

CERNET网络安全服务

中国教育和科研计算机网紧急响应组(CCERT)
清华大学信息网络工程研究中心
2002年10月，南京

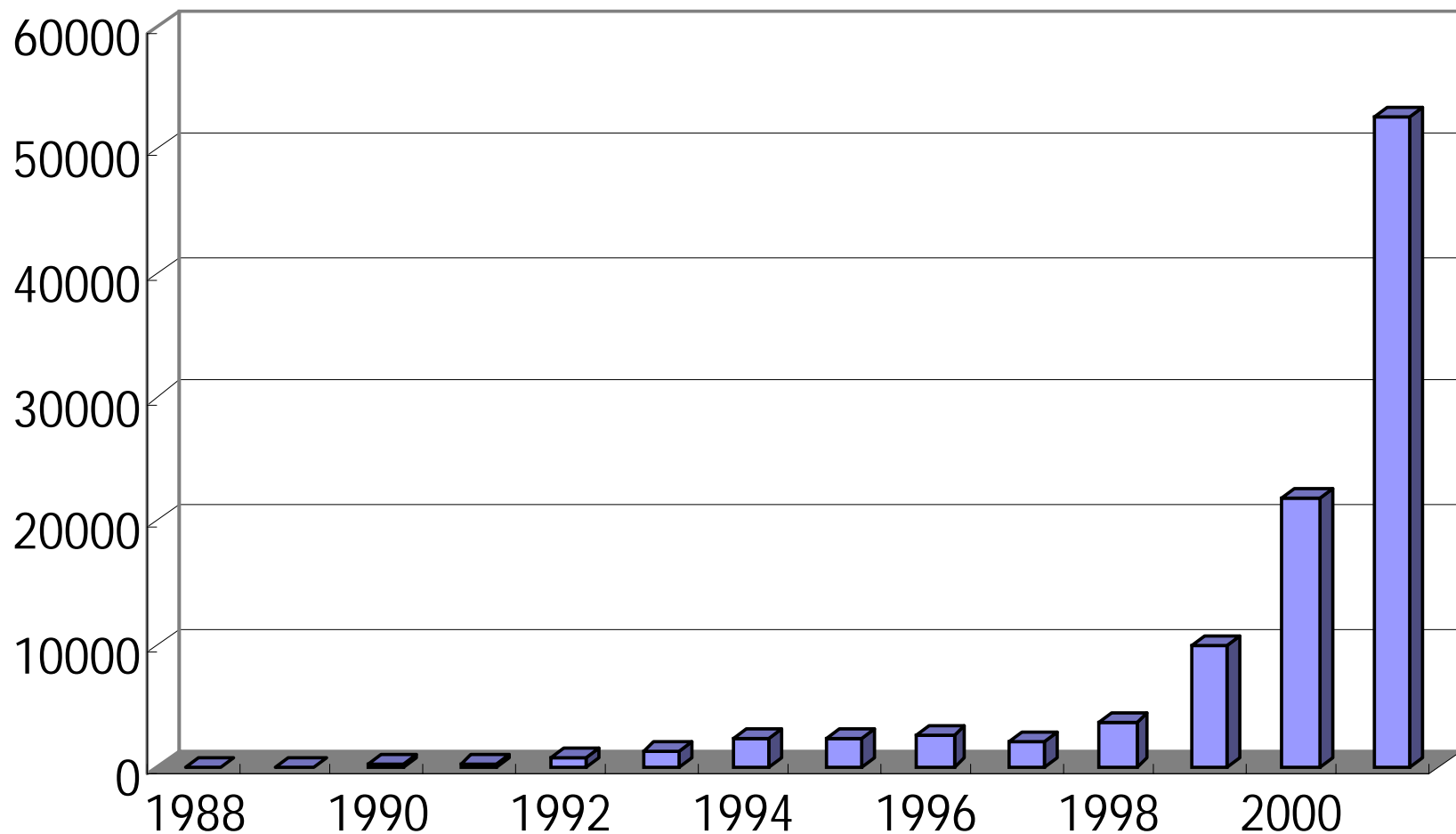
▶ 校园网安全服务需求

- CERNET安全服务
- 近期影响严重的安全事件
- 校园网常见安全问题

- 网络安全事件的增长趋势
- 网络安全的普遍威胁
- 校园网安全自身的脆弱性
- 校园网安全面临的主要威胁
- 网络安全服务的主要内容

计算机网络安全事件的增长趋势

CERT/CC incident Report



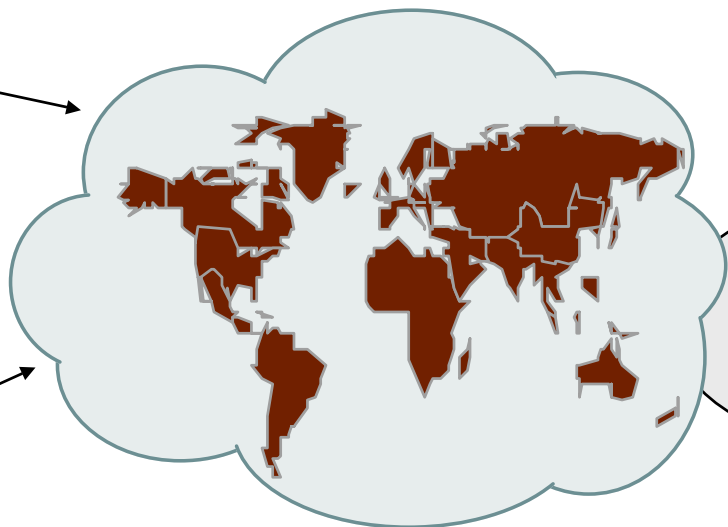
计算机网络安全普遍威胁

- 系统和网络自身的脆弱性
- 网络的开放性
- 威胁存在的普遍性
- 政策、管理方面的漏洞



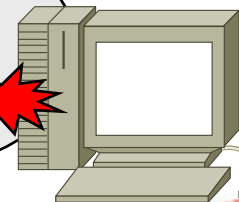
Worm

Virus



内部攻击

内部网



- 管理问题

- 缺乏接受的使用政策（AUP），规范用户的行为
- 缺乏专门的管理机构、管理岗位，明确的职责，大量开放的计算机系统无人管理
- 管理规范和管理制度，比如上岗培训制度

- 技术问题

- 过多的单一故障点：网络、DNS, Web, Email
- 软件缺省安装：不打补丁，系统帐号、缺省口令
- 大量开放的服务：Email, FTP
- 缺少数据备份
- 网络和系统管理员的技术水平

- 网络拒绝服务
 - 故障：设备、系统自身的损坏、人为的操作失误
 - 攻击：操作系统、应用系统；网络设备、链路带宽
- 恶意代码
 - 蠕虫，病毒、特洛伊木马、恶意脚本等
 - SirCam , Code Red, Nimda, Klez, Slapper
- 系统入侵
 - 篡改主页，破坏数据，远程控制
- 不良信息扩散
 - 威胁国家和社会稳定
 - 影响学校的声誉

