HIT2006

Spyware Detection :
Automated Behavior Analysis System

Birdman
2006-07-16
X-Solve

Abstract

- 分析目前流行的Spyware設計手法與運作模型。並介紹我們所開發的自動化的惡意程式行為分析系統與整合型Spyware偵察工具，用來協助資安人員研究新的Spyware與惡意程式行為模型。

- **Birdman**
  - birdman@x-solve.com, **X-Solve**
  - Our WebSite →Http://x-solve.com/blog
  - Column Writer

    http://www.informationsecurity.com.tw
  - MSDN Flush Writer

    http://www.microsoft.com/taiwan/msdn

X-Solve, Inc. is a company focusing on developing IT Security technology for the reliable and high assurance detection and eradication of Spyware and Rootkit.

Outline

- What is Spyware?
- The Malicious Behavior Models of Spyware
- Strategy of Spyware Analysis and Detection
- ***Archon Scanner*** - Spyware Detection Tools
- ***Archon Analyzer*** - Automated Malicious Behavior Analyzer
- Conclusion

What is Spyware?

- Definition
  - Spyware is considered a malicious program in that users unwittingly install the product when they install something else.

- There are two types of Spyware.
  - **Commercial Purpose**
    - This type Spyware do track your surfing habits in order to serve ads related to user.
    - Adware, Browser H… …d software
  - **Invasive Purpose**
    - This type is designed for hacker, they are more malicious than another type. Hacker utilizes them to collect private data of the certain victims or penetrate into computer system.
    - Trojan Horse, Backdoor, key-logger, Rootkit and other hacking tools.

Now, we will discuss this one in the following slices.

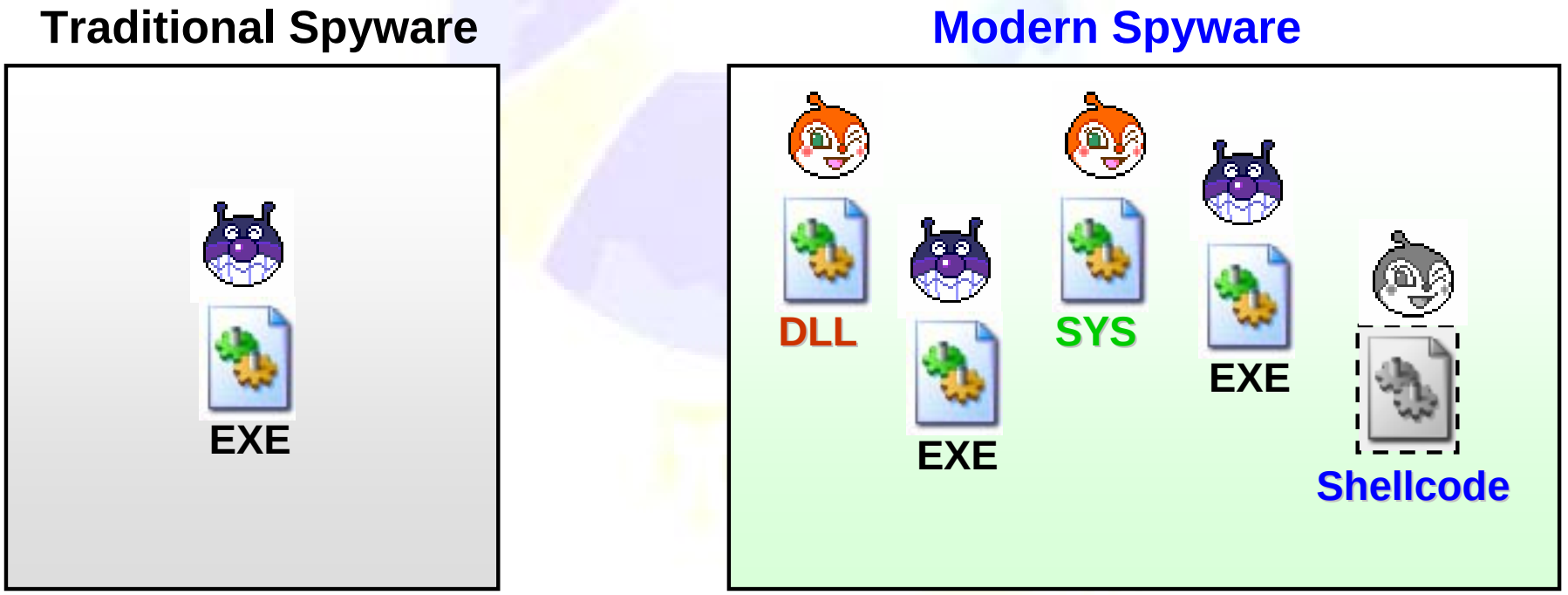
The Difference Between Virus & Spyware?

Virus VS. Spyware

Virus	Spyware
Active and Large-scale Attack	Passive, Small-scale and Stealth
Low Mutation	High Mutation, Customize
No Specific Target and Localization	Specific Target, Localization
Do Destruction	Do Information Collection

The Malicious Behavior Models of Spyware

- Traditional Spyware Behavior
  - Spyware exists as independent executable programs
- Modern Spyware Behavior

