浙江大学 360 校园版定期安全简报（2014 年 10 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

截止至 2014 年 10 月 31 日 12 点止，10.203.2.92 为 360 的总控中心，只负责分发漏洞补丁事宜，10.203.2.93 服务器安装客户端 141 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	cyjs	10.23.21.28	785	西溪-计算中心二楼
2	PC-201206091640	222.205.109.13	85	VPN
3	qq-P	10.15.101.66	14	玉泉-图书馆

4	xuhao	210.32.163.180	11	VPN
5	wangfei-PC	10.15.42.87	4	玉泉-热能所
6	rensong	210.32.168.124	4	VPN
7	ZHUHX-PC	10.49.110.13	3	华家池-宿舍 10
8	violin-lcl	192.168.1.101	3	其他
9	YeZhiguo	222.205.107.227	3	VPN
10	Jiang-PC	10.16.16.23	3	玉泉-图书馆

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	cyjs	10.23.21.28	785	西溪-计算中心二楼	清除成功
2	PC-201206091640	222.205.109.13	85	VPN	清除成功
3	qq-P	10.15.101.66	14	玉泉-图书馆	清除成功
4	xuhao	210.32.163.180	11	VPN	清除成功
5	wangfei-PC	10.15.42.87	4	玉泉-热能所	清除成功
6	rensong	210.32.168.124	4	VPN	清除成功
7	ZHUHX-PC	10.49.110.13	3	华家池-宿舍 10	清除成功
8	violin-lcl	192.168.1.101	3	其他	清除成功
9	YeZhiguo	222.205.107.227	3	VPN	清除成功
10	Jiang-PC	10.16.16.23	3	玉泉-图书馆	清除成功

二、 安全简讯

2.1 10 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
2014-10-31	141	92	94	13	15	9	18	7
2014-10-30	140	117	80	1	9	9	16	0
2014-10-29	137	116	77	5	6	12	17	0
2014-10-28	131	117	82	21	9	10	17	7
2014-10-27	129	116	82	145	5	14	13	8
2014-10-26	128	68	73	1	1	8	10	7
2014-10-25	127	61	74	6	1	11	6	7
2014-10-24	123	105	82	96	8	12	15	0
2014-10-23	122	108	78	15	4	9	12	9
2014-10-22	117	110	79	65	8	11	14	0
2014-10-21	104	105	78	20	7	11	10	8
2014-10-20	65	97	78	60	15	12	6	7
2014-10-19	64	38	80	1	4	5	4	6
2014-10-18	58	38	71	135	3	4	5	0
2014-10-17	50	52	73	131	2	9	8	0
2014-10-16	48	44	87	4	3	5	4	0
2014-10-15	45	44	87	0	2	5	6	0
2014-10-14	30	42	80	11	2	7	4	0
2014-10-13	29	27	80	0	0	5	2	0
2014-10-12	28	12	78	0	0	1	0	0
2014-10-11	28	24	86	0	0	4	3	0
2014-10-10	28	26	88	0	0	5	3	0
2014-10-09	5	28	91	3	1	6	4	0
2014-10-08	4	5	83	0	0	0	0	0
2014-10-07	4	3	97	0	0	0	0	0
2014-10-06	4	3	97	0	0	0	0	0
2014-10-05	3	3	97	0	0	0	0	0
2014-10-04	3	2	97	0	0	0	0	0

2014-10-03	1	3	48	0	0	1	0	0
2014-10-02	1	0	0	0	0	0	0	0
2014-10-01	1	0	0	0	0	0	0	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，一月时间，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
捆绑安装的网址导航图标	高	15	2014-10-30 02:28:59
带推广标记的网址导航图标	高	14	2014-10-30 02:28:59
百度地址栏搜索插件	高	10	2014-10-30 13:29:57
捆绑安装的购物类广告图标	高	8	2014-10-29 17:07:40
腾讯应用宝附带功能组件	高	6	2014-10-30 11:01:09
捆绑安装的小广告图标	高	5	2014-10-29 17:07:40
伪装的浏览器图标	高	5	2014-10-28 09:21:31
百度杀毒所附带的浏览器插件	高	4	2014-10-30 02:03:53
腾讯搜索插件	高	3	2014-10-27 19:32:57

