Don’t Touch My Winny

Moti Joseph

moti@gamepe.com

Who Am I?

- Independent Security researcher
- Previously worked at Websense Security Labs, Checkpoint

  Hunting for vulnerabilities

  Reverse engineering Microsoft patches

  Writing plug-in for IDA and OllyDbg
- Mobile developer
- Founder of the XfMobile project *www.xf-mobile.com*

Agenda

In the next hour, we will cover:

- What is Winny?
- The Story P2P information disclosure in Japan
- Exploiting P2P encrypted traffic

A Day in a life of a Hacker

Reverse engineering , bug hunting, protocol analysis

- Hunting Japanese : Live Demo 0DAY!

NOTE: a talk from a hacker perspective.

Who is Winny ?

NOT *Winny the pooh*

Winny

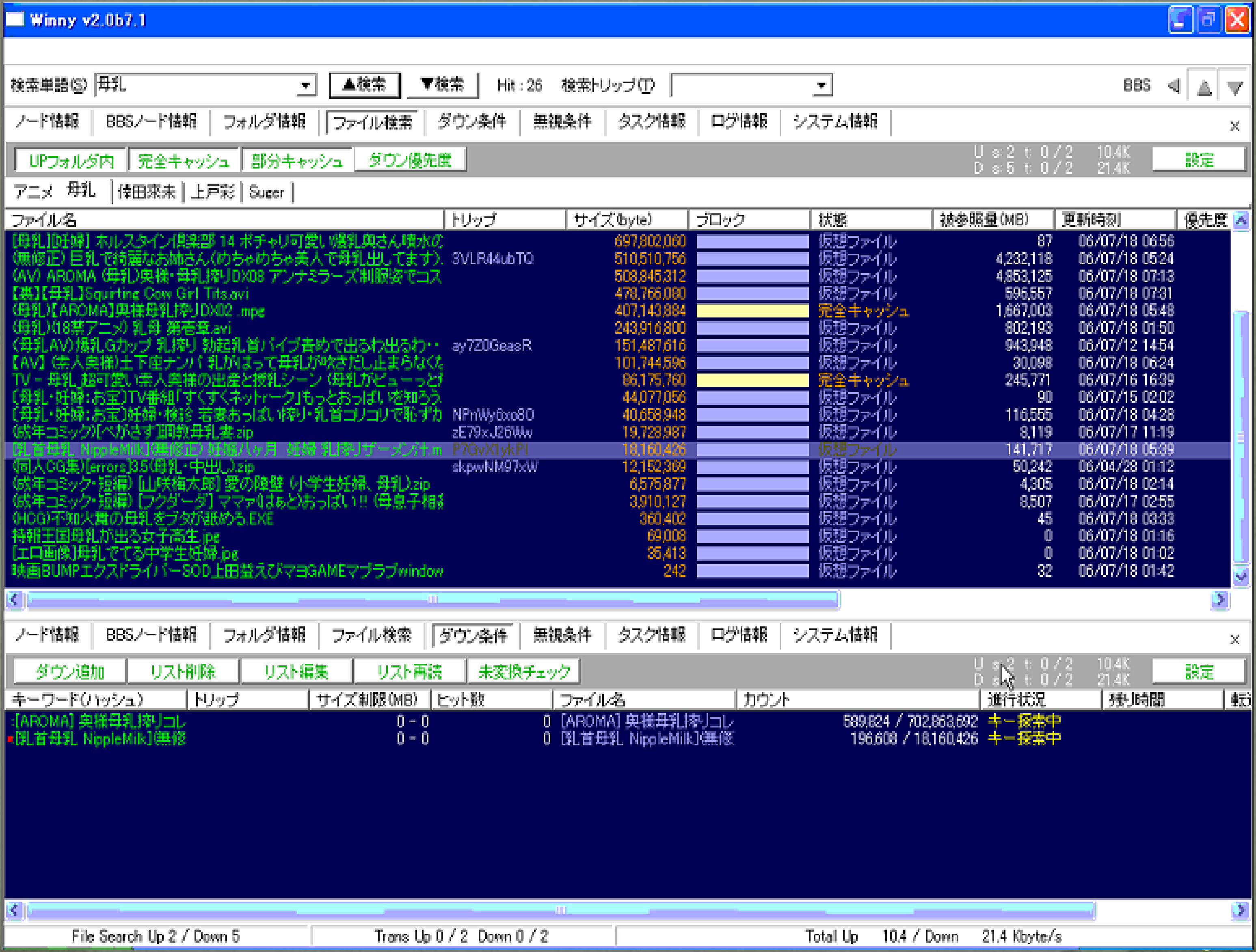
Winny (also known as WinNY) is a Japanese peer-to-peer (P2P) file-sharing program that claims to **keep user identities untraceable**

The software was developed by Isamu Kaneko

A research in a graduate course of computer engineering at the University of Tokyo in Japan.

He was also once a researcher at the Japan Atomic Energy Research Institute also known as "47-shi" ("Mr. 47").

Winny P2P Software



Winny v2.0b7.1

検索単語(S) 母乳 ▲検索 ▼検索 Hit : 26 検索トリップ(T) BBS

ノード情報 | BBSノード情報 | フォルダ情報 | ファイル検索 | ダウン条件 | 無視条件 | タスク情報 | ログ情報 | システム情報

UPフォルダ内 | 完全キャッシュ | 部分キャッシュ | ダウン優先度

U s:2 t:0 / 2 10.4K
D s:5 t:0 / 2 21.4K
設定

アニメ 母乳 | 倖田來未 | 上戸彩 | Suger |

ファイル名	トリップ	サイズ(byte)	ブロック	状態	被参照量(MB)	更新時刻	優先度
[母乳][妊婦] ホルスタイン倶楽部 14 ポチャリ可愛い爆乳奥さん噴水の		697,802,060		仮想ファイル	87	06/07/18 06:56	
(無修正) 巨乳で綺麗なお姉さん(めちゃめちゃ美人で母乳出してます).	3VLR44ubTQ	510,510,756		仮想ファイル	4,232,118	06/07/18 05:24	
(AV) AROMA (母乳)奥様・母乳搾りDX08 アンナミラーズ制服姿でコス		508,845,312		仮想ファイル	4,853,125	06/07/18 07:13	
【洋】【母乳】Squirting Cow Girl Tits.avi		478,766,080		仮想ファイル	596,557	06/07/18 07:31	
(母乳)【AROMA】奥様母乳搾りDX02 .mpe		407,143,884		完全キャッシュ	1,667,003	06/07/18 05:48	
(母乳)(18禁アニメ) 乳母 第壱章.avi		243,916,800		仮想ファイル	802,193	06/07/18 01:50	
(母乳AV)爆乳Gカップ 乳搾り 勃起乳首バイブ責めで出るわ出るわ・・	ay7Z0GeasR	151,487,616		仮想ファイル	943,948	06/07/12 14:54	
【AV】(素人奥様)土下座ナンパ 乳が張って母乳が吹きだし止まらなくた		101,744,596		仮想ファイル	30,098	06/07/18 06:24	
TV - 母乳 超可愛い素人奥様の出産と授乳シーン (母乳がピューっと!		86,175,760		完全キャッシュ	245,771	06/07/16 16:39	
(母乳・妊婦:お宝)TV番組「すくすくネットワーク」もっとおっぱいを知ろう.		44,077,056		仮想ファイル	90	06/07/15 02:02	
(母乳・妊婦:お宝)妊婦・検診 若妻おっぱい搾り・乳首コリコリで恥ずか	NPnWy6xo80	40,658,948		仮想ファイル	116,555	06/07/18 04:28	
(成年コミック)[ぺがさす宣]調教母乳妻.zip	zE79xJ26Ww	19,728,987		仮想ファイル	8,119	06/07/17 11:19	
[乳首母乳 NippleMilk](無修正) 妊娠八ヶ月 妊婦 乳搾りザーメン汁.m	P7GvX1ykPI	18,160,426		仮想ファイル	141,717	06/07/18 05:39	
(同人CG集)[errors]35(母乳・中出し).zip	skpwNM97xW	12,152,369		仮想ファイル	50,242	06/04/28 01:12	
(成年コミック・短編) [山咲梅太郎] 愛の障壁 (小学生妊婦、母乳).zip		6,575,877		仮想ファイル	4,305	06/07/18 02:14	
(成年コミック・短編) [フクダーダ] ママァ(はぁと)おっぱい!! (母息子相		3,910,127		仮想ファイル	8,507	06/07/17 02:55	
(HCG)不知火舞の母乳をブタが舐める.EXE		360,402		仮想ファイル	45	06/07/18 03:33	
特報王国母乳が出る女子高生.jpe		69,008		仮想ファイル	0	06/07/18 01:16	
[エロ画像]母乳でてる中学生妊婦.jpe		35,413		仮想ファイル	0	06/07/18 01:02	
映画BUMPエクスドライバーSOD上田益えびマヨGAMEマブラブwindow		242		仮想ファイル	32	06/07/18 01:42	

ノード情報 | BBSノード情報 | フォルダ情報 | ファイル検索 | ダウン条件 | 無視条件 | タスク情報 | ログ情報 | システム情報

ダウン追加 | リスト削除 | リスト編集 | リスト再読 | 未変換チェック

U s:2 t:0 / 2 10.4K
D s:2 t:0 / 2 21.4K
設定

キーワード(ハッシュ)	トリップ	サイズ制限(MB)	ヒット数	ファイル名	カウント	進行状況	残り時間	転
:[AROMA] 奥様母乳搾りコレ		0 - 0	0	[AROMA] 奥様母乳搾りコレ	589,824 / 702,863,692	キー探索中		
[乳首母乳 NippleMilk](無修		0 - 0	0	[乳首母乳 NippleMilk](無修	196,608 / 18,160,426	キー探索中		

File Search Up 2 / Down 5 | Trans Up 0 / 2 Down 0 / 2 | Total Up 10.4 / Down 21.4 Kbyte/s

Winny Developer

So what's the story ?