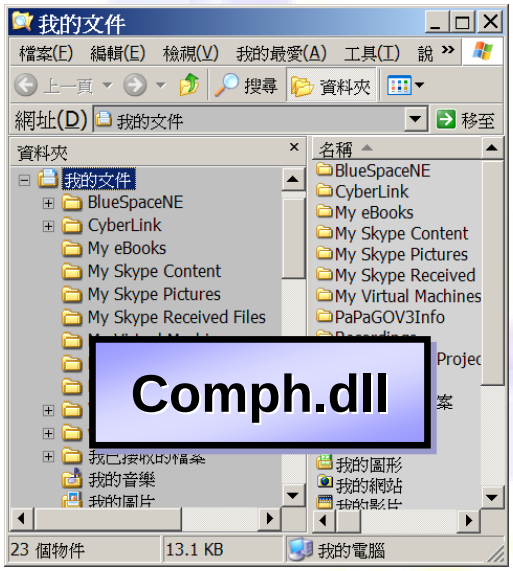


Case Study 1 : DLL Injection

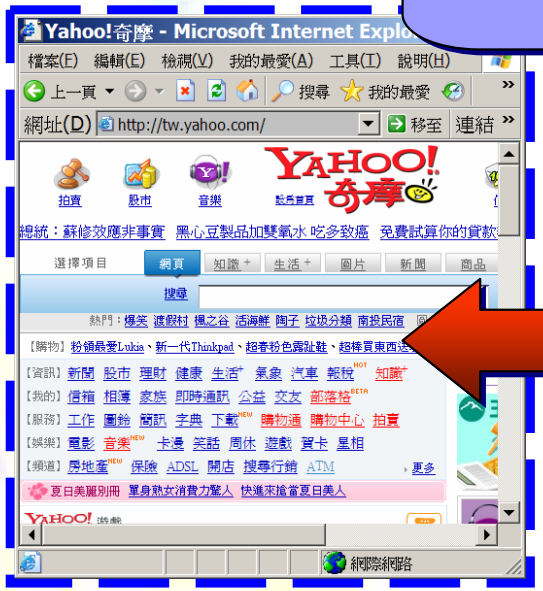
- This one is a kind of DLL Injection Spyware. It will inject a DLL into Explorer.exe and IE.

Spyware Dropper

Comph.dll



Comph.dll



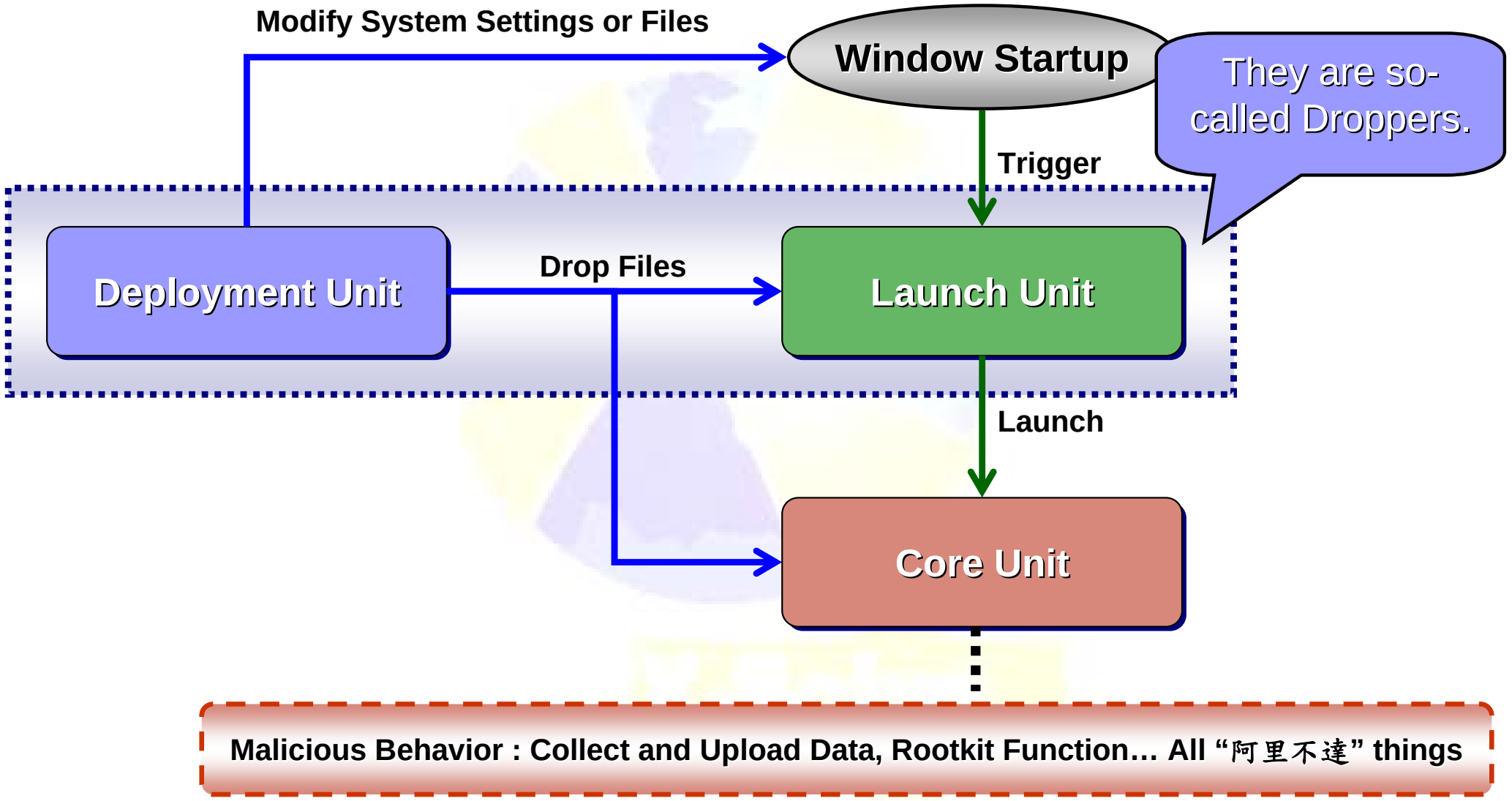
Oh YA! ^_^
Really Happy

Inject DLL into IE

Spyware Behavior

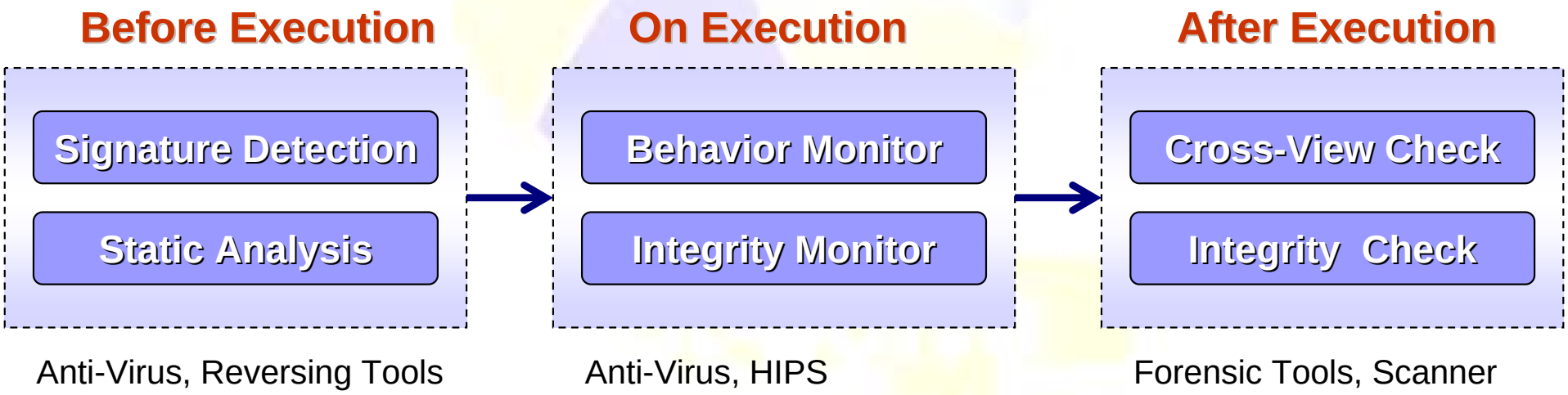
- EXE or Process are insufficient !
  - Different from traditional Spyware, the sophisticated Spyware have not just one EXE. They appear many executable types, such as DLL, SYS even Shellcode.
  - It one of reason that make Anti-Virus sucks!
- Common Malicious Behavior consists of three units
  - Deployment Unit
  - Launch Unit
  - Core Unit
    - Remote-Control
    - Data Collection
    - Self-Protection
    - Other malicious behavior

