Hunting the Shadows:
In Depth Analysis of Escalated APT Attacks

Fyodor Yarochkin, Academia Sinica
Pei Kan PK Tsung, Academia Sinica
Ming-Chang Jeremy Chiu, Xecure Lab
Ming-Wei Benson Wu, Xecure Lab

Agenda

- Why Taiwan?
- The “Lstudio” player… fun ☺
- Taking a peek at Weaponry
- APT in a Cloud
- Victimology or … chicken-logy?

whoweare

@bensonwu

[secret]

@fygrave

[censored]

Based in Taiwan
Interests in Computer Forensics
Access to some raw network traffic data (fun!)
Get to fish interesting things (PROFFFIIITT!)

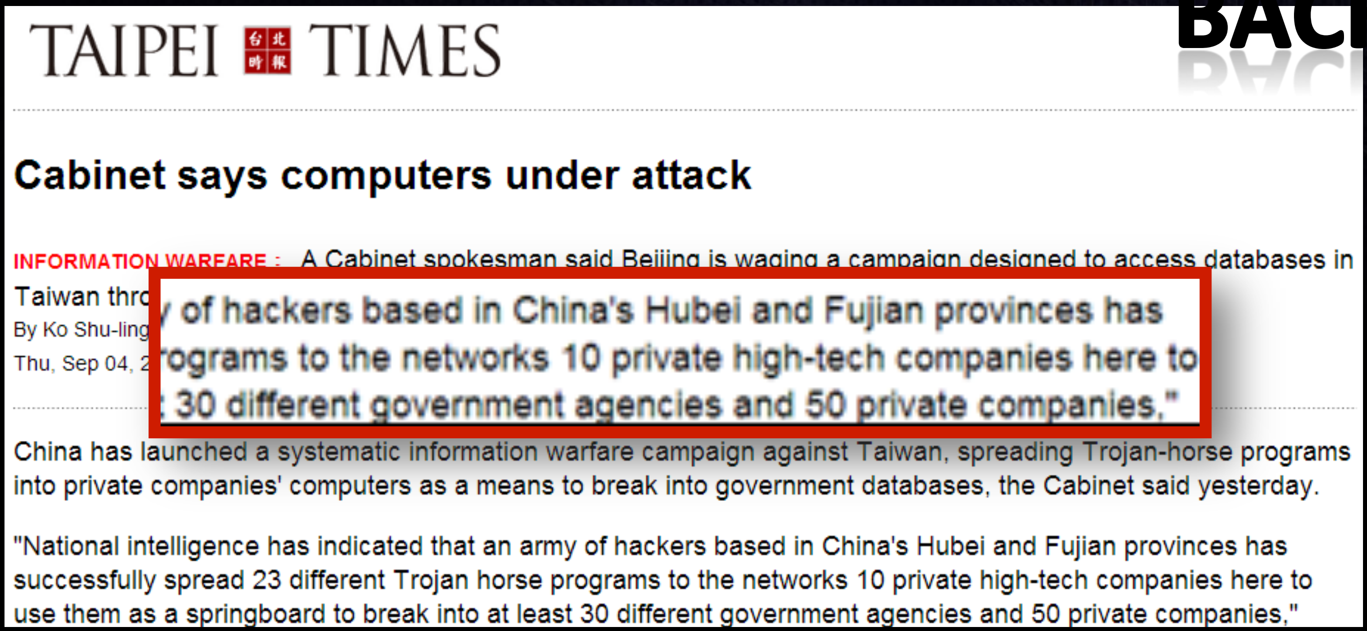
Disclaimer

A few words before we move on.

- With this research we are primarily interested in understanding the Ops and victims of discussed targeted attacks. We DO NOT attempt to perform any attribution of potential attackers.

Taiwan has been a frontline of APT battlefield for some time

BACK



TAIPEI 台北時報 TIMES

Cabinet says computers under attack

INFORMATION WARFARE : A Cabinet spokesman said Beijing is waging a campaign designed to access databases in Taiwan thro

By Ko Shu-ling

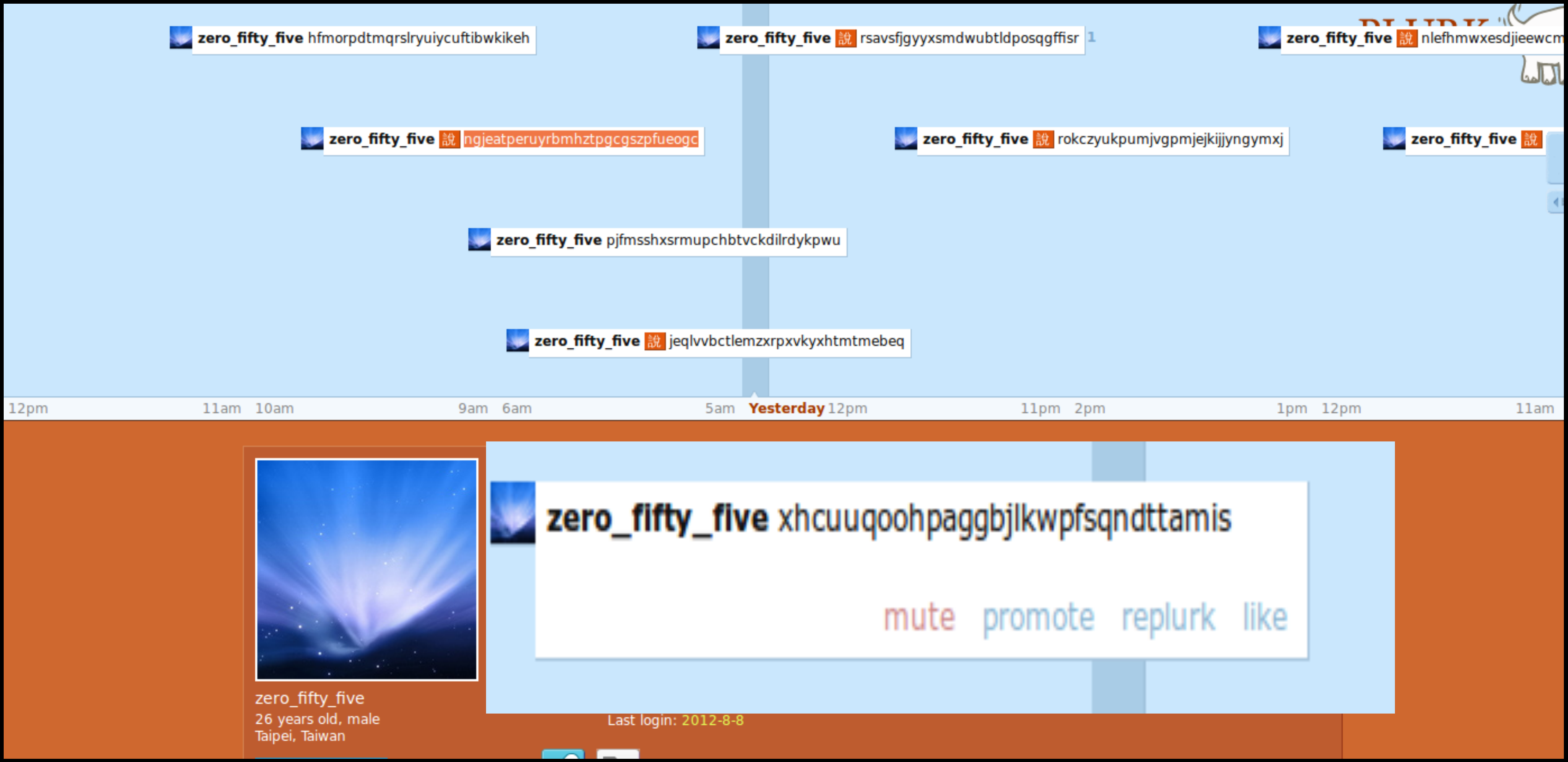
Thu, Sep 04, 2

y of hackers based in China's Hubei and Fujian provinces has
rograms to the networks 10 private high-tech companies here to
30 different government agencies and 50 private companies."

China has launched a systematic information warfare campaign against Taiwan, spreading Trojan-horse programs into private companies' computers as a means to break into government databases, the Cabinet said yesterday.

"National intelligence has indicated that an army of hackers based in China's Hubei and Fujian provinces has successfully spread 23 different Trojan horse programs to the networks 10 private high-tech companies here to use them as a springboard to break into at least 30 different government agencies and 50 private companies."

Many interesting things could be observed (though this is not “Lstudio” group)



zero_fifty_five hfmorpdtmqrslryuiycuftibwkikeh

zero_fifty_five 說 rsavsfjgyyxsmdwubtldposqgffisr 1

zero_fifty_five 說 nlefhmwxesdjieewcm

zero_fifty_five 說 ngjeatperuyrbmhztpgcgszpfueogc

zero_fifty_five 說 rokczyukpumjvgpmjejkijjyngymxj

zero_fifty_five 說

zero_fifty_five pjfmsshxsrmupchbtvckdilrdykpwu

zero_fifty_five 說 jeqlvvbctlemzxrpxvkyxhtmtmebeq

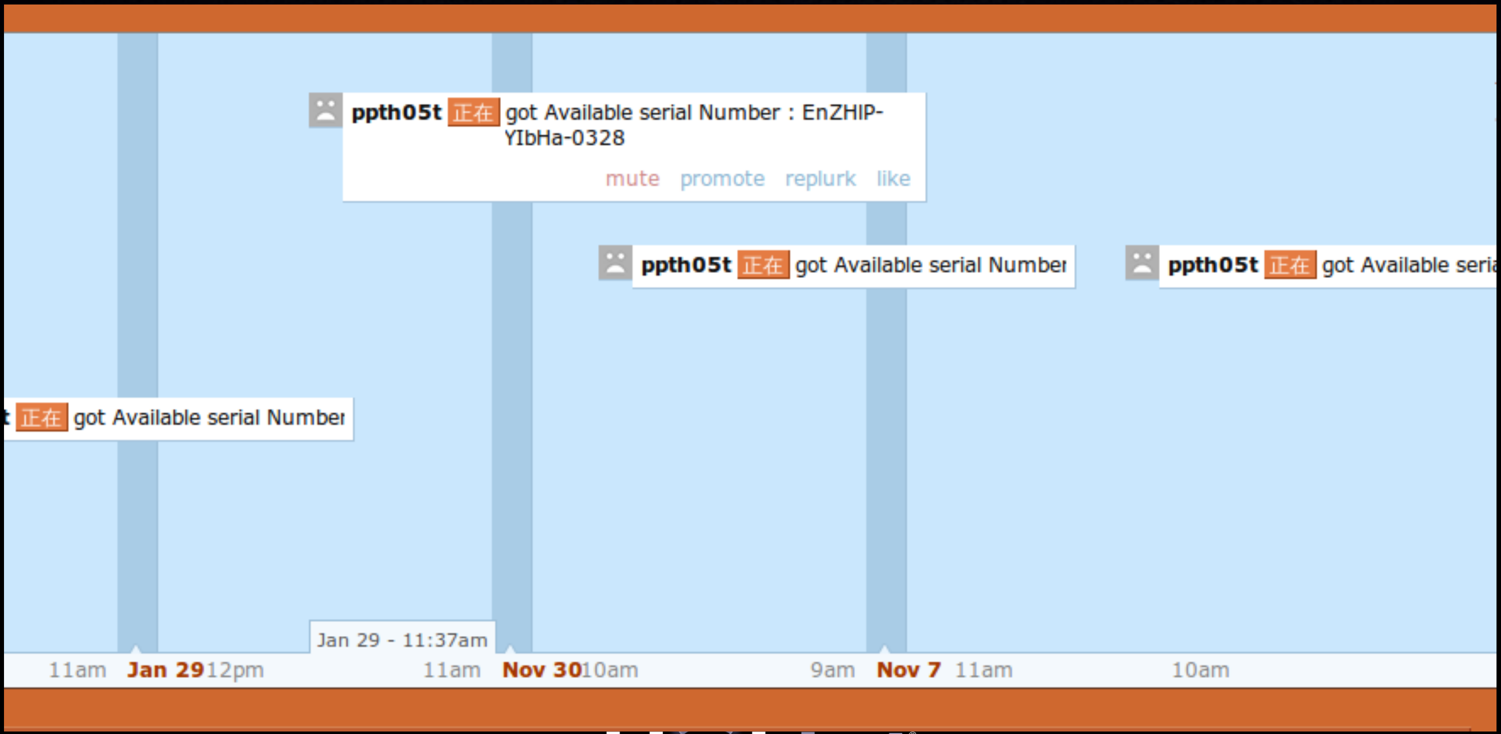
zero_fifty_five xhcuuqoohpaggbjlkwpfsqndttamis

