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**

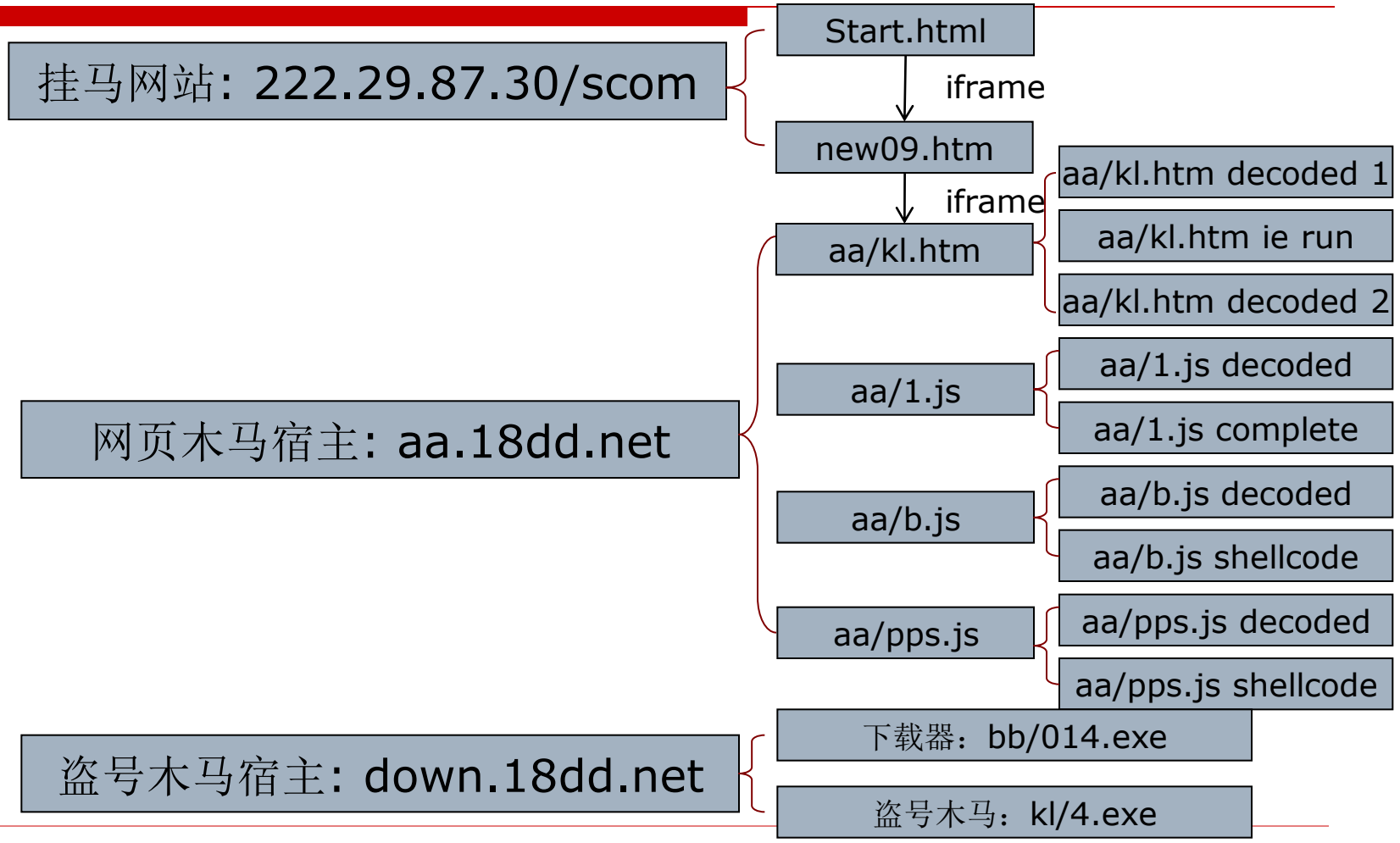
作业8说明

- 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]**
  - 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
Start.html
iframe
new09.htm
iframe
aa/kl.htm
aa/kl.htm decoded 1
aa/kl.htm ie run
aa/kl.htm decoded 2
网页木马宿主: aa.18dd.net
aa/1.js
aa/1.js decoded
aa/1.js complete
aa/b.js
aa/b.js decoded
aa/b.js shellcode
aa/pps.js
aa/pps.js decoded
aa/pps.js shellcode
盗号木马宿主: down.18dd.net
下载器：bb/014.exe
盗号木马：kl/4.exe

