18dd.net 网站挂马分析（下篇）

拿出 PEiD，看这个可执行文件的加壳情况，得出的结论是它是用 Delphi 写的。这个结论可信么？高手可能会使用修改 OEP 特征的方法来“A”一下我们的 PEiD，使其判断失效。

先不管这个，打开专门为破解 Delphi 程序而准备的利器：DeDe。分析成功，但却没有得到什么有用的信息。不过它至少证明它真的是用 Delphi 编写的。但这里我们关注的焦点不是用什么语言和工具写的，而是看它有没有被加壳。

用 W32DAsm 反汇编这个 exe 文件，然后下意识地看一下“串式参考”：

```
" goto try"
"#32770"
"(T@"
",T@"
"  .1  "
":\AutoRun.inf"
":try"
"[AutoRun]
open="
"\program files\internet explorer\IEXPLORE.EXE"
"0813"
"3 烂忽 VQ 嬝婧哳 u 3 离&j"
"60000"
"advapi32.dll"
"Alletdel.bat"
"AutoRun.inf"
"Button"
"ChangeServiceConfig2A"
"ChangeServiceConfig2W"
"cmd /c date "
"cmd /c date 1981-01-12"
"del ""
"del %0"
"drivers/klif.sys"
"Error"
"FPUMaskValue"
"http://down.18dd.net/kl/0.exe"
"http://down.18dd.net/kl/1.exe"
"http://down.18dd.net/kl/10.exe"
"http://down.18dd.net/kl/11.exe"
"http://down.18dd.net/kl/12.exe"
"http://down.18dd.net/kl/13.exe"
"http://down.18dd.net/kl/14.exe"
"http://down.18dd.net/kl/15.exe"
"http://down.18dd.net/kl/16.exe"
"http://down.18dd.net/kl/17.exe"
```

"http://down.18dd.net/kl/18.exe"
"http://down.18dd.net/kl/19.exe"
"http://down.18dd.net/kl/2.exe"
"http://down.18dd.net/kl/3.exe"
"http://down.18dd.net/kl/4.exe"
"http://down.18dd.net/kl/5.exe"
"http://down.18dd.net/kl/6.exe"
"http://down.18dd.net/kl/7.exe"
"http://down.18dd.net/kl/8.exe"
"http://down.18dd.net/kl/9.exe"
"IE 执行保护"
"IEXPLORE.EXE"
"IE 执行保护"
"if exist ""
"Kernel32.dll"
"NoDriveTypeAutoRun"
"ntdll.dll"
"QueryServiceConfig2A"
"QueryServiceConfig2W"
" S@"
"serdst.exe"
"shell\Auto\command="
"shellexecute="
"SOFTWARE\Borland\Delphi\RTL"
"Software\Microsoft\Windows\CurrentVersion\Poli"
"Telephotsgoogle"
"U 婁頔鎊 VW3 繳 h 詶@"
"U 婁筧"
"U 婁仳　　SVW?　"
"ZwUnmapViewOfSection"
"刋@"
"銼@"
"婦$ 鰼　"
"媩$(? "
"燬@"
"攕@"
"确定"
"嫕$?搡?婄 婥 t ?熋"
"瑞星卡卡上网安全助手 - IE 防漏墙"
"为即插即用设备提供支持"
"坏@"
"允许"
"允许执行"

从上面我们可以做如下推断：

1.这个程序可能生成一个叫"Alletdel.bat"的批处理文件,这个文件中有一个标签叫"try",批处理文件会不断的执行这个标签下一行的命令,命令内容可能是判断文件存在性,更改系统日期,删除某些文件(证据:" goto try", ":try", "Alletdel.bat", "cmd /c date ", "cmd /c date 1981-01-12", "del "", "del %0", "if exist "")

2.这个程序可能在磁盘根目录下生成自动运行的文件,以求用户不小心时启动程序(证据:":\AutoRun.inf", "[AutoRun] open=", "AutoRun.inf", "shell\Auto\command=")

3.这个程序要对 IE、注册表、服务和系统文件动点手脚(证据:"advapi32.dll", "drivers/klif.sys", "\program files\internet explorer\IEXPLORE.EXE", "IE 执行保护", "IEXPLORE.EXE", "Software\Microsoft\Windows\CurrentVersion\Poli"), "Kernel32.dll", "SOFTWARE\Borland\Delphi\RTL", "ChangeServiceConfig2A", "ChangeServiceConfig2W", "QueryServiceConfig2A", "QueryServiceConfig2W")

4.这个程序有一定的防系统保护软件的能力(证据:"瑞星卡卡上网安全助手 - IE 防漏墙", "允许", "允许执行")

5.这个程序要下载一堆木马(证据:一堆形如"http://down.18dd.net/kl/**.exe"的字符串,共 20 个)

