Fight against spyware on two laptops

Lei Wang

ID: 3737737

Computer Science Department

University of Auckland

Lwan159@ec.auckland.ac.nz

Abstract

Today there is more and more spyware software that compromises people's privacy rights and does harm to computers. This is now a worldwide concern. Therefore this paper gives a methodology to detect, analyze and remove this type of software. This paper recorded what I found by applying a procedure to two laptops. It focused on two spyware applications and discussed how I found them, my reasons for calling them spyware, my best guess as to when and how they were loaded, what I did to remove them and whether I was successful in removing them.

Introduction

The word "spyware" was first used to satirize Microsoft's products in a humorous post about Microsoft's business model on the Usenet on Oct. 16, 1995[1]. It started to represent a kind of malicious software programs since Zone Labs used it in a press release for their Zone Alarm Personal Firewall in 1999[1]. From then on, it started to become one of the hottest buzzwords in the world. Nowadays, several researches [2,5,6], official and individual, are targeting on it. Even some legislation issues occur around it [3,6].

1 Definition of spyware

What is spyware? Ironically, though spyware attracts more and more concerns, it does not have a precise, official, definition to date. However, people certainly have tried and are trying to define spyware: On April 19, 2004, Federal Trade Commission held a “Spyware Workshop” which took **“**Defining and Understanding Spyware, including a discussion of how spyware may differ from adware” as the first goal [2]. However, I am not aware of anyone who has made a conclusion to this question after the workshop; The “SPYWARE CONTROL ACT” in the STATE OF UTAH, USA came up with a rather complex and precise definition (38 lines in a .doc file) [3]. Unfortunately, before its definition to spyware becomes standard it has to manage to appease “the concerns from big, well-established, mainstream Internet companies -- AOL, Amazon, Google, Microsoft, Yahoo, and a dozen others” [7].

Because there are no precise definitions, I use the description from a recently published paper <Measurement and Analysis of Spyware in a University Environment>: “ ‘spyware’ is commonly used to refer to software that, from a user’s perspective, gathers information about a computer’s use and relays that information back to a third party. This data collection occurs sometimes with, but often without, the knowing consent of the user [4].”

2 Methodology about detecting and removing spyware

Based on the definition I used, spyware is called spyware because it monitors and tells. Therefore it has to connect to its server, which means that it has to store the information it has gathered (either in memory or on a hard disk). So, it is possible I can determine suspicious software by monitoring a computer’s memory operations, file operations and most importantly network communication. Immediately then boils down to how does someone get a list of suspicious software? Due to the fact that a normal PC usually has more than ten thousand files, without scanning with a program, it is almost impossible to manually check all of them for spyware. In this case I used a free anti-spyware called “Ad-Aware” to get a list of suspicious files. As a supplement, I also checked through all the computer’s auto-startup items.

Considering the limitations on the length of the paper, I will pick up one spyware that is considered to be dangerous (with higher ranking in Ad-Aware’s list) for each laptop. So, my methodology is this:

1. Run Ad-Aware to get a list of spyware.
2. Pick up one which is considered to be highly dangerous by Ad-Aware. Find when and how it was loaded. Manage to run it.
3. Monitor its disk operation to see whether it writes down personal data.
4. Sniff its network traffic to see whether it sends personal data to remote sites.
5. Install the spyware on a clean machine, record all the changes made to the system. Change all the changes back on the two machines. If Ad-Aware is able to remove it then use Ad-Aware and check the result.
6. Manually check through the startup list, services list, windows register to see whether there is any suspicious program which could be a spyware.
7. Do step 3 to 5.

Note: Firstly, it is the methodology that I used to analyze spyware on the purpose of composing a term paper, not a common procedure for normal computer users to detect and remove spyware. That is the reason why I “picked up one” in step two. However, by simply removing the limitation put on the number of spyware programs in step 2, the methodology has the ability to help users to detect and remove spyware. Secondly, From the definition of spyware, the only strong evidence, which can be captured, is available in step 4, the personal data within a packet that is sent to the spyware’s home. However, step 3 is still not trivial. It not only assists to determine spyware but also supplies a way to detect what the spyware has done in the hard disk that will be helpful when we try to remove the spyware.

I list the software used for applying the Methodology in the following table.

Name & version	Download address	Used for	Used at	Remark
Ad-Aware SE	www.lavasoft.com	Detect and remove spyware	Step 1	Using definitions file: SE1R13 16.10.2004
Process Explorer v8.25	http://www.sysintervals.com/	Find out which process calls a specific .dll file	Step 2	Freeware
FileMon v 6.11	http://www.sysintervals.com/	Monitor all the disk operations	Step 3	Freeware
CommView v3.4	www.tamos.com	Sniff network traffics	Step 4	
Regsnap v4.6	www.lastbit.com	Analyze changes made to the Windows Registry	Step 5	Also monitor changes made to the Windows directory.

Table1

3 Apply the methodology

My experiment is conducted using two personal laptops. Both of them are borrowed from anonymous friends. I list the laptops' relevant information in table2.

