HIT2011
Hacks in Taiwan Conference

APT SECRETS IN ASIA

奧義 亞洲的APT奧義

{Anthony Lai, Benson Wu, Jeremy Chiu},
Founder and Security Researcher, Xecure Lab
anthony.lai@xecure-lab.com
benson.wu@xecure-lab.com
jeremy.chiu@xecure-lab.com

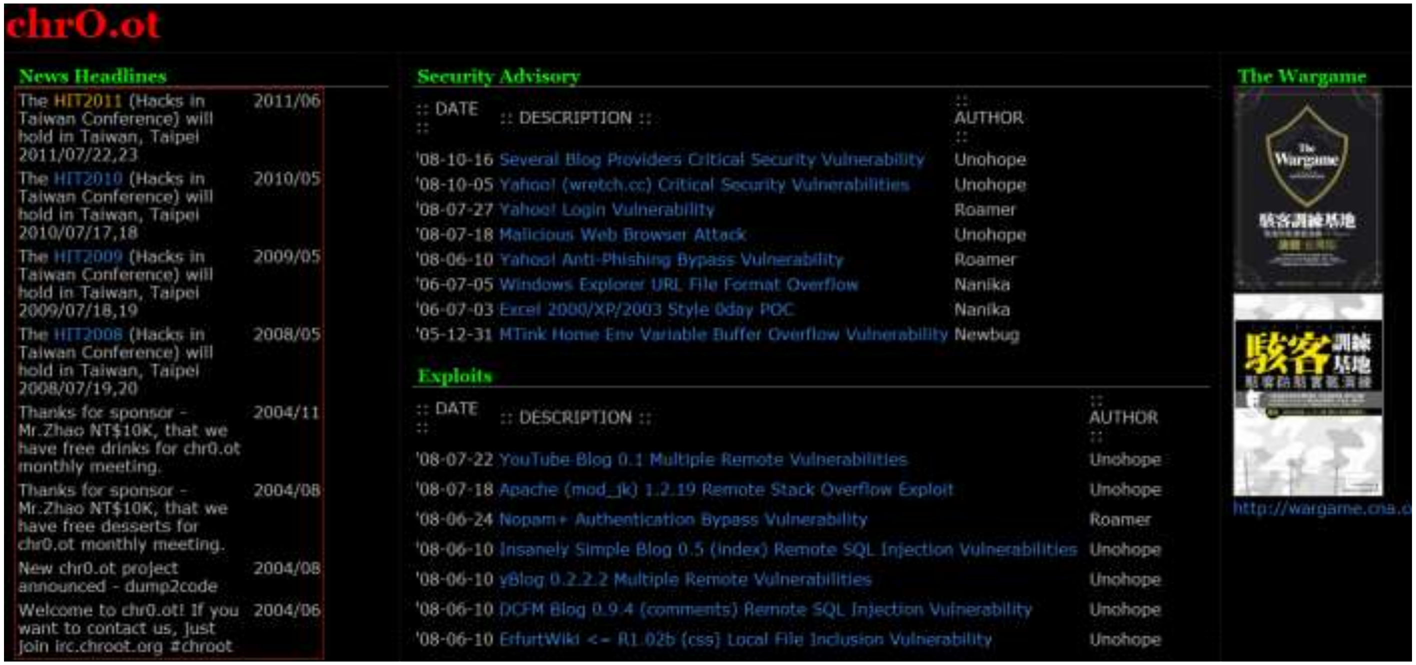
http://blog.xecure-lab.com

Xecure Lab

Chroot Security Group

http://www.chroot.org/

- CHROOT 成立於西元2004年，是台灣一群專業、優質又玉樹臨風的好孩子組成的。



chr0.ot

News Headlines

The HIT2011 (Hacks in Taiwan Conference) will hold in Taiwan, Taipei 2011/07/22,23	2011/06
The HIT2010 (Hacks in Taiwan Conference) will hold in Taiwan, Taipei 2010/07/17,18	2010/05
The HIT2009 (Hacks in Taiwan Conference) will hold in Taiwan, Taipei 2009/07/18,19	2009/05
The HIT2008 (Hacks in Taiwan Conference) will hold in Taiwan, Taipei 2008/07/19,20	2008/05
Thanks for sponsor - Mr.Zhao NT$10K, that we have free drinks for chr0.ot monthly meeting.	2004/11
Thanks for sponsor - Mr.Zhao NT$10K, that we have free desserts for chr0.ot monthly meeting.	2004/08
New chr0.ot project announced - dump2code	2004/08
Welcome to chr0.ot! If you want to contact us, just join irc.chroot.org #chroot	2004/06

Security Advisory

:: DATE ::	:: DESCRIPTION ::	:: AUTHOR ::
'08-10-16	Several Blog Providers Critical Security Vulnerability	Unohope
'08-10-05	Yahoo! (wretch.cc) Critical Security Vulnerabilities	Unohope
'08-07-27	Yahoo! Login Vulnerability	Roamer
'08-07-18	Malicious Web Browser Attack	Unohope
'08-06-10	Yahoo! Anti-Phishing Bypass Vulnerability	Roamer
'06-07-05	Windows Explorer URL File Format Overflow	Nanika
'06-07-03	Excel 2000/XP/2003 Style 0day POC	Nanika
'05-12-31	MTink Home Env Variable Buffer Overflow Vulnerability	Newbug

Exploits

:: DATE ::	:: DESCRIPTION ::	:: AUTHOR ::
'08-07-22	YouTube Blog 0.1 Multiple Remote Vulnerabilities	Unohope
'08-07-18	Apache (mod_jk) 1.2.19 Remote Stack Overflow Exploit	Unohope
'08-06-24	Nopam+ Authentication Bypass Vulnerability	Roamer
'08-06-10	Insanely Simple Blog 0.5 (index) Remote SQL Injection Vulnerabilities	Unohope
'08-06-10	yBlog 0.2.2.2 Multiple Remote Vulnerabilities	Unohope
'08-06-10	DCFM Blog 0.9.4 (comments) Remote SQL Injection Vulnerability	Unohope
'08-06-10	ErfurtWiki <= R1.02b (css) Local File Inclusion Vulnerability	Unohope

The Wargame

http://wargame.cna.c

(會員招募中，目前團報另有優惠)

Xecure Lab Team

- Yes! We are all the good guys ☺

Birdman

Benson

DarkFloyd

http://blog.xecure-lab.com

Bio

- **Jeremy Chiu (aka Birdman)**
  - He has more than ten years of experience with host-based security, focusing on kernel technologies for both the Win32 and Linux platforms. In early 2001 he was created Taiwan's first widespread trojan BirdSPY. And now, he is also a contract trainer for law enforcements, intelligence organizations, and conferences such as DEFCON 18, SySCAN (09 08), Hacks in Taiwan (07 06 05), HTICA(06 08) and OWASP Asia (08 07). Jeremy specializes in rootkit/backdoor design. Jeremy also specializes in reverse engineering and malware analysis, and has been contracted by law enforcements to assist in forensics operations. Jeremy is a sought-after speaker for topics related to security, kernel programming, and object-oriented design

- **Benson Wu**
  - He currently works as Postdoctoral Researcher from Research Center for Information Technology Innovation at Academia Sinica in Taiwan. He focuses research on malware and threat analysis, code review, secure coding and SDLC process implementation. He graduated from National Taiwan University with PhD degree in Electrical Engineering. He had spoken at NIST SATE 2009, DEFCON 18 (with Birdman), OWASP China 2010, and wrote the "Web Application Security Guideline" for the Taiwan government.

- **Anothny Lai (aka DarkFlyod)**
  - He works on code audit, penetration test, crime investigation and threat analysis and acted as security consultant in various MNCs. His interest falls on studying exploit, reverse engineering, analyse threat and join CTFs, it would be nice to keep going and boost this China-made security wind in malware analysis and advanced persistent threat areas.
  - He found security research group called VXRL in Hong Kong and has been working as visiting lecturer in HK Polytechnic University on hacking course :) Spoken at Blackhat USA 2010, DEFCON 18 and Hack In Taiwan 2010/2011

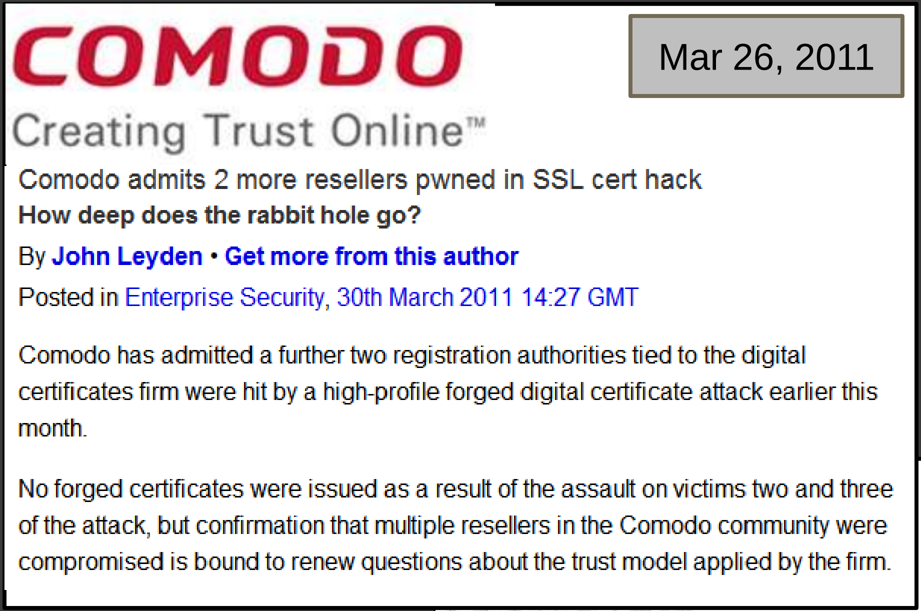
Abstract

- APT (Advanced Persistent Threat) means any targeted attacks against any specific company/organization from an or/and a group of organized attack party(ies).
- Other than providing the case studies, we would like to present and analyze APT from the malicious email document, throughout our automated analysis, we could identify and cluster the correlation among the samples featured with various exploit, malware and Botnet .

APT

- What is APT ?
- What is not APT !
- APT Events
- APT: Multi-vectors Attacking

Important APT Events In This Year



Mar 26, 2011

COMODO
Creating Trust Online™

Comodo admits 2 more resellers pwned in SSL cert hack

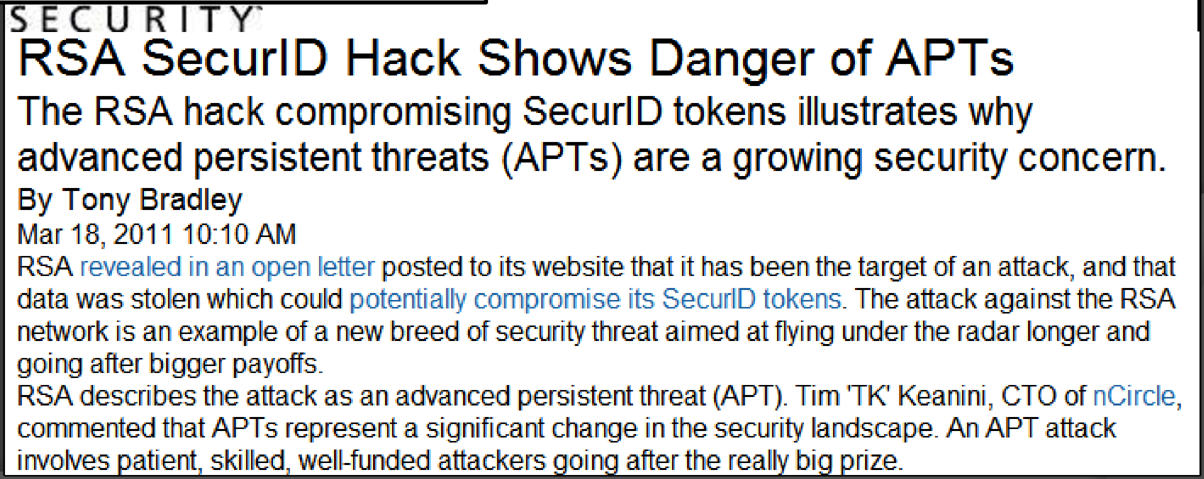
How deep does the rabbit hole go?

By **John Leyden** • **Get more from this author**

Posted in Enterprise Security, 30th March 2011 14:27 GMT

Comodo has admitted a further two registration authorities tied to the digital certificates firm were hit by a high-profile forged digital certificate attack earlier this month.

No forged certificates were issued as a result of the assault on victims two and three of the attack, but confirmation that multiple resellers in the Comodo community were compromised is bound to renew questions about the trust model applied by the firm.



Mar 18, 2011

SECURITY

RSA SecurID Hack Shows Danger of APTs

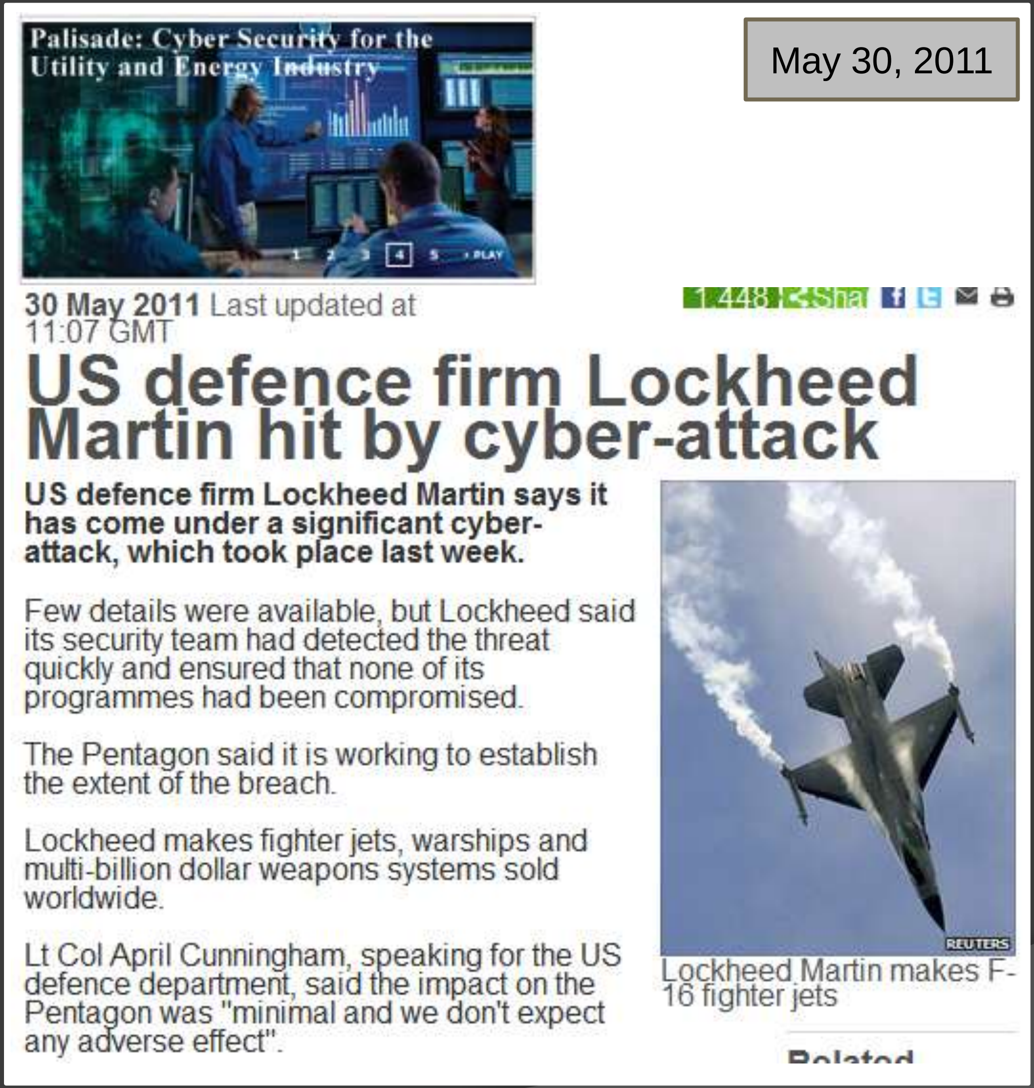
The RSA hack compromising SecurID tokens illustrates why advanced persistent threats (APTs) are a growing security concern.

