江苏省网络安全事件态势分析与响应协作

CERNET华东北地区网络中心
东南大学 计算机学院
丁伟 wding@njnet.edu.cn
杨望 wyang@njnet.edu.cn
20140418　镇江

大纲

- CERNET江苏省网的安全态势分析
- 校园网安全事件的响应与协作
- 校园网用户的CHAIRS系统使用
- 校园网用户的NBOS信息共享

CERNET江苏省网的安全态势分析

- 目前CERNET江苏省网安全监视系统
  - 基于211/3期建设
  - CHAIRS系统
  - NBOS系统
  - 部署于江苏省网主干边界
  - 部分数据来源于CERNET国内和国际互联点
  - 2013年10月～2014年4月

网站安全

- 网站后门
  - 54家单位
  - 893个网站
  - 2609个后门

网站后门--火狐大类黑客操控肉鸡网站hr	613
网页篡改--炫技/宣泄类2	474
网站后门--一句话木马0	408
网站后门--火狐大类黑客登录肉鸡网站hr	191
网站后门--ASPXSPY v2.0黑客登录肉鸡网站hr	139
网站后门--SpiderPHPShell3.0版黑客登录肉鸡网站hr	113
数据泄漏--账号泄漏5	101

被攻破主机

- 存在3389端口扫描行为
  - 84家单位
  - 335台主机
    - 扫描主机100台以上
  - 505台主机
    - 扫描主机10台以上

僵尸网络主机

- 存在僵尸网络通信协议行为
  - 67家单位
  - 5064台主机

僵尸网络--ZeroAccess	3060
僵尸网络--ZeuS类Bot连接CC服务器	660
僵尸网络-confick1	620
僵尸网络-conficker b	617
僵尸网络--conficker b	163
远程控制--未明远控类20肉鸡上线rc	93
远程控制--白金远控类v4.72/v4.73/4.83肉鸡通信rh	73
远程控制--黑蜘蛛远控2009肉鸡通信rh	72

DDos

- 未发现重大的DDoS事件
  - 大多数为教育网地址被用于伪造攻击后的反射
  - 教育网服务器被利用进行反射攻击的案例不断上升
    - DNS反射
    - NTP反射

校园网安全事件的响应与协作

- 基础设施的建设
- 响应的流程管理建设
- 事件的技术分析与协作

校园网用户的CHAIRS系统使用

- Cooperative Hybrid Aided Incident Response System
- 功能：安全事件的管理与响应
- 为211三期的主干网升级项目开发的配套系统,目前在38个主节点所管理的网络边界部署

CHAIRS系统

- 安全事件来源
  - 网络服务与网络安全态势信息发布系统（NBOS）
    - 主节点网络流量行为监测，接入网DDoS攻击检测，僵尸网络活动监测，etc.
  - 主干网有害行为分析系统
    - 全网恶意服务监测，全网网站入侵监测
  - 分布式蜜罐系统
    - 全网恶意服务监测

事件分类	子类型	来源1	来源2	处理
挂马网站	网站后门	有害代码监测系统		清理服务器
	恶意网页			
内部后门	被攻破主机	NBOS		清理主机或临时封禁
	僵尸网络后门	有害代码监测系统	分布式蜜罐系统	
	僵尸网络控制服务器			
攻击	DDOS	NBOS		洗流
外部恶意代码	潜在威胁			黑名单
	僵尸网络控制服务器器	有害代码监测系统		

CHAIRS系统

- 单位用户功能
  - 信息分享（权利）
    - 邮件通知重要的事件
    - 在线浏览自己所有的事件
    - 在线记录自己响应和处理的过程

应急响应协同服务系统

Cooperative Hybrid Aided Incidence Response System

总案件数	待处理案件数	已处理案件数
96	95	1

内部威胁

分类	涉及单位数	涉及主机数
挂马网站	54	224
内部后门	98	4354

外部威胁

分类	涉及单位数	涉及主机数
攻击	0	0
外部威胁点	338	21938

待处理事件

导出

编号	主题	单位	类型	状态	创建日期	到期日期	
NJ0-2014073612	45.124	大学	僵尸网络主机	待处理	2014-04-04 22:57:05		
NJ0-2014066302	44.166	大学	僵尸网络主机	待处理	2014-04-02 15:07:57		new
NJ0-2014063557	48.59	大学	僵尸网络主机	待处理	2014-04-01 23:46:45		
NJ0-2014062917	32.175	大学	僵尸网络主机	待处理	2014-04-01 18:20:39		new
NJ0-2014050735	2.233	大学	僵尸网络主机	待处理	2014-03-29 13:07:52		new
NJ0-2014049276	41.90	大学	僵尸网络主机	待处理	2014-03-29 00:32:58		new
NJ0-2014044397	44.12	大学	僵尸网络主机	待处理	2014-03-27 12:48:35		new
NJ0-2014043101	45.230	大学	僵尸网络主机	待处理	2014-03-27 01:06:51		new
NJ0-2014028658	112.25	大学	僵尸网络主机	待处理	2014-03-18 06:06:07		new

首页 | 事件报告 | 历史事件检索 | 帮助

编辑案件 · 删除本事件 · 取消处理 · 搜索事件库 · 上报IP信息 · 响应辅助工具

案件 #NJ0-2013431113

负责人:
主题: du.cn
状态: 待处理
分类: 网站后门
首次检测: 2014-03-03 15:03:06 最近活跃:2014-03-03 15:03:06
处理期限: 解决日期:
描述:

响应过程

增加

编号	时间	报告人	报告信息	响应人	响应内容	附件	操作
681571	2014-03-03 15:46:32	MALW-SH-00	du.cn发现Webshell,链接为' du.cn/cps/site/newweb/fckedit or/fckeditor.php,详情见证据2024958401				编辑 删除

相关报告

误报

	分析器	主机地址	主机域名	链接	密码	访问次数	首次检测	最近活跃
	MALW-SH-00	202.119.32.7	du .cn	du.cn/cps/site/newweb/fckeditor/fckeditor.php	网站后门--一句话木马0	1	2014-03-03 15:03:06	2014-03-03 15:03:06

全选 反选 共1条

CHAIRS系统的协作

- 基于CHAIRS系统的安全协作（义务）
  - 每个单位在线响应和处理自己的事件
  - 响应中的技术方案可以在各单位间共享
- 协作的益处
  - 减少本单位的安全隐患，
  - 量化安全工作的考核
  - 提高安全响应的技能

使用的申请

- 由赛尔公司的黄浩负责申请受理
  - 发申请邮件到：huangh@cernet.com
- 提供
  - 联系人：姓名、邮箱、联系电话和初始密码
  - 提供一个IP地址，只有使用该地址才能正常登录
- 在服务正式开放后，会通知用户登录名、确认后的初始密码和URL

使用的申请

- 一个校园网目前只能申请一个CHAIRS账号
- 系统目前正在进行小范围的试用和测试，但开始受理校园网用户的开户申请，预计5月份可以正式提供服务
- CHAIRS目前版本提供的校园网用户服务是完全免费的
- 山东和安徽的实施待与两省网中心协商后决定