	OS	Anti virus software	Firewall	Anti-spyware
Laptop1	Windows XP version 2002 SP1, Chinese	No	Skynet v5.2	No
Laptop2	Windows XP version 2002, SP2, Chinese	Rasing V2004	Windows-built-in	No

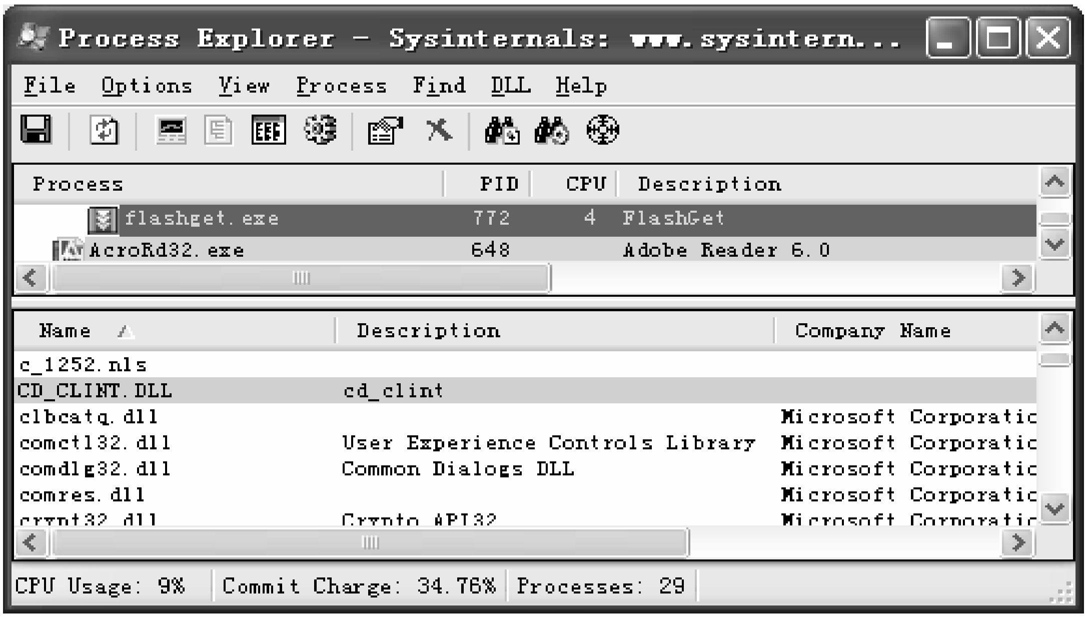
Table2

3.1 Experiment on laptop1

After scanning with Ad-Aware, I recieved a list of 35 critical objects. 22 of them were cookies, 12 of them are data files (like “089_42.swf”), the other was CD_CLINT.dll. According to the description given by Ad-Aware, CD_CLINT.dll (known as a part of “cydoor”) is considered to be dangerous. So I will target in on it.

For a .dll (dynamic link library) file, I have to find out its calling process in order to run it. Therefore I used procexp.exe (It can list all the dll files which are running) to see whether that .dll file had been running. The result was negative. By looking at its property, I got its modified date: 2002, Nov 9. One point worthy of talking about here is that in the Windows system, there are three time properties for a file: Created, Modified and Accessed and all of them are easy to be changed to any time by small software like “AttributeMagic”. Without changing, a program usually has the same modified data with the files generated by it. Hence I scanned the whole hard disk to get a list of executable files (I simply searched files which have .exe as the extension) that were modified on the same day. Fortunately, only three .exe files matched that condition. So I ran all of them. By using procexp.exe again, I found it was the process

"Flashget.exe" which caused CD_CLINT.DLL to run (see screenshot1). I need to emphasize that the Flashget I tested is of version 1.4 and version 1.65 (the latest version) is reported to no longer be a spy ware [8].



Process	PID	CPU	Description
flashget.exe	772	4	FlashGet
AcroRd32.exe	648		Adobe Reader 6.0

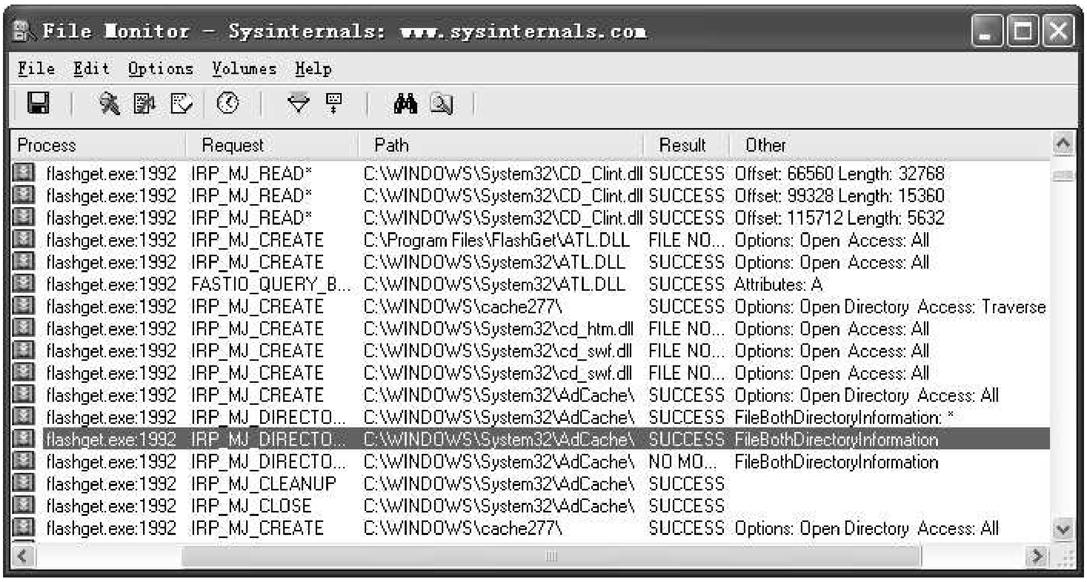
Name	Description	Company Name
c_1252.nls		
CD_CLINT.DLL	cd_clint	
clbcatq.dll		Microsoft Corporatic
comctl32.dll	User Experience Controls Library	Microsoft Corporatic
comdlg32.dll	Common Dialogs DLL	Microsoft Corporatic
comres.dll		Microsoft Corporatic
crypt32.dll	Crypto API32	Microsoft Corporatic

