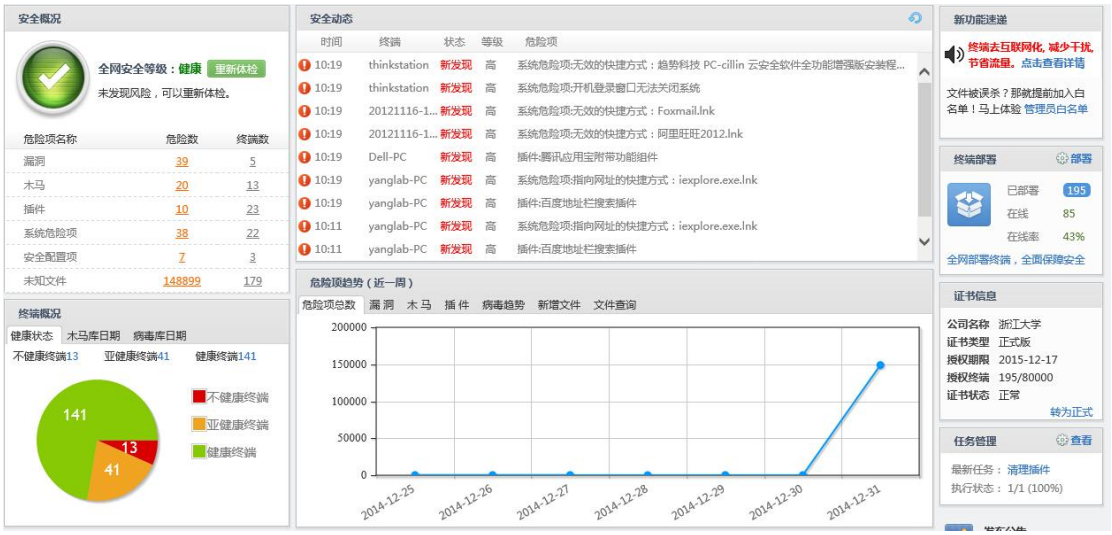
浙江大学 360 校园版定期安全简报（2014 年 12 月）

一、 360 虚拟服务器全网等级情况

目前，浙大使用了 2 台服务器为 360 天擎校园版的服务端，一台总控中心，一台分控中心，另一台为测试的实体服务器（暂时没有用户）。

1.1 服务器安全等级概况：

1) 10.203.2.93



2) 10.203.2.92

截止至 2014 年 12 月 31 日 18 点止，10.203.2.92 为 360 的总控中心，只负责分发漏洞补丁事宜，安装客户端 1 台，10.203.2.93 服务器安装客户端 195 台，卸载 48 台。

1.2 受感染用户前 10 名（总排行）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名
1	LENOVO-19B00A36	10.214.147.141	17309	玉泉-计算机学院
2	PC2013101815TCN	10.75.0.128	5420	紫金港农生环大楼
3	cyjs	10.23.21.28	786	西溪-计算中心二楼
4	Lenovo-PC	10.184.36.222	291	西溪-无线网
5	AFUAAATJSZQCTH9	10.189.234.94	111	紫金港-无线网
6	PC-201206091640	10.171.47.99	101	紫金港-碧峰
7	maoxw	10.15.41.179	46	玉泉-图书馆
8	USER-20140713WF	10.171.32.116	41	紫金港-碧峰
9	jxq-PC	10.13.83.40	30	玉泉-信电楼
10	ZhenyiNi-PC	10.18.3.98	18	玉泉硅材料实验室 3