By Tony Bradley
Mar 18, 2011 10:10 AM

RSA revealed in an open letter posted to its website that it has been the target of an attack, and that data was stolen which could potentially compromise its SecurID tokens. The attack against the RSA network is an example of a new breed of security threat aimed at flying under the radar longer and going after bigger payoffs.

RSA describes the attack as an advanced persistent threat (APT). Tim 'TK' Keanini, CTO of nCircle, commented that APTs represent a significant change in the security landscape. An APT attack involves patient, skilled, well-funded attackers going after the really big prize.

Lockheed Martin !


Palisade: Cyber Security for the Utility and Energy Industry
1 2 3 4 5 › PLAY
1,448 Sha
REUTERS

May 30, 2011

30 May 2011 Last updated at 11:07 GMT

US defence firm Lockheed Martin hit by cyber-attack

US defence firm Lockheed Martin says it has come under a significant cyber-attack, which took place last week.

Few details were available, but Lockheed said its security team had detected the threat quickly and ensured that none of its programmes had been compromised.

The Pentagon said it is working to establish the extent of the breach.

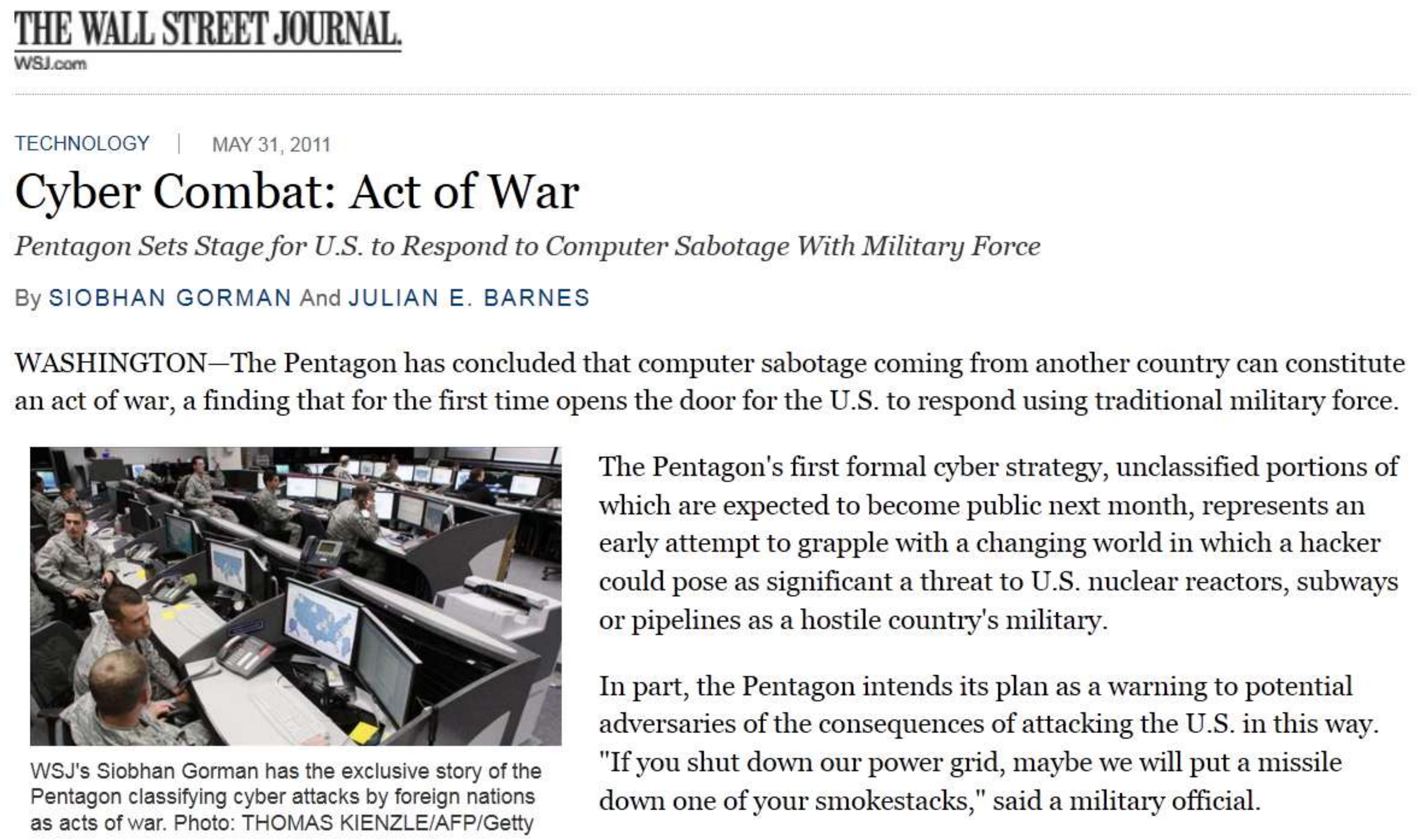
Lockheed makes fighter jets, warships and multi-billion dollar weapons systems sold worldwide.

Lt Col April Cunningham, speaking for the US defence department, said the impact on the Pentagon was "minimal and we don't expect any adverse effect".

Lockheed Martin makes F-16 fighter jets

Related

Act of WAR !



THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | MAY 31, 2011

Cyber Combat: Act of War

Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force

By SIOBHAN GORMAN And JULIAN E. BARNES

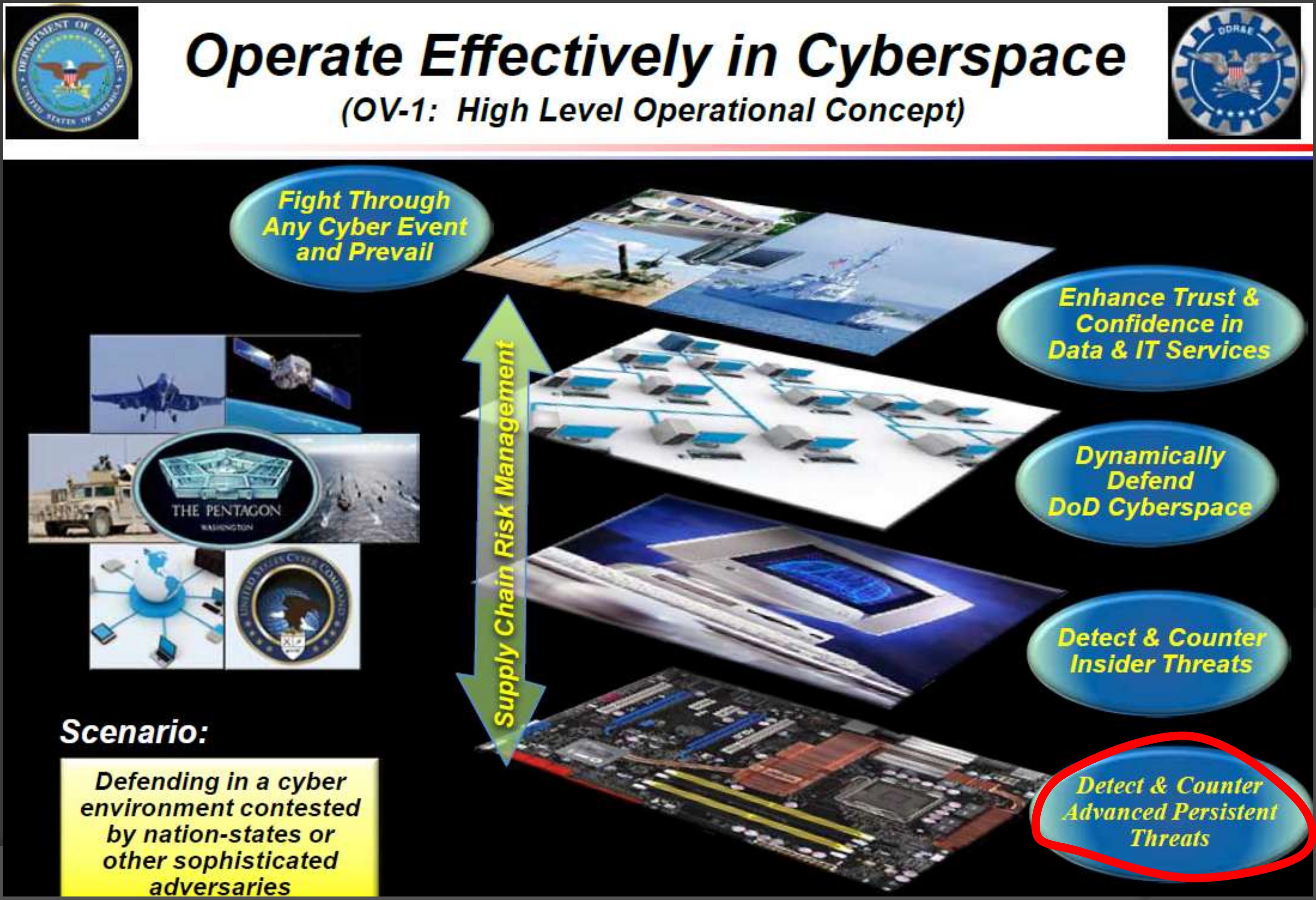
WASHINGTON—The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force.

WSJ's Siobhan Gorman has the exclusive story of the Pentagon classifying cyber attacks by foreign nations as acts of war. Photo: THOMAS KIENZLE/AFP/Getty

The Pentagon's first formal cyber strategy, unclassified portions of which are expected to become public next month, represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military.

In part, the Pentagon intends its plan as a warning to potential adversaries of the consequences of attacking the U.S. in this way. "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," said a military official.

DoD: APT偵測與防護是資訊戰基石



Operate Effectively in Cyberspace

(OV-1: High Level Operational Concept)

Fight Through Any Cyber Event and Prevail

Enhance Trust & Confidence in Data & IT Services

Dynamically Defend DoD Cyberspace

Detect & Counter Insider Threats

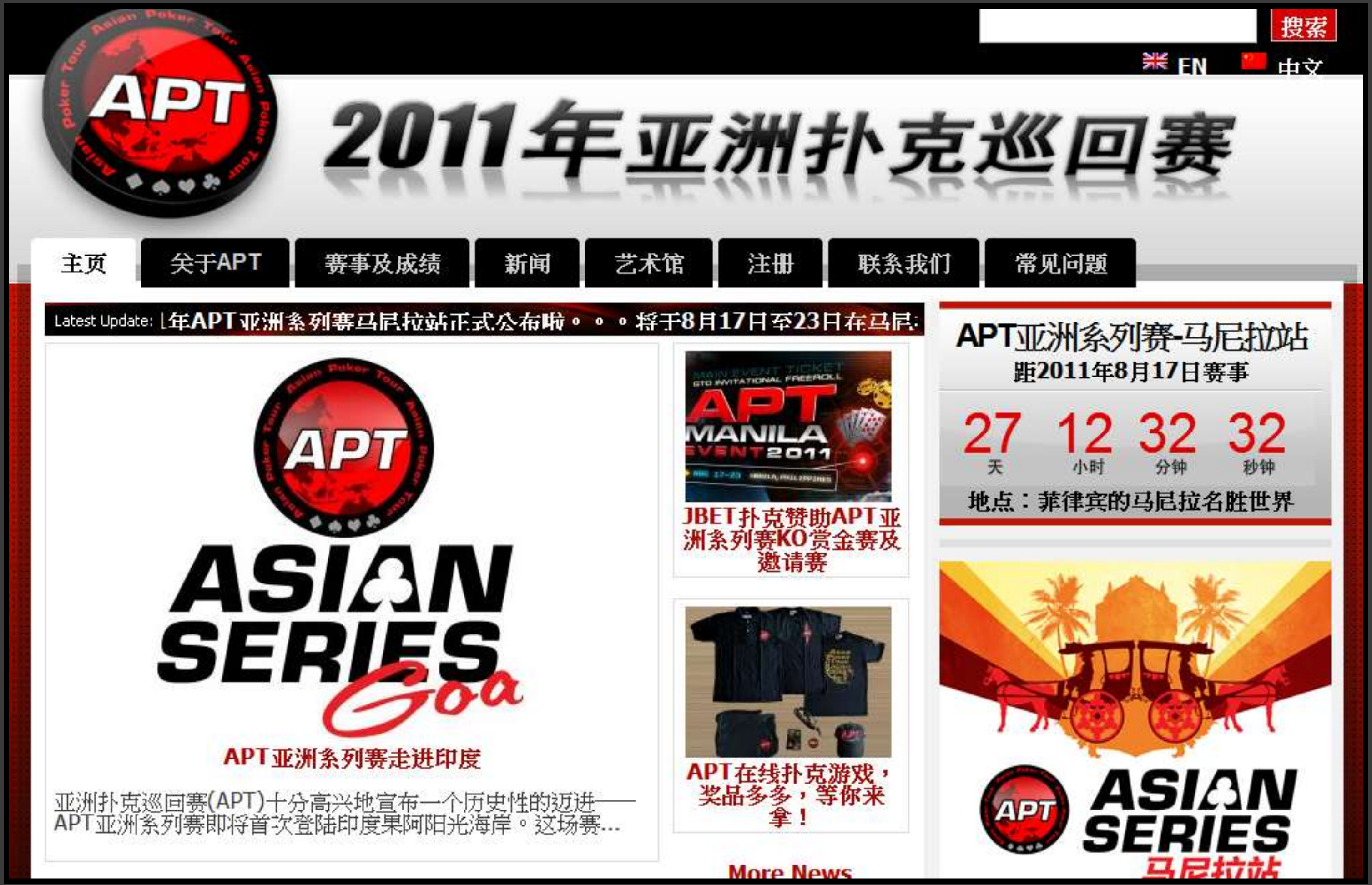
Detect & Counter Advanced Persistent Threats

Supply Chain Risk Management

Scenario:

Defending in a cyber environment contested by nation-states or other sophisticated adversaries

It is not APT !



搜索

EN 中文

2011年亚洲扑克巡回赛

主页 | 关于APT | 赛事及成绩 | 新闻 | 艺术馆 | 注册 | 联系我们 | 常见问题

Latest Update: 年APT亚洲系列赛马尼拉站正式公布啦。。。将于8月17日至23日在马尼

APT亚洲系列赛走进印度

亚洲扑克巡回赛(APT)十分高兴地宣布一个历史性的迈进——APT亚洲系列赛即将首次登陆印度果阿阳光海岸。这场赛...

