应急响应协同服务系统

杨望

- 系统架构
- 配置需求
- 事件说明
- 下一步工作

CHAIRS & 蜜罐

- CHAIRS
  - 安全事件的关联、筛选、分级和响应
- 蜜罐系统
  - Botnet主机的活动信息
  - 低交互蜜罐：通用型、SSH、WEB
- 恶意代码监控系统
  - Webshell活动，木马活动
  - 全包文采集，北京60G，上海60G，广州20G

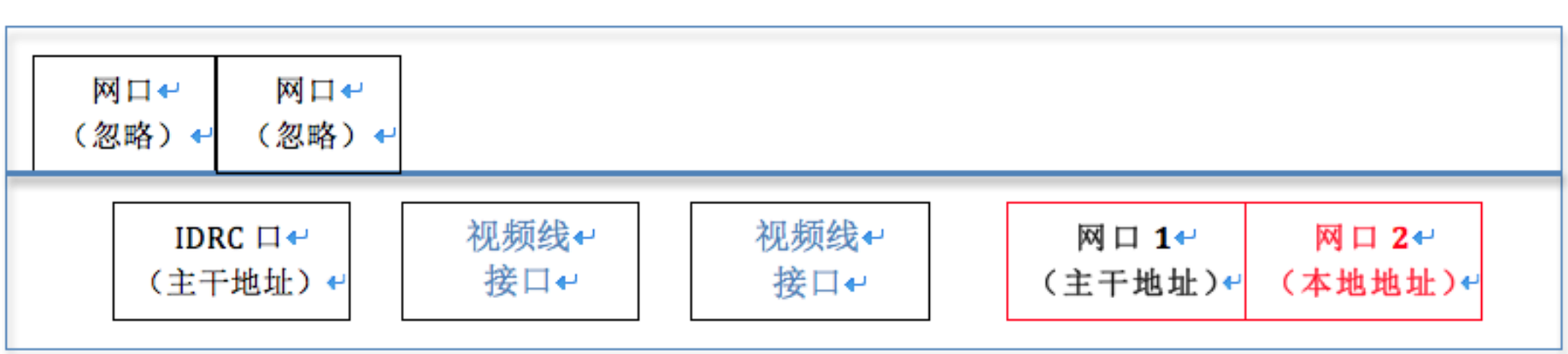
CHAIRS系统配置

- CHAIRS系统
  - 驻地提供一个本地地址
  - 和NBOS系统在一个网段和VLAN
  - 通过曙光交换机第二交换模块（右侧）第三个上联网口接入
  - 该地址通过443端口对外提供访问
  - 驻地节点对该地址要进行访问控制

蜜罐系统

- 蜜罐系统
  - 驻地系统提供4个本地地址，建议在同一个网段和VLAN
  - 接入Dell R320第二个网口
  - 如果担心流量计费问题，可限制该地址段只能访问免费地址段

