上海交通大学校园网
近期ARP欺骗分析与控制

网络信息中心: 姜开达

2008年4月1日

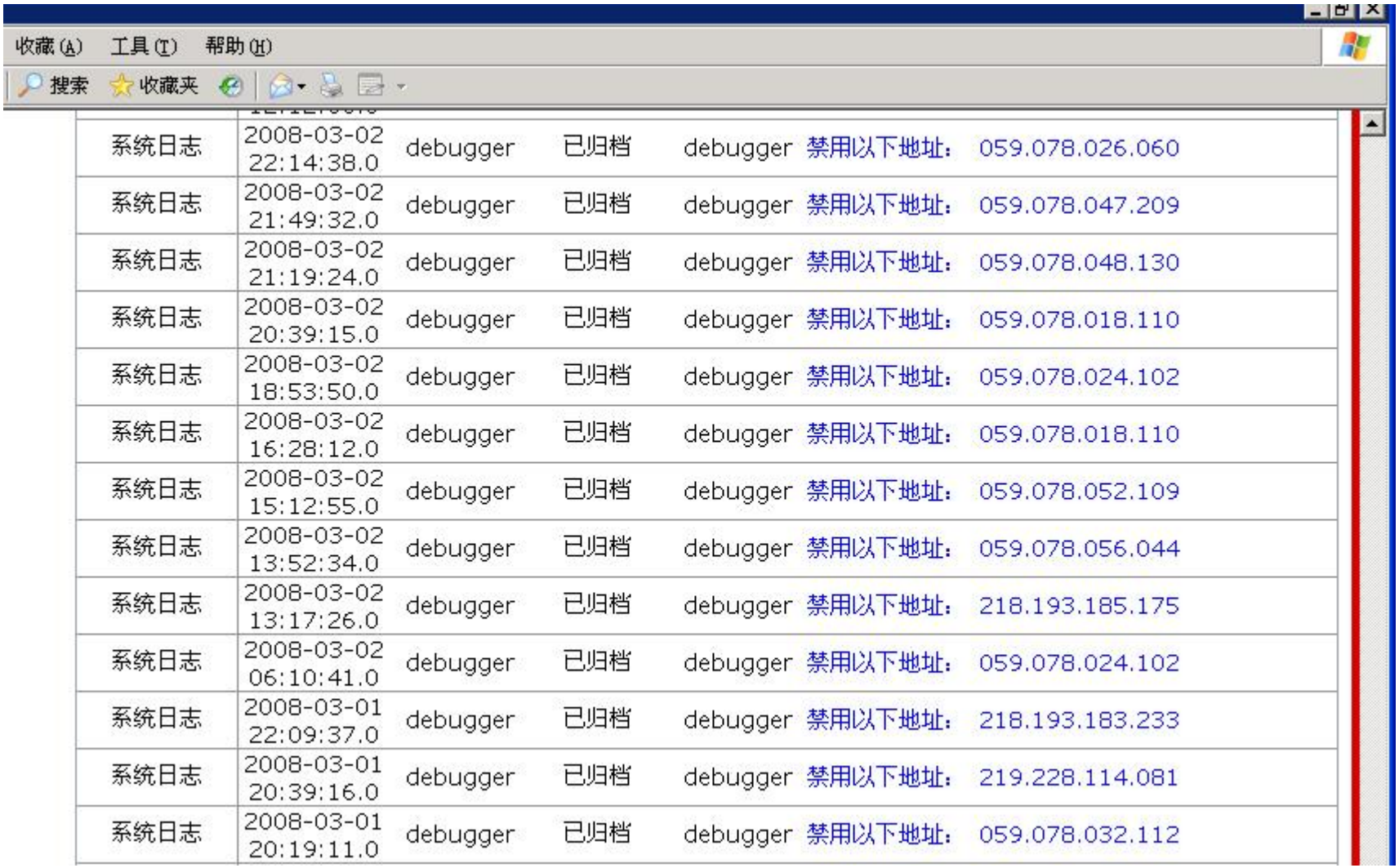
ARP欺骗引起网络用户抱怨

- ARP欺骗的发现与分析
  - 长期全面监测
  - 深入一线分析
- 针对性确定控制策略
  - 黑洞路由控制
  - 访问控制列表、防火墙
  - TCP劫持，DNS欺骗