百度工具栏	高	2	2014-10-30 11:01:09
Qvod 播放器相关插件	高	2	2014-10-30 17:24:37
隐藏系统下恶意变形程序	高	1	2014-10-29 20:32:17
系统目录存在恶意文件	高	1	2014-10-17 15:39:46
SOSO 工具栏	高	1	2014-10-30 11:01:09
Ask 工具条	高	1	2014-10-29 02:06:56
木马残留文件	高	1	2014-10-21 12:14:02
西瓜影音所附带的浏览器插件	高	1	2014-10-30 13:53:07
Conduit 工具条	高	1	2014-10-27 16:25:16

2.4 重要的安全漏洞

CNVD 整理和发布以下重要安全漏洞信息。

1、SSLV3 Protocol 产品安全漏洞

10 月 15 日，CNVD 收录了 SSL V3 协议存在的一个可导致信息泄露的高危漏洞（CNVD-2014-06718，对应 CVE-2014-3566）。攻击者可利用漏洞发起远程攻击，窃取采用 sslv3 加密通信过程中的内容，构成信息泄露安全风险。

CNVD 收录的相关漏洞包括：SSL V3 Protocol 信息泄露漏洞。上述漏洞的综合评级为“高危”。目前厂商暂时没有提供升级补丁。

2、Microsoft 产品安全漏洞

10 月 15 日,CNVD 收录了最新披露的 Windows OLE 远程代码执行漏洞（CNVD-2014-06717，对应 CVE-2014-4114）。攻击者可通过精心构造包含文件，并诱使用户执行文件触发远程代码执行漏洞，进而控制用户操作系统主机。此外，10 月 15 日，微软发布了 2014 年 10 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer、.NET Framework、ASP.NET MVC、Office、Office Services 和 Web Apps 中存在的 24 个安全漏洞。其中，3 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制。

CNVD 收录的相关漏洞包括：Microsoft Windows OLE 包管理器远程代码执行漏洞、Microsoft InternetExplorer 存在未明内存破坏漏洞（CNVD-2014-06867、CNVD-2014-06864、CNVD-2014-06866、CNVD-2014-06865、CNVD-2014-06868、CNVD-2014-06869、CNVD-2014-06870）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。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、Oracle 产品安全漏洞

10 月 14 日，Oracle 发布了 2014 年 10 月份的安全更新，修复了其多款产品存在的 154 个安全漏洞。受影响的产品包括 Oracle 数据库（31 个）、中间件产品 Fusion Middleware（18 个）；电子商务套装软件 Oracle E-Business Suite（10 个）、供应链套装软件 Oracle Supply ChainProducts Suite（5 个）、企业管理器网格控制产品 Oracle Enterprise ManagerGrid Control（2 个）；Virtualization（7 个）、PeopleSoft 产品（5 个）、Primavera 产品（2 个）、JD Edwards 产品（1 个）、Retail Applications（4 个）、Health SciencesApplications（3 个）、CommunicationsApplications（2 个）、Java SE（25 个）、Oracle Sun 系统产品（15 个）和 MySQL 数据库（24 个）。本次安全更新提供了针对 32 个高危漏洞的补丁，有 138 个漏洞可被远程利用。

CNVD 收录的相关漏洞包括：Oracle Database Server 远程代码执行漏洞、Oracle Java SE/Java SEEmbedded AWT 子件存在未明远程代码执行漏洞、Oracle Java SE 存在远程漏洞（CNVD-2014-06751）、Oracle Supply ChainProducts Suite 存在远程漏洞（CNVD-2014-06810、CNVD-2014-06811、CNVD-2014-06812）、Oracle Java SE/Java SEEmbedded/JRockit Libraries 子件存在未明漏洞、Oracle PeopleSoft Products 存在远程漏洞（CNVD-2014-06802）。其中“Oracle Database Server 远程代码执行漏洞、Oracle Java SE/Java SEEmbedded AWT 子件存在未明远程代码执行漏洞、Oracle Java SE 存在远程漏洞（CNVD-2014-06751）”漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。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、Cisco 产品安全漏洞

