



# 北京大学网络攻防技术与实践课程

---

## 作业8讲解：网站挂马案例分析

诸葛建伟

zhugejianwei@icst.pku.edu.cn

北京大学计算机研究所信安中心



# 作业8：网站挂马案例分析

---

## □ 案例分析作业内容：

- 案例背景：狩猎女神项目组于**2007年10月**进行的中国万维网挂马现象采样分析过程中，发现了一个庞大的木马网络，宿主站点为**18dd.net**，大量被挂马网站最终都将访问流量重定向到了这个宿主上的网页木马。
- 你的任务就是分析这个案例，揭露出这个木马网络。

## □ 案例分析挑战网址(目前由于单位网络调整尚无法访问，**fix**后将尽快在**BBS**上发布)

- <http://222.29.87.30/scom/>

## □ 作业9分数：20+3

## □ 作业9 Deadline: 12月30日下午17:00



# 作业8说明

---

- 挂马网站和宿主站点已无法访问，但我们在  
<http://222.29.87.30/scom/>网址保存了原始的挂马页面、网马和植入木马可执行文件
- 每解密出一个原始的**URL**
  - 例如<http://xx.18dd.net/a/b.htm>的形式
  - 对原始**URL**做**MD5**，获得**hash**值
  - 使用**hash**值构建原始文件下载地址：  
[http://222.29.87.30/scom/hashed/\[hash\\_value\]](http://222.29.87.30/scom/hashed/[hash_value])
  - 下载网页可能会被加密，需要进行解密后从中提取网马和/或植入木马的原始**URL**
  - 最终的下载器和植入木马为可执行文件(**wild malware**，注意！)，可选择性的进行分析



# 作业8-问题

---

## □ 基本问题

- 1.试述你是如何一步步地从所给的网页中获取最后的网页木马和植入木马？
- 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，攻击者的网页木马利用了那些系统和应用程序漏洞？

## □ Bonus问题

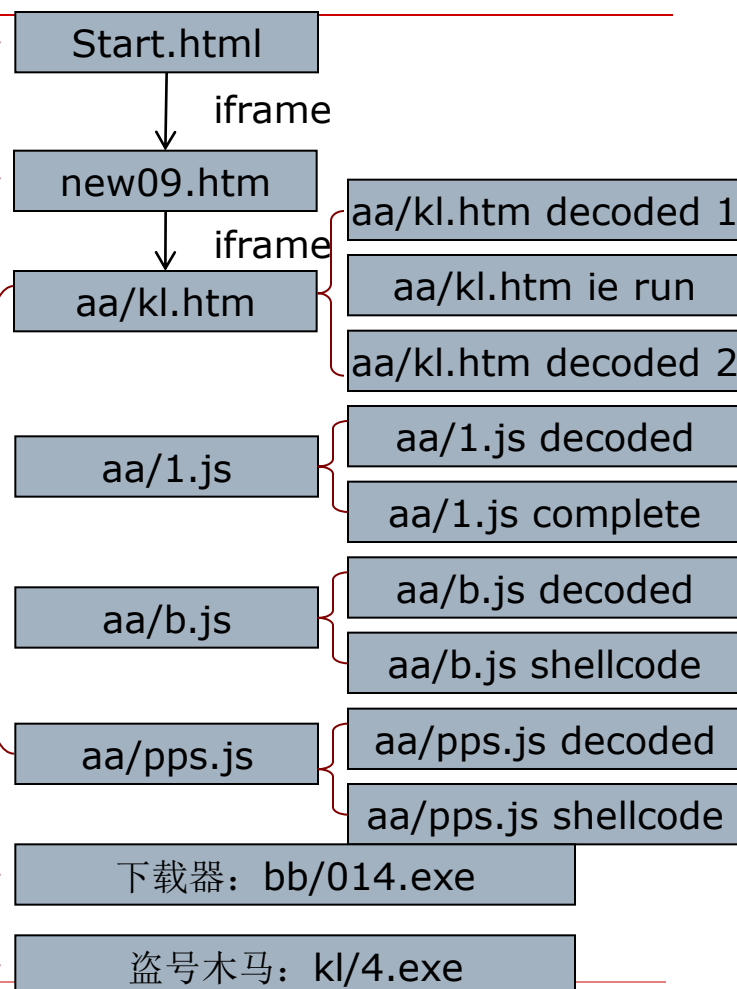
- 4.解密后发现了多少个可执行文件？其作用是什么？
- 5.这些可执行文件中有下载器么？如果有，它们下载了哪些程序？这些程序又是什么作用的？