On November 28, 2003, two Japanese users of Winny :

Yoshihiro Inoue, a 41 year-old self employed businessman from Takasaki , and an unemployed 19-year old from Matsuyama ,

were accused of sharing copyrighted material via Winny and admitted to their crimes.

Shortly following the two users' arrests,
Kaneko also had his home searched and had the source code of Winny confiscated by the Kyoto Police

Chapter 1

August 2003 : Several worms called "Antinny" spread on the winny network.

Some versions of ***Antinny*** work as follows:

Upload files in the computer onto the winny network.

Upload screenshots onto an image board.

Denial-of-service attack to a copyright protecting agency web site.

That information includes governmental documents, information about customers, and people's private files.

Chapter 2

Arguably the biggest winny-related leak however,
is that of the ***Okayama Police Force***,
whose computer leaked data on around 1,500
investigations.

This information included sensitive data ,
such as the names of sex crime victims,
and is the largest amount of information held by
Japanese police to have ever leaked online.

December 13, 2006

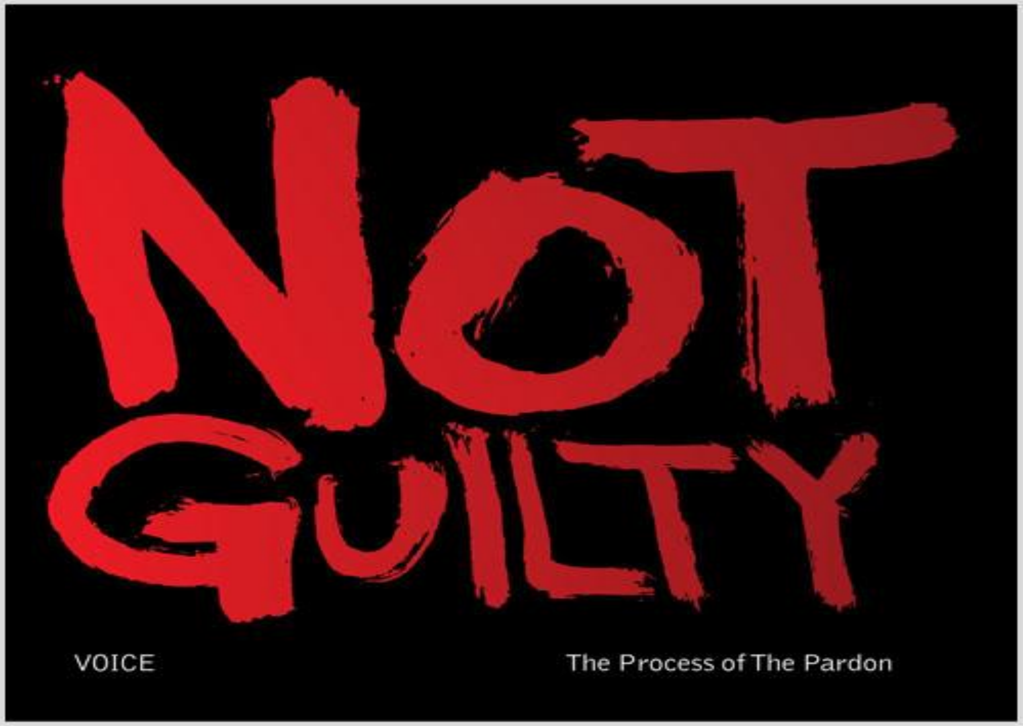
Winny Developer gets fined $12,500

The creator of WinNY, the Japanese P2P file-sharing program, has been convicted in Kyoto District Court of assisting in copyright infringement.

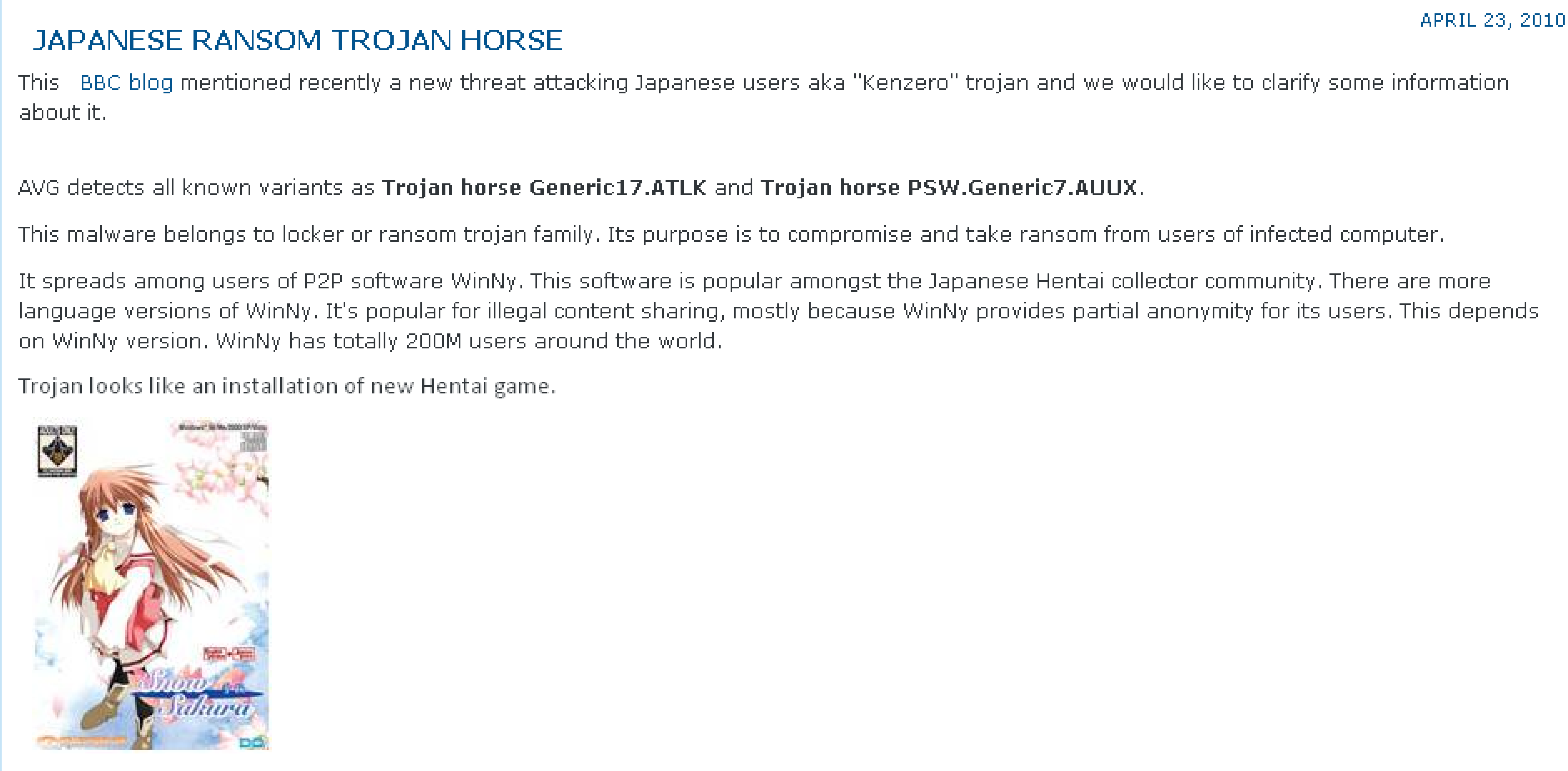
October 8, 2009

Winny Developer found not guilty

Judge Ogura at Osaka High Court found Isamu Kaneko, a developer of Winny, not guilty today, reversing the guilty ruling of 1.5 million yen fine made by the lower court.



