浙江大学 360 校园版定期安全简报（2015 年 3 月）

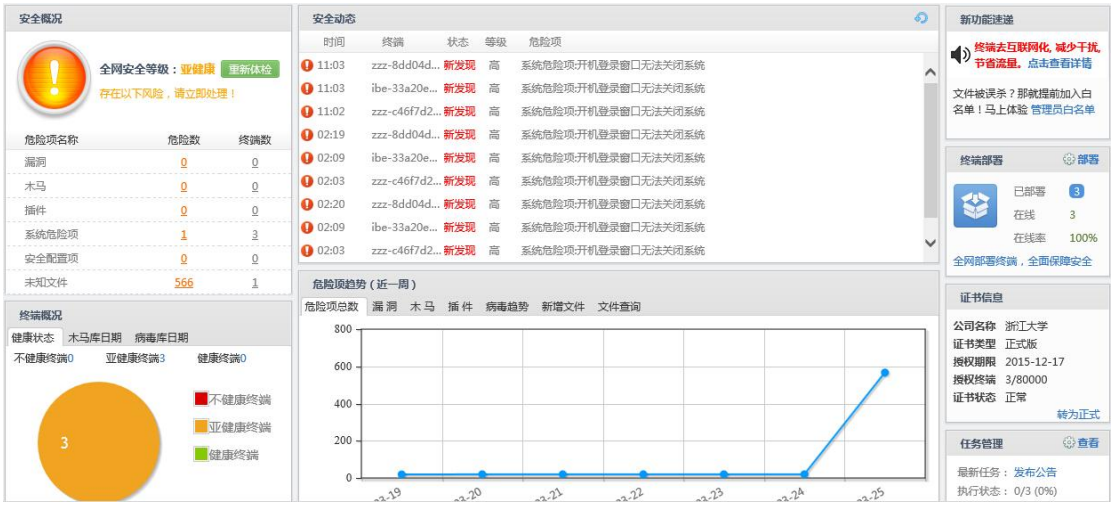
一、 360 虚拟服务器全网等级情况

目前，浙大使用了 2 台服务器为 360 天擎校园版的服务器，一台总控中心，一台分控中心。

1.1 服务器安全等级概况：

1) 10.203.2.93

2) 10.203.2.92



截止至 2015 年 3 月 25 日 15 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 3 台，10.203.2.93 服务器安装客户端 207 台，卸载 64 台。

1.2 受感染用户前 10 名（总排行 2015 年）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名
1	zju	10.15.83.72	2783	玉泉-图书馆
2	PC-201309181536	10.189.253.139	1123	紫金港-无线网
3	DELL-PC	10.78.49.49	298	紫金港生科院
4	mayanning-PC	192.168.0.106	297	VPN
5	xugangjiang-PC	10.189.251.190	227	紫金港-无线网
6	YeZhiguo	10.71.123.36	77	紫金港-医学院综合楼
7	zju-HP	10.51.120.163	54	之江-主楼
8	violin-lcl	192.168.1.100	46	VPN
9	ZhenyiNi-PC	10.18.3.98	44	玉泉硅材料实验室 3
10	PC2013101815TCN	10.75.0.128	28	紫金港农生环大楼

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	zju	10.15.83.72	2713	玉泉-图书馆	清除成功
2	PC-201309181536	10.189.253.139	1105	紫金港-无线网	清除成功
3	DELL-PC	10.78.49.49	296	紫金港生科院	清除成功
4	mayanning-PC	192.168.0.106	296	VPN	清除成功
5	xugangjiang-PC	10.189.251.190	227	紫金港-无线网	清除成功
6	YeZhiguo	10.71.123.36	39	紫金港-医学院综合楼	清除成功
7	zju-HP	10.51.120.163	27	之江-主楼	清除成功
8	ZHUHX-PC	10.49.110.13	9	华家池-无线网	清除成功
9	zjuj	10.189.253.139	8	紫金港-无线网	清除成功

