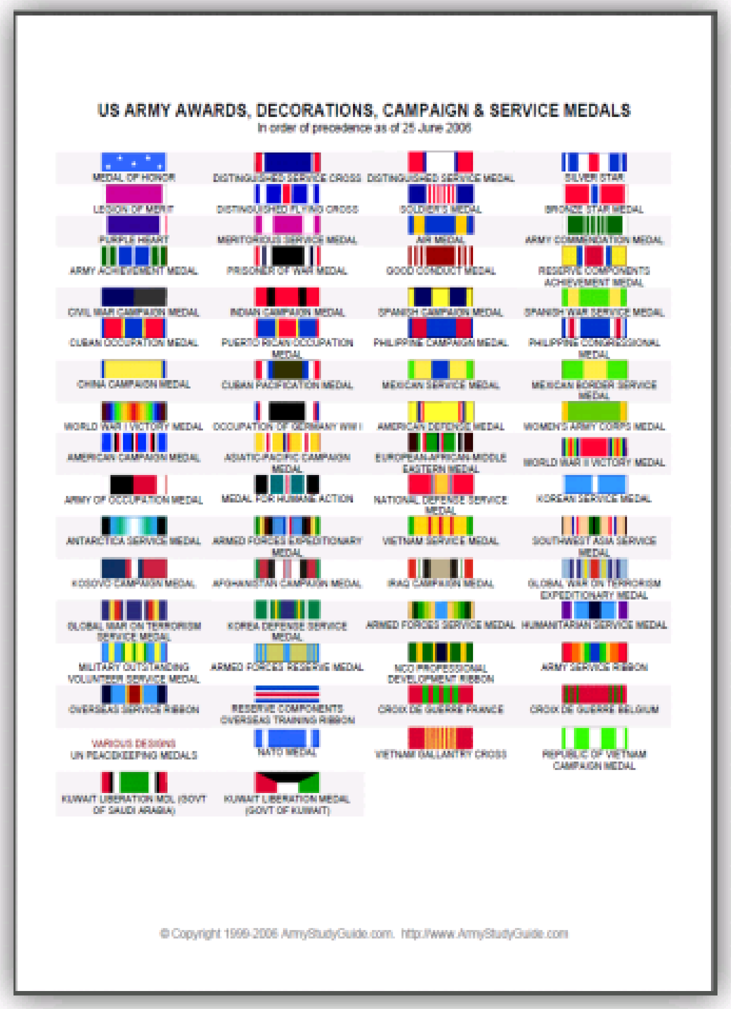
資料３に基づき内閣府から補足説明があった後、関係府省からヒアリングを行った。委員から以下のような意見があった。

○法制度整備等については、検討を急ぐべきではないか。



U.S. Army Board Study Guide
Awards, Decorations, Campaign &
Service Medals and Unit Awards

ARMYSTUDYGUIDE.COM



US ARMY AWARDS, DECORATIONS, CAMPAIGN & SERVICE MEDALS

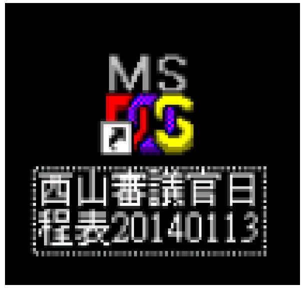
In order of precedence as of 25 June 2006

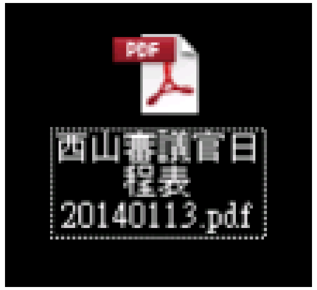
MEDAL OF HONOR	DISTINGUISHED SERVICE CROSS	DISTINGUISHED SERVICE MEDAL	SILVER STAR
LEGION OF MERIT	DISTINGUISHED FLYING CROSS	SOLDIER'S MEDAL	BRONZE STAR MEDAL
PURPLE HEART	MERITORIOUS SERVICE MEDAL	AIR MEDAL	ARMY COMMENDATION MEDAL
ARMY ACHIEVEMENT MEDAL	PRISONER OF WAR MEDAL	GOOD CONDUCT MEDAL	RESERVE COMPONENTS ACHIEVEMENT MEDAL
CIVIL WAR CAMPAIGN MEDAL	INDIAN CAMPAIGN MEDAL	SPANISH CAMPAIGN MEDAL	SPANISH WAR SERVICE MEDAL
CUBAN OCCUPATION MEDAL	PUERTO RICAN OCCUPATION MEDAL	PHILIPPINE CAMPAIGN MEDAL	PHILIPPINE CONGRESSIONAL MEDAL
CHINA CAMPAIGN MEDAL	CUBAN PACIFICATION MEDAL	MEXICAN SERVICE MEDAL	MEXICAN BORDER SERVICE MEDAL
WORLD WAR I VICTORY MEDAL	OCCUPATION OF GERMANY WW I	AMERICAN DEFENSE MEDAL	WOMEN'S ARMY CORPS MEDAL
AMERICAN CAMPAIGN MEDAL	ASIATIC-PACIFIC CAMPAIGN MEDAL	EUROPEAN-AFRICAN-MIDDLE EASTERN MEDAL	WORLD WAR II VICTORY MEDAL
ARMY OF OCCUPATION MEDAL	MEDAL FOR HUMANE ACTION	NATIONAL DEFENSE SERVICE MEDAL	KOREAN SERVICE MEDAL
ANTARCTICA SERVICE MEDAL	ARMED FORCES EXPEDITIONARY MEDAL	VIETNAM SERVICE MEDAL	SOUTHWEST ASIA SERVICE MEDAL
KOSOVO CAMPAIGN MEDAL	AFGHANISTAN CAMPAIGN MEDAL	IRAQ CAMPAIGN MEDAL	GLOBAL WAR ON TERRORISM EXPEDITIONARY MEDAL
GLOBAL WAR ON TERRORISM SERVICE MEDAL	KOREA DEFENSE SERVICE MEDAL	ARMED FORCES SERVICE MEDAL	HUMANITARIAN SERVICE MEDAL
MILITARY OUTSTANDING VOLUNTEER SERVICE MEDAL	ARMED FORCES RESERVE MEDAL	NCO PROFESSIONAL DEVELOPMENT RIBBON	ARMY SERVICE RIBBON
OVERSEAS SERVICE RIBBON	RESERVE COMPONENTS OVERSEAS TRAINING RIBBON	CROIX DE GUERRE FRANCE	CROIX DE GUERRE BELGIUM
VARIOUS DESIGNS UN PEACEKEEPING MEDALS	NATO MEDAL	VIETNAM GALLANTRY CROSS	REPUBLIC OF VIETNAM CAMPAIGN MEDAL
KUWAIT LIBERATION MDL (GOVT OF SAUDI ARABIA)	KUWAIT LIBERATION MEDAL (GOVT OF KUWAIT)		