CPU Usage: 9% Commit Charge: 34.76% Processes: 29

Screenshot1.

Therefore it is reasonable to guess that CD_CLINT.dll was loaded together with Flashget V1.4 on 2002, Nov 9. However, it is just a guess because as I said above, there are methods that exist to change the date.

Then I applied step3. I ran Filemon.exe to monitor Flashget's disk operations. Filemon showed that it frequently called CD_CLINT.dll, and access directory "c:\windows\adCache" and "c:\windows\system32\adCache"(see Screenshot2).



Process	Request	Path	Result	Other
flashget.exe:1992	IRP_MJ_READ*	C:\WINDOWS\System32\CD_Clint.dll	SUCCESS	Offset: 66560 Length: 32768
flashget.exe:1992	IRP_MJ_READ*	C:\WINDOWS\System32\CD_Clint.dll	SUCCESS	Offset: 99328 Length: 15360
flashget.exe:1992	IRP_MJ_READ*	C:\WINDOWS\System32\CD_Clint.dll	SUCCESS	Offset: 115712 Length: 5632
flashget.exe:1992	IRP_MJ_CREATE	C:\Program Files\FlashGet\ATL.DLL	FILE NO...	Options: Open Access: All
flashget.exe:1992	IRP_MJ_CREATE	C:\WINDOWS\System32\ATL.DLL	SUCCESS	Options: Open Access: All
flashget.exe:1992	FASTIO_QUERY_B...	C:\WINDOWS\System32\ATL.DLL	SUCCESS	Attributes: A
flashget.exe:1992	IRP_MJ_CREATE	C:\WINDOWS\cache277\	SUCCESS	Options: Open Directory Access: Traverse
flashget.exe:1992	IRP_MJ_CREATE	C:\WINDOWS\System32\cd_htm.dll	FILE NO...	Options: Open Access: All
flashget.exe:1992	IRP_MJ_CREATE	C:\WINDOWS\System32\cd_swf.dll	FILE NO...	Options: Open Access: All
flashget.exe:1992	IRP_MJ_CREATE	C:\WINDOWS\System32\cd_swf.dll	FILE NO...	Options: Open Access: All
flashget.exe:1992	IRP_MJ_CREATE	C:\WINDOWS\System32\AdCache\	SUCCESS	Options: Open Directory Access: All
flashget.exe:1992	IRP_MJ_DIRECTO...	C:\WINDOWS\System32\AdCache\	SUCCESS	FileBothDirectoryInformation: *
flashget.exe:1992	IRP_MJ_DIRECTO...	C:\WINDOWS\System32\AdCache\	SUCCESS	FileBothDirectoryInformation
flashget.exe:1992	IRP_MJ_DIRECTO...	C:\WINDOWS\System32\AdCache\	NO MO...	FileBothDirectoryInformation
flashget.exe:1992	IRP_MJ_CLEANUP	C:\WINDOWS\System32\AdCache\	SUCCESS	
flashget.exe:1992	IRP_MJ_CLOSE	C:\WINDOWS\System32\AdCache\	SUCCESS	
flashget.exe:1992	IRP_MJ_CREATE	C:\WINDOWS\cache277\	SUCCESS	Options: Open Directory Access: All