10	Zhang-PC	192.168.2.111	6	VPN	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：

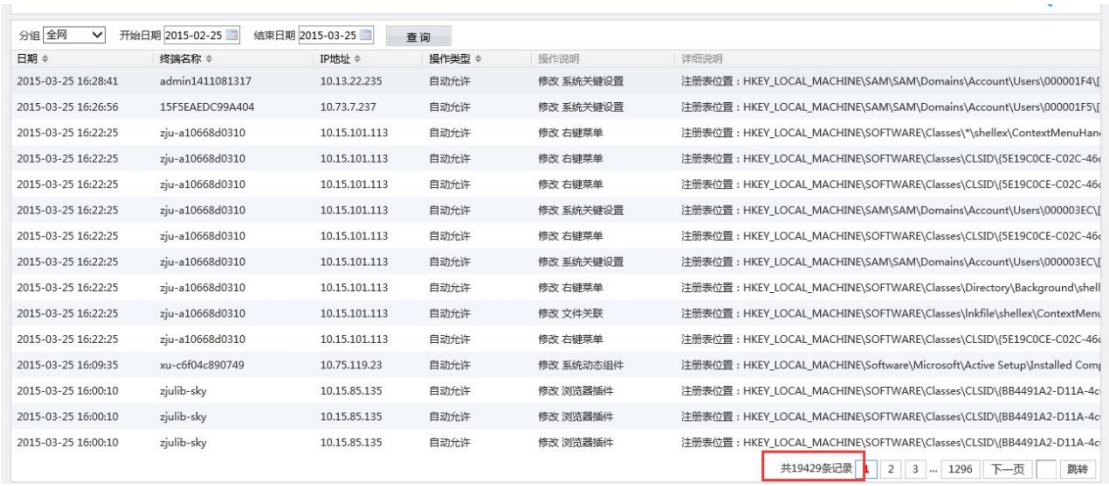
日期	终端总数	活跃终端	体检分数	漏洞	木马	插件	系统危险项	安全配置项
2015-03-25	206	107	91	77	7	8	42	8
2015-03-24	199	162	68	25	8	4	24	0
2015-03-23	199	154	70	22	93	5	31	7
2015-03-22	201	106	60	18	0	5	14	0
2015-03-21	200	103	57	1	2	3	8	0
2015-03-20	202	154	67	28	5	6	24	8
2015-03-19	197	159	68	16	4	7	21	7
2015-03-18	198	158	68	0	3	7	22	7
2015-03-17	194	156	66	4	4	5	23	7
2015-03-16	195	157	71	1	4	7	23	0
2015-03-15	198	102	62	0	2	4	23	7
2015-03-14	207	98	59	9	2	2	20	7
2015-03-13	207	163	68	1	6	5	26	8
2015-03-12	208	151	72	1	6	8	21	0
2015-03-11	207	151	74	195	6	6	31	7
2015-03-10	205	147	72	145	8	5	28	7
2015-03-09	202	145	68	132	3	7	26	7
2015-03-08	200	102	63	0	3	4	17	7
2015-03-07	199	94	63	6	2	3	13	9
2015-03-06	197	127	77	0	5	6	21	9
2015-03-05	198	88	69	1	3	4	19	7

2015-03-04	194	86	65	4	2	1	14	7
2015-03-03	195	73	62	1	1	3	14	7
2015-03-02	197	72	59	9	3	3	13	8
2015-03-01	197	49	54	0	1	1	9	0
2015-02-28	197	57	65	69	1	2	12	7
2015-02-27	197	52	63	0	1	2	7	0
2015-02-26	199	46	58	0	1	3	8	0
2015-02-25	198	38	67	20	1	2	7	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 2015 年以来，3 月份累计修复 19429 条。



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
百度地址栏搜索插件	高	13	2015-03-24 10:57:47
百度杀毒所附带的浏览器插件	高	3	2015-03-24 19:07:23
腾讯应用宝附带功能组件	高	2	2015-03-24 09:38:28
捆绑安装的工具栏按钮	高	2	2015-03-23 10:06:34
恶意的篡改程序	高	1	2015-03-24 22:13:00
网络实名	高	1	2015-03-22 18:44:15

腾讯搜索插件	高	1	2015-03-12 13:36:03
伪装的浏览器图标	高	1	2015-03-22 13:32:18
Qvod 播放器相关插件	高	1	2015-03-22 11:02:33