Dell R320 后视图



2013-10-17 8:18:48 | certuser1 | 注

应急响应协同服务系统

Cooperative Hybrid Aided Incidence Response System

首页 | 事件报告 | 安全状态 | 用户配置 | 帮助

总案件数	全新案件数	待定性案件数	跟踪案件数
0	0	0	0

内部威胁

分类	事件数	威胁源数	威胁宿数
挂马网站	28	170	51
后门	14	529	74

外部威胁

分类	事件数	威胁源数	威胁宿数
攻击	38	573	26
恶意代码	33	229	26

CHAIRS事件

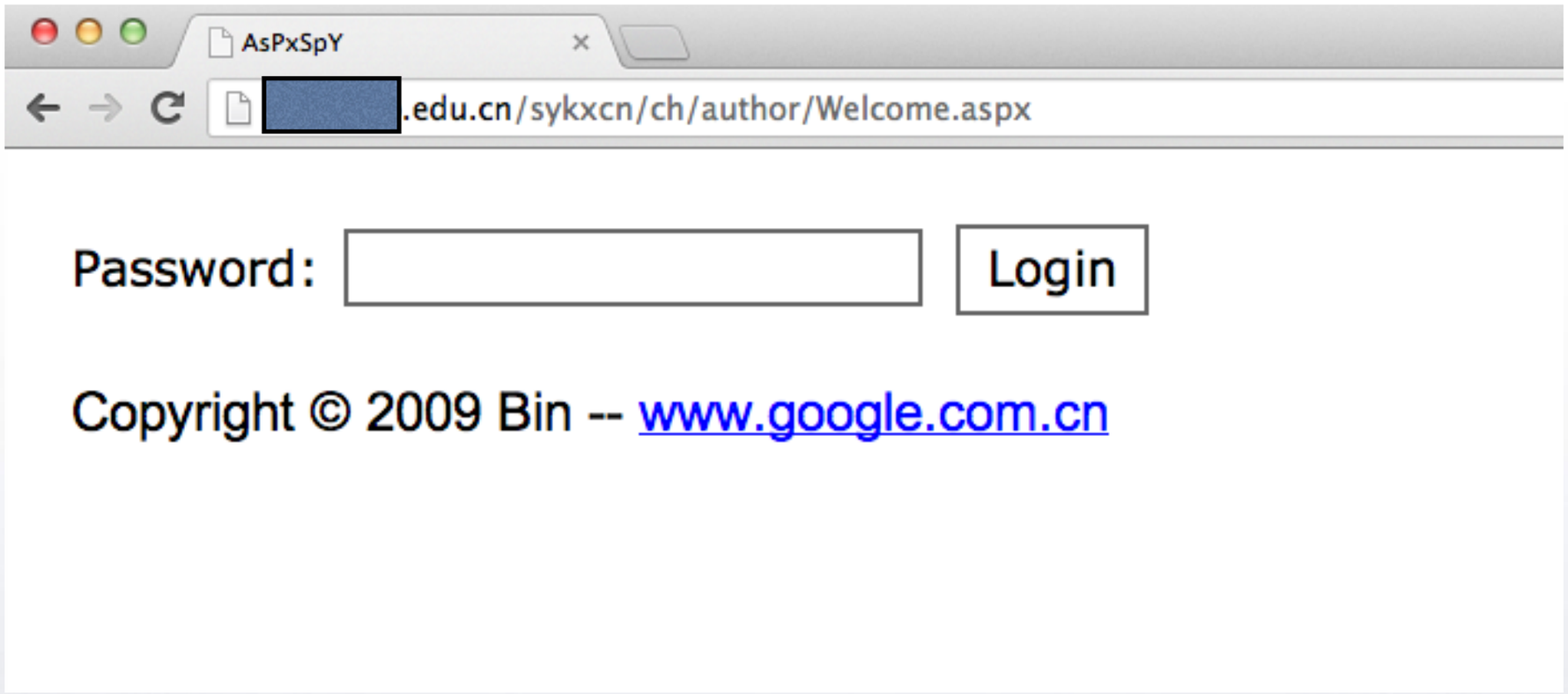
- 内部威胁
  - 挂马网站
  - 后门
- 外部威胁
  - 攻击
  - 恶意代码

CHAIRS事件

- 挂马网站
- 暗链，挂马
- Webshell
- 学校内部的网站服务器已被攻陷

Webshell

- http://xxx.xxx.edu.cn/sykxcn/ch/author/Welcome.aspx



CHAIRS事件

- 后门
  - 木马通讯活动
    - 学校内部主机和外部服务器有木马通信行为
  - 未授权服务活动
    - 学校内部主机对的3389、19等端口进行大规模或长时间的访问行为
    - 该主机一般已被攻陷