Common Malicious Behavior Model



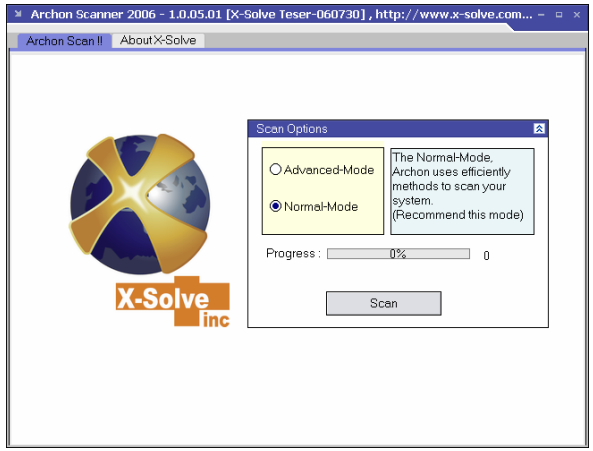
Strategy of Spyware Analysis and Detection

- There are three types for Spyware Detection.
  - **Before Execution**
  - **On Execution**
  - **After Execution**



Spyware Detection - Archon Scanner

- Rootkit Detection
- DLL Injection Backdoor Detection
- Malicious Behavior Analysis
- Zero Deployment
  - No monitor program need to install
  - No training for baseline
- A Forensic tool for Scanning Spyware



Download Trial Version Archon (2006-0701 ~ 0730)

- http://x-solve.com/Products/Archon_Scanner/Trial/Snapshot/Archon_1.JPG
- http://x-solve.com/Products/Archon_Scanner/Trial/Snapshot/Archon_2.JPG
- http://x-solve.com/Products/Archon_Scanner/Trial/ArchonScanner_1.0_Preview.zip

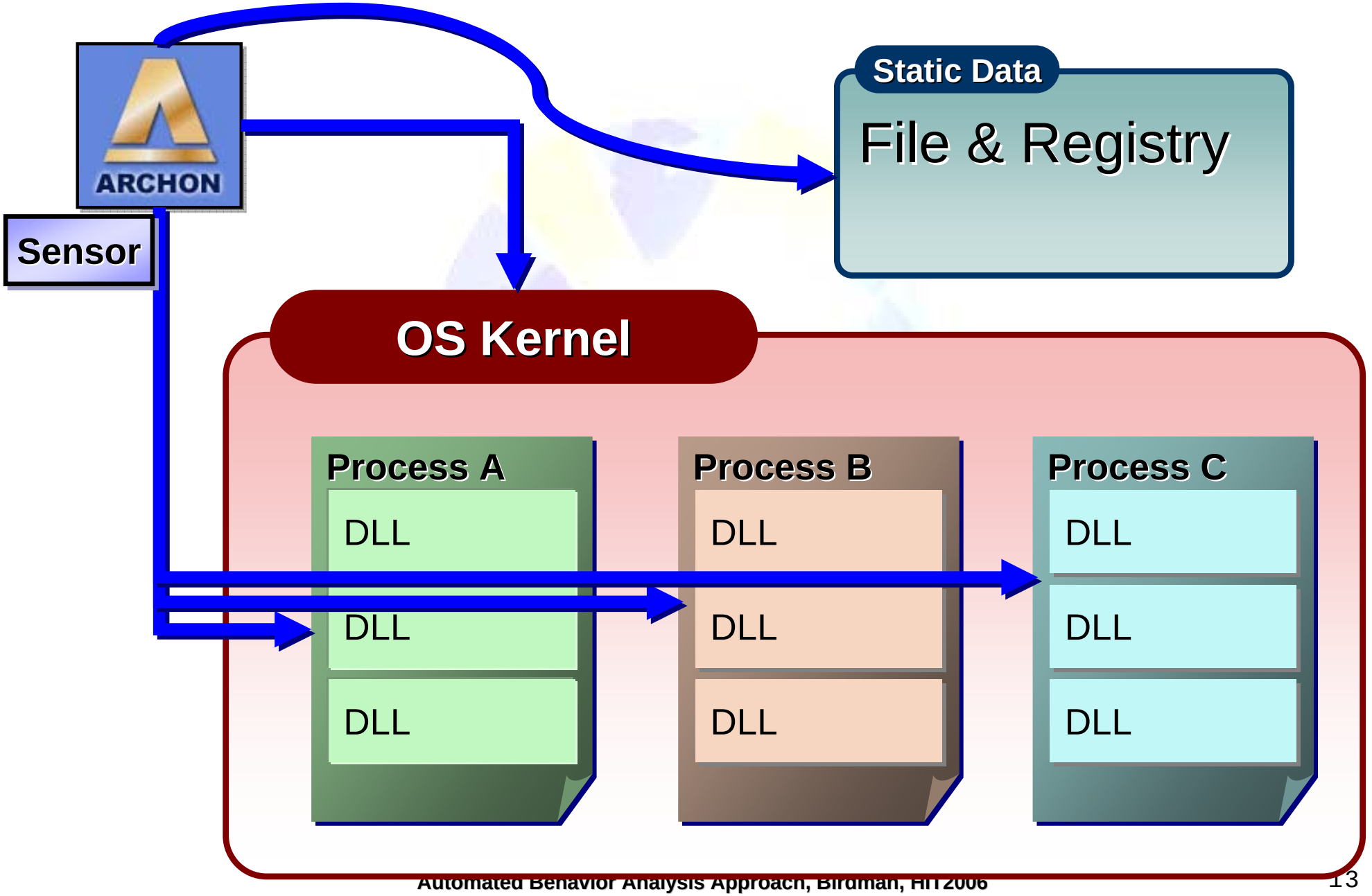
Spyware Detection - Archon Scanner

- Spyware Domain View
  - Different form other commercial Spyware Scanners, Archon Scanner is designed of Spyware domain view, we use over 25 aspects as malicious behavior features to analyze unknown Spyware or Rootkit.