2.4 Microsoft 2015 年 3 月安全更新

安全公告编号:CNTA-2015-0006

3 月 10 日，微软发布了 2015 年 3 月份的月度例行安全公告，共含 14 项更新，修复了 Microsoft Windows、Internet Explorer、Exchange、Office 和 Server 软件中存在的 45 个安全漏洞。

其中，5 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，获得敏感信息，或进行拒绝服务攻击。CNVD 提醒广大 Microsoft 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。

下表所示为了微软本月安全公告详情（按严重性排序），更多情况请参阅微软的官方网站。

公告 ID	公告标题和摘要	最高严重等级和漏洞影响	重新启动要求	受影响的软件
MS15-018	**Internet Explorer 累积安全更新 (3032359)** 此安全更新可解决 Internet Explorer 中的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看经特殊设计的网页时允许远程执行代码。成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。	严重 远程代码执行	需要重启	Microsoft Windows，Internet Explorer
MS15-019	**VBscript 脚本引擎中的漏洞可能允许远程执行代码 (3040297)** 此安全更新可解决 Microsoft Windows 的 VBscript 脚本引擎中一个漏洞。如果用户访问经特殊设计的网站，此漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户	严重 远程执行代码	可能要求重启	Microsoft Windows

	权限登录，成功利用此漏洞的攻击者便可完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。			
MS15-020	**Microsoft Windows 中的漏洞可能允许远程执行代码 (3041836)** 此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者成功诱使用户浏览经特殊设计的网站、打开经特殊设计的文件或在包含经特殊设计的 DLL 文件的工作目录中打开文件，则漏洞可能会允许远程执行代码。	严重 远程执行代码	可能要求重启	Microsoft Windows
MS15-021	**Adobe 字体驱动程序中的漏洞可能允许远程执行代码 (3032323)** 此安全更新可修复 Microsoft Windows 中的漏洞。最严重的漏洞可能在用户查看经特殊设计的文件或网站时允许远程执行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。	严重 远程执行代码	需要重启	Microsoft Windows
MS15-022	**Microsoft Office 中的漏洞可能允许远程执行代码 (3038999)** 此安全更新可修复 Microsoft Office 中的漏洞。最严重的漏洞可能在用户打开经特殊设计的 Microsoft Office 文件时允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。	严重 远程执行代码	可能要求重启	Microsoft Office，Microsoft Server 软件
MS15-023	**内核模式驱动程序中的漏洞可能允许特权提升 (3034344)** 此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者登录系统并运行旨在提升特权的经特殊设计的应用程序，最严重的漏洞可能允许特权提升。攻击者随后可安装程序；查看、更改或删除数据；或者创建拥有完全管理权限的新帐户。	重要 特权提升	需要重启	Microsoft Windows
MS15-024	**PNG 处理中的漏洞可能允许信息泄漏 (3035132)** 此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者诱使用户访问包含经特殊设计的 PNG 图像的网站，此漏洞可能允许信息泄露。	重要 信息泄露	需要重新启动	Microsoft Windows
MS15-025	**Windows 内核中的漏洞可能允许特权提升 (3038680)** 此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者登录受影响的系统并运行经特殊设计的应用程序，最严重的漏洞可能允许特权提升。成功利用该漏洞的攻击者可能在登录到受影响系统的其他用户帐户的安全上下文中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者可能创建拥有完全用户权限的新帐户。	重要 特权提升	需要重启	Microsoft Windows
MS15-0	**Microsoft Exchange Server 中的漏洞可能允许特权**	重要	无需重	Microsoft Exch