1.3 受感染用户前 10 名（本月排行）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名	处理措施
1	PC2013101815TCN	10.75.0.128	5390	紫金港农生环大楼	清除成功
2	LENOVO-19B00A36	10.214.147.141	4349	玉泉-计算机学院	清除成功
3	AFUAAATJSZQCTH9	10.189.234.94	111	紫金港-无线网	清除成功
4	maoxw	10.15.41.179	30	玉泉-图书馆	清除成功
5	jxq-PC	10.13.83.40	18	玉泉-信电楼	清除成功
6	USER-20140713WF	10.171.32.116	18	紫金港-碧峰	清除成功
7	Sc-201411231640	192.168.16.103	16	VPN	清除成功
8	sufangwang	10.12.105.79	16	玉泉	清除成功
9	gjjy-4f84cff2f2	10.202.18.47	14	玉泉	清除成功
10	a	10.180.95.207	12	玉泉-无线网	清除成功

二、 安全简讯

2.1 11 月检测统计

360 天擎自 10 月初部署以来，随着每天的人数的增多，漏洞补丁、木马、系统危险项日益增多，本月所有统计如下表所示：

日期	终端总数	活跃终端	体检分数	漏洞	木马	插件	系统危险项	安全配置项
2014-12-31	195	90	92	39	19	9	38	7
2014-12-30	195	142	76	0	9	8	23	0
2014-12-29	198	144	70	4	16	8	25	7
2014-12-28	202	89	60	15	7	9	14	0
2014-12-27	201	95	61	70	6	9	14	1
2014-12-26	202	138	68	70	18	10	24	0
2014-12-25	202	133	72	12	13	10	23	7
2014-12-24	202	140	73	3	18	9	29	8
2014-12-23	203	142	80	10	14	5	25	0
2014-12-22	203	139	71	6	18	13	22	0
2014-12-21	202	94	59	3	5	11	18	7
2014-12-20	202	93	66	2	4	8	13	7
2014-12-19	202	140	68	5	11	12	23	7
2014-12-18	202	141	69	14	9	10	24	0
2014-12-17	201	145	79	15	12	11	27	7
2014-12-16	206	146	71	2	10	10	27	7
2014-12-15	203	152	70	9	21	13	30	0
2014-12-14	206	100	68	2	7	7	14	7
2014-12-13	206	93	62	3	5	9	30	9
2014-12-12	209	139	74	5	8	11	24	0
2014-12-11	207	148	69	9	9	10	24	7
2014-12-10	198	151	74	234	11	13	36	7

2014-12-09	196	143	72	15	13	10	23	6
2014-12-08	196	143	71	1	11	11	28	7
2014-12-07	198	100	67	7	15	9	20	2
2014-12-06	194	95	64	0	5	5	12	7
2014-12-05	193	137	71	1	14	12	22	6
2014-12-04	186	141	76	4	22	10	23	8
2014-12-03	185	138	74	116	15	9	18	0
2014-12-02	185	134	80	20	7	8	21	0
2014-12-01	183	136	77	133	19	7	20	0

2.2 XP 加固日志数据

2014 年 4 月 8 日微软对 XP 系统停止服务以来，360 盾甲对 XP 的安全，防护，系统加固产生了至关重要的作用。360 天擎校园版自进入校园以来，总共累计修复 28888 条。


您可以在此查看XP盾甲防护攻击的历史记录及详细信息。 搜索

分组 全网 开始日期 2014-10-01 结束日期 2014-10-31 查 询

日期	终端名称	IP地址	操作类型	操作说明	详细说明
2014-10-28 15:15:16	LENOVO-19B00A36	10.214.12.80	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3050F3EE-98B5-1
2014-10-28 15:12:06	CHINA-9F846D022321455	10.15.101.166	自动允许	修改 IE连接设置	注册表位置：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inte
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 360SE	进程：C:\Documents and Settings\lenovo\Application Data\360se\extensions\ExtDoc
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3F4DACA0-160D-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 360SE	进程：C:\Documents and Settings\lenovo\Application Data\360se\extensions\ExtDoc
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 360SE	进程：C:\Documents and Settings\lenovo\Application Data\360se\extensions\ExtDoc
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3F4DACA1-160D-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{B196B287-BAB4-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{B196B285-BAB4-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{B196B286-BAB4-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3F4DACA2-160D-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3F4DACA1-160D-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3F4DACA0-160D-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{B196B284-BAB4-
2014-10-28 15:05:23	lenovo-26e45cf0	10.189.180.25	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3F4DACA2-160D-