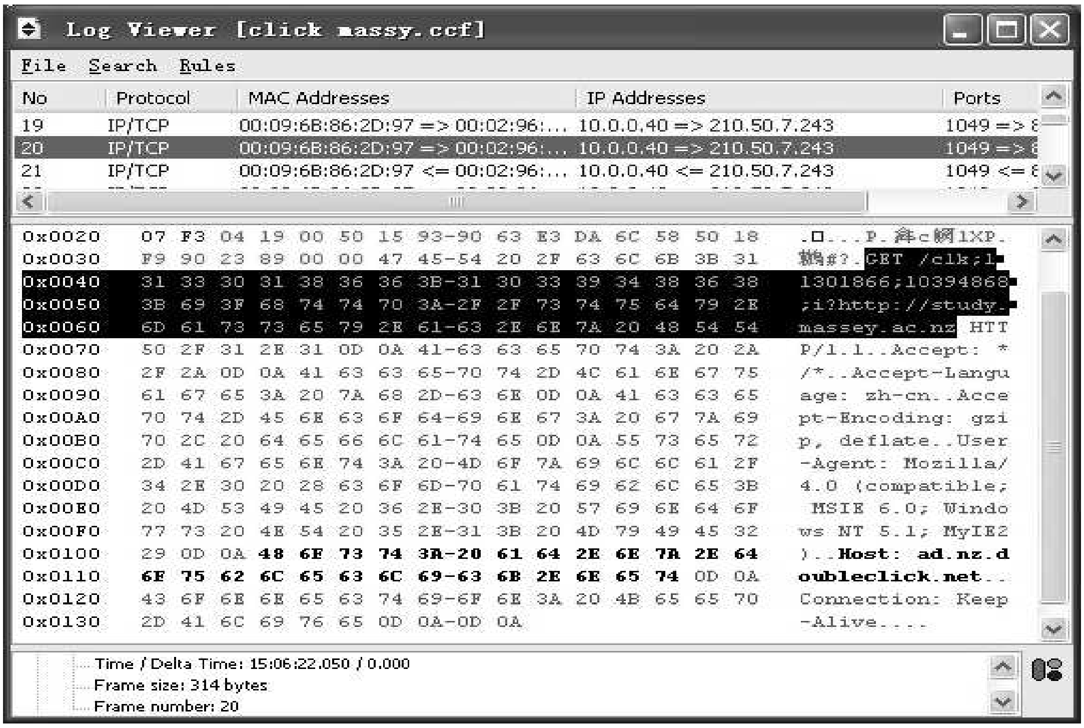
Screenshot2.

I found these two directories were used to contain advertisements. Their contents were designed to be exactly the same. Flashget kept checking whether they were consistent. If they were not consistent, Flashget would copy ads from one to the other to ensure the existence of advertisements.

During the same time, I monitored its network transmissions and found it downloaded several advertisements from two servers: z1.adserver.com and fastclick.com.edgesuit.net. A typical packet for downloading ads is like this:

> GET /8505/10002/gcs/mid751/wh_nz_468x60_1096041560.jpg HTTP/1.1..Accept: */*..Accept-Language: zh-cn..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0 (compatible;MSIE 6.0; Windows NT 5.1; MyIE2)..Connection: Keep-Alive..Host:fastclick.com.edgesuite.net....

Therefore I can see that advertisements showed up in the toolbar of Flashget. After that I surfed around the Internet to see whether Flashget (or just CD_CLINT.dll) recorded my browsing history. It was really a process of pure chance. I did not know whether it would do something or when it would do it. If I did not see any, I still could not definitely say it was not a Spyware. Maybe, it can report my personal information some other time, or in some way that I didn’t notice or detect. Fortunately, I caught its transmissions immediately after I clicked the banner “study in Massey”:



```
No      Protocol    MAC Addresses                          IP Addresses                    Ports
19      IP/TCP      00:09:6B:86:2D:97 => 00:02:96:...      10.0.0.40 => 210.50.7.243       1049 => 8
20      IP/TCP      00:09:6B:86:2D:97 => 00:02:96:...      10.0.0.40 => 210.50.7.243       1049 => 8
21      IP/TCP      00:09:6B:86:2D:97 <= 00:02:96:...      10.0.0.40 <= 210.50.7.243       1049 <= 8

0x0020    07 F3 04 19 00 50 15 93-90 63 E3 DA 6C 58 50 18    .□...P.犇c閝lXP.
0x0030    F9 90 23 89 00 00 47 45-54 20 2F 63 6C 6B 3B 31    鶘#?..GET /clk;1
0x0040    31 33 30 31 38 36 36 3B-31 30 33 39 34 38 36 38    1301866;10394868
0x0050    3B 69 3F 68 74 74 70 3A-2F 2F 73 74 75 64 79 2E    ;i?http://study.
0x0060    6D 61 73 73 65 79 2E 61-63 2E 6E 7A 20 48 54 54    massey.ac.nz HTT
0x0070    50 2F 31 2E 31 0D 0A 41-63 63 65 70 74 3A 20 2A    P/1.1..Accept: *
0x0080    2F 2A 0D 0A 41 63 63 65-70 74 2D 4C 61 6E 67 75    /*..Accept-Langu
0x0090    61 67 65 3A 20 7A 68 2D-63 6E 0D 0A 41 63 63 65    age: zh-cn..Acce
0x00A0    70 74 2D 45 6E 63 6F 64-69 6E 67 3A 20 67 7A 69    pt-Encoding: gzi
0x00B0    70 2C 20 64 65 66 6C 61-74 65 0D 0A 55 73 65 72    p, deflate..User
0x00C0    2D 41 67 65 6E 74 3A 20-4D 6F 7A 69 6C 6C 61 2F    -Agent: Mozilla/
0x00D0    34 2E 30 20 28 63 6F 6D-70 61 74 69 62 6C 65 3B    4.0 (compatible;
0x00E0    20 4D 53 49 45 20 36 2E-30 3B 20 57 69 6E 64 6F     MSIE 6.0; Windo
0x00F0    77 73 20 4E 54 20 35 2E-31 3B 20 4D 79 49 45 32    ws NT 5.1; MyIE2
0x0100    29 0D 0A 48 6F 73 74 3A-20 61 64 2E 6E 7A 2E 64    )..Host: ad.nz.d
0x0110    6F 75 62 6C 65 63 6C 69-63 6B 2E 6E 65 74 0D 0A    oubleclick.net..
0x0120    43 6F 6E 6E 65 63 74 69-6F 6E 3A 20 4B 65 65 70    Connection: Keep
0x0130    2D 41 6C 69 76 65 0D 0A-0D 0A                      -Alive....

Time / Delta Time: 15:06:22.050 / 0.000
Frame size: 314 bytes
Frame number: 20
```