校园网用户的NBOS信息共享

CERNET华东北地区网络中心
东南大学 计算机学院
丁伟 wding@njnet.edu.cn
20140418　镇江

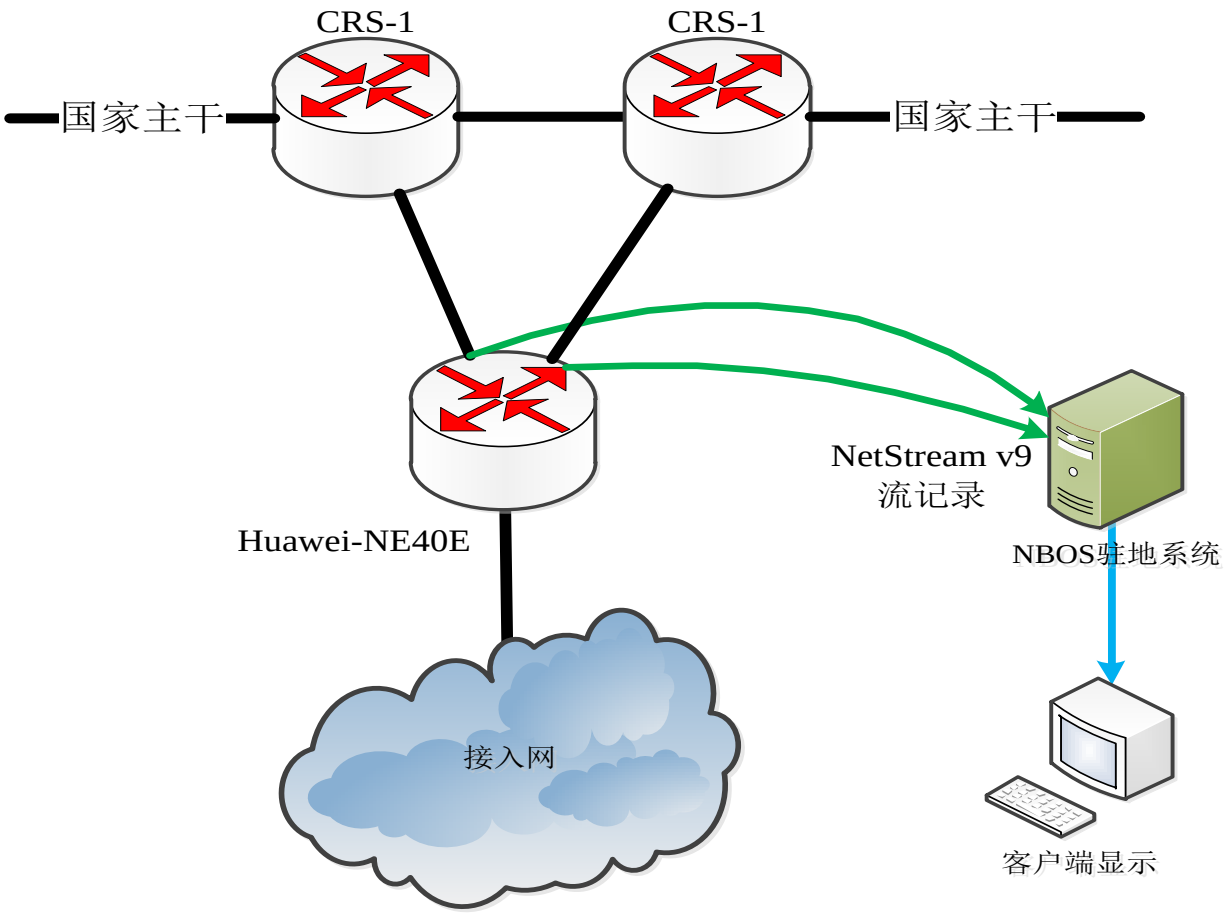
报告内容

- NBOS基本情况介绍
- NBOS对校园网用户的支持方案
- NBOS支持校园网用户的功能介绍
- 如何申请NBOS校园网用户账户
- 其他有关说明

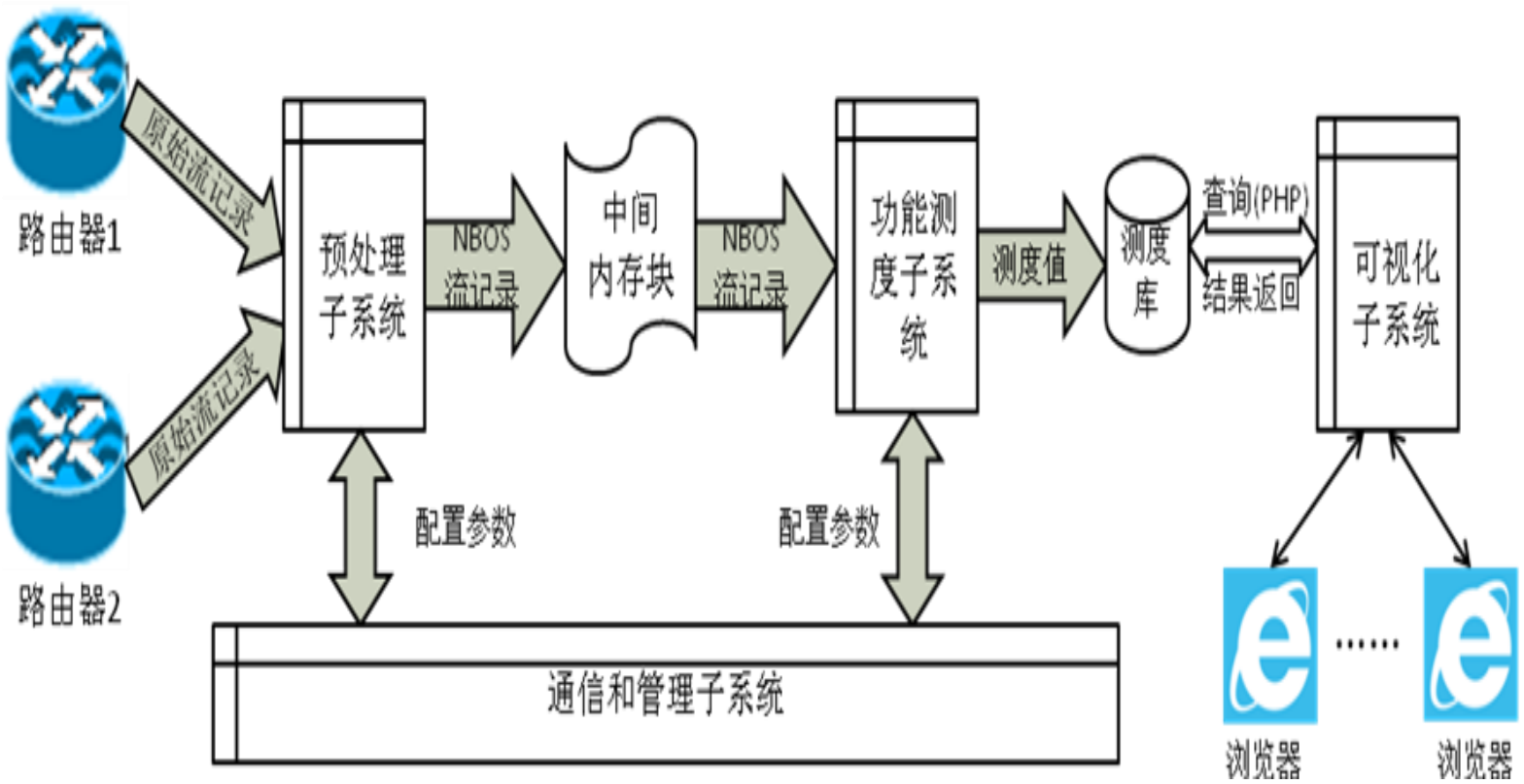
NBOS是什么

- Network Behavior Observation System
- NBOS的原型系统是在国家支撑计划项目支持下完成的以主干网流记录为数据源的网络安全监测系统。
- 目前在38个主节点所管理的网络边界部署的系统是在该原型基础上为211三期的主干网升级项目重新开发的配套系统。
- 目前在CERNET江苏省网边界运行的版本是NBOS-S2.0，以NE40的netstreamV9格式获得分析数据源，采用B/S结构工作

NBOS江苏省网边界拓扑



NBOS的基本工作流程



NBOS(南京)首页局部

网络行为观测系统

Network Behavior Observation System

首页 基本流量行为 服务质量 热点与异常 安全威胁分析 其他 CHAIRS系统 帮助

总出带宽	总入带宽	路由器1出带宽	路由器1入带宽	路由器2出带宽	路由器2入带宽
3,862 Mb/s	8,332 Mb/s	3,862 Mb/s	8,332 Mb/s	0 Mb/s	0 Mb/s

流量热点TOP5 More...