- 校园网安全服务需求

- ▶ • CERNET安全服务

- 近期影响严重的安全事件

- 校园网常见安全问题

- CCERT简介
- CCERT的主要工作
 - 安全事件的协调与处理与技术支持
 - CERNET网络安全监控
 - 系统漏洞、安全公告
 - 安全技术培训

什么是CERT 组织

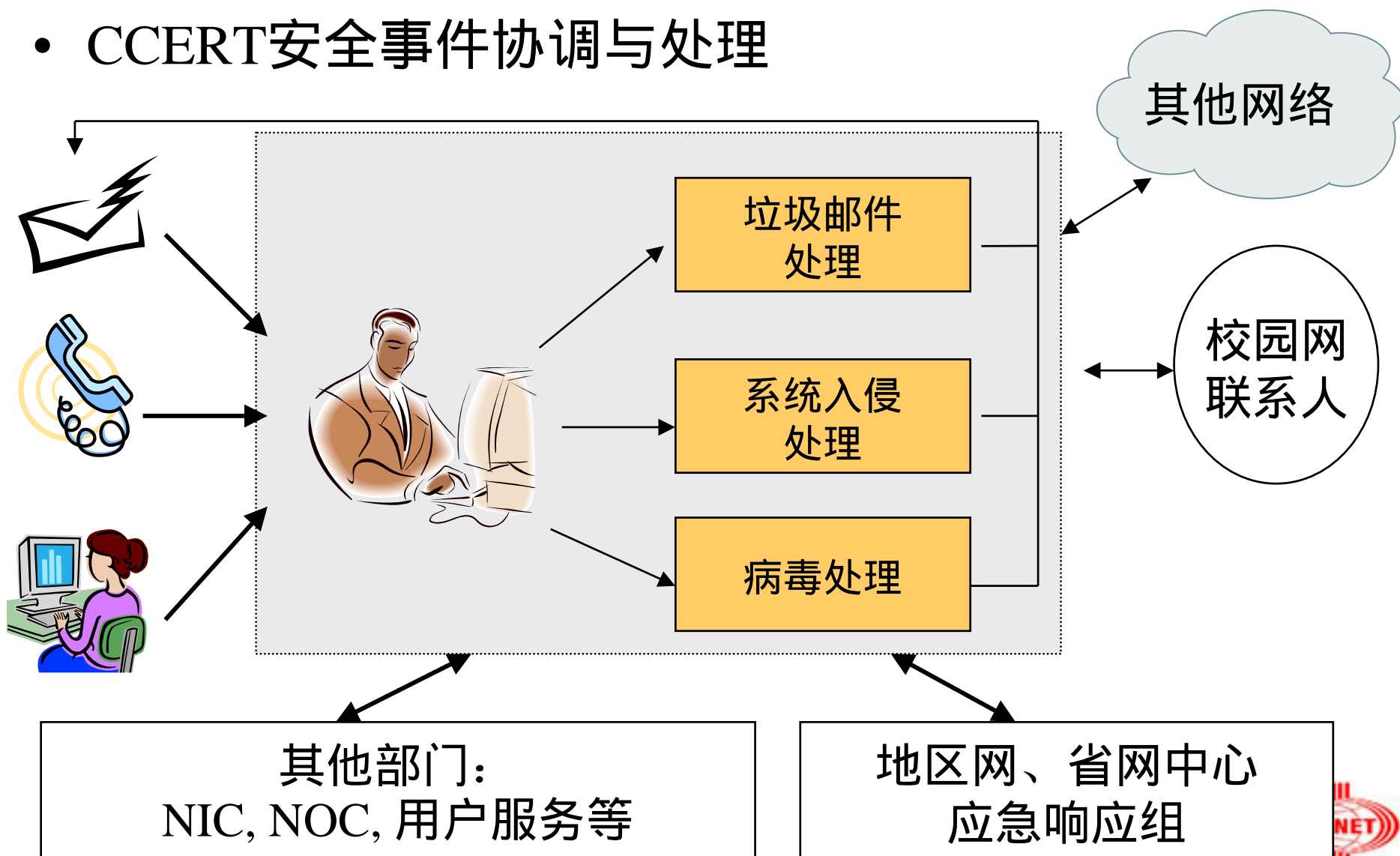
- CERT 是 Computer Emergency Response Team 的簡稱，其目的在處理電腦危機以及電腦安全相關的課題
- 最早于1988年莫里斯蠕虫事件后成立于卡耐基.梅隆大学。
- CERT组织的规范-----RFC2412
- CCERT成立于 1999年5月，从成立之日起接受事件投诉

- 中国教育和科研计算机网紧急响应组CCERT
- 主要服务对象
 - CERNET内部的会员单位
 - 向社会其他行业开放，提供公益性的安全服务
- 主要的服务提供者
 - 各级网络运行管理中心和应急响应组
 - 赛尔网络

- 1999年5月，CCERT正式成立
- 1999年10月，NJCERT成立
- 2000年6月，参加12th FIRST年会，发表第一篇介绍中国应急响应的论文，李星教授当选FIRST第13、14届程序主席
- 2000年5月，CERNET关于制止端口扫描的通告
- 2001年8月，Code Red II 事件响应
- 2001年9月，CERNET第一次全国CERT应急响应工作会议
- 2002年3月，CCERT反垃圾邮件倡议受媒体关注
- 2002年3月，亚太地区应急响应组联盟(APSIRC)
- 2002年5月，CERNET关于制止垃圾邮件的管理规定
- 2002年5月，CERNET第二次应急响应工作会议
- 2002年10月，CERNET南京年会正式确定安全服务

- 网络安全事件协调处理
- 网络安全漏洞与安全事件公告
- 网络安全管理和技术咨询与培训

- CCERT安全事件协调与处理



- 联系方式

- CCERT国家中心 <http://www.ccert.edu.cn>
邮件: report@ccert.edu.cn ,
电话: 010-62784301, 传真: 010-62785933
- NJCERT: <http://www.njnet.edu.cn/njcert/>华东北
邮件: njcert@njnet.edu.cn,
电话: (025)3614718 传真: (025)3614842
- PKU-CERT : <http://pkucert.pku.edu.cn>华北
- GZCERT : <http://http://www.gznet.edu.cn/gzcert>华南
- CDCERT : <http://www.cdnet.edu.cn/cdcert>西南
- BUPTCERT: <http://buptcert.buptnet.edu.cn>北邮
- SDCERT :<http://sdcert.sd.edu.cn>山东大学