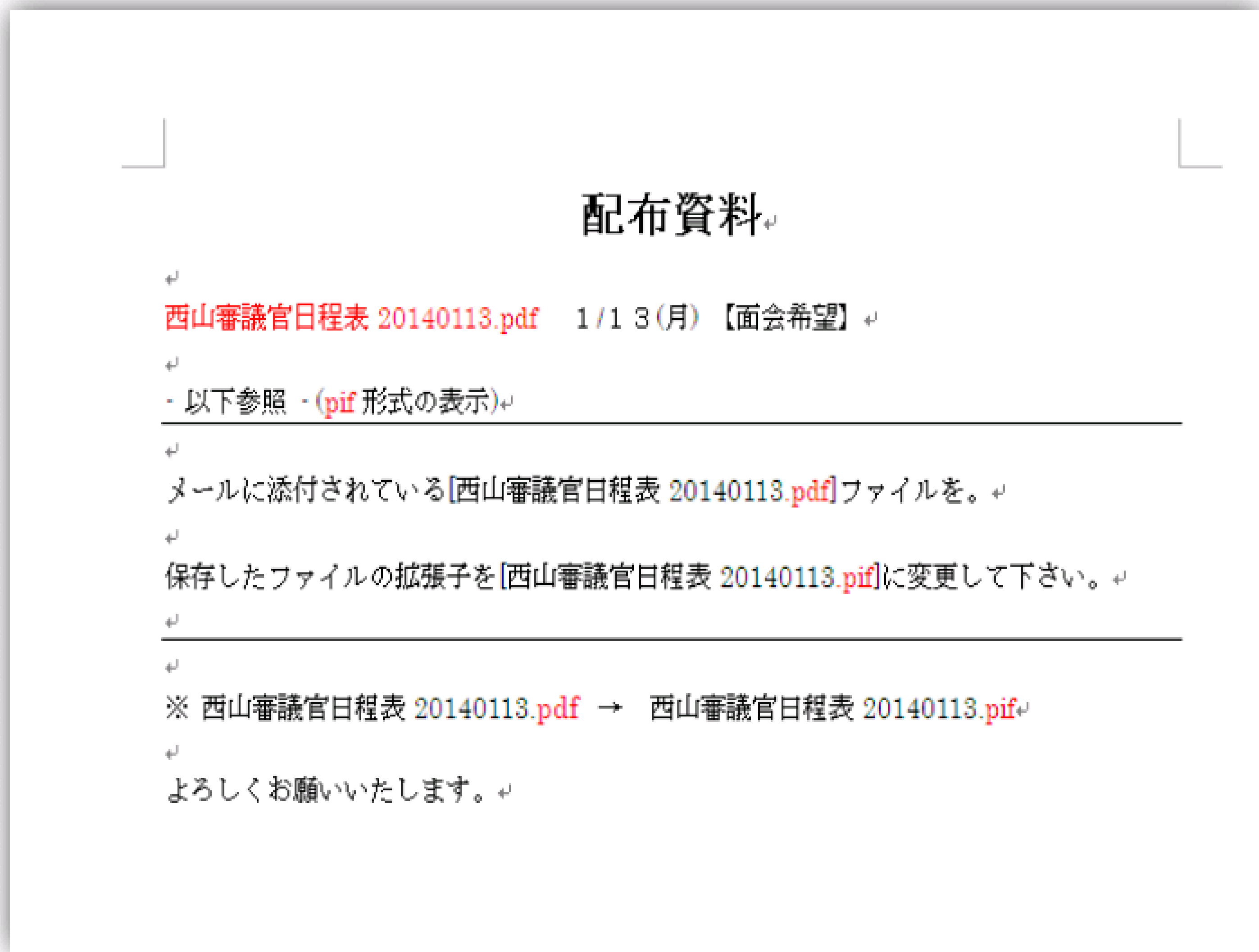
© Copyright 1999-2006 ArmyStudyGuide.com. http://www.ArmyStudyGuide.com

Capability Analysis

- Attachment file of instruction to “exploit” yourself.







配布資料

西山審議官日程表 20140113.pdf　１/１３(月)　【面会希望】

· 以下参照 ·(pif 形式の表示)

メールに添付されている[西山審議官日程表 20140113.pdf]ファイルを。

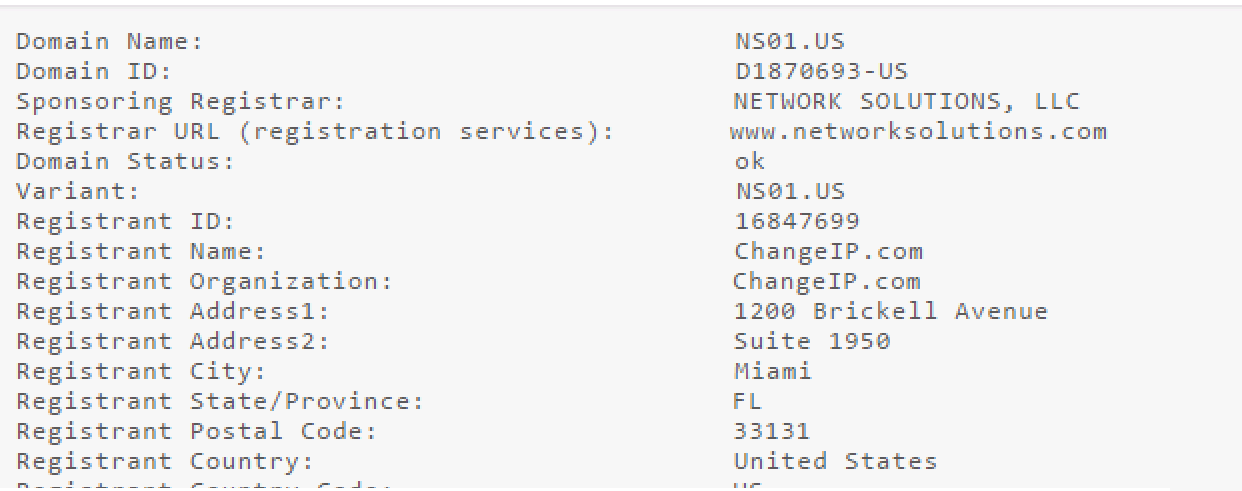
保存したファイルの拡張子を[西山審議官日程表 20140113.pif]に変更して下さい。

※ 西山審議官日程表 20140113.pdf → 西山審議官日程表 20140113.pif

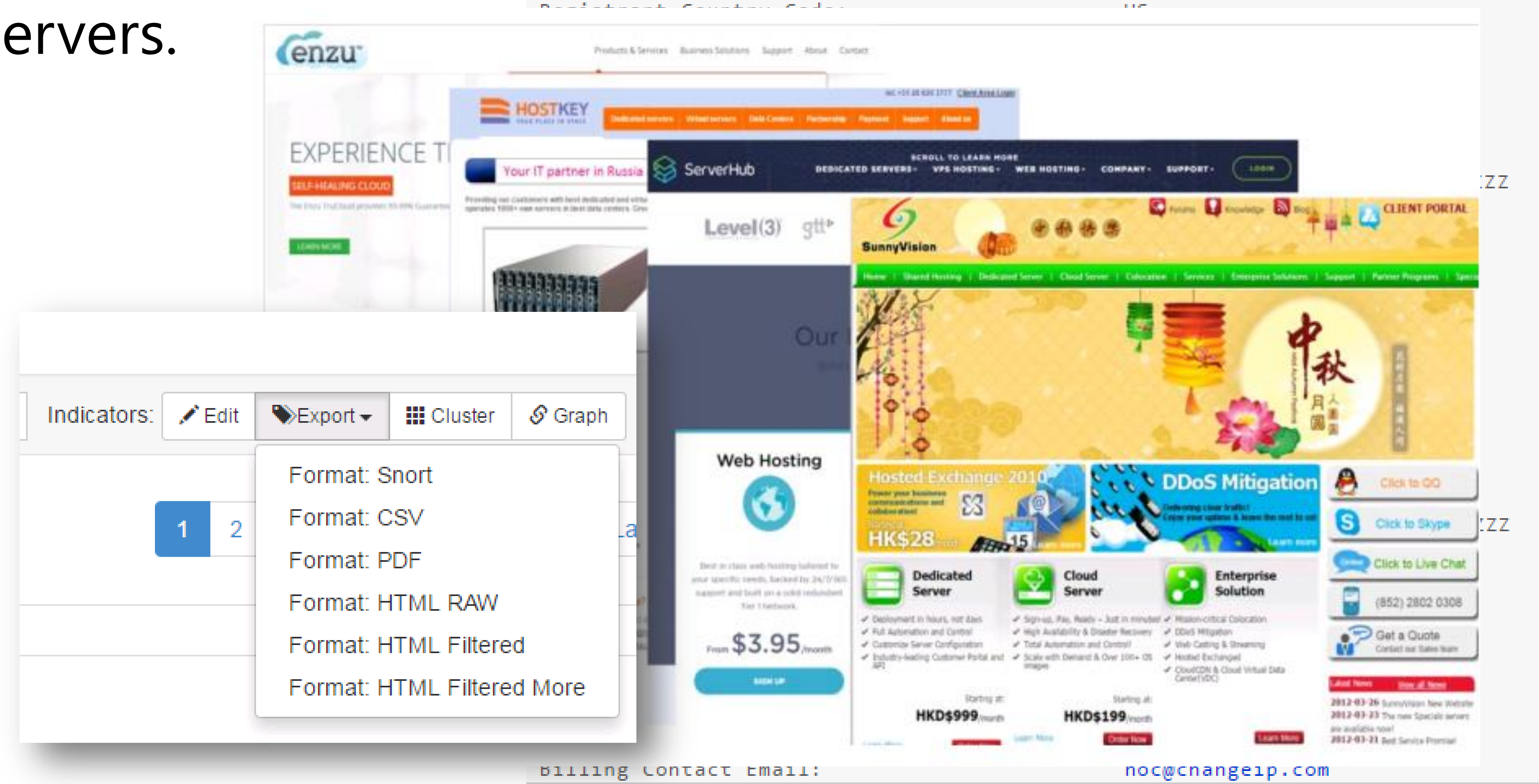
よろしくお願いいたします。

C&C Infrastructure

- 500+ C2 domains & IPs
- Favor of Dynamic DNS & Virtual Private Servers.
  - PubYun
  - ChangeIP.com
  - No-IP
  - FreeDNS
  - Dyn.com
  - Oray (花生壳)