共28888条记录 1 2 3 ... 1926 下一页 跳转

2.3 本月终端插件情况统计

本月来累计统计的插件情况如下：

插件名称	危险级别	终端数量	上报日期
带推广标记的网址导航图标	高	23	2014-12-30 23:16:28
百度杀毒所附带的浏览器插件	高	17	2014-12-30 13:23:10
捆绑安装的网址导航图标	高	13	2014-12-29 09:48:36
捆绑安装的购物类广告图标	高	8	2014-12-28 11:03:56

百度地址栏搜索插件	高	7	2014-12-30 23:16:28
捆绑安装的小广告图标	高	6	2014-12-30 23:16:28
腾讯应用宝附带功能组件	高	5	2014-12-30 09:41:10
伪装的浏览器图标	高	5	2014-12-30 02:03:20
捆绑安装的工具栏按钮	高	3	2014-12-23 09:11:55
Qvod 播放器相关插件	高	2	2014-12-30 14:32:50
百度工具栏	高	2	2014-12-25 12:11:33
广告拦截专家功能扩展	高	1	2014-12-19 13:12:45
腾讯搜索插件	高	1	2014-12-22 20:31:31
系统目录存在恶意文件	高	1	2014-12-27 11:07:23
SOSO 工具栏	高	1	2014-12-25 12:11:33
Ask 工具条	高	1	2014-12-23 02:18:52
西瓜影音所附带的浏览器插件	高	1	2014-12-29 12:50:26
金山网址导航推广组件	高	1	2014-12-05 17:56:32
恶意的篡改程序	高	1	2014-12-30 21:37:04
桌面图标不显示(需重启系统生效)	高	1	2014-12-12 10:07:46
地址搜索插件	高	1	2014-12-21 11:20:25
[捆绑]必应(Bing)浏览器主页锁定插件	高	1	2014-12-17 09:49:46

2.4 重要的安全漏洞

1、IBM 产品安全漏洞

IBM WebSphere Service Registry andRepository（WSRR）是美国 IBM 公司的一个用于服务交互端点描述的主元数据存储库，它提供了存储、访问和管理有关服务信息的功能，并且是 SOA 实现的关键组成部分。本周，上述产品被披露存在跨站脚本、信息泄露和目录遍历漏洞，攻击者可利用漏洞进行跨站攻击或获取敏感信息。

CNVD 收录的相关漏洞包括：IBM WebSphere Service Registry and Repository(WSRR)跨站脚本漏洞（CNVD-2014-09176、CNVD-2014-09175、CNVD-2014-09174、CNVD-2014-09173、CNVD-2014-09172）、IBMWebSphere Service Registry and Repository (WSRR)信息泄露漏洞（CNVD-2014-09168、CNVD-2014-09169）、IBMWebSphere Service Registry and Repository (WSRR)

目录遍历漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件 。

2、Cisco 产品安全漏洞

Cisco Unified Communications 是一款 Cisco IP 电话解决方案中的呼叫处理组件。Jabber Guest 支持即将实施的 WebRTC 标准，可与 Cisco Contact CenterEnterprise 解决方案组合使用。Cisco Identity ServicesEngine 身份服务引擎是一款用于 Cisco TrustSec 解决方案的中央策略引擎。Cisco Adaptive SecurityAppliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞提升权限、获取敏感信息或进行跨站攻击。