CCERT 什么样的事件向CCERT报告？

以下一些事件您可以向CCERT报告

- 您的系统遭受了移动恶意代码的感染。
- 您的系统遭受了黑客的入侵。
- 您的系统正在转发垃圾邮件。
- 您的系统正在遭受DOS攻击。

如果您发现您的系统有以上几种情况，请及时向我们报告 我们会及时对您的要求做出响应



怎样报告事件？（一）

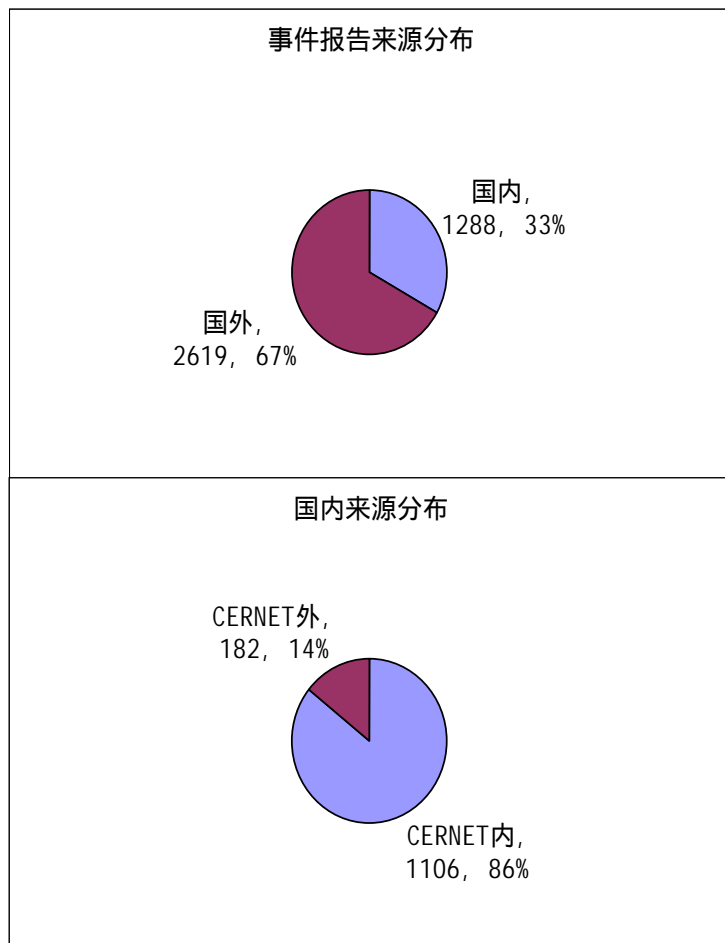
- 在您发现您的主机正在受到不法侵害的时候 越早向CCERT报告，您的损失就会将制越小 如何向CCERT报告呢？
- 我们建议您先将简要信息通过电话报告给我们 我们将会指导您采取一些措施，将损失减小 然后通过电子邮件将详细情况发给我们

怎样报告事件？（二）

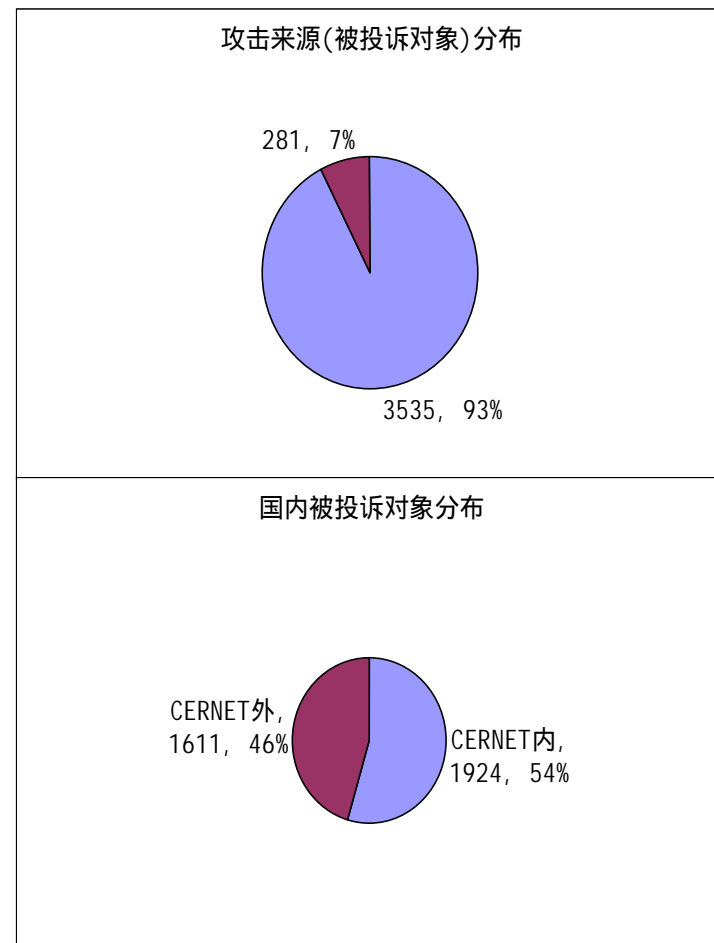
- 请记住，以下这几点很重要，这关系到您的系统的事件处理的准确性
- 请在邮件中包含以下要素：
 - **联系人信息**: 单位, 联系人, EMAIL, 电话
 - **事件简要说明**: IP地址, 域名, 操作系统版本, 应用系统版本, 事发时间, 事件的说明
 - **可供分析的证据**: 系统日志, 攻击者所留的痕迹（包括所留的软件和被修改的文件）