April 2010 Winny Trojan



APRIL 23, 2010

JAPANESE RANSOM TROJAN HORSE

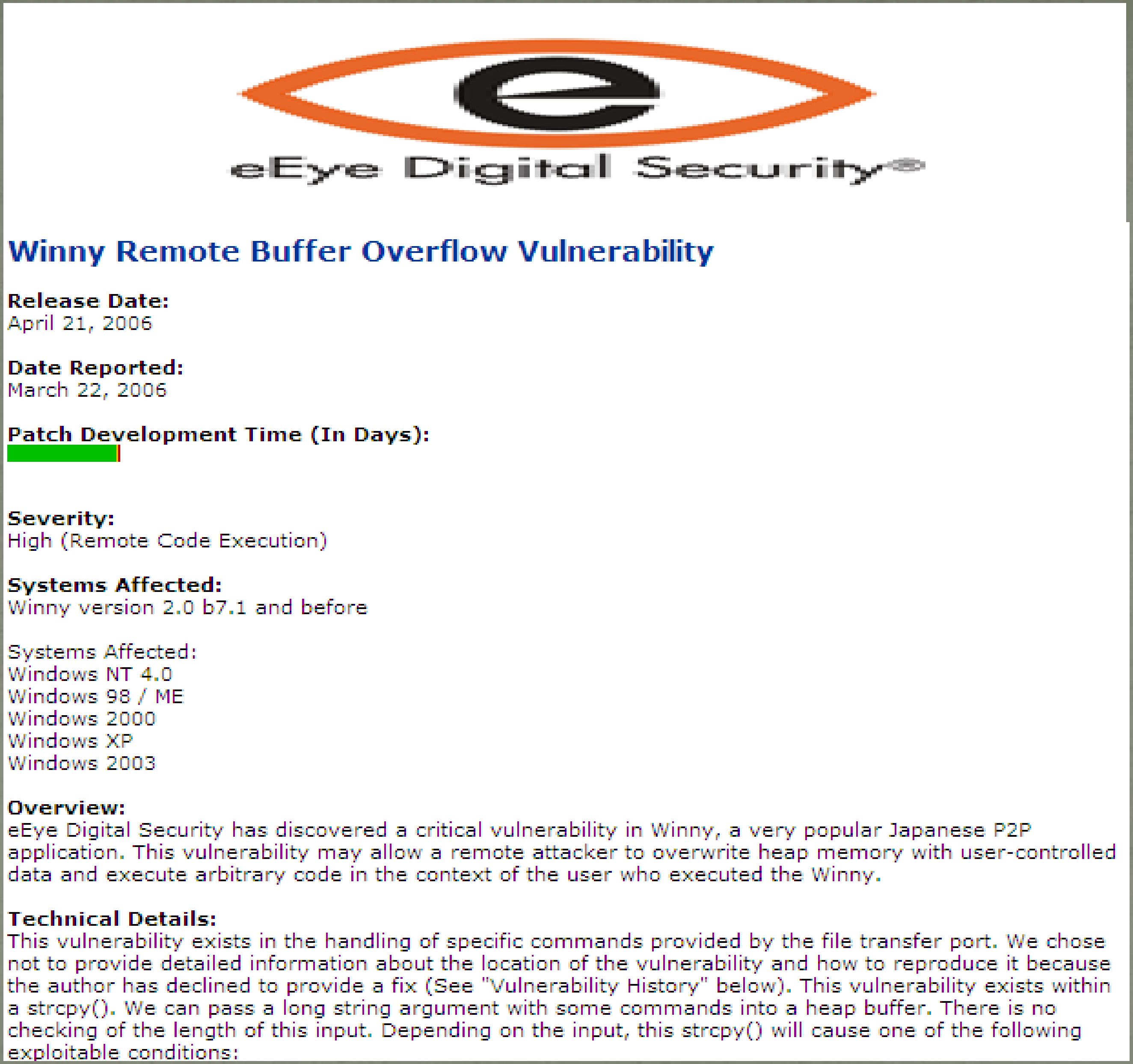
This BBC blog mentioned recently a new threat attacking Japanese users aka "Kenzero" trojan and we would like to clarify some information about it.

AVG detects all known variants as **Trojan horse Generic17.ATLK** and **Trojan horse PSW.Generic7.AUUX**.

This malware belongs to locker or ransom trojan family. Its purpose is to compromise and take ransom from users of infected computer.

It spreads among users of P2P software WinNy. This software is popular amongst the Japanese Hentai collector community. There are more language versions of WinNy. It's popular for illegal content sharing, mostly because WinNy provides partial anonymity for its users. This depends on WinNy version. WinNy has totally 200M users around the world.

Trojan looks like an installation of new Hentai game.



eEye Digital Security®

Winny Remote Buffer Overflow Vulnerability

Release Date:
April 21, 2006

Date Reported:
March 22, 2006

Patch Development Time (In Days):

Severity:
High (Remote Code Execution)

Systems Affected:
Winny version 2.0 b7.1 and before

Systems Affected:
Windows NT 4.0
Windows 98 / ME
Windows 2000
Windows XP
Windows 2003

Overview:
eEye Digital Security has discovered a critical vulnerability in Winny, a very popular Japanese P2P application. This vulnerability may allow a remote attacker to overwrite heap memory with user-controlled data and execute arbitrary code in the context of the user who executed the Winny.

Technical Details:
This vulnerability exists in the handling of specific commands provided by the file transfer port. We chose not to provide detailed information about the location of the vulnerability and how to reproduce it because the author has declined to provide a fix (See "Vulnerability History" below). This vulnerability exists within a strcpy(). We can pass a long string argument with some commands into a heap buffer. There is no checking of the length of this input. Depending on the input, this strcpy() will cause one of the following exploitable conditions:

The Story that never been told !!!

0day for the WinNY !

Today i will disclose my private 0day

Universal exploit : stack based buffer overflow

remote code execution

Day in Reverse World

The challenge :

- Reverse engineering

- bug hunting

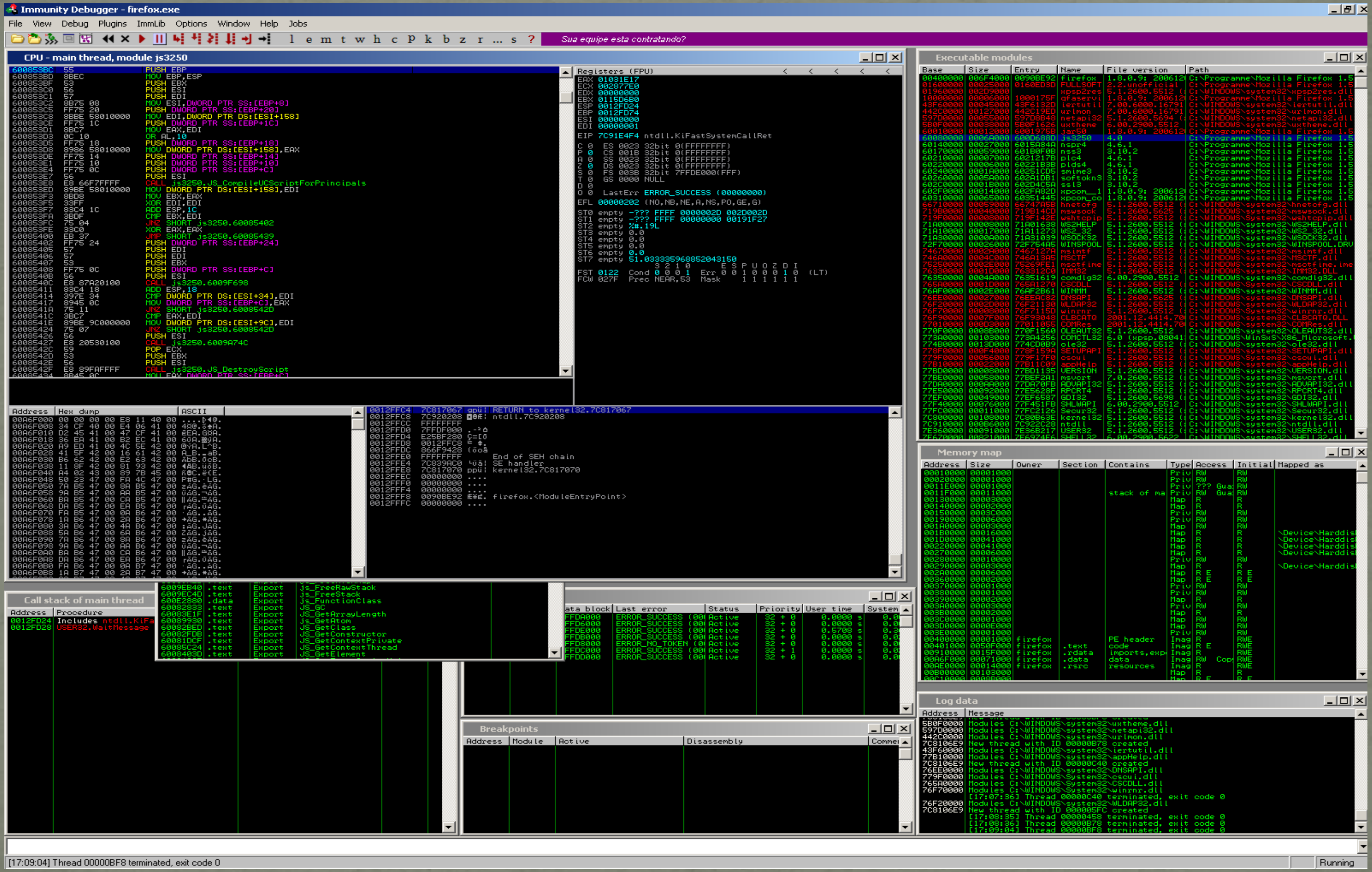
- protocol analysis

- writing the exploit

Tools we are going to use …

A zero-day (or zero-hour) attack or threat is a computer threat that tries to exploit computer software vulnerabilities
which are unknown to others, undisclosed to the software vendor, or without an available security fix

Immunity debugger


Immunity Debugger - firefox.exe
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Sua equipe esta contratando?