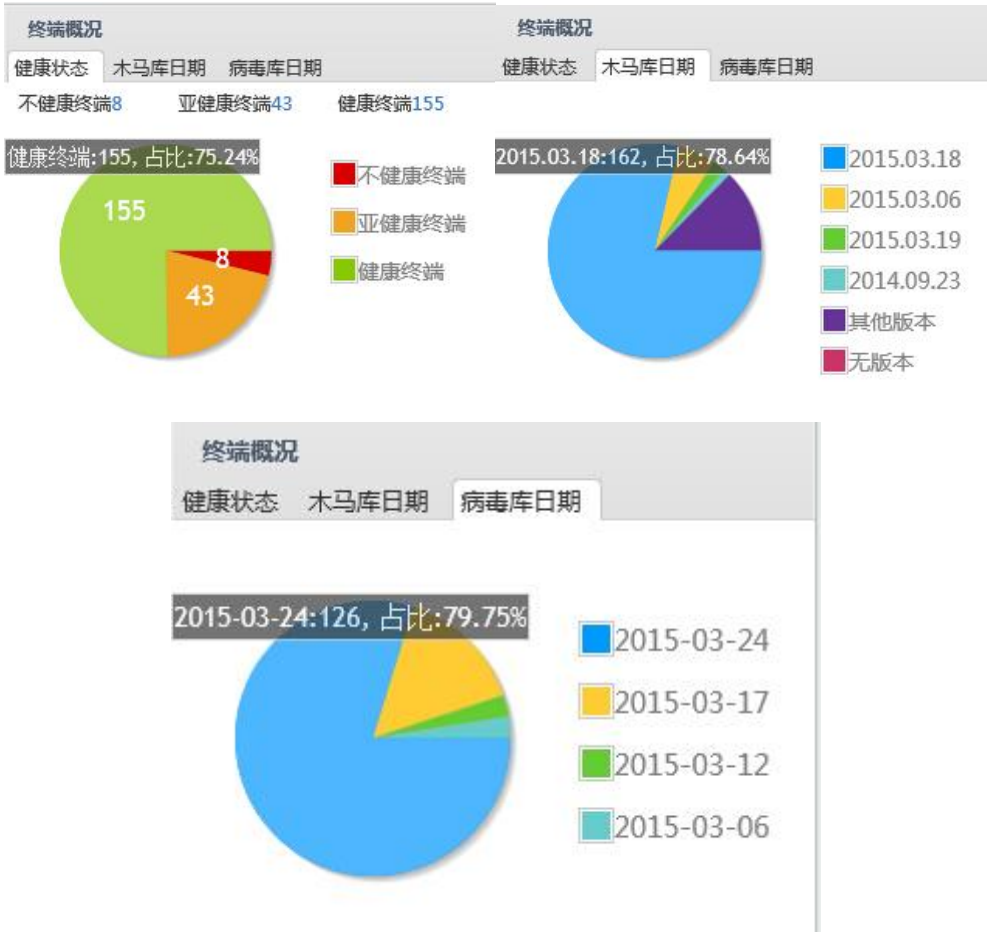
26	**提升（3040856）** 此安全更新可解决 Microsoft Exchange Server 中的漏洞。如果用户单击定向到目标 Outlook Web App 网站的经特殊设计的 URL，则其中最严重的漏洞可能允许特权提升。攻击者无法强迫用户访问经特殊设计的网站，但攻击者可能会诱使用户访问该网站，方法通常是让用户单击 Instant Messenger 消息或电子邮件中的链接以使用户链接到攻击者的网站，然后诱使用户单击经特殊设计的 URL。	特权提升	启	ange
MS15-027	**NETLOGON 中的漏洞可能允许欺骗（3002657）** 此安全更新可修复 Microsoft Windows 中的漏洞。如果登录到已加入域的系统的攻击者运行经特殊设计的应用程序，该应用程序可与作为被模拟用户或系统的其他已加入域的系统建立连接，则漏洞可能允许欺骗。攻击者必须登录到已加入域的系统，并能够观察网络流量。	重要 欺骗	需要重启	Microsoft Windows
MS15-028	**Windows 任务计划程序中的漏洞可能允许安全功能绕过（3030377）** 此安全更新可修复 Microsoft Windows 中的漏洞。该漏洞可能允许在受影响系统上权限受限的用户利用任务计划程序来执行其无权运行的文件。成功利用此漏洞的攻击者可以绕过 ACL 检查并运行特权可执行文件。	重要 安全功能规避	需要重启	Microsoft Windows
MS15-029	**Windows 照片解码器组件中的漏洞可能允许信息泄漏（3035126）** 此安全更新可修复 Microsoft Windows 中的漏洞。如果用户浏览包含经特殊设计的 JPEG XR（.JXR）图像的网站，该漏洞可能允许信息泄露。虽然攻击者无法利用此漏洞来执行代码或直接提升他们的用户权限，但此漏洞可用于获取信息，这些信息可用于试图进一步危及受影响系统的安全。	重要 信息泄露	可能要求重启	Microsoft Windows
MS15-030	**远程桌面协议中的漏洞可能允许拒绝服务（3039976）** 此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者创建的多个远程桌面协议（RDP）会话无法正确释放内存中的对象，该漏洞可能允许拒绝服务。在任何 Windows 操作系统上，RDP 默认为未启用。未启用 RDP 的系统均不存在这一风险。	重要 拒绝服务	需要重启	Microsoft Windows
MS15-031	**Schannel 中的漏洞可能允许绕过安全功能（3046049）** 此安全更新可解决 Microsoft Windows 中利用公开披露的 FREAK 技术的漏洞，这一行业范围问题并不是 Windows 操作系统特有的。此漏洞可以允许中间人（MiTM）攻击者在 TLS 连接中强制将 RSA 密钥的密钥长度降级到 EXPORT 级长度。任何使用 Schannel 连接到带有不安全密码套件的远程 TLS 服务器的 Windows 系统均会受到影响。	重要 安全功能规避	需要重启	Microsoft Windows

