BOTNET 2013

APT 網際飛梭的故事

APT CYBER SHUTTLE:
FROM AUTOMATED ANALYSIS TO TTP OBSERVATION

Version 2

沒錯，這些人並不是作者

- Birdman
- PK
- Fyodor
- Benson





Hilton Grand Vacations
planet
BALLY'S
BALLY'S

媽~ 我在 Blackhat !!

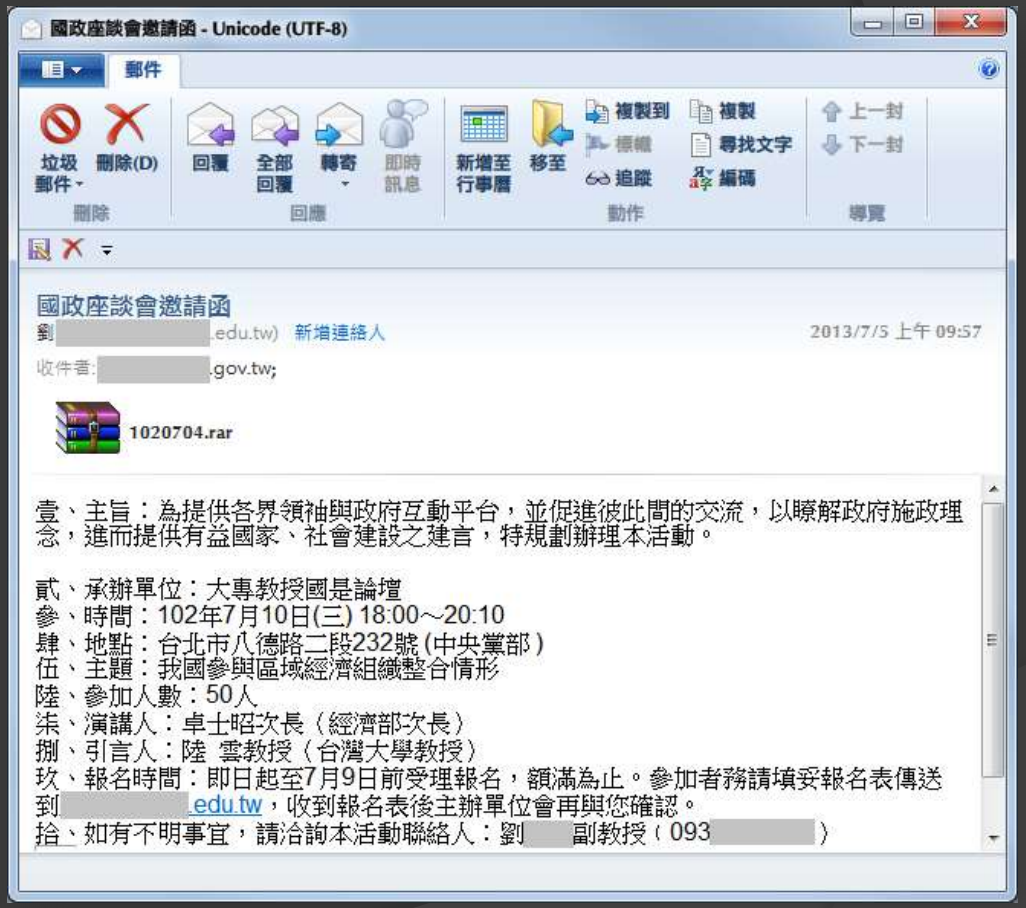

black hat
USA 2013

前言

- 我方主張
  - 以下所有資料，並不是我們做的，小弟頂多算是個天橋底下說書的
  - 資料來源，據說是某團隊分析了數個國外資安事件與 APT C2 Server，所獲得寶貴資料
  - **不能偷拍照，不能錄影錄音**
  - 下面的資料不論你信不信，我是信啦…

From APT Email Attack !

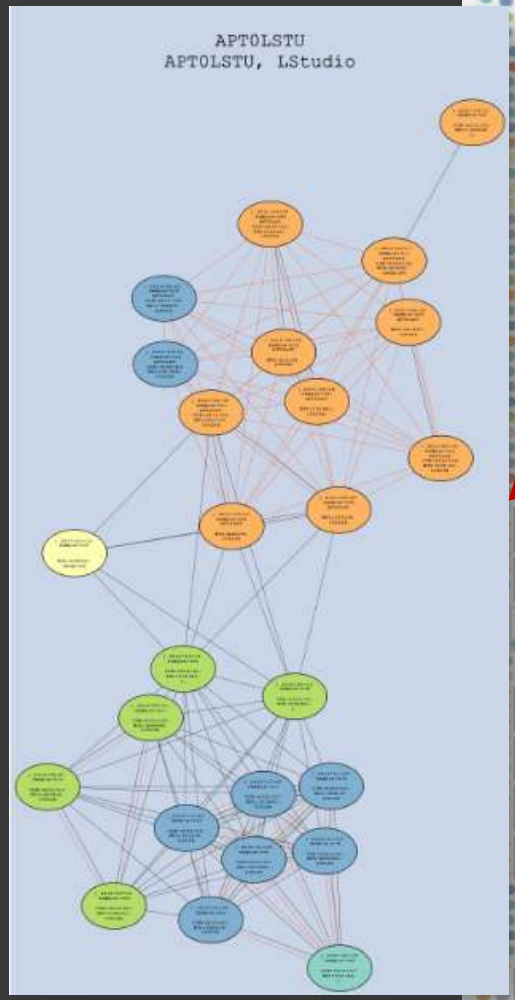
- 我們架設APT Mail 攔阻系統，觀察到許多樣本。
- 我們發現有同一來源駭客持續寄送2個以上不同的APT Malware。他們Malware類似，但Protocol卻不太一樣
- APT Campaign may own more than one APT Botnet !