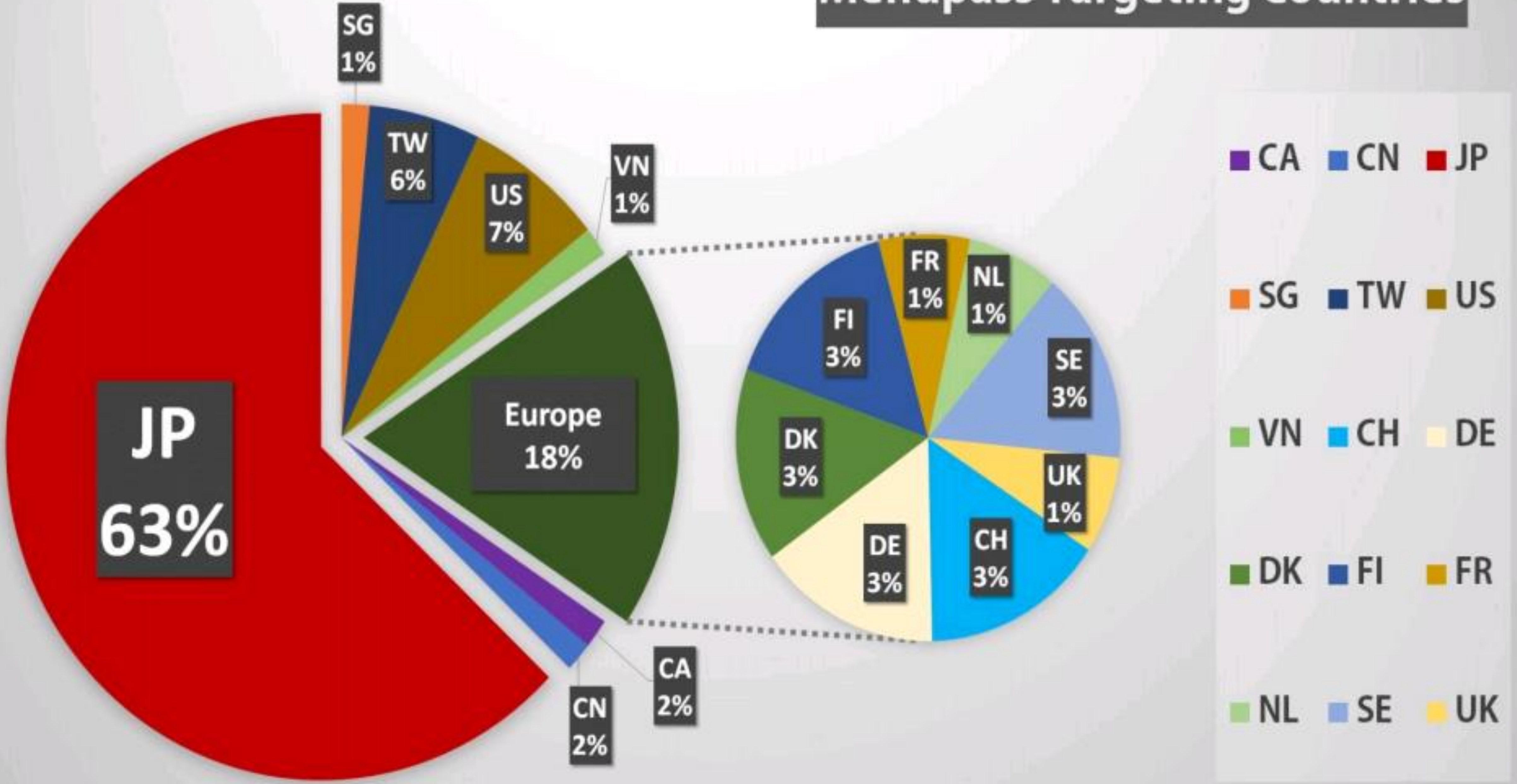


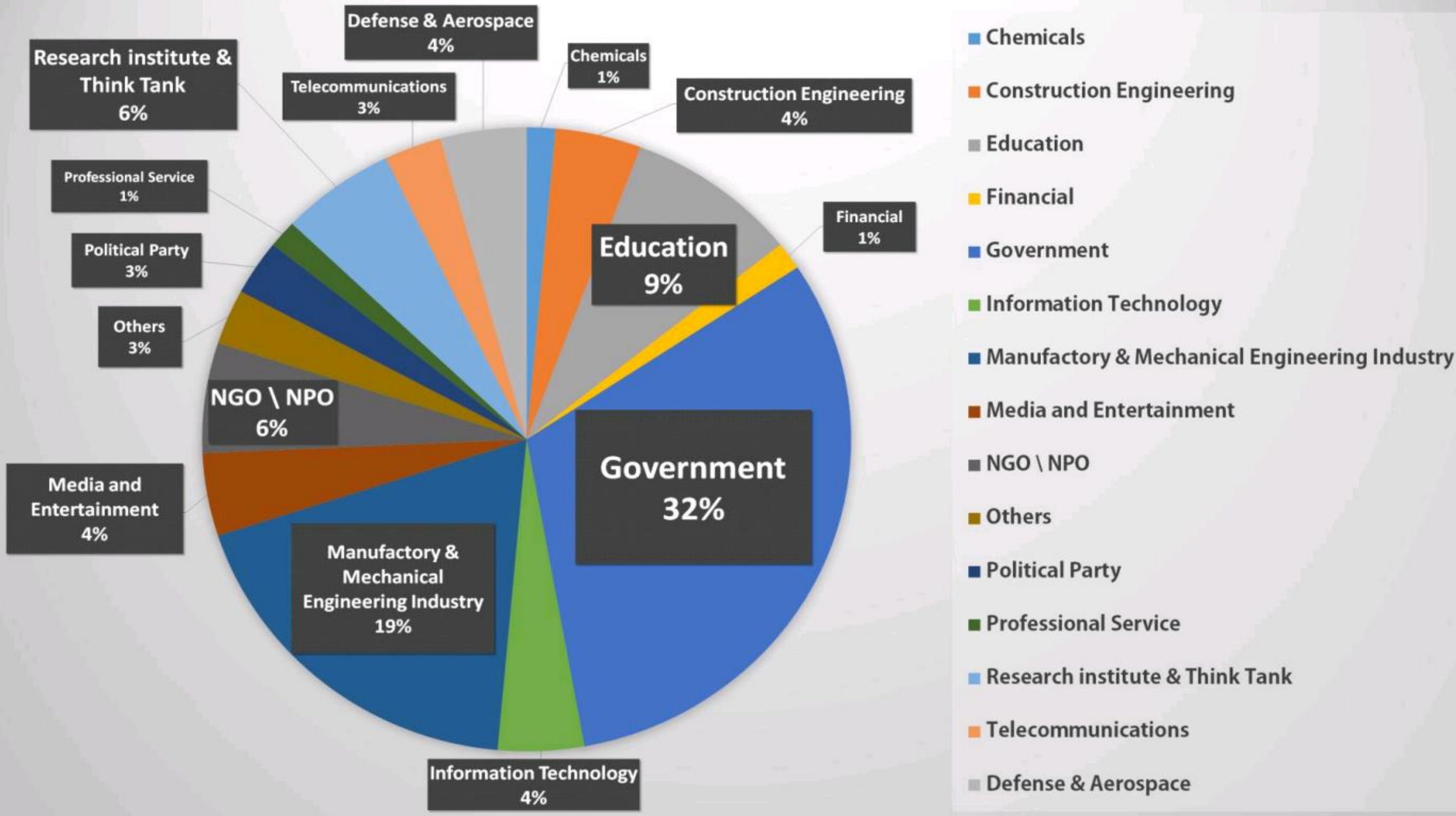
```
Domain Name:                                  NS01.US
Domain ID:                                    D1870693-US
Sponsoring Registrar:                         NETWORK SOLUTIONS, LLC
Registrar URL (registration services):       www.networksolutions.com
Domain Status:                                ok
Variant:                                      NS01.US
Registrant ID:                                16847699
Registrant Name:                              ChangeIP.com
Registrant Organization:                      ChangeIP.com
Registrant Address1:                          1200 Brickell Avenue
Registrant Address2:                          Suite 1950
Registrant City:                              Miami
Registrant State/Province:                    FL
Registrant Postal Code:                       33131
Registrant Country:                           United States
```



```
Billing Contact Email:                        noc@changeip.com
```