网内源流量热点 网内宿流量热点 网外源流量热点 网外宿流量热点

IP	归属	流量(Mb/s)	流量TOP1端口及其占用百分比	流量TOP2端口及其占用百分比
222.192.186.40	淘宝(中国)软件有...	469.46	80 | 100%	--
222.192.186.50	淘宝(中国)软件有...	447.41	80 | 100%	--
121.248.104.162	中国矿业大学	265.8	80 | 100%	--
222.192.185.9	江苏云港网络科...	204.98	80 | 99.49%	50939 | 0.08%
222.192.185.7	江苏云港网络科...	117.67	80 | 98.64%	8080 | 0.4%

访问热点TOP5 More...

网内源访问热点 网内宿访问热点 网外源访问热点 网外宿访问热点

IP	归属	关联IP数
222.192.186.40	淘宝(中国)软件有限公司（南京）	7566
222.192.184.14	江苏云港网络科技公司	7445
222.192.186.50	淘宝(中国)软件有限公司（南京）	7419
211.65.214.19	南京师范大学	6134
211.65.214.14	南京师范大学	5617

活跃连接TOP5 More...

源前缀	宿前缀	源端口	宿端口	协议	流量（Kb/s）
中国矿业大学 121.248.104.162	联通 221.205.190.217	80	58239	6	31,301

带宽占用

被管单位	出/入带宽(Mb/s)
江苏云港网络科...	839/882
东南大学	611/1,097
南京大学	226/781
南京图书馆	235/707
非正常地址	1/917
中国矿业大学	459/306
南京师范大学	89/526
淘宝(中国)软件...	4/342
扬州大学	41/303
南京林业大学	113/194

应用分布

应用名	流量比例(%)
WWW	69.46
P2P	25.69
系统端口	1.41
邮件	< 0.01
多媒体	< 0.01
FTP	2.74
交互	< 0.01
语音	< 0.01
其它	< 0.01

最近DDoS攻击检测 More...

SYN Flood TCP/UDP Flood DNS Flood

被攻击服务器	归属	类型	起始时间	终止时间
173.255.133.245	美国	1	2013-12-02 13:25:00	未终止
202.102.85.75	电信	1	2013-12-01 22:22:26	未终止
113.105.175.199	电信	51	2013-12-02 13:37:56	2013-12-02 13:42:52
192.126.127.103	澳大利亚	51	2013-12-02 11:58:28	2013-12-02 13:42:52
192.126.127.102	澳大利亚	51	2013-12-02 11:58:28	2013-12-02 13:42:52
222.192.186.40	淘宝(中国)软件...	6	2013-12-02 12:20:00	2013-12-02 13:34:58

让校园网用户共享NBOS中的数据

- 目的和方案
  - 通过为可视化子系统增加一组定制的网页，使得校园网用户可以访问NBOS测度库中的指定数据
- 安全和隐私保护
  - 在IP层和用户层增加相应的访问控制，授权校园网用户只能用特定的地址访问NBOS测度库中与各自校园网有关的测度数据

NBOS支持的校园网用户功能

首页局部（东南大学用户）

首页　基本流量行为　热点检测　安全威胁分析　其他　CHAIRS系统　帮助

最近48小时流量热点TOP5 More...

网内源流量热点　网内宿流量热点

IP及其归属	流量(Mb/s)	流量TOP1端口及其占用百分比	流量TOP2端口及其占用百分比	发生时间
58.192. 东南大学	15117.32	38108 | 100%	--	2014-04-16 08:50:00
58.192.1 东南大学	15094.98	38108 | 100%	3033 | 0%	2014-04-16 09:50:00
58.192.1 东南大学	14990.82	11088 | 100%	--	2014-04-16 07:10:00
58.192.1 东南大学	14818.98	11088 | 100%	--	2014-04-16 06:40:00
58.192 东南大学	14773.49	38108 | 100%	--	2014-04-16 09:20:00

最近48小时访问热点TOP5 More...

网内源访问热点　网内宿访问热点

IP及其归属	关联IP数	发生时间
202.119. 东南大学	18194	2014-04-15 11:40:00
202.119. 东南大学	18135	2014-04-15 11:45:00
202.119. 东南大学	18115	2014-04-15 11:55:00
202.119.2 东南大学	18013	2014-04-15 11:50:00
202.119. 东南大学	17999	2014-04-15 11:25:00

最近48小时活跃连接TOP5 More...

源前缀	宿前缀	源端口	宿端口	协议	首次检出时间	最新检出时间
美国 173.231.8.210	东南大学 223.3.	--	--	47	2014-04-07 06:00:00	2014-04-16 08:35:00
电信 113.98.233.193	东南大学 223.3.	15305	6003	17	2014-04-12 06:20:00	2014-04-16 09:15:00
东南大学 223.3.	清华大学 59.66.4.50	--	--	41	2014-04-14 00:20:00	2014-04-15 15:55:00
东南大学 121.248.	西北工业大学 202.117.81.40	19589	41106	17	2014-04-15 00:05:00	2014-04-16 00:00:00
东南大学 202.119.2	韩国 211.230.61.32	8513	29671	6	2014-04-14 17:20:00	2014-04-15 04:05:00

最近DDoS攻击检测 More...