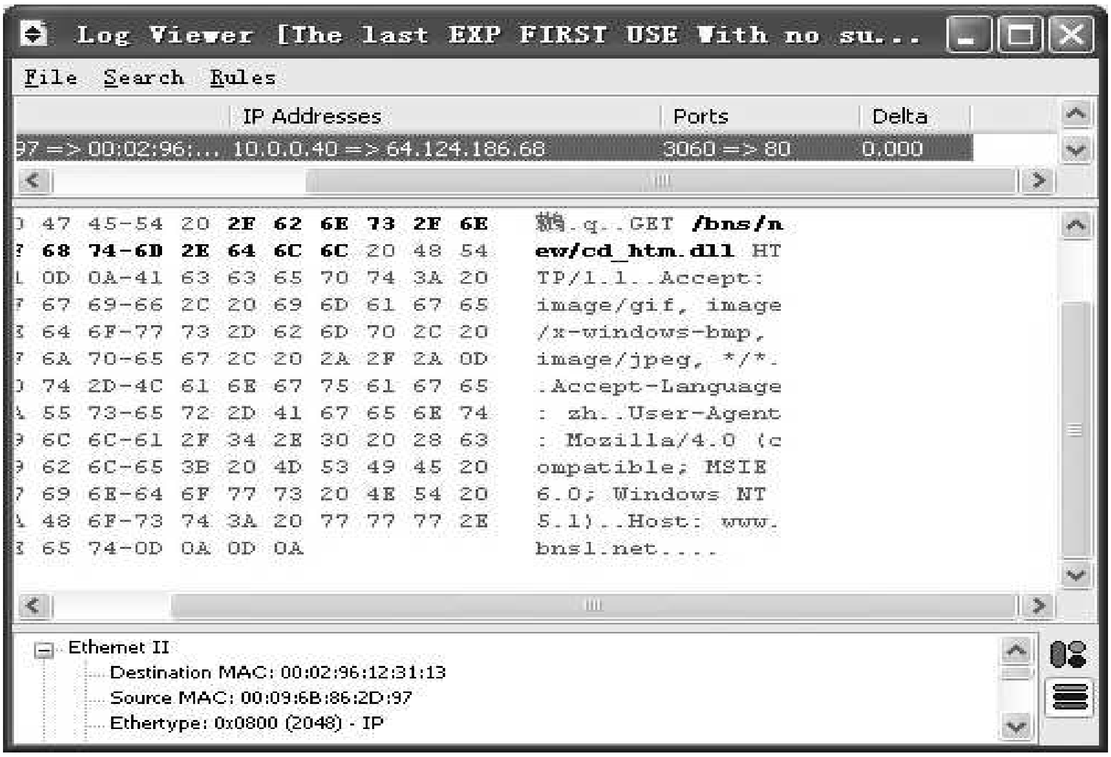
Screenshot3

It sent a packet carrying the address http://study.massey.ac.nz (the URL which I had just visited) to ad.nz.doubleclick.net. Furthermore, I also found it posting very suspicious information into www.2004cms.com. The typical HTTP request has the content:

> POST /scripts/cms/CMS.ASP HTTP/1.1..Accept: text/html, image/jpeg, image/png, image/gif, image/x-windows-bmp, */*..Accept-Language: zh..Accept-Encoding: gzip..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)..Host: www.2004cms.com..Content-Length: 432..Cache-Control: no-cache....ID=200101&D2=%3F%3F%3F%3F%3F%3F%3F%3FsL%40%3F%3F&AW=277&LV=3216&MU=1098522257&AS=442&NR=6&RS0=3180&RS1=35

84&RS2=3743&RS3=3179&RS4=3744&RS5=1440&LC=2004-10-23T05:52-04:00C01&CF=20&C1A=1800&P1A=60&C2A=0&P2A=40&C3A=0&P3A=70&ELA=45&RA0=2815&DA0=1&RA1=2994&DA1=1&PA0=2994&BA0=374300&EA0=0&FA0=2004-10-23T22:04+12:00&PA1=2815&BA1=358400&EA1=1&FA1=2004-10-23T22:12+12:00&C1B=0&P1B=60&C2B=5400&P2B=40&C3B=0&P3B=70&ELB=60&NP=1&GA0=0&HA0=1700