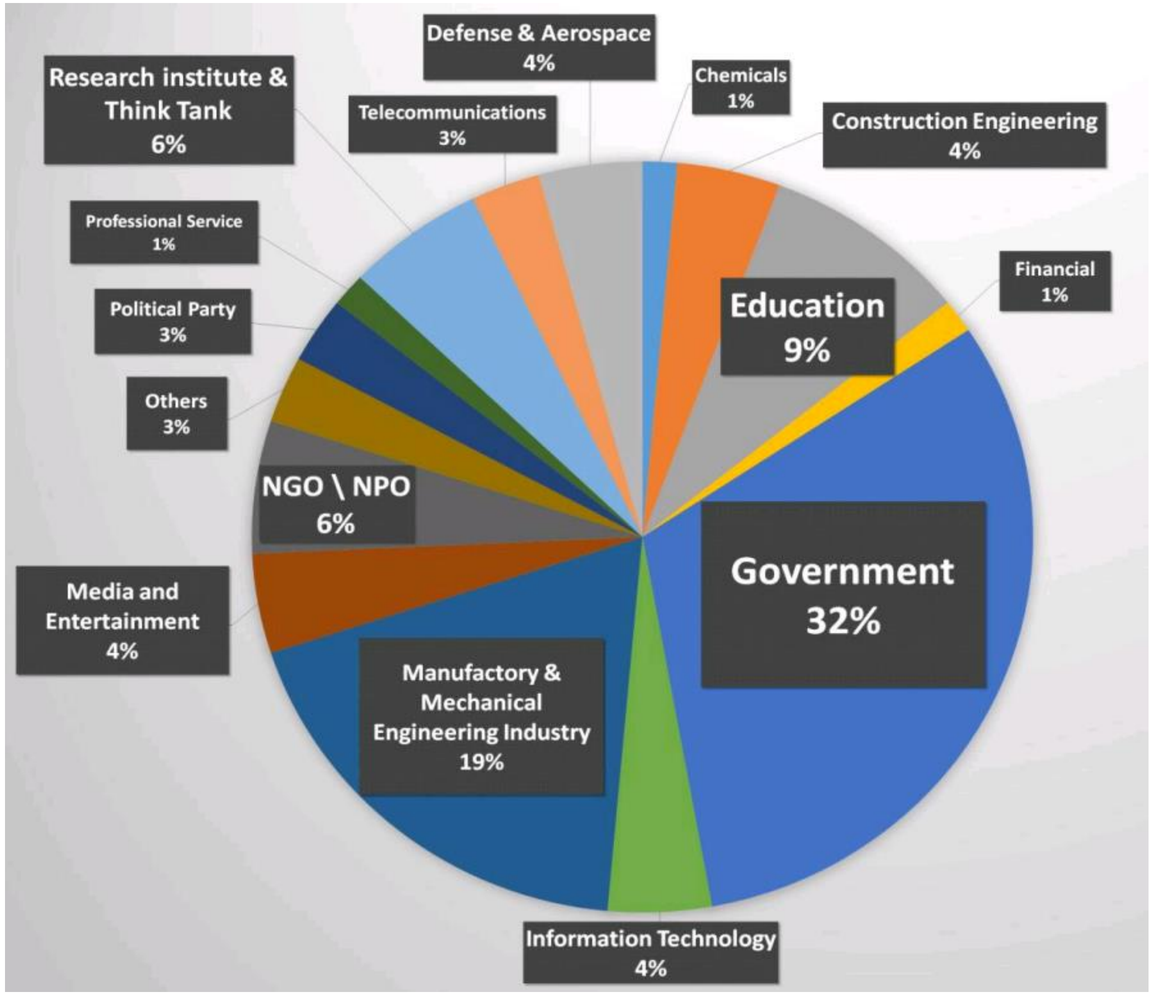
Menupass Targeting Countries

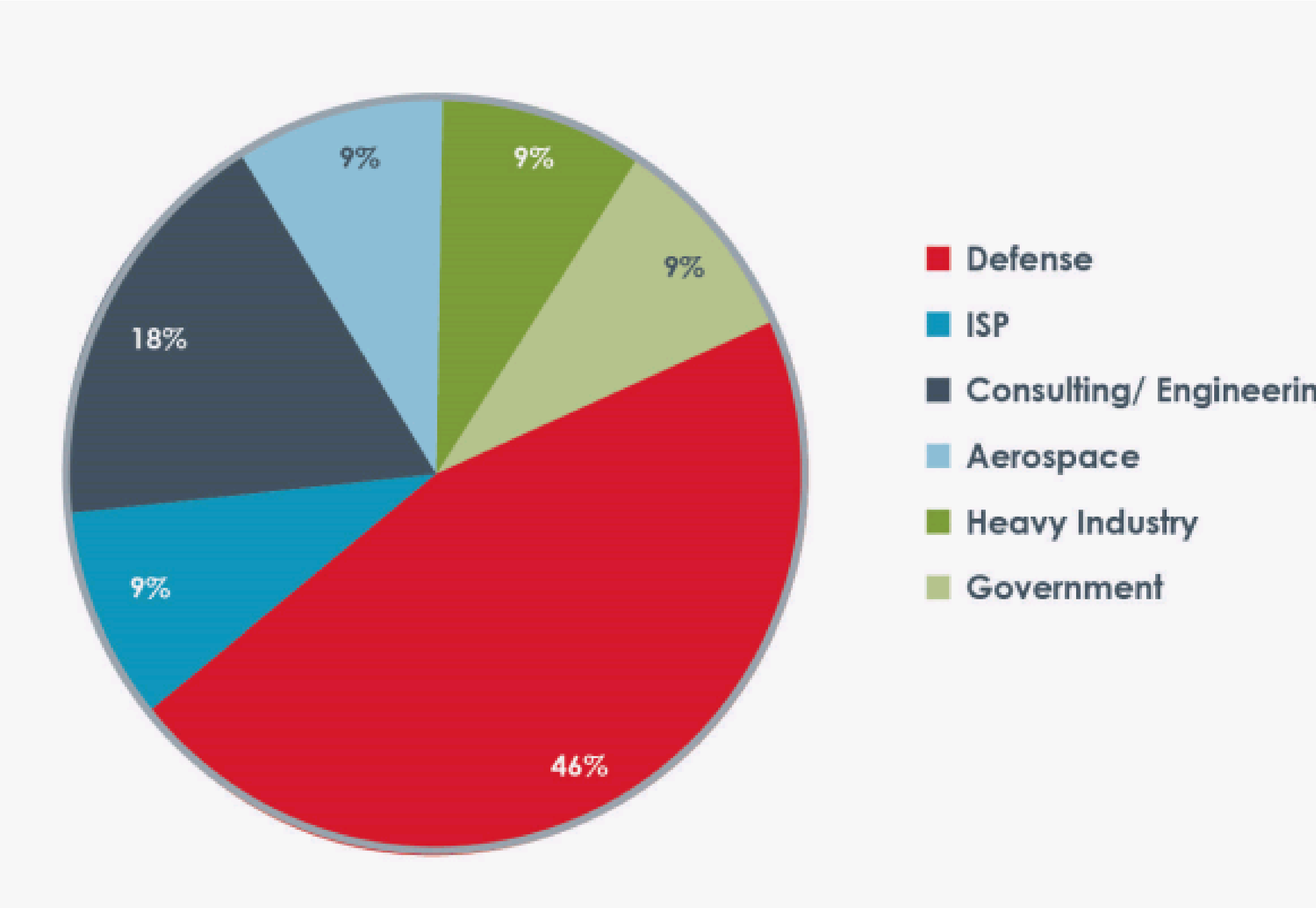



Defense & Aerospace 4%
Research institute & Think Tank 6%
Telecommunications 3%
Chemicals 1%
Construction Engineering 4%
Professional Service 1%
Political Party 3%
Others 3%
Education 9%
Financial 1%
NGO \ NPO 6%
Government 32%
Media and Entertainment 4%
Manufactory & Mechanical Engineering Industry 19%
Information Technology 4%
Chemicals
Construction Engineering
Education
Financial
Government
Information Technology
Manufactory & Mechanical Engineering Industry
Media and Entertainment
NGO \ NPO
Others
Political Party
Professional Service
Research institute & Think Tank
Telecommunications
Defense & Aerospace

Different Visibility (Our Visibility v.s. OSINT)