CNVD 收录的相关漏洞包括：Cisco Unified Communications DomainManager 跨站脚本漏洞（CNVD-2014-09142）、Cisco Jabber Guest 存在多个信息泄露漏洞（CNVD-2014-09143）、Cisco Jabber Guest Server 存在多个跨站脚本漏洞、Cisco Jabber Guest 存在多个信息泄露漏洞、Cisco Identity ServicesEngine 密码泄露漏洞、Cisco Identity ServicesEngine Software 特权提升漏洞、Cisco Adaptive Security Appliance (ASA)信息泄露漏洞、Cisco Enterprise ContentDelivery System（ECDS）任意文件访问漏洞。其中，“Cisco Identity ServicesEngine 密码泄露漏洞”厂商已经发布了该漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

3、D-Link 产品安全漏洞

DIR-655 全球首款通过 Windows Vista 认证的无线路由器无线开关定时器。本周，上述产品被披露存在信息泄露、安全绕过、跨站脚本漏洞，攻击者可利用漏洞获取敏感信息、执行未授权操作或进行跨站攻击。

CNVD 收录的相关漏洞包括：D-Link DIR-655 信息泄露漏洞、D-Link DIR-655 安全绕过漏洞、D-Link DIR-655 跨站脚本漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

4、NetIQ 产品安全漏洞

NetIQ Access Manager 是一款访问控制管理程序。NetIQ eDirectory 是一个 LDAP 目录服务。本周，上述产品被披露存在信息泄露、跨站脚本和跨站请求伪造漏洞，攻击者可利用漏洞获取敏感信息、执行未授权操作或进行跨站攻击。

CNVD 收录的相关漏洞包括:NetIQ Access Manager 跨站请求伪造漏洞、NetIQ Access Manager 存在多个信息泄露漏洞、NetIQ eDirectory NDSiMonitor 远程信息泄露漏洞、NetIQ Access Manager 存在多个漏洞、NetIQ eDirectory NDSiMonitor 跨站脚本漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

5、SAPBussinessObjects Edge 权限提升漏洞

SAP BusinessObjects 是一款商务智能软件和企业绩效解决方案。本周，SAP BusinessObjects 被披露存在综合评级为“高危”的权限提升漏洞。攻击者可以利用此漏洞提升权限。目前，厂商尚未发布该漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