作业8讲解-问题2

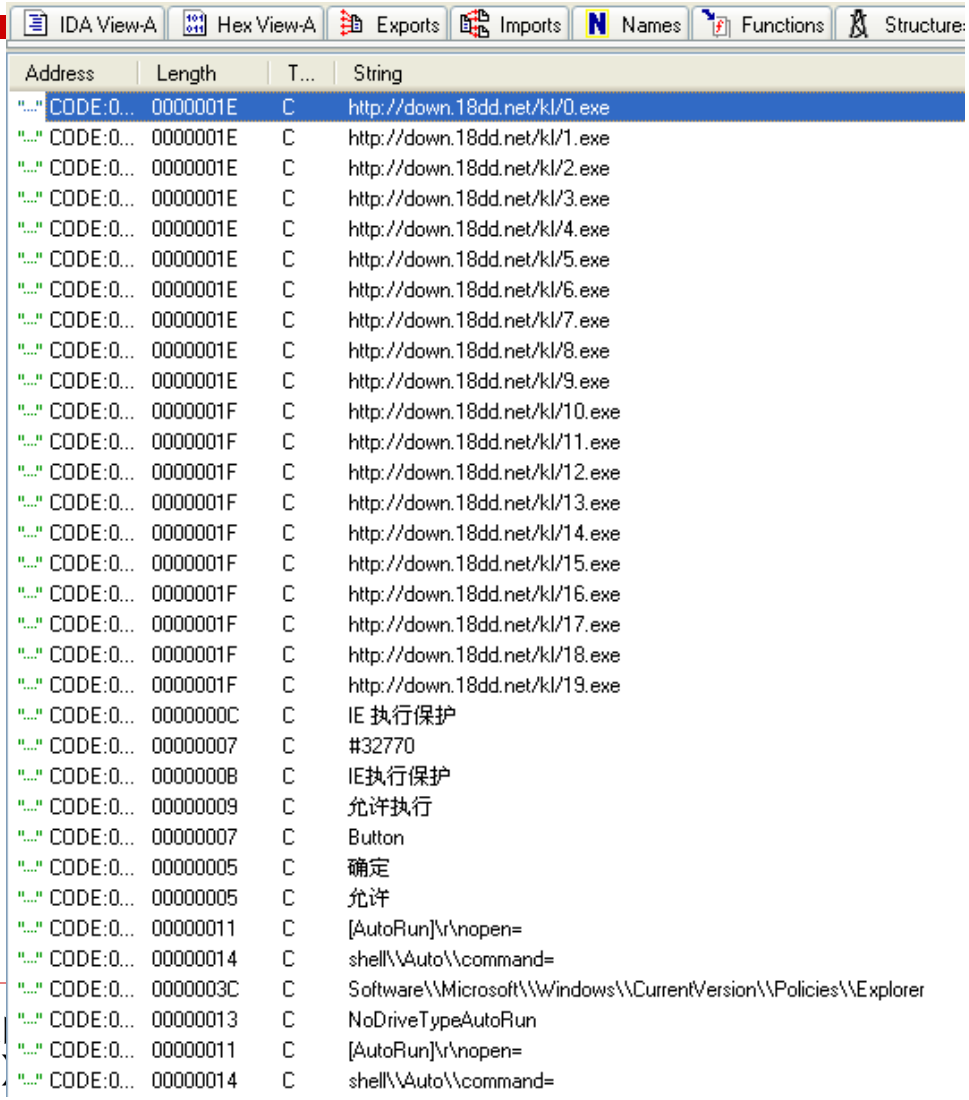
- 网页加密方法: www.cha88.cn
- **aa/kl.htm (dispatcher页面)**
  - 十六进制编码
  - **t=utf8to16(xxtea_decrypt(base64decode(t), '\x73\x63\x72\x69\x70\x74'));**
  - **Base64编码, xxtea加密(密钥:script), UTF16to8编码**
- **1.js (MS06-014网马)**
  - 十六进制编码
- **b.js (暴风影音网马)**
  - 老外写的**js**加解密工具?
- **pps.js (PPStream网马)**
  - 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