扫描器获取三层交换机ARP信息

				22:18:41.0
059.078.026.076	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:18:40.0
059.078.026.057	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:18:40.0
059.078.026.045	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:18:40.0
059.078.026.015	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:18:39.0
059.078.026.204	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:30.0
059.078.026.181	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:30.0
059.078.026.170	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:30.0
059.078.026.159	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:30.0
059.078.026.095	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:29.0
059.078.026.077	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:29.0
059.078.026.075	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:29.0
059.078.026.011	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:17:28.0
059.078.026.240	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:16:21.0
059.078.026.239	00023F:E8C678	冒用他人IP;	Sm3-D16-211601/	2008-03-02 22:16:21.0

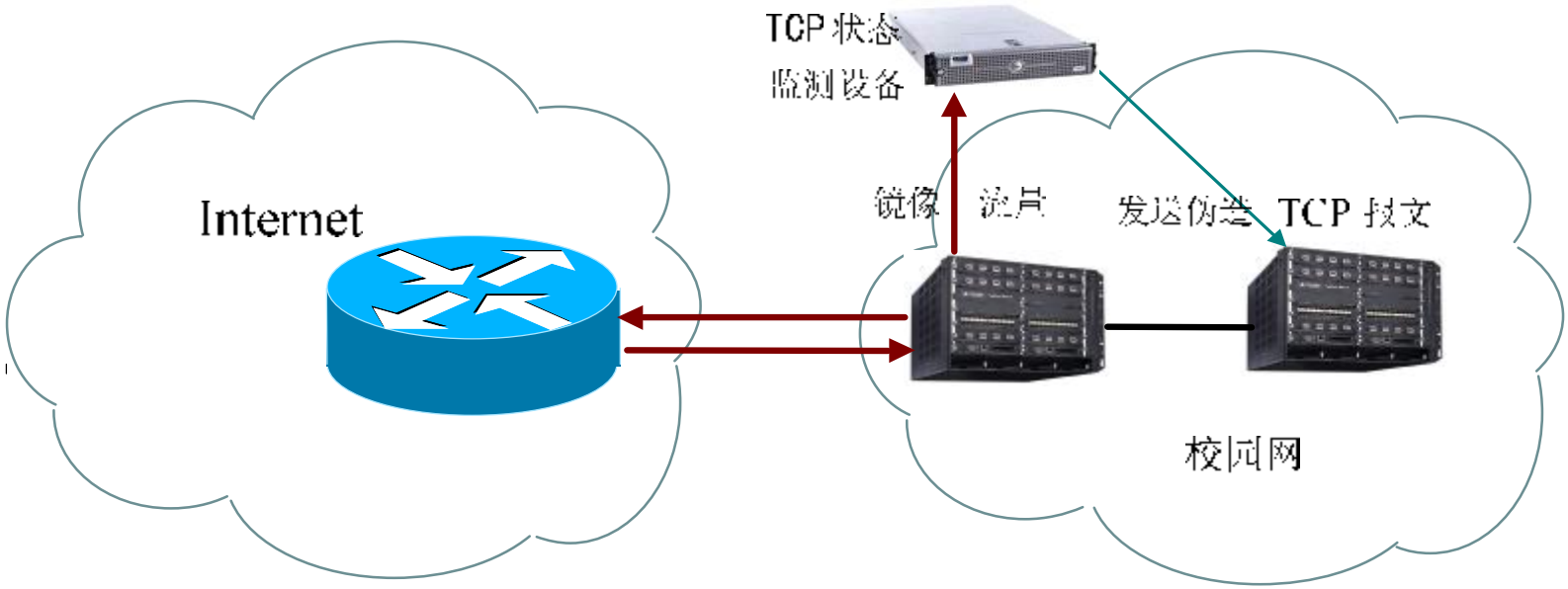
智能分析出ARP欺骗主机



系统日志	2008-03-02 22:14:38.0	debugger	已归档	debugger	禁用以下地址： 059.078.026.060
系统日志	2008-03-02 21:49:32.0	debugger	已归档	debugger	禁用以下地址： 059.078.047.209
系统日志	2008-03-02 21:19:24.0	debugger	已归档	debugger	禁用以下地址： 059.078.048.130
系统日志	2008-03-02 20:39:15.0	debugger	已归档	debugger	禁用以下地址： 059.078.018.110
系统日志	2008-03-02 18:53:50.0	debugger	已归档	debugger	禁用以下地址： 059.078.024.102
系统日志	2008-03-02 16:28:12.0	debugger	已归档	debugger	禁用以下地址： 059.078.018.110
系统日志	2008-03-02 15:12:55.0	debugger	已归档	debugger	禁用以下地址： 059.078.052.109
系统日志	2008-03-02 13:52:34.0	debugger	已归档	debugger	禁用以下地址： 059.078.056.044
系统日志	2008-03-02 13:17:26.0	debugger	已归档	debugger	禁用以下地址： 218.193.185.175
系统日志	2008-03-02 06:10:41.0	debugger	已归档	debugger	禁用以下地址： 059.078.024.102
系统日志	2008-03-01 22:09:37.0	debugger	已归档	debugger	禁用以下地址： 218.193.183.233