为了进一步分析,我们使用动态运行的方法来看这个木马到底干了些什么。不过在运行之前,我们先把那 20 个可执行文件一个个做 Hash 下载。

```
MD5(http://down.18dd.net/kl/0.exe,32) = f699dcff6930465939a8d60619372696
MD5(http://down.18dd.net/kl/1.exe,32) = 0c5abac0f26a574bafad01ebfa08cbfa
MD5(http://down.18dd.net/kl/2.exe,32) = 7ab83edbc8d2f2cdb879d2d9997dd381
MD5(http://down.18dd.net/kl/3.exe,32) = 6164f8cd47258cf5f98136b9e4164ec0
MD5(http://down.18dd.net/kl/4.exe,32) = c8620b1ee75fd54fbc98b25bd13d12c1
MD5(http://down.18dd.net/kl/5.exe,32) = a23cbbf6c2625dcc89ec5dc28b765133
MD5(http://down.18dd.net/kl/6.exe,32) = 7d023fd43d27d9dc9155e7e8a93b7861
MD5(http://down.18dd.net/kl/7.exe,32) = d6fe161bbf5e81aaf35861c938cb8bd1
MD5(http://down.18dd.net/kl/8.exe,32) = acc2bad4a01908c64d3640a96d34f16b
MD5(http://down.18dd.net/kl/9.exe,32) = 1f627136e4c23f76fa1bb66c76098e29
MD5(http://down.18dd.net/kl/10.exe,32) = c6c24984d53478b51fe3ee2616434d6f
MD5(http://down.18dd.net/kl/11.exe,32) = 248b26c81f565df38ec2b0444bbd3eea
MD5(http://down.18dd.net/kl/12.exe,32) = d59f870b2af3eebf264edd09352645e0
MD5(http://down.18dd.net/kl/13.exe,32) = 2506d70065b0accd2c94a0833846e7d8
MD5(http://down.18dd.net/kl/14.exe,32) = f9a339dc1a9e3e8449d47ab914f89804
MD5(http://down.18dd.net/kl/15.exe,32) = 18f9de3590a7d602863b406c181a7762
MD5(http://down.18dd.net/kl/16.exe,32) = 7d63bd5108983d6c67ed32865fefc27b
MD5(http://down.18dd.net/kl/17.exe,32) = 6536161fd92244f62eaac334c36db897
MD5(http://down.18dd.net/kl/18.exe,32) = 6c8d161464e5be8983f7fa42d5e09177
MD5(http://down.18dd.net/kl/19.exe,32) = 4b8597eeb55c107181bd5eb3aa8bfe3e
```

为保证系统安全,我们先装上“影子系统”。然后我们找点小工具吧:

1.Process Monitor(微软旗下 SysInternals 公司出品),之前我用的是同一公司出品的两款软件即 File Monitor 和 Registry Monitor,而 ProcMon 集 FileMon 和 RegMon 的功能于一体并更加强大,试用后感觉不错,于是不再使用 FileMon 和 RegMon(感谢宋程昱同学的推荐)。

2.SysInspector(ESET 公司出品),可对系统进行扫描并生成日志,更可进行日志比较以反映系统变化。优点:界面华丽且易上手,功能比较强大。缺点:扫描系统时间太长,个别位置仍没有关注到。

3.Total Uninstall（Gavrila Martau 出品），功能非常强大的安装监视工具，在安装程序前扫描一遍系统，安装结束后再扫描一遍，比较两次扫描结果得出系统变化情况，报告内容包括文件系统、注册表和服务，较为全面。

我们先启动影子系统，然后用 Total Uninstall 记录安装过程中注册表的变化。发现了两处。

一是在系统文件夹(system32)下创建了一个 serdst.exe 的文件。经 MD5 检查，该文件就是这个可执行文件。

二是安装了一个服务。服务名为“Wdswsdewn”，显示名为“Telephotsgoogle“，描述为“为即插即用设备提供支持”,还是比较有迷惑性的。这个服务启动的就是上面那个 serdst.exe 文件。

当然，由于各种条件限制（比如那 20 个 exe 文件就已经不存在了，而且病毒有些行为可能是有条件才触发的），这里没有观察到其它的改变。

再用 Process Monitor 对原 exe 和 serdst.exe 进行行为监视，捕获到了 1400 多条信息，太多了，就没再进一步分析，主要就是程序在运行过程中生成了几个批处理文件，当然更重要的是生成了病毒文件。而 SysInspector 的分析结果显示没有不正常的进程注入现象。

再回头看那些新下载的可执行文件。先用 MD5 看有没有重复的文件，没有。再用 PEiD 看是否有壳，除了 1.exe 是“Nothing found”外，其它的都用“Upack 0.3.9 beta2s -> Dwing”加密过。硬着头皮用“超级巡警之虚拟机自动脱壳机”一个个脱壳。脱完一遍，再用 PEiD 看，显示还有壳“Morphine 1.2 - 1.3 -> rootkit”。网上说这是一个伪装壳。不管它，再用 W32DAsm 打开看。这些文件都能正常显示出“串式参考”的内容。从这些字符串的内容来看，这些文件不

类似地，我们先用 W32Dasm 查找程序中的字符串，再拿 Total Uninstall 监视病毒文件给系统带来的改变，用 Process Monitor 对病毒对文件系统和注册表的每一步操作做记录。同时辅助以 SysInspector 以便查看有没有 DLL 被附加到进程。