# 作业8讲解-问题1

挂马网站: 222.29.87.30/scom

网页木马宿主: aa.18dd.net

盗号木马宿主: down.18dd.net





# 作业8讲解-问题2

- 网页加密方法: [www.cha88.cn](http://www.cha88.cn)
- **aa/kl.htm (dispatcher页面)**
  - 十六进制编码
  - `t=utf8to16(xxtea_decrypt(base64decode(t), '\x73\x63\x72\x69\x70\x74'));`
  - Base64编码, xxtea加密(密钥:script), UTF16to8编码
- **1.js (MS06-014网马)**
  - 十六进制编码
- **b.js (暴风影音网马)**
  - 老外写的js加解密工具?
- **pps.js (PPStream网马)**
  - 八进制编码



# 作业8讲解-问题3

- ❑ **dispatcher**页面链接了**4**个网马
- ❑ **MS06-014**网马
  - 攻击**MS06-014**安全漏洞
  - **MDAC RDS.Dataspace ActiveX**控件远程代码执行漏洞
- ❑ 暴风影音网马
  - 攻击**CVE-2007-4816**安全漏洞
  - 暴风影音**2 mps.dll**组件多个缓冲区溢出漏洞
- ❑ **PPStream**网马
  - 攻击**CVE-2007-4748**安全漏洞
  - **PPStream** 堆栈溢出
- ❑ 百度搜霸网马
  - 攻击**CVE-2007-4105**安全漏洞
  - 百度搜霸**ActiveX**控件远程代码执行漏洞



# 作业8讲解-问题4

## □ 网马植入的可执行文件木马

- 下载器：  
**bb/014.exe**
- 下载器进一步植入：
  - **down.18dd.net**
  - **kl/0-19.exe**
  - 盗号木马

IDA View-A Hex View-A Exports Imports Names Functions Structure				
Address	Length	T...	String	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/0.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/1.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/2.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/3.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/4.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/5.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/6.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/7.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/8.exe	
"..." CODE:0...	0000001E	C	http://down.18dd.net/kl/9.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/10.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/11.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/12.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/13.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/14.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/15.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/16.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/17.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/18.exe	
"..." CODE:0...	0000001F	C	http://down.18dd.net/kl/19.exe	
"..." CODE:0...	0000000C	C	IE 执行保护	
"..." CODE:0...	00000007	C	#32770	
"..." CODE:0...	00000008	C	IE执行保护	
"..." CODE:0...	00000009	C	允许执行	
"..." CODE:0...	00000007	C	Button	
"..." CODE:0...	00000005	C	确定	
"..." CODE:0...	00000005	C	允许	
"..." CODE:0...	00000011	C	[AutoRun]\r\nopen=	
"..." CODE:0...	00000014	C	shell\Auto\command=	
"..." CODE:0...	0000003C	C	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	
"..." CODE:0...	00000013	C	NoDriveTypeAutoRun	
"..." CODE:0...	00000011	C	[AutoRun]\r\nopen=	
"..." CODE:0...	00000014	C	shell\Auto\command=	



# 作业8讲解-问题5

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

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	名称	详细信息
<b>恶评插件 (2)</b>	<input type="checkbox"/> 梦幻西游盗号木马	
其它插件 (0)	插件类型：木马 出品公司：未知 文件路径：D:\windows\system32\LYLOADER.EXE <a href="#">清理效果反馈</a> <a href="#">举报恶意软件</a>	
信任插件 (6)	<input type="checkbox"/> 梦幻西游盗号木马变种vs	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
	插件类型：木马 出品公司：未知 文件路径：d:\windows\system32\lyloader.exe <a href="#">清理效果反馈</a> <a href="#">举报恶意软件</a>	

管理记录  
查看管理历史

全选 全不选 立即清除 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：1.0.1.1820 检测版本信息失败 [立即升级](#) [下载离线升级包](#)



# 盗号木马4.Exe动态行为分析

**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

已监视的应用程序

应用程序名称	监视日期	大小
4	2008-5-20 16:24	5.46 KB

**4 [全部详细信息]** 2008年5月20日 16:24

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

enweafx.fon 2008-5-20 16:23, 91 字节, A

system32

kwdacr.dll 2008-5-20 16:23, 52 字节, A

kwdbar.exe 2008-4-25 16:20, 13957 字节, A

kwdbzy.dll 2004-8-4 16:23, 20048 字节, H

verclsid 2008-4-13 19:14, 28672 字节

ShadowService... 2008-5-20 16:22, 1123 字节, HA 2008-5-20 16:23, 1235 字节, HA

注册表

HKEY\_LOCAL\_MACHINE

SOFTWARE

Classes

CLSID

{28907901-1416-3389-9981-372178569982}

InprocServer32

(默认) REG\_SZ, "D:\windows\system32..."