CPU - main thread, module js3250

```
600853BC  55              PUSH EBP
600853BD  8BEC            MOV EBP,ESP
600853BF  53              PUSH EBX
600853C0  56              PUSH ESI
600853C1  57              PUSH EDI
600853C2  8B75 08         MOV ESI,DWORD PTR SS:[EBP+8]
600853C5  FF75 20         PUSH DWORD PTR SS:[EBP+20]
600853C8  8BBE 58010000   MOV EDI,DWORD PTR DS:[ESI+158]
600853CE  FF75 1C         PUSH DWORD PTR SS:[EBP+1C]
600853D1  8BC7            MOV EAX,EDI
600853D3  0C 10           OR AL,10
600853D5  FF75 18         PUSH DWORD PTR SS:[EBP+18]
600853D8  8986 58010000   MOV DWORD PTR DS:[ESI+158],EAX
600853DE  FF75 14         PUSH DWORD PTR SS:[EBP+14]
600853E1  FF75 10         PUSH DWORD PTR SS:[EBP+10]
600853E4  FF75 0C         PUSH DWORD PTR SS:[EBP+C]
600853E7  56              PUSH ESI
600853E8  E8 66F7FFFF     CALL js3250.JS_CompileUCScriptForPrincipals
600853ED  89BE 58010000   MOV DWORD PTR DS:[ESI+158],EDI
600853F3  8BD8            MOV EBX,EAX
600853F5  33FF            XOR EDI,EDI
600853F7  83C4 1C         ADD ESP,1C
600853FA  3BDF            CMP EBX,EDI
600853FC  75 04           JNZ SHORT js3250.60085402
600853FE  33C0            XOR EAX,EAX
60085400  EB 37           JMP SHORT js3250.60085439
60085402  FF75 24         PUSH DWORD PTR SS:[EBP+24]
60085405  57              PUSH EDI
60085406  57              PUSH EDI
60085407  53              PUSH EBX
60085408  FF75 0C         PUSH DWORD PTR SS:[EBP+C]
6008540B  56              PUSH ESI
6008540C  E8 87A20100     CALL js3250.6009F698
60085411  83C4 18         ADD ESP,18
60085414  397E 34         CMP DWORD PTR DS:[ESI+34],EDI
60085417  8945 0C         MOV DWORD PTR SS:[EBP+C],EAX
6008541A  75 11           JNZ SHORT js3250.6008542D
6008541C  3BC7            CMP EAX,EDI
6008541E  89BE 9C000000   MOV DWORD PTR DS:[ESI+9C],EDI
60085424  75 07           JNZ SHORT js3250.6008542D
60085426  56              PUSH ESI
60085427  E8 20530100     CALL js3250.6009A74C
6008542C  59              POP ECX
6008542D  53              PUSH EBX
6008542E  56              PUSH ESI
6008542F  E8 89FAFFFF     CALL js3250.JS_DestroyScript
```

```
Registers (FPU)
EAX 01031E17
ECX 002877E0
EDX 00000000
EBX 0115D6B0
ESP 0012FD24
EBP 0012FD74
ESI 00000000
EDI 00000001

EIP 7C91E4F4 ntdll.KiFastSystemCallRet

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty -??? FFFF 0000002D 002D002D
ST1 empty -??? FFFF 00000000 00191F27
ST2 empty %#.19L
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 51.033335968852043150
               3 2 1 0      E S P U O Z D I
FST 0122  Cond 0 0 0 1  Err 0 0 1 0 0 0 1 0  (LT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                 ASCII
00A6F000  00 00 00 00 E8 11 40 00  ....Þ◄@.
00A6F008  34 CF 40 00 E4 06 41 00  4¤@.õ♠A.
00A6F010  D2 45 41 00 47 CF 41 00  ÊEA.G¤A.
00A6F018  36 EA 41 00 B2 EC 41 00  6ÛA.▓ýA.
00A6F020  A9 ED 41 00 4C 5E 42 00  ®ÝA.L^B.
00A6F028  41 5F 42 00 16 61 42 00  A_B.▬aB.
00A6F030  B6 62 42 00 E2 63 42 00  ÂbB.ÔcB.
00A6F038  11 8F 42 00 81 93 42 00  ◄ÅB.üôB.
00A6F040  A4 02 43 00 89 7B 45 00  ñ☻C.ë{E.
00A6F048  50 23 47 00 FA 4C 47 00  P#G.·LG.
00A6F050  7A B5 47 00 8A B5 47 00  zÁG.èÁG.
00A6F058  9A B5 47 00 AA B5 47 00  ÜÁG.¬ÁG.
00A6F060  BA B5 47 00 CA B5 47 00  ║ÁG.╩ÁG.
00A6F068  DA B5 47 00 EA B5 47 00  ┌ÁG.ÛÁG.
00A6F070  FA B5 47 00 0A B6 47 00  ·ÁG..ÂG.
00A6F078  1A B6 47 00 2A B6 47 00  →ÂG.*ÂG.
00A6F080  3A B6 47 00 4A B6 47 00  :ÂG.JÂG.
00A6F088  5A B6 47 00 6A B6 47 00  ZÂG.jÂG.
00A6F090  7A B6 47 00 8A B6 47 00  zÂG.èÂG.
00A6F098  9A B6 47 00 AA B6 47 00  ÜÂG.¬ÂG.
00A6F0A0  BA B6 47 00 CA B6 47 00  ║ÂG.╩ÂG.
00A6F0A8  DA B6 47 00 EA B6 47 00  ┌ÂG.ÛÂG.
00A6F0B0  FA B6 47 00 0A B7 47 00  ·ÂG..ÀG.
00A6F0B8  1A B7 47 00 2A B7 47 00  →ÀG.*ÀG.
```

```
0012FFC4  7C817067  gpü¦  RETURN to kernel32.7C817067
0012FFC8  7C920208  ■●Æ¦  ntdll.7C920208
0012FFCC  FFFFFFFF
0012FFD0  7FFDF000  .-²⌂
0012FFD4  E25BF280  Ç=[Õ
0012FFD8  0012FFC8  ╚ ‡.
0012FFDC  866F9428  (öoå
0012FFE0  FFFFFFFF        End of SEH chain
0012FFE4  7C839AC0  └üä¦  SE handler
0012FFE8  7C817070  ppü¦  kernel32.7C817070
0012FFEC  00000000  ....
0012FFF0  00000000  ....
0012FFF4  00000000  ....
0012FFF8  0090BE92  Æ¥É.  firefox.<ModuleEntryPoint>
0012FFFC  00000000  ....
```

Call stack of main thread

```
Address   Procedure
0012FD24  Includes ntdll.KiFa
0012FD28  USER32.WaitMessage
```

```
6009EB40  .text  Export  js_FreeRawStack
6009EC4D  .text  Export  js_FreeStack
600E2880  .data  Export  js_FunctionClass
60082833  .text  Export  JS_GC
60083E1F  .text  Export  JS_GetArrayLength
60089930  .text  Export  js_GetAtom
60082BED  .text  Export  JS_GetClass
60082FDB  .text  Export  JS_GetConstructor
60081DCF  .text  Export  JS_GetContextPrivate
60085C24  .text  Export  JS_GetContextThread
6008403D  .text  Export  JS_GetElement
```

```
ata block  Last error            Status  Priority  User time   System
FFDA000    ERROR_SUCCESS (00(    Active  32 + 0    0.0000 s    0.0(
FFD6000    ERROR_SUCCESS (00(    Active  32 + 0    0.0000 s    0.0(
FFDE000    ERROR_SUCCESS (00(    Active  32 + 0    0.5708 s    0.3(
FFDB000    ERROR_SUCCESS (00(    Active  32 + 0    0.0000 s    0.0(
FFD8000    ERROR_NO_TOKEN (0(    Active  32 + 0    0.0000 s    0.0(
FFDC000    ERROR_SUCCESS (00(    Active  32 + 1    0.0000 s    0.0(
FFDD000    ERROR_SUCCESS (00(    Active  32 + 0    0.0000 s    0.0(
```