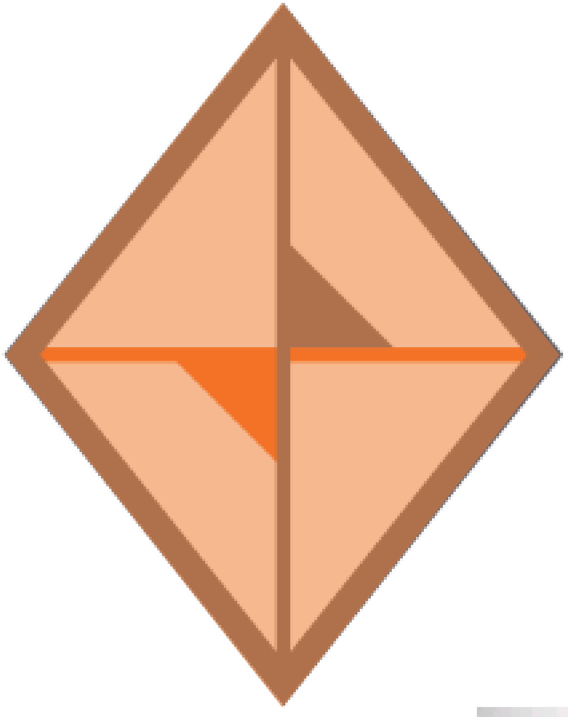
Region, Timeframe, Visibility





ADVERSARY

Interested in State Secret
Probably State-sponsor be
hide the group



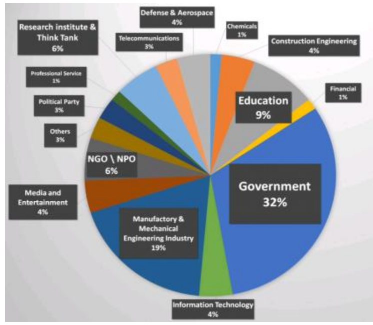
CAPABILITIES

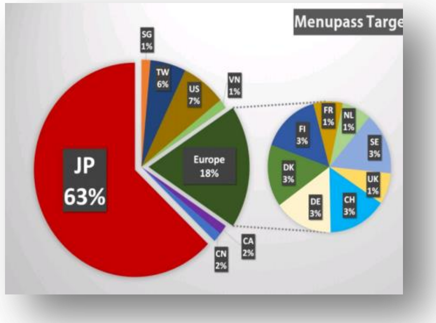
Spear-Phishing Emails
Waterhole Attack
PlugX, Poison Ivy, Evilgrab, Gh0st, SPIVY
CVE 2012-0158, CVE-2014-7247…

INFRASTRUCTURE

C2 Domains, IPs
Preferring DNS & VPS

VICTIM

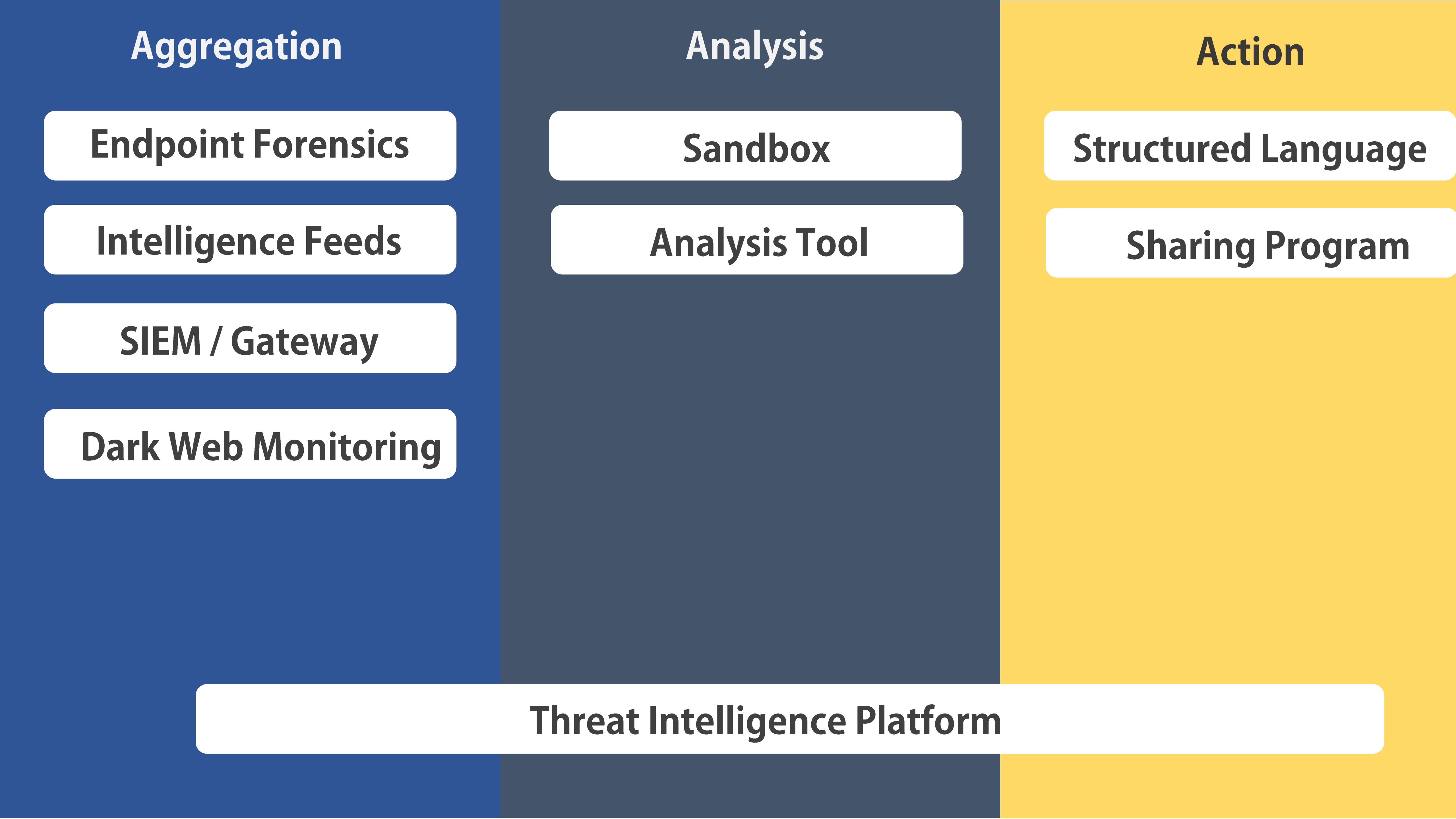




Products Available

TEAM T5

Cyber Security Research



Aggregation

- Endpoint Forensics
- Intelligence Feeds
- SIEM / Gateway
- Dark Web Monitoring

Analysis

- Sandbox
- Analysis Tool

Action

- Structured Language
- Sharing Program

Threat Intelligence Platform

Products Available

SIEM / Gateway

- HP ArcSight ($)
- IBM QRadar ($)
- Cisco Source Fire AMP ($)
- AlienVault (FREE /$)
- CHT EyeQuila ($)

Endpoint Forensics

- Google Rapid Response (FREE)
- Mandiant RedLine/MIR (FREE / $)
- Guidance EnCase Cyber Security ($)
- Verint XecProbe ($)
- Carbon Black ($)
- Falcon Host ($)

Intelligence Feeds

- Mandiant + Fireeye + iSIGHT Partners ($)
- iDEFENSE ($)
- Dell SecureWorks ($)
- CrowdStrike ($)
- LookingGlass ($)

Products Available

Analysis Tool

- Maltego (FREE / $)
- DomainTools IRIS ($)
- ThreatCrowd (FREE)
- PassiveTotal (FREE / $)

Sandbox

- FireEye MVX ($)
- Damballa ($)
- Lastline ($)
- ThreatTrack ($)
- ThreatGRID ($)
- Cuckoo (FREE)

TIP

- Threat Connect (FREE/ $)
- MISP (FREE)
- MITRE CRITS (Free)
- IBM X-Force ($)
- EclecticIQ Platform ($)
- ThreatScap ($)

Structured Language

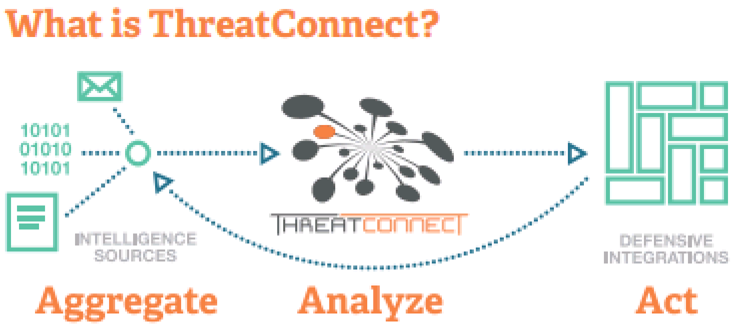
- STIX (FREE)
- TAXII (FREE)
- CybOX (FREE)

