

## 网络安全信息与动态周报

## 一、本周网络安全基本态势（5月10日-5月16日）



本周互联网网络安全态势整体评价为**良**。我国互联网基础设施运行整体平稳，全国范围或省级行政区域内未发生造成重大影响的基础设施运行安全事件。针对政府、企业以及广大互联网用户的主要安全威胁来自于软件高危漏洞、恶意代码传播活动以及网页篡改。依据 CNCERT 抽样监测结果，境内被木马控制的主机 IP 地址数目为 5087 个，与前一周环比增长 12%；境内被僵尸网络控制的主机 IP 地址数目为 6186 个，环比下降 6%；境内被篡改政府网站数量为 81 个，环比下降 35%。

## 本周重点网络安全事件

本周 CNCERT 监测发现，境内被篡改政府网站数量较上周有所下降，个别省部级政府网站位列其中。截至 5 月 17 日 12 时仍未恢复的被篡改的部分地市级以上（含地市级）政府部门网站如下表所示。

被篡改页面 URL	所属部门或地区	级别
<a href="http://jtkx.ahjt.gov.cn/default.asp">http://jtkx.ahjt.gov.cn/default.asp</a>	安徽省	省部级
<a href="http://jsmf.gov.cn/test.asp">http://jsmf.gov.cn/test.asp</a>	江苏省	省部级
<a href="http://scmz.gov.cn/index.htm">http://scmz.gov.cn/index.htm</a>	四川省	省部级
<a href="http://www.xznjw.gov.cn/xznjw_jw.asp">http://www.xznjw.gov.cn/xznjw_jw.asp</a>	西藏自治区	省部级
<a href="http://czqs.gov.cn/index.htm">http://czqs.gov.cn/index.htm</a>	安徽省滁州市	地市级
<a href="http://mjw.luan.gov.cn">http://mjw.luan.gov.cn</a>	安徽省六安市	地市级
<a href="http://jwj.qzlj.gov.cn/index.htm">http://jwj.qzlj.gov.cn/index.htm</a>	福建省泉州市	地市级
<a href="http://www.cdws.gov.cn/bbs/bang.asp">http://www.cdws.gov.cn/bbs/bang.asp</a>	河北省承德市	地市级
<a href="http://zx.zjkqx.gov.cn/default.asp">http://zx.zjkqx.gov.cn/default.asp</a>	河北省张家口市	地市级
<a href="http://www.zhq.gov.cn/1.htm">http://www.zhq.gov.cn/1.htm</a>	河南省平顶山市	地市级
<a href="http://www.sysld.gov.cn/index.htm">http://www.sysld.gov.cn/index.htm</a>	黑龙江省双鸭山市	地市级
<a href="http://xfxc.gov.cn/1.htm">http://xfxc.gov.cn/1.htm</a>	湖北省襄城市	地市级
<a href="http://yhz.xfjt.gov.cn/index.asp">http://yhz.xfjt.gov.cn/index.asp</a>	湖北省襄樊市	地市级
<a href="http://old.xfjt.gov.cn/default.asp">http://old.xfjt.gov.cn/default.asp</a>	湖北省襄樊市	地市级
<a href="http://www.cscdc.gov.cn/index.htm">http://www.cscdc.gov.cn/index.htm</a>	湖南省长沙市	地市级
<a href="http://www.czcl.gov.cn/default.asp">http://www.czcl.gov.cn/default.asp</a>	湖南省郴州市	地市级

被篡改页面 URL	所属部门或地区	级别
http://bbs.syxgt.gov.cn	湖南省邵阳市	地市级
http://zjj315.gov.cn/default.asp	湖南省张家界市	地市级
http://hnzz.gov.cn/index.asp	湖南省株洲市	地市级
http://www.hnzz.gov.cn/default.htm	湖南省株洲市	地市级
http://www.zzslj.gov.cn/1.htm	湖南省株洲市	地市级
http://www.ntgzw.gov.cn/gqxc/yqlj/index.aspx	江苏省南通市	地市级
http://taishankj.gov.cn	山东省泰安市	地市级
http://bledu.gov.cn/neo.txt	陕西省西安市	地市级
http://ltjsj.gov.cn/neo.txt	陕西省西安市	地市级
http://www.cdjustice.chengdu.gov.cn/index.htm	四川省成都市	地市级
http://cdepb.gov.cn/index.htm	四川省成都市	地市级
http://hnmzj.gov.cn/test.asp	浙江省海宁市	地市级
http://shangyu.gov.cn/hex.htm	浙江省上虞市	地市级