被攻击服务器	归属	类型	起始时间	终止时间
202.119.	东南大学	22	2013-12-29 17:50:00	2013-12-29 20:24:59
202.119.	东南大学	21	2013-12-29 18:05:00	2013-12-29 19:34:59
202.119.	东南大学	22	2013-12-29 15:15:00	2013-12-29 15:19:59
202.119.	东南大学	22	2013-12-15 12:55:00	2013-12-15 13:09:59
202.119.	东南大学	21	2013-11-11 17:20:00	2013-11-11 19:39:59

首页局部

最近48小时活跃地址对TOP5 More...

源前缀	宿前缀	字节数	报文数	源端口数	宿端口数
东南大学 58.192.[illegible]	美国 97.95.88.161/32	159,809,534,976	149,915,136	1	1
东南大学 58.192.1[illegible]	美国 69.31.20.78/32	54,155,392,512	50,802,432	1	1
东南大学 58.192.[illegible]	美国 76.29.6.248/32	33,992,744,448	31,888,128	1	1
东南大学 58.192.[illegible]	美国 74.69.219.241/32	32,611,344,896	30,592,256	1	1
东南大学 58.192.[illegible]	美国 98.210.8.42/32	32,323,712,512	30,322,432	1	1

当前周 东南大学安全状态 More...

活动主机IP	威胁源IP及其归属	威胁源类型	最近活动时间
223.3.60.184	61.240.136.66 联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 15:54:49
223.3.57.131	61.240.136.66 联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 15:51:45
223.3.21.51	61.240.136.66 联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 15:51:23
202.119.25.226	61.240.136.66 联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 15:51:17
202.119.25.69	61.240.136.66 联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 15:51:02

疑似非授权流量

事件类型	当前数量	事件类型	当前数量	事件类型	当前数量	事件类型	当前数量	事件类型	当前数量	事件类型	当前数量	事件类型	当前数量
2002	2	3389	2	445	0	445A	0	135	0	135A	0	4002	0

Flow Time From: 2014-04-14 15:50 To 2014-04-14 15:55

最后刷新时间：2014/04/14 15:58（服务器时间）

其他功能(从导航条进入)-活跃地址对：按周统计的IP间大流量情况

2014/04/07-2014/04/13聚合分析

活跃源前缀 活跃宿前缀 活跃连接 **活跃IP地址前缀对**

活跃IP地址前缀对

序号	源前缀	源前缀归属	宿前缀	宿前缀归属	最大流量（Kb/s）	平均流量（Kb/s）	出现时间比
1	173.231.8.210/32	美国	223.3.54.[illegible]	东南大学	203,654	100,208.38	0.6%
2	113.98.233.193/32	电信	223.3.[illegible]	东南大学	161,312	48,940.06	0.4%
3	58.192.1[illegible]	东南大学	37.187.26.152/32	欧盟	3,051,730	2,176,844.58	0.35%
4	202.119.[illegible]	东南大学	116.233.160.108/32	电信	122,029	120,970.35	0.25%
5	202.117.4.246/32	西安交通大学	202.119.[illegible]	东南大学	67,213	59,514.56	0.2%
6	202.117.4.247/32	西安交通大学	202.119.[illegible]	东南大学	108,623	70,752.29	0.15%
7	211.65.[illegible]	东南大学	119.75.220.51/32	中国	38,865	36,217.58	0.15%
8	202.119.[illegible]	东南大学	211.69.161.101/32	中南财经政法大学	98,995	88,912.95	0.15%
9	202.119.[illegible]	东南大学	218.199.207.114/32	华中师范大学	114,607	84,610.15	0.15%
10	122.143.1.0/26	联通	121.248.[illegible]	东南大学	54,279	48,152.41	0.15%
11	58.192.[illegible]	东南大学	66.96.147.103/32	美国	293,334	253,338.45	0.1%
12	202.119.[illegible]	东南大学	123.126.88.100/32	联通	71,860	71,363.14	0.1%
13	202.119.[illegible]	东南大学	223.19.65.70/32	中国香港	54,165	48,672.46	0.1%
14	123.225.2.202/32	日本	202.119.[illegible]	东南大学	63,247	49,721.97	0.1%
15	202.119.[illegible]	东南大学	211.223.68.57/32	韩国	54,551	50,826.19	0.1%
16	202.119.[illegible]	东南大学	14.198.93.193/32	中国香港	52,375	51,167.16	0.1%
17	211.65.[illegible]	东南大学	119.75.220.51/32	中国	36,698	34,882.75	0.1%
18	58.192.[illegible]	东南大学	108.61.238.203/32	美国	848,059	834,727.75	0.1%

校园网主机与黑名单交互情况

最近威胁活动

序号	感染IP	感染IP归属	威胁源IP	威胁源IP归属	威胁类型	首次检出时间	最后检出时间
1	223.3.[redacted]	东南大学	61.240.136.66	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:15	2014-04-14 16:15
2	121.248.[redacted]	东南大学	61.240.136.66	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:15	2014-04-14 16:15
3	223.3.[redacted]	东南大学	61.240.136.66	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:15	2014-04-14 16:15
4	223.3.[redacted]	东南大学	61.135.217.6	联通	僵尸网络--confick2	2014-04-14 16:10	2014-04-14 16:10
5	223.3	东南大学	61.240.136.66	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:10	2014-04-14 16:10
6	223.3.[redacted]	东南大学	61.240.136.66	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:05	2014-04-14 16:05
7	223.3.[redacted]	东南大学	1.25.36.76	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:05	2014-04-14 16:05
8	223.3.[redacted]	东南大学	61.240.136.66	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:05	2014-04-14 16:05
9	121.249.[redacted]	东南大学	221.130.179.36	移动	灰鸽子远控类肉鸡上线rh	2014-04-14 16:05	2014-04-14 16:05
10	121.249.[redacted]	东南大学	221.130.179.36	移动	灰鸽子远控类肉鸡上线rh	2014-04-14 16:00	2014-04-14 16:00
11	223.3.[redacted]	东南大学	61.240.136.66	联通	僵尸网络--ZeuS类Bot连接C&am	2014-04-14 16:00	2014-04-14 16:00
12	121.24[redacted]	东南大学	221.130.179.36	移动	灰鸽子远控类肉鸡上线rh	2014-04-14 16:00	2014-04-14 16:00
13	223.3.[redacted]	东南大学	202.106.182.22	联通	远程控制--灰鸽子远控类肉鸡上线rh	2014-04-14 16:00	2014-04-14 16:00