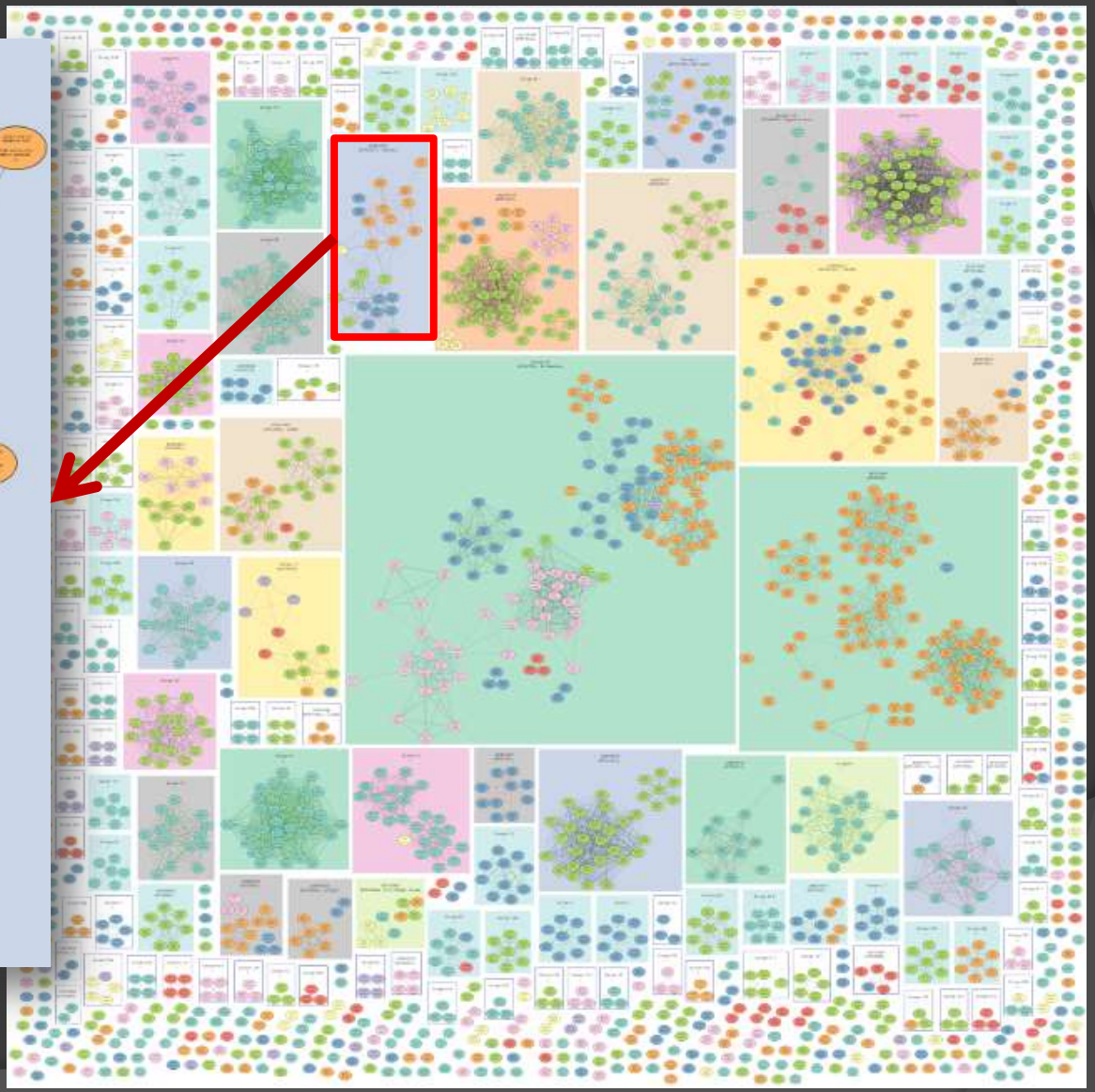


Anti - AntiVirus Vendor


About this Campaign :
APT101
隨裕而安
http://yuann.myphotos.cc/

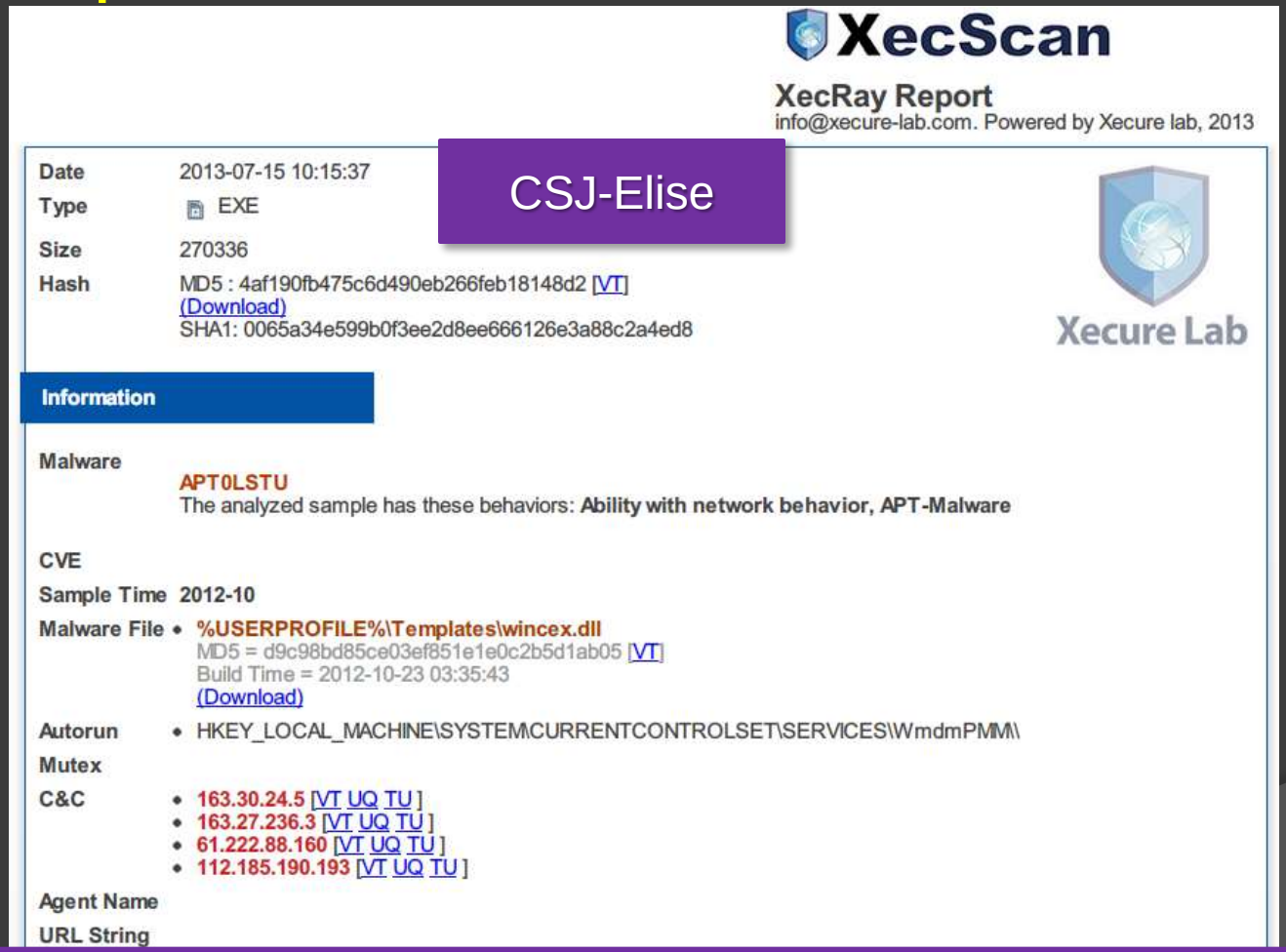
The APT Landscape in Taiwan





拆解 APT101惡意程式

http://scan.xecure-lab.com



XecScan

XecRay Report

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

CSJ-Elise

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

Xecure Lab

Information

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	

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

XecScan 自動產出偵測用的 Rule

Yara Rule

```
rule XecScanRule_8a423502392f9b58d6e246866be80ca8 : APT
{

 meta:
      author = "XecScan API 2.0 beta"
      date = "2013-07-15 10:43:08"
      PoweredBy = "Xecure Lab, http://scan.xecure-lab.com"
      hash0 = "8a423502392f9b58d6e246866be80ca8"

 strings:
     $string0 = "140.119.73.142"
     $string1 = "mailstar.dyndns.info"
     $string2 = "sharezone.dyndns.org"
     $string3 = "mvpstar.crabdance.com"


 condition:
         any of them
}
```