•CCERT 2002年安全事件统计

事件报告来源分布

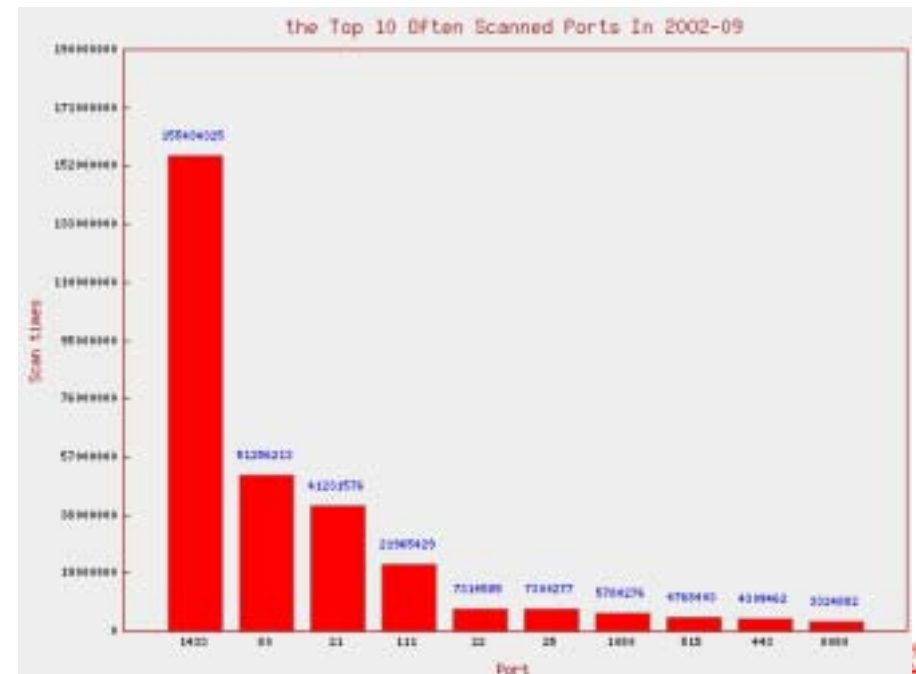
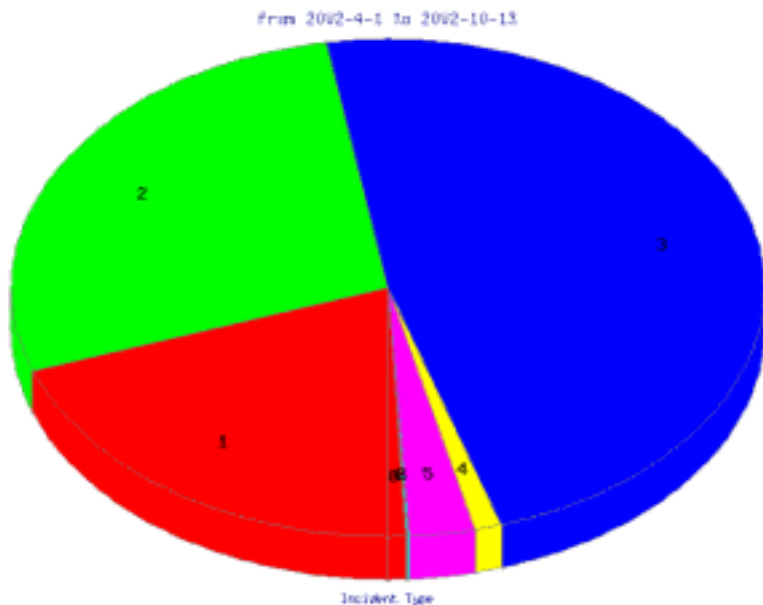