## 本周活跃恶意域名

根据 CNCERT 自主监测结果以及各单位报送的信息：1) 近期，黑客注册.CN 域名用于网页挂马的势头有所抬升，且集团化特征明显；2) .xorg.pl 恶意域名组近期在互联网上异常活跃，该组的恶意域名数量高达 100 余个，侵害了我国较多的网站和网站用户。whois 查询结果显示这组域名的注册地在波兰。本周，CNCERT 重点关注的.CN 恶意域名组和.xorg.pl 恶意域名组如下表所示，其中，微软公司（Microsoft）提供了大部份.xorg.pl 的恶意域名信息。

组别	域名列表
.CN 恶意域名	c.nje1.cn、c.vcmart.com.cn、w.ckt4.cn、w.ckt7.cn、w.ckt9.cn、r.jsguangji.cn、r.vcmart.com.cn、r.vesaweb.com.cn、q.ckt9.cn、q.siyu.org.cn、q.ustocn.com.cn、c.ckt9.cn、c.nje2.cn、c.wvg5.cn、w.jsguangji.cn、e.ckt7.cn、q.ckt4.cn
.XORG.PL 恶意域名	haw.xorg.pl、hce.xorg.pl、hea.xorg.pl、hen.xorg.pl、het.xorg.pl、hff.xorg.pl、hfh.xorg.pl、hfj.xorg.pl、hfn.xorg.pl、hfo.xorg.pl、hfq.xorg.pl、hfv.xorg.pl、hgb.xorg.pl、hgi.xorg.pl、hgo.xorg.pl、hgw.xorg.pl、hic.xorg.pl、hip.xorg.pl、hiq.xorg.pl、hiv.xorg.pl、hjb.xorg.pl、hjh.xorg.pl、hjk.xorg.pl、hkb.xorg.pl、hkc.xorg.pl、hkg.xorg.pl、hki.xorg.pl、hkm.xorg.pl、hkq.xorg.pl、hkv.xorg.pl、hkx.xorg.pl、hkz.xorg.pl、hlb.xorg.pl、hlc.xorg.pl、hlf.xorg.pl、hli.xorg.pl、hll.xorg.pl、hlo.xorg.pl、hlt.xorg.pl、hlv.xorg.pl、hlw.xorg.pl、hlx.xorg.pl、hmb.xorg.pl、hmc.xorg.pl、hme.xorg.pl、hmg.xorg.pl、hmi.xorg.pl、hmj.xorg.pl、hmk.xorg.pl、hmm.xorg.pl、hmo.xorg.pl、hmp.xorg.pl、hmr.xorg.pl、hmt.xorg.pl、hmu.xorg.pl、hmv.xorg.pl、hmw.xorg.pl、hmx.xorg.pl、hmy.xorg.pl、hmz.xorg.pl、hna.xorg.pl、hnc.xorg.pl、hnd.xorg.pl、hne.xorg.pl、hnf.xorg.pl、

<p>hnh.xorg.pl、hni.xorg.pl、hnj.xorg.pl、hnk.xorg.pl、hnl.xorg.pl、hnm.xorg.pl、hnn.xorg.pl、hno.xorg.pl、hnp.xorg.pl、hnq.xorg.pl、hnr.xorg.pl、hns.xorg.pl、hnw.xorg.pl、hnx.xorg.pl、hny.xorg.pl、hnz.xorg.pl、hob.xorg.pl、hoc.xorg.pl、hod.xorg.pl、hoe.xorg.pl、hog.xorg.pl、hoi.xorg.pl、hoj.xorg.pl、hok.xorg.pl、hom.xorg.pl、hoo.xorg.pl、hos.xorg.pl、hot.xorg.pl、how.xorg.pl、hoz.xorg.pl、hpb.xorg.pl、hpd.xorg.pl、hpe.xorg.pl、hpf.xorg.pl、hpl.xorg.pl、hpp.xorg.pl、hpq.xorg.pl、hps.xorg.pl、hpt.xorg.pl、hpu.xorg.pl、hqv.xorg.pl、hpx.xorg.pl、hqe.xorg.pl、hqq.xorg.pl、hrb.xorg.pl、hre.xorg.pl、hrg.xorg.pl、hrm.xorg.pl、hrn.xorg.pl、hrq.xorg.pl、vsf.xorg.pl、dav.xorg.pl、ddf.xorg.pl、dvg.xorg.pl、dxb.xorg.pl、hak.xorg.pl、hef.xorg.pl、hgg.xorg.pl、hgm.xorg.pl、hqb.xorg.pl、vsa.xorg.pl、hcb.xorg.pl、hfu.xorg.pl、hih.xorg.pl、neb.xorg.pl</p>
--

