A TROJAN THAT CAN MODIFY THE HARD DISK FIRMWARE

——A Discovery to the Attack Components of the EQUATION Group

Antiy Labs

Time of the first version: 10:00 a.m. March 5, 2015

The updated time of this version: 09:45 a.m. March 9, 2015

Content

1 Background

According to the emergency study, Antiy Labs has started to analysis and verify the attack components of the attack organization called Equation by our friend of business on February 18th, 2015. Then we set up the inter-departmental JAG (Joint Analysis Group) on February 25th and finished the first edition of this report on March 4th.

The relevant background is as follows: Kaspersky Labs issued a series of reports on February 16th, which revealed the most complex network attack organization -- Equation Group[1]—that may exist in the world. According to Kaspersky Labs, the C&C used by this group has been registered in 1996, which indicates that this group might have been active for 20 years. As they can always find vulnerabilities earlier than other groups, they have had absolute advantages for years. The Group has a super standard information weapon arsenal, which includes two malware modules that can reprogram dozens of common brands of hard disk firmware. This might be the most characteristic attack weapon the Group possesses and the first known malware that can infect hard disk firmware. The reports of Kaspersky issued on February 17 and 19 have published the detail analysis result of 2 modules, which are Fanny and DoubleFantasy. According to the analysis of relevant clues, Kaspersky believes the attack targets include Russia, India, China and other countries. While the relevant media has concludes that this Group may be related to the intelligence agencies of America.

In light of the complexity of samples and the unique characteristic of attacking hard disk firmware, our analysis progress is extremely slow. Now we share the limited analysis results in order to promote more and more participations and collaborations among our industry. Our report does not make more references and repeats on the contents that have been fully discussed in Kaspersky’s report. Therefore, readers are advised to read Kaspersky’s report in the first place, and then read this report to give valuable comments.

2 The components used by the Equation Group

The discovered arsenal of the Equation Group has at least 6 pieces of equipment: EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny and GrayFish. The engineers of

Antiy Labs called them “components”. Except for these components, Kaspersky also provided other malware hashes that might be used by Equation. The corresponding programs include: EQUESTRE (being similar with EquationDrug), GROK keylogger, installation program of DoubleFantasy, LNK exploit program of _SD_IP_CF.dll and module nls_933w.dll that can reprogram the hard disk.

Component Name	Introduction	Time
EquationLaser	The implantation program used by the Equation Group during 2001 and 2004 is compatible both Windows 95 and Windows 98.	2001-2003
EquationDrug	It is a complex attack component used by this Group that can be used for supporting the module plug-in system which is uploaded dynamically and uninstalled by the attackers. It is suspected as the upgrading version of EquationLaser.	2003-2013
DoubleFantasy	It is a kind of authentication Trojan that can confirm whether the targets are the expected ones. When it confirms the target, the implanted malware would upgrade to a more complex platform, such as EQUATIONDRUG or GRAYFISH.	2004-2012
TripleFantasy	It is the full-featured backdoor that cooperates with GRAYFISH sometimes. It seems to be the upgraded version of DOUBLEFANTASY. It might be the updated authentication plug-in.	2012- Now
Fanny	It is a kind of worm established in 2008 that makes use of USB devices to spread. It can attack the physically isolated network and return the collected information. It is used to collect the target information that located in the Middle East and Asia. Some victims appeared to have been upgraded to DoubleFantasy, then EQUATIONDRUG. It makes use of two zero-day vulnerabilities that are applied to Stuxnet.	2008-2011
GrayFish	It is the most complex attack component that resides entirely in the registry. It executes when the bootkit enables in the operation system.	2008- Now

The schematic diagram of the six components of the Equation Group:

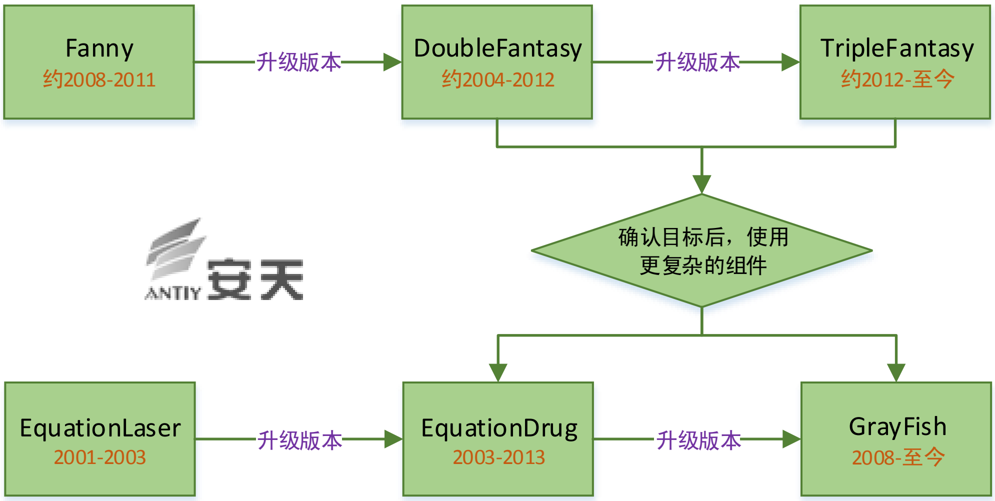


Figure 1 The schematic diagram of the component relationship

The Equation Group selects Fanny or DoubleFantasy or TripleFantasy as the leading part of attack. When the Group confirms the expected targets, it would use more complex component EquationDrug or GrayFish.

Currently, the analysis team of Antiy Labs focuses on the attack leading component (DoubleFantasy) and the more complex component (EquationDrug and GrayFish). Meanwhile, we analyze the component that can reprogram the hard disk firmware, namely nls_933w.dll.

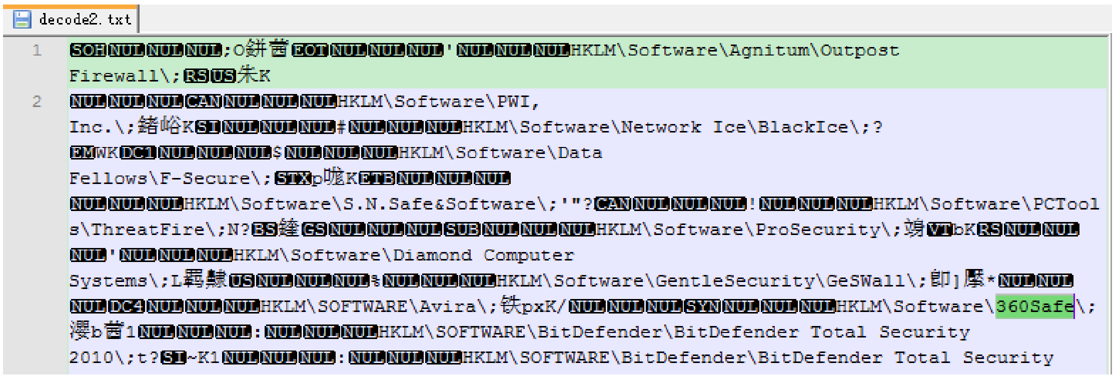
3 Analysis on DoubleFantasy

Component DoubleFantasy is used for confirming the attack target. If the target belongs to the field that the Equation Group is interested in, then other more complex components will be injected into the attacked machine from the remote points.

The Kaspersky's report has analyzed DoubleFantasy in detail; the analysis team of Antiy Labs was going to verify DoubleFantasy. However, we have found that this component has been analyzed before during the verification process and found other relevant malware. Meanwhile, we also found the information that has not been revealed by our friend of business.

3.1 Detecting the security software

Component DoubleFantasy enumerates the registry key to find out whether the system installs security software. The security software list is in the resource section and uses 0x79 XOR encryption. The Kaspersky's report provided the security software list; there are 10 types in total. While the analysis team of Antiy Labs found this component detects 13 kinds of security software. Except for the 10 types of products, there are products of 360, BitDefender and Avira.



```
SOHNULNULNUL;O鉼茜EOTNULNULNUL'NULNULNULHKLM\Software\Agnitum\Outpost
Firewall\;RSUS朱K
NULNULNULCANNULNULNULHKLM\Software\PWI,
Inc.\;鍺峪KSINULNULNUL#NULNULNULHKLM\Software\Network Ice\BlackIce\;?
EMWKDC1NULNULNUL$NULNULNULHKLM\Software\Data
Fellows\F-Secure\;STXp哤KETBNULNULNUL
NULNULNULHKLM\Software\S.N.Safe&Software\;'"?CANNULNULNUL!NULNULNULHKLM\Software\PCTool
s\ThreatFire\;N?BS鏲GSNULNULNULSUBNULNULNULHKLM\Software\ProSecurity\;竴VTbKRSNULNUL
NUL'NULNULNULHKLM\Software\Diamond Computer
Systems\;L羁隸USNULNULNUL%NULNULNULHKLM\Software\GentleSecurity\GeSWall\;即]槧*NULNUL
NULDC4NULNULNULHKLM\SOFTWARE\Avira\;铁pxK/NULNULNULSYNNULNULNULHKLM\Software\360Safe\;
瀴b茜1NULNULNUL:NULNULNULHKLM\SOFTWARE\BitDefender\BitDefender Total Security
2010\;t?SI~K1NULNULNUL:NULNULNULHKLM\SOFTWARE\BitDefender\BitDefender Total Security
```