系统日志	2008-03-01 20:39:16.0	debugger	已归档	debugger	禁用以下地址： 219.228.114.081
系统日志	2008-03-01 20:19:11.0	debugger	已归档	debugger	禁用以下地址： 059.078.032.112

自动采取措施（1）

- 对用户在线告警
  - 利用TCP劫持来实现网页重定向
  - 用户端浏览器弹出告警网页



文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 搜索 收藏夹

地址(D) http://cert.sjtu.edu.cn/black/ 转到 链

SJTU CERT 上海交通大学 计算机紧急响应组

关于我们 安全公告 安全建议 杀毒中心 工具补丁 病毒库自动更新 校内WindowsUpdate自动更新

警告：

您的电脑已经被黑客远程控制

请按下文说明操作清除木马和后门。如果已清除，明天会再提醒一次，后天开始不再提醒。

关于近期清理校内感染木马用户的说明

您的IP地址是 202.120.2.231

校园网禁用/告警用户名单

如果您确认问题已解决并采取有效措施防止此类事件重演，请联系网络信息中心解封，联系方式如下：

电子邮件：cert@sjtu.edu.cn
徐汇校区：浩然高科技大厦4F网络信息中心 62932944-0
闵行校区：闵行计算中心2F网络信息中心(地图) 54742547-0

相关背景文章

基于TCP会话劫持的校园网安全告警系统

推荐 下载阅读CAJ格式全文 下载阅读PDF格式全文

【英文篇名】	Campus Network Security Alarm System Based on TCP Session Hijack
【作者中文名】	佘华君; 姜开达; 黄保青;
【作者英文名】	SHE Hua-jun; JIANG Kai-da; HUANG Bao-qing（Network & Information Center; Shanghai Jiaotong University; Shanghai 200030; China）;
【作者单位】	上海交通大学网络信息中心; 上海交通大学网络信息中心 上海;
【文献出处】	厦门大学学报(自然科学版), Journal of Xiamen University(Natural Science), 编辑部邮箱 2007年 S2期 期刊荣誉：中文核心期刊要目总览 ASPT来源刊 中国期刊方阵 CJFD收录刊
【关键词】	三次握手; TCP会话劫持; 网络安全;
【英文关键词】	three-way handshake; TCP session hijack; network security;
【摘要】	本系统通过端口镜像对校园网边界出口处的网络流量中TCP三次握手状态信息进行监测,并根据自定义的匹配过滤策略来精心构造会话劫持报文,以旁路方式发回给校园网内主机,来达到干预有问题的用户到外网的TCP会话的目的.干预的结果可以是立即中断TCP连接,也可以是将用户的所有HTTP访问请求重定向到指定的安全告警页面.本研究为在校园网内构建一种有效的安全告警系统提供了方向,同时也在过滤不良网站,用户身份认证等方面有着广泛应用.
【英文摘要】	We monitor the "three-way handshake" states of the net flow at the boundary of campus network and intervene the TCP sessions of th e users who have network security problems.We achieve this goal by using TCP hijack,and construct the TCP packets elaborately and send them to client computer who is on the blacklist.Through this way we can redirect all HTTP requests to the network security alarm webpage o f Computer Emergency Response Team of Shanghai Jiao Tong University or we can break off the TCP connection im...
【DOI】	CNKI:SUN:XDZK.0.2007-S2-018