- Major Malicious Behavior Features
  - Hidden Process Detection
  - Kernel Hooking Detection (SSDT Hook)
  - User Mode Global API-Hooking Detection
  - Hidden Registry Key Detection
  - Malicious DLL Injection Analysis
  - Raw Socket Detection
  - LDR Modification Tricks Detection
  - Message Hooker Detection

- Archon Scanner focus on the user mode Spyware detection.

Spyware Inspection of Archon Scanner



Rootkit Detection

- Against Hooking
  - There are many Hooking approaches in the world, but we just focus on the major tricks which are popular among Spyware writers.
    - Kernel Mode Hook : SSDT Hooking
    - User Mode Hook : IAT Hooking, EAT Hooking, Inline Hooking
- Hidden Process Detection
  - We use the “Process Handle Tracking Approach” to detect all kind of hidden processes, such as Hxdef, Fu, AFX, vanquish or other Rootkits.
  - In next version Archon, we will add new approach to detect hidden process by FuTo.
- Hidden Objects are easy to discover with Cross-View approach.

How to find out injected DLL?

- Theoretically, it is impossible to determine which DLL is injected in a process without behavior monitor. Because, all the important evidence were disappear after injection.
- Other Clues
  - Find out all explicit load DLLs with LDR Information
    - PEB -> LDR Table
  - IAT Scanning
  - Malicious PE Check : Packer Analysis

Archon

掃描引擎版本：1.0E.06

版本宣告：For X-Solve Teser-060730, Power By X-Solve Inc,艾克索夫公司
起始時間：04 July 2006 11:26.05
掃瞄時間：22 秒
掃瞄目標：XSERVER
作業系統：Microsoft Windows XP Professional Service Pack 2 (Build 2600) - VM
掃描模式：Normal Mode
報表模式：專家模式 (Expert-01)

危害等級	種類	惡意程式名稱	說明
55399	Module	C:\WINDOWS\system32\HookApi.dll	**JMP Hook** :C:\WINDOWS\system32\ntdll.dll:NtQuerySystemInformation **JMP Hook** :C:\WINDOWS\system32\ntdll.dll:RtlGetNativeSystemInformation **JMP Hook** :C:\WINDOWS\system32\ntdll.dll:ZwQuerySystemInformation **JMP Hook** :C:\WINDOWS\system32\kernel32.dll:CreateProcessW **JMP Hook** :C:\WINDOWS\system32\kernel32.dll:FindNextFileW **JMP Hook** :C:\WINDOWS\system32\kernel32.dll:OpenProcess **JMP Hook** :C:\WINDOWS\system32\advapi32.dll:RegEnumValueW **Load DLL** :(1536)C:\WINDOWS\explorer.exe **Load DLL** :(168)C:\WINDOWS\system32\hkcmd.exe **Load DLL** :(1616)C:\Archon.exe **MessageHooker** :WH_CALLWNDPROC
10277	Process	C:\Program Files\Internet Explorer\IEXPLORE.EXE	**Hidden Process** : **IE AP** :PID=1120, Malicious Code Injected !
7700	Module	C:\WINDOWS\JiurlPortHide.sys	**SDT Hook** :NTOSKRNL.EXE:ZwDeviceIoControlFile **AutoRun** :SYSTEM\CURRENTCONTROLSET\SERVICES\JiurlPortHide\
2400	Process	C:\WINDOWS\system32\hkcmd.exe	**DataThief** : **AutoRun** :SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\HotKeyCmds

列印結果 | 另存新檔

Element of Intrusion Detection System

- There are many IDS around us.
  - Guard → Person
  - NIDS → IP (Session)
  - Anti-Virus → File
  - HIPS/Personal Firewall → Process

We need more precise answers !