I do not know what the content really is. But the long string in the end which starts with "ID=" looks really like a unique identifier assigned just to me. Probably, that ID is used to identify a user for the purpose of supplying the advertisements according to that user's interests. Besides that, it also downloaded executable code as shown in Screenshot4.



```
97 => 00:02:96:...  10.0.0.40 => 64.124.186.68     3060 => 80     0.000

 47 45-54 20 2F 62 6E 73 2F 6E     鹅.q..GET /bns/n
 68 74-6D 2E 64 6C 6C 20 48 54     ew/cd_htm.dll HT
 0D 0A-41 63 63 65 70 74 3A 20     TP/1.1..Accept:
 67 69-66 2C 20 69 6D 61 67 65     image/gif, image
 64 6F-77 73 2D 62 6D 70 2C 20     /x-windows-bmp,
 6A 70-65 67 2C 20 2A 2F 2A 0D     image/jpeg, */*.
 74 2D-4C 61 6E 67 75 61 67 65     .Accept-Language
 55 73-65 72 2D 41 67 65 6E 74     : zh..User-Agent
 6C 6C-61 2F 34 2E 30 20 28 63     : Mozilla/4.0 (c
 62 6C-65 3B 20 4D 53 49 45 20     ompatible; MSIE
 69 6E-64 6F 77 73 20 4E 54 20     6.0; Windows NT
 48 6F-73 74 3A 20 77 77 77 2E     5.1)..Host: www.
 65 74-0D 0A 0D 0A                 bns1.net....

Ethernet II
    Destination MAC: 00:02:96:12:31:13
    Source MAC: 00:09:6B:86:2D:97
    Ethertype: 0x0800 (2048) - IP
```

Screenshot4

From the screenshot, we can see that it tried to download a file called "cd_htm.dll" from www.bns1.net. This .dll file was not successfully downloaded to the experiment laptop for unknown reason. However, downloading a .DLL is a fairly unpleasant action that could cause serious security problems. Without careful authentication, attacker could make the auto-download action perform operations not intended by the designer of the initial software. In fact, there is a guy called Benjamin Edelman who used DNS interception to demonstrate that a spyware program could automatically download and run the code he wrote [8].

To make sure Flashget V1.4 did these actions without a users' knowledge, I checked its end user license. There is no statement saying that it will send out a users' browser history and download executable file automatically. In conclusion, Flashget V1.4 that bonded with CD_CLINT.dll (a part of "cydoor") transmitted my web exploring history (study.massey.ac.nz) to the third party (ad.nz.doubleclick.net) and tried to download executable files without my consent. According to the definition I used, CD_CLINT.dll (cydoor) is spyware.

For removing the CD_CLINT.dll, I used Regsnap to take a snapshot of the windows register and the current system directories (c:\windows; c:\windows\system and c:\windows\system32). Then I simply used Ad-Aware to remove all the found spyware. Then I reboot the laptop and took another snapshot. By comparing the two snapshots, I found the changes made to the system were not complicated: It deleted seven register key values, three directories (c:\windows\adcache and c:\windows\system32\adcache, c:\flashget\backup\CD_install.exe), CD_CLINT.dll. After three days testing, I did not see Flashget communicate with servers. It even did not show advertisement any more. Therefore I believe the removal was successful.

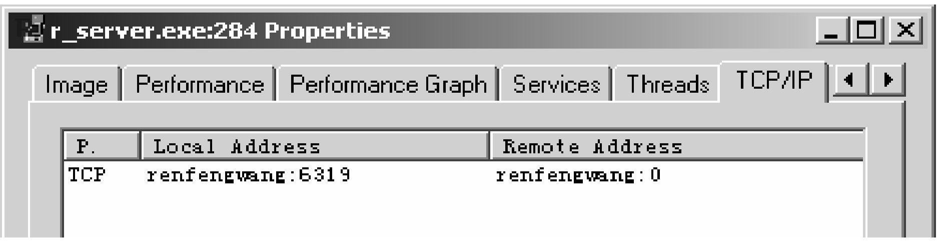
I searched information that was relevant to CD_CLINT.dll, cydoor and Spyware on the Internet. I found there was a web page (http://cexx.org/cydoor.htm) that showed similar results with mine, except for the differences on the names of servers that cydoor called back to. It also gave out a way to disable the spy functionality by replacing the CD_CLINT.dll file. Interesting enough, it said, "The current version [of cydoor] appears to respect the user's privacy and informed consent. We therefore consider this version most accurately categorized as "*Adware"*. Older versions could more accurately be considered *"Spyware"*." Without testing, I cannot comment on that. But, I guess the one I came across should be an early version one. I also downloaded Flashget of the latest version (v1.65) and I found it was no longer bonded with CD_CLINT.dll. By doing similar testing, I did not see it send out my personal data. If I want to prove Flashget v1.65 is not a spyware, further research is required.

3.2 Experiment on laptop2

After running Ad-Aware, I received a list of 109 "critical items" according to Ad-Aware's report. However, most of them (89) were cookies. Cookies are considered to be of reduced danger according to Ad-Aware. Moreover, from George Lawton, cookies are more often used "not to link specific users with their Web activity but instead to aggregate multiple users' browsing behavior"[5].

Consequently, I would not do an analysis on that. So I jumped into step6 to check whether there were some abnormal phenomena which indicated the existence of some other spyware.

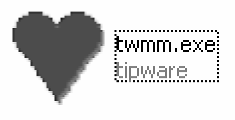
When I checked through the startup list, I found a suspicious item "r_server.exe" in it that was registered as a system service. By checking the memory, I found it was running at that time. As shown in the screenshot below, it was listening on port 6319.