下面以 4.exe 文件为例作个说明：

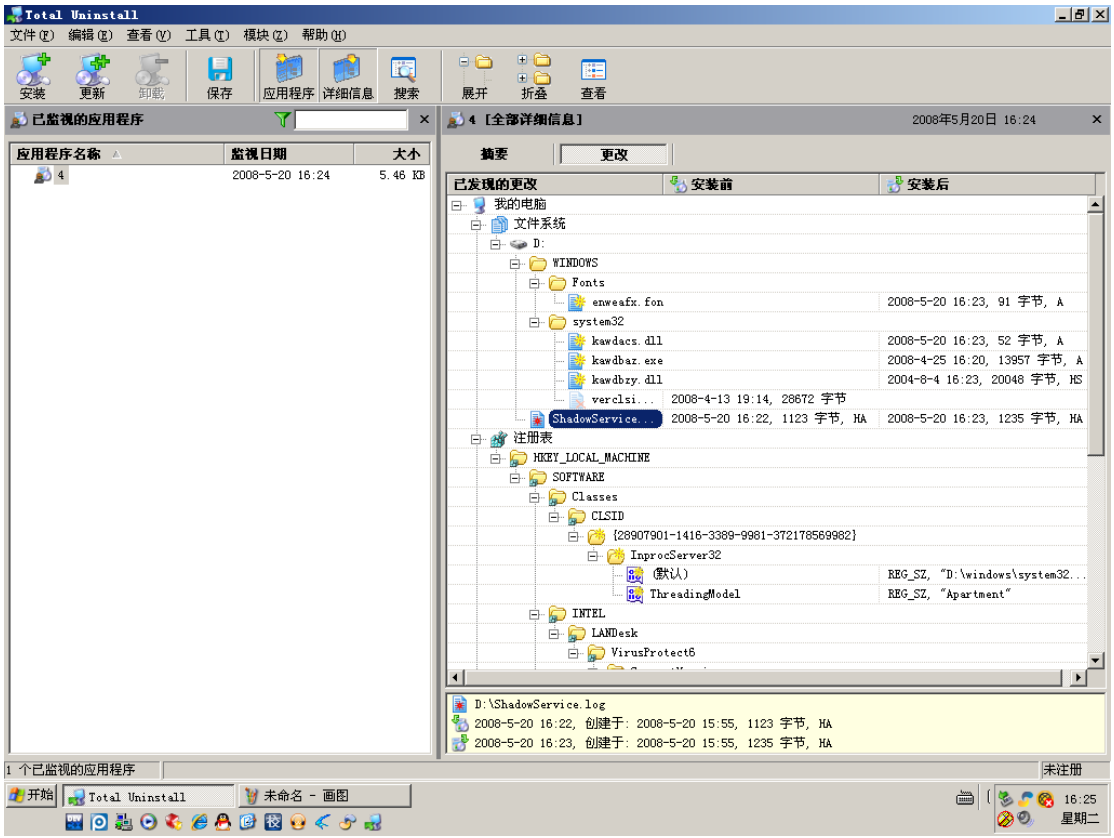
1.用 W32Dasm 对脱壳后的 4.exe 文件其中的字符串作分析

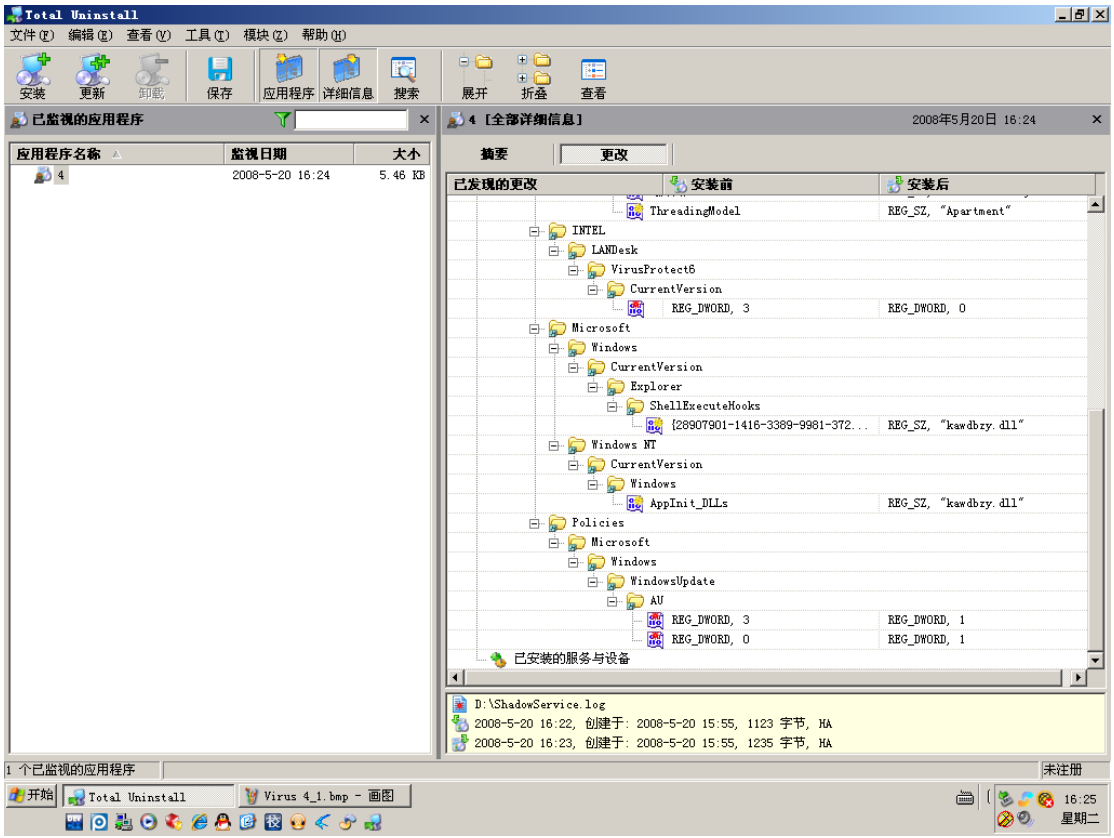
```
" "
"" goto Loop
del %0
"
"" -r -a -s -h
del ""
""
if exist ""
"%d"
".bat"
".mod"
":Loop
"
"@echo off
"
"\"
"\InprocServer32"
" ^B*"
"{28907901-1416-3389"
"1"
"-9981-372178569982}"
```

"a"
"Apartment"
"asktao"
"attrib ""
"C:\DFD"
"CLSID\"
"EnHookWindow"
"enweafx.fon"
"Fonts\"
"id.exe"
"kawdacs.dll"
"kawdazy.d"
"kawdbaz.exe"
"kawdbzy.dll"
"ll"
"MP3"
"Music"
"q@ "
"Send"
"Software\Microsoft\Windows\CurrentVersion\expl"
"S 鏍? 呷 t 嬝 覽?
"ThreadingModel"
"Url%d"
"Url1"
"U 婁 S 瑙? 嬝杓 铖? +?? "
"vercls"
"wddpri.d"
"獲 "
"嬂 % Q@"

从上面不能推出很多信息,主要可以看到这个病毒可能要生成一个批处理文件并进行删除文件操作，因为"goto Loop del %0"，" -r -a -s -h del "，"if exist ""， ":Loop"，"@echo off"，"attrib ""这些内容都是批处理文件中的字符串。同时其中还有 ClassID 标识和注册表键值和一些文件名。