Breakpoints

```
Address  Module  Active  Disassembly  Commen
```

Executable modules

```
Base      Size      Entry     Name      File version      Path
00400000  006F4000  0090BE92  firefox   1.8.0.9: 200612(  C:\Programme\Mozilla Firefox 1.5
01600000  00025000  0160ED3D  FULLSOFT  2.2.unofficial    C:\Programme\Mozilla Firefox 1.5
01960000  002D9000            xpsp2res  5.1.2600.5512 (:  C:\WINDOWS\system32\xpsp2res.dll
10000000  00006000  1000175F  qfaservi  1.8.0.9: 200612(  C:\Programme\Mozilla Firefox 1.5
43F60000  00045000  43F6132D  iertutil  7.00.6000.16791   C:\WINDOWS\system32\iertutil.dll
442C0000  00127000  442C19ED  urlmon    7.00.6000.16791   C:\WINDOWS\system32\urlmon.dll
597D0000  00055000  597D8B48  netapi32  5.1.2600.5694 (:  C:\WINDOWS\system32\netapi32.dll
5B0F0000  00038000  5B0F1626  uxtheme   6.00.2900.5512    C:\WINDOWS\system32\uxtheme.dll
60010000  00012000  6001975B  jar50     1.8.0.9: 200612(  C:\Programme\Mozilla Firefox 1.5
60080000  0006A000  600D688D  js3250    4.0               C:\Programme\Mozilla Firefox 1.5
60140000  00027000  6015A84A  nspr4     4.6.1             C:\Programme\Mozilla Firefox 1.5
60170000  00059000  601B0F0B  nss3      3.10.2            C:\Programme\Mozilla Firefox 1.5
60210000  00007000  6021217B  plc4      4.6.1             C:\Programme\Mozilla Firefox 1.5
60220000  00006000  60221B3B  plds4     4.6.1             C:\Programme\Mozilla Firefox 1.5
60240000  0001A000  60251CD5  smime3    3.10.2            C:\Programme\Mozilla Firefox 1.5
60260000  0005A000  602A1DB1  softokn3  3.10.2            C:\Programme\Mozilla Firefox 1.5
602C0000  0001B000  602D4C5A  ssl3      3.10.2            C:\Programme\Mozilla Firefox 1.5
602F0000  00014000  602FA82D  xpcom__1  1.8.0.9: 200612(  C:\Programme\Mozilla Firefox 1.5
60310000  00065000  60351445  xpcom_co  1.8.0.9: 200612(  C:\Programme\Mozilla Firefox 1.5
66710000  00059000  66747A5B  hnetcfg   5.1.2600.5512 (:  C:\WINDOWS\system32\hnetcfg.dll
719B0000  00040000  719B14CD  mswsock   5.1.2600.5625 (:  C:\WINDOWS\system32\mswsock.dll
719F0000  00008000  719F142E  wshtcpip  5.1.2600.5512 (:  C:\WINDOWS\System32\wshtcpip.dll
71A00000  00008000  71A01638  WS2HELP   5.1.2600.5512 (:  C:\WINDOWS\system32\WS2HELP.dll
71A10000  00017000  71A11273  WS2_32    5.1.2600.5512 (:  C:\WINDOWS\system32\WS2_32.dll
71A30000  0000A000  71A31039  WSOCK32   5.1.2600.5512 (:  C:\WINDOWS\system32\WSOCK32.dll
72F70000  00026000  72F754A5  WINSPOOL  5.1.2600.5512 (:  C:\WINDOWS\system32\WINSPOOL.DRV
74670000  0002A000  7467127A  msimtf    5.1.2600.5512 (:  C:\WINDOWS\system32\msimtf.dll
746A0000  0004C000  746A13A5  MSCTF     5.1.2600.5512 (:  C:\WINDOWS\system32\MSCTF.dll
75250000  0002E000  75269FE1  msctfime  5.1.2600.5512 (:  C:\WINDOWS\system32\msctfime.ime
76330000  0001D000  763312C0  IMM32     5.1.2600.5512 (:  C:\WINDOWS\system32\IMM32.DLL
76350000  0004A000  76351619  comdlg32  6.00.2900.5512    C:\WINDOWS\system32\comdlg32.dll
765A0000  0001D000  765A1270  CSCDLL    5.1.2600.5512 (:  C:\WINDOWS\System32\CSCDLL.dll
76AF0000  0002E000  76AF2B61  WINMM     5.1.2600.5512 (:  C:\WINDOWS\system32\WINMM.dll
76EE0000  00027000  76EEAC82  DNSAPI    5.1.2600.5625 (:  C:\WINDOWS\system32\DNSAPI.dll
76F20000  0002D000  76F21130  WLDAP32   5.1.2600.5512 (:  C:\WINDOWS\system32\WLDAP32.dll
76F70000  00008000  76F7115D  winrnr    5.1.2600.5512 (:  C:\WINDOWS\System32\winrnr.dll
76F90000  0007F000  76F93048  CLBCATQ   2001.12.4414.70(  C:\WINDOWS\system32\CLBCATQ.DLL
77010000  000D3000  77011055  COMRes    2001.12.4414.70(  C:\WINDOWS\system32\COMRes.dll
770F0000  0008B000  770F1560  OLEAUT32  5.1.2600.5512     C:\WINDOWS\system32\OLEAUT32.dll
773A0000  00103000  773A4256  COMCTL32  6.0 (xpsp.08041:  C:\WINDOWS\WinSxS\X86_Microsoft.
774B0000  0013D000  774CD0B9  ole32     5.1.2600.5512 (:  C:\WINDOWS\system32\ole32.dll
778F0000  000F4000  778F159A  SETUPAPI  5.1.2600.5512 (:  C:\WINDOWS\system32\SETUPAPI.dll
779F0000  00056000  779F17F0  cscui     5.1.2600.5512 (:  C:\WINDOWS\System32\cscui.dll
77B10000  00022000  77B11C09  appHelp   5.1.2600.5512 (:  C:\WINDOWS\system32\appHelp.dll
77BD0000  00008000  77BD1135  VERSION   5.1.2600.5512 (:  C:\WINDOWS\system32\VERSION.dll
77BE0000  00058000  77BEF2A1  msvcrt    7.0.2600.5512 (:  C:\WINDOWS\system32\msvcrt.dll
77DA0000  000AA000  77DA70FB  ADVAPI32  5.1.2600.5512 (:  C:\WINDOWS\system32\ADVAPI32.dll
77E50000  00092000  77E5628F  RPCRT4    5.1.2600.5512 (:  C:\WINDOWS\system32\RPCRT4.dll
77EF0000  00049000  77EF6587  GDI32     5.1.2600.5698 (:  C:\WINDOWS\system32\GDI32.dll
77F40000  00076000  77F451FB  SHLWAPI   6.00.2900.5512    C:\WINDOWS\system32\SHLWAPI.dll
77FC0000  00011000  77FC2126  Secur32   5.1.2600.5512 (:  C:\WINDOWS\system32\Secur32.dll
7C800000  00108000  7C80B63E  kernel32  5.1.2600.5512 (:  C:\WINDOWS\system32\kernel32.dll
7C910000  000B6000  7C922C28  ntdll     5.1.2600.5512 (:  C:\WINDOWS\system32\ntdll.dll
7E360000  00091000  7E36B217  USER32    5.1.2600.5512 (:  C:\WINDOWS\system32\USER32.dll
```