JBET扑克赞助APT亚洲系列赛KO赏金赛及邀请赛

APT在线扑克游戏，奖品多多，等你来拿！

More News

APT亚洲系列赛-马尼拉站

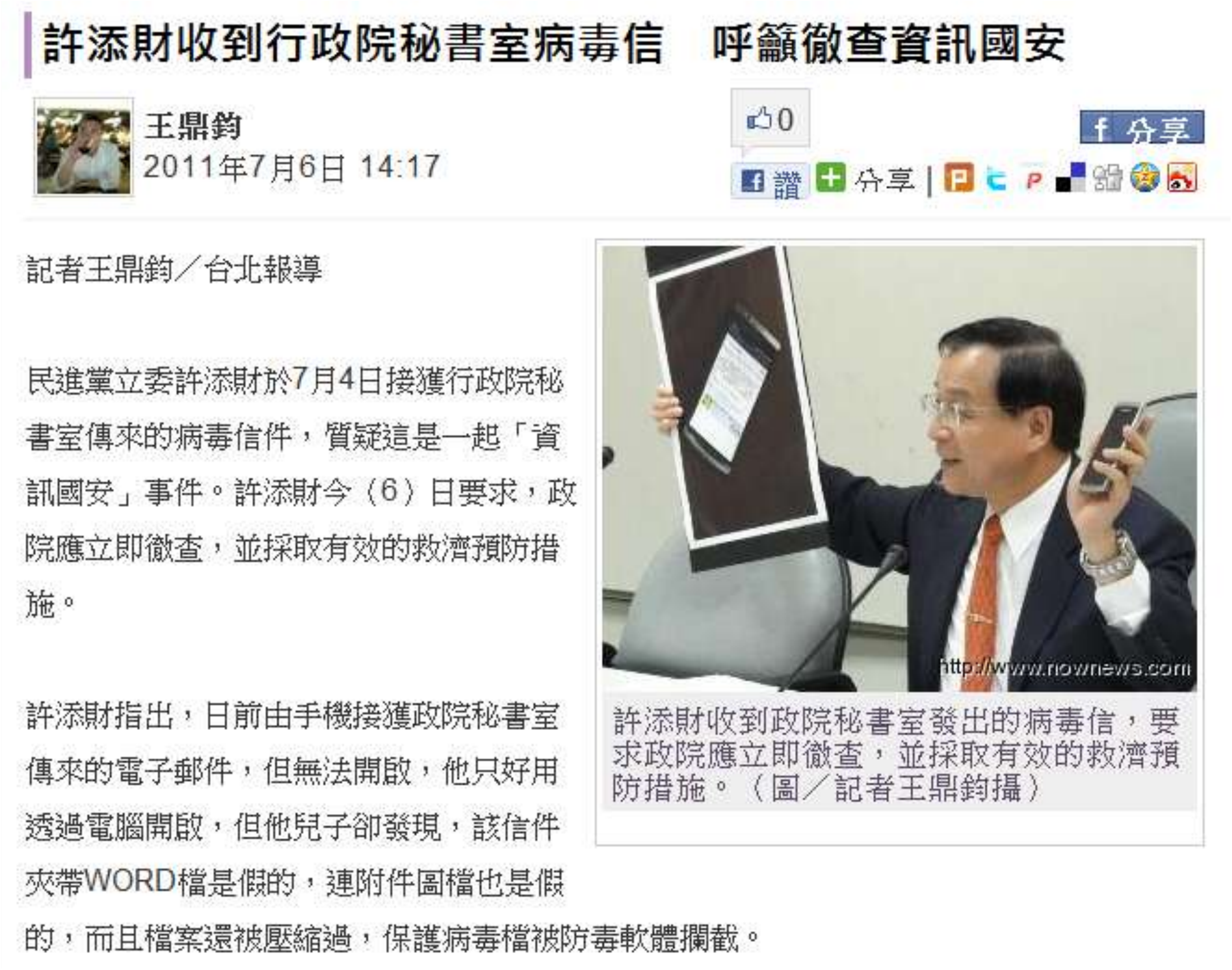
距2011年8月17日赛事

27 天 12 小时 32 分钟 32 秒钟

地点：菲律宾的马尼拉名胜世界

ㄟ~這個…不是那個… !!

APT is not Virus problem !



許添財收到行政院秘書室病毒信　呼籲徹查資訊國安

王鼎鈞
2011年7月6日 14:17

記者王鼎鈞／台北報導

民進黨立委許添財於7月4日接獲行政院秘書室傳來的病毒信件，質疑這是一起「資訊國安」事件。許添財今（6）日要求，政院應立即徹查，並採取有效的救濟預防措施。

許添財收到政院秘書室發出的病毒信，要求政院應立即徹查，並採取有效的救濟預防措施。（圖／記者王鼎鈞攝）

許添財指出，日前由手機接獲政院秘書室傳來的電子郵件，但無法開啟，他只好用透過電腦開啟，但他兒子卻發現，該信件夾帶WORD檔是假的，連附件圖檔也是假的，而且檔案還被壓縮過，保護病毒檔被防毒軟體攔截。

APT是多種面向的攻擊路徑

- 外網主機如Web伺服器遭突破成功，多半是被SQL注入攻擊
- 受駭Web伺服器被作為跳板，對內網的其他伺服器或桌機進行偵蒐
- 內網機器如AD伺服器或開發人員電腦遭突破成功，多半是被密碼暴力破解
- 受害者的工作與私人信箱被設定自動被份給駭客
- 受駭機器遭植入惡意程式，多半被安裝遠端控制工具（RAT），傳回大量機敏文件（WORD、PPT、PDF等等），包括所有會議記錄與組織人事架構圖
- 更多內網機器被"設計"遭入侵成功，多半為高階主管點擊了看似正常的郵件附檔，卻不知其中含有惡意程式

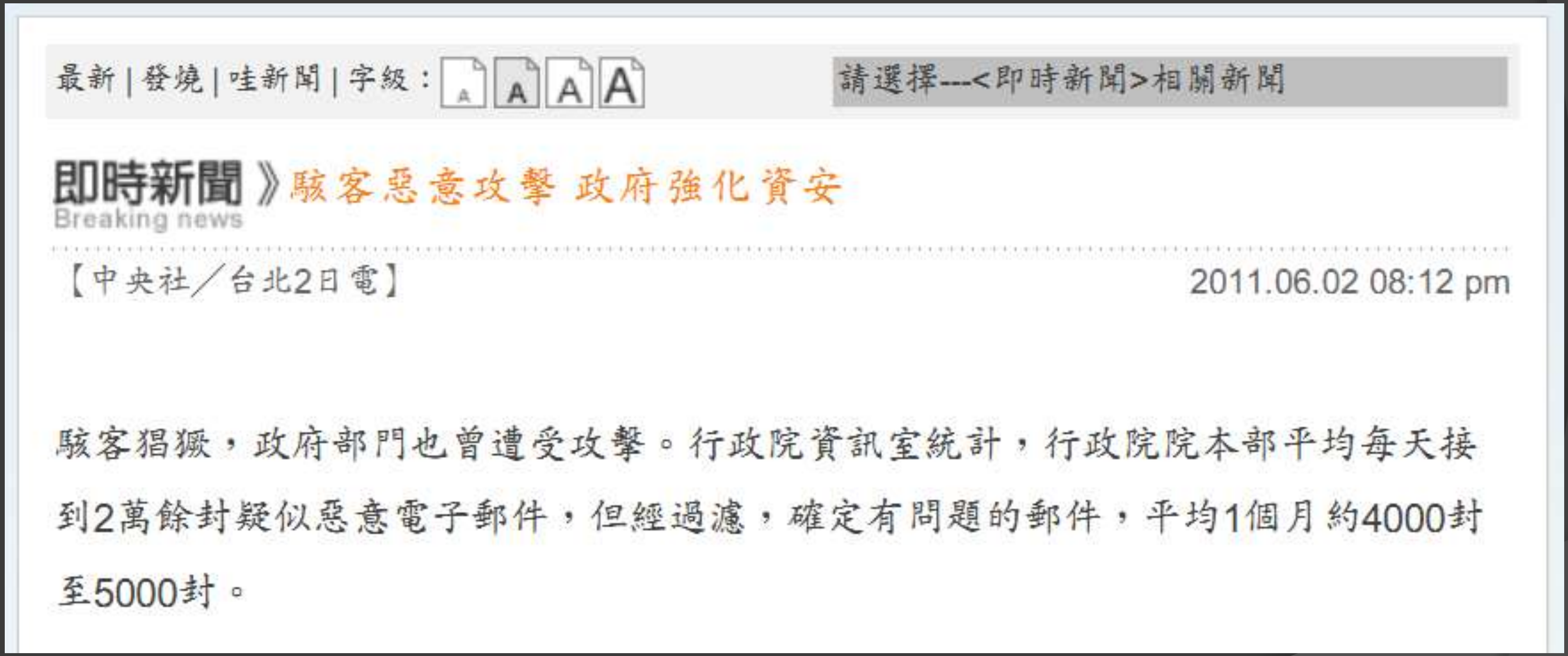
APT Attack Vs Traditional Botnet Activities

	APT Activities	Crime-Group Activities
	With organized planning	Mass distribution over regions
Cause damage?	No	No
Target or Not	Targeted (only a few groups/organizations)	Not targeted (large area spread-out)
Target Audience	Particular organization/company	Individual credentials including online banking account information
Frequency of attacks	Many times	Once
Weapon	• Zero-Day Exploit • Drop Embedded RAT • Dropper or Backdoor	• Multiple-Exploits, All in one! • URL Download Botnet • Full function RAT
Detection Rate	Detection rate is lower than 10% if the sample comes out within one month	Detection rate is around 95% if the sample comes out within one month

Remarks: IPS, IDS and Firewall cannot help and detect in this area

Continued APT Mail EVERYDAY!

- 20,000 Malicious Mails !?



最新 | 發燒 | 哇新聞 | 字級：A A A A

即時新聞 Breaking news 》駭客惡意攻擊 政府強化資安

【中央社／台北2日電】 2011.06.02 08:12 pm

駭客猖獗，政府部門也曾遭受攻擊。行政院資訊室統計，行政院院本部平均每天接到2萬餘封疑似惡意電子郵件，但經過濾，確定有問題的郵件，平均1個月約4000封至5000封。

Major APT Activity: Targeted-Attack Email

- In APT activities, we have observed there are three major types of Targeted-Attack Email：
  - Phishing mail: Steal user ID and password
  - Malicious script: Detect end-use computing environment
  - Install and deploy Malware (Botnet) !

APT Mail = Document Exploit + Malware

Research Direction (1/2)

- We are not just focusing on a single one-off attack, we tend to observe the entire APT attack plan and trend
  - Traditionally, we just focus on malware forensics or analyze a single victim’ s machine. We cannot understand the APT attack plan and its trend indeed.

Research Direction (2/2)

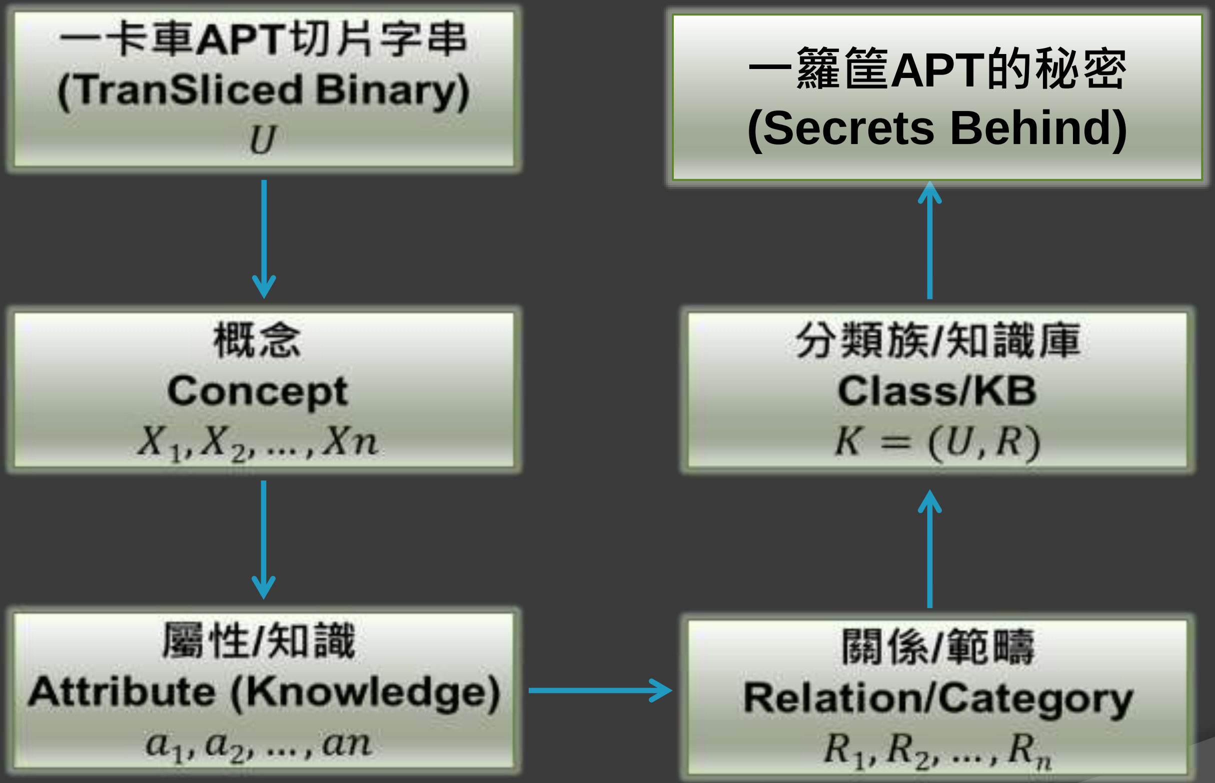
- **Analyze and extract features and characteristics of APT taskforce via:**
  - Malware features
  - Exploit
  - C&C Network
  - Speared Email
  - Victim’ s background
  - Time of attack

APT File Analysis and Grouping

- Theoretically, in an information system (i.e. malware analysis system), if we could collect all the attributes/properties of our malicious sample sets, we could identify whether the executable/document/sample is malicious.

- However, the research issues are insufficient collection in attributes/characteristics (for example, the malware has been packed and engage various anti-debugging capabilities), so that we get the indiscernibility relation.