Snort Rule

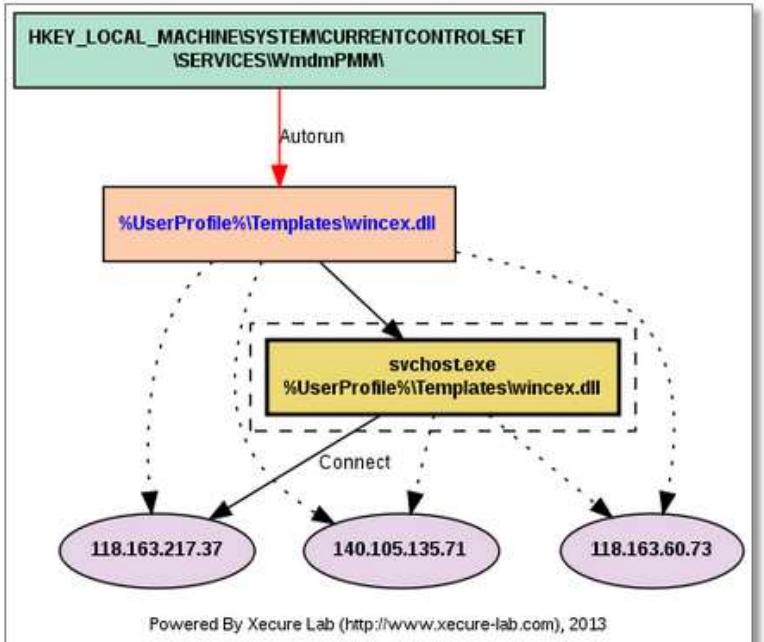
```
alert udp $HOME_NET any -> any 53 (msg:"APT C2 mailstar.dyndns.info"; flow:to_server;
byte_test:1,!&,0xF8,2; content:"|8|mailstar|6|dyndns|4|info"; nocase; fast_pattern:only; metadata:impact_flag
red, policy balanced-ips drop, policy security-ips drop, service dns; classtype:trojan-activity; sid:3414765911;
rev:1;)

alert udp $HOME_NET any -> any 53 (msg:"APT C2 sharezone.dyndns.org"; flow:to_server;
byte_test:1,!&,0xF8,2; content:"|9|sharezone|6|dyndns|3|org"; nocase; fast_pattern:only;
metadata:impact_flag red, policy balanced-ips drop, policy security-ips drop, service dns; classtype:trojan-
activity; sid:1914026624; rev:1;)

alert udp $HOME_NET any -> any 53 (msg:"APT C2 mvpstar.crabdance.com"; flow:to_server;
byte_test:1,!&,0xF8,2; content:"|7|mvpstar|9|crabdance|3|com"; nocase; fast_pattern:only;
```

CSJ-Elise Malware Analysis

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 \000ELISEA380.TMP %d-%02d-%02d %02d:%02d:%0 f:\tools\code\CS_\Elise\Release\

Malware Behavior Graph



TAABAMoGvBjTVXHUHaibnwrAWfchx2x17Rf2roRBnbD/9lu13lWnlAUbBgqw+YNld2vcV5krtXoG__FXI43BxueF4FChFrkSRgNVP2WQ==

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

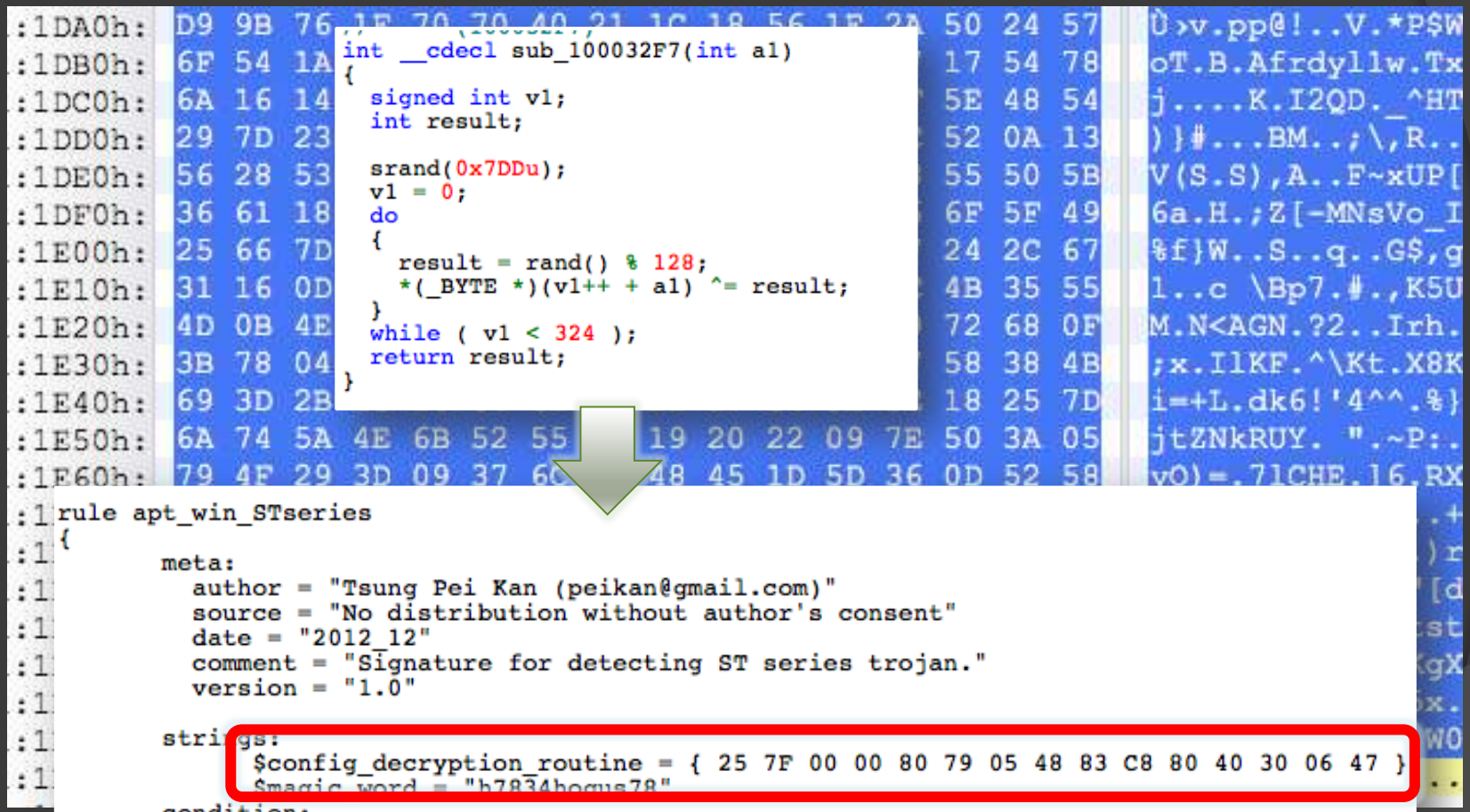
Elise

整體設計上Elise，將摒棄現行概念底盤以鋁合金打造、車身鈑件也大量採用碳纖維材質的Elise全車重僅1095公斤，而在Lotus的規劃下，未來Elise將搭載擁有約320匹馬力輸出之2.0升四缸引擎。從近來幾部全新發表的Lotus之上，我們能夠看見新一代Lotus係採用源自"鯊魚"的設計概念，並隨著各車型與定位著不同，而各自發展屬於單一車型的獨特風格，而在Elise之上我們也能看見更多銳利的線條與充滿殺氣的勾勒樂手法，以營造出Elise特別的霸氣！
http://cool3c.incar.tw/article/34399

Always Http


Generated by LocalTIme
C2 config
Customized User-agent
Use a cookie to transfer data(encrypted by base64 like algo)
GET /29b544bb/page_12190736.ht
Accept: */*
Host: 118.163.217.37
Content-Length: 0
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Connection: Keep-Alive
Cookie: A=F04BAGgsrxyJLl+w59Ul0vdXqIwMJ
+5bWBImPRvz3lWcKhUDKnfDS4mYpqcVj
+rlhgEyqrhUmMId__USgfTbl42aW9fClaaLO3NIaripmVN
6dvzM0sXTBBgn0H05tDc/e/a__IRWBViHZHtemSUpVSkE8
+UmyzClaQbGttbEwym4CjK9hLHzw
+VCcJw5POrBN6dynXS__6KrEPs2EpZq7IiCHv9v0v5+
Q8AS6pw0BZGWgRrh059douM0DQqSsi2n7LaSFt__3qA9LGo
3aGX5GcXzFbi/0N43xx4b8/I+VufHGJlDtJc2o9xA3NDpdr__3pS8NuIbc+Sa4o
+3LzmfC06YQGbxHXEfPQanYvgRQbbUzvFlxqtCfD1EOF37U8pilJQuSVqYZnOQ__
MJgyR4KUNq+eLR9DRY8QMzMNNHdPlCCtnkDPVWpDHULgYvb
+hRGrK1L5Yi6rGcGMgj816HK__y2nJE0udAecGkQQOrN/
yBFf8KOzkLkK0Vq7I2Z5jx7Me6EVp6algQyzztslbjW9A0niFhCzlIflN__wqD+B
soGsrysrOkhnfrBjromX4x6jvFEL5LdC9BsRtgtHpiC
+wm8UKZ1qOWq4csUN5LGGqM3O__zGK9vZVN1ob+hTR7N6u9RtBHPvnyU/
pEf9FCg4Y45naV5dmuL6GWbwy/giNFWQ+RHOb5H/YbOQ6C__FkO/
tdlbhvtl8seZKrzXaPql__QeqNekahamHeUS81vJqXdeC0vWbK6rM7yhwecB75JxRgwvq
O08guN5HnfR51w/08+pyP9T3G+urN__3eLertgC21A2wAkeeFl6pulh2uV79+OhE1Ki
+xESMegP3crigr3tk9UqxTwX1Lx9RQkMOXyDbiTE__z06FQWjQZIE0ZZqWkCYWrVnVm/