Memory map

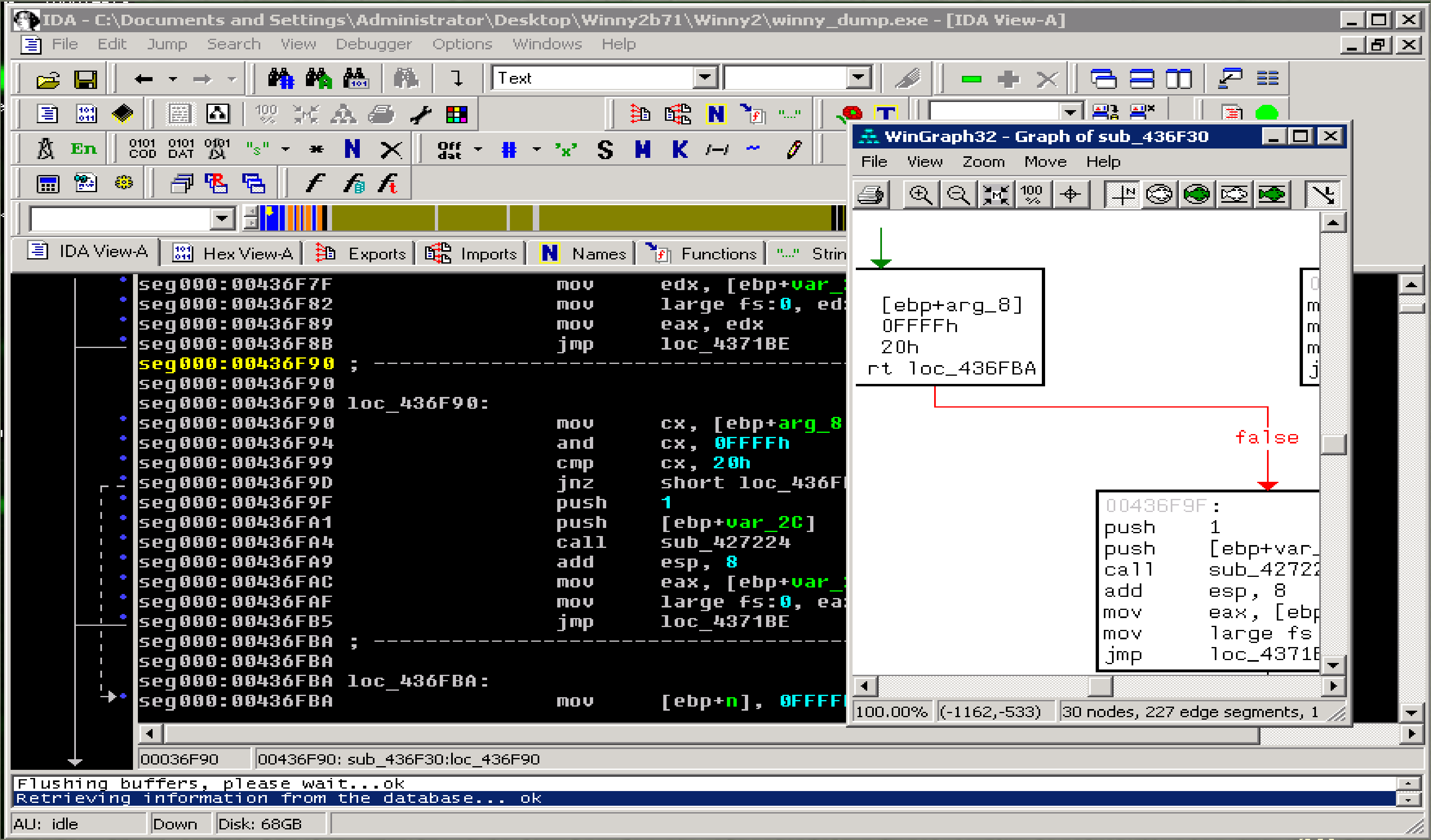
```
Address   Size      Owner    Section  Contains         Type  Access    Initial  Mapped as
00010000  00001000                                     Priv  RW        RW
00020000  00001000                                     Priv  RW        RW
0011E000  00001000                                     Priv  ??? Gua:  RW
0011F000  00011000                    stack of ma      Priv  RW  Gua:  RW
00130000  00003000                                     Map   R         R
00140000  00002000                                     Map   R         R
00150000  0003C000                                     Priv  RW        RW
00190000  00006000                                     Priv  RW        RW
001A0000  00003000                                     Map   RW        RW
001B0000  00016000                                     Map   R         R        \Device\Harddisk
001D0000  00041000                                     Map   R         R        \Device\Harddisk
00220000  00041000                                     Map   R         R        \Device\Harddisk
00270000  00006000                                     Map   R         R        \Device\Harddisk
00280000  00010000                                     Priv  RW        RW
00290000  00003000                                     Map   R         R        \Device\Harddisk
002A0000  00006000                                     Map   R E       R E
00360000  00002000                                     Map   R E       R E
00370000  00001000                                     Priv  RW        RW
00380000  00001000                                     Priv  RW        RW
00390000  00002000                                     Map   R         R
003A0000  00003000                                     Priv  RW        RW
003B0000  00002000                                     Map   R         R
003C0000  00001000                                     Map   RW        RW
003D0000  0000E000                                     Map   RW        RW
003E0000  00001000                                     Priv  RW        RW
00400000  00001000  firefox           PE header        Imag  R         RWE
00401000  0050F000  firefox  .text    code             Imag  R E       RWE
00910000  0015F000  firefox  .rdata   imports,exp(     Imag  R         RWE
00A6F000  00071000  firefox  .data    data             Imag  RW  Cop:  RWE
00AE0000  00014000  firefox  .rsrc    resources        Imag  R         RWE
00B00000  00103000                                     Map   R         R
```

Log data

```
Address   Message
5B0F0000  Modules C:\WINDOWS\system32\uxtheme.dll
597D0000  Modules C:\WINDOWS\system32\netapi32.dll
442C0000  Modules C:\WINDOWS\system32\urlmon.dll
7C8106E9  New thread with ID 00000B78 created
43F60000  Modules C:\WINDOWS\system32\iertutil.dll
77B10000  Modules C:\WINDOWS\system32\appHelp.dll
7C8106E9  New thread with ID 00000C40 created
76EE0000  Modules C:\WINDOWS\system32\DNSAPI.dll
779F0000  Modules C:\WINDOWS\System32\cscui.dll
765A0000  Modules C:\WINDOWS\System32\CSCDLL.dll
76F70000  Modules C:\WINDOWS\System32\winrnr.dll
          [17:07:36] Thread 00000C40 terminated, exit code 0
76F20000  Modules C:\WINDOWS\system32\WLDAP32.dll
7C8106E9  New thread with ID 000005FC created
          [17:08:35] Thread 00000458 terminated, exit code 0
          [17:08:36] Thread 00000B78 terminated, exit code 0
          [17:09:04] Thread 00000BF8 terminated, exit code 0
```

```
[17:09:04] Thread 00000BF8 terminated, exit code 0        Running
```

IDA PRO 5 DISASSEMBLER



IDA - C:\Documents and Settings\Administrator\Desktop\Winny2b71\Winny2\winny_dump.exe - [IDA View-A]

```
seg000:00436F7F                 mov     edx, [ebp+var_
seg000:00436F82                 mov     large fs:0, ed
seg000:00436F89                 mov     eax, edx
seg000:00436F8B                 jmp     loc_4371BE
seg000:00436F90 ; ---------------------------------
seg000:00436F90
seg000:00436F90 loc_436F90:
seg000:00436F90                 mov     cx, [ebp+arg_8
seg000:00436F94                 and     cx, 0FFFFh
seg000:00436F99                 cmp     cx, 20h
seg000:00436F9D                 jnz     short loc_436F
seg000:00436F9F                 push    1
seg000:00436FA1                 push    [ebp+var_2C]
seg000:00436FA4                 call    sub_427224
seg000:00436FA9                 add     esp, 8
seg000:00436FAC                 mov     eax, [ebp+var_
seg000:00436FAF                 mov     large fs:0, ea
seg000:00436FB5                 jmp     loc_4371BE
seg000:00436FBA ; ---------------------------------
seg000:00436FBA
seg000:00436FBA loc_436FBA:
seg000:00436FBA                 mov     [ebp+n], 0FFFF
```

WinGraph32 - Graph of sub_436F30

```
 [ebp+arg_8]
 0FFFFh
 20h
rt loc_436FBA
```

```
00436F9F:
push    1
push    [ebp+var_
call    sub_42722
add     esp, 8
mov     eax, [ebp
mov     large fs
jmp     loc_4371E
```

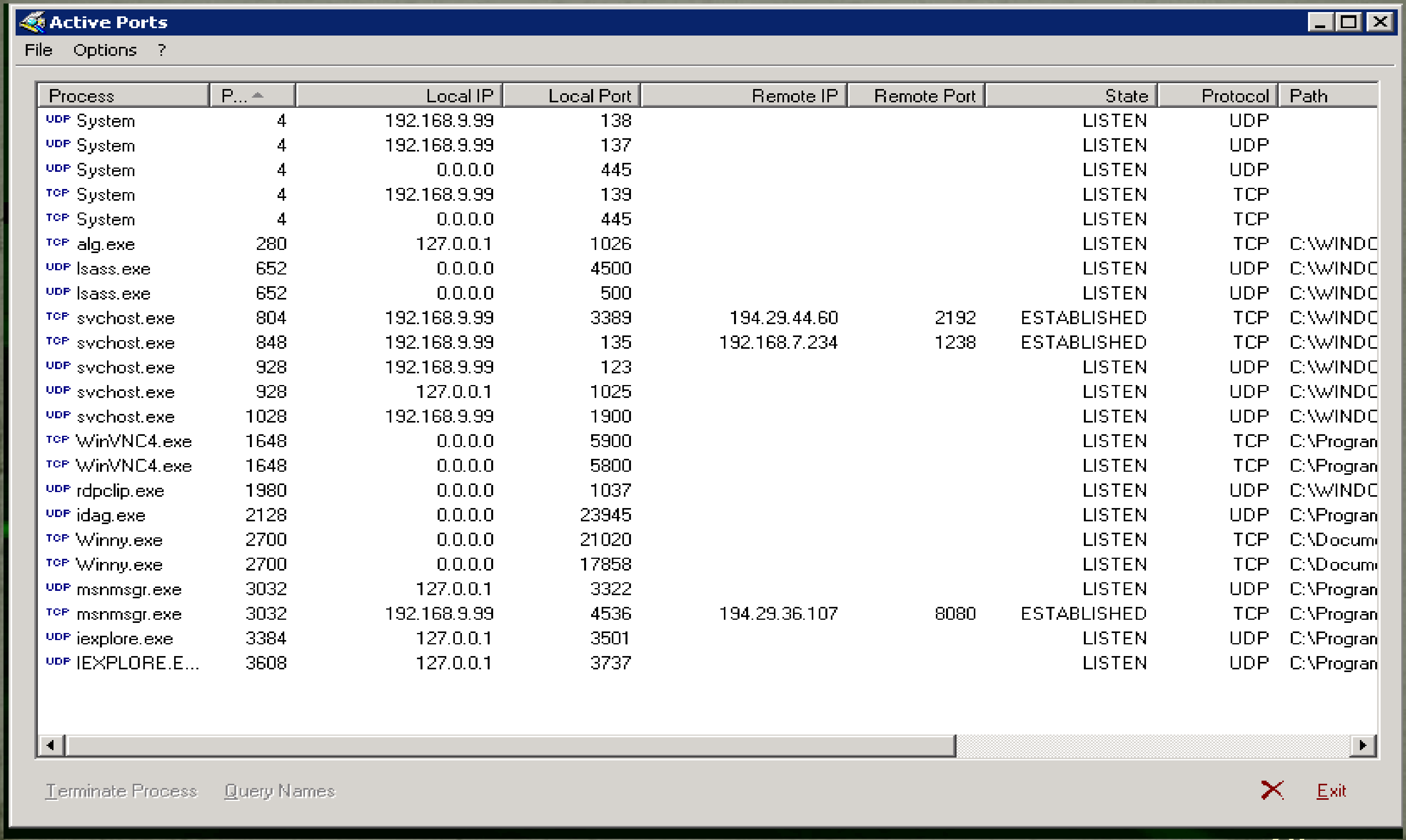
100.00% (-1162,-533) 30 nodes, 227 edge segments, 1