Research



一卡車APT切片字串
(TranSliced Binary)
U

概念
Concept
$X_1, X_2, \dots, Xn$

屬性/知識
Attribute (Knowledge)
$a_1, a_2, \dots, an$

關係/範疇
Relation/Category
$R_1, R_2, \dots, R_n$

分類族/知識庫
Class/KB
$K = (U, R)$

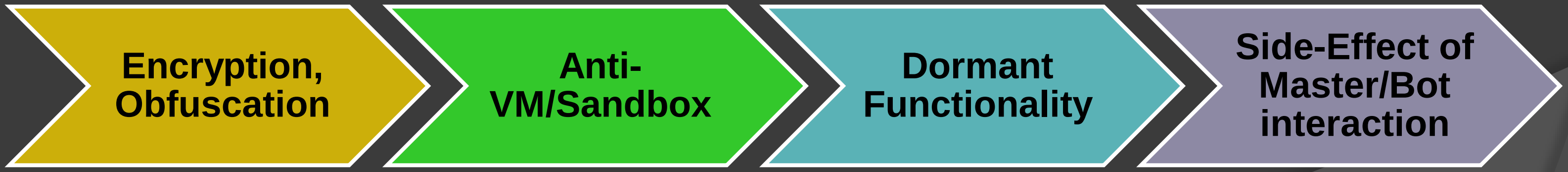
一籮筐APT的秘密
(Secrets Behind)

Standard Analysis Method

- Static Approach
  - Extract signature/features from file format
  - Reversing

- Dynamic Approach
  - Execute it under controlled environment and capture/log all the behaviors
  - Analyze networking traffic

- Challenge of Malware/Exploit Analysis



Encryption, Obfuscation

Anti-VM/Sandbox

Dormant Functionality

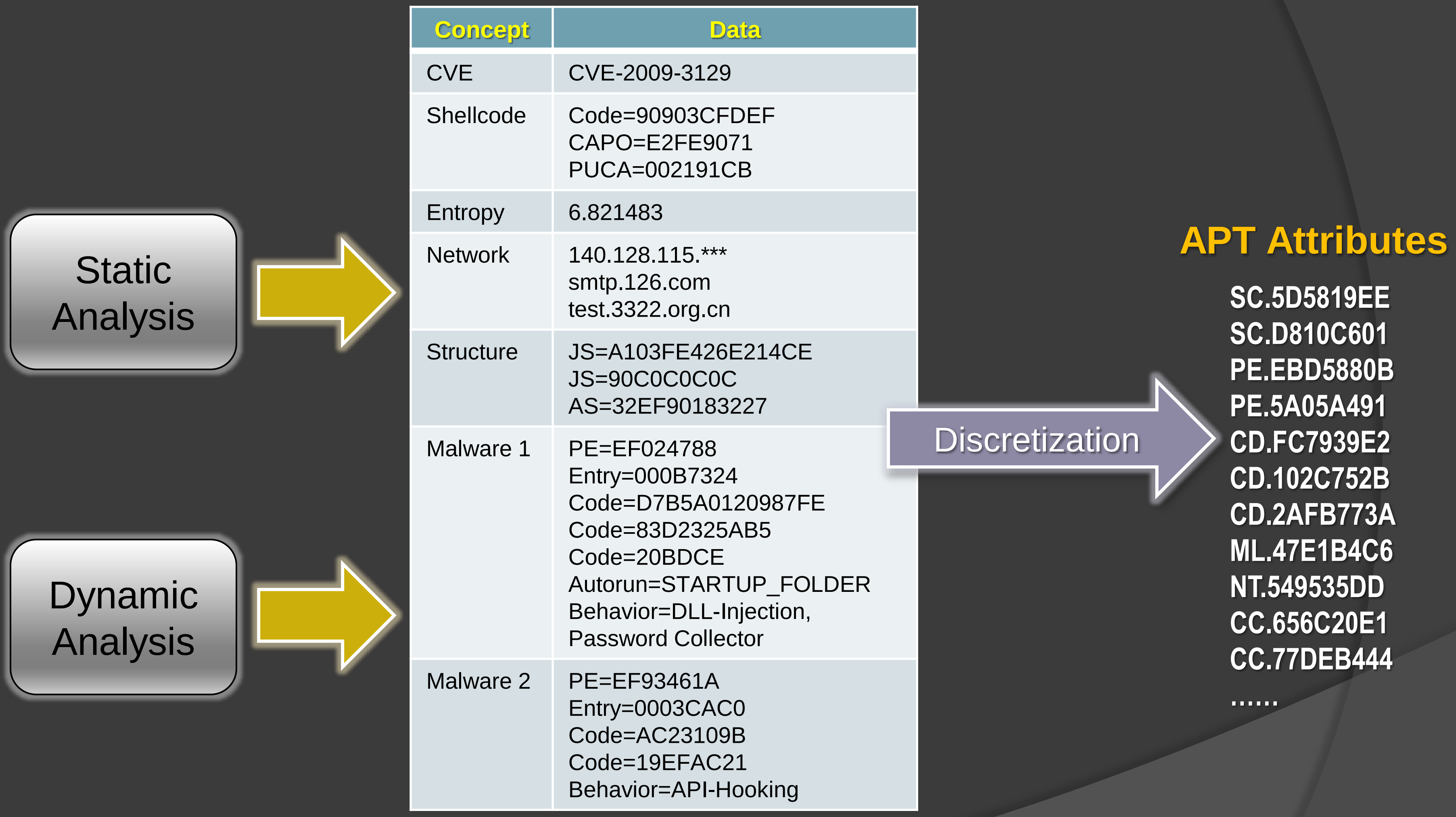
Side-Effect of Master/Bot interaction

We prefer using static analysis to prevent from Anti-VM, dormant functionality and side effect of master/bot interaction.

What APT Attributes we focused?

- We work on the analysis on multi-concepts basis.
- Throughout static analysis:
  - Extract and review executable, Shellcode and PE header
  - Objects and abnormal structure in file
- Throughout dynamic analysis:
  - Install the system into Windows
  - Scan Process Memory to detect abnormal structure
  - Code-Injection, API Hooking …
  - Detect any known Code Snippet
  - Rootkit, KeyLogger, Password Collector, Anti-AV…
  - Suspicious strings: email address, domain, IP, URL

Extract Attributes from APT File



Static Analysis

Dynamic Analysis

Concept	Data
CVE	CVE-2009-3129

Shellcode	Code=90903CFDEF
	CAPO=E2FE9071
	PUCA=002191CB

Entropy	6.821483
Network	140.128.115.*** smtp.126.com test.3322.org.cn

Structure	JS=A103FE426E214CE
	JS=90C0C0C0C
	AS=32EF90183227

Malware 1	PE=EF024788
	Entry=000B7324
	Code=D7B5A0120987FE
	Code=83D2325AB5
	Code=20BDCE
	Autorun=STARTUP_FOLDER
	Behavior=DLL-Injection,
	Password Collector

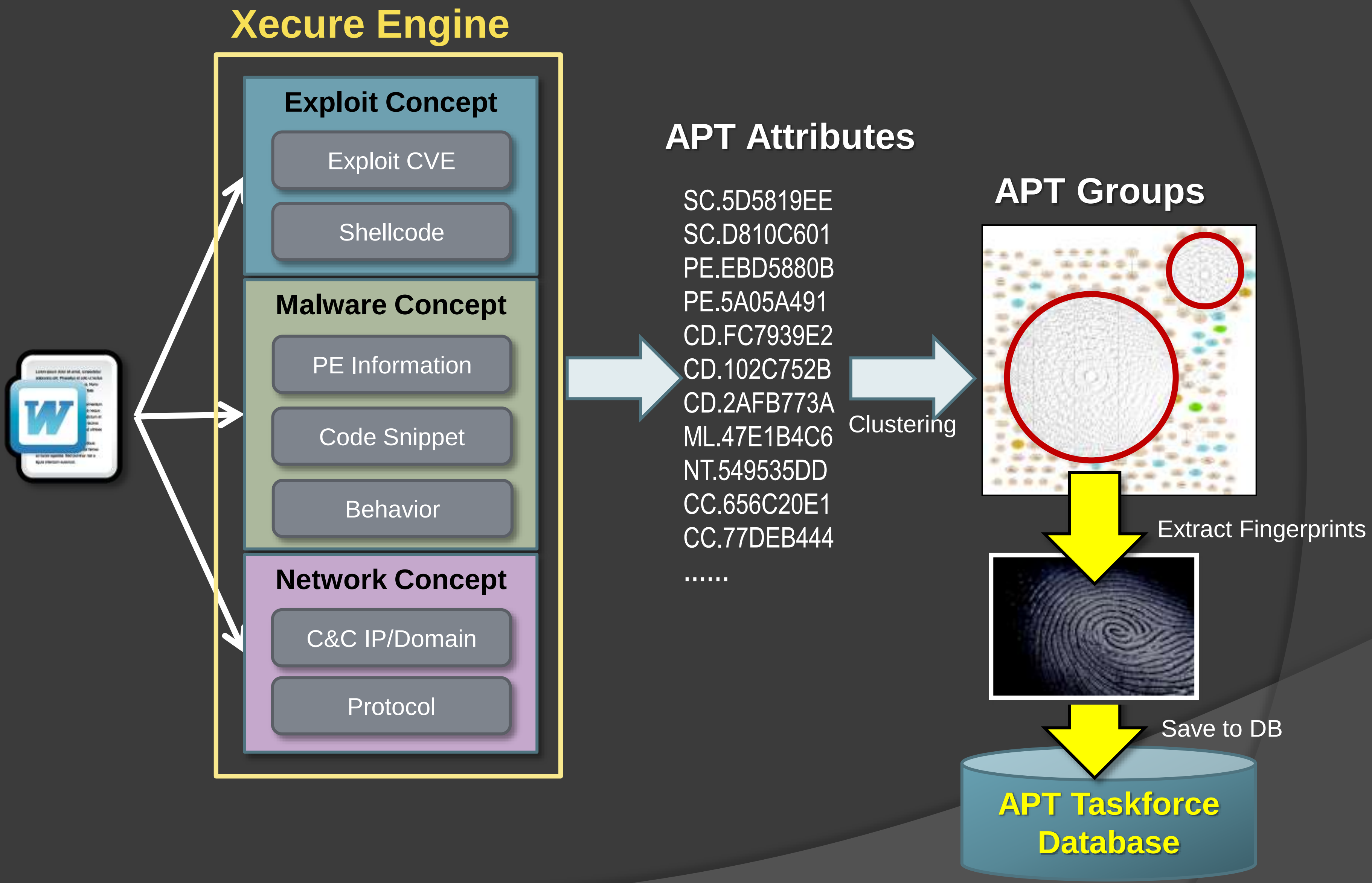
Malware 2	PE=EF93461A
	Entry=0003CAC0
	Code=AC23109B
	Code=19EFAC21
	Behavior=API-Hooking

Discretization

APT Attributes

SC.5D5819EE
SC.D810C601
PE.EBD5880B
PE.5A05A491
CD.FC7939E2
CD.102C752B
CD.2AFB773A
ML.47E1B4C6
NT.549535DD
CC.656C20E1
CC.77DEB444
……

Clustering !



Xecure Engine

Exploit Concept

- Exploit CVE
- Shellcode

Malware Concept

- PE Information
- Code Snippet
- Behavior

Network Concept

- C&C IP/Domain
- Protocol

APT Attributes

SC.5D5819EE
SC.D810C601
PE.EBD5880B
PE.5A05A491
CD.FC7939E2
CD.102C752B
CD.2AFB773A
ML.47E1B4C6
NT.549535DD
CC.656C20E1
CC.77DEB444
……

Clustering

APT Groups

Extract Fingerprints

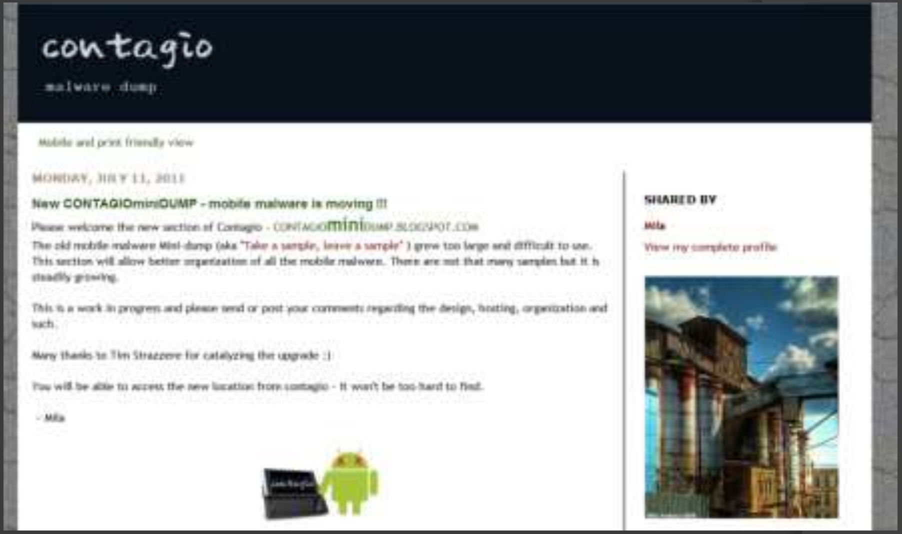
Save to DB

APT Taskforce Database

Experiment

- Mila's provided APT sample archives are confirmed to malicious
- Those archives are open to public for downloading and analysis (Collection1, 242 APT files)
- The sample archives are used by many researchers

- http://contagiodump.blogspot.com/



contagio

malware dump

Mobile and print friendly view

MONDAY, JULY 11, 2011

New CONTAGIOminiDUMP - mobile malware is moving !!!

Please welcome the new section of Contagio - CONTAGIOminiDUMP.BLOGSPOT.COM

The old mobile malware Mini-dump (aka "Take a sample, leave a sample") grew too large and difficult to use. This section will allow better organization of all the mobile malware. There are not that many samples but it is steadily growing.

This is a work in progress and please send or post your comments regarding the design, hosting, organization and such.

Many thanks to Tim Strazzere for catalyzing the upgrade :)

You will be able to access the new location from contagio - it won't be too hard to find.

- Mila

SHARED BY

Mila

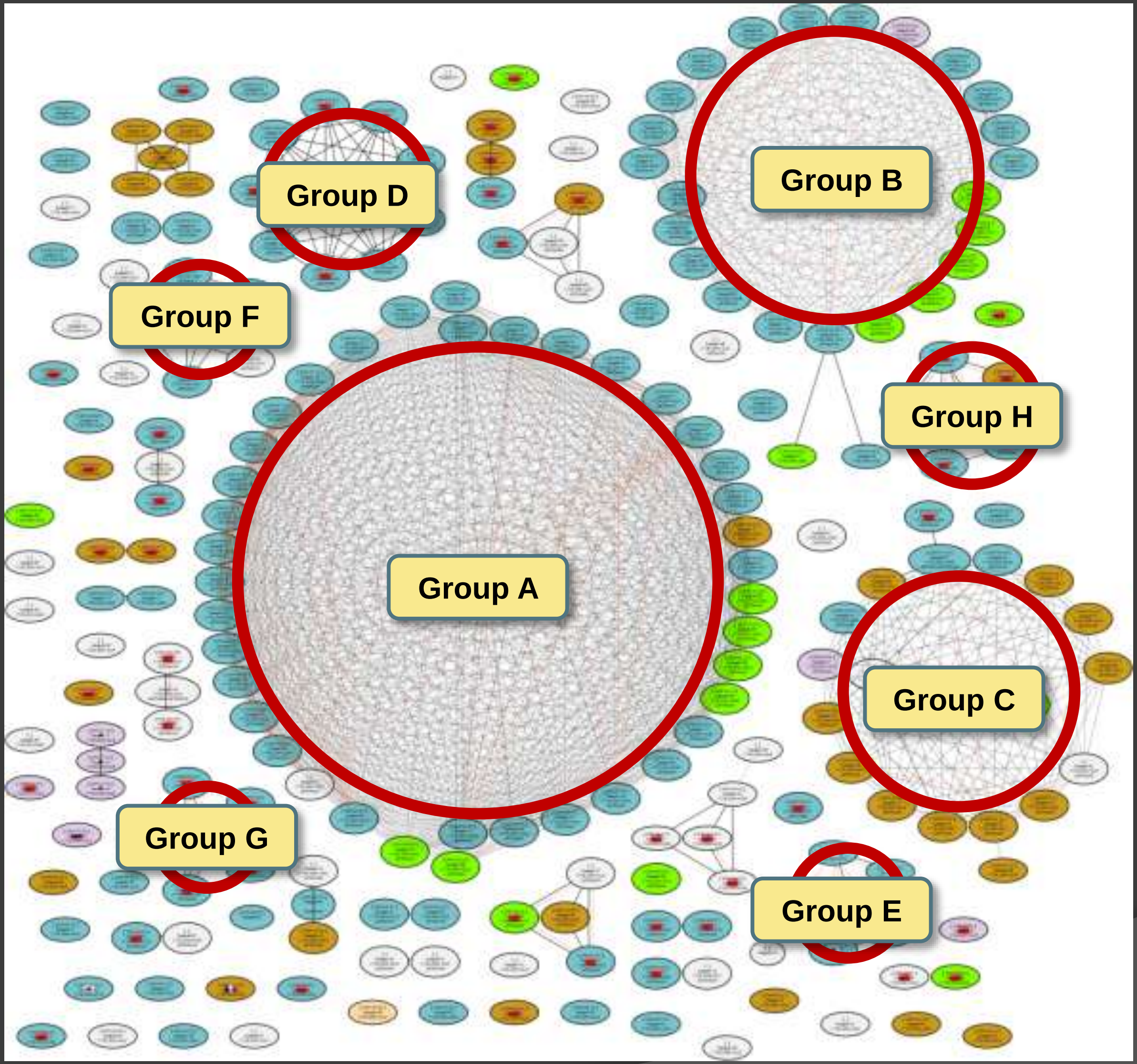
View my complete profile

Detection Rate

- Xecure Inspector
  - 94.62 % (229 / 242)