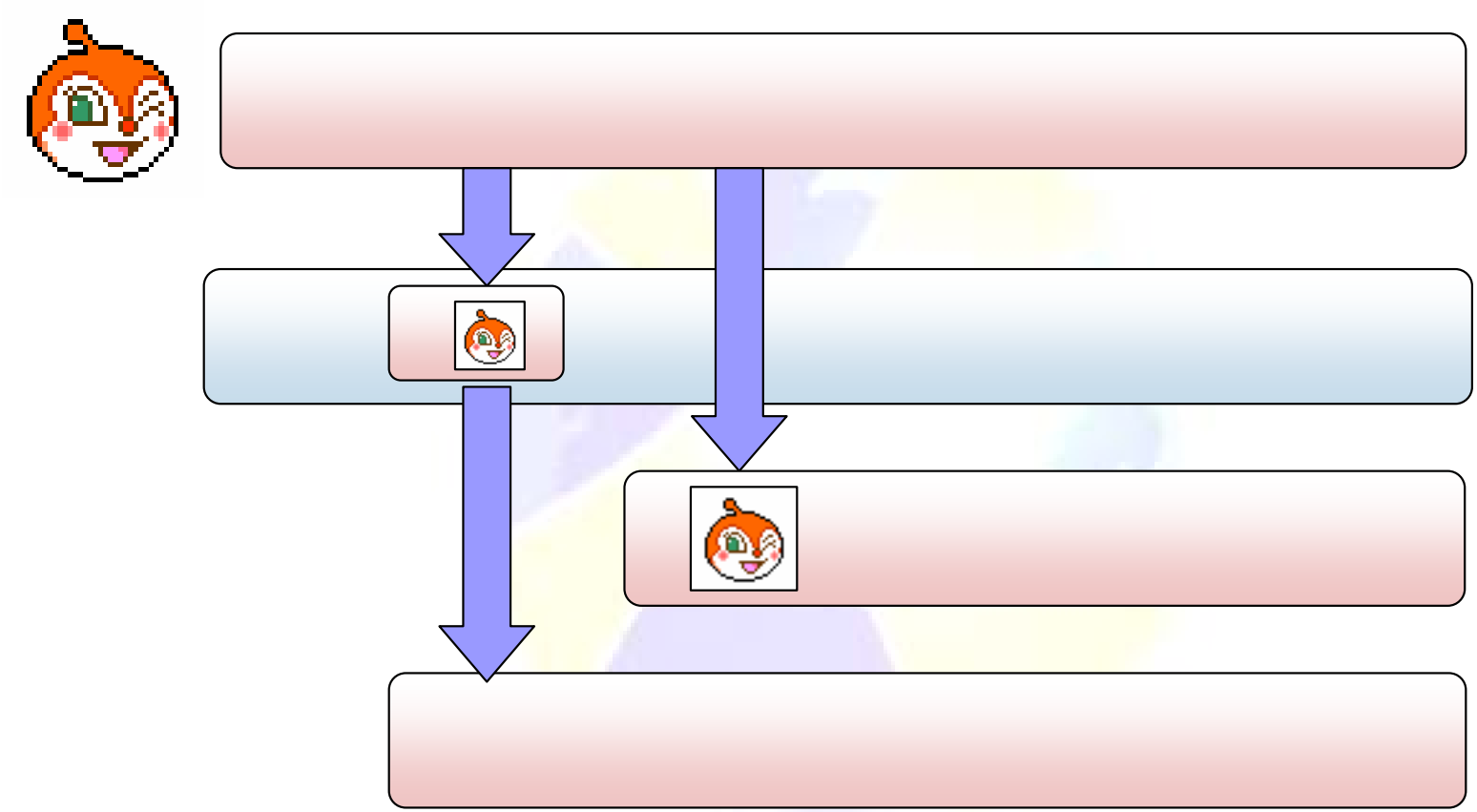
How about DLL Injection Spyware?

How about Code Injection Spyware?

How about Kernel mode Spyware?

How about Rootkit!?

Malicious Behavior Set



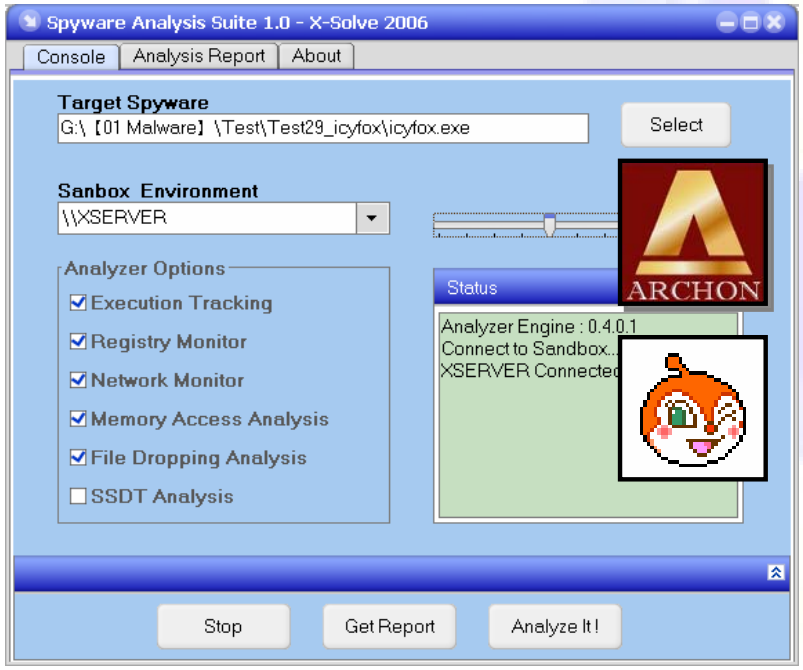
In order to cover all the malicious behavior, including remote threading and DLL injection. We track the relationship of process and thread to identify the "**Malicious Behavior Set**."

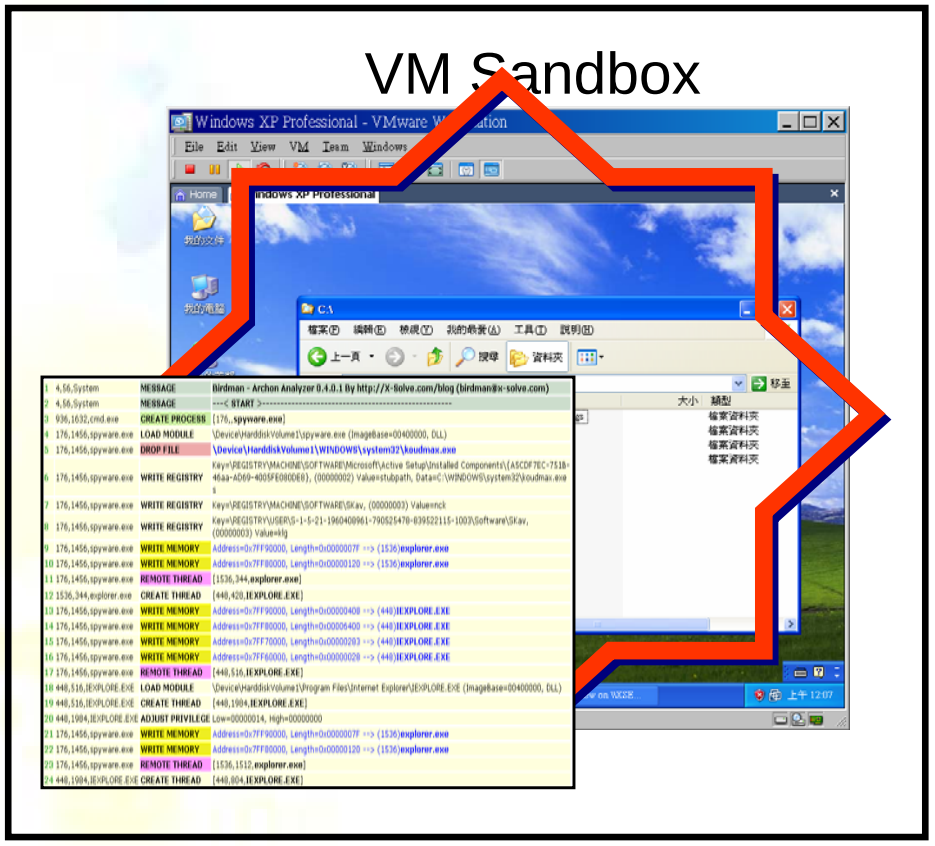
Automated Malicious Behavior Analyzer

- We need an automated analyzer to profile malicious behavior of Spyware.
- Implementation
  - To Capture all the user mode Spyware behavior, we have developed a pure Kernel mode monitor, **Archon Analyzer**.
  - Behavior Monitor:
    - Process and Thread Tracking
    - File Dropping Monitor
    - Remote Threading Monitor
    - Process Memory Access Monitor
    - Registry Access Monitor
    - Networking Monitor

Virtual Lab For Spyware Analysis

- Virtual Lab = Archon Analyzer + VM Sandbox
- Automated ! Efficient !