zero_fifty_five
26 years old, male
Taipei, Taiwan

Last login: 2012-8-8

Elirks: earlier campaign

Reported by Dell/Secureworks as Elirks http://www.secureworks.com/cyber-threat-intelligence/threats/chasing_apt/



ppth05t 正在 got Available serial Number : EnZHIP-YIbHa-0328

ppth05t 正在 got Available serial Number

ppth05t 正在 got Available seria

t 正在 got Available serial Number

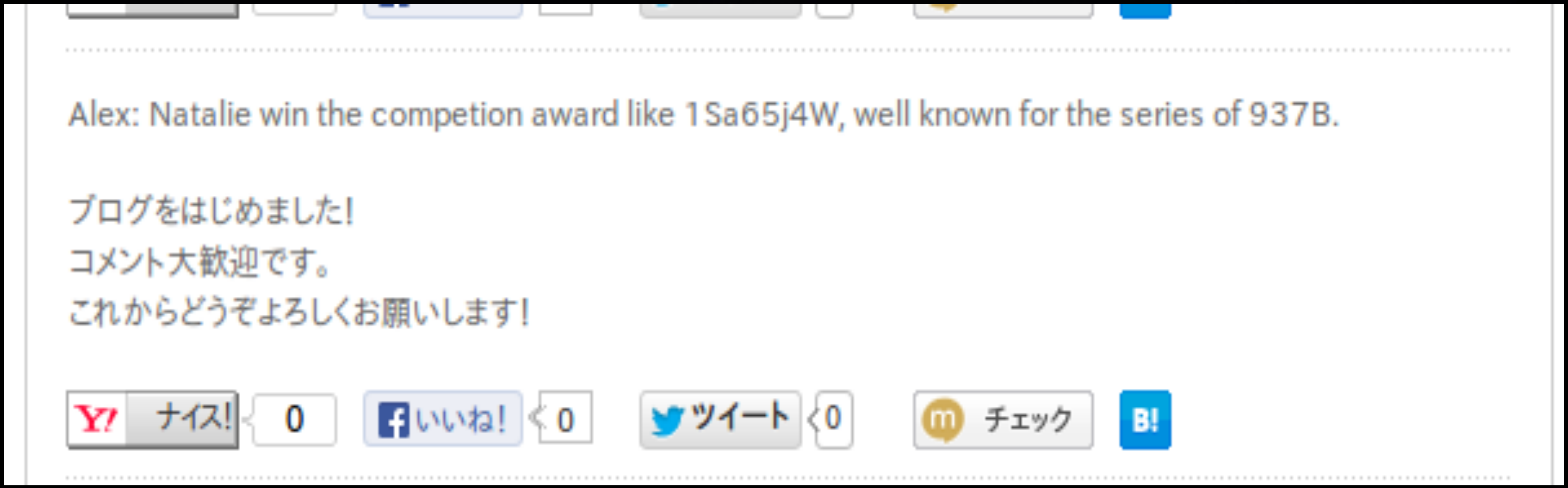
Elirks evolution

http://tw.myblog.yahoo.com/jw!uzrxZwSGHxowPMGZAaj4I5

http://blog.yam.com/minzhu0906/article/54726977

http://diary.blog.yam.com/bigtree20130514/article/10173342

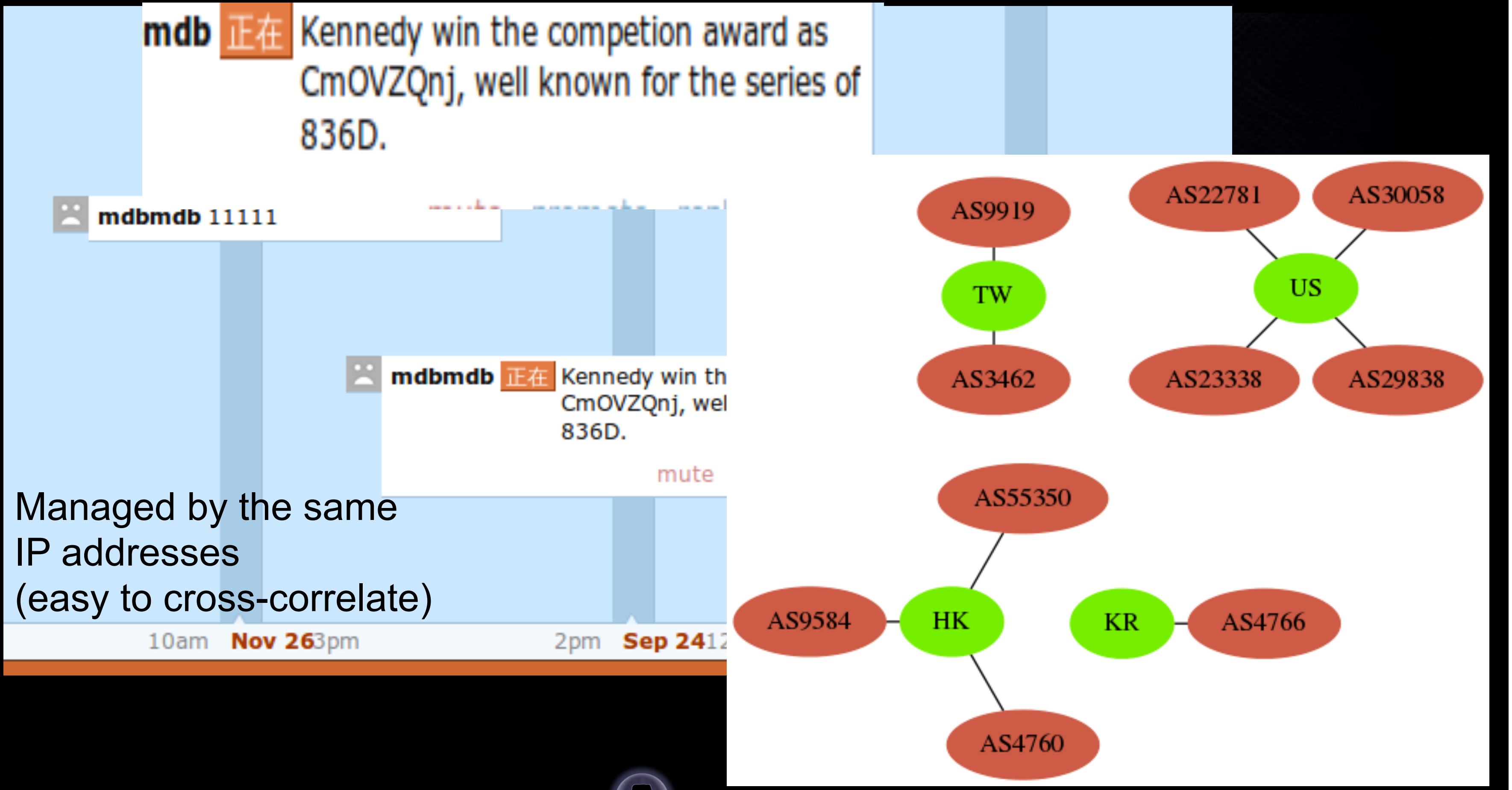
http://tw.myblog.yahoo.com/jw!



Alex: Natalie win the competion award like 1Sa65j4W, well known for the series of 937B.

ブログをはじめました!
コメント大歓迎です。
これからどうぞよろしくお願いします!

Elirks 2.0 – silly to reuse the address-space



mdb 正在 Kennedy win the competion award as CmOVZQnj, well known for the series of 836D.

mdbmdb 11111

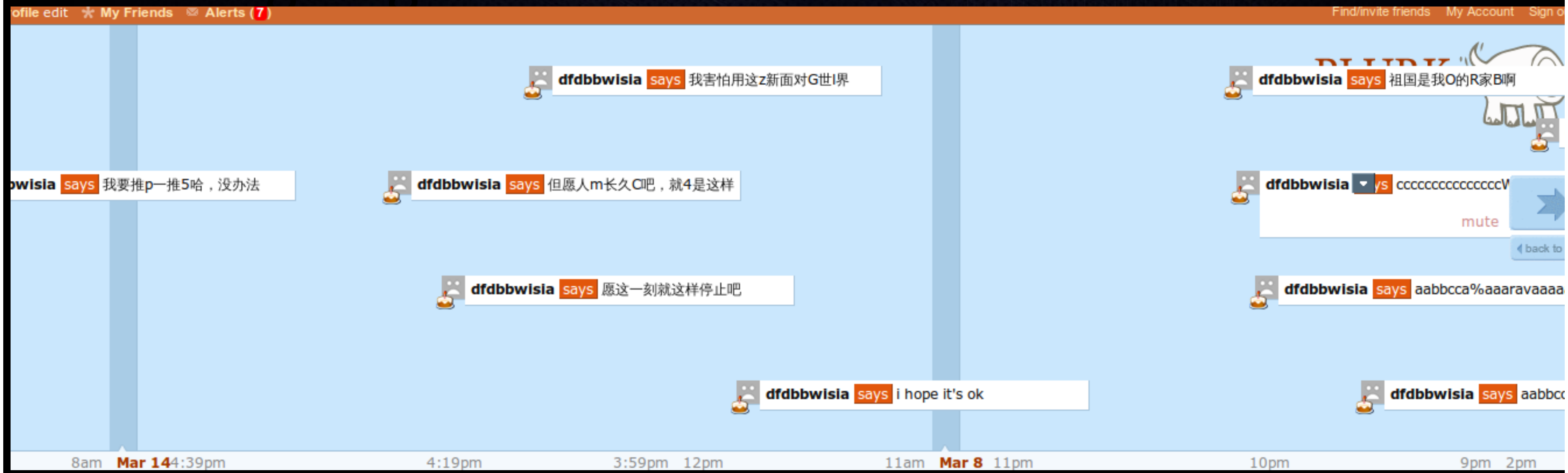
mdbmdb 正在 Kennedy win th CmOVZQnj, wel 836D.

mute

10am Nov 26 3pm 2pm Sep 24 12

Managed by the same IP addresses (easy to cross-correlate)

Another on-going Campaign



dfdbbwisia says 我害怕用这z新面对G世l界

wisia says 我要推p一推5哈，没办法

dfdbbwisia says 但愿人m长久C吧，就4是这样

dfdbbwisia says 愿这一刻就这样停止吧

dfdbbwisia says i hope it's ok

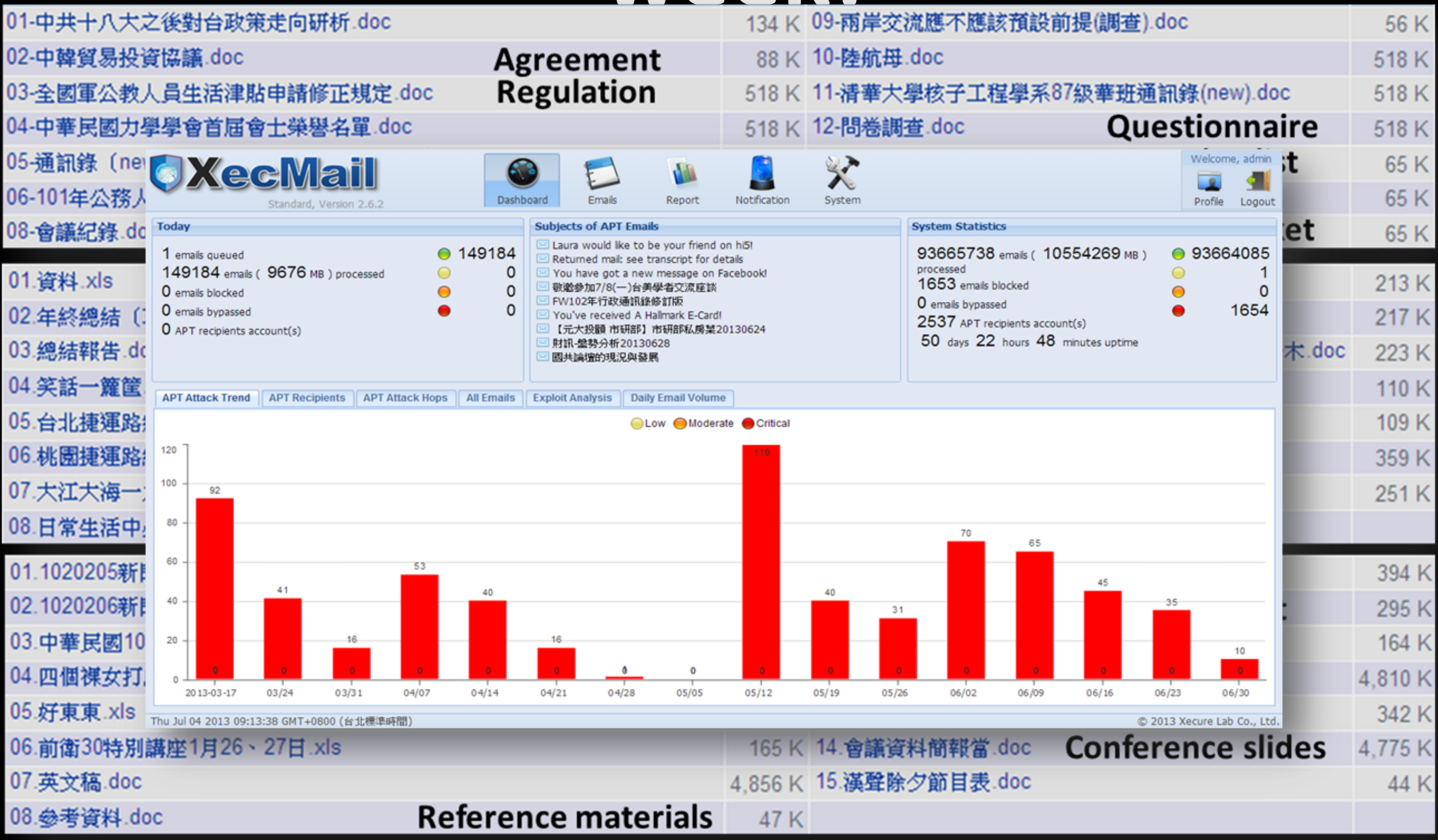
dfdbbwisia says 祖国是我O的R家B啊

dfdbbwisia ys cccccccccccccW

dfdbbwisia says aabbcca%aaaravaaaa

dfdbbwisia says aabbc

On average, 48 APT emails a week!