- Definition updated to 2011/6/11
  - Microsoft Security Essentials
    - 21.4 % (52 / 242)
  - Sophos
    - 35.9 % (87/242)
  - AntiVir
    - 56.6 % (137/242)

There are 8 major APT-Taskforce Groups



🟩 2011

🟦 2010

🟧 2009

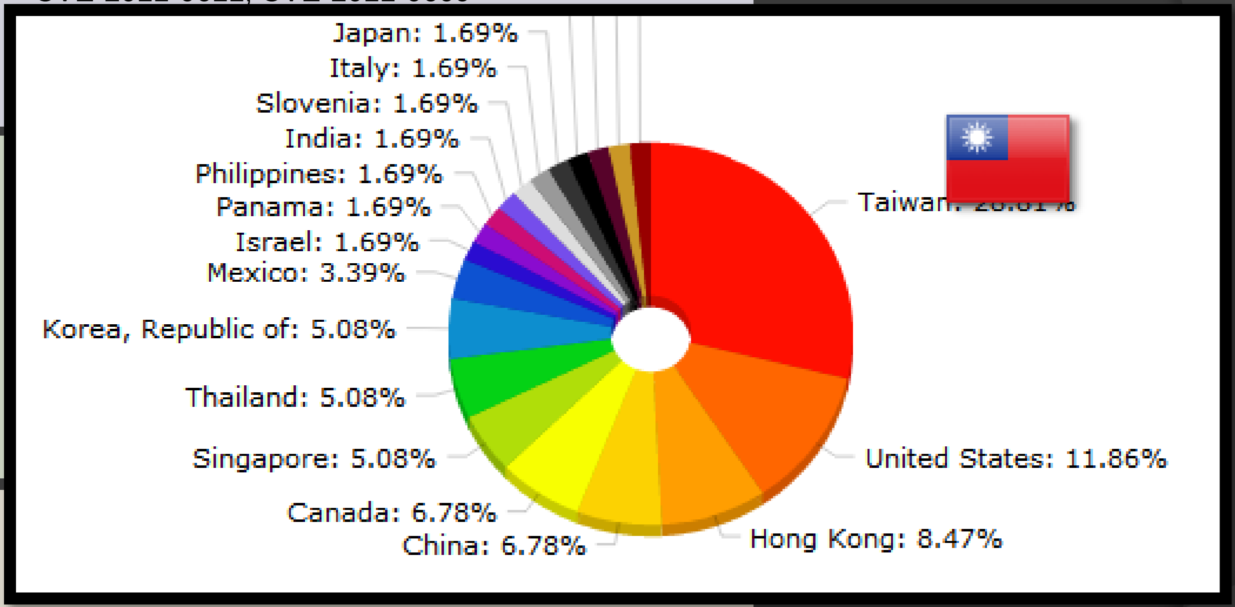
🟥 2008

⬜ other

Groups of Mila Sample Set Collection1

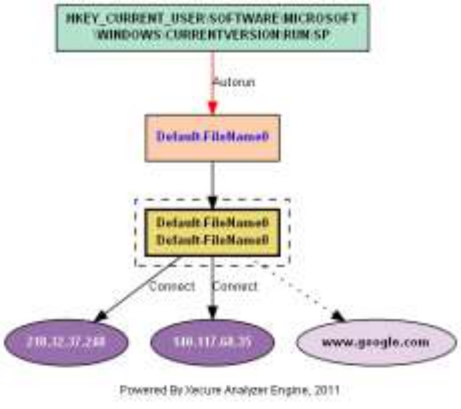
Top 3 APT Taskforce Groups

Group A	Active	2009-0923 ~ 2011-0420
	Number	40
	CVE	CVE-2009-4841, CVE-2009-0927, CVE-2009-3129, CVE-2009-4324, CVE-2010-0188, CVE-2010-2833, CVE-2011-0611, CVE-2011-0609
	Malware	
	C&C	
Group B	**Active**	
	Number	
	CVE	
	Malware	
	C&C	
Group C	**Active**	
	Number	
	CVE	CVE-2007-5659, CVE-2008-4841, CVE-2009-1862, CVE-2009-3129, CVE-2009-4324, CVE-2009-0658, CVE-2009-0927,
	Malware	APT00200
	C&C	IP:5, Domain:11

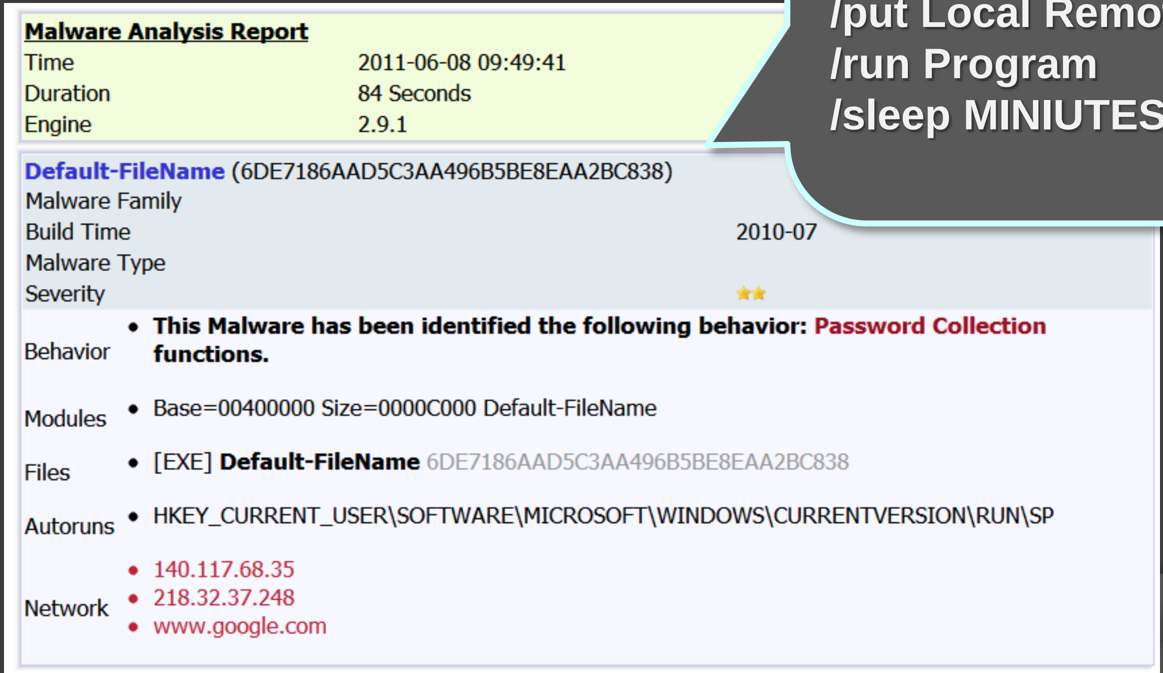


Malware of APT Group A

Malware Attack Graph



Malware Fix Suggestion



Malware Analysis Report

Time	2011-06-08 09:49:41
Duration	84 Seconds
Engine	2.9.1

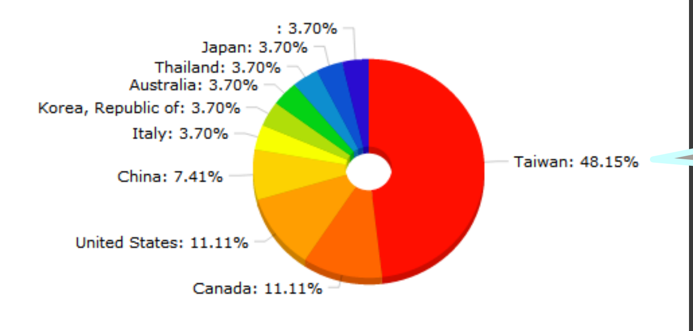
Default-FileName (6DE7186AAD5C3AA496B5BE8EAA2BC838)

Malware Family	
Build Time	2010-07
Malware Type	
Severity	★★
Behavior	- **This Malware has been identified the following behavior: Password Collection functions.**
Modules	- Base=00400000 Size=0000C000 Default-FileName
Files	- [EXE] **Default-FileName** 6DE7186AAD5C3AA496B5BE8EAA2BC838
Autoruns	- HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\SP
Network	- 140.117.68.35 - 218.32.37.248 - www.google.com

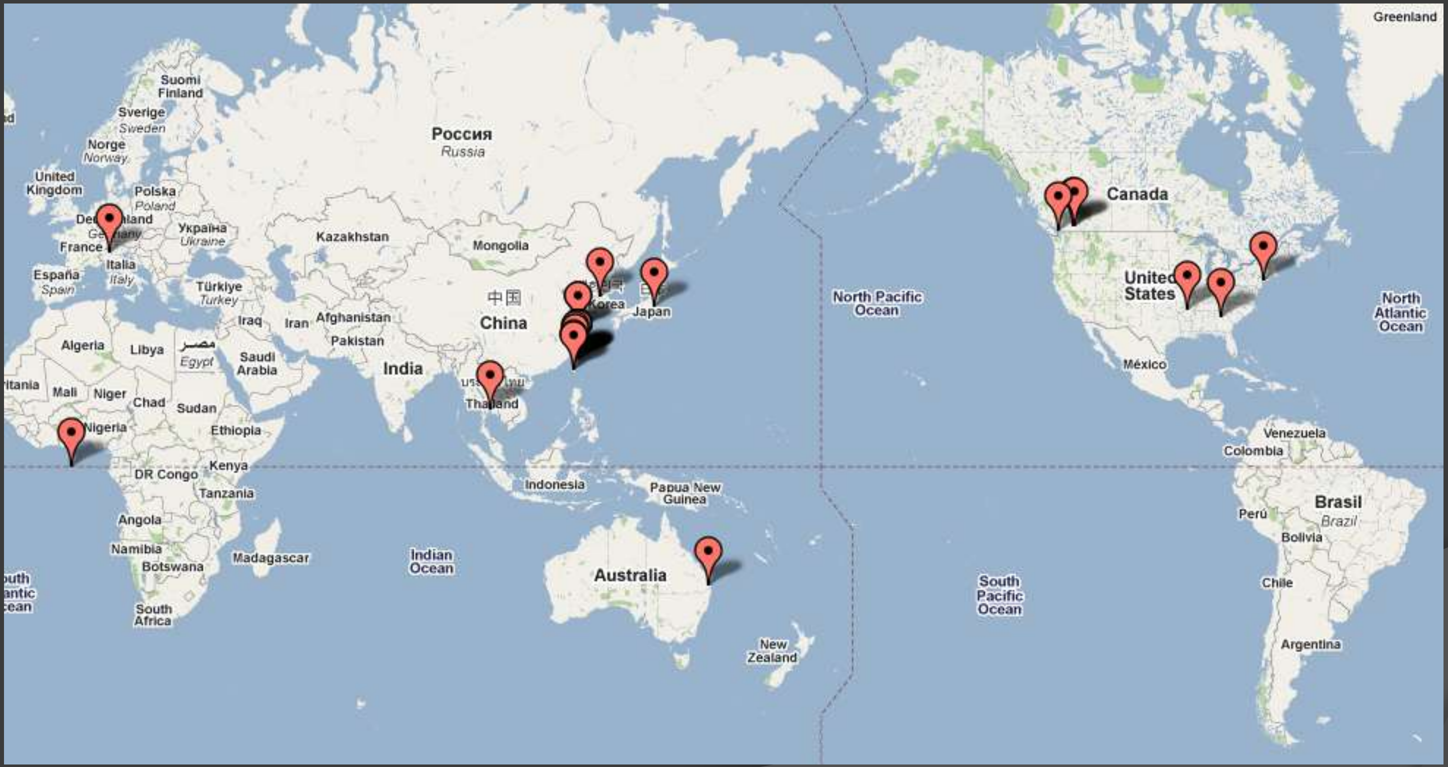
Bot Command

/get Remote Local
/rsh [SHELL FILE]
/shr [wins.exe]
/put Local Remote
/run Program
/sleep MINIUTES

C&C Location of APT Group A

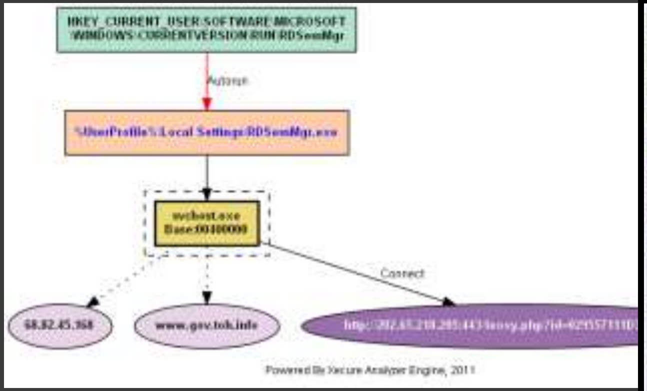


48.1% C&C IP located in Taiwan

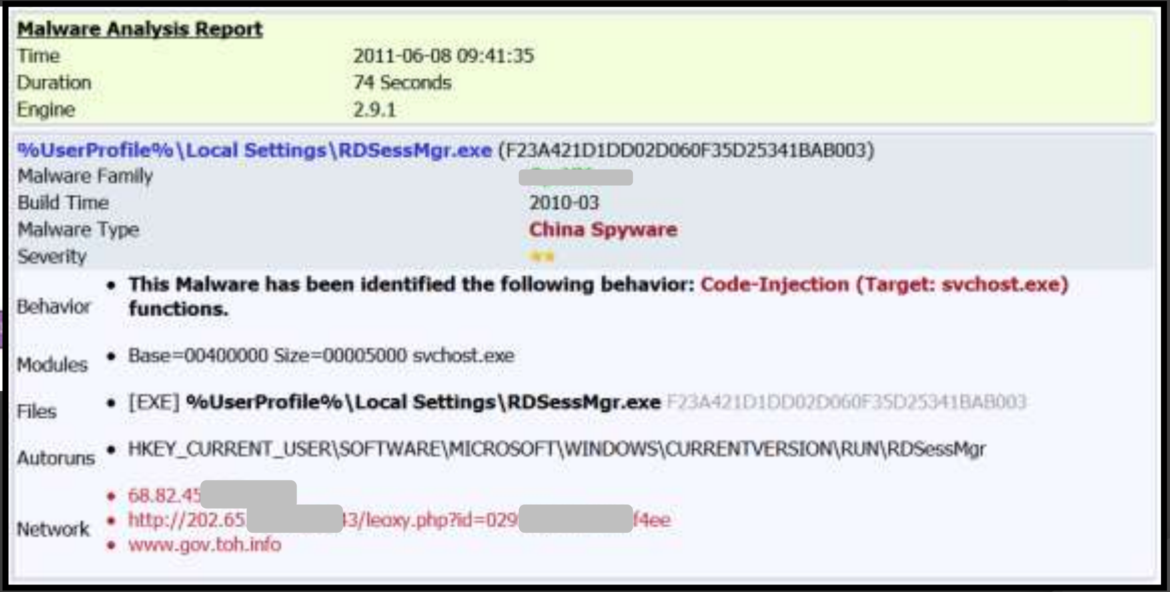


Malware of APT Group B

Malware Attack Graph


HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\RDSessMgr
Autorun
%UserProfile%\Local Settings\RDSessMgr.exe
svchost.exe
Base:00400000
Connect
68.82.45.168
www.gov.toh.info
http://202.65.218.285:443/leoxy.php?id=02955711
Powered By Xecure Analyzer Engine, 2011