自动采取措施（2）

- 用户离线隔离
  - 在接入层交换机上操作
  - 不同类型交换机开发不同的接口
  - SNMP等操作自动关闭对应接入交换机端口

大规模爆发ARP欺骗的控制

- 近期磁碟机(DiskGen)病毒大面积爆发，这种病毒会利用ARP欺骗技术来进行传播。
- 三月初校内有ARP欺骗现象的电脑90％以上都伴随有磁碟机病毒的影子。
- 更详细的磁碟机病毒分析请Google获取。

磁碟机病毒的实时监测

转到 请选择日期 20080319 上海教科网磁碟机病毒(ARP欺骗类型)分布报表(流出) 按目的IP地址重新排序

No.	Start Time	源IP	目标IP	URL	出现次数
1.	2008-3-19 17:43:33	58.198.74.235	222.208.183.204	http://w.cOmo.com/r.htm	1
2.	2008-3-19 15:13:24	58.198.83.194	222.208.183.204	http://jj.gxgxy.net/html/dg2.html	5
3.	2008-3-19 15:05:33	58.198.83.194	222.208.183.243	http://js.k0102.com/goto.htm	5
4.	2008-3-19 9:27:38	58.198.97.213	222.208.183.204	http://w.cOmo.com/r.htm	2
5.	2008-3-19 9:25:38	58.198.126.230	222.208.183.204	http://w.cOmo.com/r.htm	1
6.	2008-3-19 18:52:03	59.78.125.243	222.208.183.204	http://g.52hxsh.com/1.js	5
7.	2008-3-19 8:44:05	59.79.0.53	222.208.183.204	http://w.cOmo.com/r.htm	3
8.	2008-3-19 8:45:09	59.79.0.53	222.208.183.243	http://js.k0102.com/goto.htm	7
9.	2008-3-19 23:47:52	59.79.16.7	222.208.183.243	http://js.k0102.com/ad.asp	21
10.	2008-3-19 17:00:14	59.79.16.153	222.208.183.204	http://w.cOmo.com/r.htm	4
11.	2008-3-19 22:59:19	59.79.16.153	222.208.183.243	http://js.k0102.com/ad.asp	32
12.	2008-3-19 17:14:48	59.79.44.24	222.208.183.204	http://w.cOmo.com/r.htm	2
13.	2008-3-19 18:51:23	59.79.54.153	222.208.183.204	http://w.cOmo.com/r.htm	2
14.	2008-3-19 18:52:26	59.79.54.153	222.208.183.243	http://js.k0102.com/goto.htm	2
15.	2008-3-19 20:14:45	59.79.58.27	222.208.183.204	http://jj.gxgxy.net/html/dg2.html	8
16.	2008-3-19 20:09:51	59.79.58.27	222.208.183.243	http://js.k0102.com/goto.htm	5

域名的解析结果可能会改变

2008-3-19 17:43:33 222.208.183.204 http://w.c0mo.com/r.htm
2008-3-24 21:56:03 125.65.165.133 http://w.c0mo.com/r.htm

2008-3-19 15:05:33 222.208.183.243 http://js.k0102.com/go.asp
2008-3-22 20:05:20 218.83.175.154 http://js.k0102.com/go.asp
2008-3-25 8:16:24 125.65.165.133 http://js.k0102.com/go.asp