As the main customers of 360 Security are located in China, it also verifies in a further step that China is one of the targets of the Equation Group

3.2 Returning the information

DoubleFantasy collects the system information and returns to the attacker. The returning pattern is as follows:

000:MAC add. 001:IP add.......019: current time

The detail information returned is as follows:

No.	Explanation	No.	Explanation	No.	Explanation
000	MAC address	**007**	System patch information (CSDVersion， such as sp1)	**014**	Network connecting type
001	IP address	**008**	CurrentBuildNumber (such as 2600)	**015**	The installed software informaiton
002	Sample version No.	**009**	System CurrentVersion (5.1)	**016**	Unknown
003	Sample ID	**010**	ProductID	**017**	N/A
004	Proxy setting information	**011**	Location information 1	**018**	32 bit or 64 bit
005	Registry information 1	**012**	Location information 2	**019**	Current time

	(RegisteredOwner)				
006	Registry information 2 (RegisteredOrganization)	013	System directory		

3.3 Communication protocol

The returning package of the controlled end of DoubleFantasy is: the first byte does not encrypt and the following data is in encryption. For instance, 0x42 command is as follows:

The detail functionality of 0x42 command branch

- Functionality: back on-line, initiating the communication key, deleting itself, clearing the infected traces.
- The pattern of the controlling end: the first byte is command code 0x42, the second byte is command branch that includes three types: 00 instant back on-line, 01 initiating the communication key, back on-line after sleeping 60 seconds, 02 deleting itself, clearing the infected traces.
- The returning package pattern of the controlled end: none.

3.4 New version, C&C, Keys

The Kaspersky's report has provided the following information about the relevant components: version, C&C lists and keys. After further analysis, we have obtained more relevant information. The green parts in the following are from Kaspersky's report, while the red (Bold) parts are the new information analyzed by Antiy Labs.

List of versions:

8.1.0.4 (MSREGSTR.EXE)
008.002.000.006
008.002.001.001
008.002.001.004
008.002.001.04A (subversion "IMIL3.4.0-IMB1.8.0")
008.002.002.000
008.002.003.000
008.002.004.000
008.002.005.000
008.002.005.001
008.002.006.000
011.000.001.001
012.001.000.000
012.001.001.000
012.002.000.001
012.003.001.000

012.003.004.000
012.003.004.001
013.000.000.000

C&C:

advancing-technology[.]com
avidnewssource[.]com
businessdealsblog[.]com
businessedgeadvance[.]com
charging-technology[.]com
computertechanalysis[.]com
config.getmyip[.]com - SINKHOLED BY KASPERSKY LAB
globalnetworkanalys[.]com
melding-technology[.]com
myhousetechnews[.]com - SINKHOLED BY KASPERSKY LAB
newsterminalvelocity[.]com - SINKHOLED BY KASPERSKY LAB
selective-business[.]com
slayinglance[.]com
successful-marketing-now[.]com - SINKHOLED BY KASPERSKY LAB
taking-technology[.]com
techasiamusicsvr[.]com - SINKHOLED BY KASPERSKY LAB
technicaldigitalreporting[.]com
timelywebsitehostesses[.]com
www.dt1blog[.]com
www.forboringbusinesses[.]com
Ign***list.com
Dat***cemgmt.net
Imp***today.com
Bud***nessnews.com

The new keys:

37 08 EF 89 29 A7 4B 6B AB 3E 5D 03 F6 B0 B5 B3
66 39 71 3C 0F 85 99 81 20 19 35 43 FE 9A 84 11
8B 4C 25 04 56 85 C9 75 06 33 C0 5E C2 08 31 F6
32 EC 89 D8 0A 78 47 22 BD 58 2B A9 7F 12 AB 0C

Component DoubleFantasy is usually the first step of victims being infected by the Equation Group. It confirms the victim’s information through communicating with the backdoor and examining different system parameters. Once the victim is confirmed, the Equation Group would adopt the more complex components EquationDrug or Grayfish.

4 Analysis on component EquationDrug

Component EquationDrug is a very complex module. It has existed for nearly ten years and later been replaced by the GrayFish upgrading. We found in our analysis that some file names of the two modules share similarity; there are also some similar techniques in terms of obfuscation encryption. They decrypt, decompress and release files from the resources. We found SYS file and VXD file existed in the resource during our analysis. VXD is the driving mechanism on Windows 9x, so we firmly believe that this module has the capability of infecting Windows 9x. EquationDrug is a plug-in platform with the functionalities of installing and uninstalling the plug-ins.

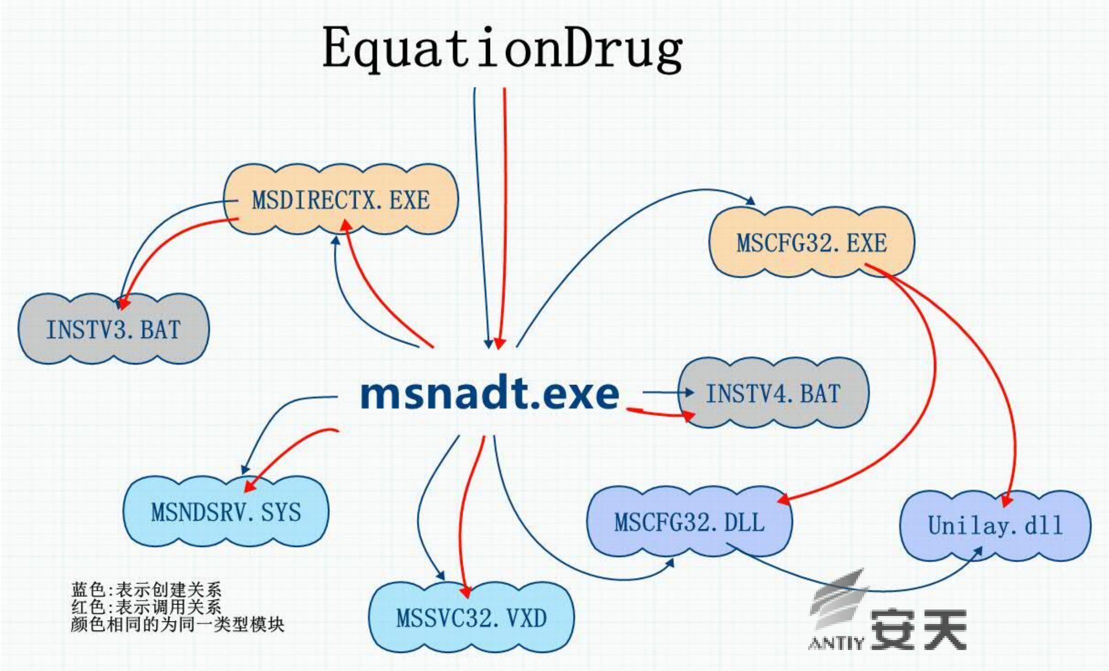


Figure 2 The relationship diagram of the establishment and calling of component EquationDrug

Module name	Functionality
msnadt.exe	The main functionalities are as follows: releasing files, decrypting resources, judging system types, injecting code into the specified process and downloading drives and so on.
MSDIRECTX.EXE	Setting up INSTV3.BAT and executing self-deleting.
MSCFG32.exe	Downloading MSCFG32.DLL, adding and modifying the registry.
MSCFG32.DLL	It can add and modify the registry, release unity.dll file. It has relationship with the driving files with networking functionality.

unity.dll	There are a large amount of file operations and registry operations.
MSNDSRV.SYS MSSVC32.VXD	Sharing the same functionalities basically. VXD is used on Wndows9.x, which main functionalities are hook, network monitoring and writing files. It can also determine whether there is MSlog32.dat; if so, it would open to write data; if not, it would establish a new one.
INSTV3.BAT INSTV4.BAT	Deleting files by itself.

4.1 Detecting the security software

It enumerates the registry key to check whether the system installs security software. The security software list is under the resource chapter.