Malware Fix Suggestion



Malware Analysis Report

Time	2011-06-08 09:41:35
Duration	74 Seconds
Engine	2.9.1

%UserProfile%\Local Settings\RDSessMgr.exe (F23A421D1DD02D060F35D25341BAB003)

Malware Family	[redacted]
Build Time	2010-03
Malware Type	**China Spyware**
Severity	★★

Behavior
- **This Malware has been identified the following behavior: Code-Injection (Target: svchost.exe) functions.**

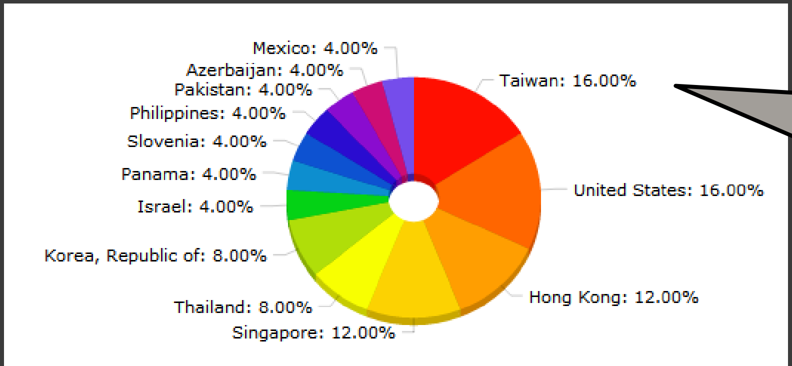
Modules
- Base=00400000 Size=00005000 svchost.exe

Files
- [EXE] **%UserProfile%\Local Settings\RDSessMgr.exe** F23A421D1DD02D060F35D25341BAB003

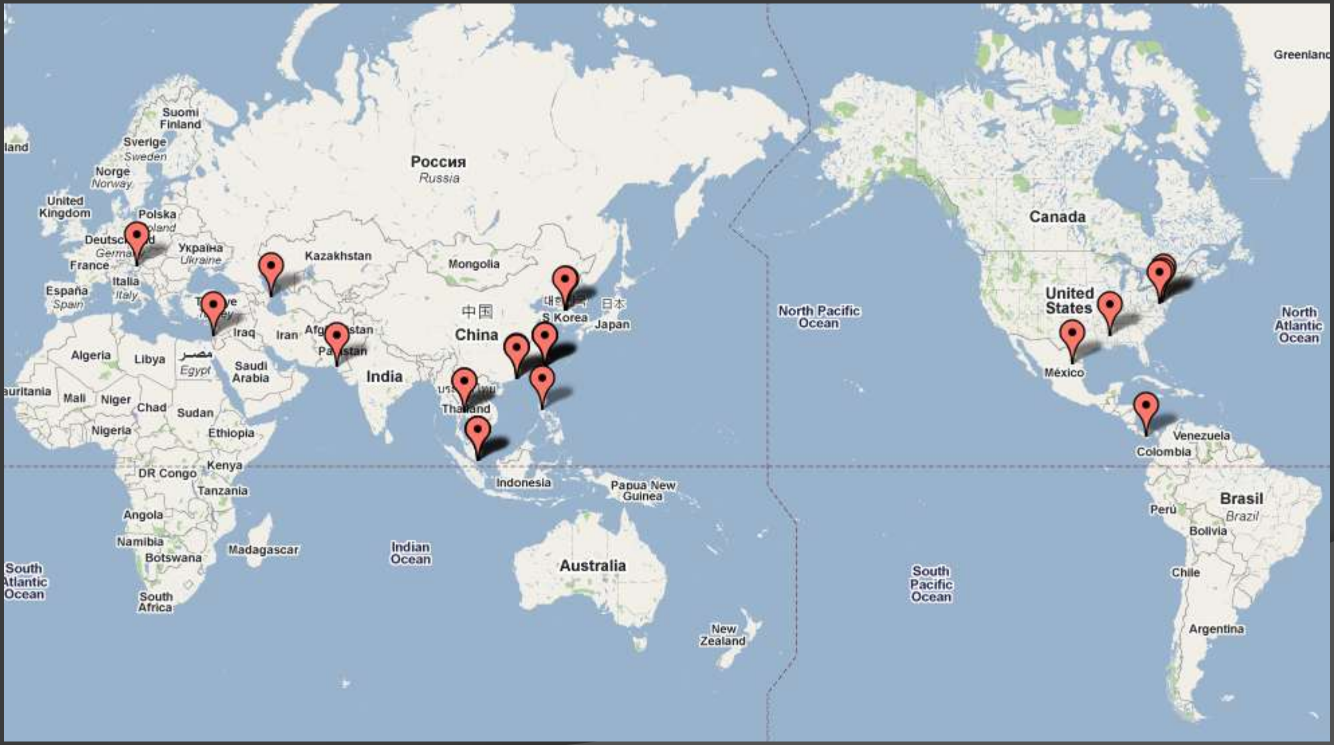
Autoruns
- HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\RDSessMgr

Network
- 68.82.45[redacted]
- http://202.65[redacted]3/leoxy.php?id=029[redacted]f4ee
- www.gov.toh.info

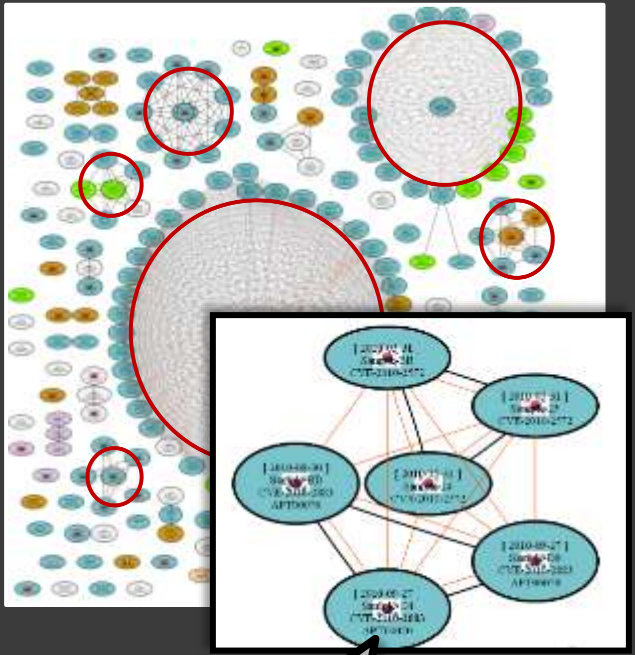
C&C Location of APT Group B



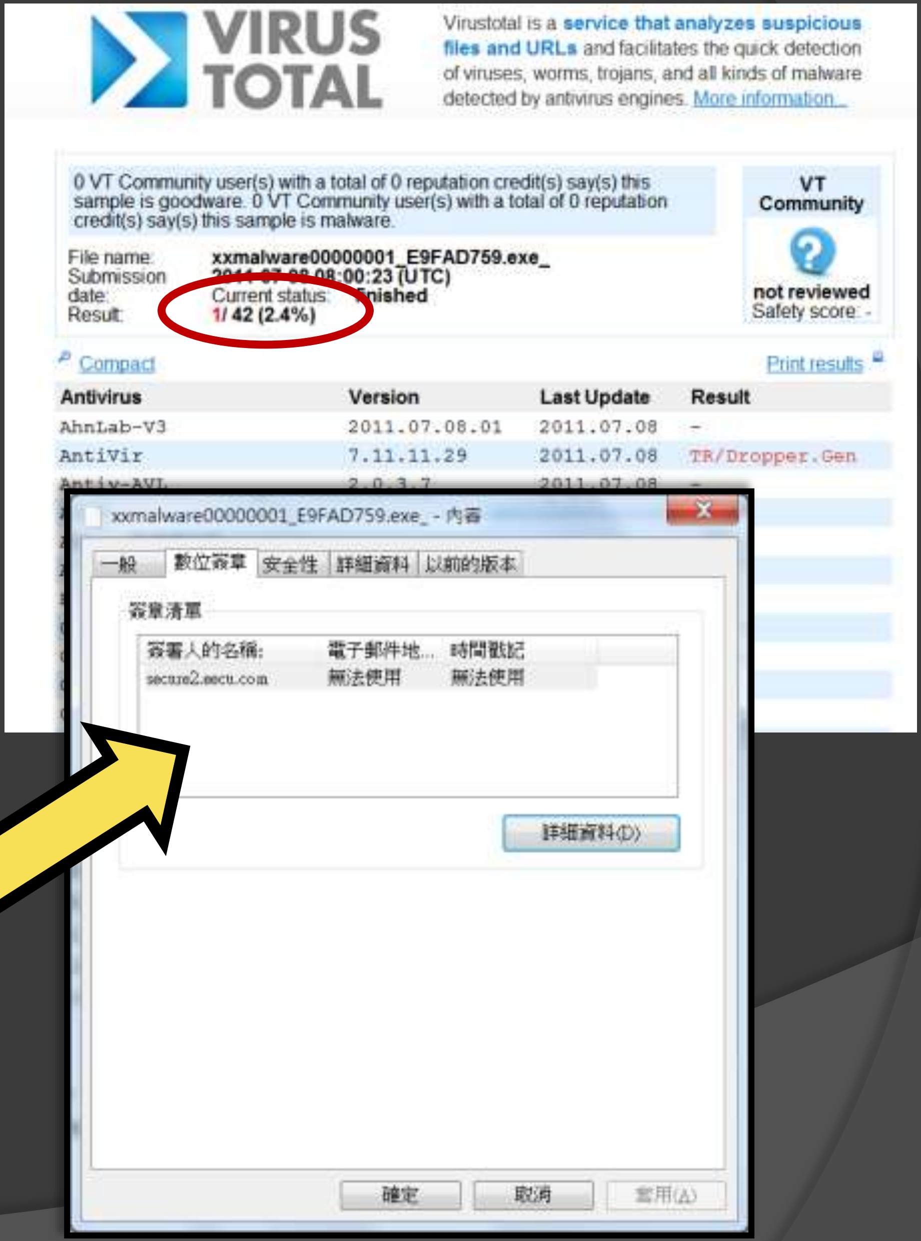
16% C&C IP located in Taiwan



Malware of Group E



Group-E
Language = Korean 🇰🇷



VIRUS TOTAL

Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: xxmalware00000001_E9FAD759.exe_
Submission date: 2011-07-08 08:00:23 (UTC)
Current status: finished
Result: 1/ 42 (2.4%)

VT Community
not reviewed
Safety score: -

Compact
Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.07.08.01	2011.07.08	-
AntiVir	7.11.11.29	2011.07.08	TR/Dropper.Gen
Antiy-AVL	2.0.3.7	2011.07.08	-

xxmalware00000001_E9FAD759.exe_ - 內容

簽章清單

簽署人的名稱:	電子郵件地...	時間戳記
secure2.secu.com	無法使用	無法使用

Findings from Mila Sample Set (1/2)

- Our analysis against Mila Sample set could identify 8 major APT taskforces.
- There are around 12 different CVEs and exploits are identified.
- We have found that even APT taskforce uses 8-9 different exploits, however, the type of malware used is limited to a few one. There is no surprise at all □
- We identify APT Taskforce based on CnC server location and malware they have used. The exploit the taskforce used is not very related to our analysis.

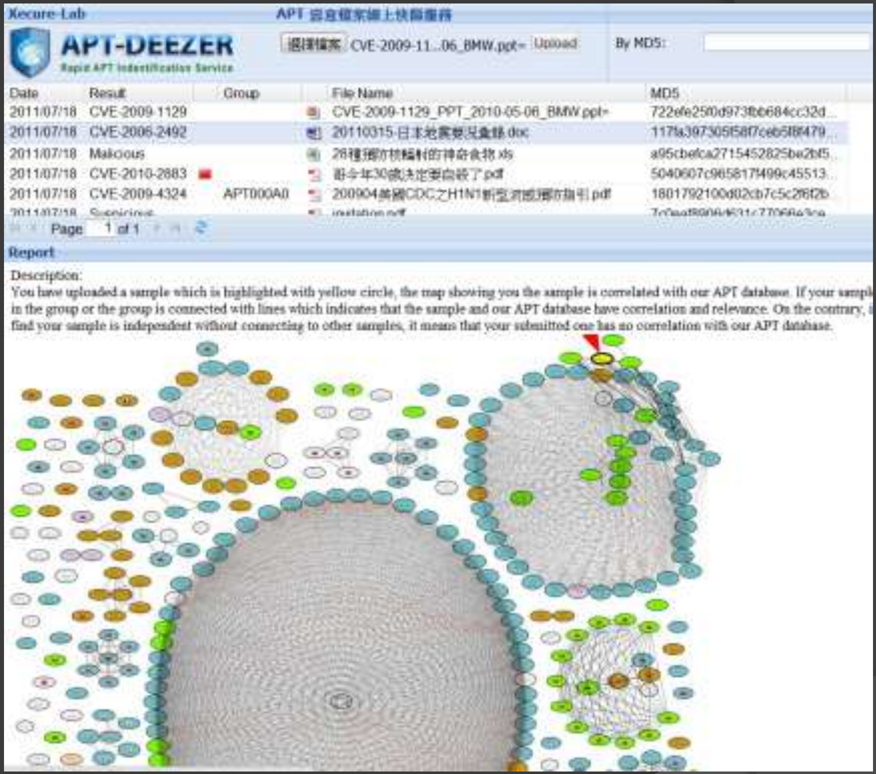
Findings from Mila Sample Set (2/2)

- Language used in APT sample：
  24% of the samples is from China 🇨🇳
- 3.9% of the samples is from Korean 🇰🇷 ，
- We also found some are from Russia 🇷🇺 and France 🇫🇷
- APT CnC server location Top 3 Ranking:
  - Taiwan (28%) 🇹🇼
  - US
  - Hong Kong (HK is readily another CnC heaven)

APT-DEEZER

Rapid APT Indentification Service

- APT-Deezer provides a free online service to check whether your submitted sample whether it is an APT sample
  - We took Mila sample set as the base training set
  - Identify Exploit CVE and Malware family
  - Zero-Day Exploit detection and analysis
  - APT Malware sample DNA analysis and comparison
  - APT sample clustering and grouping
  - Support file formats including DOC,PPT,XLS,PDF,RTF