控制磁碟机病毒爆发思路

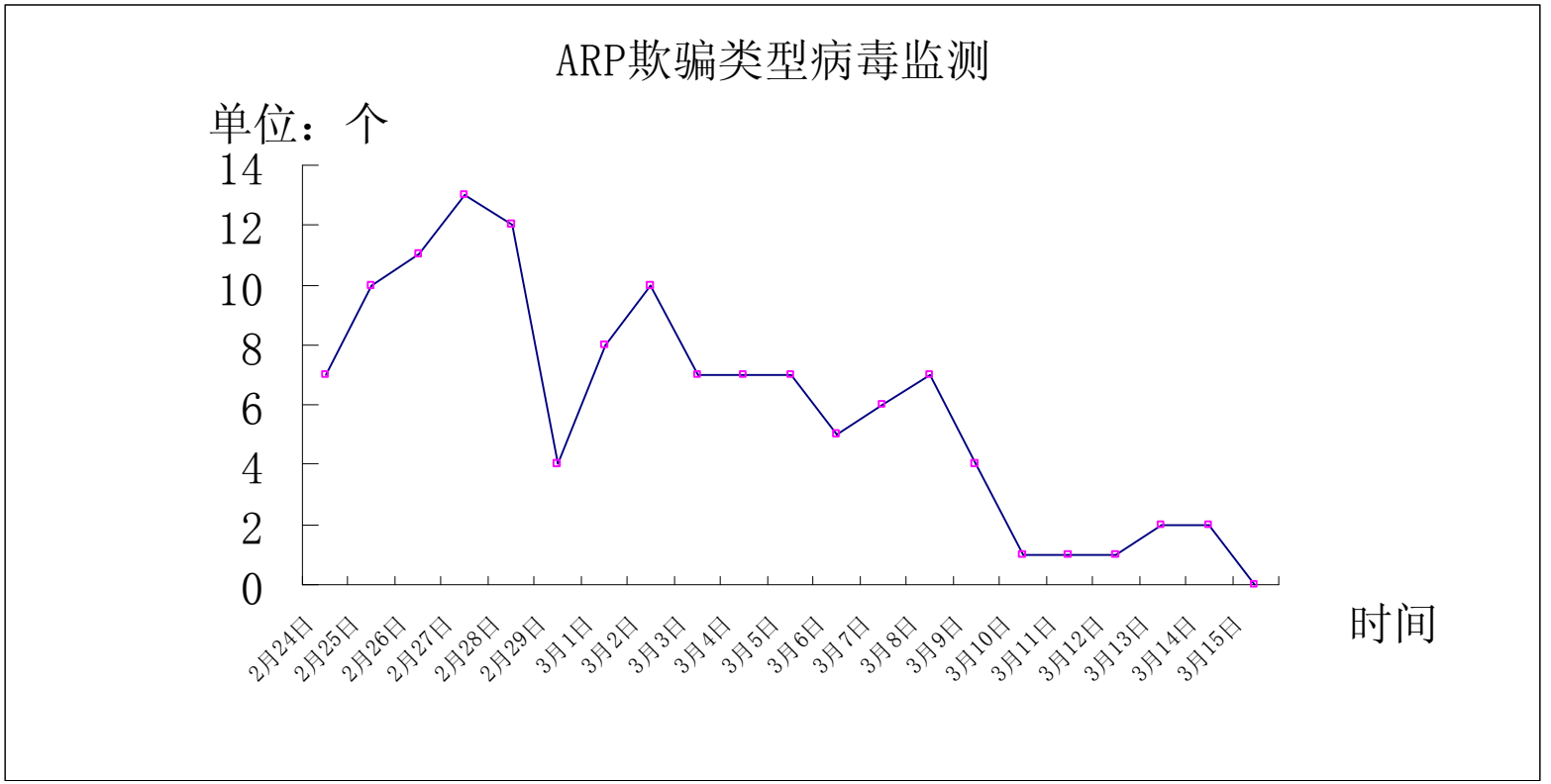
- 核心或边界路由器、防火墙上直接封掉

  ip route 222.208.183.0/24 null0 （需要人工频繁干预）

- 通过动态路由协议在其他位置进行控制
  - Linux ＋ Zebra 软件路由器
  - 使用脚本定时动态解析域名
  - 自动生成 相关路由 命令

  降低人工干预频率

控制磁碟机病毒爆发思路



最近一周校内基本没有发现ARP欺骗现象

谢 谢！

kaida@sjtu.edu.cn