00036F90 00436F90: sub_436F30:loc_436F90

```
Flushing buffers, please wait...ok
Retrieving information from the database... ok
```

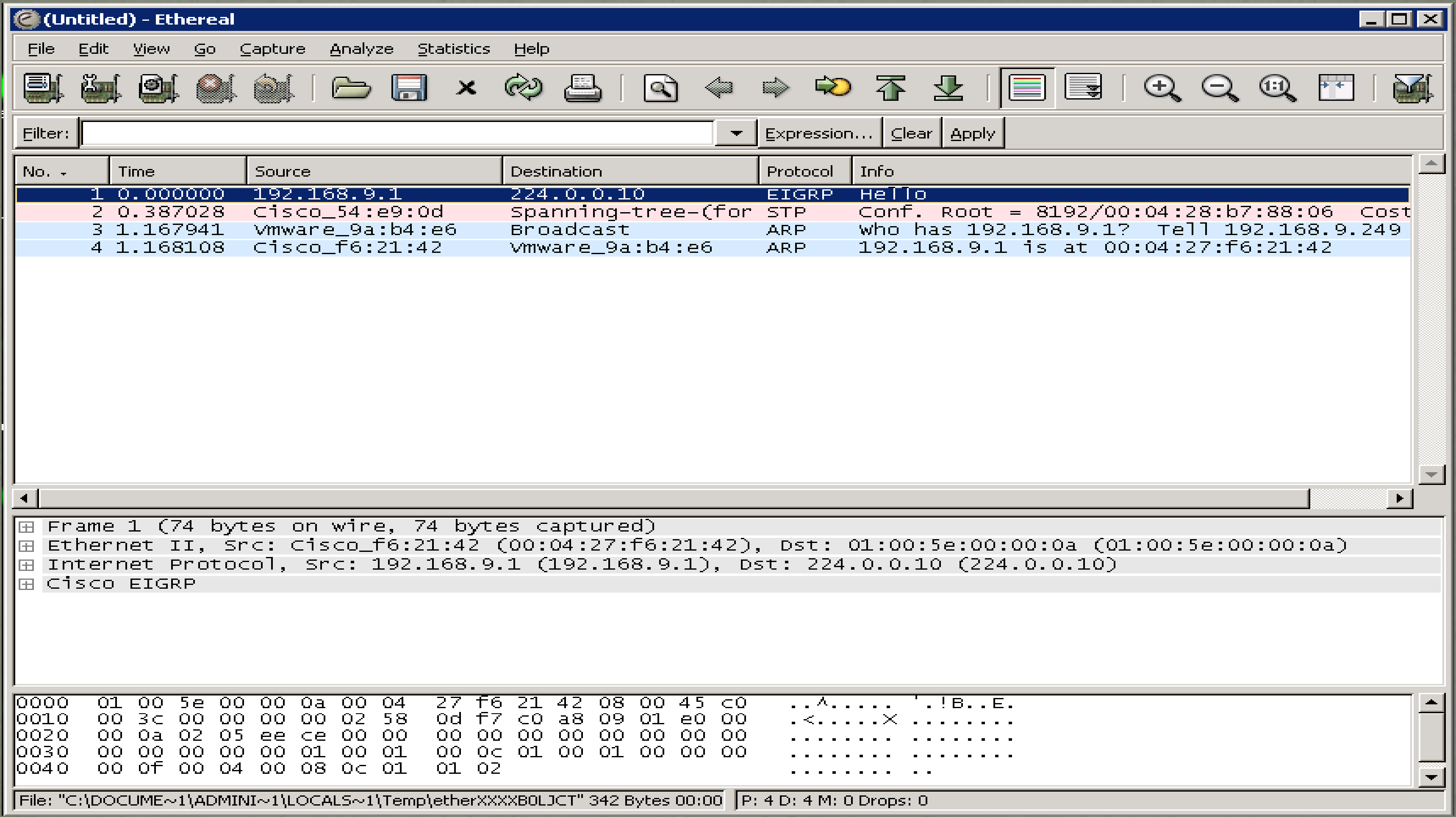
AU: idle Down Disk: 68GB

Active Ports



Process	P...	Local IP	Local Port	Remote IP	Remote Port	State	Protocol	Path
UDP System	4	192.168.9.99	138			LISTEN	UDP	
UDP System	4	192.168.9.99	137			LISTEN	UDP	
UDP System	4	0.0.0.0	445			LISTEN	UDP	
TCP System	4	192.168.9.99	139			LISTEN	TCP	
TCP System	4	0.0.0.0	445			LISTEN	TCP	
TCP alg.exe	280	127.0.0.1	1026			LISTEN	TCP	C:\WINDC
UDP lsass.exe	652	0.0.0.0	4500			LISTEN	UDP	C:\WINDC
UDP lsass.exe	652	0.0.0.0	500			LISTEN	UDP	C:\WINDC
TCP svchost.exe	804	192.168.9.99	3389	194.29.44.60	2192	ESTABLISHED	TCP	C:\WINDC
TCP svchost.exe	848	192.168.9.99	135	192.168.7.234	1238	ESTABLISHED	TCP	C:\WINDC
UDP svchost.exe	928	192.168.9.99	123			LISTEN	UDP	C:\WINDC
UDP svchost.exe	928	127.0.0.1	1025			LISTEN	UDP	C:\WINDC
UDP svchost.exe	1028	192.168.9.99	1900			LISTEN	UDP	C:\WINDC
TCP WinVNC4.exe	1648	0.0.0.0	5900			LISTEN	TCP	C:\Progran
TCP WinVNC4.exe	1648	0.0.0.0	5800			LISTEN	TCP	C:\Progran
UDP rdpclip.exe	1980	0.0.0.0	1037			LISTEN	UDP	C:\WINDC
UDP idag.exe	2128	0.0.0.0	23945			LISTEN	UDP	C:\Progran
TCP Winny.exe	2700	0.0.0.0	21020			LISTEN	TCP	C:\Docum
TCP Winny.exe	2700	0.0.0.0	17858			LISTEN	TCP	C:\Docum
UDP msnmsgr.exe	3032	127.0.0.1	3322			LISTEN	UDP	C:\Progran
TCP msnmsgr.exe	3032	192.168.9.99	4536	194.29.36.107	8080	ESTABLISHED	TCP	C:\Progran
UDP iexplore.exe	3384	127.0.0.1	3501			LISTEN	UDP	C:\Progran
UDP IEXPLORE.E...	3608	127.0.0.1	3737			LISTEN	UDP	C:\Progran