注：根据微软、华为、奇虎、知道创宇、启明星辰、安天、东软等公司报送的网页挂马信息整理。



### 本周活跃恶意代码

名称	特点
<b>Hack.Exploit.Script.JS.Agent.ju</b>	该病毒是一段加密病毒脚本，利用 RealPlay 播放器的溢出漏洞下载病毒文件进行执行和传播。病毒会将网页脚本加密成乱码字符，普通用户很难知道这是一段病毒代码。病毒通过调用 RealPlayer 组件，用病毒作者特定 shellcode 溢出，成功之后，就会打开病毒作者的下载地址，下载运行其他病毒。
<b>Trojan.DL.PicFrame.a</b>	这是一个下载者病毒，利用浏览器查看图片文件解析漏洞进行传播。该病毒在 JPG 文件末尾附加了包含恶意网站链接的<iframe><iframe>，由于 iframe 的 width 和 height 都很小，用户极易在未察觉的情况下访问恶意网址。
<b>Trojan.DL.Gifframe.a</b>	这是一个下载者病毒，利用浏览器 GIF 文件解析漏洞进行传播。黑客通过诱导用户浏览含有恶意代码的 GIF 文件的网页，来控制用户连接到特定的包含恶意程序的网页。Windows 图片查看器打开含有恶意代码的 GIF 文件不受影响。
<b>Worm.Win32.MS08-067.c</b>	这是一个以微软系统 MS08-067 漏洞为主要传播手段的蠕虫病毒。另外该病毒亦可通过 U 盘以自动加载运行的方式进行传播、并且由于病毒自身带一个弱密码表，会猜解网络中计算机的登录密码，通过局域网传播。
<b>Hack.Exploit.Script.JS.ShellCode.co</b>	该病毒利用微软 IE 浏览器相关组件的漏洞，构造畸形字符串，使浏览器在解析代码时触发相关漏洞，从而运行有关病毒代码。

注：根据瑞星、金山等企业报送的恶意代码信息整理。

本周，利用操作系统及应用软件漏洞进行传播的恶意代码仍占较高比例。CNCERT 提醒互联网用户一方面要加强系统漏洞的修补加固，另一方面要加装安全防护软件。

## 本周重要安全漏洞

本周，国家信息安全漏洞共享平台（CNVD）整理和发布以下重要安全漏洞信息。

### 1、Microsoft Outlook Express 和 Windows Mail 存在远程执行代码漏洞

Outlook Express 和 Windows Mail 是 Windows 操作系统中默认捆绑的邮件和新闻组客户端。Outlook Express 和 Windows Mail 客户端所使用的通用库验证特制邮件响应的方式存在整数溢出漏洞，如果用户受骗使用 POP3 和 IMAP 邮件协议连接到恶意的服务器并收到畸形的 STAT 响应就会触发上述溢出，导致在用户系统上执行任意代码。微软已于 5 月 11 日发布安全公告（MS10-030）修复了该漏洞，建议尚未安装补丁的用户尽快下载使用。

### 2、Microsoft Visual Basic for Applications 存在远程执行代码漏洞

Microsoft Visual Basic for Applications（VBA）是微软开发出来在其桌面应用程序中执行通用的自动化（OLE）任务的编程语言。在搜索支持 VBA 的文档（如 Office 文档）中的 ActiveX 控件时 VBA 所使用的 VBE6.dll 库中的文本解析代码存在单字节栈溢出漏洞。如果主机应用程序打开一个特制文件并将其传递到 VBA runtime，就会将缓冲区外的值为 0x2E 的单个字节转换为 0x00，成功利用此漏洞的攻击者便可完全控制受影响的系统。微软已于 5 月 11 日发布安全公告（MS10-031）修复了该安全漏洞，建议尚未安装补丁的用户尽快下载使用。

### 3、Adobe Shockwave Player 存在多个远程安全漏洞

Adobe Shockwave Player 是专门播放使用 Director Shockwave Studio 制作的网页的外挂软件。Adobe Shockwave Player 播放器存在多个远程安全漏洞，具体漏洞信息为：Adobe Shockwave Player Director 文件解析非法偏移远程代码执行漏洞、Director 文件分析 ATOM size 无限循环漏洞、Director 文件解析 RCSL 指针覆盖漏洞、Director 文件解析整型溢出漏洞、Adobe Shockwave Player（CVE-2010-1289）未明远程代码执行漏洞、嵌入式字体解析堆溢出漏洞、.dir 文件处理整数溢出漏洞、3D 对象解析内存破坏漏洞、PAMI 块远程代码执行漏洞、Asset Entry 解析内存破坏漏洞等。目前厂商已经发布了升级补丁以修复该安全问题，建议相关用户尽快下载使用。