ThreadingModel REG\_SZ, "Apartment"

INTEL

LANDesk

VirusProtect6

CurrentVersion

REG\_DWORD, 3 REG\_DWORD, 0

Microsoft

Windows

CurrentVersion

Explorer

ShellExecuteHooks

{28907901-1416-3389-9981-372178569982} REG\_SZ, "kwdbzy.dll"

Windows NT

CurrentVersion

Windows

AppInit\_DLLs REG\_SZ, "kwdbzy.dll"

Policies

Microsoft

Windows

WindowsUpdate

AU

REG\_DWORD, 3 REG\_DWORD, 1

REG\_DWORD, 0 REG\_DWORD, 1

已安装的服务与设备

D:\ShadowService.log

2008-5-20 16:22, 创建于: 2008-5-20 15:55, 1123 字节, HA

2008-5-20 16:23, 创建于: 2008-5-20 15:55, 1235 字节, HA

1 个已监视的应用程序

开始 Total Uninstall Virus 4\_1.bmp - 画图

16:25 星期二



# 盗号木马4.Exe释放的特殊文件

---

## □ \$WINDOWS\Fonts\enweafx.fon

- 伪装为Windows字体文件，内容却是一个加密的可疑URL地址
- [Send]  
**Url1=EC1A060602485D5D0505055C  
02064B47420B005C111C5D1907084  
A0A185D021D01065C130102**
- 使用了一种简单加密方法
- 如何解密？

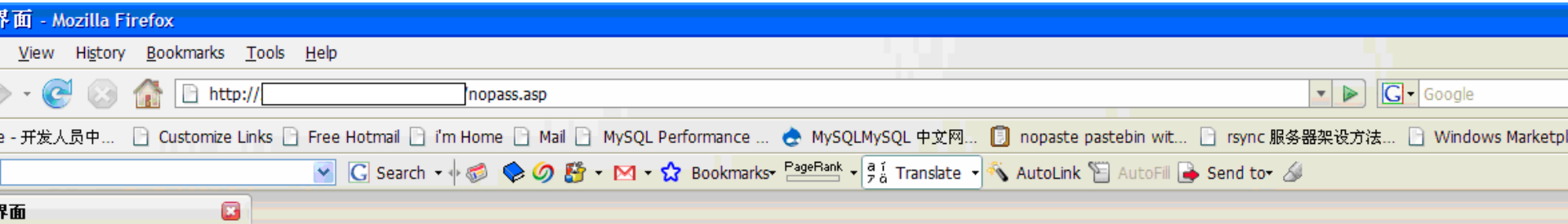


# 特殊文件解密结果

- 密文=EC 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
- 明文= 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 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
- XOR 0x72



# 挂马网站案例中追踪到的箱子



天下無馬QQ:333849

## 信息列表

1 2 页次:1/2

服务器组	账户号码	账户密码	仓库密码	识别码	角色金钱	备注	IP
华东二区 青冥剑	yinming345	*****	*****	***	209353		218.76.85.240
华东一区 斩楼刀	xybwj	*****	*****	***	2451		61.175.234.237
华北一区 百胜刀	xralyang	*****	*****	***	10417		221.215.106.158
华东一区 七宝珠	250764045	*****	*****	***	999		58.223.139.80
华东二区 古锭刀	qq594598047	*****	*****	***	9559		121.9.185.132
华北一区 赤焰枪	tianlun456789	*****	*****	***	27916		222.174.176.138
华东二区 古锭刀	gudiandao	*****	*****	***	91279		121.9.185.132
西南一区 朱雀剑	13474218680	*****	*****	***	47964		61.185.64.158
西南一区 朱雀剑	fu80725984	*****	*****	***	0		61.185.64.158
东北一区 七杀刀	wangweidong1230	*****	*****	***	12710		61.185.82.137
华北一区 百胜刀	xxyyqq116633	*****	*****	***	207		221.215.106.158
东北一区 七杀刀	fu5201iao	*****	*****	***	0		61.185.82.137
华北二区 碧血剑	kai4672593	*****	*****	***	87865		121.16.19.89

# Thanks

---

诸葛建伟

**zhugejianwei@icst.pku.edu.cn**