校园网服务器被DDOS攻击情况

2014年内被攻击服务器为202.195.[redacted]的记录

序号	被攻击服务器	归属	类型	起始时间	结束时间	pps	最大pps	Kbps	最大Kbps	平均IP数	最大IP数
1	202.195.[redacted]	南京中医药大学	21	2014-03-21 16:31:39	2014-03-21 16:49:02	1,291,243	1,779,143	2,181,472	3,077,960	26,164	36,254
2	202.195.[redacted]	南京中医药大学	21	2014-03-21 11:27:12	2014-03-21 12:00:44	352,733	623,287	2,011,622	3,159,321	22,516	40,889
3	202.195.[redacted]	南京中医药大学	21	2014-03-19 13:05:38	2014-03-19 13:23:32	476,873	480,826	1,886,373	1,893,616	618	620
4	202.195.[redacted]	南京中医药大学	21	2014-03-15 11:10:39	2014-03-16 17:56:46	10,528	52,532	27,490	316,078	2,268	25,796
5	202.195.[redacted]	南京中医药大学	21	2014-03-14 14:54:18	2014-03-15 01:14:49	9,563	14,171	4,314	6,421	216	287
6	202.195.[redacted]	南京中医药大学	21	[redacted]47:46	2014-03-13 21:59:59	163,474	244,858	1,151,983	1,725,489	140,386	212,428
7	202.195.[redacted]	南京中医药大学	21	[redacted]45:44	2014-03-13 19:56:12	176,948	238,862	1,246,936	1,683,234	139,030	208,662
8	202.195.[redacted]	南京中医药大学	21	2014-03-13 17:41:31	2014-03-13 17:51:37	187,705	237,509	1,322,736	1,673,691	141,132	209,991
9	202.195.[redacted]	南京中医药大学	21	2014-03-13 15:37:19	2014-03-13 15:47:47	147,131	165,079	1,036,816	1,163,286	69,709	102,614
10	202.195.[redacted]	南京中医药大学	21	2014-03-12 12:06:20	2014-03-12 18:45:13	5,975	12,510	2,697	5,668	213	263
11	202.195.[redacted]	南京中医药大学	6	2014-03-12 18:35:00	2014-03-12 18:44:59	1,981	2,467	928	1,156	178	191

类型意义

类型=21：SYN flood攻击，被攻击服务器在被管网内，攻击源在网外

校园网服务器参与DDOS攻击情况

- 这些地址曾经出现在某个具体的被NBOS检测到的参与DDOS攻击的地址中，但存在被假冒的可能
- 表中表项依次为：序号、地址、攻击类型、检出次数、首次检出时间和末次检出时间

15	202. .59	1	1	2014-04-13 13:25:01	2014-04-13 14:19:59
16	202. 241	11	7	2014-02-03 04:15:00	2014-04-12 15:17:40
17	202. .77	11	12	2014-01-19 16:25:00	2014-04-12 15:17:40
18	202. 57	11	5	2014-02-17 17:43:40	2014-04-12 15:17:38

到境外主机的大流量事件：58.192.114.8

- 这是东南大学的BBS服务器
- 数据有效期内有过2次到境外大流量事件
- 2次事件详情在下页，初步判断事件原因是非洲和美国的爬虫程序在获取网页数据。

IP:58.192.114.8未授权事件2002的近期情况表

* 2002事件是被管网内主机向境外主机发送流量超过阈值的事件 * 点击事件编号获取对端详情
* 点击详情获取按时间粒度的统计数据 * 点击IP获取该地址所有事件
* 点击归属获取该单位近期所有2002事件 所有相关单位

查询事件主机: 58.192.114.8 确定

序号	事件编号	事件主机	归属	最大并发对端IP数	总流量(MB)	起始时间粒度	终止时间粒度
1	2002-0x533f431a	58.192.114.8	东南大学	9	54.11	2014-04-12 03:35:00	2014-04-12 03:35:00
2	2002-0x533eee05	58.192.114.8	东南大学	9	54.25	2014-04-10 09:25:00	2014-04-10 09:25:00