### 4、Free Download Manager 存在多个缓冲区溢出漏洞

Free Download Manager 是一款支持多线程分割下载的工具。Free Download Manager 存在多个缓冲区溢出漏洞，可导致应用程序崩溃。具体漏洞信息为："Site Explorer"功能中打开文件夹时、"Site Explorer"功能中打开 WEB 站点时、解析 FTP URIs 时、处理重定向时均存在边界错误。目前 Free Download Manager 3.0.Build 852 已经修复了以上漏洞，建议相关用户尽快下载使用。

## 5、MySQL 数据库存在多个安全漏洞

MySQL 是一个小型关系型数据库管理系统。MySQL 数据库存在多个安全漏洞，远程攻击者可以利用漏洞以应用程序权限执行任意代码。具体漏洞信息为：MySQL 在处理 COM\_FIELD\_LIST 命令的表格名称参数时没有正确的执行权限检查，用户对一个表格拥有 DELETE 或 SELECT 权限可以读取或删除其他表格的内容；服务程序在处理攻击者提交的其大小远超过单个报文规定的最大值的报文时存在一个错误，可锁死服务器状态，造成拒绝服务攻击；COM\_FIELD\_LIST 命令报文处理表名参数缺少正确的边界检查，攻击者通过构建一个超长的表名参数传递给 COM\_FIELD\_LIST，可触发缓冲区溢出。目前 MySQL 5.1.47 已经修复了上述漏洞，建议相关用户尽快下载使用。

**小结：**本周，微软公司发布 5 月份安全公告修复了 Windows 邮件系统和 VBA 中的两个严重漏洞、Adobe 公司发布安全公告 APSB10-12 修复了 Adobe Shockwave Player 的 18 个安全漏洞，这些漏洞可被攻击者利用来进行拒绝服务攻击或远程执行任意代码，对我国网民的上网安全造成严重影响。请广大用户尽快下载相关补丁程序，避免受漏洞的影响。

*注：CNVD 是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。*

## 二、业界新闻速递

### 政府监管和政策法规动态

#### 1、工信部整治手机淫秽色情专项行动取得阶段性成果

新华网消息：工业和信息化部自 2009 年 11 月起组织开展的为期 14 个月的整治手机淫秽色情专项行动目前已经取得阶段性成果。具体包括：1) 深入对业务推广渠道、网站接入管理、接入资源层层转租、手机上网代收费、域名实名注册五个手机涉黄关键环节进行整治，实现全面排查、重点治理；2) 完成网站备案系统改造，全速推进各系统建设工作，提升维护网络信息安全的管控能力；3) 完善管理制度建设，实现对互联网信息安全长效管理。工信部有关负责人表示，下一步将继续认真履行行业管理职责，做好基础工作，配合公安等部门完善管理机制，使针对网络不良信息管理的各项措施和手段常态化、制度化，构建健康和谐网络环境，为社会和经济发展做好服务。

#### 2、日本制定信息安全战略，加强网络反黑

中国日报网消息：据日本共同社报道，日本政府 5 月 11 日在信息安全政策会议上正式批准制定“保护国民信息安全战略”。该战略将制定 2010 年至 2013 年具体的实施项目，重点实施当铁路部门、金融机构的电脑系统等重要基础设施遭受黑客攻击时的早期行动演习，以将损失降到最小。日本各中央省厅将根据此统一战略展开联合行动，同时加强与外国政府及民间企业的合作，力争使日本成为信息安全先进国。

### 3、美国网络管制的内容及手段

求是理论网消息：高声宣扬“网络自由”的美国，从未对互联网“疏于”防范和管控。美国一直通过各种途径，对网络实施成熟和有效的监控和管制措施，包括：1) 监控和管制网络信息，维护国家安全；2) 多管齐下，严格监控和管制儿童色情的传播与泛滥；3) 制定了一系列保护知识产权的政策法规保护网络版权；4) 高度重视并研究制定有效的措施以保护计算机安全；5) 垄断着国际互联网的战略资源，并主宰着互联网产业链的关键环节；6) 拥有专门的反黑客部队，并在国际范围内招募黑客精英为其服务；7) 拥有成熟、强大的网络监控手段。