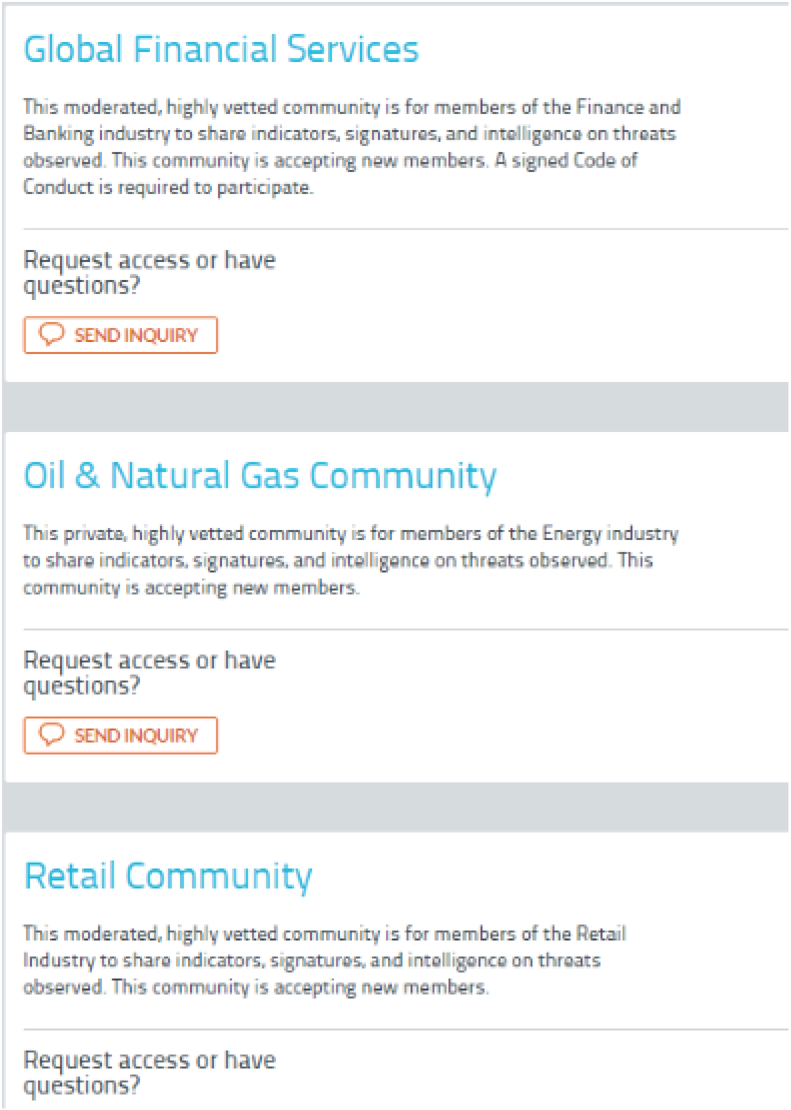
Sharing Program

- TAXII (FREE)
- Libtaxii TAXII Library (FREE)
- Yeti TAXII Server (FREE)

ThreatConnect

- Community driven threat intelligence platform
- Every instance of ThreatConnect includes access to Public Cloud Common Community.
- Provide API, Threat Connect Marketplace





Global Financial Services

This moderated, highly vetted community is for members of the Finance and Banking industry to share indicators, signatures, and intelligence on threats observed. This community is accepting new members. A signed Code of Conduct is required to participate.

Request access or have questions?

SEND INQUIRY

Oil & Natural Gas Community

This private, highly vetted community is for members of the Energy industry to share indicators, signatures, and intelligence on threats observed. This community is accepting new members.

Request access or have questions?

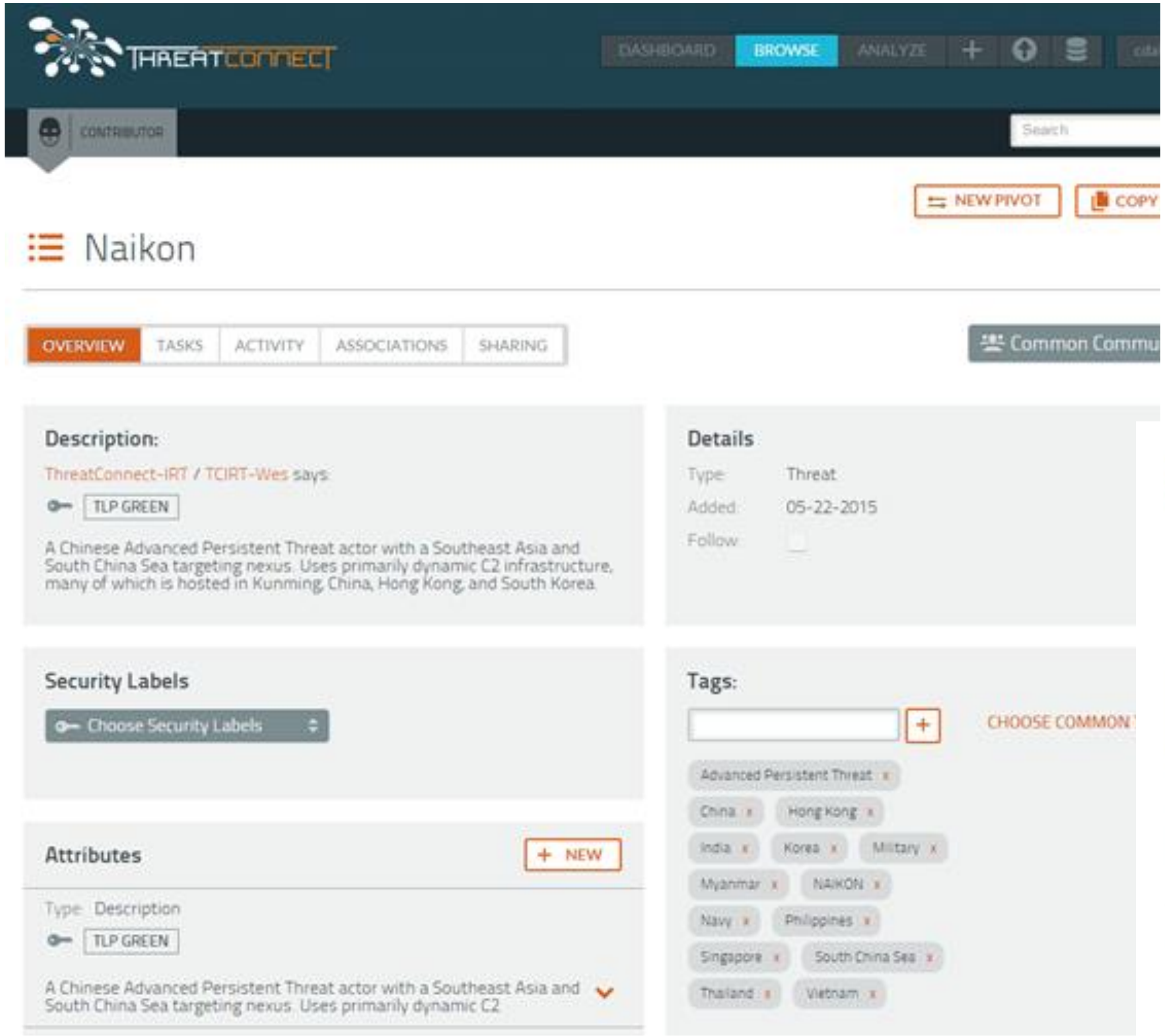
SEND INQUIRY

Retail Community

This moderated, highly vetted community is for members of the Retail Industry to share indicators, signatures, and intelligence on threats observed. This community is accepting new members.

Request access or have questions?

THREATCONNECT



Description:

ThreatConnect-IRT / TCIRT-Wes says:

TLP GREEN

A Chinese Advanced Persistent Threat actor with a Southeast Asia and South China Sea targeting nexus. Uses primarily dynamic C2 infrastructure, many of which is hosted in Kunming, China, Hong Kong, and South Korea.