作业8讲解-问题3

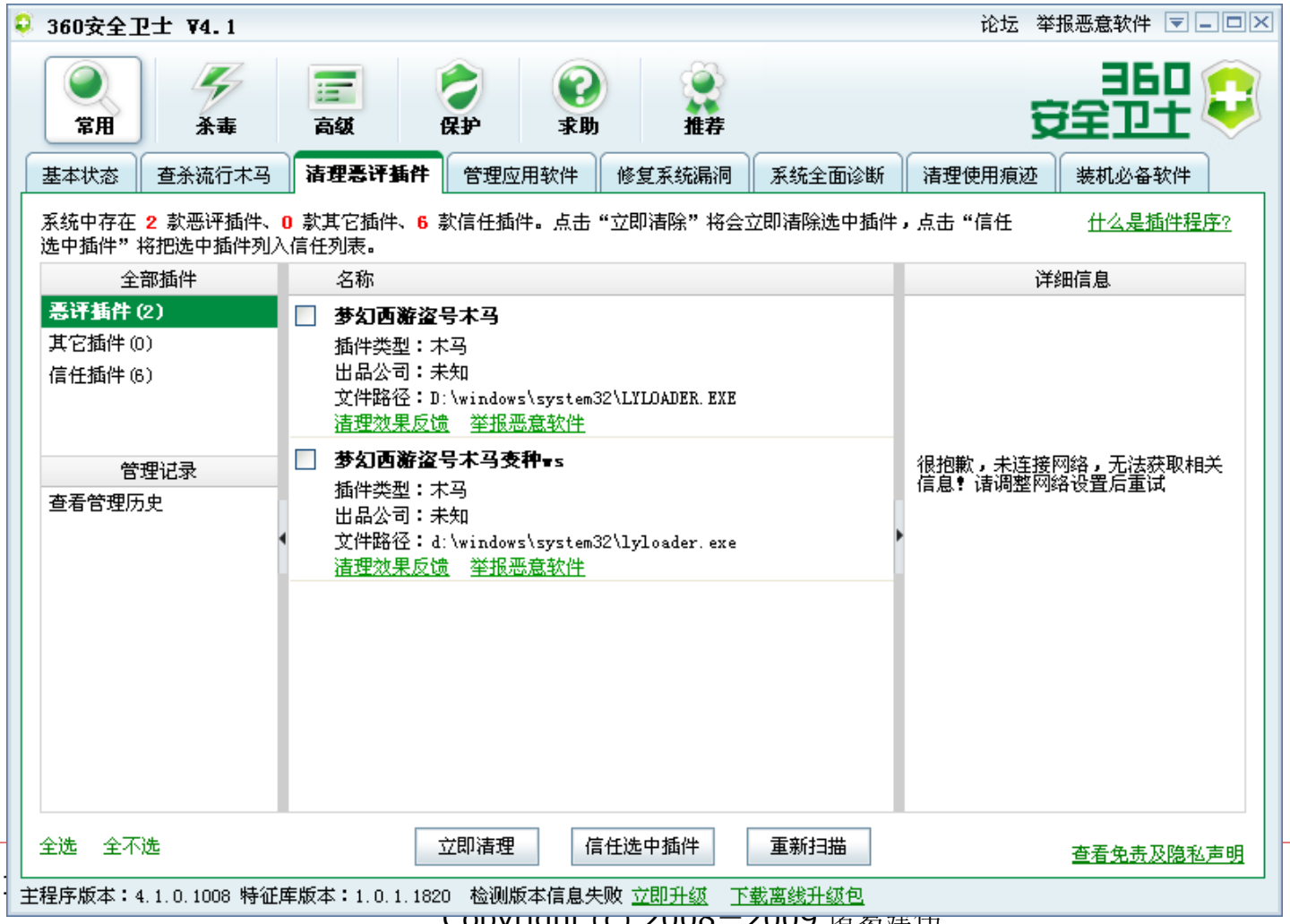
- dispatcher页面链接了4个网马
- MS06-014网马
  - 攻击MS06-014安全漏洞
  - MDAC RDS.Dataspace ActiveX控件远程代码执行漏洞
- 暴风影音网马
  - 攻击CVE-2007-4816安全漏洞
  - 暴风影音2 mps.dll组件多个缓冲区溢出漏洞
- PPStream网马
  - 攻击CVE-2007-4748安全漏洞
  - PPStream 堆栈溢出
- 百度搜霸网马
  - 攻击CVE-2007-4105安全漏洞
  - 百度搜霸ActiveX控件远程代码执行漏洞