### 4、美将考虑对网络攻击做出军事反应

新华网消息：美国国防部副部长詹姆斯·米勒5月12日表示，美国在遭遇网络攻击的情况下，五角大楼会考虑做出军事反应。詹姆斯·米勒认为，目前还不好界定网络空间的战争行为，网络空间的敌对行为涵盖范围很广，很多行为诸如网络间谍等不代表全面战争；但恐怖分子、犯罪分子等对美国网络空间带来的威胁是真实的，而且在不断增加。

## 网络安全事件与威胁

### 5、临近高考百余家高校网站被挂马

硅谷动力消息：随着高考临近，与高考内容相关的网站成了黑客关注的重点，据悉高考前后一个专业黑客通过挂马网页至少可以获利万元以上。360 安全卫士恶意网页监测数据显示，有关高考的挂马网页正急剧上升，仅5月14日一天，就有包括北大、清华等在内的128家高校网站遭遇挂马。安全专家预计，这股挂马风潮还将持续到高考录取工作结束，建议广大考生和家长在浏览相关信息时，一定要防范木马的入侵，安装必要的杀毒软件和可查杀木马的浏览器。

### 6、“僵尸网络”利用 Web 服务器发起 DoS 攻击

赛迪网消息：Imperva 安全公司近日发现了一种利用 web 服务器发起 DoS 攻击（拒绝服务器攻击）的僵尸网络。该僵尸网络涵盖约 300 个 web 服务器，利用 PHP 语言存在的安全漏洞，发起 DoS 攻击。黑客只是简单的利用单一用户接口，该接口不仅允许攻击者具体指定被攻击者的 IP 地址和端口，而且可以确定攻击时间的长短。Imperva 首席技术主管阿玛柴·舒尔曼（Amachai Shulman）表示，黑客之所以选择 web 服务器而非 PC 进行 DoS 攻击，主要是由于 web 服务器占用带宽较大，仅需很少的“僵尸电脑”就能完成攻击；另外，web 服务器通常不运行防毒软件，可大大降低攻击被发现的机率。

### 7、俄罗斯黑客批量出售 Twitter 帐号

cnBeta 网站消息：据俄罗斯安全研究人员表示，在俄罗斯网络罪犯聚集的论坛里，黑客正将每一个 Twitter 帐号以 100 美元或 200 美元的价格出售给欺诈者和垃圾邮件发送者，价格主要根据被黑的 Twitter 帐号追随者数量而定。由于 Twitter 这类社交圈是基于信任为

基础的，因此用户对于来自信任来源的链接不会有很高的警惕性，通常 10%到 20%的用户会去点击信任来源发送的链接。

## 业界动态

### 8、国际电信联盟成立云计算工作组，制定相关标准

比特网消息：国际电信联盟（ITU）成立“云计算专项工作组”，主要负责制定云计算标准。旨在达成一个“全球性生态系统”，确保各个系统之间安全地交换信息。工作组将对当前的各项标准进行评估，并将推出新的标准。在此之前国际标准化组织和中国也成立由相应的工作组研究云计算标准。国际标准化组织/国际电工委员会、第一联合技术委员会（ISO/IEC、JTC1）成立了分布应用平台服务分技术委员会（SC38），下设云计算研究组；中国组建了云计算标准化产业联盟，开展云计算标准化需求研究。

### 9、谷歌称其街景采集车错误地收集了个人信息

新华网消息：谷歌（Google）5月14日表示，地图服务“街景视图”（Street View）的制图车，因“程序错误”和疏忽在过去的几年间意外搜集了部分用户通过未加密的无线网络（WiFi）传输的私密信息。谷歌街景采集车以拍摄全球各地的街景全景照片而闻名，自2006年以来已在30多个国家收集了信息。谷歌称，公司从未使用过这些私密信息，公司目前正与美国、德国、法国、巴西、中国和中国香港等相关国家和地区的管理部门商议如何处理这些数据。德国负责处理此次事件的负责人 Johannes Caspar 表示，欧盟将成立调查小组负责对此事进行调查，调查结果直接向欧委会汇报，但未透露欧盟官员将采取何种措施应对此事件。谷歌表示，街景采集车以后将不再收集任何 WiFi 数据。

## 关于国家互联网应急中心（CNCERT）

国家互联网应急中心的全称是国家计算机网络应急技术处理协调中心（英文简称是CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

## 联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：刘军

网址：[www.cert.org.cn](http://www.cert.org.cn)

Email：[cncert\\_report@cert.org.cn](mailto:cncert_report@cert.org.cn)

电话：010-82990125