01-中共十八大之後對台政策走向研析.doc 134 K
02-中韓貿易投資協議.doc 88 K
03-全國軍公教人員生活津貼申請修正規定.doc 518 K
04-中華民國力學學會首屆會士榮譽名單.doc 518 K
05-通訊錄（ne
06-101年公務人
08-會議紀錄.do

Agreement
Regulation

09-兩岸交流應不應該預設前提(調查).doc 56 K
10-陸航母.doc 518 K
11-清華大學核子工程學系87級華班通訊錄(new).doc 518 K
12-問卷調查.doc 518 K
65 K
65 K
65 K

Questionnaire

st

et

01.資料.xls
02.年終總結（
03.總結報告.do
04.笑話一籮筐
05.台北捷運路
06.桃園捷運路
07.大江大海一
08.日常生活中

木.doc

213 K
217 K
223 K
110 K
109 K
359 K
251 K

01.1020205新
02.1020206新
03.中華民國10
04.四個裸女打
05.好東東.xls
06.前衛30特別講座1月26、27日.xls 165 K
07.英文稿.doc 4,856 K
08.參考資料.doc 47 K

Reference materials

394 K
295 K
164 K
4,810 K
342 K
14.會議資料簡報當.doc 4,775 K
15.漢聲除夕節目表.doc 44 K

Conference slides

XecMail
Standard, Version 2.6.2

Welcome, admin

Today

1 emails queued
149184 emails (9676 MB) processed
0 emails blocked
0 emails bypassed
0 APT recipients account(s)

● 149184
● 0
● 0
● 0

Subjects of APT Emails

- Laura would like to be your friend on hi5!
- Returned mail: see transcript for details
- You have got a new message on Facebook!
- 敬邀參加7/8(一)台美學者交流座談
- FW102年行政通訊錄修訂版
- You've received A Hallmark E-Card!
- 【元大投顧 市研部】市研部私房菜20130624
- 財訊-盤勢分析20130628
- 國共論壇的現況與發展

System Statistics

93665738 emails (10554269 MB) processed
1653 emails blocked
0 emails bypassed
2537 APT recipients account(s)
50 days 22 hours 48 minutes uptime

● 93664085
● 1
● 0
● 1654

Thu Jul 04 2013 09:13:38 GMT+0800 (台北標準時間)

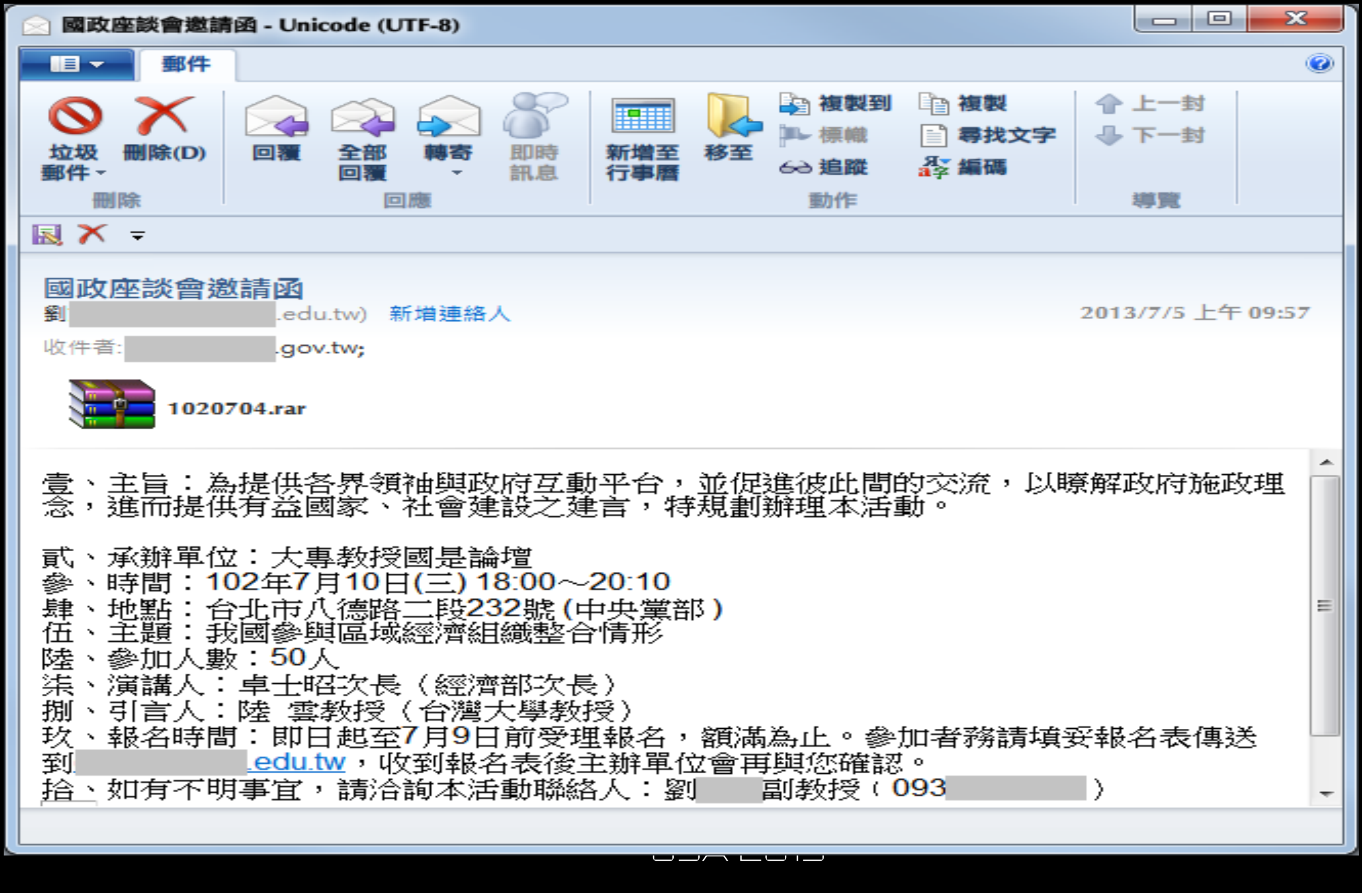
© 2013 Xecure Lab Co., Ltd.

The “Lstudio” group:

Exploring fun things in a greater detail :)

隨裕而安
http://yuann.myphotos.cc/

They start with a boring spearphhiissh



國政座談會邀請函

劉[redacted].edu.tw) 新增連絡人　2013/7/5 上午 09:57

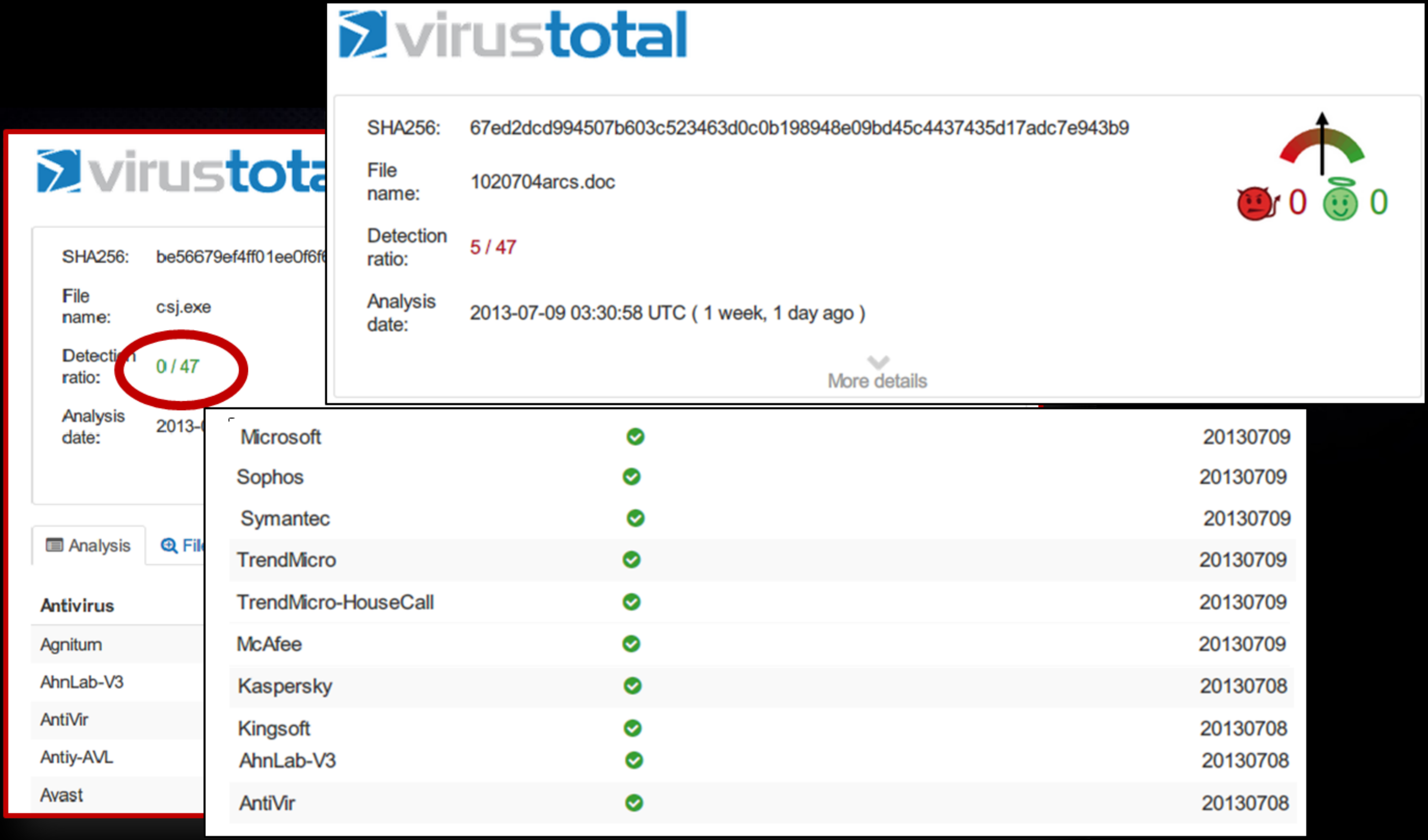
收件者: [redacted].gov.tw;

1020704.rar

壹、主旨：為提供各界領袖與政府互動平台，並促進彼此間的交流，以瞭解政府施政理念，進而提供有益國家、社會建設之建言，特規劃辦理本活動。

貳、承辦單位：大專教授國是論壇
參、時間：102年7月10日(三) 18:00～20:10
肆、地點：台北市八德路二段232號 (中央黨部)
伍、主題：我國參與區域經濟組織整合情形
陸、參加人數：50人
柒、演講人：卓士昭次長（經濟部次長）
捌、引言人：陸　雲教授（台灣大學教授）
玖、報名時間：即日起至7月9日前受理報名，額滿為止。參加者務請填妥報名表傳送到[redacted].edu.tw，收到報名表後主辦單位會再與您確認。
拾、如有不明事宜，請洽詢本活動聯絡人：劉[redacted]副教授（093[redacted]）