2.用 Total Uninstall 对该病毒的执行情况进行监视





主要内容如下：

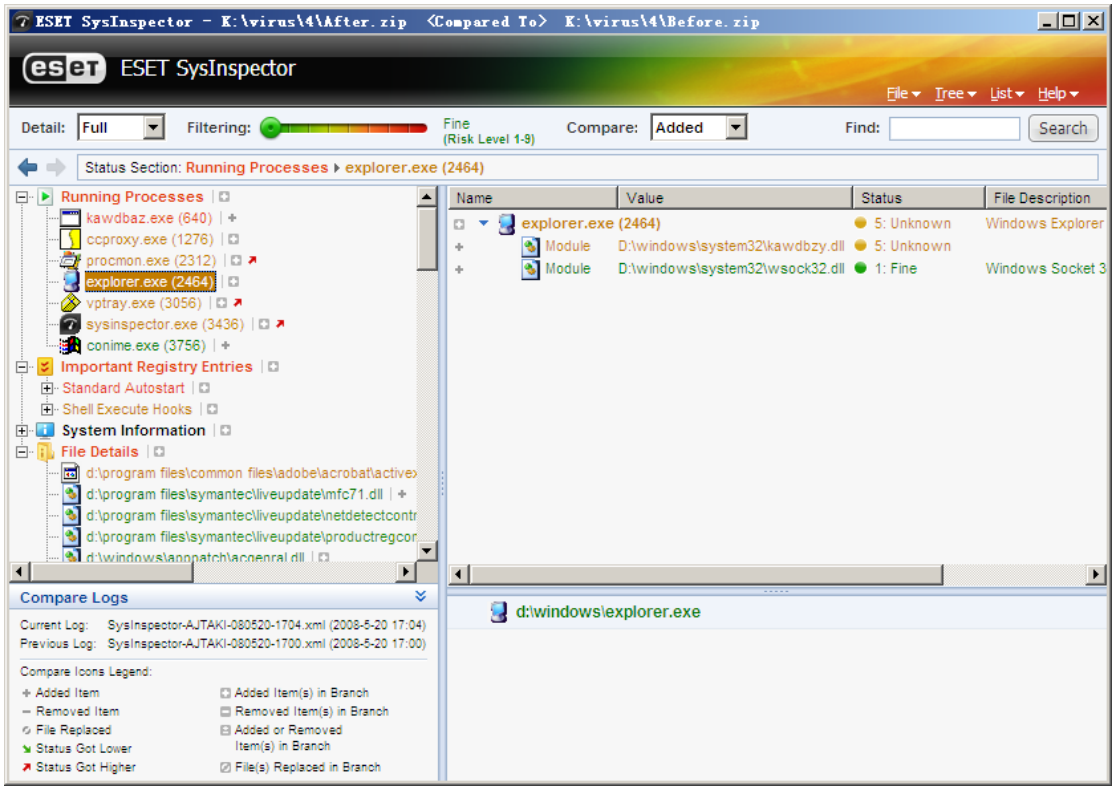
生成了一些文件，包括 enweafx.fon（91Bytes），kawdacs.dll（52Bytes），kawdbaz.exe（13957Bytes），kawdbzy.dll（20048Bytes），同时删除了 verclsid.exe（截图没处理好，文件

名没显示全)。

更改了一些注册表项目，主要是设置了一个钩子，加载了一个启动 DLL，另外把 Windows 的自动更新功能给禁用了。

3.用 SysInspector 对病毒运行前后的变化做比较

SysInspector 可以看出 DLL 注入一个进程的情况，这是它的一个特色功能，其它方面的功能 Total Uninstall 都能看出来。



上图中显示出了 explorer.exe 程序中被注入了动态链接库 kawdbzy.dll。而实际上，除了病毒的主程序文件 kawdbaz.exe 的进程外，Process Monitor、Norton 系统托盘和 SysInspector 自己的进程中都被注入了该 DLL。

在 Total Uninstall 给出的被创建的文件中，有个反常的现象，即生成的一个字体文件和一个 DLL 文件的大小才几十字节。这显然不是真正的字体和 DLL，用记事本打开，看到他们的内容是：

enweafx.fon

```
[Send]
Url1=EC1A060602485D5D0505055C02064B47420B005C111C5D1907084A0A185D021D01065C130102
```

kawdacs.dll

```
[Send]
Url1=http://www.pt950yr.cn/kuz8xj/post.asp
```

这两个文件显然是类似于 INI 格式的文件，即配置文件。其作用是指定 URL，其中 enweafx.fon 中给出的是密文形式，而 kawdacs.dll 给出的是明文形式。因密文只包括了数字和 A 到 E 的字母（F 没有出现），因此初步确定为 16 进制加密。而密文长度为 76，明文长度为 37。密文长度比明文的长度多 2，所以其中应有冗余的部分，考虑到一般的古典加密中，相同明文对应相同的密文。看到明文中有 www，所以就在密文中找三个连续出现的十六进制代码，把目标锁定在 050505 上面。于是得出密文开始的 EC 不是明文加密后的一部分。