Encrypted C2 config can be found in the end of file(srand+xor)



Using user-agent to find more suspicious connections

@fields.httplog_agent:"Mozilla/4.0 (compatible; MSIE 8.0)" AND NOT @fields.httplog_agent:"Windows" AND NOT @fields.httplog_agent:"Win32"

	(compatible; MSIE 8.0)|
06/10 16:25:40	Jun 10, 2013 16:23:46.669044000|202.169.162.1|163.27.236.3|4793,8080|GET|163.27.236.3|/8c21bd0f/thread_10165823.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 16:15:43	Jun 10, 2013 16:13:46.947680000|202.169.162.1|163.27.236.3|4523,8080|GET|163.27.236.3|/8c21bd0f/thread_10165813.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 15:59:36	Jun 10, 2013 15:57:41.278954000|140.109.221.143|114.134.85.200|1357,80|GET|hk.qq.com|/cgi-bin/personal_info?category=1&uin=1247195680&userip=140.10
06/10 15:55:36	Jun 10, 2013 15:53:47.061743000|202.169.162.1|163.27.236.3|4023,8080|GET|163.27.236.3|/8c21bd0f/thread_10155853.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 15:49:27	Jun 10, 2013 15:46:59.059076000|202.169.166.224|114.134.85.199|54726,80|GET|hk.qq.com|/cgi-bin/personal_info?category=1&uin=1405894971&userip=202.1
06/10 15:45:38	Jun 10, 2013 15:43:47.099331000|202.169.162.1|163.27.236.3|3880,8080|GET|163.27.236.3|/8c21bd0f/thread_10155843.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 15:35:29	Jun 10, 2013 15:33:47.131369000|202.169.162.1|163.27.236.3|3807,8080|GET|163.27.236.3|/8c21bd0f/thread_10155533.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 15:25:45	Jun 10, 2013 15:23:44.245728000|202.169.162.1|163.27.236.3|3596,8080|GET|163.27.236.3|/8c21bd0f/thread_10155223.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 15:19:25	Jun 10, 2013 15:16:50.443119000|202.169.166.224|114.134.85.199|53024,80|GET|hk.qq.com|/cgi-bin/personal_info?category=1&uin=1405894971&userip=202.1
06/10 15:15:45	Jun 10, 2013 15:13:41.393158000|202.169.162.1|163.27.236.3|3408,8080|GET|163.27.236.3|/8c21bd0f/thread_10154913.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 15:15:44	Jun 10, 2013 15:13:38.378989000|202.169.162.1|163.27.236.3|3408,8080|GET|163.27.236.3|/8c21bd0f/thread_10154913.html|Mozilla/4.0 (compatible; MSIE 8.0)|
06/10 15:13:02	Jun 10, 2013 15:03:38.449376000|202.169.162.1|163.27.236.3|3323,8080|GET|163.27.236.3|/8c21bd0f/thread_10154903.html|Mozilla/4.0 (compatible; MSIE 8.0)|

他們似乎都是這家出品 LStudio

- 這族算是容易研究，因為都有明顯的特徵

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

D:\Lotus\Elise\Release\EliseDLL.pdb

d:\tools\code\CSJ\Evora\Release\Evora.pdb

d:\lstudio\projects\config007\insconfig\objfre_wxp_x86\i386\InsConfig.pdb

d:\lstudio\projects\stseries\zcstcreator\Release\ZCSTEntity\i386\ZCSTEntity.pdb

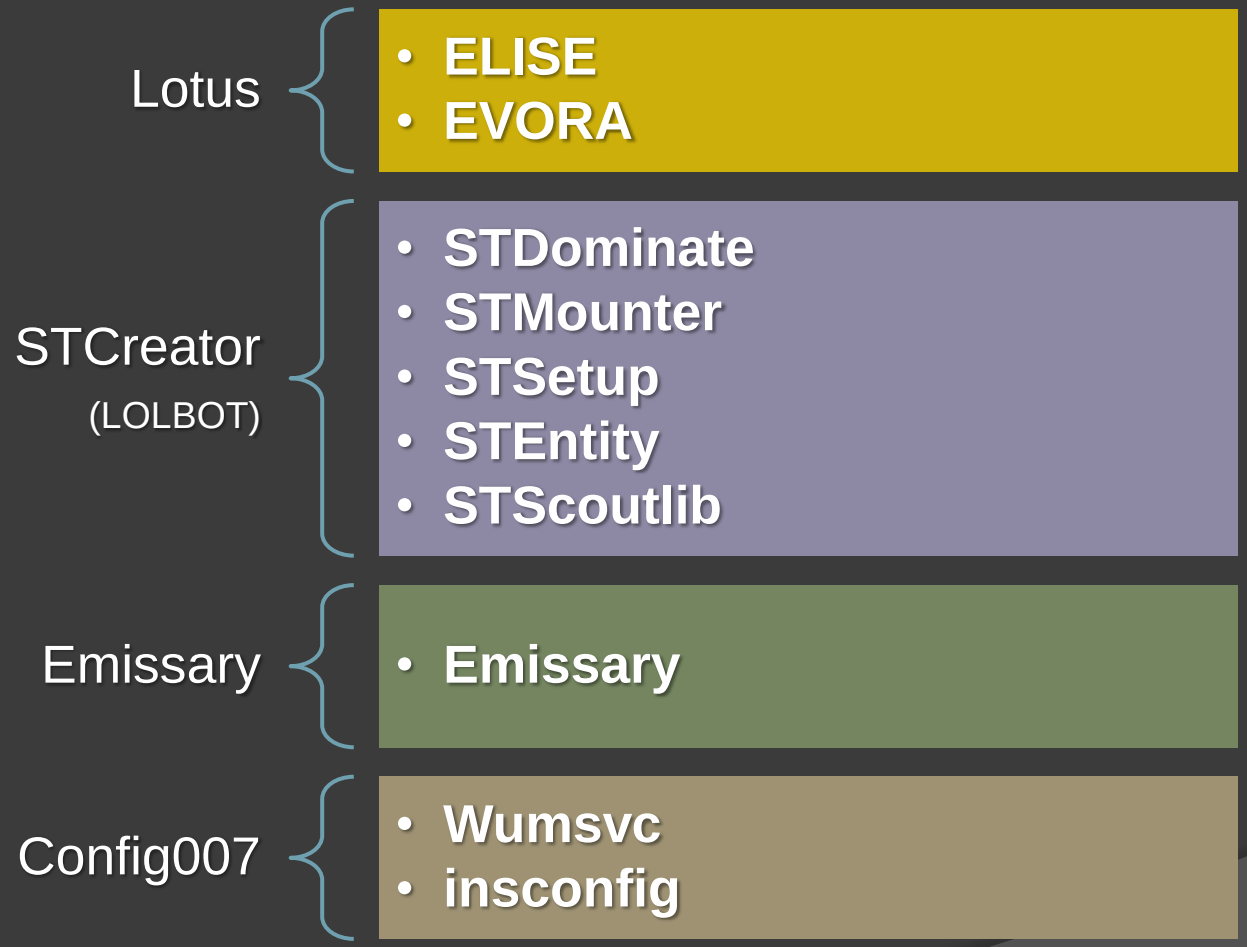
d:\lstudio\projects\stseries\ksstcreator\Release\KSSTEntity\i386\KSSTEntity.pdb