Almost clean :)



virustotal

SHA256: be56679ef4ff01ee0f6f

File name: csj.exe

Detection ratio: 0 / 47

Analysis date: 2013-

Analysis | Fil

Antivirus
Agnitum
AhnLab-V3
AntiVir
Antiy-AVL
Avast

virustotal

SHA256: 67ed2dcd994507b603c523463d0c0b198948e09bd45c4437435d17adc7e943b9

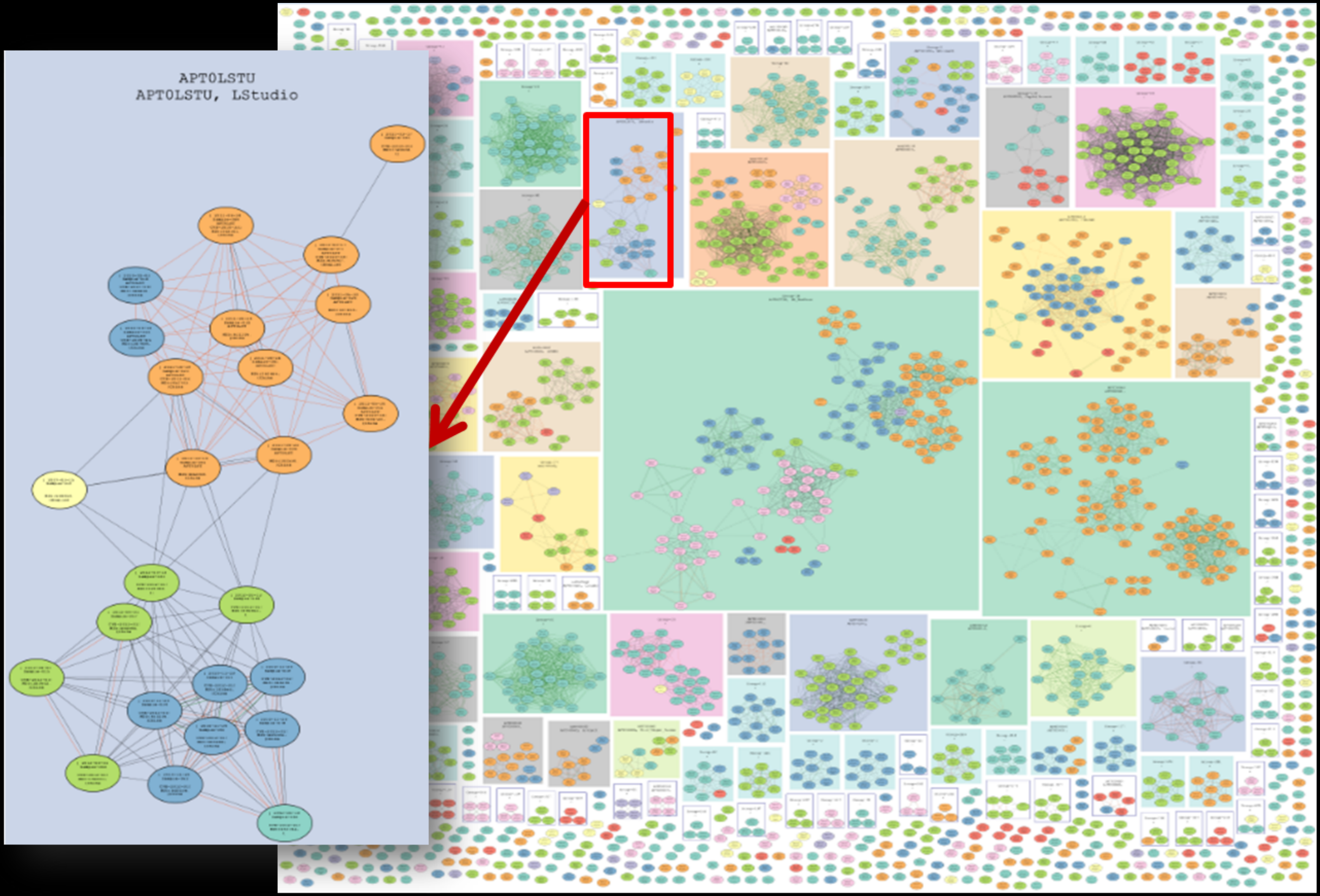
File name: 1020704arcs.doc

Detection ratio: 5 / 47

Analysis date: 2013-07-09 03:30:58 UTC (1 week, 1 day ago)

Microsoft	✓	20130709
Sophos	✓	20130709
Symantec	✓	20130709
TrendMicro	✓	20130709
TrendMicro-HouseCall	✓	20130709
McAfee	✓	20130709
Kaspersky	✓	20130708
Kingsoft	✓	20130708
AhnLab-V3	✓	20130708
AntiVir	✓	20130708

The APT Landscape in Taiwan



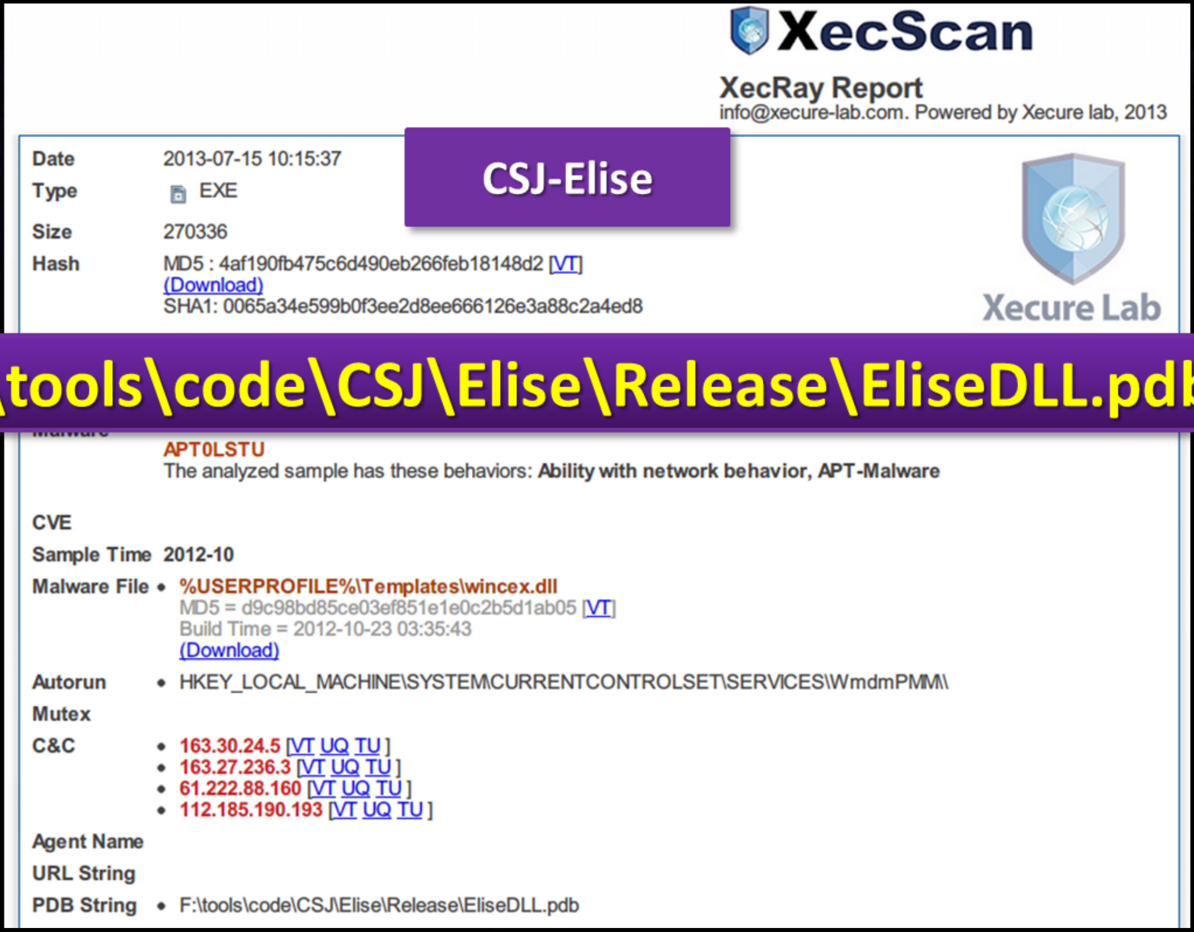
We’ll examine the “LStudio” group today

- Unique indicators of the “LStudio” group:
  - Debug symbols (.pdb)
  - “horse” label and generator tag

- Some curious discoveries from the “Lstudio” backend data center … ;-)

LStudio binaries have cute things

http://scan.xecure-lab.com



XecScan

XecRay Report
info@xecure-lab.com. Powered by Xecure lab, 2013

Xecure Lab

CSJ-Elise

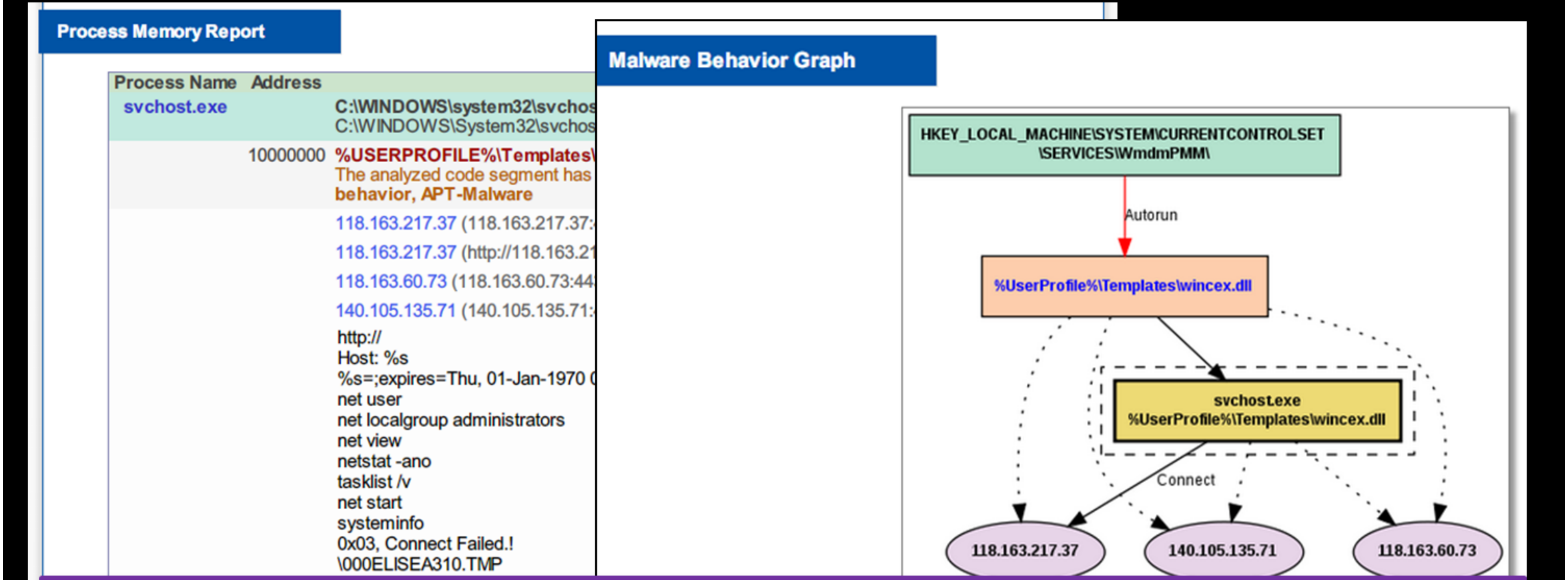
Date 2013-07-15 10:15:37
Type EXE
Size 270336
Hash MD5 : 4af190fb475c6d490eb266feb18148d2 [VT]
(Download)
SHA1: 0065a34e599b0f3ee2d8ee666126e3a88c2a4ed8

f:\tools\code\CSJ\Elise\Release\EliseDLL.pdb

Malware APT0LSTU
The analyzed sample has these behaviors: **Ability with network behavior, APT-Malware**

CVE
Sample Time 2012-10
Malware File • %USERPROFILE%\Templates\wincex.dll
MD5 = d9c98bd85ce03ef851e1e0c2b5d1ab05 [VT]
Build Time = 2012-10-23 03:35:43
(Download)
Autorun • HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\WmdmPMM\
Mutex
C&C • 163.30.24.5 [VT UQ TU]
• 163.27.236.3 [VT UQ TU]
• 61.222.88.160 [VT UQ TU]
• 112.185.190.193 [VT UQ TU]
Agent Name
URL String
PDB String • F:\tools\code\CSJ\Elise\Release\EliseDLL.pdb

CSJ-Elise ..