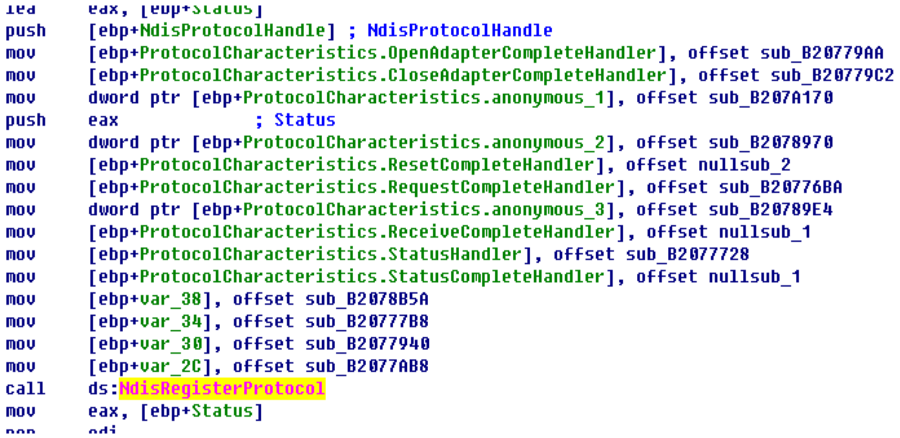
The security software it detected is more than the one DoubleFantasy component did with more different types. The Chinese security software it detected is Rising, instead of the current popular 360. Therefore, this also verified the conclusion above that this component has been replaced by the updated one. The relevant detected registry key is as follows:

Zone Labs\TrueVector\
Zone Labs\ZoneAlarm\
KasperskyLab\
Network Ice\BlackIce\
Agnitum\Outpost Firewall\
Sygate Technologies, Inc.\Sygate Personal Firewall\
Norman\
Data Fellows\F-Secure\
PWI, Inc.\
rising\
Softwin\
network associates\tvd\shared components\on access scanner\behaviourblocking\FileBlockEnabled_27!=0
network associates\tvd\shared components\on access scanner\behaviourblocking\FileBlockEnabled_28!=0
network associates\tvd\shared components\on access scanner\behaviourblocking\FileBlockEnabled_29!=0
network associates\tvd\shared components\on access scanner\behaviourblocking\FileBlockEnabled_30!=0
McAfee\ePolicy Orchestrator\Application Plugins\VIRUSCAN8600
Sophos\
CA\CAPF\
CA\HIPSEngine\
Cisco\
Symantec\IDS\
Symantec\Norton 360\

Symantec\Internet Security\SuiteOwnerGuid\
Symantec\Norton AntiBot
Symantec\Symantec Endpoint Protection
Tiny Software\Tiny Firewall
CyberMedia Inc\Guard Dog
McAfee\Guard Dog
McAfee\McAfee Firewall
McAfee\Personal Firewall
McAfee.com\Personal Firewall
Network Associates\McAfee Fire
Kerio
BullGuard Ltd.\BullGuard
TheGreenBow
Panda Software\Firewall\
TrendMicro\PC-cillin\
ComputerAssociates\eTrust Suite Personal\pfw\
Grisoft\Firewall\

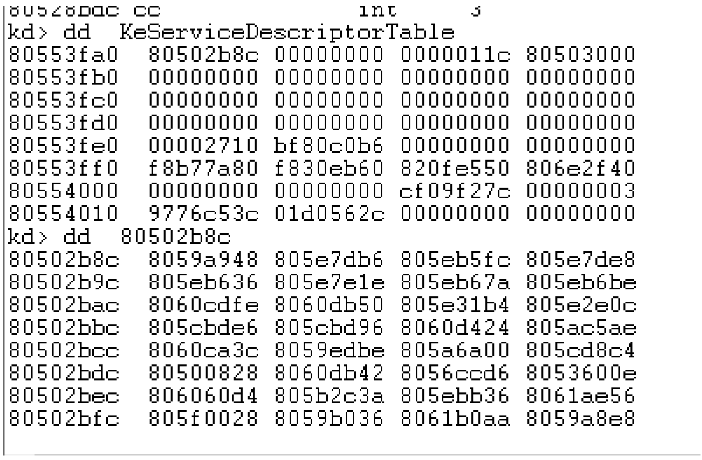
4.2 Analysis on the drive moduleMSNDSRV.SYS

1. It retrieved the entire network adapter during the drive initialization process. Then it called function NdisRegisterProtocol to registered a NDIS protocol related structure for NDIS base. Then the drive can receive all the network traffic, which is similar with package capture mechanism of WinPcap. The relevant code is as follows:



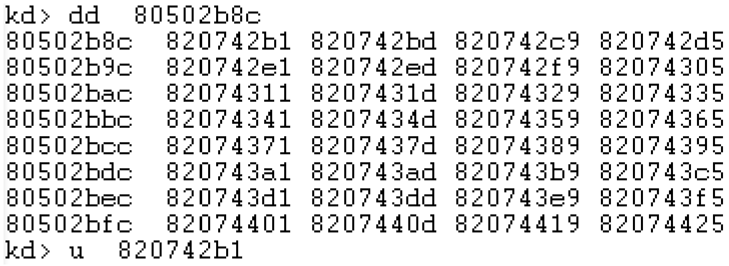
```
lea     eax, [ebp+Status]
push    [ebp+NdisProtocolHandle] ; NdisProtocolHandle
mov     [ebp+ProtocolCharacteristics.OpenAdapterCompleteHandler], offset sub_B20779AA
mov     [ebp+ProtocolCharacteristics.CloseAdapterCompleteHandler], offset sub_B20779C2
mov     dword ptr [ebp+ProtocolCharacteristics.anonymous_1], offset sub_B207A170
push    eax             ; Status
mov     dword ptr [ebp+ProtocolCharacteristics.anonymous_2], offset sub_B2078970
mov     [ebp+ProtocolCharacteristics.ResetCompleteHandler], offset nullsub_2
mov     [ebp+ProtocolCharacteristics.RequestCompleteHandler], offset sub_B20776BA
mov     dword ptr [ebp+ProtocolCharacteristics.anonymous_3], offset sub_B20789E4
mov     [ebp+ProtocolCharacteristics.ReceiveCompleteHandler], offset nullsub_1
mov     [ebp+ProtocolCharacteristics.StatusHandler], offset sub_B2077728
mov     [ebp+ProtocolCharacteristics.StatusCompleteHandler], offset nullsub_1
mov     [ebp+var_38], offset sub_B2078B5A
mov     [ebp+var_34], offset sub_B20777B8
mov     [ebp+var_30], offset sub_B2077940
mov     [ebp+var_2C], offset sub_B2077AB8
call    ds:NdisRegisterProtocol
mov     eax, [ebp+Status]
pop     edi
```

2. Modifying the function address of KeServiceDescriptorTable.



```
80528bac cc              int     3
kd> dd  KeServiceDescriptorTable
80553fa0  80502b8c 00000000 0000011c 80503000
80553fb0  00000000 00000000 00000000 00000000
80553fc0  00000000 00000000 00000000 00000000
80553fd0  00000000 00000000 00000000 00000000
80553fe0  00002710 bf80c0b6 00000000 00000000
80553ff0  f8b77a80 f830eb60 820fe550 806e2f40
80554000  00000000 00000000 cf09f27c 00000003
80554010  9776c53c 01d0562c 00000000 00000000
kd> dd  80502b8c
80502b8c  8059a948 805e7db6 805eb5fc 805e7de8
80502b9c  805eb636 805e7e1e 805eb67a 805eb6be
80502bac  8060cdfe 8060db50 805e31b4 805e2e0c
80502bbc  805cbde6 805cbd96 8060d424 805ac5ae
80502bcc  8060ca3c 8059edbe 805a6a00 805cd8c4
80502bdc  80500828 8060db42 8056ccd6 8053600e
80502bec  806060d4 805b2c3a 805ebb36 8061ae56
80502bfc  805f0028 8059b036 8061b0aa 8059a8e8
```

Figuer 3 The original function address in KeServiceDescriptorTable



```
kd> dd  80502b8c
80502b8c  820742b1 820742bd 820742c9 820742d5
80502b9c  820742e1 820742ed 820742f9 82074305
80502bac  82074311 8207431d 82074329 82074335
80502bbc  82074341 8207434d 82074359 82074365
80502bcc  82074371 8207437d 82074389 82074395
80502bdc  820743a1 820743ad 820743b9 820743c5
80502bec  820743d1 820743dd 820743e9 820743f5
80502bfc  82074401 8207440d 82074419 82074425
kd> u  820742b1
```

Figure 4 The modified function address of KeServiceDescriptorTable

The modified function address only includes one JMP command. If the function in KeServiceDescriptorTable is not its hook target, it would return to the original function address, otherwise it would jump to the functions that drive itself.

The address of nt!NtAcceptConnectPort in KeServiceDescriptorTable is 820742b1.