未授权服务活动

编号	主题	未授权访问主机数量	检测到活跃次数	开始日期	最近活跃
NJ0-2013007413	发现未授权流量活动, 未授权访问者202.119.120.122 ,未授权端口 3389	27126	1604	2013-10-10 15:00:11	2013-10-17 08:14:52
NJ0-2013007423	发现未授权流量活动, 未授权访问者210.28.101.74 ,未授权端口 3389	26631	1568	2013-10-10 15:00:23	2013-10-17 08:14:54
NJ0-2013007431	发现未授权流量活动, 未授权访问者58.213.129.215 ,未授权端口 3389	26352	1546	2013-10-10 15:00:18	2013-10-17 08:14:59
NJ0-2013007432	发现未授权流量活动, 未授权访问者58.213.129.214 ,未授权端口 3389	26076	1544	2013-10-10 15:00:04	2013-10-17 08:14:53
NJ0-2013012311	发现未授权流量活动, 未授权访问者202.119.199.108 ,未授权端口 3389	13366	537	2013-10-11 18:58:35	2013-10-15 17:42:36
NJ0-2013007421	发现未授权流量活动, 未授权访问者210.29.134.178 ,未授权端口 3389	9464	1541	2013-10-10 15:01:56	2013-10-17 08:13:52
NJ0-2013007467	发现未授权流量活动, 未授权访问者222.192.184.43 ,未授权端口 3389	3976	375	2013-10-10 15:20:27	2013-10-17 08:06:00
NJ0-2013008004	发现未授权流量活动, 未授权访问者219.219.117.6 ,未授权端口 3389	3160	121	2013-10-11 03:09:39	2013-10-11 13:34:27
NJ0-2013007448	发现未授权流量活动, 未授权访问者202.119.236.9 ,未授权端口 3389	2557	316	2013-10-10 15:16:58	2013-10-17 06:44:24
	发现未授权流量活动, 未授权访问者114.214.80.65 ,未授权端口 3			2013-10-13 00:09:4	2013-10-15 02:32:

主题：发现未授权流量活动, 未授权访问者202.119.120.122 ,未授权端口 3389

状态：新建

分类：未授权流量

首次检测：2013-10-10 15:00:11　　最近活跃:2013-10-17 08:14:52

处理期限：　　解决日期：

威胁源IP：	IP 总数：1	202.119.120.122
	网段 总数：1	202.119.120.0/24
	国家 总数：1	中国
	组织 总数：1	大学
威胁源域名：	域名 总数：0	

威胁宿IP：	IP 总数：27126	128.1.93.100	128.2.83.146	128.4.46.63	128.6.177.82	128.7.236.4	...
	网段 总数：27070	128.1.93.0/24	128.2.83.0/24	128.4.46.0/24	128.6.177.0/24	128.7.236.0/24	...
	国家 总数：136	中国	中国台湾	中国澳门	中国香港	...	
	组织 总数：6168	##### BLIC.NET AS peering info	"Armentel" CJSC . Armenia Telephone Company	"RELCOM.BUSINESS NETWORK" Ltd	"St.Petersburg Telephone Network"	(aq) Networks Limited	...
威胁宿域名：	域名 总数：0						

描述：

	分析器	源端口	威胁宿IP	威胁宿IP归属描述	宿端口	检测到活跃次数	检测到活跃时间(秒)	流数	吞吐量(bytes)	吞吐量(pkts)	开始时间	最后活动
	NBOS-NJ-01	*	175.139.135.210	马来西亚 CORE IP DEVELOPMENT	3389	16	651	25	767/2573	4/22	2013-10-12 13:09:00	2013-10-1 14:30:13
	NBOS-NJ-01	*	23.108.7.193	美国 Akamai Technologies, Inc	3389	15	1700	32	563/2799	9/25	2013-10-14 08:20:53	2013-10-1 09:37:59
	NBOS-NJ-01	*	128.143.127.22	美国 University of Virginia	3389	15	106	16	54/2444	1/15	2013-10-15 02:39:03	2013-10-1 04:48:10
	NBOS-NJ-01	*	187.75.255.182	巴西 Comite Gestor da Internet no Brasil	3389	13	1748	29	999/1791	8/23	2013-10-12 13:44:27	2013-10-1 14:48:46
	NBOS-NJ-01	*	15.203.200.30	美国 Hewlett-Packard Company	3389	13	1362	25	522/3373	8/20	2013-10-14 02:08:54	2013-10-1 03:12:18
	NBOS-NJ-01	*	211.240.36.40	韩国 ELIMNET, INC	3389	13	1232	26	885/2656	5/22	2013-10-15 13:53:12	2013-10-1 15:01:12
	NBOS-NJ-01	*	114.246.111.13	中国 China Unicom Beijing province network	3389	13	1225	25	268/2590	4/22	2013-10-11 22:10:21	2013-10-1 23:19:42
	NBOS-NJ-01	*	203.34.124.205	iiNet Limited	3389	13	1170	21	809/2203	4/18	2013-10-15 09:10:05	2013-10-1 10:10:05
	NBOS-NJ-01	*	172.247.58.186	美国 America Online	3389	13	893	22	1141/6309	3/21	2013-10-14 19:44:18	2013-10-1 20:45:26
	NBOS-NJ-01	*	75.220.105.231	美国 Cellco Partnership DBA Verizon Wireless	3389	12	1304	29	766/2989	10/21	2013-10-15 07:33:37	2013-10-1 08:26:06