Process Memory Report

Process Name	Address	
svchost.exe		C:\WINDOWS\system32\svchos C:\WINDOWS\System32\svchos
	10000000	%USERPROFILE%\Templates\ The analyzed code segment has behavior, APT-Malware
		118.163.217.37 (118.163.217.37: 118.163.217.37 (http://118.163.21 118.163.60.73 (118.163.60.73:44 140.105.135.71 (140.105.135.71:
		http:// Host: %s %s=;expires=Thu, 01-Jan-1970 (net user net localgroup administrators net view netstat -ano tasklist /v net start systeminfo 0x03, Connect Failed.! \000ELISEA310.TMP

Malware Behavior Graph

HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET \SERVICES\WmdmPMM\

Autorun

%UserProfile%\Templates\wincex.dll

svchost.exe %UserProfile%\Templates\wincex.dll

Connect

118.163.217.37

140.105.135.71

118.163.60.73

TAABAMoGvBjTVXHUHaibnwrAWfchx2x17Rf2roRBnbD/9lu13lWnlAUbBgqw+YNld2vcV5krtXoG__FXI43BxueF4FChFrk
SRgNVP2WQ==

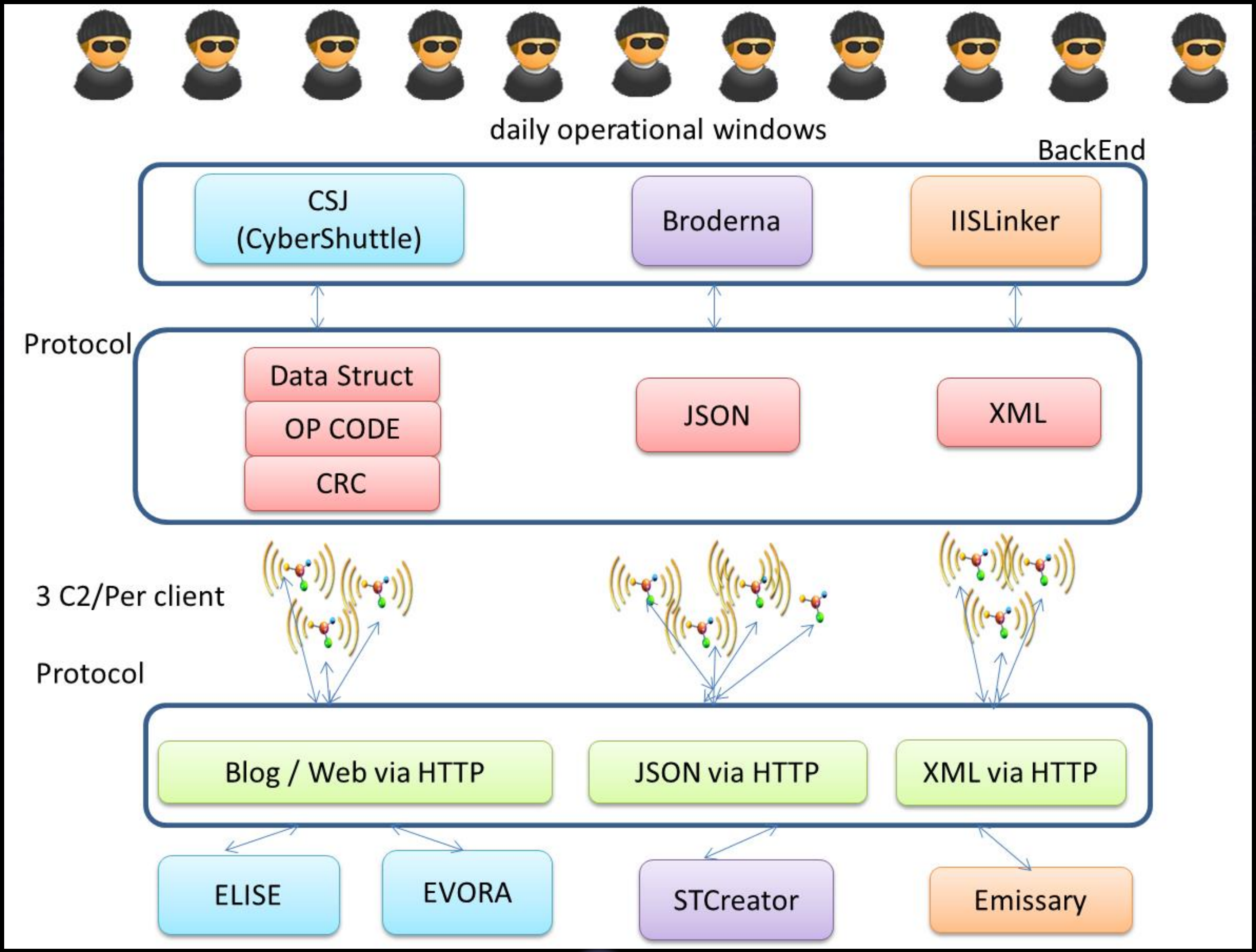
http://140.105.135.71:443/2995ebc9/page_12180900.html
http://118.163.60.73:443/2995ebc9/page_12180912.html