Details

Type: Threat
Added: 05-22-2015
Follow: □

Security Labels

Choose Security Labels

Tags:

CHOOSE COMMON

Advanced Persistent Threat x
China x
Hong Kong x
India x
Korea x
Military x
Myanmar x
NAIKON x
Navy x
Philippines x
Singapore x
South China Sea x
Thailand x
Vietnam x

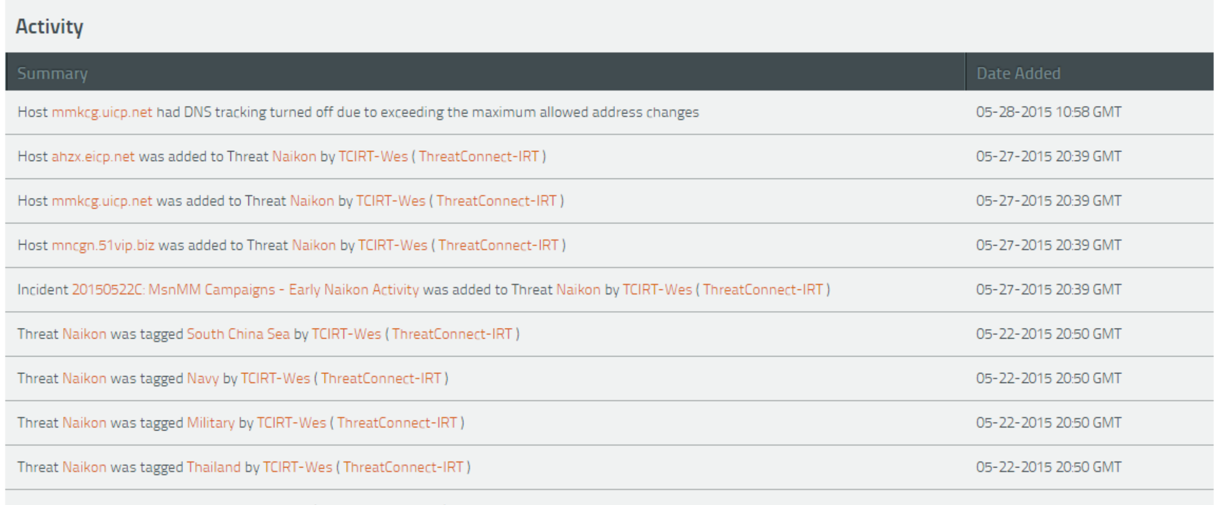
Attributes

+ NEW

Type: Description

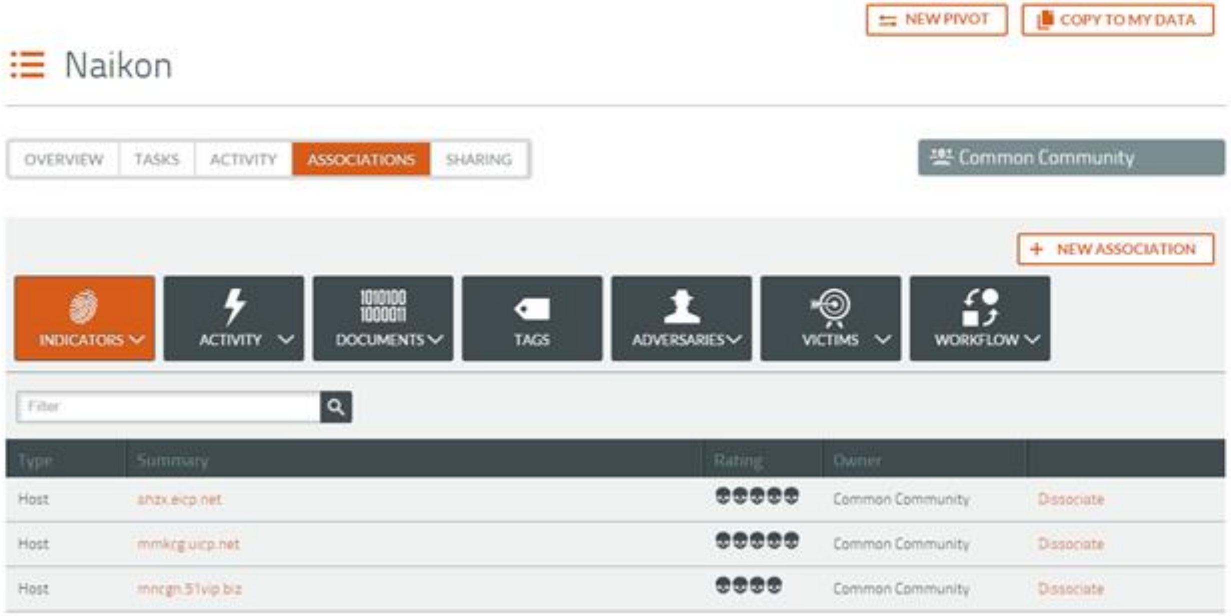
TLP GREEN

A Chinese Advanced Persistent Threat actor with a Southeast Asia and South China Sea targeting nexus. Uses primarily dynamic C2



Activity

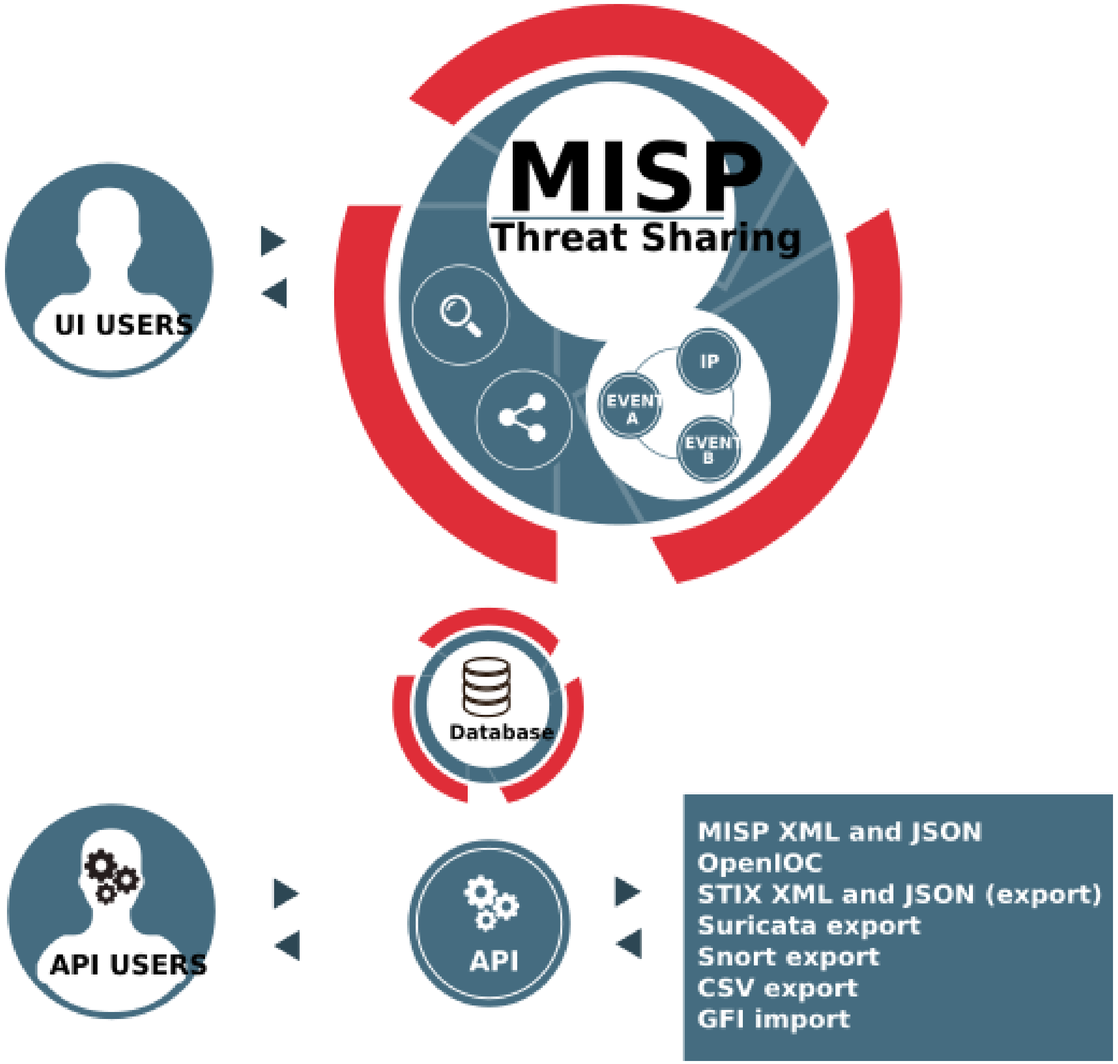
Summary	Date Added
Host mmkcg.uicp.net had DNS tracking turned off due to exceeding the maximum allowed address changes	05-28-2015 10:58 GMT
Host ahzx.eicp.net was added to Threat Naikon by TCIRT-Wes (ThreatConnect-IRT)	05-27-2015 20:39 GMT
Host mmkcg.uicp.net was added to Threat Naikon by TCIRT-Wes (ThreatConnect-IRT)	05-27-2015 20:39 GMT
Host mncgn.51vip.biz was added to Threat Naikon by TCIRT-Wes (ThreatConnect-IRT)	05-27-2015 20:39 GMT
Incident 20150522C: MsnMM Campaigns - Early Naikon Activity was added to Threat Naikon by TCIRT-Wes (ThreatConnect-IRT)	05-27-2015 20:39 GMT
Threat Naikon was tagged South China Sea by TCIRT-Wes (ThreatConnect-IRT)	05-22-2015 20:50 GMT
Threat Naikon was tagged Navy by TCIRT-Wes (ThreatConnect-IRT)	05-22-2015 20:50 GMT
Threat Naikon was tagged Military by TCIRT-Wes (ThreatConnect-IRT)	05-22-2015 20:50 GMT
Threat Naikon was tagged Thailand by TCIRT-Wes (ThreatConnect-IRT)	05-22-2015 20:50 GMT