Here the instruction is as follows:

```
820742b1 2eff25b8420782    jmp        dword ptr cs:[820742B8h]
```

820742B8 is the corresponding address of NtAcceptConnectPort. While the address of function NtTerminateProcess in KeServiceDescriptorTable is 0x81cf9ebd. Here the command is:

```
81cf9ebd 2eff25c49ecf81    jmp        dword ptr cs:[81CF9EC4h]
```

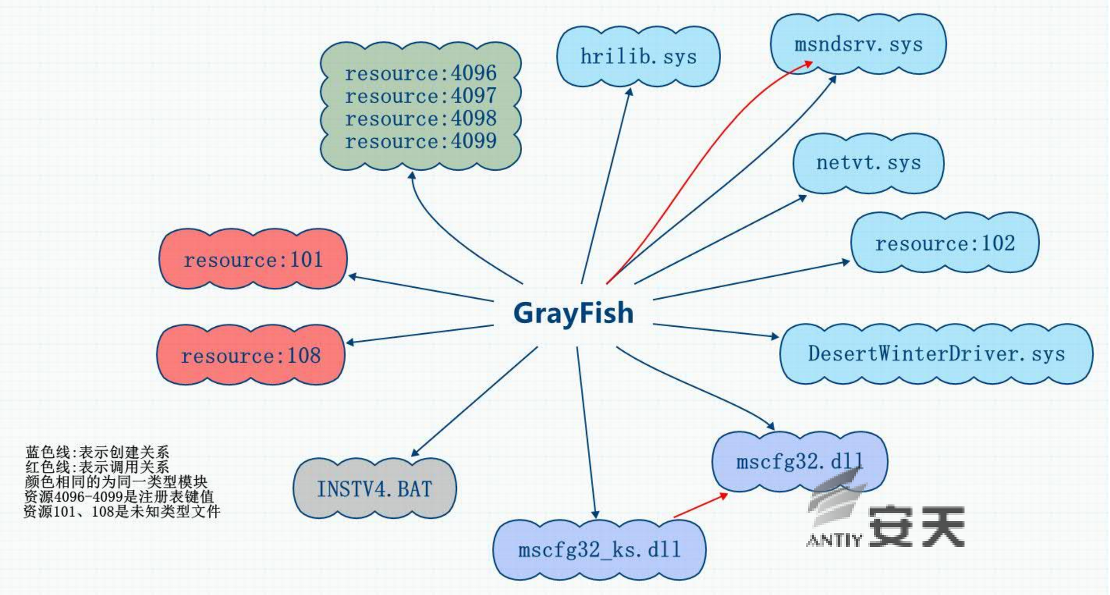
The address contains in 81CF9EC4 is b1fd6eae which directs to a drive function. The function that drives hook is:

NtClose
NtCreateFile
NtCreateKey
NtCreateProcess
NtCreateProcessEx

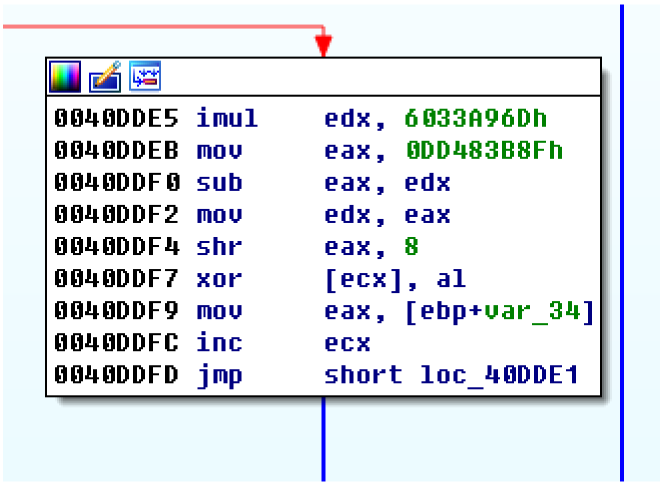
NtCreateThread
NtEnumerateKey
NtOpenFile
NtOpenKey
NtOpenProcess
NtQueryAttributesFile
NtQueryDirectoryFile
NtQueryDirectoryObject
NtQueryFullAttributesFile
NtQueryKey
NtQuerySystemInformation
NtSetInformationFile
NtTerminateProcess

5 Analysis on component GrayFish

GrayFish is the most complex component of the Equation Group. It is the new version of EquationDrug. The most important characteristics we believe are: it does not depend on the file carrier, completely existing in the registry, executing by bootkit when system is enabling. This mechanism penetrated the limitation of security products of making files as detecting objects and the solutions based on whitelist and trusted computing.



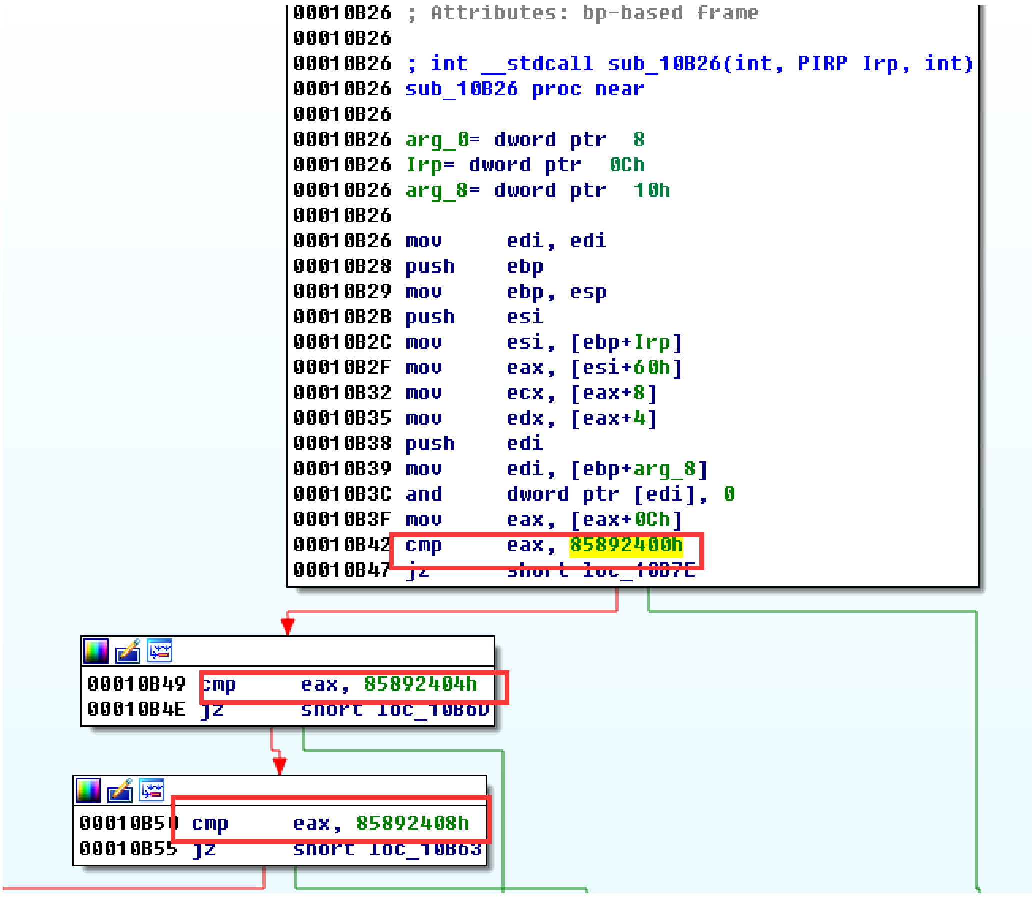
The resource section of component GrayFish includes 13 kinds of encryption resource, which are decrypted by the same paragraph decryption algorithm.



```
0040DDE5 imul    edx, 6033A96Dh
0040DDEB mov     eax, 0DD483B8Fh
0040DDF0 sub     eax, edx
0040DDF2 mov     edx, eax
0040DDF4 shr     eax, 8
0040DDF7 xor     [ecx], al
0040DDF9 mov     eax, [ebp+var_34]
0040DDFC inc     ecx
0040DDFD jmp     short loc_40DDE1
```

The decrypted 13 files include five SYS files, two DLL files, four files with registry data, a configuration file with string “services.exe” and an encrypted data file.

After dynamic debugging, it is found that three SYS files (hrilib.sys, msndsrv.sys and netvt.sys) were released by the original samples, including network drive and registry-related operation functions. mscfg32_ks.dll, having the functionalities of establishing remote thread, accessing system information, establishing and deleting registry key, would call mscfg32.dll. Besides these three released SYS files, resource 102 contains the functions that operates the registry, while DesertWinterDriver.sys contains the comparisons with IoControlCode, the specific functionality is to be analyzed.



```
00010B26 ; Attributes: bp-based frame
00010B26
00010B26 ; int __stdcall sub_10B26(int, PIRP Irp, int)
00010B26 sub_10B26 proc near
00010B26
00010B26 arg_0= dword ptr  8
00010B26 Irp= dword ptr  0Ch
00010B26 arg_8= dword ptr  10h
00010B26
00010B26 mov     edi, edi
00010B28 push    ebp
00010B29 mov     ebp, esp
00010B2B push    esi
00010B2C mov     esi, [ebp+Irp]
00010B2F mov     eax, [esi+60h]
00010B32 mov     ecx, [eax+8]
00010B35 mov     edx, [eax+4]
00010B38 push    edi
00010B39 mov     edi, [ebp+arg_8]
00010B3C and     dword ptr [edi], 0
00010B3F mov     eax, [eax+0Ch]
00010B42 cmp     eax, 85892400h
00010B47 jz      short loc_10B7E

00010B49 cmp     eax, 85892404h
00010B4E jz      short loc_10B6D

00010B50 cmp     eax, 85892408h
00010B55 jz      short loc_10B63
```

Besides, the original sample would generate batch to delete itself. The batch file name is the same one that EquationDrug used to delete itself, which also indicates a close relationship between them.

6 Analysis on the reprogramming module nls_933w.dll

nls_933w.dll is the module that can reprogram hard disk firmware. As Antiy analysis team lacks the reserve knowledge of hard disk firmware field, the analysis is processing very slowly. According to current analysis, when module nls_933w.dll is called by other programs, it would release file win32m.sys which is responsible for communicating with hard disk controller. File win32m.sys can determine the types of hard disk controller and send corresponding control commands, such as IED, SATA and so on. Therefore, if the attackers are familiar with the ATA commands that different vendors specified, then they can carry out malicious tampering on hard disk firmware.