2.5 截止至本月月底的全网安全状况如下：

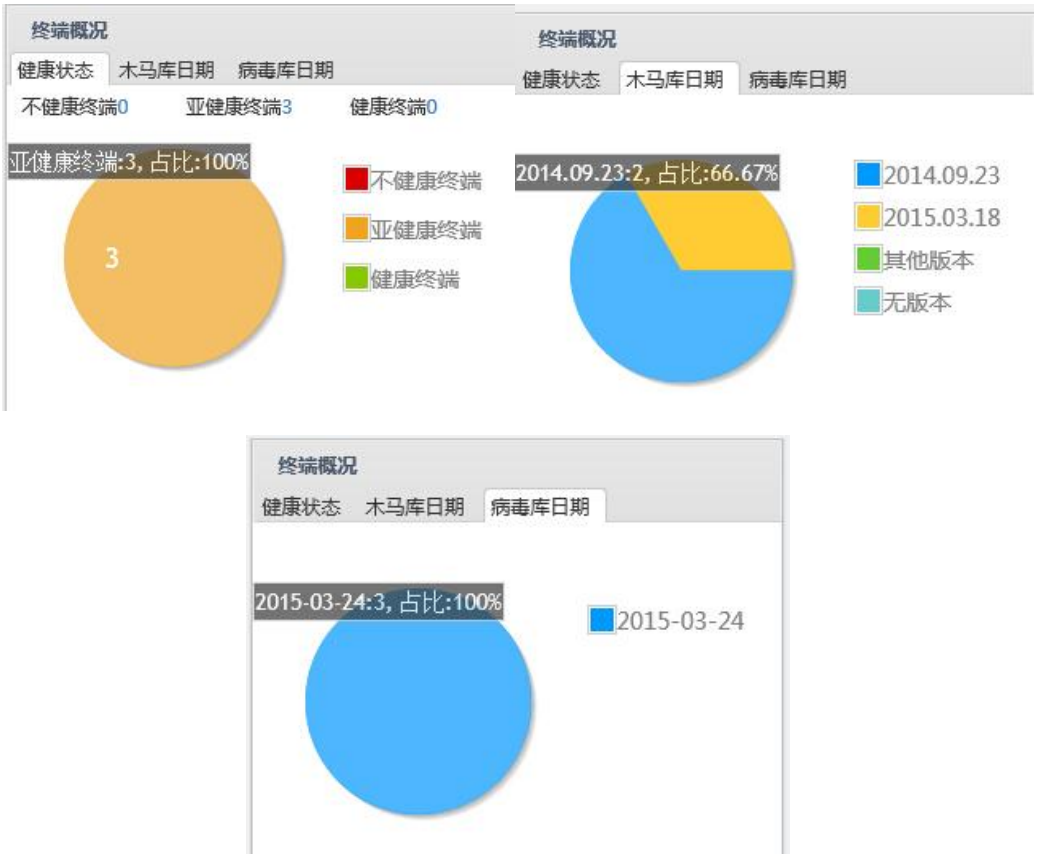
10.203.2.93　　10.203.2.92

2．6 终端概况如下

1）10.203.2.93



2）10.203.2.92



三、 2015 年 3 月计算机二级考试 OFFICE 高级应用计算机病毒防治

以下为计算机考吧总结：

第 9 章 计算机病毒及其防治

9.1 计算机病毒的特征和分类

1.计算机病毒

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。计算机病毒主要通过移动存储介质(如 U 盘、移动硬盘)和计算机网络两大途径进行传播计算机病毒的特点如下。

(1)寄生性

(2)破坏性

(3)潜伏性

(4)隐蔽性

2.计算机病毒类型

计算机的病毒类型主要有以下几种。

(1)系统病毒

(2)蠕虫病毒

(3)木马病毒、黑客病毒

(4)脚本病毒

(5)宏病毒

(6)后门病毒

(7)病毒种植程序病毒

(8)破坏性程序病毒

(9)玩笑病毒

(10)捆绑机病毒

3.计算机感染病毒的常见症状

计算机受到病毒感染后会表现出如下症状。

(1)机器不能正常启动

(2)运行速度降低

(3)磁盘空间迅速变小

(4)文件内容和长度有所改变

(5)经常出现“死机”现象

(6)外部设备工作异常

(7)文件的日期和时间被无缘无故的修改成新的时间日期。

(8)显示器上经常出现一些怪异的信息，和异常现象。

9.2 计算机病毒的防治与清除

1.防治计算机病毒

对计算机病毒的防治应遵循以下原则，防患于未然。

(1)使用新设备和新软件之前要检查。

(2)使用反病毒软件。及时升级反病毒软件的病毒库.开启病毒实时监控。

(3)制作一张无毒的系统软盘。将其写保护，妥善保管，以便应急。

(4)制作应急盘/急救盘/恢复盘。按照反病毒软件的要求制作应急盘/急救盘/恢复盘，以便恢复系统急用。

(5)不要随便使用别人的软盘或光盘。