木马活动

TH0-2013002990	发现BOTNET-conficker b僵尸网络活动, 控制服务器149.20.56.34	BOTNET-conficker b	0	190	2013-06-22 00: 7:09
TH0-2013002991	发现白金远控类v4.72/v4.73/4.83肉鸡通信rh僵尸网络活动, 控制服务器120.1.19.146	白金远控类v4.72/v4.73/4.83肉鸡通信rh	0	179	2013-06-22 19: 8:44
TH0-2013002992	发现千里目远控v2.1/v2.4/上兴远控v5.0肉鸡上线hr僵尸网络活动, 控制服务器123.126.34.130	千里目远控v2.1/v2.4/上兴远控v5.0肉鸡上线hr	0	178	2013-06-22 20: 4:51
TH0-2013002993	发现千里目远控v2.1/v2.4/上兴远控v5.0肉鸡上线hr僵尸网络活动, 控制服务器123.126.34.26	千里目远控v2.1/v2.4/上兴远控v5.0肉鸡上线hr	0	348	2013-06-22 16: 8:31
TH0-2013002994	发现千里目远控v2.1/v2.4/上兴远控v5.0肉鸡上线hr僵尸网络活动, 控制服务器124.95.136.193	千里目远控v2.1/v2.4/上兴远控v5.0肉鸡上线hr	0	208	2013-06-22 12: 0:04

- 外部威胁
  - 攻击：DDoS
  - 恶意代码：外部botnet活动主机，控制服务器
  - 保持关注

被攻击IP	攻击IP数目	攻击强度(pps)	攻击强度(kbps)	攻击时间(min)	规则	附件	首次检测	最近活跃
166.111.30.55	14	292	2644	3850	伪造源地址TCP Flood攻击	**NBOSDDOS1379839348222.log**	2013-09-22 15:35:47	2013-09-22 16:39:57
59.66.123.26	1	318	2560	18452	伪造源地址TCP Flood攻击	**NBOSDDOS1379839348226.log**	2013-09-22 16:06:17	2013-09-22 18:06:37
101.6.30.38	1	344	3378	4626737	伪造源地址TCP Flood攻击	**NBOSDDOS1379839948576.log**	2013-09-22 05:12:01	2013-10-15 18:34:53
166.111.65.35	1	372	3322	3656	伪造源地址TCP Flood攻击	**NBOSDDOS1379840256825.log**	2013-09-22 16:24:00	2013-09-22 18:27:57
166.111.134.52	1	291	2656	12951	伪造源地址TCP Flood攻击	**NBOSDDOS1379840256825.log**	2013-09-22 16:24:59	2013-09-22 18:25:32
166.111.3.3	40	208	2235	17600	伪造源地址TCP Flood攻击	**NBOSDDOS1379840557023.log**	2013-09-22 15:58:10	2013-10-16 08:24:59
59.66.190.232	8	425	4993	1882	伪造源地址TCP Flood攻击	**NBOSDDOS1379840847021.log**	2013-09-22 16:32:24	2013-09-22 17:03:46
59.66.62.232	44	300	3080	1563	伪造源地址TCP Flood攻击	**NBOSDDOS1379841148237.log**	2013-09-22 17:05:14	2013-09-30 19:24:59
59.66.212.43	4	304	2557	1806	伪造源地址TCP Flood攻击	**NBOSDDOS1379841447341.log**	2013-09-22 16:43:11	2013-09-22 17:13:17
59.66.120.151	2	221	2557	3598	伪造源地址TCP Flood攻击	**NBOSDDOS1379841447343.log**	2013-09-22 16:43:49	2013-09-22 18:14:06
101.5.153.254	1	276	2680	1801	伪造源地址TCP Flood攻击	**NBOSDDOS1379841447344.log**	2013-09-22 16:44:02	2013-09-22 17:14:03
					伪造源地址TCP Flo	**NBOSDDOS1379841475**	2013-09-22 17:1	2013-09-22 17:1

- 下一步工作
- 进一步提供事件的可信度
- 如何开展响应工作

友情通知

- 38个节点NOC请到姚星昆老师处领取个人证书优盘
- 地址：用户体验中心
- 电话：13810978844