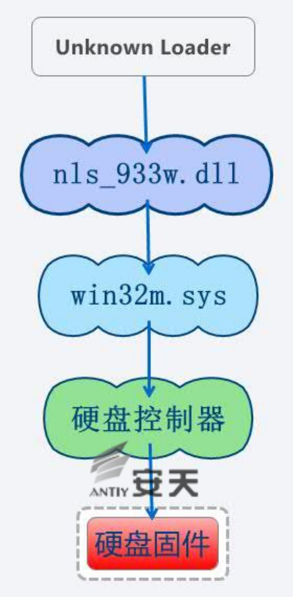
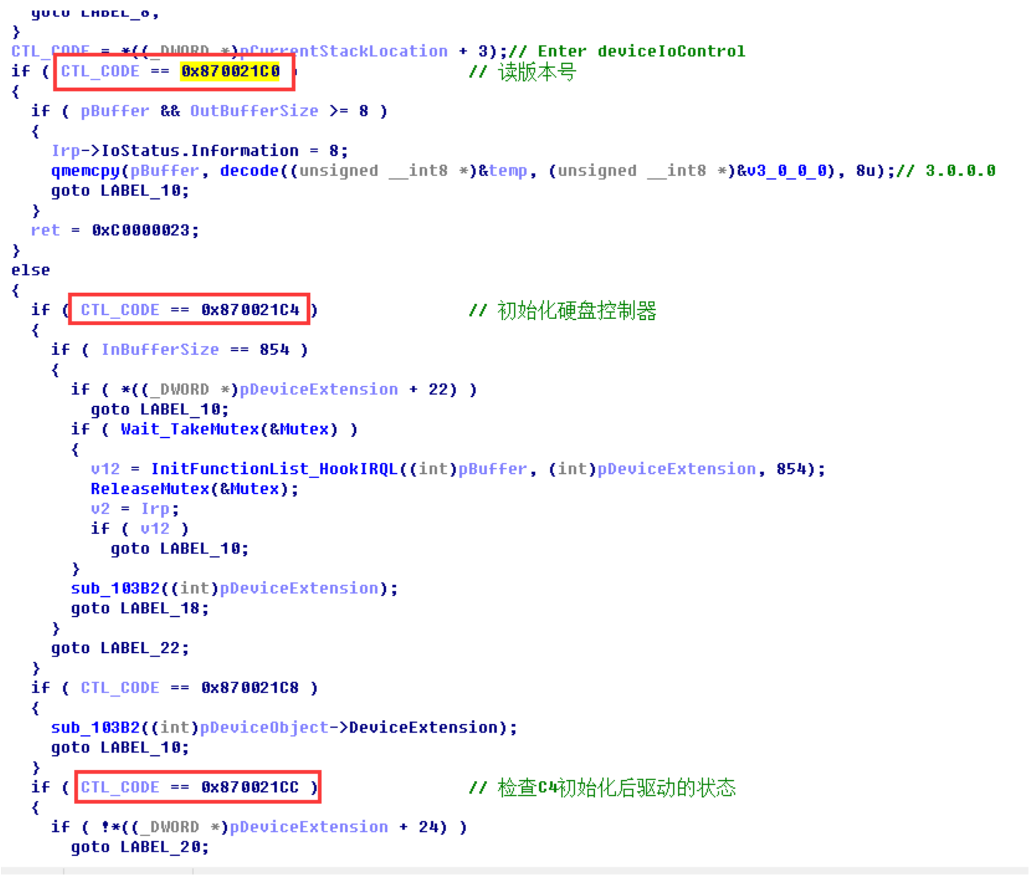


Figure 5 The flow chart of modifying the hard disk's firmware

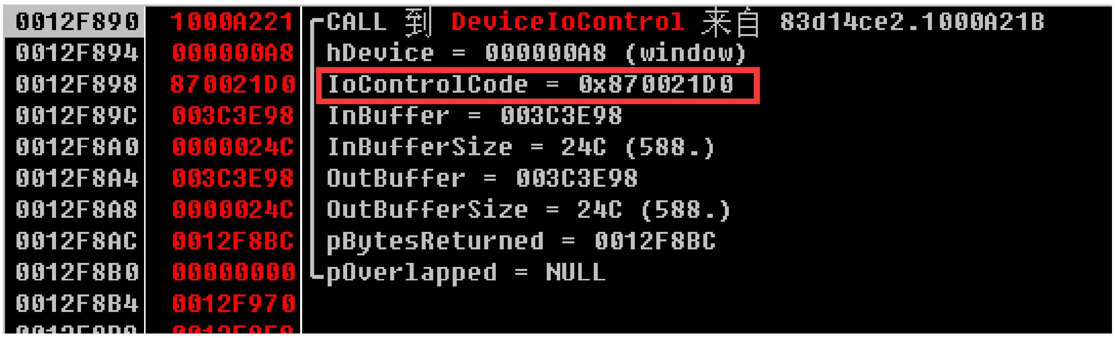
With the dynamic debugging operation, Antiy analysis team found that this module called the function DeviceIoControl to interact with win32m.sys. For the win32m.sys, the team found several IoControlCodes and analyzed their corresponding functions.



```
    goto LABEL_8;
  }
  CTL_CODE = *((_DWORD *)pCurrentStackLocation + 3);// Enter deviceIoControl
  if ( CTL_CODE == 0x870021C0 )                      // 读版本号
  {
    if ( pBuffer && OutBufferSize >= 8 )
    {
      Irp->IoStatus.Information = 8;
      qmemcpy(pBuffer, decode((unsigned __int8 *)&temp, (unsigned __int8 *)&v3_0_0_0), 8u);// 3.0.0.0
      goto LABEL_10;
    }
    ret = 0xC0000023;
  }
  else
  {
    if ( CTL_CODE == 0x870021C4 )                    // 初始化硬盘控制器
    {
      if ( InBufferSize == 854 )
      {
        if ( *((_DWORD *)pDeviceExtension + 22) )
          goto LABEL_10;
        if ( Wait_TakeMutex(&Mutex) )
        {
          v12 = InitFunctionList_HookIRQL((int)pBuffer, (int)pDeviceExtension, 854);
          ReleaseMutex(&Mutex);
          v2 = Irp;
          if ( v12 )
            goto LABEL_10;
        }
        sub_103B2((int)pDeviceExtension);
        goto LABEL_18;
      }
      goto LABEL_22;
    }
    if ( CTL_CODE == 0x870021C8 )
    {
      sub_103B2((int)pDeviceObject->DeviceExtension);
      goto LABEL_10;
    }
    if ( CTL_CODE == 0x870021CC )                    // 检查C4初始化后驱动的状态
    {
      if ( !*((_DWORD *)pDeviceExtension + 24) )
        goto LABEL_20;
```

Figure 6 The functions corresponding to the IoControlCode

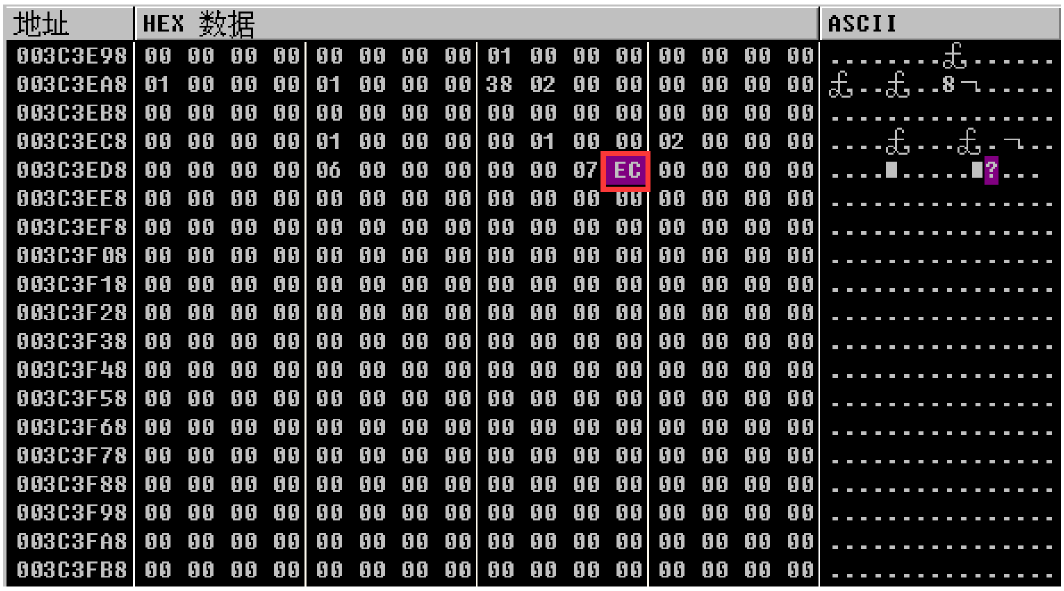
Antiy team found that when IoControlCode was 0x870021D0, nls_933w.dll delivered ATA control command to hard disk controller, i.e. 0xEC , getting the related information about the hard disk.