作业8讲解-问题4

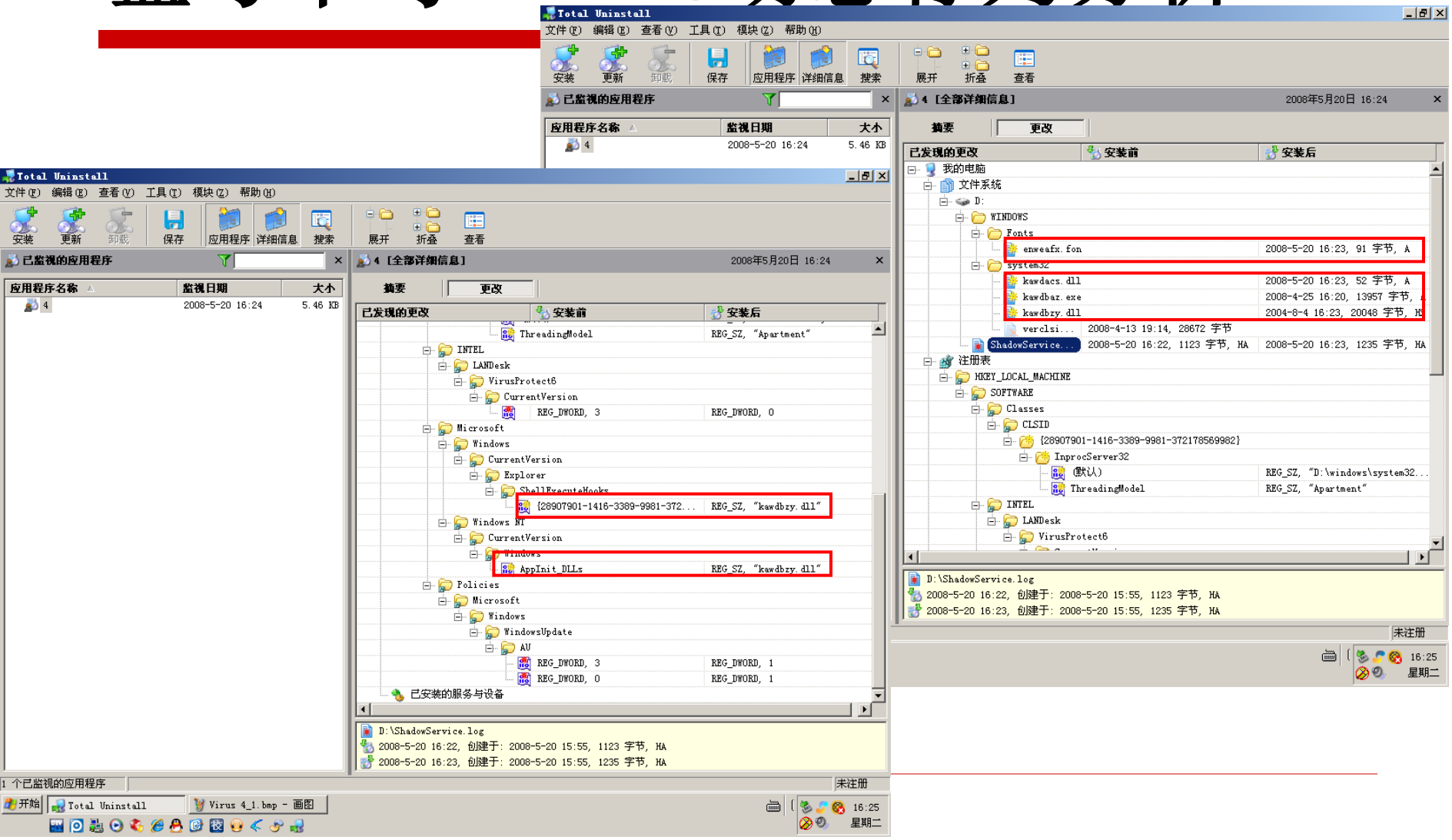
- 网马植入的可执行文件木马
  - 下载器：**bb/014.exe**
  - 下载器进一步植入：
    - **down.18dd.net**
    - **kl/0-19.exe**
    - 盗号木马