被投诉对象分布

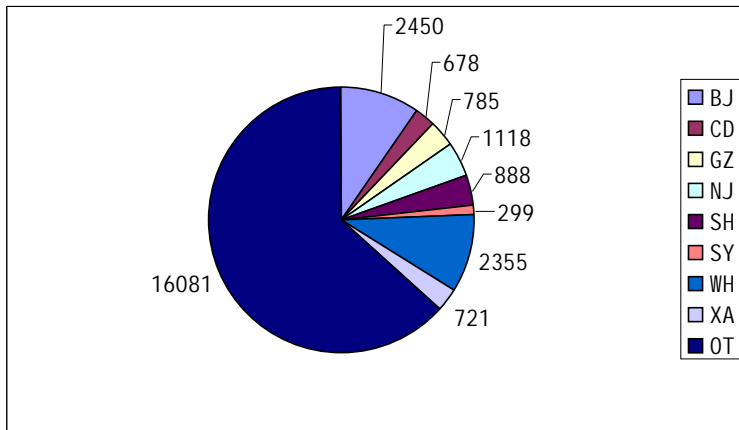
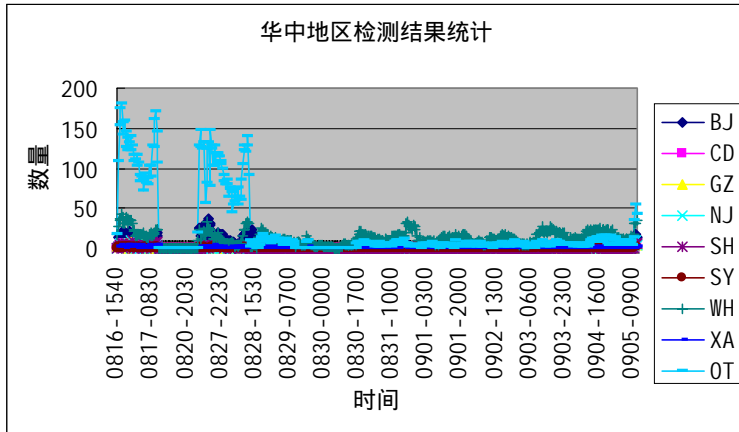


CCERT CCERT安全事件协调与处理 (Cont.)

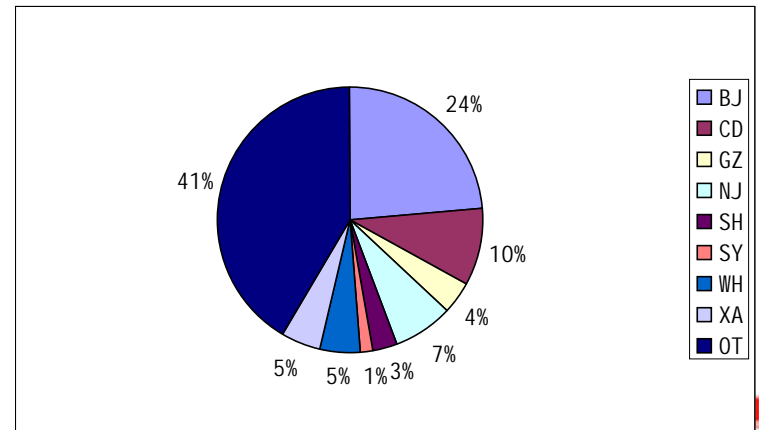
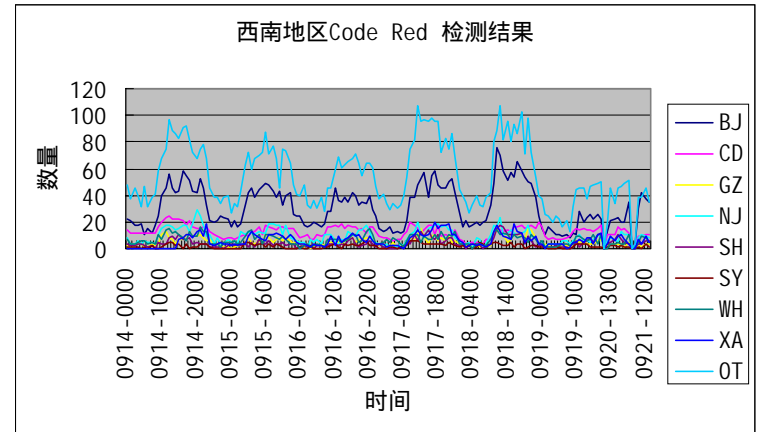
- 事件类型分布
 1. 扫描、入侵： 49%
 2. 蠕虫、病毒： 27%
 3. 垃圾邮件： 9%