They love fast cars ☺

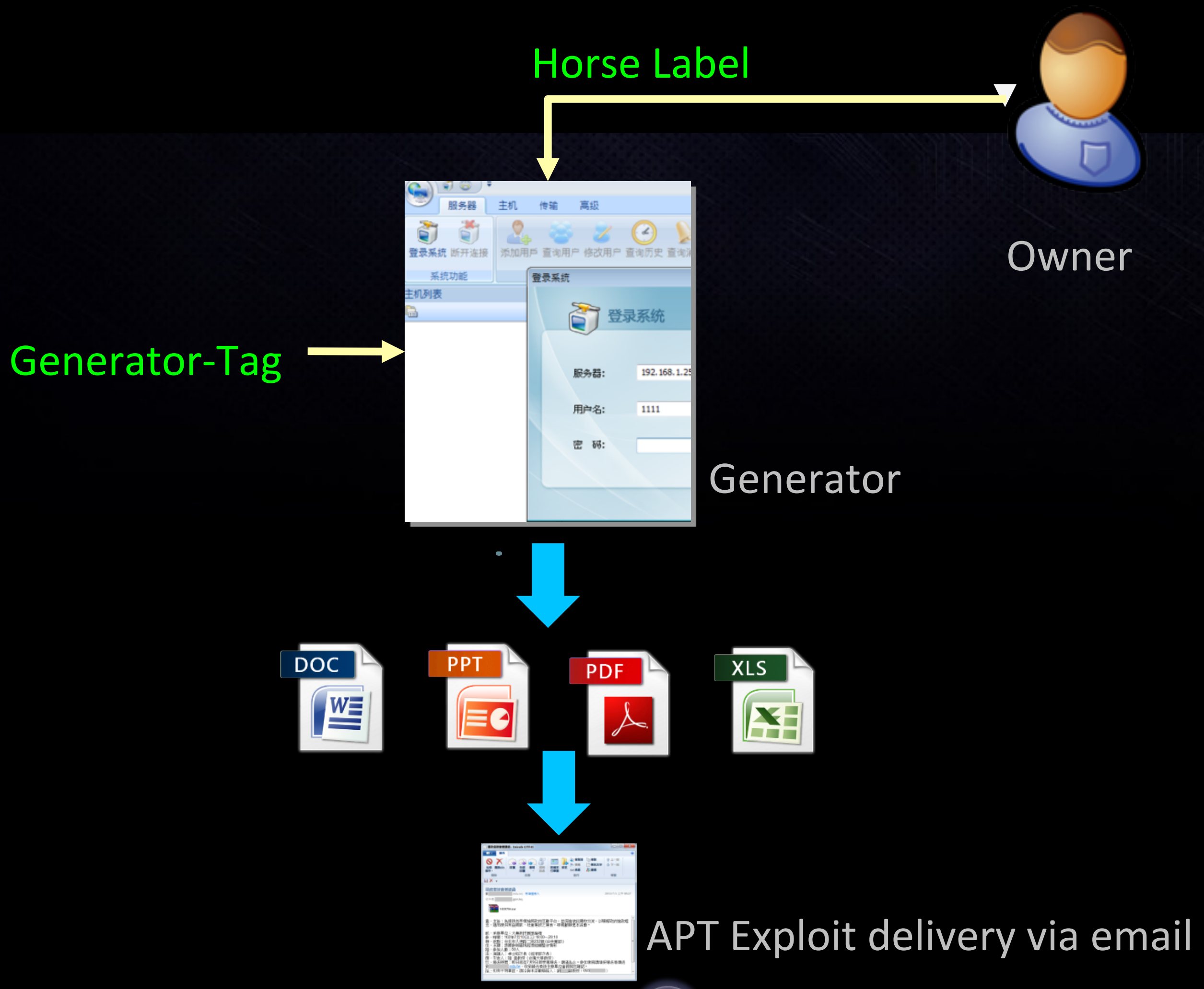
FASST CARS ☺

Evora

Lstudio Operations and C2



“Lstudio” payload Generator



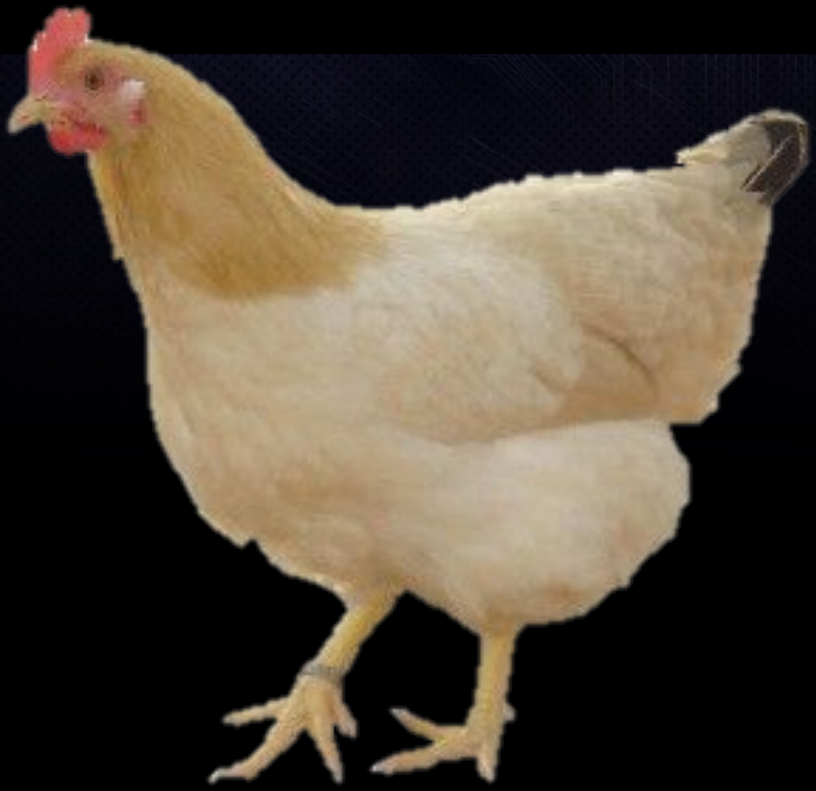
服务器: 192.168.1.25

用户名: 1111

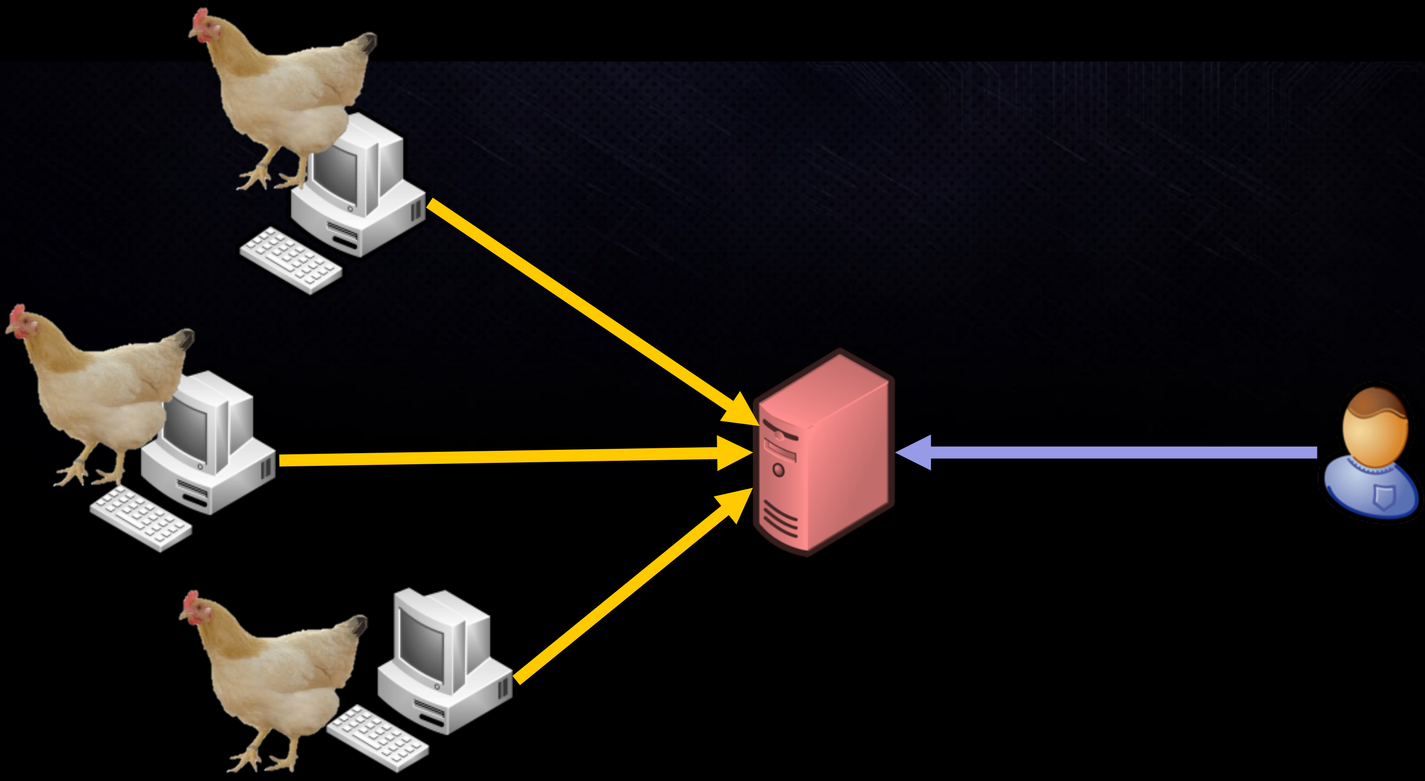
密　码:

We don’t say victim

肉雞 = G



The typical botnet model

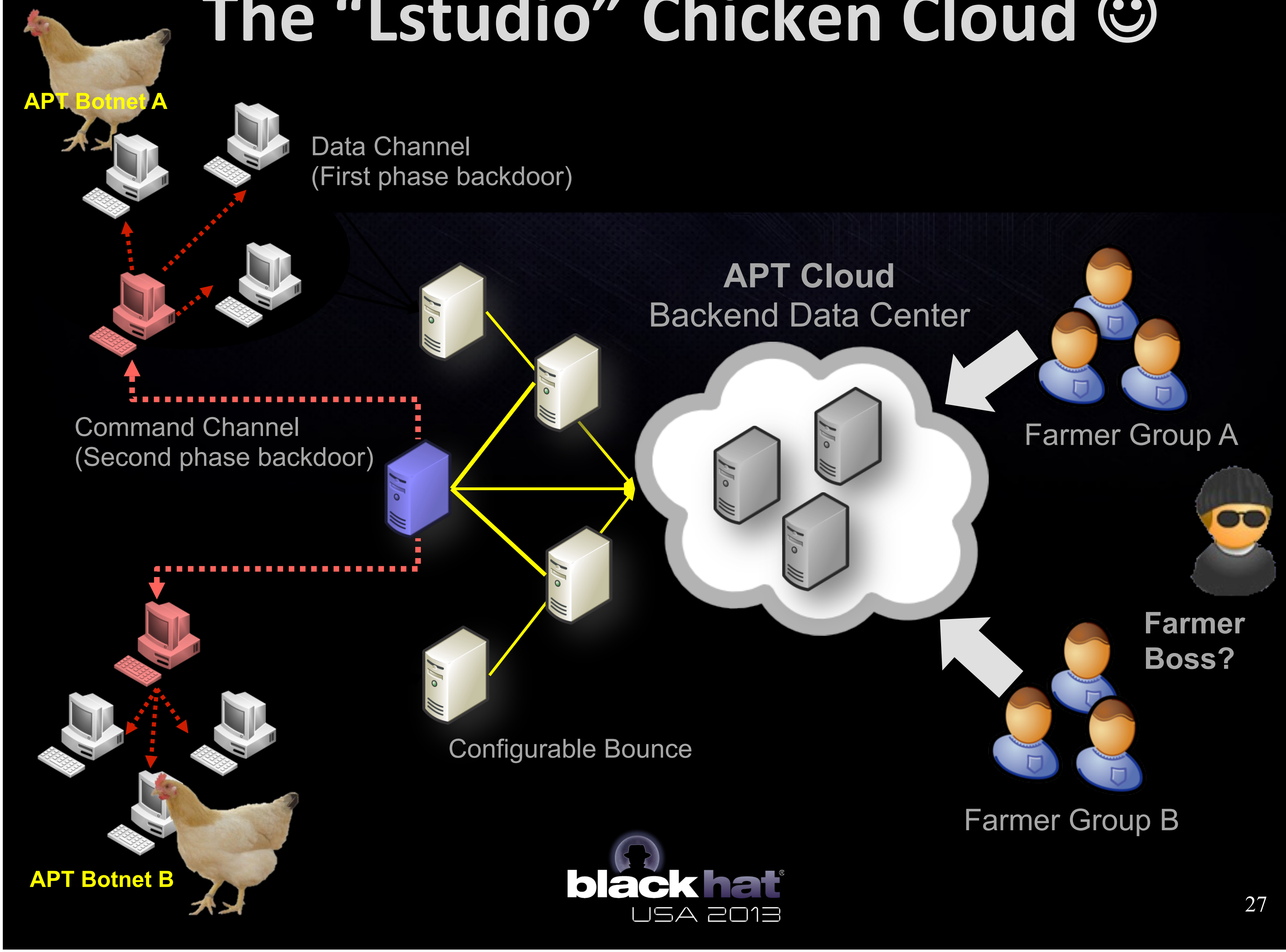


Very advanced Zoo-management skills :)

APT advanced farming :)

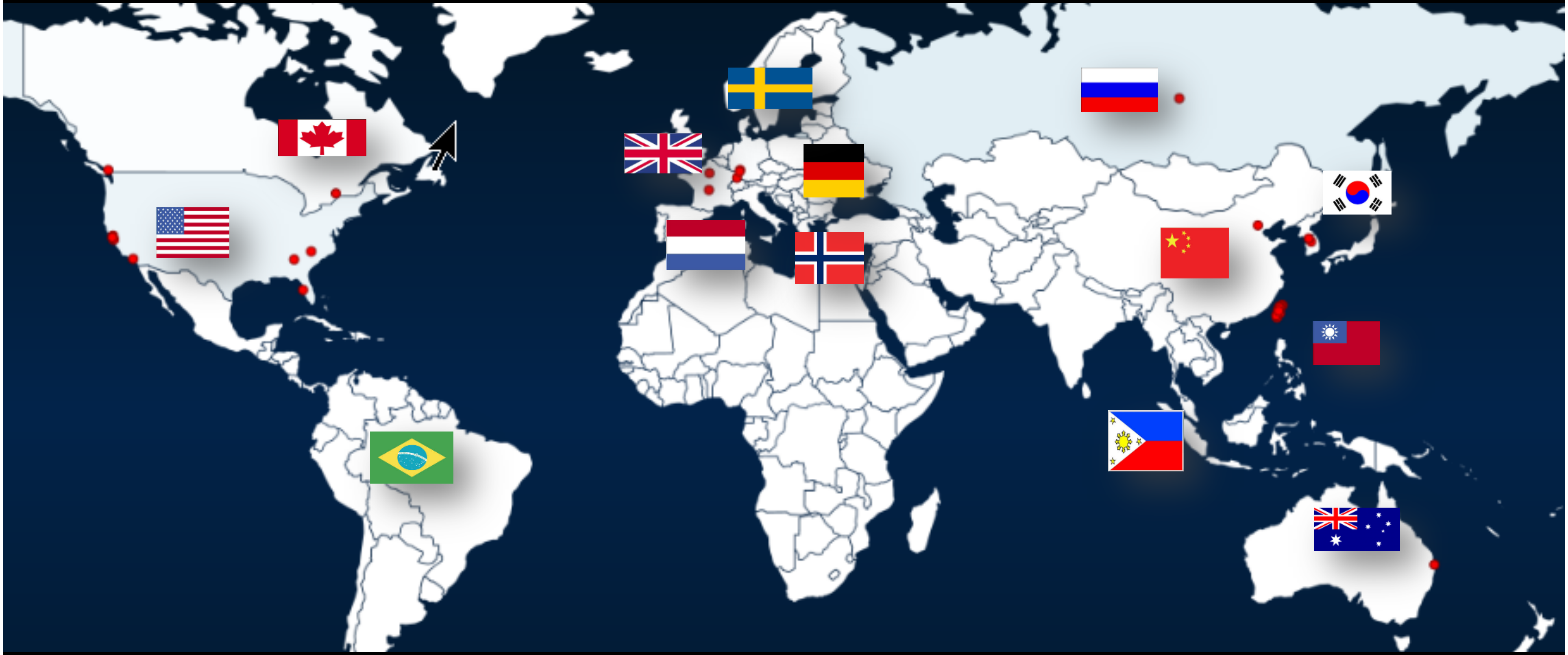
- Operated by roughly 25 “farmers”
- Has controlled over 5,884 machines
- International coverage over 30 countries
- Utilizes 4 different Botnet software families
- Active since 2007