于是我们列出明文的 ASCII 码与密文的对应关系，如下：

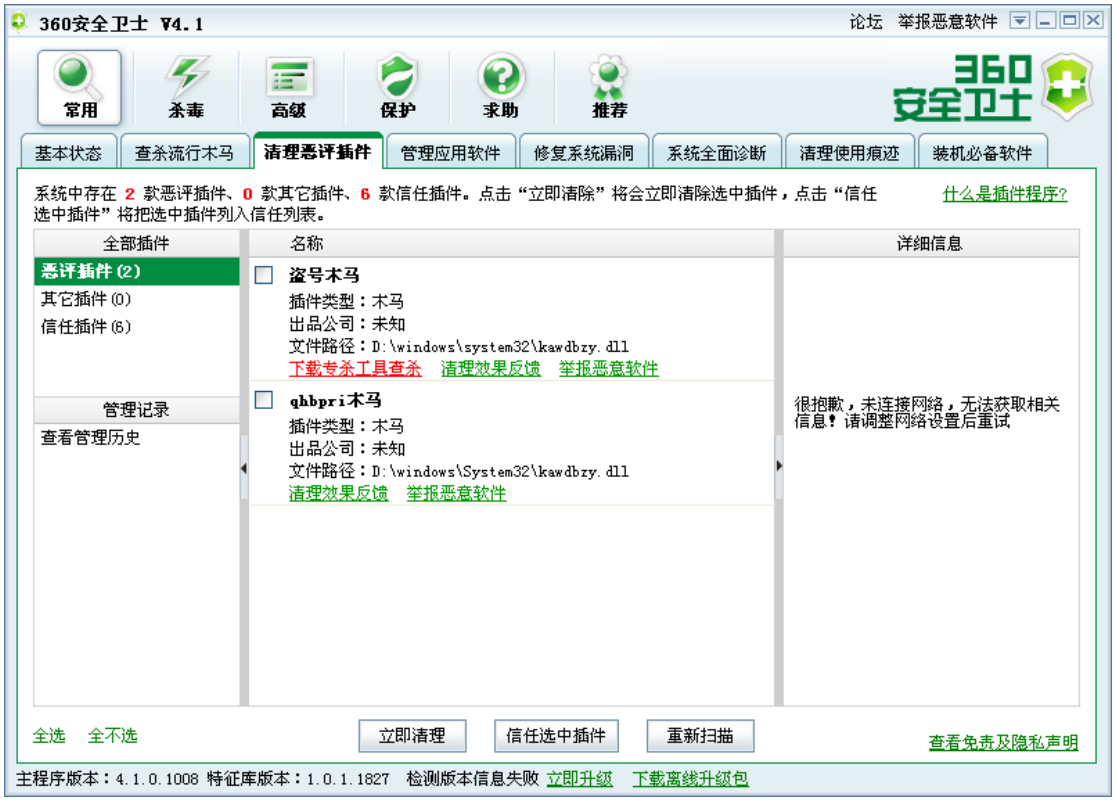
1A060602485D5D0505055C02064B47420B005C111C5D1907084A0A185D021D01065C130102（密文）
h t t p : / / w w w . p t 9 5 0 y r . c n / k u z 8 x j / p o s t . a s p （明文）

再把明文字符换成对应的 ASCII 码：

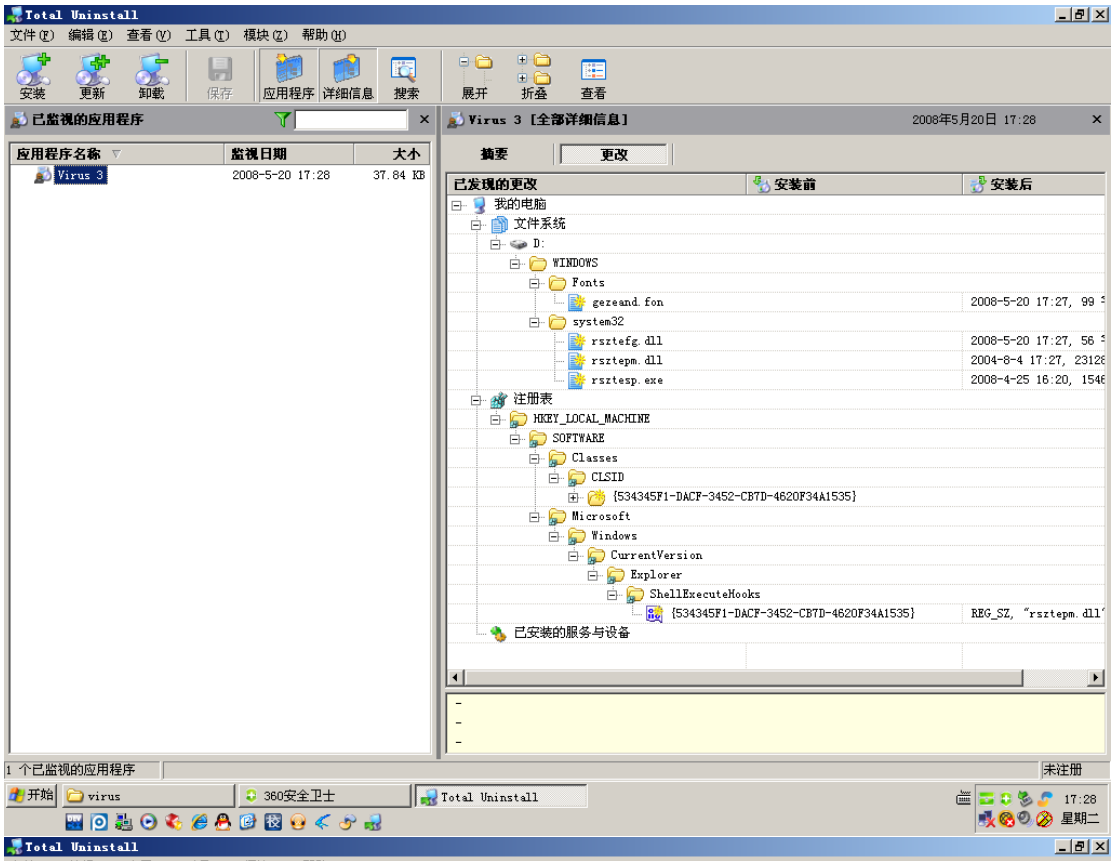
1A 06 06 02 48 5D 5D 05 05 05 5C 02 06 4B 47 42 0B 00 5C 11 1C 5D 19 07 08 4A 0A 18 5D 02 1D 01 06 5C 13 01 02（密文）
68 74 74 70 3a 2f 2f 77 77 77 2e 70 74 39 35 30 79 72 2e 63 6e 2f 6b 75 7a 38 78 6a 2f 70 6f 73 74 2e 61 73 70（明文字符的 ASCII 码）