Code Red in Central China



Code Red in Southwest China



- 课程特点
 - 注重网络安全整体性和系统性
 - 注重实用性
 - 结合校园网安全管理的实际情况

- 培训课程的主要内容（上）
 - 计算机网络安全风险分析
 - 网络安全体系结构
 - 密码学基础和公钥基础设施（PKI）
 - 身份认证技术
 - 访问控制

- 培训课程的主要内容（下）
 - 防火墙技术
 - 安全通信协议
 - 操作系统安全
 - 应用系统安全
 - 恶意移动代码
 - 入侵检测与应急响应
 - 校园网安全管理相关的政策

CCERT 网络应急响应组 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址(Q) http://www.ccert.edu.cn/advisories/index.htm 转到

CCERT CERNET COMPUTER EMERGENCY RESPONSE TEAM
中国教育和科研计算机网紧急响应组

关于我们 | 加入我们 | 安全漏洞 | 常见问题 | 安全论坛 | 事件报告 | 教育培训 | 信息发布 | 垃圾邮件 | 安全资源 | 相关链接

-首页 English

|安全漏洞

漏洞检索

共1页 第 1 页

CCERT编号	标题	作者	来源
CCERT-25	Sun Solaris /bin/login验证绕过漏洞	starry	转自safocus
CCERT-23	多个厂商CDE ToolTalk数据库服务器远程溢出缺陷	starry	CERT 安全公告
CCERT-22	XDR Library存在整数溢出缺陷	starry	CERT 安全公告
CCERT-24	ISC BIND 9存在拒绝服务漏洞	chapson	CERT/CC
CCERT-21	微软安全公告 MS02-045	starry	
CCERT-20	SQL Server 2000 存在严重的拒绝服务和缓冲区溢出缺陷	starry	微软安全公告
CCERT-19	SQL Server 2000允许用户执行任意指令/非法提升用户权限	starry	微软安全公告
CCERT-18	PHP multipart/form-data POST请求处理远程漏洞	cc	Stefan Esser
CCERT-17	CERT安全公告CA-2002-17 Apache Web服务器快捷操作漏洞	zln	CERT/CC
CCERT-15	ADL即时传递信息漏洞	zln	
CCERT-14	ISAPI过滤器中未加限制的缓冲区会危及商业服务器	zln	微软安全公告
CCERT-13	IE中不正确的VBScript操作会让网页访问本地文件	zln	微软安全公告
CCERT-12	XMLHTTP 控件提供访问本地文件的后门	zln	微软安全公告
CCERT-11	SNMP 实现中的漏洞	zln	CERT/CC

Internet

攻击特征库检索 - Microsoft Internet Explorer

地址: http://202.112.50.136/admin/attack/search.php

当前1/3页 转到第 1 页 GO

选择攻击类型

- 选择攻击类型
- bed-traffic
- exploit
- scan
- finger
- ftp
- telnet
- smtp
- rpc
- rservices
- dos

攻击类型	警告及记录信息	CCERT编号
POP3 EXPLOIT qpopper overflow	exploit	
POP3 EXPLOIT x86 ace overflow	exploit	
POP3 EXPLOIT x86 linux overflow	exploit	
POP3 EXPLOIT x86 bsd overflow	exploit	
POP3 EXPLOIT x86 bsd overflow	exploit	
POP3 APOP overflow attempt	exploit	
POP3 PASS overflow attempt	exploit	
POP3 USER overflow attempt	exploit	
IMAP EXPLOIT partial body attempt	exploit	
IMAP EXPLOIT partial body overflow attempt	exploit	
IMAP EXPLOIT x86 linux overflow	exploit	
IMAP EXPLOIT x86 linux overflow	exploit	

攻击类型 修改 删除

警告及记录信息

添加新攻击特征

攻击类型

修改

删除

Internet

CERT 网络应急响应组 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址: <http://www.ccert.edu.cn/announce/index.php>