The "Lstudio" Chicken Cloud ☺

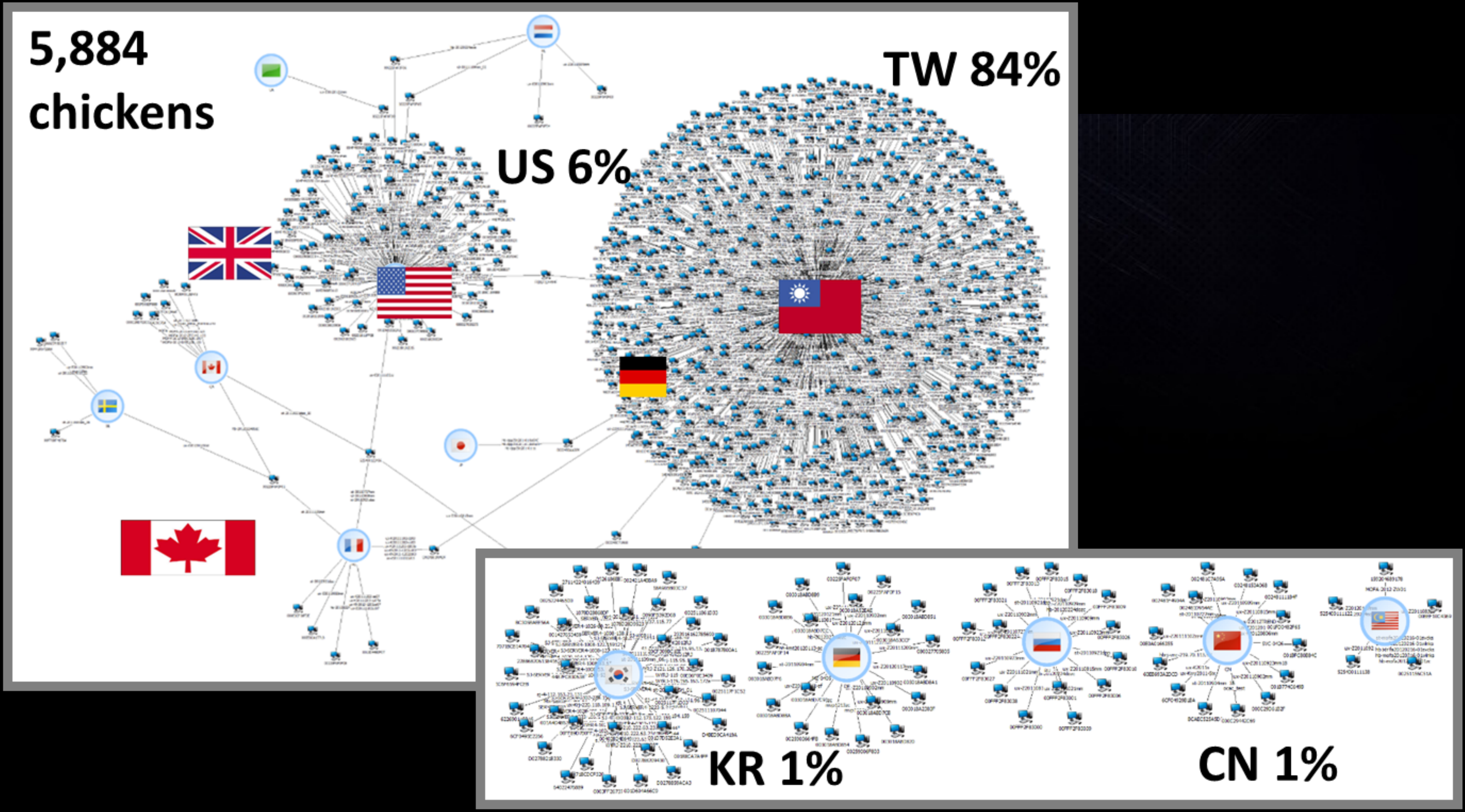


.. And who are the Chicken ?! ☺

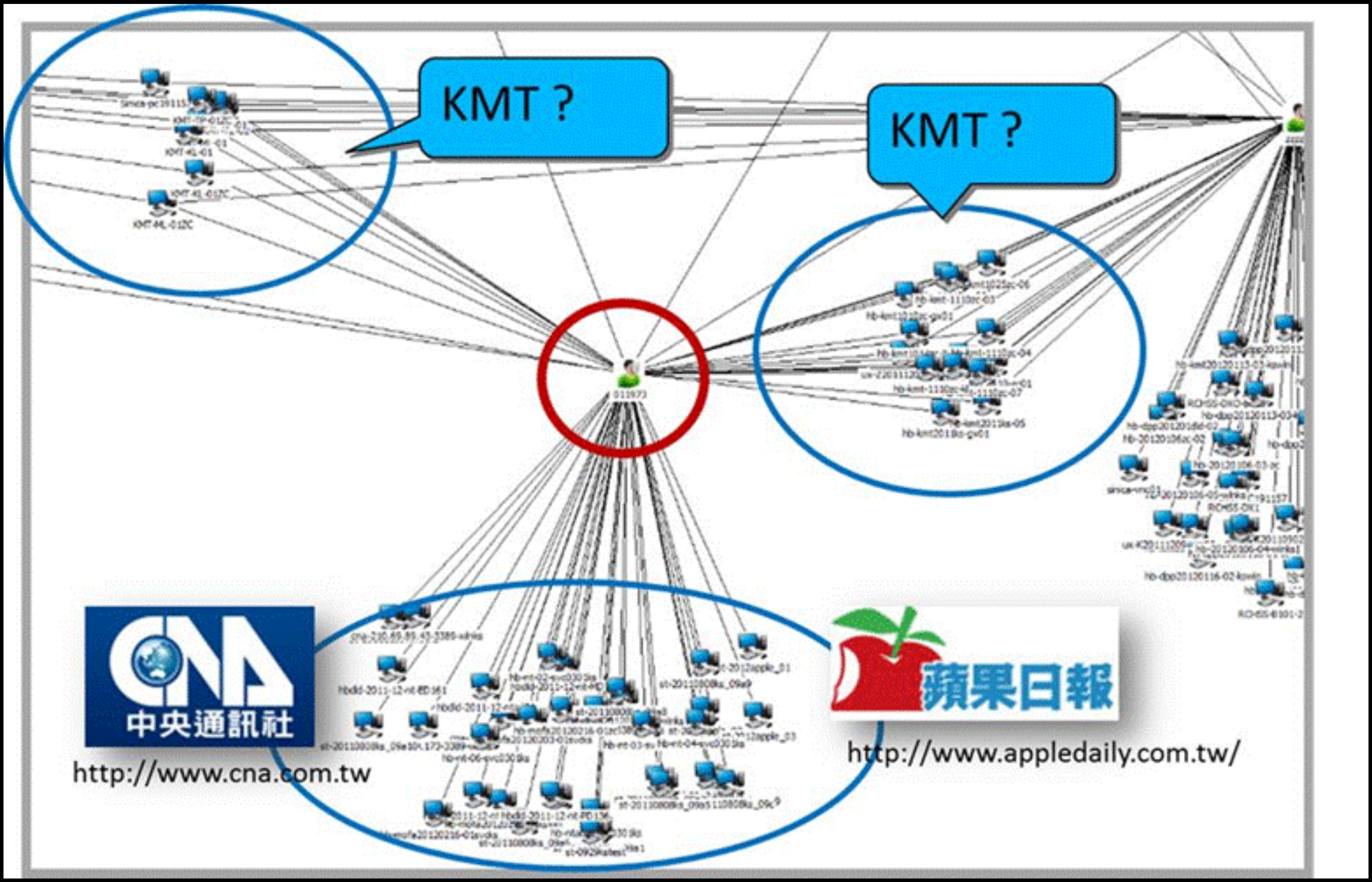
International Chicken Farm Corp.



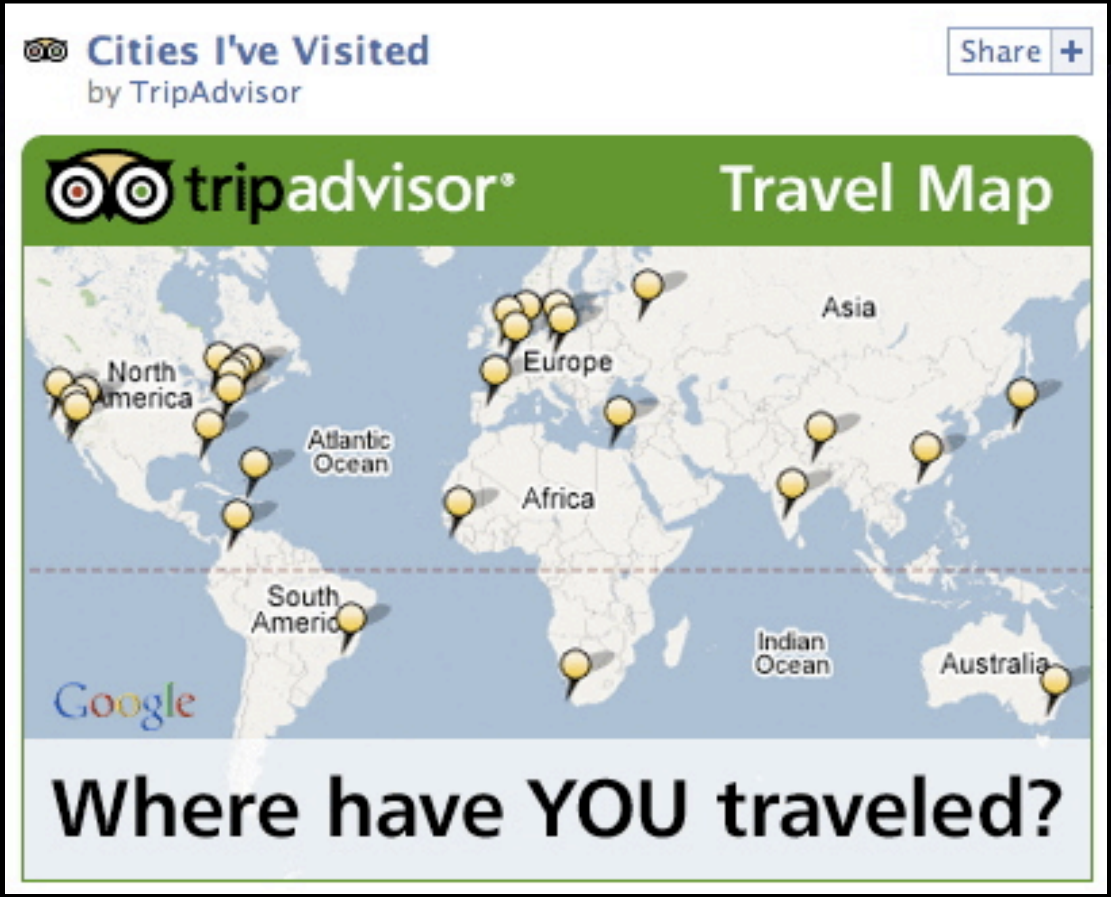
chicken farms went international



Share some Chicken ☺

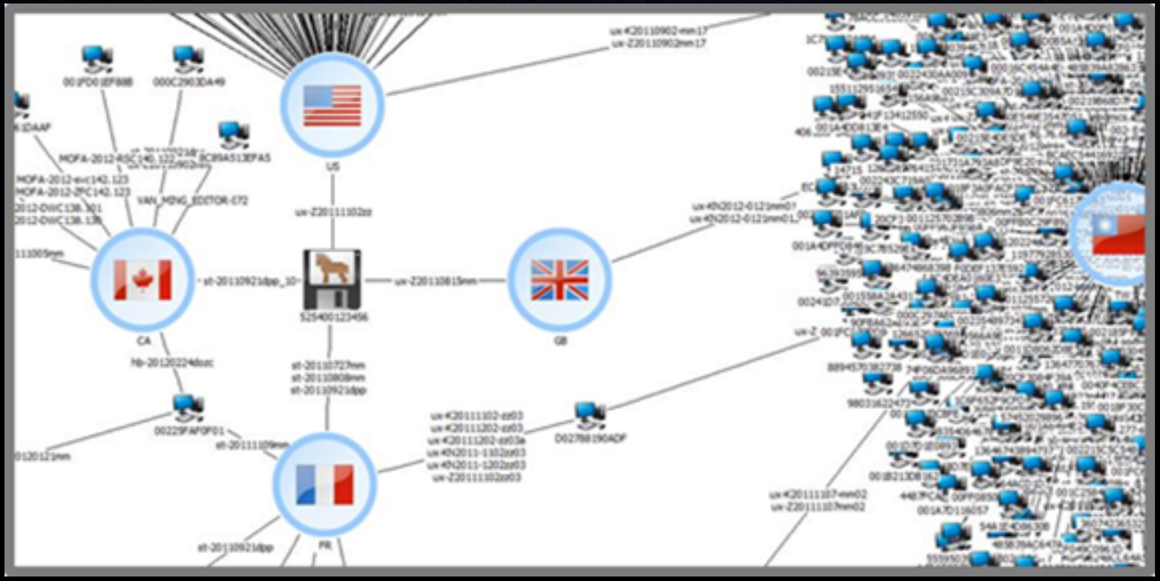


When you travel, your chicken travel too... ☺


Cities I've Visited
by TripAdvisor

Where have YOU traveled?