d:\LStudio\Projects\STCreatorII\Release\STDominatelib.pdb

D:\LStudio\Projects\STCreator\Release\STScoutlib.pdb

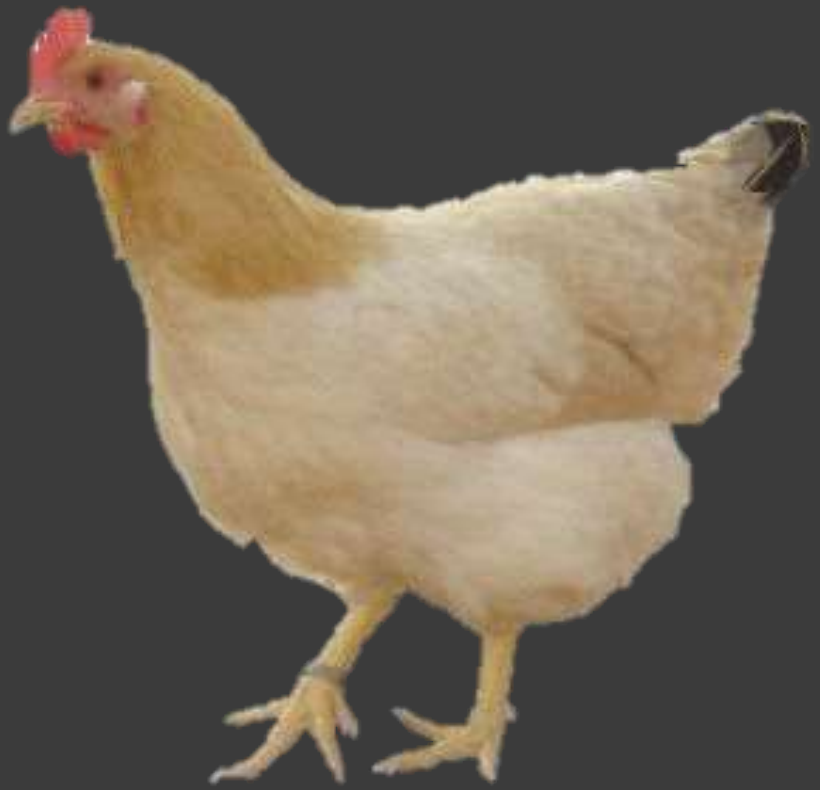
Evora

Lstudio Production



We don’t say victim

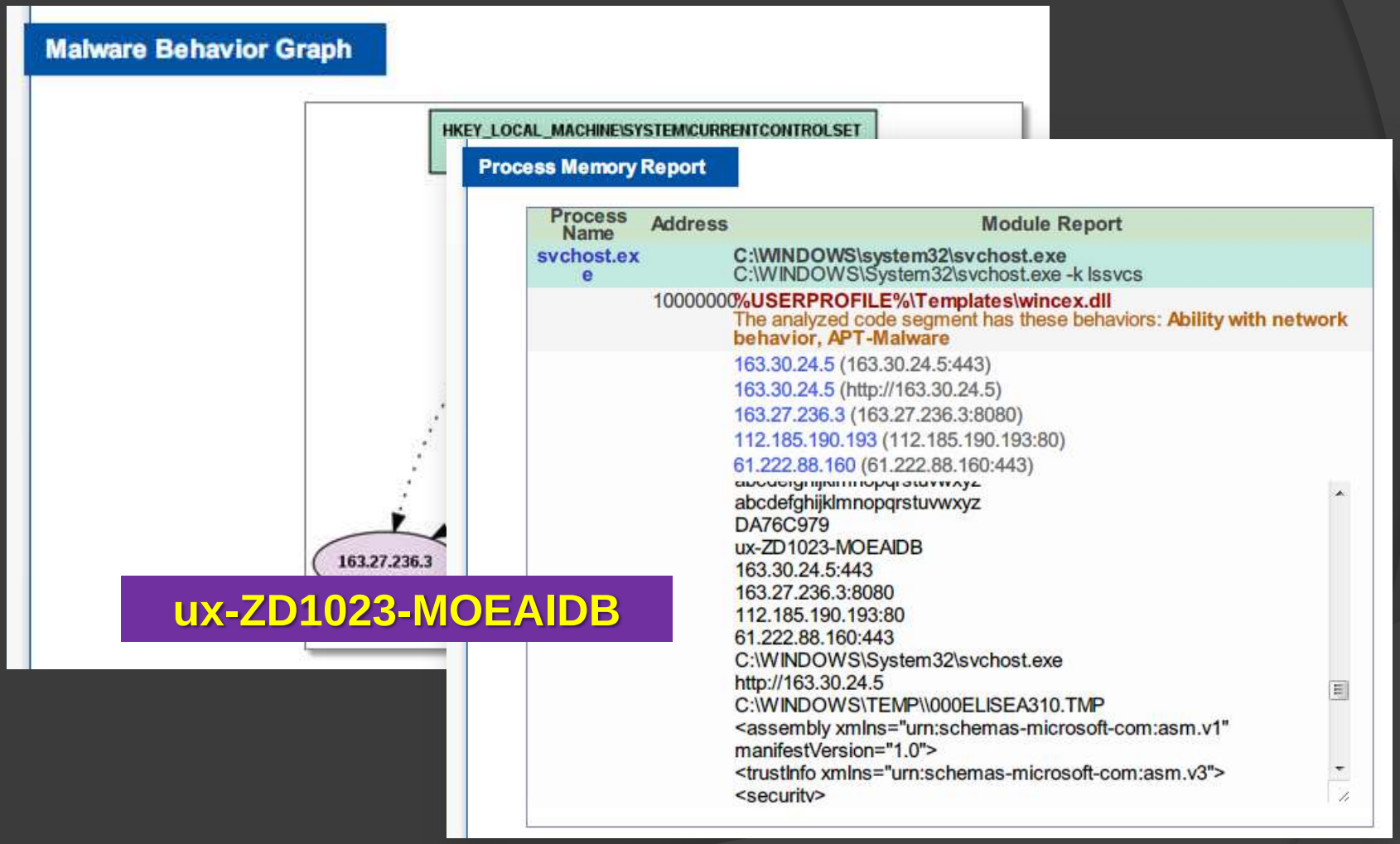
肉雞 = G



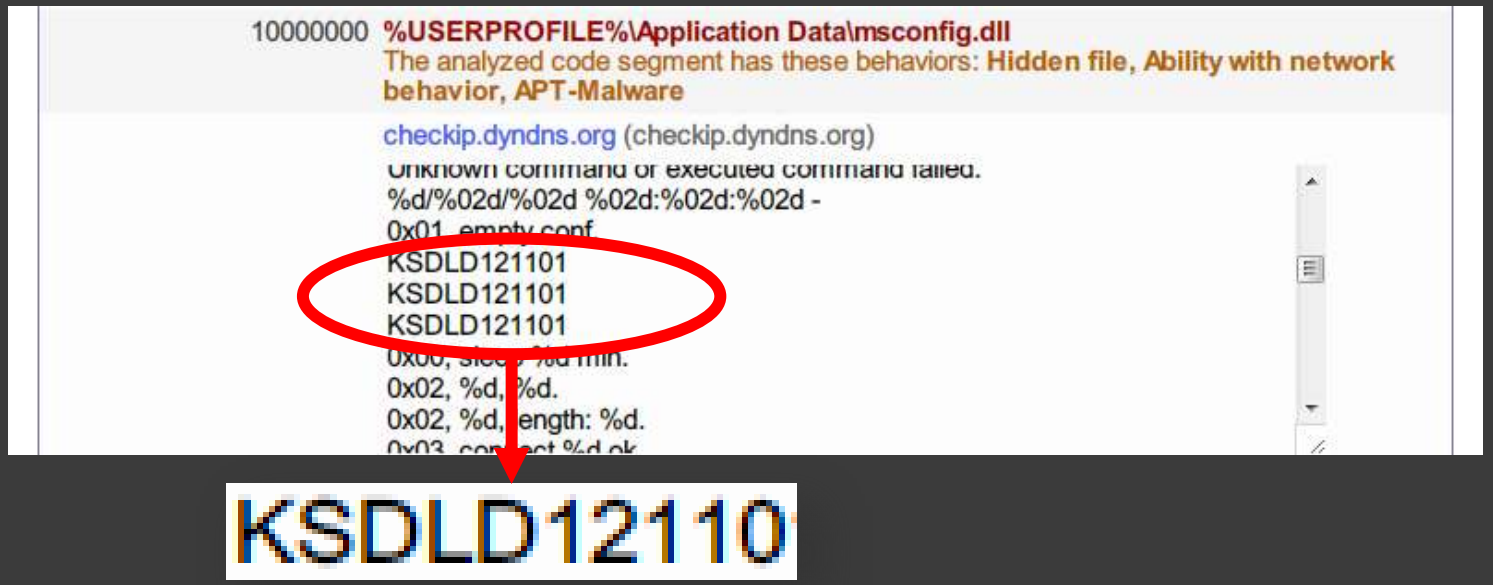
滿地都是雞隻，該如何識別?

- 身為農場園長，管理是很講究的

Horse-label : 馬碼 = 雞碼 ?



Generator-Tag



