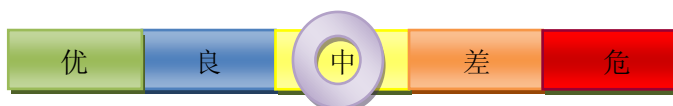




CNCERT互联网安全威胁报告

2011 年 6 月

总第 6 期



摘要：

本报告以 CNCERT 监测数据和通报成员单位报送数据作为主要依据，对我国互联网面临的各类安全威胁进行总体态势分析，并对重要预警信息和典型安全事件进行探讨。

2011 年 6 月，互联网网络安全状况整体评价为中。主要数据如下：

- 境内感染网络病毒的终端数约为815万个；
- 境内被篡改网站数量为3164个，其中被篡改政府网站数量为333个；
- 国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞447个，其中，高危漏洞250个，可被利用来实施远程攻击的漏洞有406个。

热线电话：+8610 82990999（中文），82991000（英文） 传真：+8610 82990399

电子邮件：cncert@cert.org.cn

PGP Key：<http://www.cert.org.cn/cncert.asc>

网址：<http://www.cert.org.cn/>

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 (英文简称为 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。

2003 年，CNCERT 在我国大陆 31 个省、自治区、直辖市成立分中心，完成了跨网络、跨系统、跨地域的公共互联网网络安全应急技术支撑体系建设，形成了全国性的互联网网络安全信息共享、技术协同能力。目前，CNCERT 作为国家互联网安全应急体系的核心技术协调机构，在协调国内网络安全应急组织 (CERT) 共同处理互联网安全事件方面发挥着重要作用。

CNCERT 的业务能力主要包括：

- **监测发现：**依托“863-917 网络安全监测系统”实现网络安全事件的监测发现。863-917 网络安全监测系统是一个全程全网、多层次、多渠道延伸的网络安全综合监测平台，目前已具备对安全漏洞、恶意代码、网页篡改、网页挂马、拒绝服务攻击、域名劫持、路由劫持等各种网络威胁或攻击的监测发现能力。
- **通报预警：**依托对丰富数据资源的综合分析和多渠道的信息获取实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等。此外，按照 2009 年工业和信息化部颁布实施的《互联网网络安全信息通报实施办法》承担通信行业互联网网络安全信息通报工作。
- **应急处置：**依托与运营商、域名注册商、安全服务厂商等相关部门的快速工作机制和与涉及国计民生的重要信息系统部门及执法机关密切合作机制实现网络安全事件的快速处置；同时作为国际著名网络安全合作组织 FIRST 和 APCERT 的重要成员，与多个世界著名的网络安全机构和各个国家级应急组织建立了网络安全事件处理合作机制。面向国内外用户受理网络安全事件报告，及时掌握和处置突发重大网络安全事件。

版权及免责声明

《CNCERT 互联网安全威胁报告》(以下简称“报告”)为国家计算机网络应急技术处理协调中心(简称国家互联网应急中心, CNCERT 或 CNCERT/CC)的电子刊物,由 CNCERT 编制并拥有版权。报告中凡摘录或引用内容均已指明出处,其版权归相应单位所有。本报告所有权利及许可由 CNCERT 进行管理,未经 CNCERT 同意,任何单位或个人不得将本报告以及其中内容转发或用于其他用途。

CNCERT 力争保证本报告的准确性和可靠性,其中的信息、数据、图片等仅供参考,不作为您个人或您企业实施安全决策的依据, CNCERT 不承担与此相关的一切法律责任。

编者按:

感谢您阅读《CNCERT 互联网安全威胁报告》,如果您发现本报告存在任何问题,请您及时与我们联系,来信地址为: cncert@cert.org.cn。

本月网络安全基本态势分析

2011 年 6 月，互联网网络安全状况整体评价为中。我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未发生较大以上网络安全事件。在我国互联网网络安全环境方面，我国境内感染“飞客”蠕虫的主机数量和被篡改政府网站数量、新发现信息系统安全漏洞数量较上月明显增多，但境内感染木马或僵尸程序的主机数量则继续呈下降趋势。总体上，6 月公共互联网网络安全态势较上月有所恶化。

◆ 基础网络安全

2011 年 6 月，我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未出现省级行政区域以上的造成较大影响的基础网络运行故障，未发生较大以上网络安全事件，但存在一定数量的流量不大的针对互联网基础设施实施的拒绝服务攻击事件。