Cisco Adaptive Security Appliance 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拒绝服务和信息泄露漏洞，攻击者可利用漏洞获取敏感信息或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco ASA Software 拒绝服务漏洞（CNVD-2014-06771、CNVD-2014-06770、CNVD-2014-06768、CNVD-2014-06769、CNVD-2014-06767、CNVD-2014-06766、CNVD-2014-06765）、Cisco ASA Software 信息泄露漏洞（CNVD-2014-06764）。上述漏洞的综合评级为“高危”。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、vBulletin’breadcrumbs_create.php’ SQL 注入漏洞

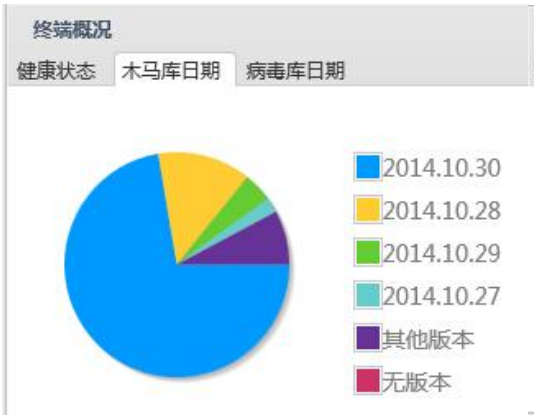
vBulletin 是款论坛程序套件。本周，vBulletin 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用漏洞危及应用程序，访问或修改数据。目前，厂商尚未发布该漏洞的修补程序。提醒广大用户随时关注厂商主页，以获取最新版本。

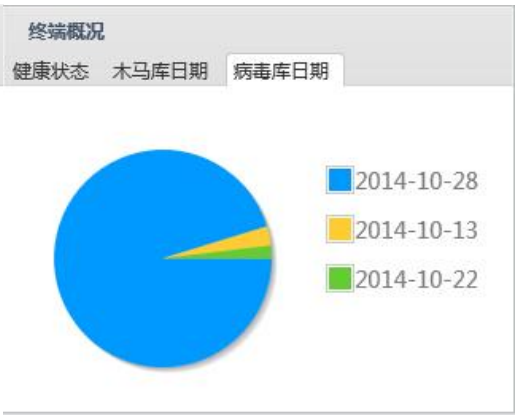
2.5 截止至本月月底的全网安全状况如下：


安全概况
全网安全等级：健康
重新体检
未发现风险，可以重新体检。
危险项名称 危险数 终端数
漏洞 13 4
木马 15 10
插件 9 10
系统危险项 18 13
安全配置项 7 1
未知文件 2096 90

2．6 终端概况如下


终端概况
健康状态
木马库日期
病毒库日期
不健康终端9
亚健康终端23
健康终端109
109
9
23
不健康终端
亚健康终端
健康终端


终端概况
健康状态
木马库日期
病毒库日期
2014.10.30
2014.10.28
2014.10.29
2014.10.27
其他版本
无版本


终端概况
健康状态
木马库日期
病毒库日期
2014-10-28
2014-10-13
2014-10-22

三、　计算机浏览器常用防范知识

3.1 360 针对浏览器及主页的设定方法

1、打开 360 天擎校园版：如下图一：

图一

2、点击图一上红色框框内的 “进入”。如图二：

图二

3、点击图二红色框框，会显示“收起状态”，点击下图三红色框框内的红色圆圈，“设置”选项：

图三

4、打开设置选项，可以看到设置内容，设置好主页后，也可以设置默认浏览器，设置完成后点击后面的“滚动条”，使之成为绿色的（点击一下绿点往右）即可，如图四：

图四

3.2 针对浏览器弹出垃圾网页及广告过滤方法

1、打开 360 天擎校园版：如下图一：

图一

2、点击图一上红色框框内的 “进入”。如图二：

图二

3、点击图二红色框框，会显示“收起状态”，点击下图三红色框框内的红色圆圈，“设置”选项：

图三

4、打开设置选项，可以看到设置内容，如图四：

图四

以上设置界面可以详细看一看，针对各个方面的设置。但是由于弹出的网页不一点含有挂马信息，所以未必能拦截掉。大部分都是由于访问的网站上带有的，这种问题很难 100%解决。