- KS = STCreator
- DLD = 低權限版本
- 12110 = 2012-01-10 製造

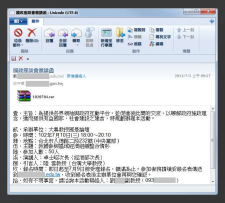
APT Attack Generator

Horse label

Owner

Generator-Tag

Generator



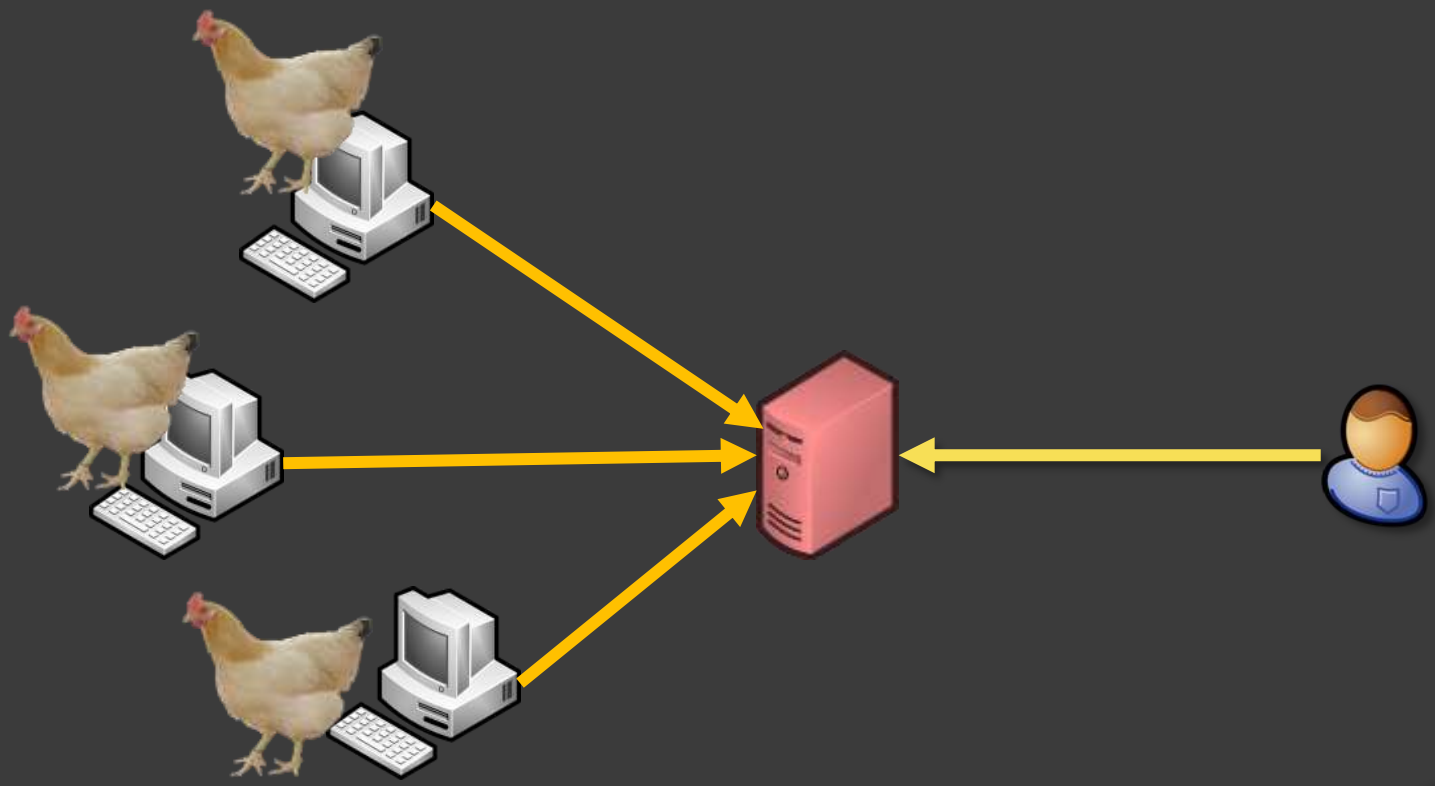
APT Email Attack !

APT駭客是如何管理龐大的肉雞群

就我們對 APT101 統計資料顯示

- 他們約有 25 位專業農夫 (工作人員)
- 控制過至少超過 5800 肉雞電腦
- 他們雞隻是分散在各地，共含蓋 30 國家/地區
- 使用 4 種不同的 Botnet，但是卻統一管理
- 這是如何辦到的…