◆ 重要联网信息系统安全

政府网站和金融行业网站仍然是不法分子攻击的重点目标，安全漏洞是重要联网信息系统遭遇攻击的重要内因。本月，监测发现被篡改政府网站数量为 333 个，较上月的 212 个大幅增长 57%，占境内被篡改网站比例由 6.31% 上升到 10.52%；接收的网页仿冒事件报告数量为 381 个，较上月 480 个下降 21%，这些仿冒事件绝大多数都是针对金融机构、电子商务、第三方在线支付网站；此外，“Microsoft Word 文件指针远程代码执行漏洞”、“Xitami HTTP 头远程缓冲区溢出漏洞”、“Opera Web Browser 拒绝服务漏洞”影响较为严重，互联网上已经出现有关攻击代码。

◆ 公共网络环境安全

2011 年 6 月，根据 CNCERT 的监测数据和通信行业报送数据，我国互联网网络安全环境主要指标情况如下：①网络病毒¹活动情况方面，境内感染网络病毒的终端数约为 815 万个，较上月大幅增长 76%；获得新增网络病毒名称 953 个，较上月增长 31%，获得新增网络病毒家族 38 个，较上月大幅增长 65%；各安全企业报送的网络病毒捕获数量总体呈下降趋势，瑞星公司截获的病毒数量较上月减少 5.7%，新增病毒数量比上月减少 42.2%；金山公司报送的计算机病毒事件数量较上月减少 15.7%；安天公司捕获的样本总数较上月减少 10.5%，新增病毒种类较上月增加 14.1%。②网站安全方面，本月境内被篡改网站数量为 3164 个，较上月下降 6%；接收网页仿冒事件报告 381 个，较上月下降 21%；各安全企业报送的网页挂马情况中，奇虎 360 公司、安天公司、浪潮公司报送的网页挂马事件数量较上月均呈现上升趋势，分别上升了 2.8%、12.4%、27.1%，但金山公司和网御星云公司报送的网页挂马事件数量较上月有所下降，降幅分别为 19.7% 和 13%。③安全漏洞方面，国家信息安全漏洞共享平台（CNVD²）收集整理信息系统安全漏洞 447 个，较上月增长 23%，其中高危漏洞 250 个，可被利用来实施远程攻击的漏洞有 406 个。④垃圾邮件方面，从中国互联网协会反垃圾邮件中心报送数据看，本月共接收 11164 件垃圾邮件事件举报，较上月下降 31%。⑤事件受理方面，CNCERT 接收到网络安全事件报告 1344 件，数量较上月增长 2%。

注1：一般情况下，恶意代码是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。其中，网络病毒是特指有网络通信行为的恶意代码。6 月，CNCERT 在对网络病毒进行抽样监测时，对 177 种木马家族和 65 种僵尸程序家族进行了抽样监测。

注2：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。

◆ 网络病毒监测数据分析

2011 年 6 月，境内感染网络病毒的终端数约为 815 万个。其中，境内被木马或僵尸程序控制的主机 IP 约为 38 万个，环比下降 6%；境内感染飞客蠕虫的主机 IP 约为 777 万个，环比大幅增长 84%；

➤ 木马僵尸网络监测数据分析

2011 年 6 月，CNCERT 监测发现境内约 38 万个 IP 地址对应的主机被木马或僵尸程序控制，按地区分布感染数量排名前三位的分别是江苏省、广东省、山东省。

木马或僵尸网络控制服务器 IP 总数为 31507 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 24662 个；境外木马或僵尸网络控制服务器 IP 数量为 6845 个，按国家或地区分布数量排名前三位的分别为日本、美国、韩国。

➤ 飞客蠕虫监测数据分析

2011 年 6 月，CNCERT 监测到全球互联网约 4256 万个主机 IP 地址感染飞客蠕虫，按国家或地区分布感染数量排名前三位的分别是中国大陆、巴西、俄罗斯。

境内感染飞客蠕虫的主机 IP 约为 777 万个，按地区分布感染数量排名前三位的分别是广东省、浙江省、江苏省。

➤ 恶意代码捕获和传播情况

2011 年 6 月，CNCERT 通过多种渠道获得新增网络病毒名称数为 953 个，新增网络病毒家族数为 38 个。网络病毒主要针对一些防护比较薄弱，特别是访问量较大的网站通过网页挂马的方式进行传播。当存在安全漏洞的用户主机访问了这些被黑客挂马的网站后，会经过多级跳转暗中连接黑客最终“放马”的站点下载网络病毒。这些放马站点是网络病毒散播的源头，是黑色地下产业链中非常重要的一个环节。2011 年 6 月，CNCERT 监测发现排名前五的活跃放马站点域名和活跃放马站点 IP 如表 1 所示。