Lets look at some travelers ☺



US

England

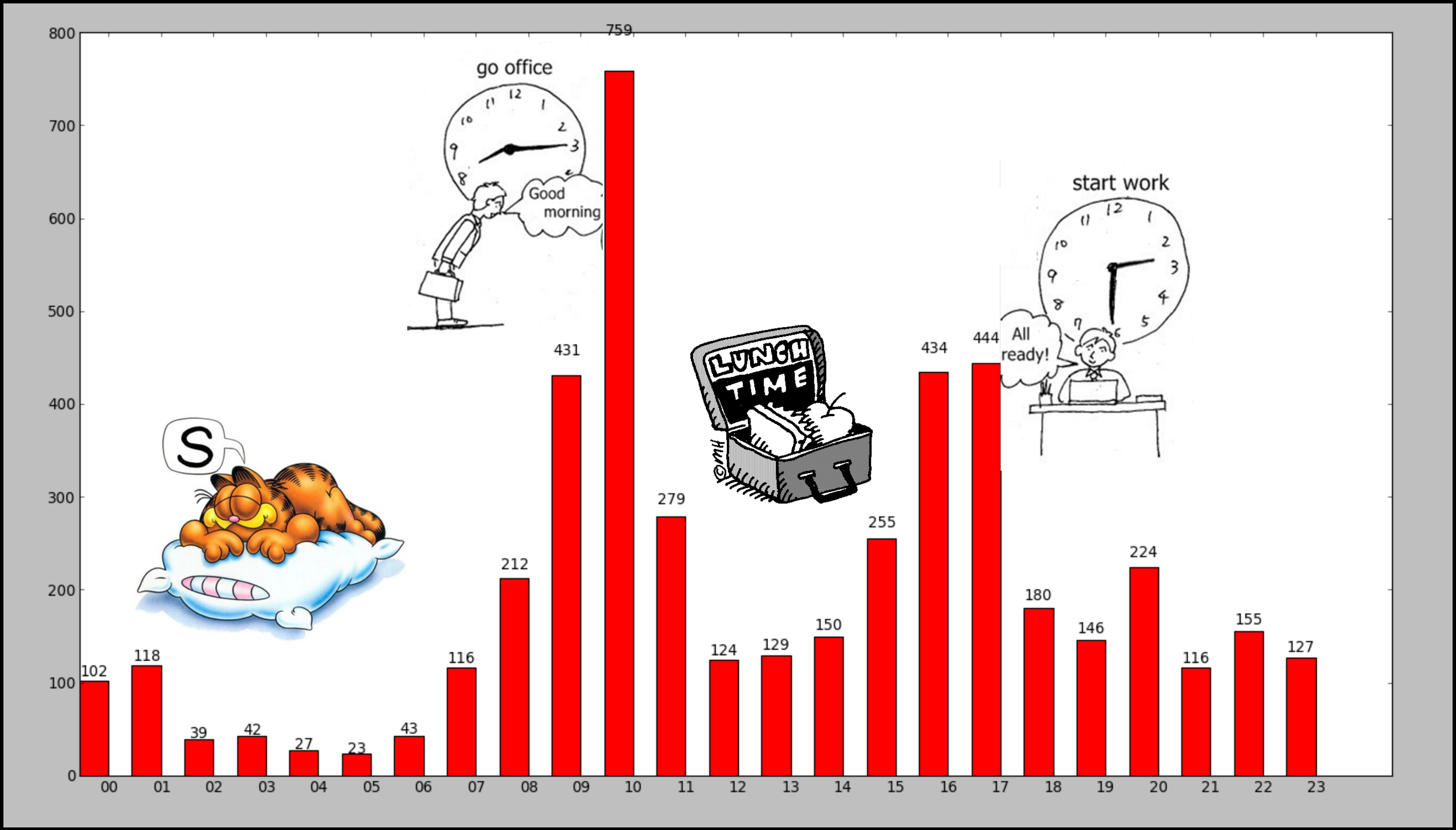
Canada

Taiwan

France

ANOTHER DISCOVERY!!

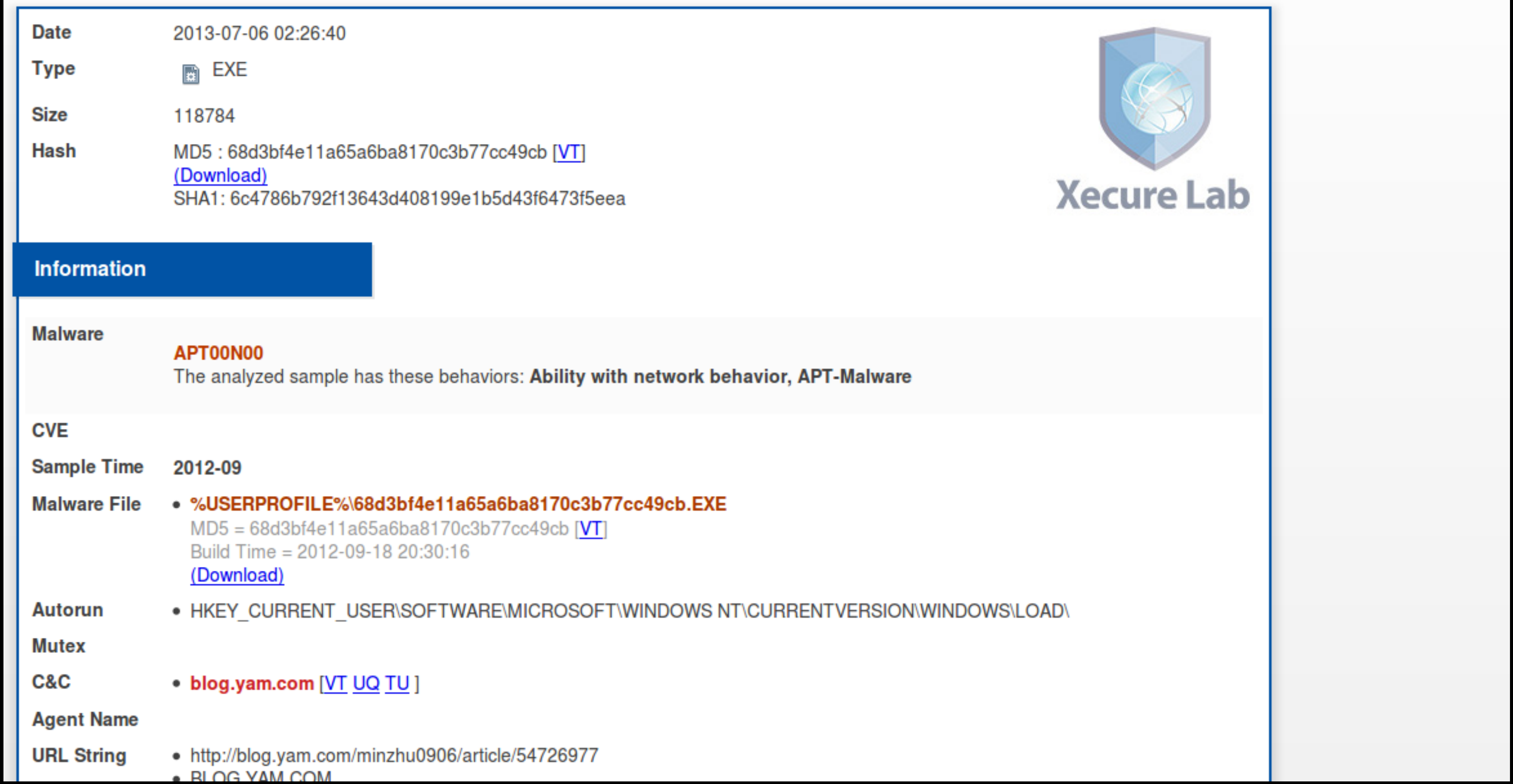
.. do have 9 to 5 job ;)…



Just like some security researchers do ☺

AND THE LAST .. SOME HANDY TOOLS TO SHARE ☺

XecScan: Free API



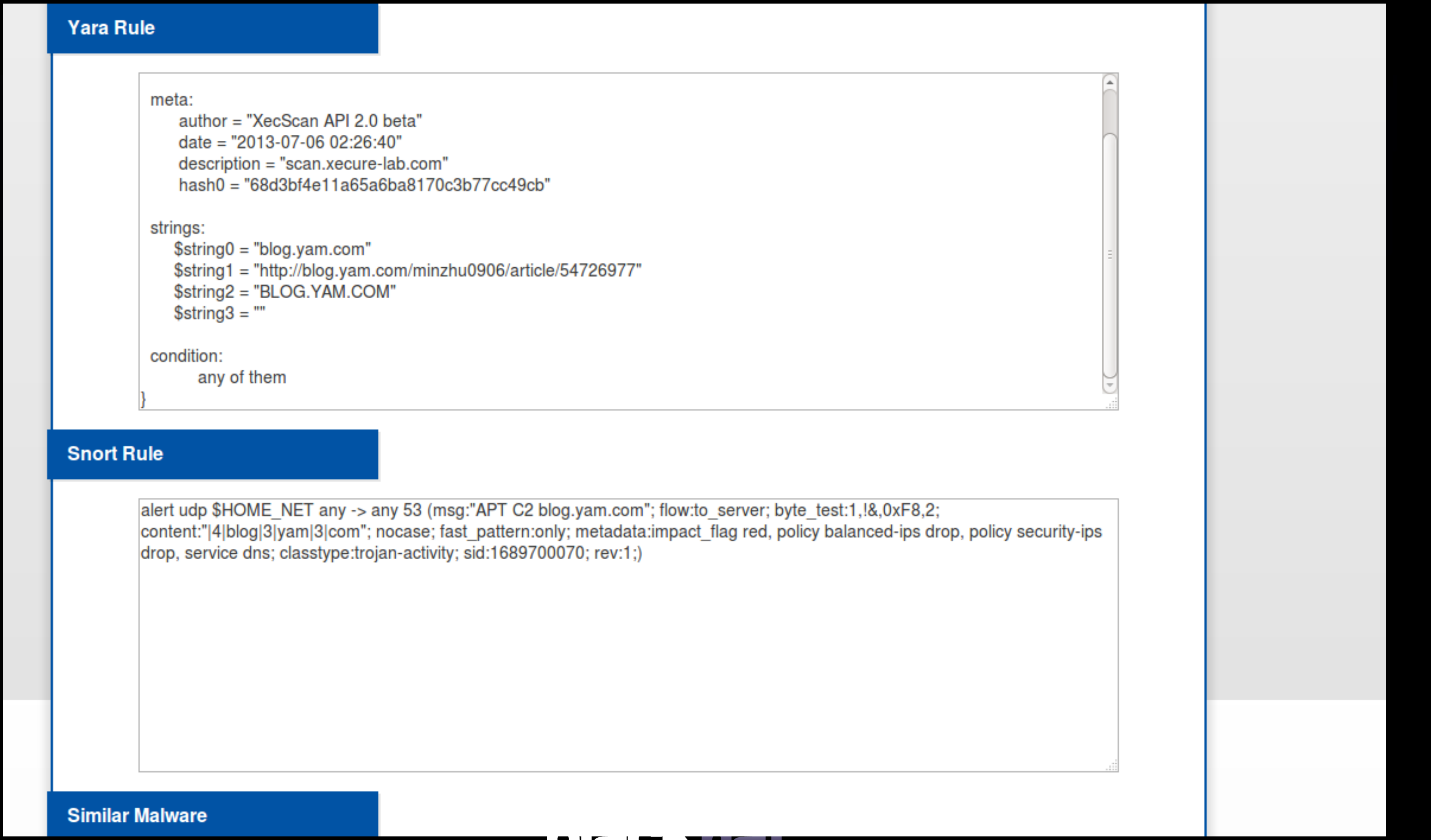
Date	2013-07-06 02:26:40
Type	EXE
Size	118784
Hash	MD5 : 68d3bf4e11a65a6ba8170c3b77cc49cb [VT] (Download) SHA1: 6c4786b792f13643d408199e1b5d43f6473f5eea

Xecure Lab

Information

Malware	APT00N00 The analyzed sample has these behaviors: **Ability with network behavior, APT-Malware**
CVE	
Sample Time	**2012-09**
Malware File	• **%USERPROFILE%\68d3bf4e11a65a6ba8170c3b77cc49cb.EXE** MD5 = 68d3bf4e11a65a6ba8170c3b77cc49cb [VT] Build Time = 2012-09-18 20:30:16 (Download)
Autorun	• HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS\LOAD\
Mutex	
C&C	• **blog.yam.com** [VT UQ TU]
Agent Name	
URL String	• http://blog.yam.com/minzhu0906/article/54726977 • BLOG.YAM.COM

Yara: a swiss-knife of static sigs ;)



```
meta:
     author = "XecScan API 2.0 beta"
     date = "2013-07-06 02:26:40"
     description = "scan.xecure-lab.com"
     hash0 = "68d3bf4e11a65a6ba8170c3b77cc49cb"

strings:
    $string0 = "blog.yam.com"
    $string1 = "http://blog.yam.com/minzhu0906/article/54726977"
    $string2 = "BLOG.YAM.COM"
    $string3 = ""

condition:
        any of them
}
```

```
alert udp $HOME_NET any -> any 53 (msg:"APT C2 blog.yam.com"; flow:to_server; byte_test:1,!&,0xF8,2;
content:"|4|blog|3|yam|3|com"; nocase; fast_pattern:only; metadata:impact_flag red, policy balanced-ips drop, policy security-ips
drop, service dns; classtype:trojan-activity; sid:1689700070; rev:1;)
```

USA 2013

Yara use

Easy to integrate with your scripts

Integration with a proxy server is possible via icap yara plugin: https://github.com/fygrave/c_icap_yara

Raw network traffic monitoring project (and http/DNS indexing):

https://github.com/fygrave/eyepkflow

More cool tools

Moloch https://github.com/aol/moloch

Yara mail https://github.com/kevthehermit/yaraMail

Yara pcap https://github.com/kevthehermit/YaraPcap

Conclusions

Complex infrastructure

Operates since 2007

Multiple software versions

Multiple back-ends

Victims – government and private sector

Mainly Taiwan but also seen world-wide

Questions?

benson.wu@xecure-lab.com
jeremy.chiu@xecure-lab.com
pk@hitcon.org
f@plurk.com