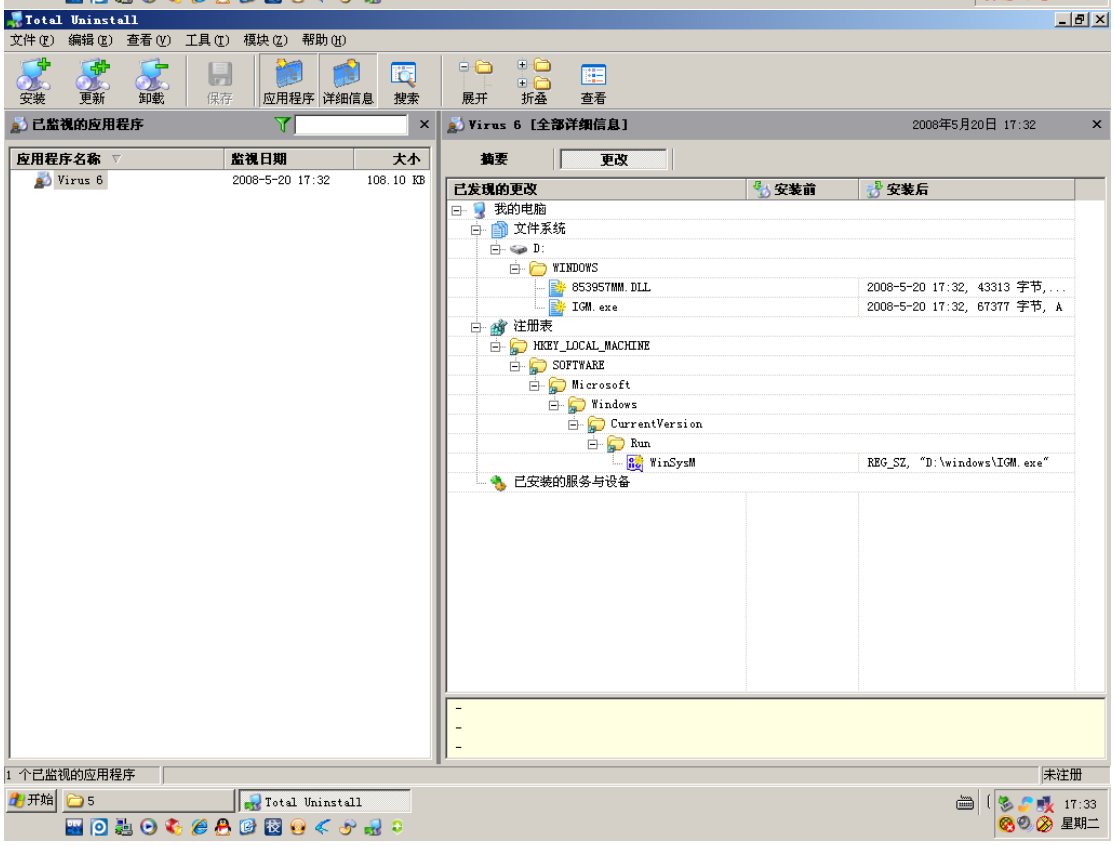
于是我们发现，即对于每一组明文和密文（如 1A 和 68,06 和 74 等），存在这样的规律，即首位的和总是 7（如 1+6=7，0+7=7，其它的也一样），而末位的差总是 2（如 A-8=2，6-4=2，其它也一样，注意要让大的减小的）。于是我们得出结论：即密文和明文之间是按位异或关系，为寻找异或操作使用的密钥，我们取出一组明文和密文并分别转化成二进制：比如我们取 1A 和 68，其二进制形式分别为 00011010 和 01101000，从而解出 Key=01110010=72。不过没觉得这个 72 和那个冗余的 EC 有什么关系。

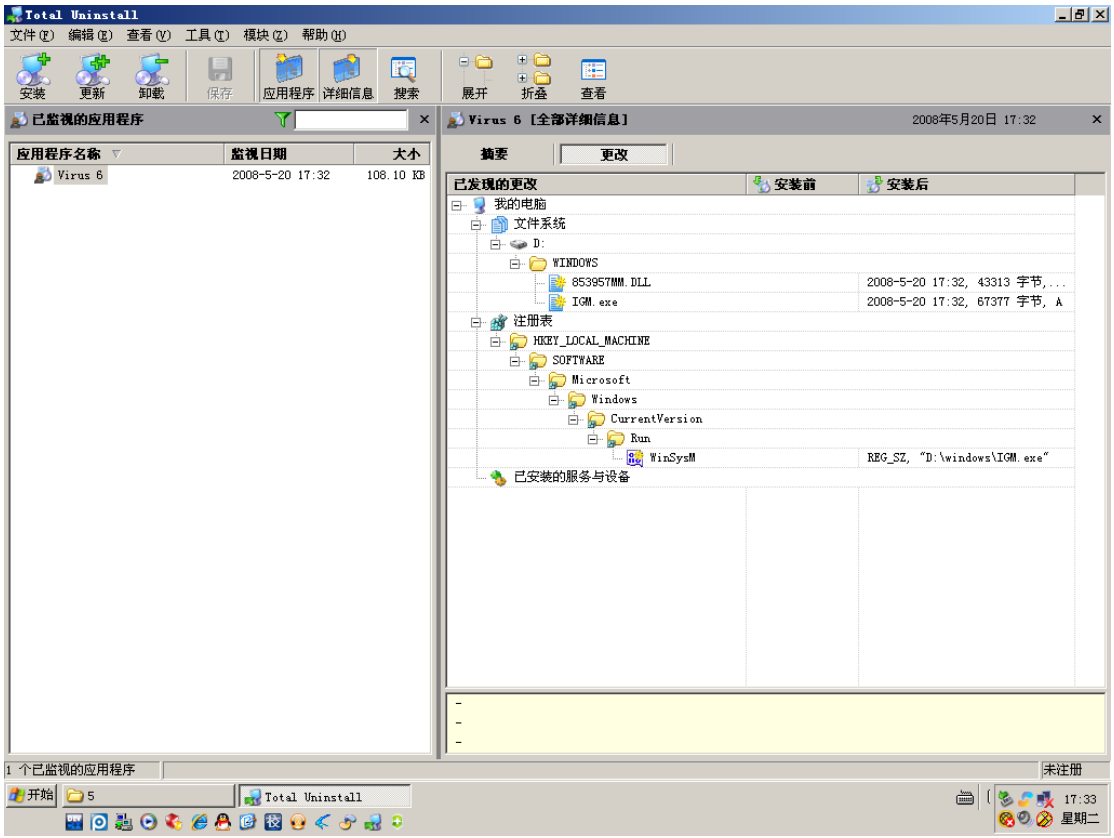
既然这个 URL 是一个动态页面，因此怀疑程序会向该页面提交信息，那这个病毒很可能就是一个盗号木马。而 360 安全卫士的检测也证明了这一点：