表 1： 2011 年 6 月活跃放马站点域名和 IP

排序	活跃放马站点域名	排序	活跃放马站点 IP
1	dd.qzgsl.com	1	218.93.205.238
2	v.avpic.net	2	174.127.96.29
3	www.be92ew.com	3	121.10.107.78
4	Ea.510xy.Com	4	121.11.76.58
5	471.tzwxr.info	5	121.12.168.129

网络病毒在传播过程中,往往需要利用黑客注册的大量域名。根据 CNCERT 对活跃恶意域名的分类跟踪,2011 年 6 月,活跃恶意域名所属顶级域名及地理分布情况如表 2 所示,绝大多数恶意域名分布在极少数的顶级域名上;活跃恶意域名在域名服务机构的注册情况如图 1 所示,请各域名服务机构注意加强域名服务的安管理和域名滥用处理。特别是,由于不法分子为降低传播网络病毒的成本往往申请大量的免费域名,所以免费域名服务机构更需加强有关工作。

表 2： 2011 年 6 月活跃恶意域名所属顶级域名及地理分布

排序	顶级域名 (TLD)	顶级域名地理位置
1	.info	通用顶级域名 (gTLD)
2	.com	通用顶级域名 (gTLD)
3	.tk	托克劳群岛
4	.org	通用顶级域名 (gTLD)
5	.net	通用顶级域名 (gTLD)

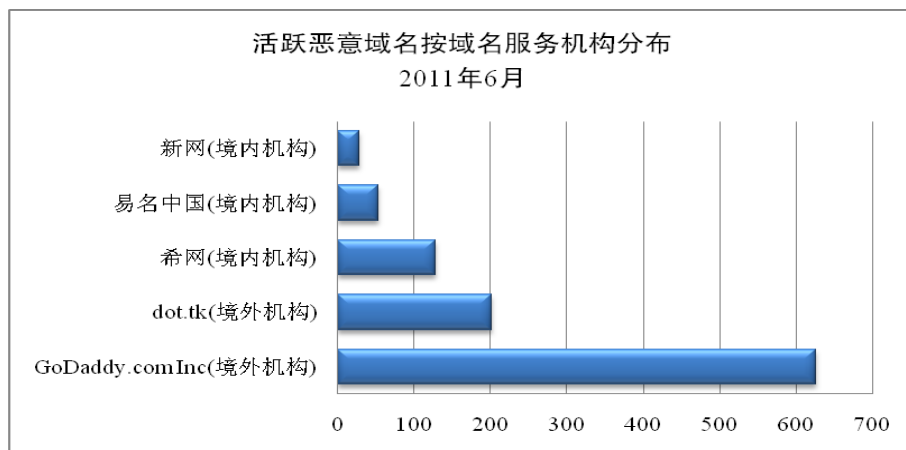


图 1：活跃恶意域名按域名服务机构分布

◆ 网站安全情况分析

➤ 境内网站被篡改情况

2011 年 6 月，境内被篡改网站的数量为 3164 个，其中代号为“soojoy”、“twy”和“s4r4d0”的攻击者对境内网站进行了大量篡改。

境内被篡改网站数量按地区分布排名前三位的分别是北京市、广东省、福建省。按网站类型统计，被篡改数量最多的是.com 和.com.cn 域名类网站，其多为商业类网站；值得注意的是，被篡改的.gov.cn 域名类网站有 333 个，占境内被篡改网站的比例为 10.52%。

截至 6 月 30 日仍未恢复的部分被篡改政府网站³如表 3 所示。

表 3：截至 6 月底仍未恢复的部分政府网站

被篡改网站	所属部门或地区
gysfj.gov.cn	安徽省亳州市
www.dzlsj.gov.cn	安徽省池州市
zgsxsf.gov.cn	安徽省淮北市
www.pljc.gov.cn	甘肃省平凉市
www.tsqs.gov.cn	甘肃省天水市
wp.pingguo.gov.cn	广西自治区百色市
www.zhenyuan.gov.cn	贵州省黔东南苗族侗族自治州
al.yanlingagri.gov.cn	河南省许昌市
www.qgnnet.gov.cn	黑龙江省绥化市
www.hlwangkui.gov.cn	黑龙江省绥化市
www.muyun.gov.cn	湖南省长沙市
fg.shimen.gov.cn	湖南省常德市
www.smr dw.gov.cn	湖南省常德市
wh.shimen.gov.cn	湖南省常德市
argtzy.gov.cn	湖南省郴州市
lxx.rc.gov.cn	湖南省郴州市