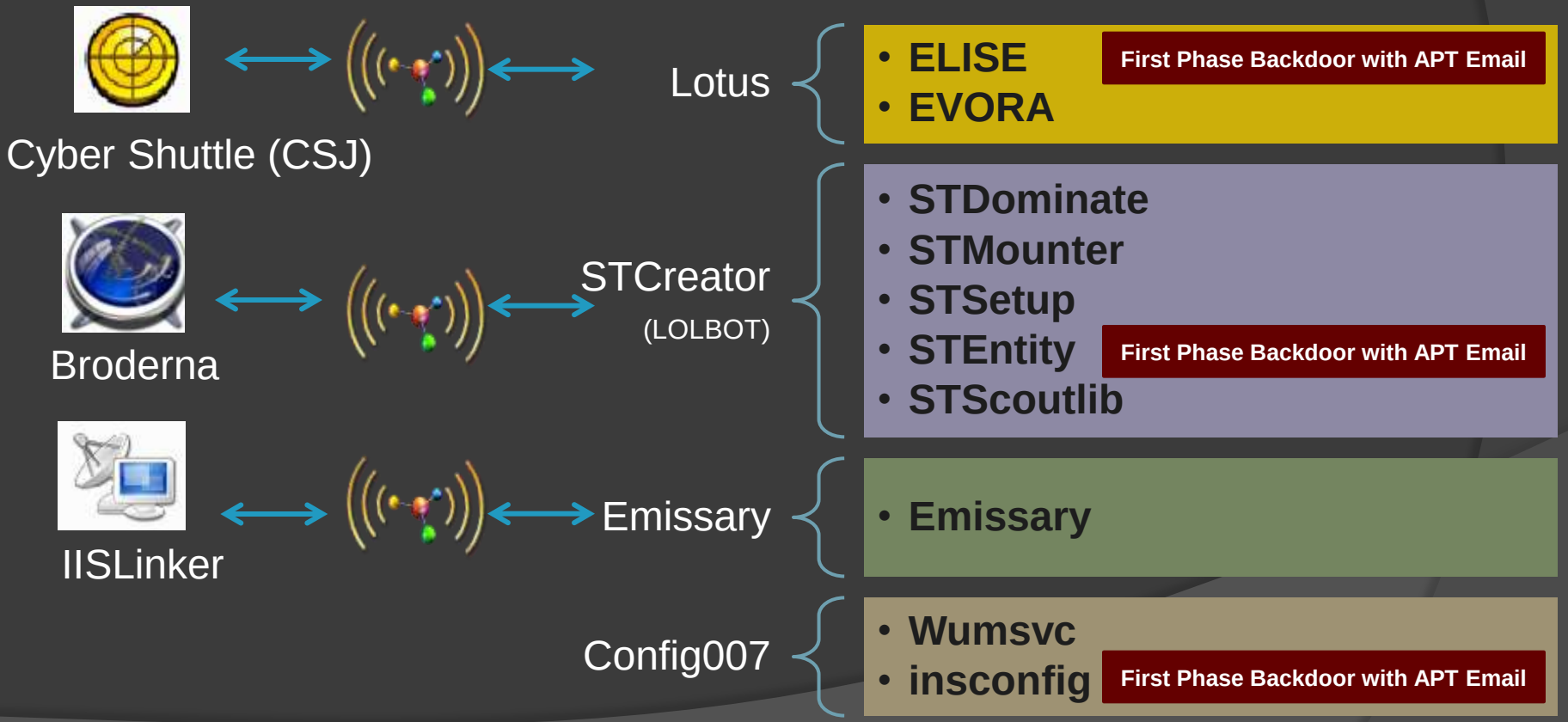
The typical botnet model



原來如此

APT101 Crew

- 其實駭客有很多不同的後門程式



daily operational windows

BackEnd

CSJ

Broderna

IISLinker

Protocol

Data

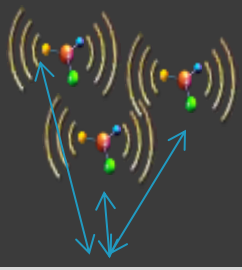
OP CODE

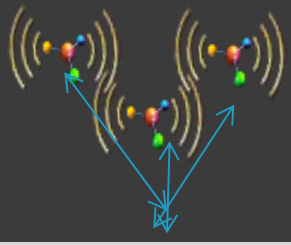
CRC

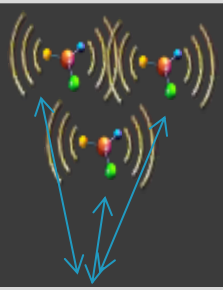
JSON

XML

3 C2/Per client







Protocol

Blog / Web via HTTP

JSON via HTTP

XML via HTTP

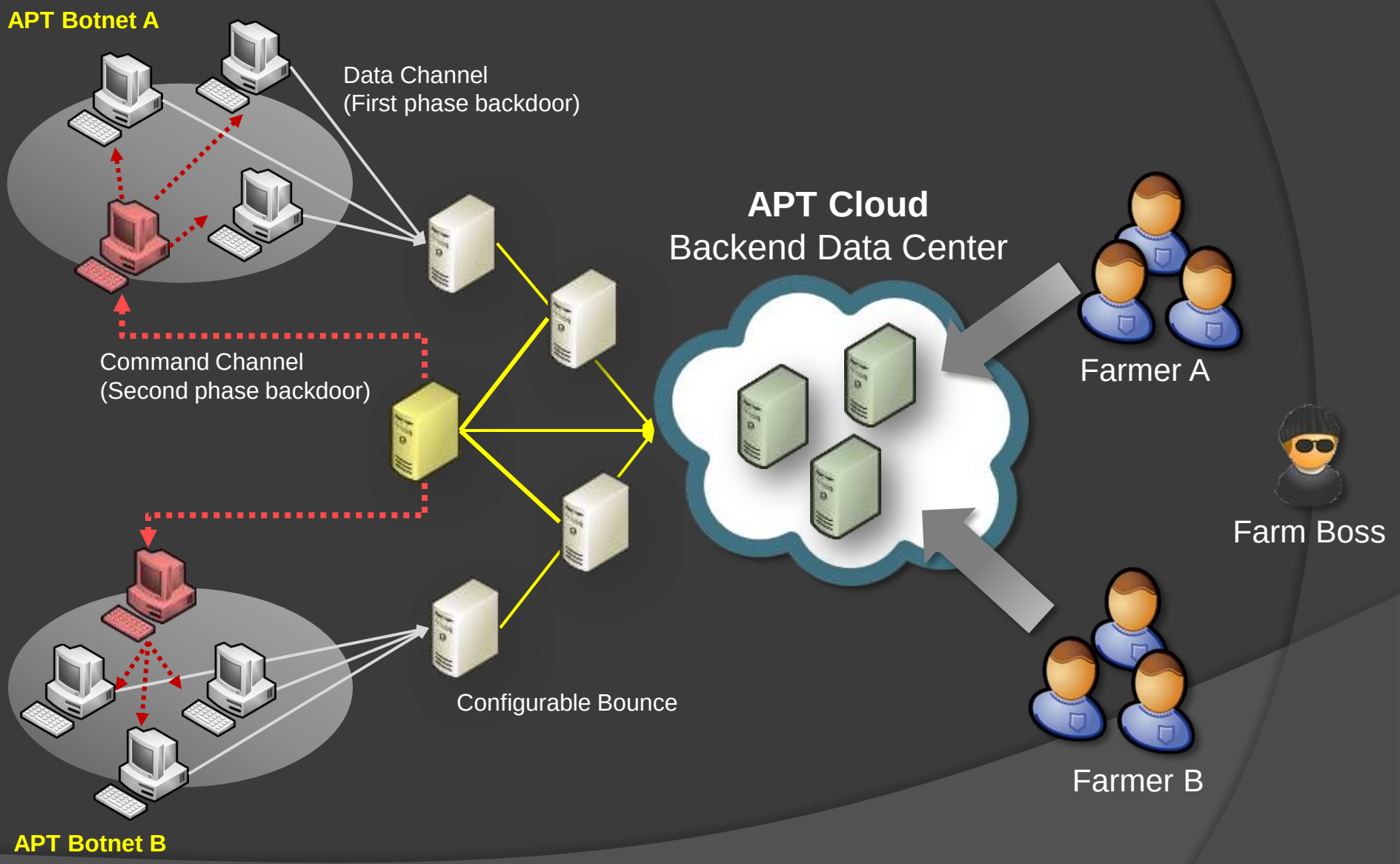
ELISE

EVORA

STCreator

Emissary

原來駭客才是掌握雲端運算精髓...