(6)不要使用盗版软件。

(7)有规律地制作备份，养成备份重要文件的习惯。

(8)不要随便下载网上的软件。

(9)注意计算机有没有异常现象。

(10)发现可疑情况及时通报以获取帮助。

(11)重建硬盘分区，减少损失。若硬盘资料已经遭到破坏，不必急着格式化，因病毒不可能在短时间内将全部硬盘资料破坏，故可利用“灾后重建”程序加以分析和重建。

(12)扫描系统漏洞，及时更新系统补丁。

(13)在使用移动存储设备时，应先对其进行杀毒。

(14)不要打开陌生可疑的邮件。

(15)浏览网页时选择正规的网站。

(16)禁用远程功能，关闭不需要的服务。

2.清除计算机病毒

(1)用防病毒软件清除病毒

计算机一旦感染了病毒,最好立即关闭系统。如果继续使用,会使更多的文件遭受破坏。针对已经感染病毒的计算机.建议使用防病毒软件进行全面杀毒。用防病毒软件消除病毒是当前比较流行的方法。此类软件都具有清除病毒并恢复原有文件的内容的功能。杀毒后，被破坏的文件有可能恢复成正常的文件。对未感染的文件，建议用户打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御。

一般来说，使用杀毒软件是能清除病毒的，但考虑到病毒在正常模式下比较难清理，所以需要重新启动计算机在安全模式下查杀。若遇到比较顽固的病毒可通过下载专杀工具来清除，再恶劣点的病毒就只能通过重装系统来彻底清除!

(2)重装系统并格式化硬盘是最彻底的杀毒方法。

格式化会破坏硬盘上的所有数据，因此，格式化前必须确定硬盘中的数据是否还需要。要先做好备份工作。格式化时一般是进行高级格式化。需要说明的是，用户最好不要轻易进行低级格式化。因为低级格式化是一种损耗性操作，它对硬盘寿命有一定的负面影响。

(3)手工清除方法。

手工清除计算机病毒对技术要求高，需要熟悉机器指令和操作系统，难度比较大，一般只能由专业人员操作。

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