IP:58.192.114.8（东南大学）的对端情况

* NBOS在每个时间粒度只记录一定数量的对端IP信息，因此本页的对端IP总数可能与上页的“最大并发对端IP数”不一致

序号	对端IP	归属	是否种子	出方向		入方向		首次活跃时间粒度	末次活跃时间粒度	活跃时间粒度数	协议占用比	最大并发绑定端口	最大并发对端端口数
				总字节数(MB)	总报文数	总字节数(MB)	总报文数						
1	196.203.83.3	突尼斯	是	44.99	36096	1.69	21760	2014-04-12 03:35:00	2014-04-12 03:35:00	1	查看	1	38
2	173.0.48.133	美国	否	3.70	2560	0.03	512	2014-04-12 03:35:00	2014-04-12 03:35:00	1	查看	1	1
3	184.154.208.21	美国	否	2.22	1536	0.07	1024	2014-04-12 03:35:00	2014-04-12 03:35:00	1	查看	1	1
4	75.154.237.11	加拿大	否	1.18	1024	0.03	512	2014-04-12 03:35:00	2014-04-12 03:35:00	1	查看	1	3
5	178.32.54.240	英国	否	0.74	512	0.013	256	2014-04-12 03:35:00	2014-04-12 03:35:00	1	查看	1	1

IP:58.192.114.8（东南大学）的对端情况

* NBOS在每个时间粒度只记录一定数量的对端IP信息，因此本页的对端IP总数可能与上页的“最大并发对端IP数”不一致

序号	对端IP	归属	是否种子	出方向		入方向		首次活跃时间粒度	末次活跃时间粒度	活跃时间粒度数	协议占用比	最大并发绑定端口	最大并发对端端口数
				总字节数(MB)	总报文数	总字节数(MB)	总报文数						
1	76.164.234.178	美国	是	45.11	31488	0.52	9984	2014-04-10 09:25:00	2014-04-10 09:25:00	1	查看	1	12
2	192.3.60.237	澳大利亚	否	4.44	3072	0.06	1024	2014-04-10 09:25:00	2014-04-10 09:25:00	1	查看	1	1
3	208.115.111.70	美国	否	1.48	1024	0	0	2014-04-10 09:25:00	2014-04-10 09:25:00	1	查看	1	1
4	5.135.58.153	法国	否	1.11	768	0.03	512	2014-04-10 09:25:00	2014-04-10 09:25:00	1	查看	1	2
5	198.204.225.90	美国	否	0.74	512	0.013	256	2014-04-10 09:25:00	2014-04-10 09:25:00	1	查看	1	2

到境外主机的大流量事件：*.*.112.111

IP:[redacted].112.111未授权事件2002的近期情况表

* 2002事件是被管网内主机向境外主机发送流量超过阀值的事件 * 点击事件编号获取对端详情
* 点击详情获取按时间粒度的统计数据 * 点击IP获取该地址所有事件
* 点击归属获取该单位近期所有2002事件 所有相关单位

查询事件主机: [redacted] 确定

序号	事件编号	事件主机	归属	最大并发对端IP数	总流量(MB)	起始时间粒度	终止时间粒度
1	2002-0x5340126b	[redacted].112.111	[redacted]	3	132692.22	2014-04-15 09:25:00	2014-04-15 09:25:00
2	2002-0x533f9b45	[redacted].112.111	[redacted]	3	15120.58	2014-04-13 09:55:00	2014-04-13 09:55:00
3	2002-0x533f99df	[redacted].112.111	[redacted]	3	30431.75	2014-04-13 09:25:00	2014-04-13 09:25:00
4	2002-0x533f9700	[redacted].112.111	[redacted]	3	31337.33	2014-04-13 08:25:00	2014-04-13 08:25:00
5	2002-0x533f957e	[redacted].112.111		3	32435.85	2014-04-13 07:45:00	2014-04-13 07:45:00

共5条记录，每页显示50条，当前第1/1页 [首页] [上一页] [1][下一页] [尾页]

到境外主机的大流量事件：*.*.112.111

- 下图上页列表中第一事件的详情
- 所有流量均为单边的UDP:80，符合UDPflood特征
- 后面2页是另外4个事件的详情，大流量主机特征完全相同，但均同时用TCP交互澳大利亚主机192.151.154.154，可能为控制器

IP:[redacted].112.111（[redacted]）的对端情况

* NBOS在每个时间粒度只记录一定数量的对端IP信息，因此本页的对端IP总数可能与上页的“最大并发对端IP数”不一致

序号	对端IP	归属	是否种子	出方向		入方向		首次活跃时间粒度	末次活跃时间粒度	活跃时间粒度数	协议占用比	最大并发绑定端口	最大并发对端端口数
				总字节数(MB)	总报文数	总字节数(MB)	总报文数						
1	192.99.45.57	澳大利亚	是	93402.05	72980224	0	0	2014-04-15 09:25:00	2014-04-15 09:25:00	1	查看	1	1
2	98.193.51.77	美国	是	19651.72	15359744	0	0	2014-04-15 09:25:00	2014-04-15 09:25:00	1	查看	1	1
3	24.61.89.191	美国	是	19625.18	15339520	0	0	2014-04-15 09:25:00	2014-04-15 09:25:00	1	查看	1	1

共3条记录，每页显示50条，当前第1/1页 [首页] [上一页] [1][下一页] [尾页]