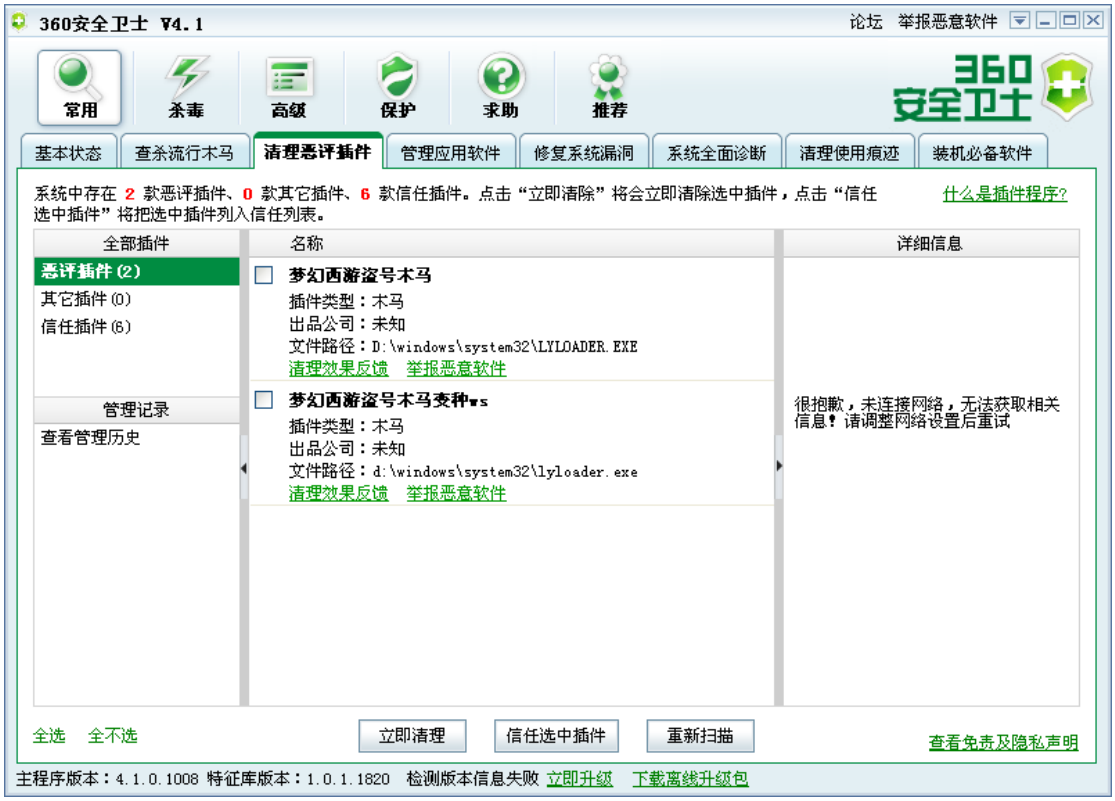
对于其它程序，使用同样的方法进行分析就可。这里只用了 Total Uninstall 监控了部分病毒程序的运行结果，它们都大同小异。


Total Uninstall
文件(F) 编辑(E) 查看(V) 工具(T) 模块(Z) 帮助(H)
安装 更新 卸载 保存 应用程序 详细信息 搜索 展开 折叠 查看
已监视的应用程序
应用程序名称 监视日期 大小
Virus 3 2008-5-20 17:28 37.84 KB
Virus 3 [全部详细信息] 2008年5月20日 17:28
摘要 更改
已发现的更改 安装前 安装后
我的电脑
文件系统
D:
WINDOWS
Fonts
gezeand.fon 2008-5-20 17:27, 99
system32
rsztefg.dll 2008-5-20 17:27, 56
rsztepm.dll 2004-8-4 17:27, 2312
rsztesp.exe 2008-4-25 16:20, 154
注册表
HKEY_LOCAL_MACHINE
SOFTWARE
Classes
CLSID
{534345F1-DACF-3452-CB7D-4620F34A1535}
Microsoft
Windows
CurrentVersion
Explorer
ShellExecuteHooks
{534345F1-DACF-3452-CB7D-4620F34A1535} REG_SZ, "rsztepm.dll"
已安装的服务与设备
1 个已监视的应用程序
未注册
开始 virus 360安全卫士 Total Uninstall 17:28 星期二