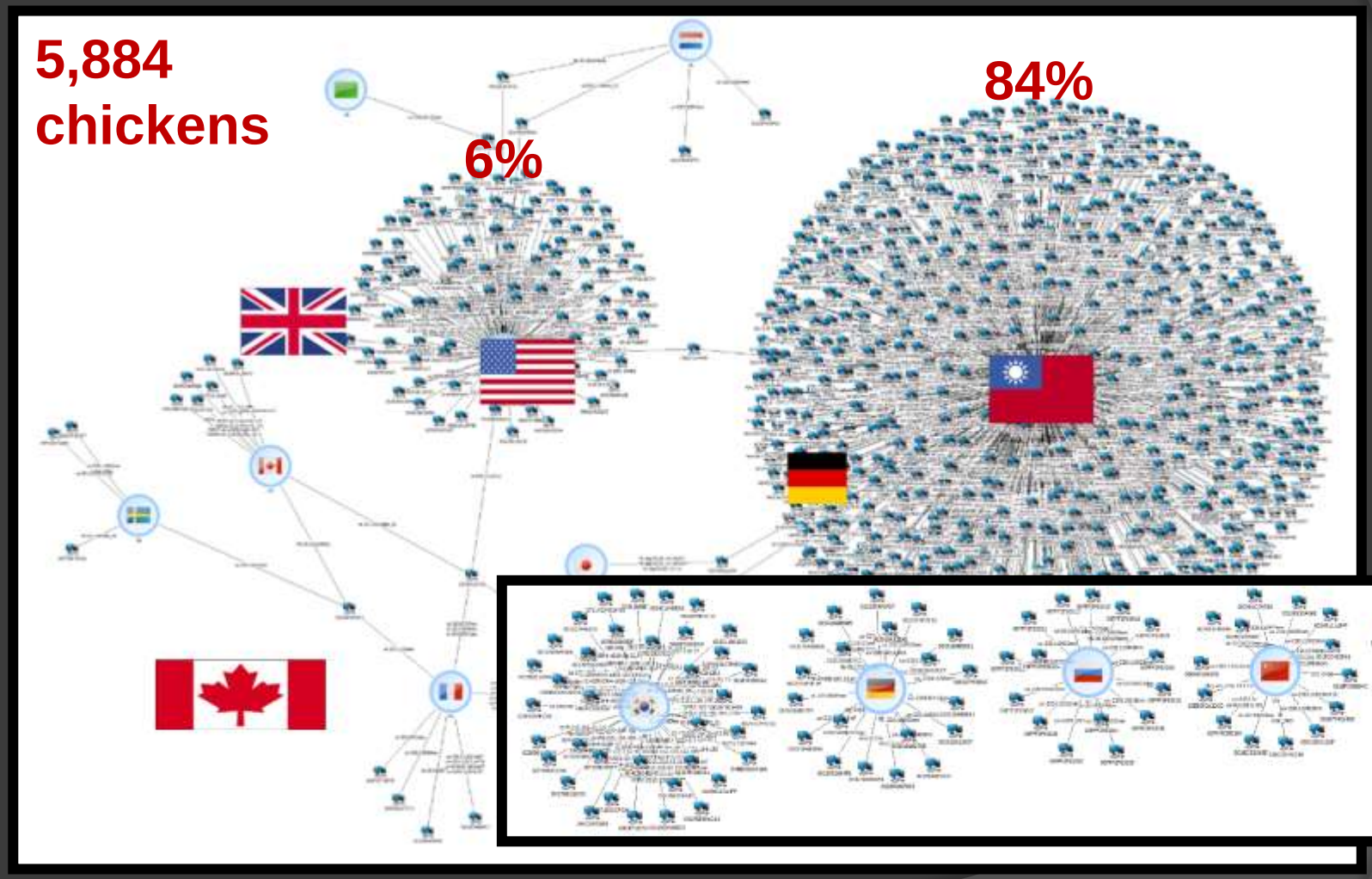


TTP - Hacking follow..

APT101 目前的數據研究

- 在世界各國都有活動，受害者超過30個國家，但以台灣、美國、韓國與大陸最多
- 目前有紀錄的最早活動時間是2007，到目前7月都還在活動
- 他們至少控制過 5800 台電腦
- 約有 25位操作人員
- 操控 4種 Botnet
- 一年半內使用產生器約產生過 210 隻後門程式

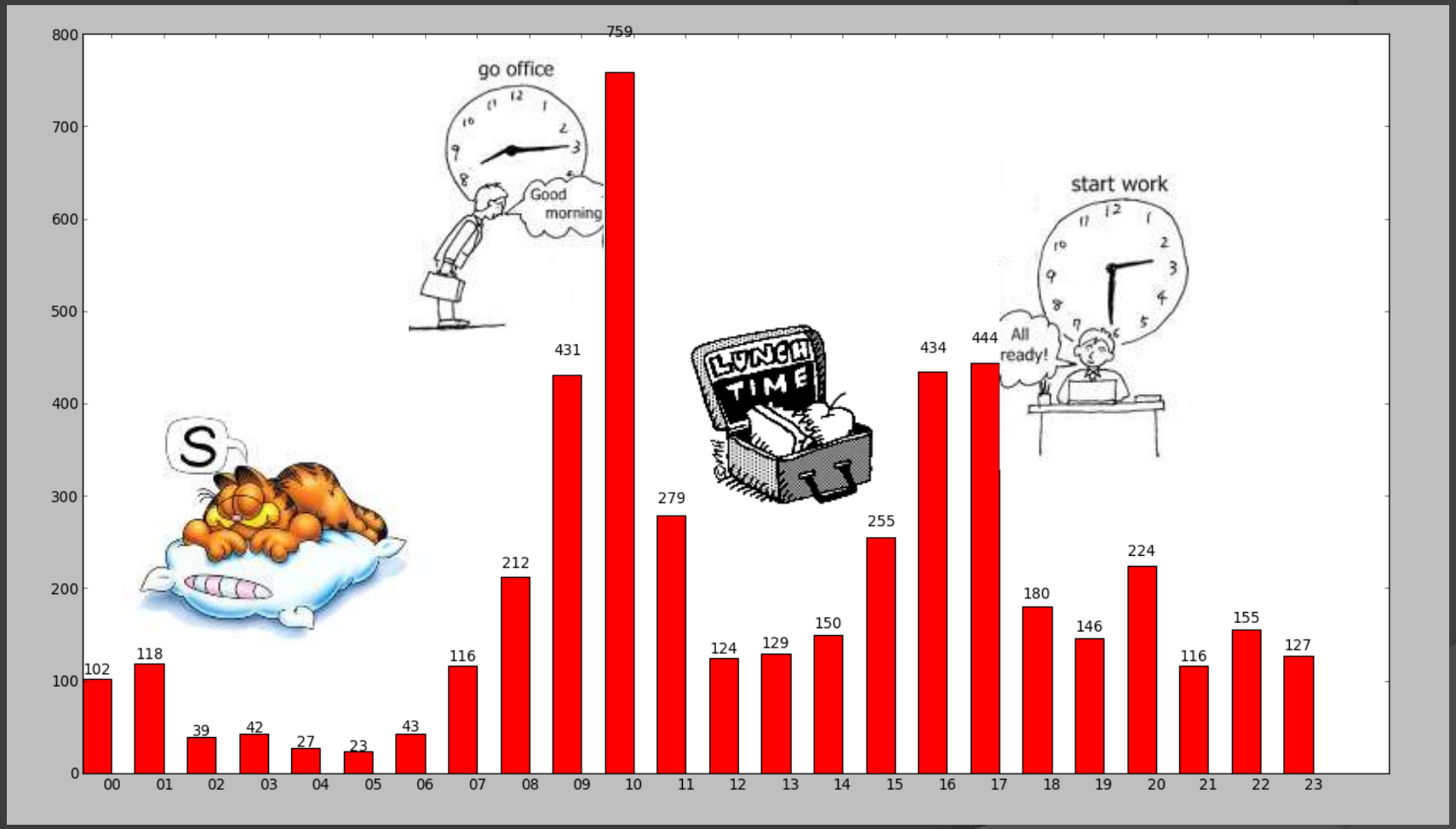
chicken farms went international



When you travel, your chicken travel too… ☺

ANOTHER DISCOVERY!!

.. do have 9 to 5 job ;)…



我們提供

- 我們提供資安研究員免費的 XecScan APT 分析平台帳號，歡迎跟我們申請 http://scan.xecure-lab.com

- 我們也提供分析服務，如果發現APT惡意樣本也歡迎分享

See you at Blackhat 2013 ☺