Xecure-Lab APT 惡意檔案線上快篩服務

APT-DEEZER Rapid APT Indentification Service

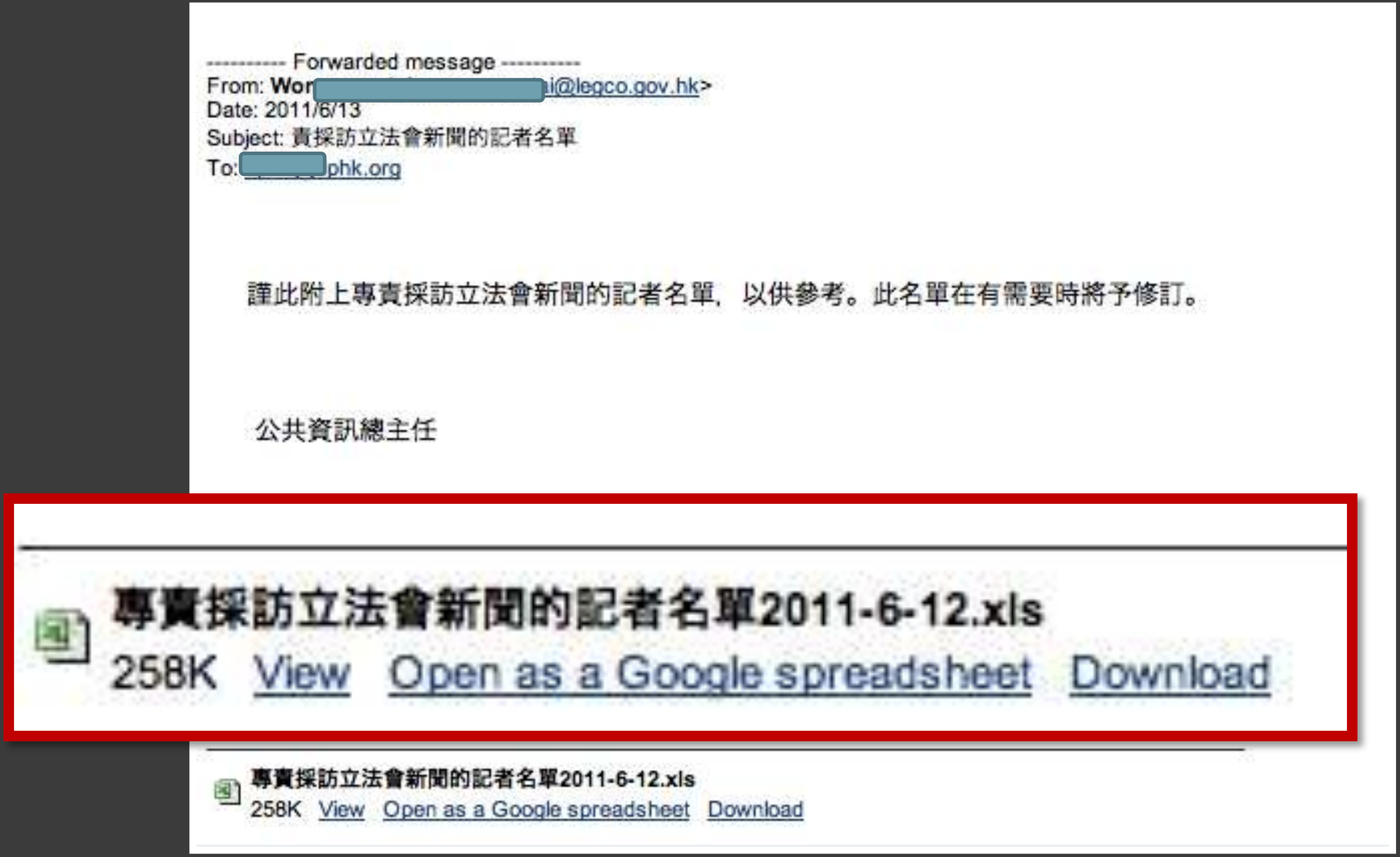
Date	Result	Group	File Name	MD5
2011/07/18	CVE-2009-1129		CVE-2009-1129_PPT_2010-05-06_BMW.ppt~	722efe250d973fbb684cc32d...
2011/07/18	CVE-2006-2492		20110315-日本地震狀況彙錄.doc	117fa397305f58f7ceb5f8479...
2011/07/18	Malicious		28種抵抗核輻射的神奇食物.xls	a95cbefca2715452825be2bf5...
2011/07/18	CVE-2010-2883		哥今年30歲決定要自殺了.pdf	5040607c965817f499c45513...
2011/07/18	CVE-2009-4324	APT000A0	200904美國CDC之H1N1新型流感擬防指引.pdf	1801792100d02cb7c5c2f6f2b
2011/07/18	Suspicious		invitation.pdf	7c0eaf8906d631c7706fa3ca

Report

Description:
You have uploaded a sample which is highlighted with yellow circle, the map showing you the sample is correlated with our APT database. If your sampl in the group or the group is connected with lines which indicates that the sample and our APT database have correlation and relevance. On the contrary, i find your sample is independent without connecting to other samples, it means that your submitted one has no correlation with our APT database.

- http://aptdeezer.xecure-lab.com

Case Study A(1/4), Hong Kong APT!



---------- Forwarded message ----------
From: **Wor**[redacted]i@legco.gov.hk>
Date: 2011/6/13
Subject: 責採訪立法會新聞的記者名單
To: [redacted]phk.org

謹此附上專責採訪立法會新聞的記者名單，以供參考。此名單在有需要時將予修訂。

公共資訊總主任

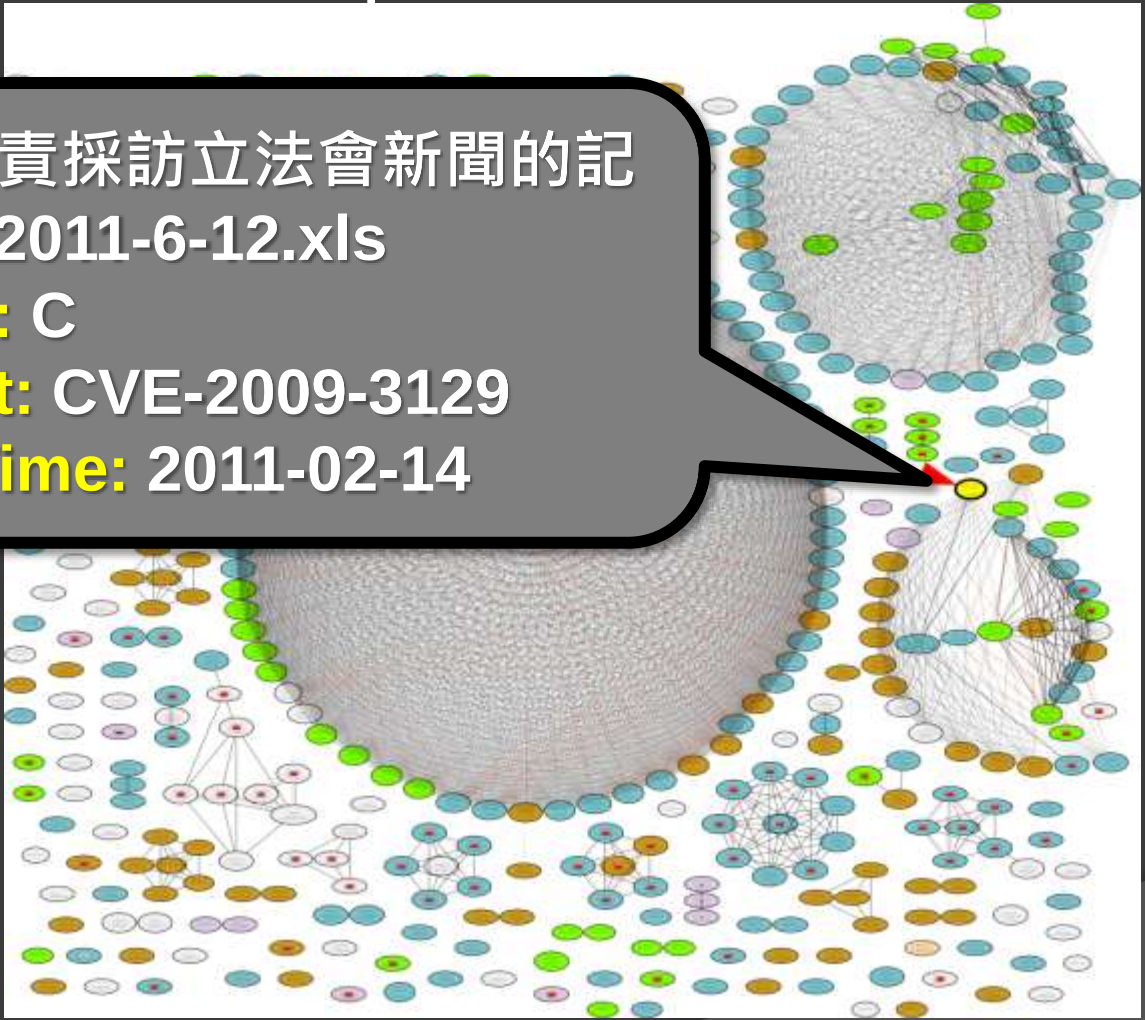
專責採訪立法會新聞的記者名單2011-6-12.xls
258K View Open as a Google spreadsheet Download

專責採訪立法會新聞的記者名單2011-6-12.xls
258K View Open as a Google spreadsheet Download

Case Study A(2/4), Hong Kong APT!

- Characteristics:
  1. A democratic party in HK2.
  2. Fake as a staff in LEGCO council
  3. Google cannot detect it
  4. The email is sent before 1 July

Case Study A(3/4), It is from Group-C



File:專責採訪立法會新聞的記者名單2011-6-12.xls

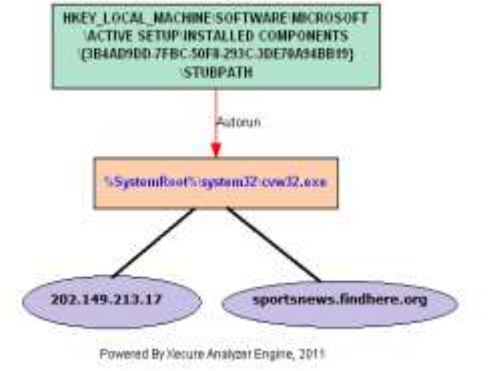
Group: C

Exploit: CVE-2009-3129

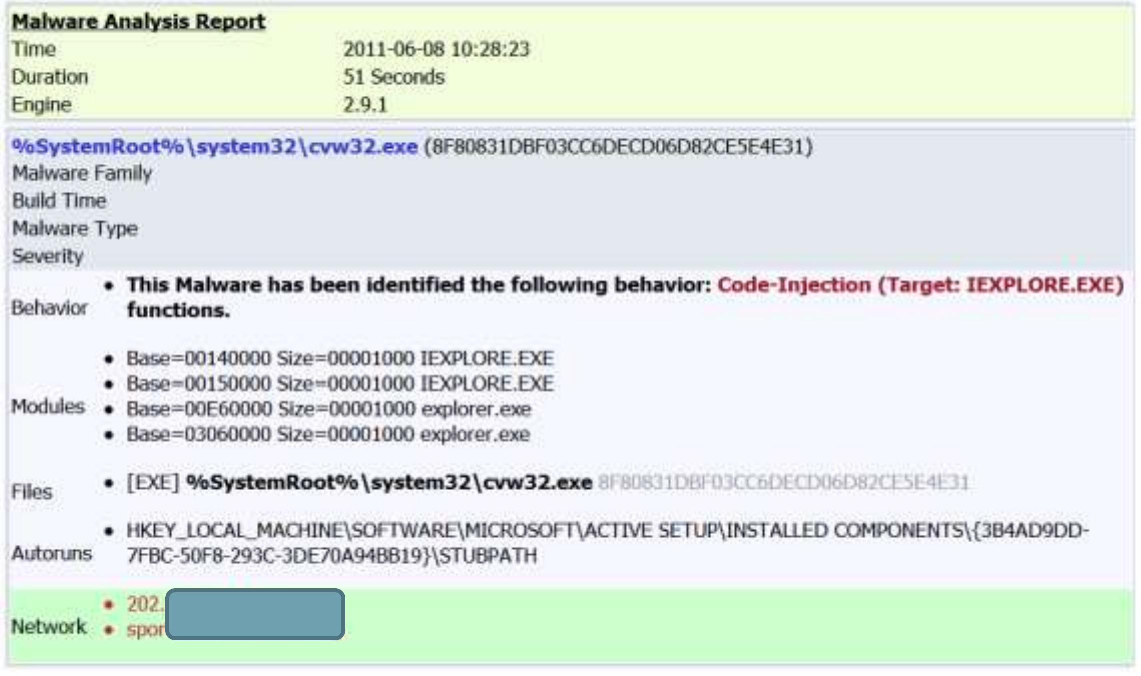
BuildTime: 2011-02-14

Case Study A(4/4),
Malware of APT Group C

Malware Attack Graph


HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ACTIVE SETUP\INSTALLED COMPONENTS\{3B4AD9DD-7FBC-50F8-293C-3DE70A94BB19}\STUBPATH
Autorun
%SystemRoot%\system32\cvw32.exe
202.149.213.17
sportsnews.findhere.org
Powered By Xecure Analyzer Engine, 2011

Malware Fix Suggestion



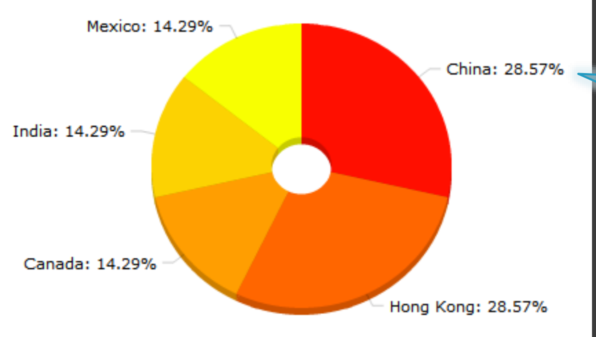
Malware Analysis Report

Time	2011-06-08 10:28:23
Duration	51 Seconds
Engine	2.9.1

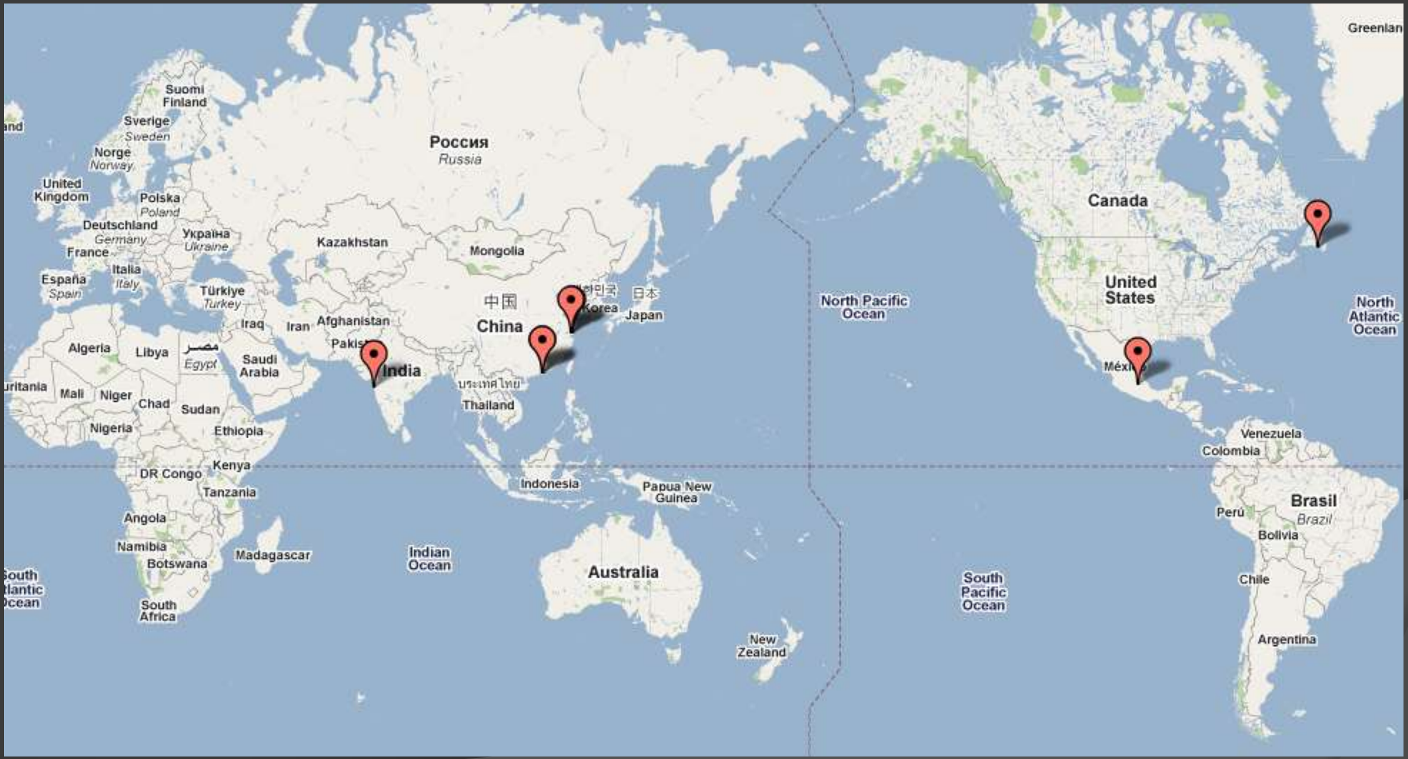
%SystemRoot%\system32\cvw32.exe (8F80831DBF03CC6DECD06D82CE5E4E31)