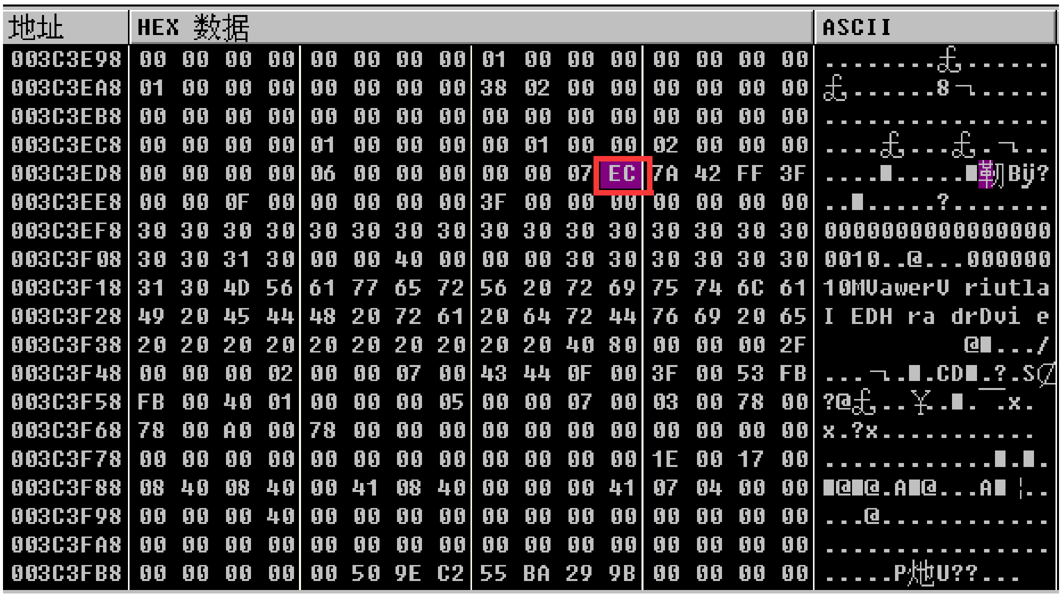
```
0012F890  1000A221  ┌CALL 到 DeviceIoControl 来自 83d14ce2.1000A21B
0012F894  000000A8  │hDevice = 000000A8 (window)
0012F898  870021D0  │IoControlCode = 0x870021D0
0012F89C  003C3E98  │InBuffer = 003C3E98
0012F8A0  0000024C  │InBufferSize = 24C (588.)
0012F8A4  003C3E98  │OutBuffer = 003C3E98
0012F8A8  0000024C  │OutBufferSize = 24C (588.)
0012F8AC  0012F8BC  │pBytesReturned = 0012F8BC
0012F8B0  00000000  └pOverlapped = NULL
0012F8B4  0012F970
```

Figure 7 Getting information about the hard disk

The data comparison in the memory before and after calling DeviceIoControl, and it returns the hard disk information after the calling:



```
地址      HEX 数据                                            ASCII
003C3E98  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ........£.......
003C3EA8  01 00 00 00 01 00 00 00 38 02 00 00 00 00 00 00  £...£...8¬......
003C3EB8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3EC8  00 00 00 00 01 00 00 00 00 01 00 00 02 00 00 00  ....£....£..¬...
003C3ED8  00 00 00 00 06 00 00 00 00 00 07 EC 00 00 00 00  ....█.....█?....
003C3EE8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3EF8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F08  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F18  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F28  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F38  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F48  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F58  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F68  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F78  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F88  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3F98  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3FA8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3FB8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```