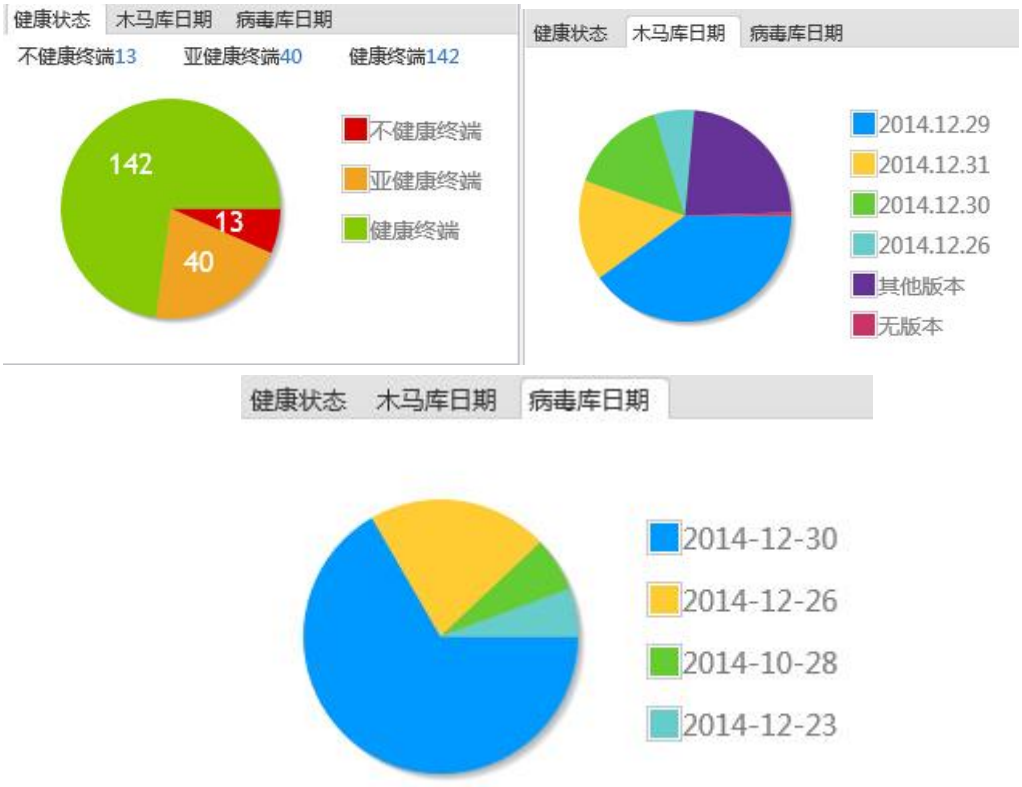
CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2014-09053	ULTRAPOP.JP i-HTTPD 任意命令执行漏洞	高	暂无
CNVD-2014-09048	PHP 'ext/standard/var_unserializer.re'内存错误引用漏洞	高	用户可以联系供应商获得补丁信息: http://php.net/ChangeLog-5.php
CNVD-2014-09052	Innominate mGuard 未授权修改漏洞	高	用户可以联系供应商获得补丁信息: http://www.innominate.com/en/
CNVD-2014-09057	Hopper Mach-O Loader 缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: http://hopperapp.com/
CNVD-2014-09065	Git 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载: https://www.kernel.org/pub/software/scm/git/ https://kernel.googlesource.com/pub/scm/git/git https://code.google.com/p/git-core/ https://github.com/gitster/git
CNVD-2014-09064	GLPI 盲 SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: http://www.glpi-project.org/spip.php?page=annonce&id_breve=334&lang=en
CNVD-2014-09063	miniBB 'code' SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: http://www.minibb.com/forums/news-9/blind-sql-injection-fix-6430.html http://security.szurek.pl/minibb-31-blind-sql-injection.html
CNVD-2014-09096	SafeNet Authentication Service Outlook Web Access Agent 目录遍历漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞: http://appcheck-ng.com/safenet-sas-owa-agent-directory-traversal-vulnerability/
CNVD-2014-09092	EMC Documentum Content Server 权限提升漏洞	高	目前厂商已经发布升级补丁/版本以修复这个安全问题，请用户及时下载更新: http://www.emc.com/domains/documentum/index.htm
CNVD-2014-09094	Movable Type SQL 注入漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞: http://secunia.com/advisories/61227