Malware Family	
Build Time	
Malware Type	
Severity	
Behavior	• **This Malware has been identified the following behavior: Code-Injection (Target: IEXPLORE.EXE) functions.**
Modules	• Base=00140000 Size=00001000 IEXPLORE.EXE • Base=00150000 Size=00001000 IEXPLORE.EXE • Base=00E60000 Size=00001000 explorer.exe • Base=03060000 Size=00001000 explorer.exe
Files	• [EXE] **%SystemRoot%\system32\cvw32.exe** 8F80831DBF03CC6DECD06D82CE5E4E31
Autoruns	• HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ACTIVE SETUP\INSTALLED COMPONENTS\{3B4AD9DD-7FBC-50F8-293C-3DE70A94BB19}\STUBPATH
Network	• 202.[redacted] • spor

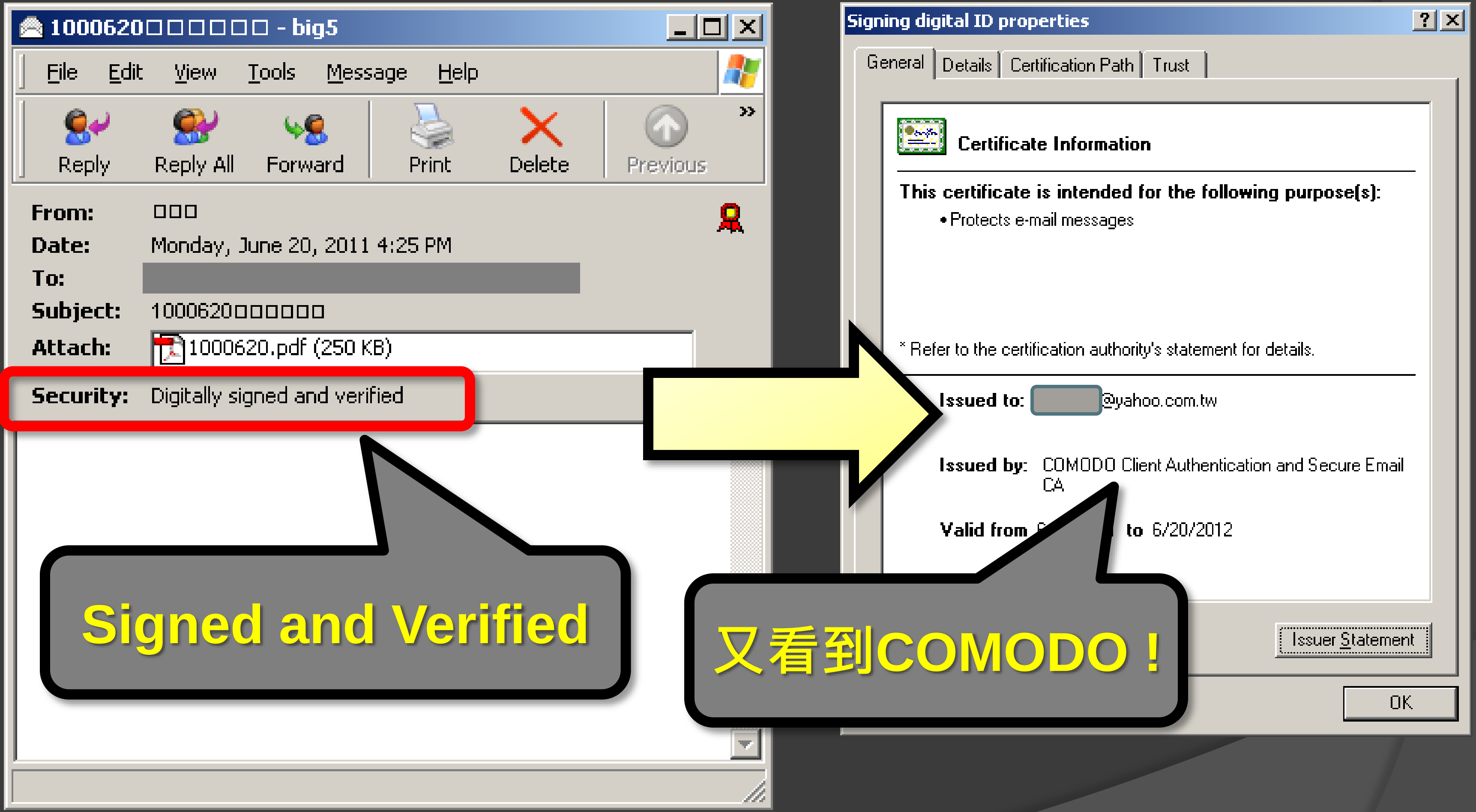
C&C Location of APT Group C



28.5% C&C IP located in China



Case Study (1/4)
Target Attack Mail has been signed !?



1000620□□□□□□□ - big5
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous

From: □□□

Date: Monday, June 20, 2011 4:25 PM

To: [redacted]

Subject: 1000620□□□□□□□

Attach: 1000620.pdf (250 KB)

Security: Digitally signed and verified

Signed and Verified

Signing digital ID properties
General Details Certification Path Trust

Certificate Information

This certificate is intended for the following purpose(s):

- Protects e-mail messages

* Refer to the certification authority's statement for details.

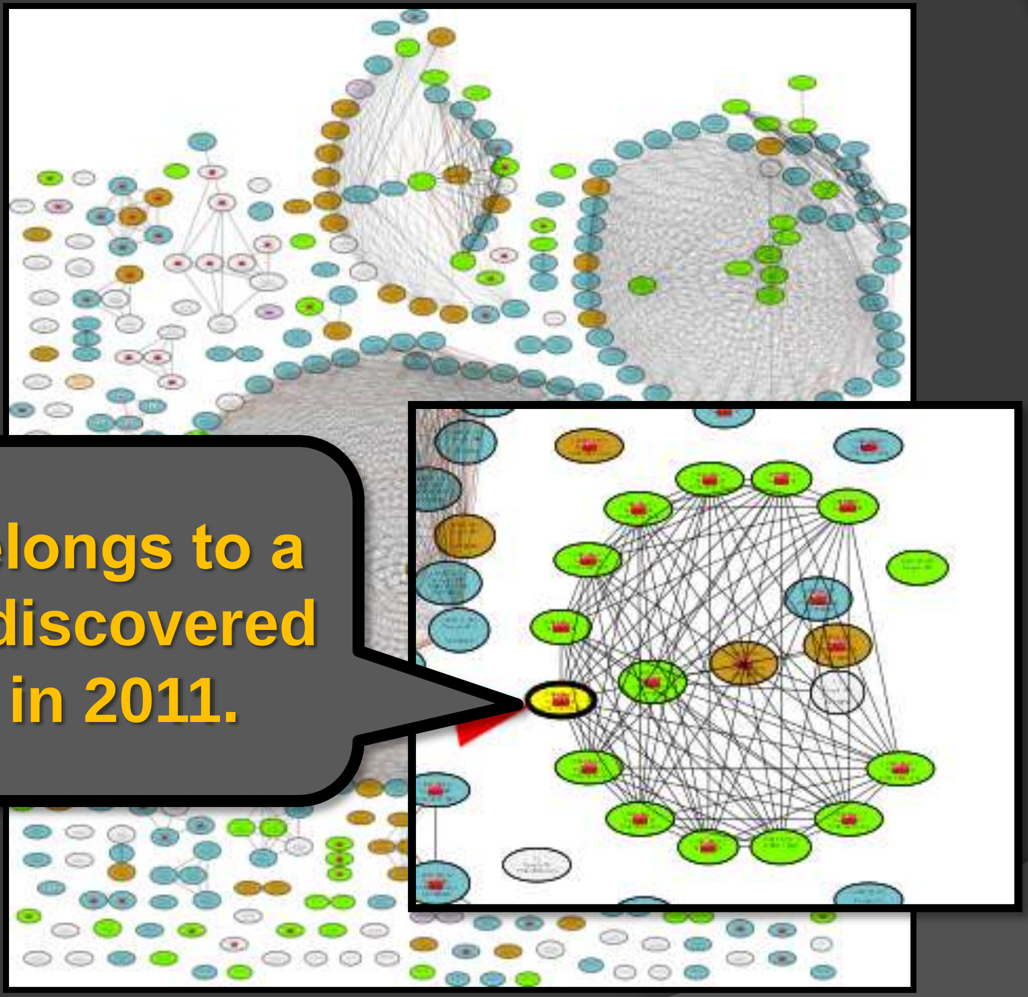
Issued to: [redacted]@yahoo.com.tw

Issued by: COMODO Client Authentication and Secure Email CA

Valid from 6/ **to** 6/20/2012

又看到COMODO！

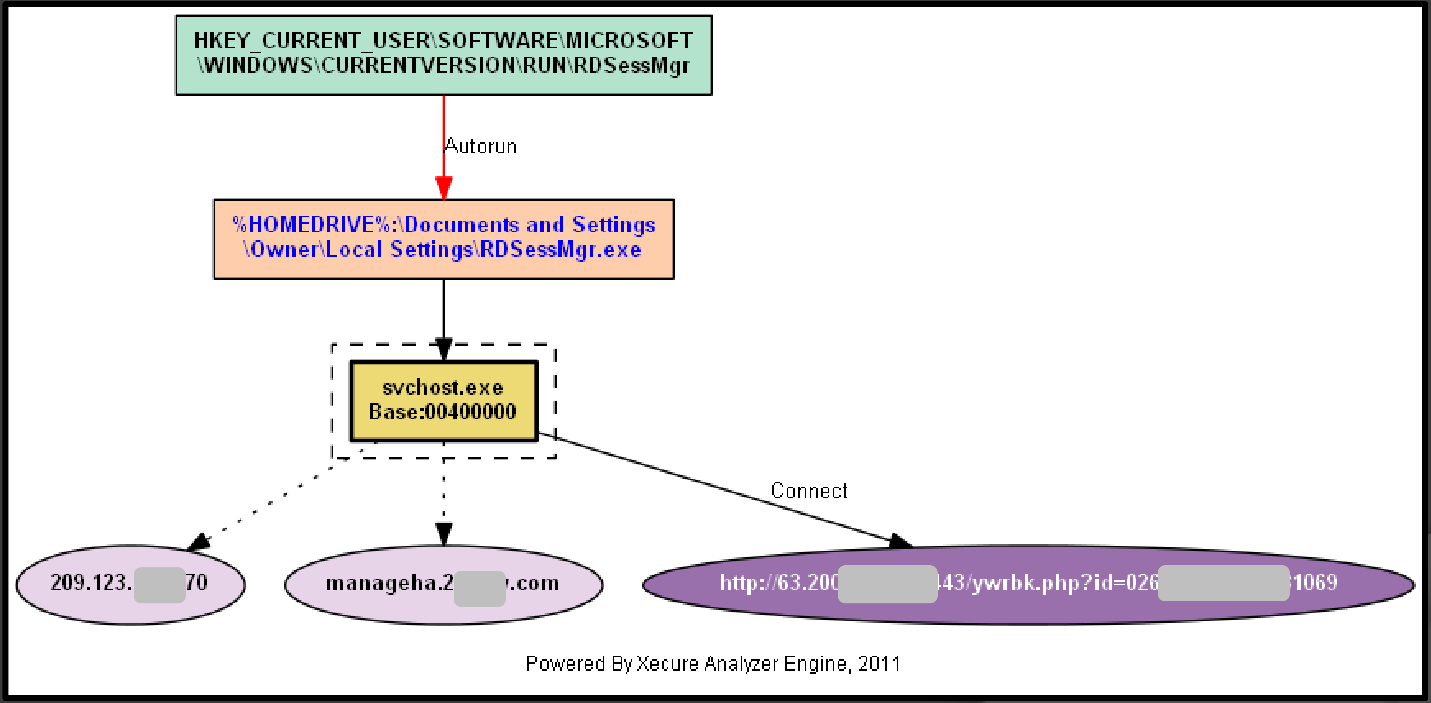
(2/4) Identify the APT Taskforce Group



‘100620.pdf’ belongs to a known, newly discovered APT Taskforce in 2011.

(3/4)

- But Malware is a known family, it is same as APT-Group-B !


HKEY_CURRENT_USER\SOFTWARE\MICROSOFT
\WINDOWS\CURRENTVERSION\RUN\RDSessMgr
Autorun
%HOMEDRIVE%:\Documents and Settings
\Owner\Local Settings\RDSessMgr.exe
svchost.exe
Base:00400000
Connect
209.123.[redacted]70
manageha.2[redacted].com
http://63.20[redacted]43/ywrbk.php?id=026[redacted]1069

Powered By Xecure Analyzer Engine, 2011

新一代的資安策略 - 情資導向的防護思維

- **正視威脅，謀定而後動**
  - 先進國家已將 APT 防護議題拉高至國家層級，而非視為個資外洩等民生議題。
- **工欲善其事，必先利其器**
  - 資安防護產業也正面臨挑戰，APT時代的來臨可能意味著，將會越來越多針對性的 Malware，難以利用蜜罐（honeypot）和蜜網（honeynet）誘捕到APT樣本，因為僅有特定人士會收到這些天上掉下來的禮物。
- **正兵當敵，奇兵致勝**
  - 如果是以不變應萬變，那遲早有被攻破的一天！防守方務必也要持續收集與分析戰情，才能知彼知己，百戰百勝。
  - 分析一系列的攻擊活動並歸納奧義，才有辦法歸納出攻擊行動的組織、活動甚至計劃。
- **安全基準，最佳實務**
  - 落實執行資安政策，實體隔離，公務公辦，嚴禁USB隨身碟任意插拔等基本要求都已推行多年。

總結

- APT有組織有計劃的網路間諜活動，特別針對高價值目標如政治,經濟,高科技與軍事。雖然是個新的熱門名詞，但是卻存在已久。

- APT以目標式攻擊的惡意郵件為主要活動，其中使用各種 Zero-Day Exploit，與專門開發的 RAT，傳統資安設備無法自動偵測與防禦APT惡意郵件攻擊。

- 要有正確的資安關念，才不會有錯誤的政策。APT惡意郵件不能只是作一般病毒信件處理而敷衍過去，攻擊事件將一再發生。

- 唯有透過大量且跨區域的APT樣本分析才能觀察到攻擊全貌。目前觀察到香港，台灣與美國的APT樣本有很高的相關性。

- 分析各國APT樣本來看 APT活動前三大地區就占了超過一半比例，台灣、美國與香港，其中台灣最高約 28% 。綜觀來看，亞洲是APT最主要活動的地區。

Any Feedbacks? Let us know! ;-)

- Xecure Lab (http://www.xecure-lab.com)
- We keep collecting samples for analysis
- Enhance the capability to analyze APT DNA family in more accurate manner.
- Together, we make homeland secured.