IP:[redacted].112.111（[redacted]）的对端情况

* NBOS在每个时间粒度只记录一定数量的对端IP信息，因此本页的对端IP总数可能与上页的“最大并发对端IP数”不一致

序号	对端IP	归属	是否种子	出方向		入方向		首次活跃时间粒度	末次活跃时间粒度	活跃时间粒度数	协议占用比	最大并发绑定端口	最大并发对端端口数
				总字节数(MB)	总报文数	总字节数(MB)	总报文数						
1	50.136.214.239	美国	是	15114.53	14873088	0	0	2014-04-13 09:55:00	2014-04-13 09:55:00	1	查看	1	1
2	192.3.52.6	澳大利亚	否	0.18	1536	0.05	768	2014-04-13 09:55:00	2014-04-13 09:55:00	1	查看	6	1
3	192.151.154.154	澳大利亚	否	0.17	2304	0.29	1792	2014-04-13 09:55:00	2014-04-13 09:55:00	1	查看	9	1

IP:[redacted].112.111（[redacted]）的对端情况

* NBOS在每个时间粒度只记录一定数量的对端IP信息，因此本页的对端IP总数可能与上页的“最大并发对端IP数”不一致

序号	对端IP	归属	是否种子	出方向		入方向		首次活跃时间粒度	末次活跃时间粒度	活跃时间粒度数	协议占用比	最大并发绑定端口	最大并发对端端口数
				总字节数(MB)	总报文数	总字节数(MB)	总报文数						
1	68.96.185.119	美国	是	15547.58	15295488	0	0	2014-04-13 09:25:00	2014-04-13 09:25:00	1	查看	1	1
2	71.80.128.32	美国	是	14878.08	14638592	0	0	2014-04-13 09:25:00	2014-04-13 09:25:00	1	查看	1	1
3	192.151.154.154	澳大利亚	否	0.26	3584	0.37	3072	2014-04-13 09:25:00	2014-04-13 09:25:00	1	查看	13	1

IP: .112.111 ( ) 的对端情况

* NBOS在每个时间粒度只记录一定数量的对端IP信息，因此本页的对端IP总数可能与上页的“最大并发对端IP数”不一致

序号	对端IP	归属	是否种子	出方向		入方向		首次活跃时间粒度	末次活跃时间粒度	活跃时间粒度数	协议占用比	最大并发绑定端口	最大并发对端端口数
				总字节数(MB)	总报文数	总字节数(MB)	总报文数						
1	71.201.103.211	美国	是	16094.85	15833856	0	0	2014-04-13 08:25:00	2014-04-13 08:25:00	1	查看	1	1
2	202.128.94.74	关岛	是	15236.21	14991104	0	0	2014-04-13 08:25:00	2014-04-13 08:25:00	1	查看	1	1
3	192.151.154.154	澳大利亚	否	0.15	2304	0.29	3072	2014-04-13 08:25:00	2014-04-13 08:25:00	1	查看	9	1

IP: .112.111 ( ) 的对端情况

* NBOS在每个时间粒度只记录一定数量的对端IP信息，因此本页的对端IP总数可能与上页的“最大并发对端IP数”不一致

序号	对端IP	归属	是否种子	出方向		入方向		首次活跃时间粒度	末次活跃时间粒度	活跃时间粒度数	协议占用比	最大并发绑定端口	最大并发对端端口数
				总字节数(MB)	总报文数	总字节数(MB)	总报文数						
1	72.216.23.239	美国	是	16227.66	15962880	0	0	2014-04-13 07:45:00	2014-04-13 07:45:00	1	查看	1	1
2	70.196.130.5	美国	是	16204.95	15942656	0	0	2014-04-13 07:45:00	2014-04-13 07:45:00	1	查看	1	1
3	192.151.154.154	澳大利亚	否	0.15	2048	0.14	2048	2014-04-13 07:45:00	2014-04-13 07:45:00	1	查看	8	1

..112.111首页


网络
NETWORKS
网络接入认证系统
加入收藏 | 帮助 | 语言: 简体中文
网络认证登录
用户名
internet
密码
登录IP: 211.65.192.17
当前位置: 403房间
登录
网络沟通你我 科技改变生活
版权所有 © 2014 南京 . 息技术有限公司

如何申请NBOS的校园网账户

- 由JSERNET的NOC负责受理
  - 发申请邮件到：nbos-js@njnet.edu.cn
- 提交申请时需同时提供
  - 联系人：姓名、邮箱、联系电话和初始密码
  - 一个不超过/28的IP地址段：只有使用这段地址才能正常登录
- JSERNET NOC受理后会通知用户登录名、确认后的初始密码和URL

其他

- 一个校园网目前只能申请一个NBOS账号
- 系统目前正在进行最后的测试，但开始受理校园网用户的开户申请，预计5月初可以正式提供服务
- NBOS目前版本提供的校园网用户服务是完全免费的
- 项目组可能会要求校园网协助分析个别地址的流量行为，请所有开户单位给予支持
- 山东和安徽的实施待与两省网中心协商后决定

其他使用中的问题

- 没有数据：NBOS只记录全网范围内排名靠前的大流量事件，流量较小的校园网可能出现没有数据的情况
- 分析数据覆盖范围：只提供校园网经CERNET出口与JSERNET以外交互流量中出现的情况。无法观测其他运行商和JSERNET内的流量情况。
- 时间粒度：NBOS的时间粒度是5分钟，这是NBOS定位事件的最小时间单位

NBOS与Chairs

- NBOS是一个IP级的网管系统，提供全网综合网管数据，chairs是一个安全事件报告系统，报告网络中具体的安全事件
- NBOS具有一定的发现流量行为异常主机的能力
- NBOS对确定的安全事件报告chairs
- 除NBOS外，chairs还有其他的分析数据来源

END

Thanks&Questions