```
地址      HEX 数据                                          ASCII
003C3E98  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ........£.......
003C3EA8  01 00 00 00 00 00 00 00 38 02 00 00 00 00 00 00  £.......8¬......
003C3EB8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3EC8  00 00 00 00 01 00 00 00 00 01 00 00 02 00 00 00  ....£...£.¬...
003C3ED8  00 00 00 00 06 00 00 00 00 00 07 EC 7A 42 FF 3F  ....■......■剌Bÿ?
003C3EE8  00 00 0F 00 00 00 00 00 3F 00 00 00 00 00 00 00  ..■.....?.......
003C3EF8  30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
003C3F08  30 30 31 30 00 00 40 00 00 00 30 30 30 30 30 30  0010..@...000000
003C3F18  31 30 4D 56 61 77 65 72 56 20 72 69 75 74 6C 61  10MVawerV riutla
003C3F28  49 20 45 44 48 20 72 61 20 64 72 44 76 69 20 65  I EDH ra drDvi e
003C3F38  20 20 20 20 20 20 20 20 20 20 40 80 00 00 00 2F            @■.../
003C3F48  00 00 00 02 00 00 07 00 43 44 0F 00 3F 00 53 FB  ...¬.■.CD■.?.S∅
003C3F58  FB 00 40 01 00 00 00 05 00 00 07 00 03 00 78 00  ?@£..￥.■. ̄.x.
003C3F68  78 00 A0 00 78 00 00 00 00 00 00 00 00 00 00 00  x.?x...........
003C3F78  00 00 00 00 00 00 00 00 00 00 00 00 1E 00 17 00  ............■.■.
003C3F88  08 40 08 40 00 41 08 40 00 00 00 41 07 04 00 00  ■@■@.A■@...A■¦..
003C3F98  00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
003C3FA8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003C3FB8  00 00 00 00 00 50 9E C2 55 BA 29 9B 00 00 00 00  .....P炧U??...
```

Other functions corresponding to the IoControlCode and ATA commands need to be further analyzed and found.

7 The mechanism analysis of attacking the hard disk firmware

7.1 The structure and working principle of the hard disk

Whether the traditional mechanical hard disk or the solid state disk, they are similar on the structure. In terms of the mechanical hard disk, motor drive circuit and head control circuit, the hard disk is composed primarily of processor, cache, Boot ROM and main storage medium.

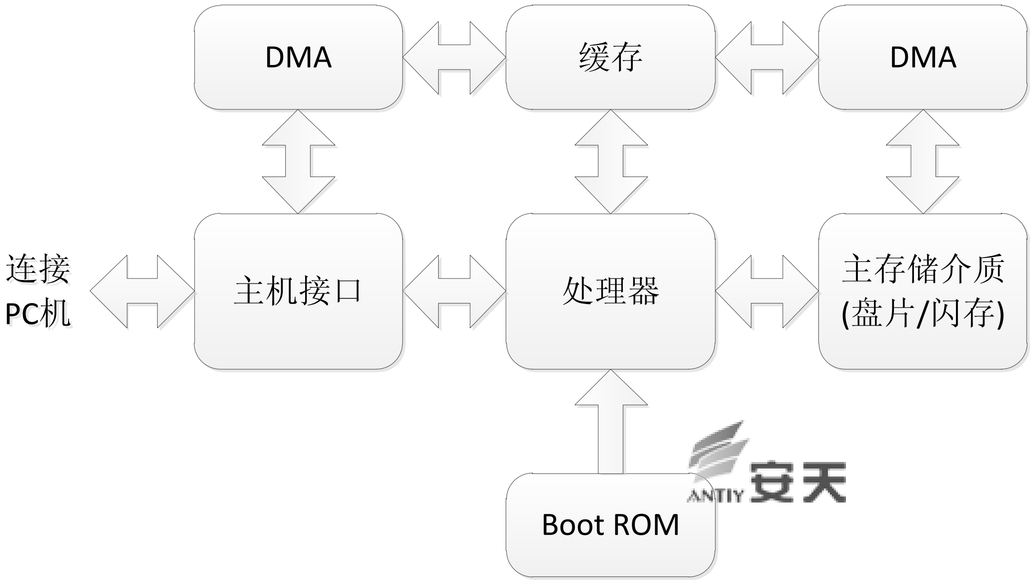


Figure 8 The functional block diagram of the hard disk

Since there are CPU, memory and ROM on the circuit board, the hard disk can be considered as a small computer system, and implement its own actions under the control of the firmware. The current common hard disk's processors are all based on the ARM core, while the multi-core structure is even adopted by new processors to ensure the rapid data transmission.

When the hard disk is energized, the processor execute on-chip Loader code, which will load and execute the Boot ROM to the cache (for the embedded processor, this is the internal storage). Boot ROM may be stored at on-chip FLASH in the main control, independent I2C EEPROM, SPI FLASH chip or NAND FLASH array in solid state disk. After getting the control right, Boot ROM will initialize the basic device and the main storage medium, load the firmware's main body from the main storage medium, start the driver module of IDE/SATA bus interface, and entry standby state, at this time the computer can operate the hard disk.

1) The traditional mechanical hard disk

For the most mechanical hard disks, the main parts of their firmwares are normally stored in the hidden sector of the disk, and after initializing the head assembly according to the calibration data, Boot ROM reads the firmware data from the hidden sector and transfers the control right to the firmware's main body, and after the main body is initialized with itself, the bus interface driver module is loaded and executed. So far, the hard disk finishes the power-on starting procedure.

The internal structure of the mechanical hard disk as shown:

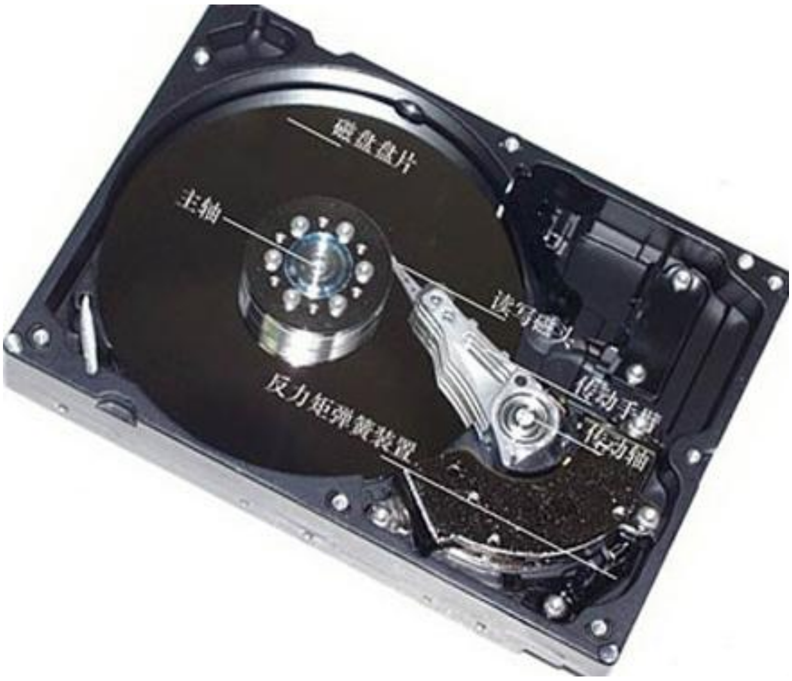


Figure 9 The composition and structure of the mechanical hard disk

（http://jingyan.baidu.com/article/ab0b5630d88efdc15bfa7d60.html）

With the hard disk's data stored on the disk platter, when the hard disk is under the working state, the principal axis drives the platter to rotate in high speed, and the read-write head suspends several microns on the top of the platter and conducted through the giant magnetoresistance effect. The transmission arm makes track seeking with the help of the voice coil motor composed of the strong magnet and the coil to locate the read-write content. In the figure, this countertorque spring device is used to provide the restoring force for the transmission arm, and can ensure that the head is put automatically to Park area in the case of the hard disk's power outage. In the Park area, there is a soft supporting device, which can read and write the arm to avoid the platter crash due to the outside shock when the hard disk is not working.

2) The solid state disk

Compared with the mechanical hard disk, as the solid state disk has no mechanical structure, its own structure is becoming much easier, normally descried as follows:

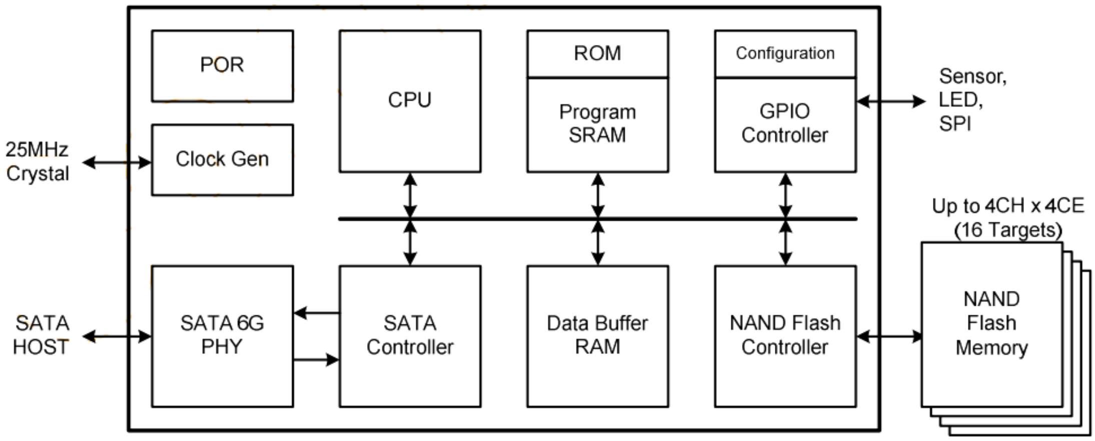


Figure 10 The structure diagram of the solid state disk and its controller

(《JMF608SATA III NAND Flash Controller datasheet》)

In the figure, the left frame refers to the controller of solid state disk, and the right refers to the onboard device and NAND FLASH array, and some controllers also need the external Data Buffer RAM, i.e. the cache. Seen from the figure, the controller itself can form a complete computer system, of which boot process is similar with the mechanical hard disk, so we don’t repeat it here.

3) The interface rules of the hard disk

As the current common IDE and SATA disks follow ATA instruction set, the PC machine makes the read-write operation by delivering ATA commands.

ATA technology is a technical specification family about IDE（Integrated Device Electronics）. Originally, IDE was just a hard disk interface technology which intended mainly to combine the controller with the disk body. As IDE/EIDE is more and more widely used, all technologies used by this interface are summarized as the global hard disk standards by the global standardized agreement, so this created ATA（Advanced Technology Attachment）. So far, ATA has been modified and upgraded for several times, and the interface of each edition is based on the previous one and maintains the backward compatibility. In addition to the read-write command, the hard disk also is available to some high level functions, such as the self-monitoring function（SMART）, capability setting（HPA）,and acoustic management（AAS）. See“ATA/ATAPI Command Set - 2 (ACS-2)”(An standard document with 500 pages).

7.2 The information security vulnerability of the hard disk

It is worth noting that most hard disks support the upgrade function of the firmware (through loading the microcode command or private command of the vendor). The user can update the firmware on the hard disk drive through the ATA command specified by the vendor. This allows that the vendor can upgrade the firmware and remediate the defect on the user system through the software tools, for example, in December 2008, when a failure existed on Seagate hard disk, the firmware update tool and instruction were released officially to allow users to refresh new firmware solutions. Another similar case is C1 event of Western Digital.

Taking the solid state disk of Seagate SandForce SF-2200 series as an example to illustrate the update process of the hard disk firmware:

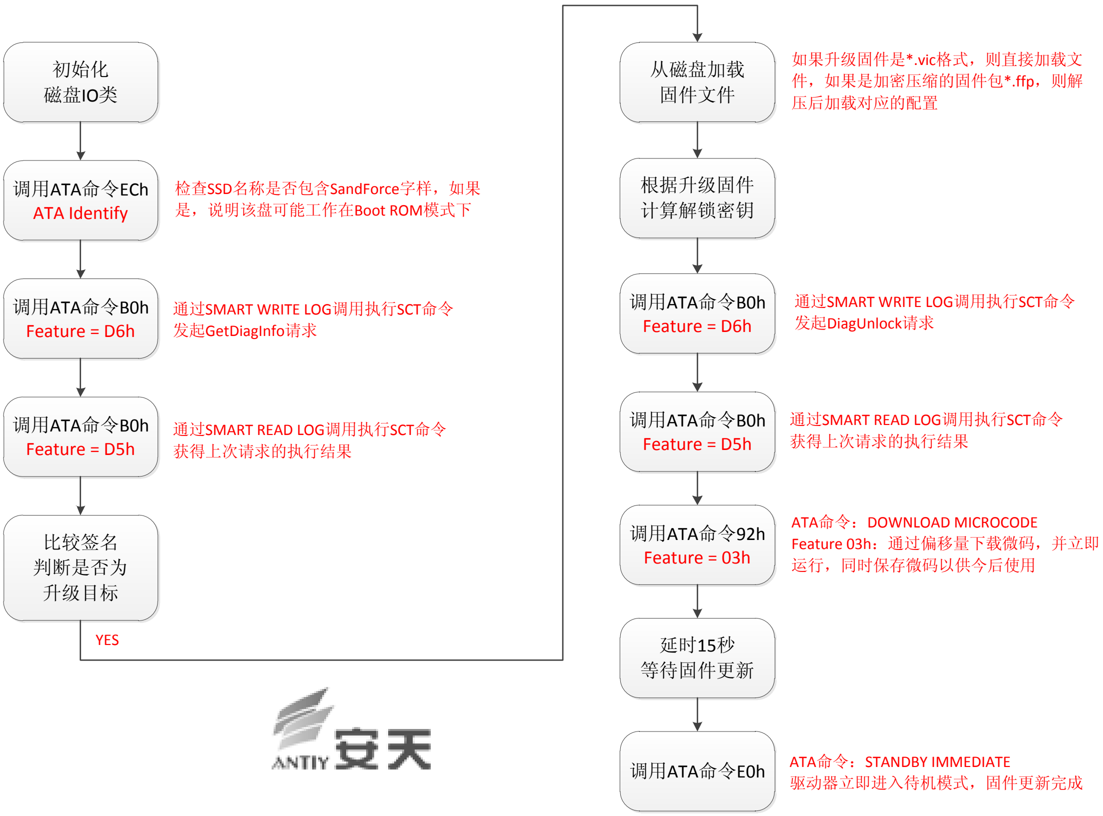

初始化
磁盘IO类
调用ATA命令ECh
ATA Identify
检查SSD名称是否包含SandForce字样，如果是，说明该盘可能工作在Boot ROM模式下
调用ATA命令B0h
Feature = D6h
通过SMART WRITE LOG调用执行SCT命令发起GetDiagInfo请求
调用ATA命令B0h
Feature = D5h
通过SMART READ LOG调用执行SCT命令获得上次请求的执行结果
比较签名
判断是否为