CERNET COMPUTER EMERGENCY RESPONSE TEAM

CCERT 中国教育和科研计算机网紧急响应组

关于我们 | 加入我们 | 安全漏洞 | 常见问题 | 安全论坛 | 事件报告 | 教育培训 | 信息发布 | 垃圾邮件 | 安全资源 | 相关链接

English

— 首页

— 信息发布

cernet 国际出口 slapper病毒扫描最新走势图

slapper蠕虫在cernet最新传播趋势

slapper蠕虫最新动向

slapper蠕虫有了新的变种

安全公告邮件列表开通

为了使用户更快的得到漏洞的相关信息, 补丁的最新更新和最新的解决措施, 特开设了此邮件列表 advisory@ccert.edu.cn

一种危害巨大的apache蠕虫正在迅速传播, 敬请关注并升级您的系统。

Slapper蠕虫攻击Apache服务器

CCERT安全管理与实践第一期培训班开始招生

应广大用户的要求, 经过长期的准备, CCERT从2002年秋季开始举办“CCERT网络安全管理和实践”培训课程。本课程参考当前网络安全技术的载论, 结合CCERT多年的网络安全事件处理经验, 注重实用性。本课程由CCERT资深成员设计, 结合长期网络安全技术研究和实践的基础上完成, 具有很强的针对性和实用性。详细信息, 参见 <http://www.ccert.edu.cn/education/index.php>

Windows 2000 SP3 简体中文版发布请尽快下载

Windows 2000服务包3是微软要求在地产品增加新功能前必须考虑安全之后发布的首个升级包, 它修正了五百多个BUG。

新环境rtree 老树

Internet

- CCERT安全公告邮件列表
advisory@ccert.edu.cn
- 订阅方式:
 - 给majordomo@ccert.edu.cn 发一封电子邮件，在邮件正文的第一行写上: subscribe advisory email@address
把 email@address 替换成你的电子邮件。
 - 需要发回确认，具体操作方法见你所收到的电子邮件。
- 退定方式:
 - 给majordomo@ccert.edu.cn 发一封电子邮件，在邮件正文的第一行写上: unsubscribe advisory

- 校园网安全服务需求
- CERNET安全服务
- ▶ • 近期影响严重的安全事件
- 校园网常见安全问题

近期常见安全事件

- Nimda 蠕虫
 - <http://www.cert.org/advisories/CA-2001-26.html>
- MS SQL Server 多个安全漏洞
 - <http://www.cert.org/advisories/CA-2002-22.html>
- Apache+ mod_ssl （Slapper 蠕虫）
 - <http://www.cert.org/advisories/CA-2002-27.html>
 - 扫描端口80,443,
 - 通过1978/udp, 2002/udp, or 4156/udp 通信
- Sun Solaris /bin/login验证绕过漏洞
 - <http://www.ccert.edu.cn/advisories/all.php?ROWID=25>

- CCERT
 - <http://www.ccert.edu.cn>
- CERT/CC
 - <http://www.cert.org>
- SANS
 - <http://www.sans.org>

- 校园网安全服务需求
- CERNET安全服务
- 近期影响严重的安全事件
- ▶ • 校园网常见安全问题

- 垃圾邮件的危害
 - 网络流量和带宽、系统负载
 - 影响组织的声誉
 - 利于不良信息的扩散
- 发送垃圾邮件的技巧
 - 群发邮件软件、邮件地址列表
 - 利用开放的邮件中转服务（Open Relay）
 - 直接发送到接收者的邮件服务器

垃圾邮件防范办法

- 关闭邮件中转服务
- 配置发邮件认证
- DNS 屏蔽
- 网络边界屏蔽

- RBL黑名单
 - FEATURE(rbl)
- 基于内容的过滤
 - 对每封邮件过滤一次，而不是对每个接收者过滤一次(基于Procmail的做法)
 - 如果安装在企业的主邮件服务器上，可以在第一道入口拒绝进来的带有可执行附件的邮件
 - 可以防止企业内部用户发出可执行的附件的邮件给外部用户。

引起流量异常的原因

- 内部用户大量下载
- Web Proxy: 3128, 1080, 8080
- Sendmail Open Relay
- DNS : 区传输、递规查询
- 病毒/蠕虫感染 , 大量扫描
- 被黑客控制, 扫描
- 受DOS攻击

流量异常的处理

- 检查内部用户的使用情况，删除一切不必要帐号
- 关闭一切不必要的网络服务
- 关闭代理服务、或增加认证、访问控制机制
- 关闭DNS 区传输、递归查询
- 检测、清除病毒/蠕虫感染
- 监测是否被黑客控制
- 如确实受DOS攻击：
 - 通过网络边界的访问控制
 - 域名切换

校园网安全管理的建议

- 明确校园网安全管理政策
- 设立安全管理岗位，逐步建立管理制度
- 对校园网和计算机系统进行安全性评估
- 建立校园网安全监测和控制的技术措施
- 对校园网、院(系)系统和网络管理员培训
- 应对突发的安全事件，建立应急响应程序

联系方式

主页: <http://www.ccert.edu.cn>

邮件: report@ccert.edu.cn

电话: 010-62784301

传真: 010-62785933

地址: 北京 清华大学中央主楼310房间

邮编: 100084