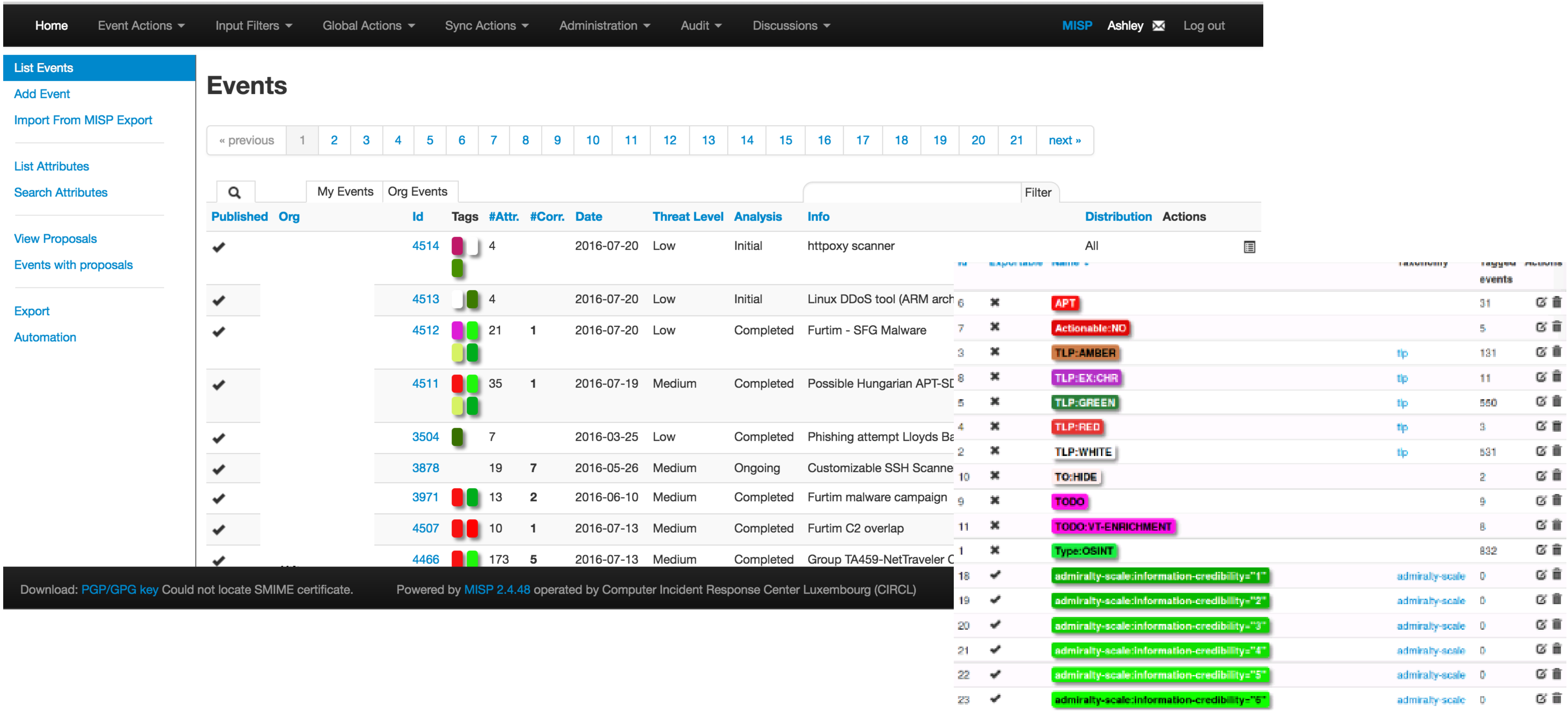
Type	Summary	Rating	Owner	
Host	ahzx.eicp.net	●●●●●	Common Community	Dissociate
Host	mmkcg.uicp.net	●●●●●	Common Community	Dissociate
Host	mncgn.51vip.biz	●●●●	Common Community	Dissociate

MISP

- Malware information sharing platform
- Storing and sharing Indicators of compromise (IP, domain, hashes)
- Open source platform model (available on Github)
- Sharing information between MISP instances



MISP (CIRCL)



Events

Published	Org	Id	Tags	#Attr.	#Corr.	Date	Threat Level	Analysis	Info	Distribution	Actions
✓		4514	🟪⬜🟩	4		2016-07-20	Low	Initial	httpoxy scanner	All	▤
✓		4513	⬜🟩	4		2016-07-20	Low	Initial	Linux DDoS tool (ARM arch		
✓		4512	🟪🟩🟩🟩	21	1	2016-07-20	Low	Completed	Furtim - SFG Malware		
✓		4511	🟥🟩🟩🟩	35	1	2016-07-19	Medium	Completed	Possible Hungarian APT-SD		
✓		3504	🟩	7		2016-03-25	Low	Completed	Phishing attempt Lloyds Ba		
✓		3878		19	7	2016-05-26	Medium	Ongoing	Customizable SSH Scanne		
✓		3971	🟥🟩	13	2	2016-06-10	Medium	Completed	Furtim malware campaign		
✓		4507	🟥🟥	10	1	2016-07-13	Medium	Completed	Furtim C2 overlap		
✓		4466	🟥🟩	173	5	2016-07-13	Medium	Completed	Group TA459-NetTraveler C		

Download: PGP/GPG key Could not locate SMIME certificate.   Powered by MISP 2.4.48 operated by Computer Incident Response Center Luxembourg (CIRCL)

Id	Exportable	Name ↓	Taxonomy	Tagged events	Actions
6	✗	APT		31	✎ 🗑
7	✗	Actionable:NO		5	✎ 🗑
3	✗	TLP:AMBER	tlp	131	✎ 🗑
8	✗	TLP:EX:CHR	tlp	11	✎ 🗑
5	✗	TLP:GREEN	tlp	550	✎ 🗑
4	✗	TLP:RED	tlp	3	✎ 🗑
2	✗	TLP:WHITE	tlp	531	✎ 🗑
10	✗	TO:HIDE		2	✎ 🗑
9	✗	TODO		9	✎ 🗑
11	✗	TODO:VT-ENRICHMENT		8	✎ 🗑
1	✗	Type:OSINT		832	✎ 🗑
18	✓	admiralty-scale:information-credibility="1"	admiralty-scale	0	✎ 🗑
19	✓	admiralty-scale:information-credibility="2"	admiralty-scale	0	✎ 🗑
20	✓	admiralty-scale:information-credibility="3"	admiralty-scale	0	✎ 🗑
21	✓	admiralty-scale:information-credibility="4"	admiralty-scale	0	✎ 🗑
22	✓	admiralty-scale:information-credibility="5"	admiralty-scale	0	✎ 🗑
23	✓	admiralty-scale:information-credibility="6"	admiralty-scale	0	✎ 🗑

Conclusion

TEAM T5
Cyber Security Research

Takeaways

- Cyber Threat Intelligence provides researched and analyzed knowledge about adversaries to help quickly adapt to an ever-changing threat landscape.
- The most important source of relevant threat data of an organization is your own attack surface.
- Threat Intelligence Platform fusing internal and external sources, facilitating analysis and support your actions.

Q&A

ashley@teamt5.org
zha0@teamt5.org