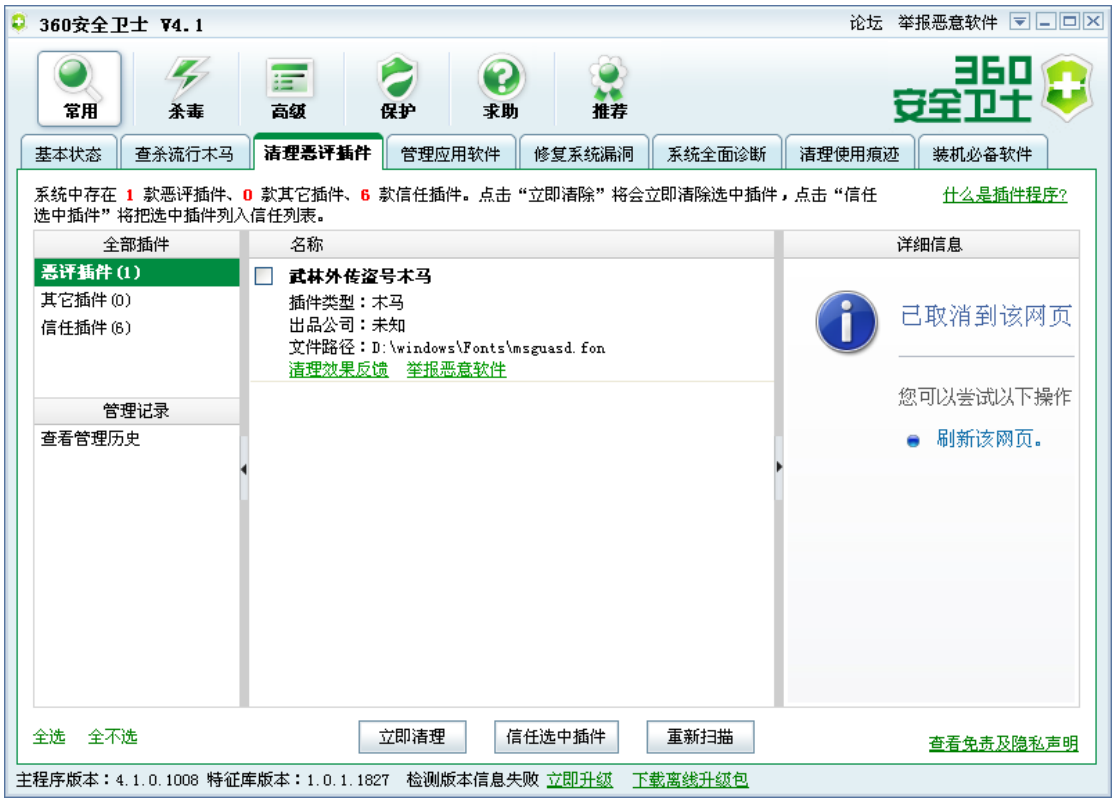

Total Uninstall
文件(F) 编辑(E) 查看(V) 工具(T) 模块(Z) 帮助(H)
安装 更新 卸载 保存 应用程序 详细信息 搜索 展开 折叠 查看
已监视的应用程序
应用程序名称 监视日期 大小
Virus 6 2008-5-20 17:32 108.10 KB
Virus 6 [全部详细信息] 2008年5月20日 17:32
摘要 更改
已发现的更改 安装前 安装后
我的电脑
文件系统
D:
WINDOWS
853957MM.DLL 2008-5-20 17:32, 43313 字节,...
IGM.exe 2008-5-20 17:32, 67377 字节, A
注册表
HKEY_LOCAL_MACHINE
SOFTWARE
Microsoft
Windows
CurrentVersion
Run
WinSysM REG_SZ, "D:\windows\IGM.exe"
已安装的服务与设备
1 个已监视的应用程序
未注册
开始 5 Total Uninstall 17:33 星期二



它们的共同点是向系统目录和字体目录下添加一些文件，包括真正的病毒部分（EXE 和 DLL），还有虚构的字体文件和 DLL，里面以明文或密文的形式来保存着 URL 以便提交。同时这些程序还会使用 DLL 注入，设置钩子等方法确保自身被执行。有的还会关闭自动更新，隐藏文件显示。这些分析未必可靠，但我们有 360 安全卫士的确认：




360安全卫士 V4.1
论坛 举报恶意软件
常用
杀毒
高级
保护
求助
推荐
360安全卫士
基本状态
查杀流行木马
清理恶评插件
管理应用软件
修复系统漏洞
系统全面诊断
清理使用痕迹
装机必备软件
系统中存在 2 款恶评插件、0 款其它插件、8 款信任插件。点击“立即清除”将会立即清除选中插件，点击“信任选中插件”将把选中插件列入信任列表。
什么是插件程序?
全部插件
恶评插件 (2)
其它插件 (0)
信任插件 (8)
管理记录
查看管理历史
名称
详细信息
诛仙盗号木马
插件类型：木马
出品公司：未知
文件路径：D:\windows\Fonts\mszhasd.fon
清理效果反馈 举报恶意软件
kafy盗号木马
插件类型：木马
出品公司：未知
文件路径：D:\windows\system32\avrxemn.dll
清理效果反馈 举报恶意软件
很抱歉，未连接网络，无法获取相关信息！请调整网络设置后重试
全选 全不选
立即清理
信任选中插件
重新扫描
查看免责及隐私声明
主程序版本：4.1.0.1008 特征库版本：1.0.1.1827 检测版本信息失败 立即升级 下载离线升级包


360安全卫士 V4.1
论坛 举报恶意软件
常用
杀毒
高级
保护
求助
推荐
360安全卫士
基本状态
查杀流行木马
清理恶评插件
管理应用软件
修复系统漏洞
系统全面诊断
清理使用痕迹
装机必备软件
系统中存在 1 款恶评插件、0 款其它插件、6 款信任插件。点击“立即清除”将会立即清除选中插件，点击“信任选中插件”将把选中插件列入信任列表。
什么是插件程序?
全部插件
恶评插件 (1)
其它插件 (0)
信任插件 (6)
管理记录
查看管理历史
名称
详细信息
武林外传盗号木马
插件类型：木马
出品公司：未知
文件路径：D:\windows\Fonts\msguasd.fon
清理效果反馈 举报恶意软件
已取消到该网页
您可以尝试以下操作
刷新该网页。
全选 全不选
立即清理
信任选中插件
重新扫描
查看免责及隐私声明
主程序版本：4.1.0.1008 特征库版本：1.0.1.1827 检测版本信息失败 立即升级 下载离线升级包