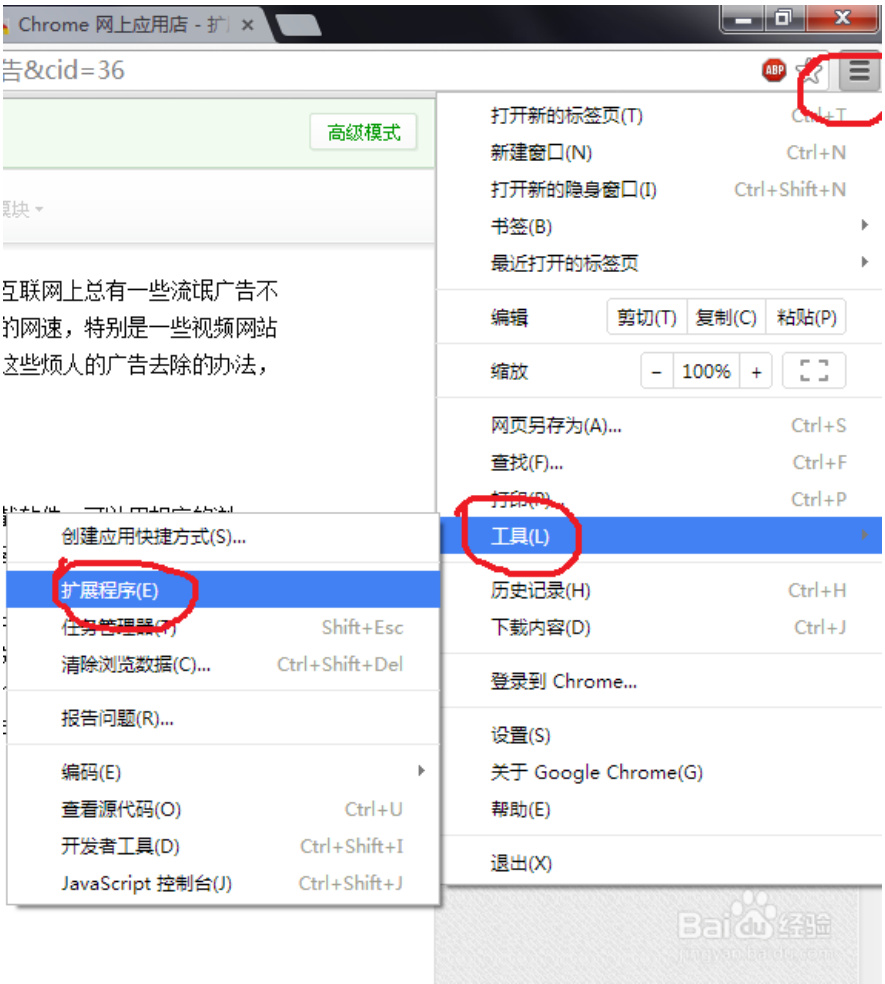
以下提供浏览器的设置方法：

一、360 浏览器：

先点击浏览器上的，扩展。点击进去以后 选择“广告终结者”的插件，点击安装即可拦截大部分广告网页。具体如下图：

二、谷歌浏览器(以下来自百度)：

先进入谷歌浏览器，点击自定义及控制 GoogleChrome-->工具-->扩展程序，然后里面有个“获取跟多扩展程序”的链接，点击它就可以进入 Chrome 网上应用商店，然后就可以在里面通过关键字搜索包括广告拦截插件在内的各种你需要的插件。



三、IE 浏览器(以下来自百度)：

需要在网上下载一个名叫 Adblock 的广告拦截软件，可以用相应的浏览器在百度上搜索 Adblock 直接到官网上下载然后傻瓜式安装。

这里介绍的相当于插件之类的广告拦截工具，可能会在一定程度上拖慢浏览器速度，软件毕竟是软件，正所谓上有政策下有对策，毕竟不是万能的，还是会遗漏掉部分顽强不能过滤的

网页，但是这种情况并不多见。

四、 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