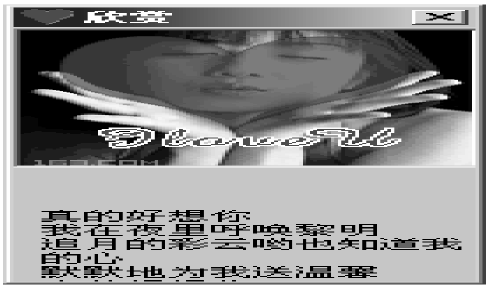
P.	Local Address	Remote Address
TCP	renfengwang:6319	renfengwang:0

Screenshot6

Because it was just listening on a port instead of actively connecting to somewhere, I could just wait until a program connected to the r_server.exe on that port. However, it is possible to wait for years but not see anything. Furthermore, the LAN that the laptop was actually in prevented an outsider to connect in to it. So, I could not wait for connections to happen. By searching “r_server.exe” as the key word, I found it was the name of a server side program (install in the computer to be controlled) of a famous remote control software called Radmin (Also known as Remote Administrator). On the laptop1, I downloaded it from www.radmin.com for testing purposes. I connected the two laptops with a router and assigned the one that had r_server.exe IP address 10.0.0.39 and the other 10.0.0.40. Then I ran the Remote Administrator Viewer, that is included in Radmin Administrator v2.2, that I just downloaded in to the machine with the IP address 10.0.0.40 and I had it connected to 10.0.0.39 on port 6319. However, A window popped up to ask for a password. Of course, I did not know the password. So, I started to try to find out some other clues. By looking at the property of the r_server.exe, I knew it was created on 2004, Aug 4. Then I searched the whole hard disk to list all the .exe files that were created on the same day. Fortunately, only one existed. It was named twmm.exe and had a lovely icon (see Screenshot6).



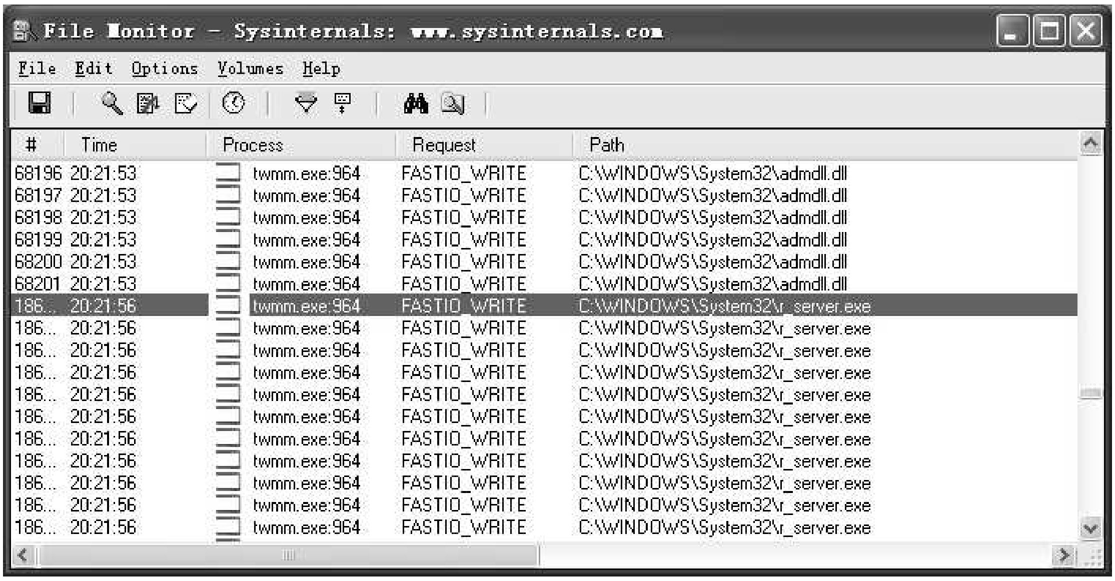
Screeshot6



真的好想你
我在夜里呼唤黎明
追月的彩云哟也知道我
的心
默默地为我送温馨

Screenshot7

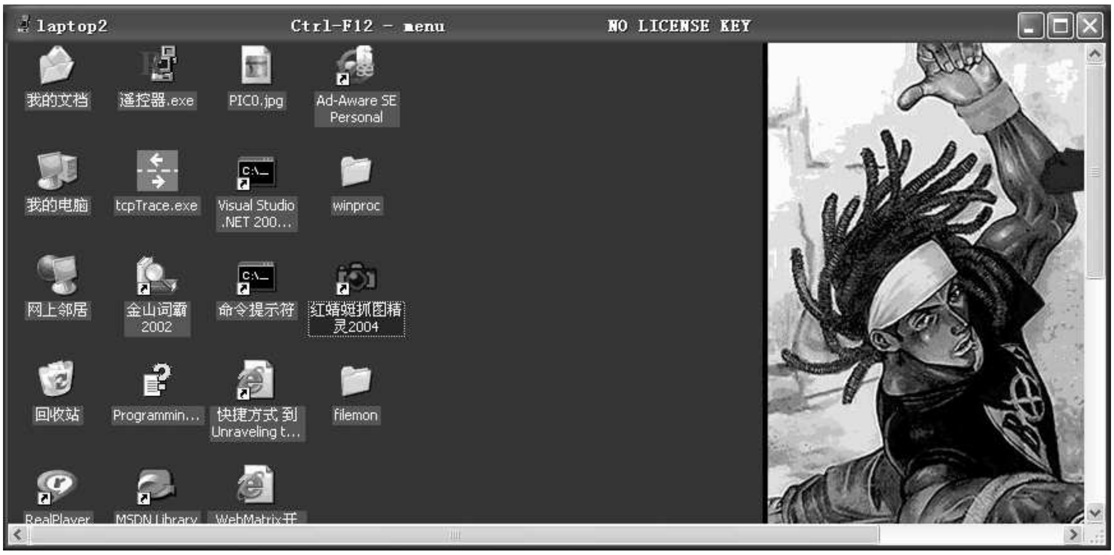
Once it was running it started to play music and showed the lyrics (see screenshot7): “I missed you so much…” It looked like a love letter which was from an admirer. For monitoring its underground operation, I installed it on a “clean” computer and found it was the one that installed r_server.exe into the laptop2! Look at screenshot8 that shows it writing to the disk file “r_server.exe”.



```
#      Time      Process        Request       Path
68196 20:21:53   twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\admdll.dll
68197 20:21:53   twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\admdll.dll
68198 20:21:53   twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\admdll.dll
68199 20:21:53   twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\admdll.dll
68200 20:21:53   twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\admdll.dll
68201 20:21:53   twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\admdll.dll
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
186... 20:21:56  twmm.exe:964   FASTIO_WRITE  C:\WINDOWS\System32\r_server.exe
```