2.5 截止至本月月底的全网安全状况如下：

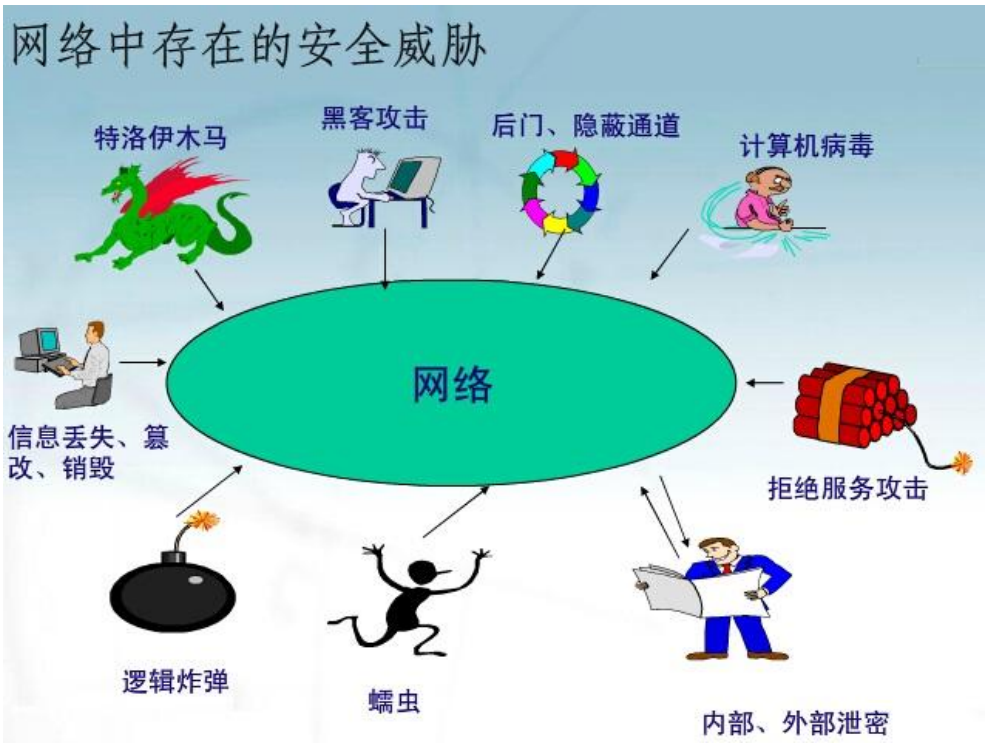
10.203.2.93　　10.203.2.92

2．6 终端概况如下

1）10.203.2.93



三、网络安全常用防范小常识



互联网是一把两刃利剑，一方面为日常生活带来便利，另一方面又为黑客入侵电脑系统开放更多渠道。一般如何防范？请看下面能保障个人隐私信息的十个基本常识：

1.采用匿名方式浏览，因为许多网站利用 cookies 跟踪网友的互联网活动，从而确定网友喜好。你可以在使用浏览器时关闭电脑接收 cookie 的选项，避免受到 cookies 的追踪。

2.进行任何网上交易或发送电邮前，切记阅读网站的隐私保护政策，因为有些网站会将你的个人资料卖给第三方。

3.安装个人防火墙，以防止个人资料和财务数据被窃取。及时升级是非常重要的一环，否则防火墙的作用就没有被完全发挥，被攻击的可能性依然很大。此外，你还可利用保安软件将重要资料保密，减少不慎把这些资料发送到不安全网站的可能性。

4.使用保安软件或防火墙以防止黑客攻击和 spyware（一个连接外部服务器并将个人资料传送至网络的软件）。这些软件能够保护个人电脑和资料免受黑客窃取，并防止 spyware 自动连接网站并发送你的资料。

5.在网上购物时，确保已采用安全的连接方式。可以透过查看浏览器上方的闭锁图标（closedlockicon），以确定连接是否安全。

6.黑客有时会假装成互联网服务供应商的代表，并询问你的密码及个人资料，谨记上网时不要向任何人透露这些资料。

7.经常更改你的密码，使用包含字母和数字的多位数的密码，从而干扰黑客利用软件程序来搜寻最常用的密码。

8.在不需要文件和打印共享时，关闭这些功能。文件和打印共享功能虽然非常有用，但也会暴露你的电脑给予寻找安全漏洞的黑客。黑客一旦进入个人电脑，便能窃取私隐资料。

9.不要打开来自陌生人的电子邮件附件。这些附件可能包含一个特洛伊木马程式，该程序让黑客长驱真入电脑文档，甚至控制外设，有些黑客甚至能潜入互联网照相机（Webcamera）进行监视。此外，你还应当安装一个具备防病毒程式的软件，保护电脑免受病毒、特洛伊木马程序和蠕虫的侵害。

10.可以利用一些网络安全公司的实时检查。以确定电脑是否备有防护电脑病毒和恶意代码的能力。此功能还可以扫描电脑，寻找安全漏洞和病毒，并将扫描结果与其他已经扫描的系统作比较。

总之，在网络安全越来越重要的今天，不要抱着“被黑的不会是我”的侥幸心理，只有做好良好的防卫工作才行。

三、 技术交流

欢迎老师和同学们前来交流问题，多提建议，希望下期简报内容更加接近大家的需求。

咨询服务电话：87951669
邮箱: netsafe@zju.edu.cn

工程师联系方式：
13588277982 章荣伟