Case Study 2 - (1/2)

			Birdman - Archon Analyzer 0.4.0.1 By http://X-Solve.com/blog
			---< START >----------
3	1632,1300,cmd.exe	CREATE PROCESS	[1456,,**spyware.exe**]
4	1456,728,spyware.exe	LOAD MODULE	\Device\HarddiskVolume1\spyware.exe (ImageBase=00400000, DLL)
5	1456,728,spyware.exe	DROP FILE	**\Device\HarddiskVolume1\WINDOWS\system32\temp1**
6	1456,728,spyware.exe	DROP FILE	**\Device\HarddiskVolume1\WINDOWS\system32\Shell32.exe**
7	1456,728,spyware.exe	CREATE PROCESS	[344,,**Shell32.exe**]
8	1456,728,spyware.exe	CREATE THREAD	[344,448,**Shell32.exe**]
9	344,448,Shell32.exe	LOAD MODULE	\Device\HarddiskVolume1\WINDOWS\system32\Shell32.exe (ImageBase=00400000, DLL)
		DROP FILE	**\Device\HarddiskVolume1\DOCUME~1\birdman\LOCALS~1\Temp\xyztmp2.exe**
		CREATE PROCESS	[428,,**xyztmp2.exe**]
		CREATE THREAD	[428,516,**xyztmp2.exe**]
		LOAD MODULE	\Device\HarddiskVolume1\DOCUME~1\birdman\LOCALS~1\Temp\xyztmp2.exe (ImageBase=00400000, DLL)
14	428,516,xyztmp2.exe	DROP FILE	**\Device\HarddiskVolume1\WINDOWS\system32\wlogntiy.dll**
15	428,516,xyztmp2.exe	DROP FILE	**\Device\HarddiskVolume1\WINDOWS\system32\KavPot.sys**
16	428,516,xyztmp2.exe	DROP FILE	**\Device\HarddiskVolume1\WINDOWS\system32\KavPot2.sys**
17	676,824,services.exe	LOAD DRIVER	\Registry\Machine\System\CurrentControlSet\Services\AVPort
18	676,1008,services.exe	LOAD DRIVER	\Registry\Machine\System\CurrentControlSet\Services\AVPort2
19	428,516,xyztmp2.exe	WRITE REGISTRY	Key=\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\sysupdate, (00000001) Value=DllName, Data=wlogntiy.dll
20	428,516,xyztmp2.exe	WRITE REGISTRY	Key=\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\sysupdate, (00000004) Value=Asynchronous, Data=12FC78
21	428,516,xyztmp2.exe	WRITE REGISTRY	Key=\REGISTRY\MACHINE\SOFTWARE\Microsoft\...\sysupdate, (00000004) Value=Impersonate, Data=12FC80
		WRITE REGISTRY	Key=\REGISTRY\MACHINE\SOFTWARE\Microsoft\...\sysupdate, (00000001) Value=StartShell, Data=WinlogonSta
		CREATE PROCESS	[1872,,**IEXPLORE.EXE**]
		CREATE THREAD	[1872,1984,**IEXPLORE.EXE**]
		LOAD MODULE	\Device\HarddiskVolume1\Program Files\Internet Explorer\IEXPLORE.EXE (ImageBase=00400000, DLL)
		WRITE MEMORY	Address=0x00140000, Length=0x00000042 --> (1872)**IEXPLORE.EXE**
		REMOTE THREAD	[1872,1512,**IEXPLORE.EXE**]
28	428,516,xyztmp2.exe	CREATE THREAD	[428,1096,**xyztmp2.exe**]
29	1872,1512,IEXPLORE.EXE	LOAD MODULE	\Device\HarddiskVolume1\Program Files\Internet Explorer\IEXPLORE.EXE (ImageBase=00400000, DLL)
30	428,1096,xyztmp2.exe	WRITE REGISTRY	Key=\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\srservice, (00000004) Value=Start, Data=AFFF90
31	428,1096,xyztmp2.exe	ADJUST PRIVILEGE	Low=00000014, High=00000000
32	428,1096,xyztmp2.exe	WRITE MEMORY	Address=0x009F0000, Length=0x00000042 --> (1592)**spoolsv.exe**
33	428,1096,xyztmp2.exe	REMOTE THREAD	[1592,1612,**spoolsv.exe**]

Drop EXE, shell32.exe and xyztmp2.exe

Driver !! Rootkit??

Winlogon Notification !! Wlogntiy.dll (Autorun!)