Screenshot8

By using the key word “twmm.exe” and “6319”, I located one web address from Google. It is a Chinese web page that supplies a lot of hacker tools. From there, I found that the default password of the twmm.exe is “ufo1314520”. I used it to connect r_server.exe on laptop2. Immediately, I got complete control of the whole machine, including screen monitoring, mouse and keyboard control (see screenshot9)!



Screenshot9

In conclusion, twmm.exe installed a control program without the user’s consent. It definitely could cause damage to a user's privacy. According to the definition I used, this twmm.exe is indeed a type of Spyware although it also falls into the category of Trojan programs. As it is based on a legitimate software product called "Radmin Administrator" made by Famatech International Corp, it avoids lots of anti-virus and anti-spyware products. I tried Symantec's online virus and Trojan scan but even Symantec failed to find it out, which means that it is a really dangerous variation of spyware. Furthermore, if the bad guy changed the name of the process "r_server.exe", or port, or the name of the host software "twmm.exe", it would be much harder for me to find what that program was designed to do.

When I tested running twmm.exe I recorded all the changes it did to my system. There were 71 changes made to windows register and 8 new files created into c:\windows\system32. With this knowledge, I just changed the two laptops back to their original state before running twmm.exe. So the removal of this spyware was done.

4 Conclusion

Using a rough definition of spyware, I designed a seven-step methodology to detect and remove spyware. By applying the methodology, I conducted an experiment on two laptops. In the experiment, I detected and removed two spyware programs. The first one was a single file CD_CLINT.dll bounded with Flashget v1.4. This dll file (known as Cydoor") is a real Spyware programme that not only tracks a users' browsing history but also downloads executable files. The anti-Spyware software, Ad-Aware, is able to remove it. The second one is a Trojan horse which installs a remote control software "Radmin". It allows people to do anything to the infected computer without the owner's consent. As it is based on a legitimate well known software (Radmin), I have not found any anti-virus or anti-spyware software program which can detect it. By recording its install procedures, I managed to remove it.

5 Acknowledgements

I reserve my deepest gratitude to Renfeng Wang and Justin Faulke for letting me keep their laptops for a long time and do experiments on them. Without their help, I could not finish this paper.

I am most grateful to Benjamin Edelman and Justin Faulke for their inspiring comments, suggestions and help in making my writing understandable. Benjamin's published results on spyware directly help me to confirm the correctness of the experiments' results.

My warm thanks go to Clark Thomborson for his guidance and suggestions while I am writing the paper and for the extension of the deadline which allows me to have my friends correct my grammar mistakes.

6 References

[1] Sharon Wienbar, *The spyware inferno.* Available from http://www.zdnet.com.au/insight/security/0,39023764,39156395,00.htm.

[2] FEDERAL TRADE COMMISSION, Public Workshop: *Monitoring Software on Your PC: Spyware, Adware, and Other Software*
Available from http://www.ftc.gov/bcp/workshops/spyware/

[3] *SPYWARE REGULATION 2004, STATE OF UTAH.* Available from http://www.le.state.ut.us/%7E2004/htmdoc/hbillhtm/HB0323S04.htm

[4] Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, *Measurement and Analysis of Spyware in a University Environment.*
Available from http://www.cs.washington.edu/homes/gribble/papers/**spyware**.pdf

[5] George Lawton**,** *Invasive Software: Who's Inside Your Computer* (Computer, IEEE, July 2002, pp 15- 18)

[6] Benjamin Edelman, *"Spyware": Research, Testing, Legislation, and Suits.*
Available from http://www.benedelman.org/spyware/

[7] Benjamin Edelman, *A Close Reading of Utah's Spyware Control Act.*
Available from http://www.benedelman.org/spyware/utah-mar04/

[8] Benjamin Edelman, *WhenU Security Hole Allows Execution of Arbitrary Software.*
Available from http://www.benedelman.org/spyware/whenu-security/

[9] *Advertising Spyware: CyDoor CD_Load.exe and CD_Clint.dll.*
Available from http://www.cexx.org/cydoor.htm