作业8讲解-问题5



盗号木马4.Exe动态行为分析



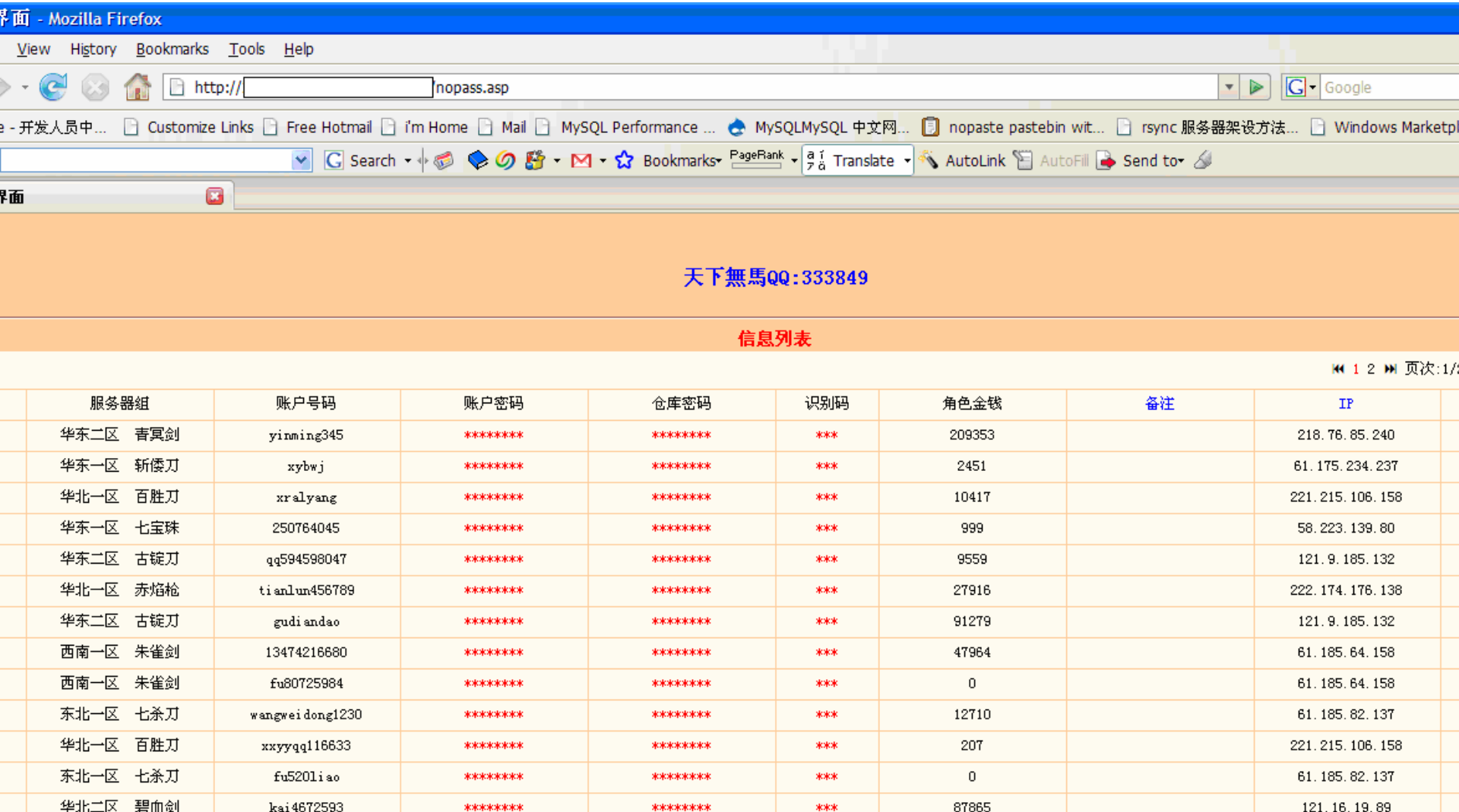
盗号木马4.Exe释放的特殊文件

- **$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=EC1A060602485D5D0505055C02064B47420B005C111C5D1907084A0A185D021D01065C130102
  - 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



Thanks

诸葛建伟

zhugejianwei@icst.pku.edu.cn