DLL Injection !! Inject to IE and spoolsv.exe

Case Study 2 - (2/2) Network Traffic Recording

DNS Query

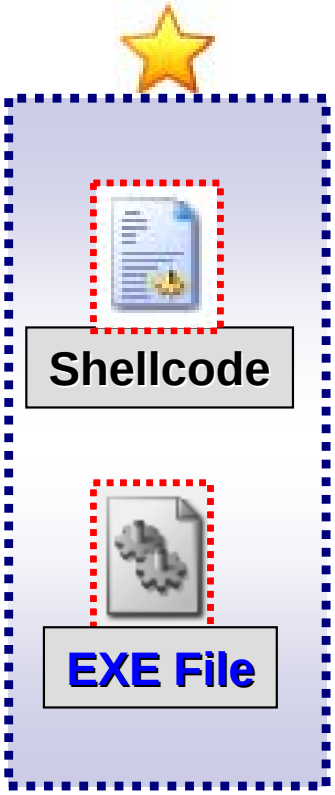
85	1872,1304,IEXPLORE.EXE	NETWORK	UDP: 192.168.88.128:1157 -=> **192.168.88.2:53**, (OUT) Length=8
			00000000 : 45 00 00 3B 08 E7 00 00 80 11 00 00 C0 A8 58 80 | E..;.....X. 00000010 : C0 A8 58 02 00 00 00 00 00 00 00 00 | ..X.....
86	1872,1304,IEXPLORE.EXE	NETWORK	ICMP: 192.168.88.2 -=> **192.168.88.128**, (IN) Length=67
			00000000 : 45 00 00 57 6A 72 00 00 80 01 9E 60 C0 A8 58 02 | E..Wjr.....`..X. 00000010 : C0 A8 58 80 03 07 2F 05 00 00 00 00 45 00 00 3B | ..X.../.....E..; 00000020 : 08 E7 00 00 80 11 FF F7 C0 A8 58 80 C0 A8 58 02 | ..........X...X. 00000030 : 04 85 00 35 00 27 19 43 F3 CE 01 00 00 01 00 00 | ...5.'.C........ 00000040 : 00 00 00 00 03 77 77 77 05 62 61 69 64 75 03 63 | .....www.baidu.c 00000050 : 6F 6D 00 00 01 00 01 | om.....
87	1872,1304,IEXPLORE.EXE	NETWORK	ICMP: 192.168.88.2 -=> **192.168.88.128**, (IN) Length=67
			00000000 : 45 00 00 57 6A 73 00 00 80 01 9E 5F C0 A8 58 02 | E..Wjs....._..X. 00000010 : C0 A8 58 80 03 01 2F 0B 00 00 00 00 45 00 00 3B | ..X.../.....E..; 00000020 : 08 E7 00 00 80 11 FF F7 C0 A8 58 80 C0 A8 58 02 | ..........X...X. 00000030 : 04 85 00 35 00 27 19 43 F3 CE 01 00 00 01 00 00 | ...5.'.C........ 00000040 : 00 00 00 00 03 77 77 77 05 62 61 69 64 75 03 63 | .....www.baidu.c 00000050 : 6F 6D 00 00 01 00 01 | om.....
88	1872,1984,IEXPLORE.EXE	WRITE REGISTRY	Key=\REGISTRY\USER\S-1-5-21-1960408961- \Software\Microsoft\Windows\CurrentVersio 00004) Value=ProxyBypass, Data=12B638
89	1872,1984,IEXPLORE.EXE	WRITE REGISTRY	Key=\REGISTRY\USER\S-1-5-21-196040896 \Software\Microsoft\Windows\CurrentVersio 00004) Value=IntranetName, Data=12B638
90	1872,1984,IEXPLORE.EXE	WRITE REGISTRY	Key=\REGISTRY\USER\S-1-5-21-1960408961-790525478-839522115-1003 \Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap, (00000004) Value=UNCAsIntranet, Data=12B638
91	1872,1984,IEXPLORE.EXE	CREATE THREAD	[1872,1740,**IEXPLORE.EXE**]
92	428,516,xyztmp2.exe	ACCESS FILE	**\Device\HarddiskVolume1\DOCUME~1\birdman\LOCALS~1\Temp\tmpkill1.bat**

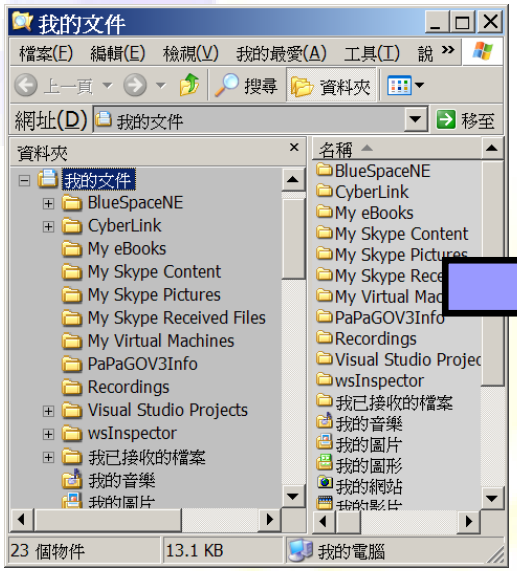
Query:
www.baidu.com ?

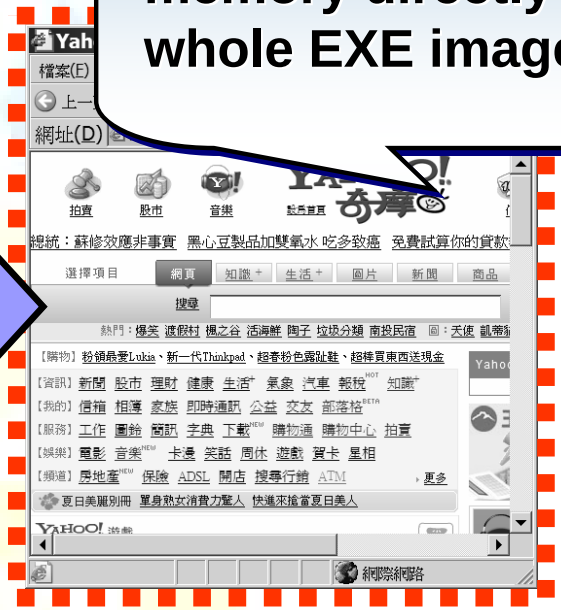
- Archon Analyzer also records the traffic of TCP, UDP and ICMP.

Case Study 3 : Code Inject

- In this case, we will reveal some sophisticated tricks about code injection. It never drop any files into disk. That is why they are so difficult to det







It overwrite the IE memory directly with a whole EXE image.