Ethereal Network Sniffer



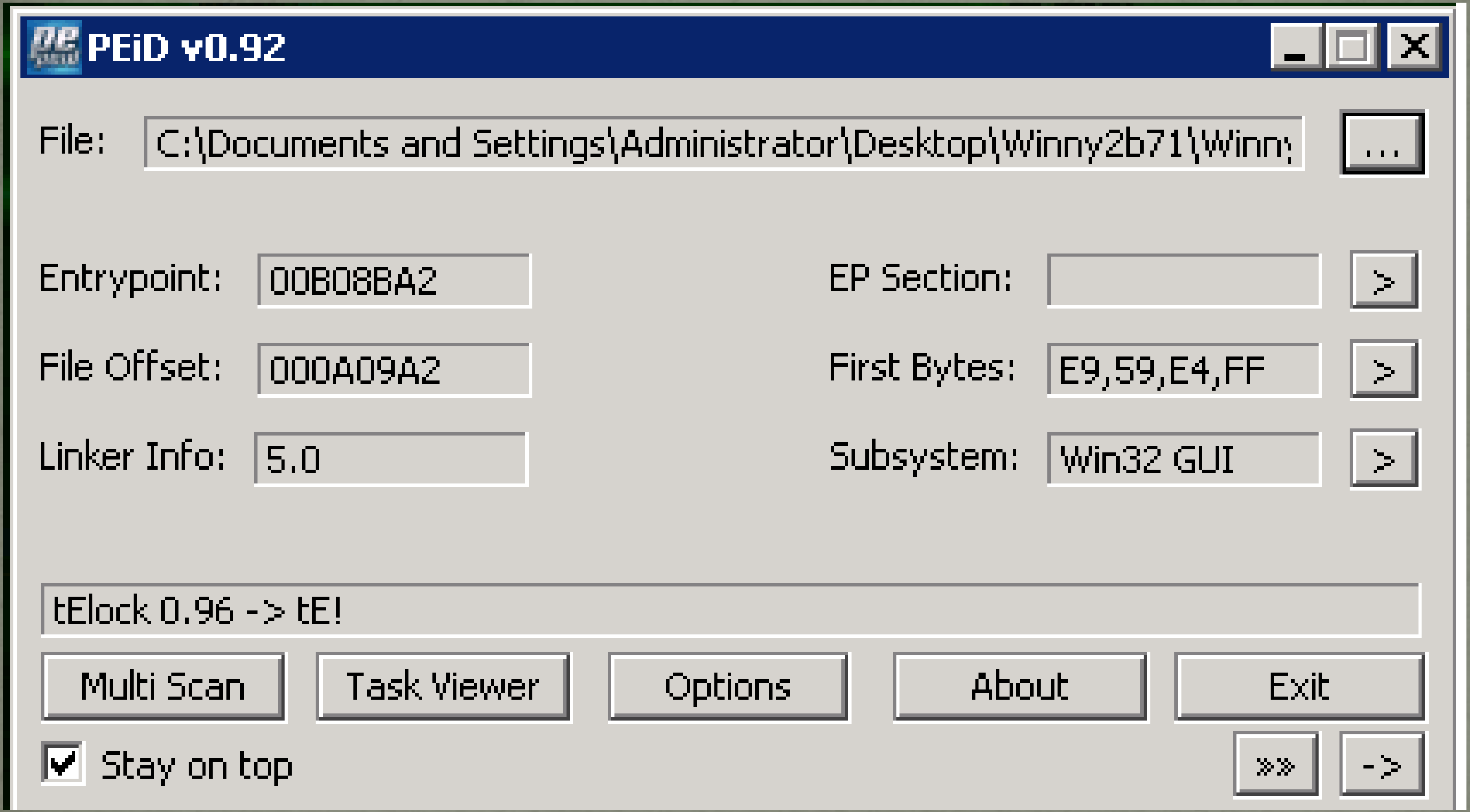
```
No. -     Time          Source               Destination           Protocol  Info
    1 0.000000   192.168.9.1          224.0.0.10            EIGRP     Hello
    2 0.387028   Cisco_54:e9:0d       Spanning-tree-(for    STP       Conf. Root = 8192/00:04:28:b7:88:06  Cost
    3 1.167941   Vmware_9a:b4:e6      Broadcast             ARP       Who has 192.168.9.1?  Tell 192.168.9.249
    4 1.168108   Cisco_f6:21:42       Vmware_9a:b4:e6       ARP       192.168.9.1 is at 00:04:27:f6:21:42
```

```
⊞ Frame 1 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Cisco_f6:21:42 (00:04:27:f6:21:42), Dst: 01:00:5e:00:00:0a (01:00:5e:00:00:0a)
⊞ Internet Protocol, Src: 192.168.9.1 (192.168.9.1), Dst: 224.0.0.10 (224.0.0.10)
⊞ Cisco EIGRP
```

```
0000   01 00 5e 00 00 0a 00 04  27 f6 21 42 08 00 45 c0   ..^.....  '.!B..E.
0010   00 3c 00 00 00 00 02 58  0d f7 c0 a8 09 01 e0 00   .<.....X ........
0020   00 0a 02 05 ee ce 00 00  00 00 00 00 00 00 00 00   ........ ........
0030   00 00 00 00 00 01 00 01  00 0c 01 00 01 00 00 00   ........ ........
0040   00 0f 00 04 00 08 0c 01  01 02                     ........ ..
```

```
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXB0LJCT" 342 Bytes 00:00   P: 4 D: 4 M: 0 Drops: 0
```

PEiD Packer Detector



PEiD v0.92

File: C:\Documents and Settings\Administrator\Desktop\Winny2b71\Winn

Entrypoint: 00B08BA2

EP Section:

File Offset: 000A09A2

First Bytes: E9,59,E4,FF

Linker Info: 5.0

Subsystem: Win32 GUI

tElock 0.96 -> tE!

☑ Stay on top

Let's go hunting

Binary Audit

LET THE GAME BEGIN

Hunting for 0day Winny Vulnerability

The Plan:

Find out which kind of encryption was used .

Find out where is the vulnerability.

Remotely execute code by exploiting the vulnerability

LET THE GAME BEGIN

Hunting for 0day Vulnerability

The Plan:

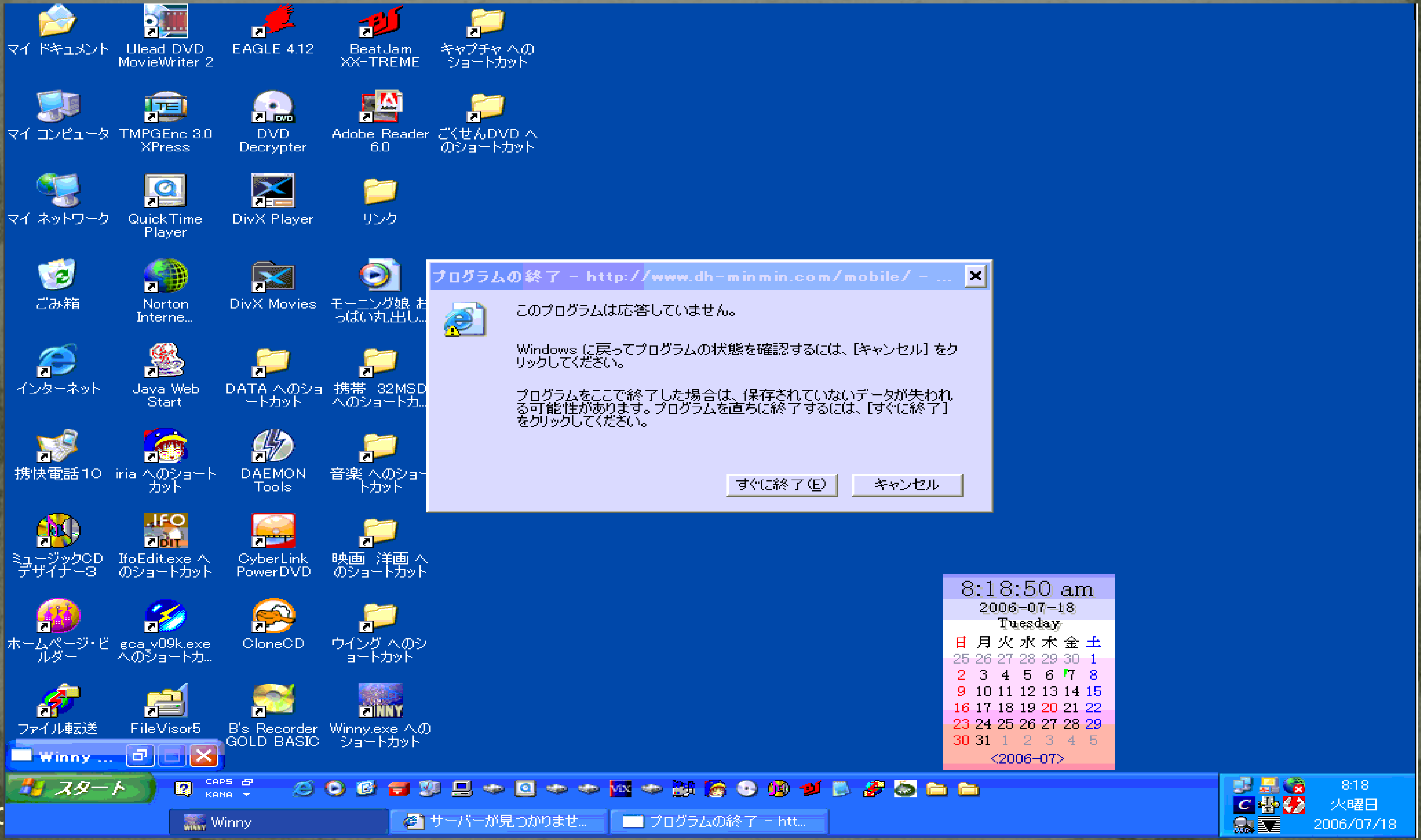
Find out which kind of encryption was used .

Find out where is the vulnerability.

Remotely execute code by exploiting the vulnerability

Live Session/Demo ■

Game Over !　;)



プログラムの終了 - http://www.dh-minmin.com/mobile/ - ...

このプログラムは応答していません。

Windows に戻ってプログラムの状態を確認するには、[キャンセル] をクリックしてください。

プログラムをここで終了した場合は、保存されていないデータが失われる可能性があります。プログラムを直ちに終了するには、[すぐに終了] をクリックしてください。

Credit

Kobi Pariente
Dror Shalev
eEye Digital Secuirty
Check Point

Questions?