升级目标
YES
从磁盘加载
固件文件
如果升级固件是*.vic格式，则直接加载文件，如果是加密压缩的固件包*.ffp，则解压后加载对应的配置
根据升级固件
计算解锁密钥
调用ATA命令B0h
Feature = D6h
通过SMART WRITE LOG调用执行SCT命令发起DiagUnlock请求
调用ATA命令B0h
Feature = D5h
通过SMART READ LOG调用执行SCT命令获得上次请求的执行结果
调用ATA命令92h
Feature = 03h
ATA命令：DOWNLOAD MICROCODE
Feature 03h：通过偏移量下载微码，并立即运行，同时保存微码以供今后使用
延时15秒
等待固件更新
调用ATA命令E0h
ATA命令：STANDBY IMMEDIATE
驱动器立即进入待机模式，固件更新完成

Figure 11 The upgrade flow chart of solid state disk's firmware of Seagate SandForce SF-2200 series

This mechanism which upgrades the firmware in the system through host software is very convenient, which also means that the possibility that the firmware is changed maliciously exists. This malicious change can be operated through software without you knowing it.

As described in the previous section, the hard disk itself is a complete embedded system, which internal firmware runs independent of computer’s firmware. The firmware controls completely the read-write operation of the hard disk, and even processes the data independently without the permission of the host. If the attacker designs the smart codes in the hard disk’s firmware, it can intercept and disturb the read-write operation of the user, or obtain the highest control right of the system. All of these operations are completed on the hard disk, so the user and the soft and hardware can’t percept the process and even stop these operations.

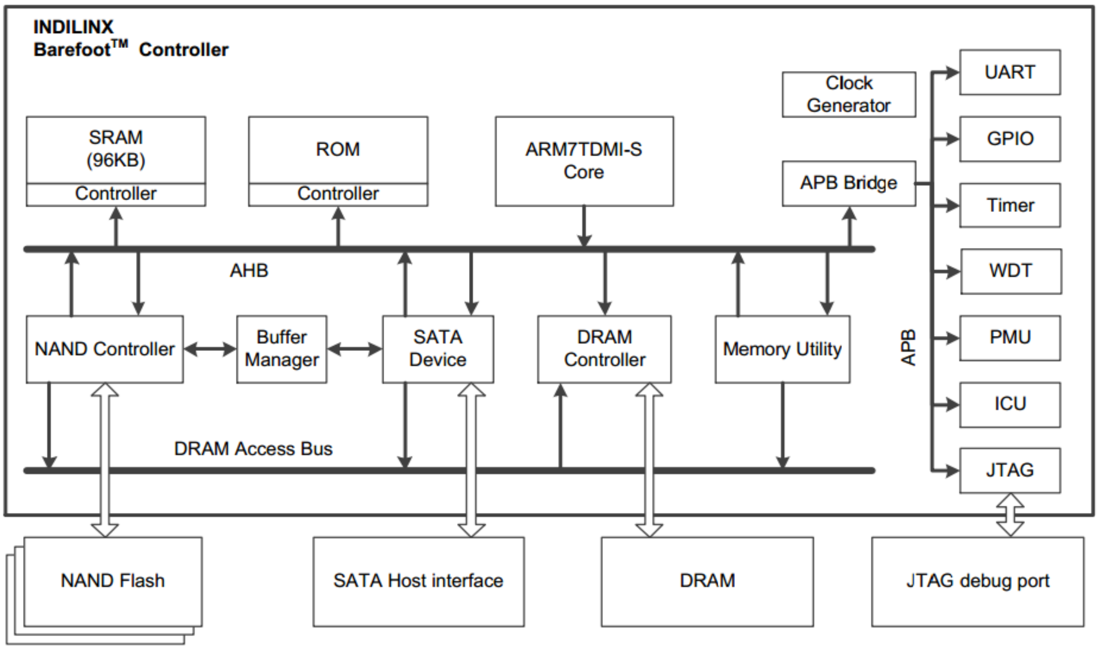


Figure 12 The structure diagram of Jasmine development board

（http://www.openssd-project.org）

Taking the Jasmine development board in the OpenSSD project as an example (An open-source hard disk project with a research purpose), if the attacker understands totally the structure of the hard disk’s controller, including the address space, this attacker can intercept some certain behaviors of the controller through the carefully constructed firmware, and modified the data in the DRAM during the process of the data transmission. For example, intercepting the ATA read-write command 20h, when reading the specified sector, the attacker tampers with the data in the DRAM to make the data discrepancy between the computer obtained and at the hard disk so that to remain its destruction after the system re-installment and the low level format.

8 Summary

The information about Equation Group appeared on February 16, two days before the Spring Festival. Time makes us think of Slammer worm appeared on December 23 Lunar New Year, 2003, Sasser worm on May 1, 2004, and the Shellshock before National Day 2014. These events impact our emergency speed, while Equation Group tests our comprehensive reserve and ability depth, and the analysis.

For Antiy team, this is the first time to get anxious when issuing an analysis report. In 2003, we were eager to issue the Dvldr analysis report to offer the solution for users quickly; issued the Stuxnet analysis report blindly when we though the effort was enough; and issued the Flame analysis report indulgently in a relay way. But this time, we are blocked due to the disk firmware but not encryption, driving and hidden problems. In the term of the attacker with a long-term preparation, the key of understanding the situation for the defender is rely on the manpower and time.

We have paid attention to the embedded firmware very early, but when the threat really appeared, we found the rival was more sophisticated and stronger.

We also get extremely worried that the reports of related events are deviating from the core theme. Many users have asked us “whether all disks have been put into Trojan horse.

So although we continue to make the analysis work, the following conclusions or judgments should be given:

1. With the hardware and software system development, it is an inevitable trend that the updatable mechanism is achieved for the hardware device’s firmware, and this mechanism itself can’t be called as the backdoor.
2. According to the current analysis results from Antiy, partners and organizations, in the related attacks the writing firmware operation occurs when the leading malicious code sends the host information back and when it is judged the valuable object——that is a high conditional intrusion behavior.
3. Through the long-term analysis and research, the attacker can achieve independently the related mechanism without intruding the vendor to obtain the technology paper.
4. The writing firmware operation is used to implement the latency and persistence, but the upper operation ability still exists on the host system, obtaining the other operation modules through the network.

5. In the view of the previous behaviors of the related countries, there are reasons to doubt that the same component may be used to the logistics chain hijack, i.e. injecting it during the processes of specified objects determination and the host or disk repair. But based on its operations and risk analysis, we believe that the batch operations will not be conducted, according to the operation method of Bootkit+firmware.
6. As the Bruce Schneier warned that “more and more tactical behaviors are used widely in the cyberspace”, and upon the exposure of new methods, the enlightenment effect will be created for hackers so that to encourage the threats.
7. The related attacks really embody some security blind sports, for example, whether the signature verification mechanism is adopted by the disk’s firmware and written to the firmware at the same time. At present, we have no found the low-cost and unconditional interface for reading. Similar deigns make some difficulties for security analysts to implement detection and verification actions.

The plan for defensive positions must not depend on imagining the rival. To view the security and development relation in the objective way, to conduct the depth and specific analysis for threats and to study and judge the strategies and paths of rivals, always are our critical points responding to threats.

Appendix I Reference

[1] Equation: The Death Star of Malware Galaxy
http://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/

[2] A Fanny Equation: "I am your father, Stuxnet"
http://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/

[3] Equation Group: from Houston with love
http://securelist.com/blog/research/68877/equation-group-from-houston-with-love/

Appendix II Event log

Updated date	Updated content
2015-02-18	The start of study and judgment and verification for events
2015-02-21	The establishment of the joint analysis group by Antiy CERT and Microelectronic and

	Embedded Security Development Center
2015-02-25	The start of comprehensive analysis
2015-03-02	The compilation of preliminary analysis report
2015-03-04	The first edition of analysis report
2015-03-05	The content corrected by Antiy CERT and updated to V1.3

Appendix III About Antiy Labs

Antiy Labs is a professional next-generation security-testing engine R&D enterprise. Antiy’s engines provide the ability to detect various viruses and malware for network security products and mobile devices. They are used by more than ten well known security vendors. Antiy’s engines are embedded in tens of thousands of firewalls and tens of millions of mobile phones all over the world. Antiy Labs is awarded the “Best Protection” prize by AV-TEST in 2013. Based on engines, sandboxes and background systems, Antiy Labs will continue to provide traffic-based anti-APT solutions for enterprises.

More information about anti-virus engines:	http://www.antiy.com（Chinese）
	http://www.antiy.net（English）
More about Antiy anti-APT products:	http://www.antiy.cn