Anti-Virus : No File to Detect !! Orz

Case Study 3 : Behavior Analysis (1/2)

Drop EXE

		SSAGE	Birdman - Archon Analyzer 0.4.0.1 By http://X-Solve.com/blog (birdman@x-solve.com)
		SSAGE	---< START >----------
3	936,1632,cmd.ex	CREATE PROCESS	[176,,**spyware.exe**]
4	176,1456,spyware.ex	LOAD MODULE	\Device\HarddiskVolume1\spyware.exe (ImageBase=00400000, DLL)
5	176,1456,spyware.exe	DROP FILE	**\Device\HarddiskVolume1\WINDOWS\system32\koudmax.exe**
6	176,1456,spyware.exe	WRITE REGISTRY	Key=\REGISTRY\MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}, (00000002) Value=stubpath, Data=C:\WINDOWS\system32\koudmax.exe s
7	176,1456,spyware.exe	WRITE REGISTRY	Key=\REGISTRY\MACHINE\SOFTWARE\SKav, (00000003) Value=nck
8	176,1456,spyware.exe	WRITE REGISTRY	Key=\REGISTRY\USER\S-1-5-21-1960408961-790525478-839522115-1003\Software\SKav, (00000003) Value=klg
9	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF90000, Length=0x0000007F --> (1536)**explor**
10	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF80000, Length=0x00000120 --> (1536)**explor**
11	176,1456,spyware.exe	REMOTE THREAD	[1536,344,**explorer.exe**]
12	1536,344,explorer.exe	CREATE THREAD	[448,428,**IEXPLORE.EXE**]
13	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF90000, Length=0x00000408 --> (448)**IEXPLORE.E**
14	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF80000, Length=0x00006400 --> (448)**IEXPLORE.EXE**
15	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF70000, Length=0x00000283 --> (448)**IEXPLORE.EXE**
16	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF60000, Length=0x00000028 --> (448)**IEXPLORE.EXE**
17	176,1456,spyware.exe	REMOTE THREAD	[448,516,**IEXPLORE.EXE**]
18	448,516,IEXPLORE.EXE	LOAD MODULE	\Device\HarddiskVolume1\Program Files\Internet Explorer\IEXPLORE.EXE (ImageBase=00400000, DLL)
19	448,516,IEXPLORE.EXE	CREATE THREAD	[448,1984,**IEXPLORE.EXE**]
20	448,1984,IEXPLORE.EXE	ADJUST PRIVILEGE	Low=00000014, High=00000000
21	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF90000, Length=0x0000007F --> (1536)**explorer.exe**
22	176,1456,spyware.exe	WRITE MEMORY	Address=0x7FF80000, Length=0x00000120 --> (1536)**explorer.exe**
23	176,1456,spyware.exe	REMOTE THREAD	[1536,1512,**explorer.exe**]
24	448,1984,IEXPLORE.EXE	CREATE THREAD	[448,804,**IEXPLORE.EXE**]

Copy a whole EXE Image into IE

Case Study 3 : Behavior Analysis (2/2)

24	448,1984,IEXPLORE.EXE	**CREATE THREAD**	[448,804,**IEXPLORE.EXE**]
25	448,1984,IEXPLORE.EXE	**NETWORK**	UDP: 192.168.88.128:1157 -=> **192.168.88.2:53**, (OUT) Length=8
			00000000 : 45 00 00 3B 08 E7 00 00 80 11 00 00 C0 A8 58 80 | E..;.....X. 00000010 : C0 A8 58 02 00 00 00 00 00 00 00 00 | ..X.....
26	1744,184,Dbgview.exe	**NETWORK**	UDP: 192.168.88.2:53 -=> **192.168.88.128:1157**, (IN) Length=131
			00000000 : 45 00 00 97 00 75 00 00 80 11 08 0E C0 A8 58 02 | E....u.....X. 00000010 : C0 A8 5 AD 85 80 | ..X..5....s.$... 00000020 : 00 01 4 32 32 | .....kimo.22 00000030 : 38 38 0 01 00 | 88.org..... 00000040 : 01 00 0 02 00 | ....<..... 00000050 : 01 00 8 32 32 | ...Q....ns1.3322 00000060 : 03 6E 00 | .net.....Q.. 00000070 : 06 03 F4 49 | ..ns2.?.;.....I 00000080 : 72 00 00 02 8F | r..=._).U..... 00000090 : 65 00 04 DE B9 F5 FE | e.....
27	448,1984,IEXPLORE.EXE	**NETWORK**	TCP: 192.168.88.128:1158 -=> **210.177.146.251:443**, (OUT) Length=28
			00000000 : 45 00 00 30 08 E8 40 00 80 06 00 00 C0 A8 58 80 | E..0..@.....X. 00000010 : D2 B1 92 FB 00 00 00 00 00 00 00 00 00 00 00 00 | .... 00000020 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ....
28	448,1984,IEXPLORE.EXE	**NETWORK**	TCP: 192.168.88.128:1158 -=> **210.177.146.251:443**, (OUT) Length=20
			00000000 : 45 00 00 67 08 EA 40 00 80 06 00 00 C0 A8 58 80 | E..g..@.....X. 00000010 : D2 B1 92 FB 00 00 00 00 00 00 00 00 00 00 00 00 | .... 00000020 : 00 00 00 00 00 00 00 00 | ....
29	448,1984,IEXPLORE.EXE	**NETWORK**	TCP: 192.168.88.128:1158 -=> **210.177.146.251:443**, (OUT) Length=20
			0000 6 00 00 C0 A8 58 80 | E..(..@.....X. 0000 00 00 00 00 00 00 | .... 0000 | ....
30	4,56,System	**ACCESS FILE**	**\Device\HarddiskVolume1\Documents and Settings\birdman\NTUSER.DAT.LOG**
31	4,56,System	**ACCESS FILE**	**\Device\HarddiskVolume1\WINDOWS\system32\config\software.LOG**
32	4,56,System	**ACCESS FILE**	**\Device\HarddiskVolume1\WINDOWS\system32\config\system.LOG**

DNS Query:
kimo.2288.org
ns1.3322.net

Spyware Log file

Scanner VS. Analyzer

- **Archon Scanner**
  - **Work In the wild**
    - It works in the uncontrolled environment.
  - Focus on find out unknown malicious software
  - Behavior Scanner
  - Forensic Tool

- **Archon Analyzer**
  - **Work In the zoo**
  - Focus on analyze malicious behavior of certain target.
  - Behavior Monitor
  - ***Software Malicious Behavior Testing Tool***
  - Lab Tool

Conclusion

- The danger of Spyware is very real, and Rootkit technology is the latest trend in hiding Spyware from users and Anti-Spyware software. Stealing of information and compromise of private data can continue unnoticed for days, weeks and sometimes months. Through personal policies and the latest technology, you can actively protect your company's network, and take a stand against Malware.

Q&A&THX

- Greez
  - All the great Rootkit hackers on Earth.
  - Mr. SSCAN, ICST
  - Archon Team, **X-Solve**
  - And all my friends ☺