注3：政府网站是指英文域名以“.gov.cn”结尾的网站，但不排除个别非政府部门也使用“.gov.cn”的情况。表格中仅列出了被篡改网站或被挂马网站的域名，而非具体被篡改或被挂马的页面 URL。

被篡改网站	所属部门或地区
www.yz110.gov.cn	湖南省郴州市
hnxgtj.gov.cn	湖南省衡阳市
law.bjzf.gov.cn	湖南省湘西州
jjd.xx.gov.cn	湖南省湘西自治州
huji.gov.cn	江苏省南通市
www.ta.gov.cn	江苏省扬州市
8.shicheng.gov.cn	江西省赣州市
www.ydpop.gov.cn	江西省赣州市
www.yugan.gov.cn	江西省上饶市
www.zbjr.gov.cn	山东省淄博市
www.chinaqx.gov.cn	山西省长治市
www.stats-hq.gov.cn	山西省忻州市
www.sxly.gov.cn	山西省运城市
www.dyysj.gov.cn	四川省成都市
www.xjbhdj.gov.cn	新疆自治区巴州
www.xjzepu.gov.cn	新疆自治区喀什地区
www.yrjy.gov.cn	云南省楚雄州
zjjiasan.lss.gov.cn	浙江省嘉兴市
www.smly.gov.cn	浙江省台州市

➤ 境内网站被挂马情况

根据 CNCERT 监测和通信行业报送数据，截至 6 月 30 日仍存在被挂马或被植入不正当广告链接（如：网络游戏、色情网站链接）的部分政府网站如表 4 所示。

表 4：截至 6 月底仍存在挂马的部分政府网站

被挂马网站	所属部门或地区
www.ahgtt.gov.cn	安徽省
www.hlfire.gov.cn	黑龙江省
www.miisd.gov.cn	山东省
www.zxj.gov.cn	浙江省
www.ngzx.gov.cn	安徽省宁国市
www.whfdc.gov.cn	安徽省芜湖市
www.dna.gov.cn	海南省儋州市

被挂马网站	所属部门或地区
www.dingzhou.gov.cn	河北省定州市
www.dzs.gov.cn	河北省定州市
www.qhdinfo.gov.cn	河北省秦皇岛市
www.aqzy.gov.cn	黑龙江省安庆市
www.jlcc.gov.cn	吉林省吉林市
www.jkrlj.gov.cn	江苏省镇江市
www.asfdc.gov.cn	辽宁省鞍山市
www.sqjwc.asga.gov.cn	辽宁省鞍山市
www.hldsafety.gov.cn	辽宁省葫芦岛市
www.tlgtj.gov.cn	辽宁省铁岭市
www.dyxjxy.rz.gov.cn	山东省日照市
www.zcrsrc.gov.cn	山东省诸城市
www.yafc.gov.cn	陕西省延安市
www.dyaj.gov.cn	四川省德阳市
www.wrf.gov.cn	新疆维吾尔自治区乌鲁木齐市
www.hzxhjcy.gov.cn	浙江省杭州市

◆ 网络安全的主要威胁

近期披露的一些严重安全漏洞是互联网所面临的主要安全威胁。2011 年 6 月，国家信息安全漏洞共享平台 (CNVD) 收集整理信息系统安全漏洞 447 个。其中，高危漏洞 250 个，可被利用来实施远程攻击的漏洞有 406 个。受影响的软硬件系统厂商包括 Adobe、Apple、Cisco、Google、IBM、Linux、Microsoft、Mozilla、Novell 等。

根据漏洞影响对象的类型，漏洞可分为操作系统漏洞、应用程序漏洞、WEB 应用漏洞、数据库漏洞、网络设备漏洞（如路由器、交换机等）和安全产品漏洞（如防火墙、入侵检测系统等）。本月 CNVD 收集整理的漏洞中，按漏洞类型分布排名前三位的分别是应用程序漏洞、WEB 应用漏洞、操作系统漏洞。

本月，“Microsoft Word 文件指针远程代码执行漏洞”、“Xitami HTTP 头远程缓冲区溢出漏洞”、“Opera Web Browser 拒绝服务漏洞”影响较为严重，互联网上已经出现有关攻击代码，为避免受到漏洞影响，请广大用户及时采取补丁修复、提高主机操作系统安全防范等级等防御措施。

本月网络安全事件接收与处理情况

◆ 事件接收情况

2011 年 6 月 , CNCERT 收到国内外通过电子邮件、热线电话、网站提交、传真等方式报告的网络安全事件 1344 件 (合并了通过不同方式报告的同一网络安全事件 , 且不包括扫描和垃圾邮件类事件) , 其中来自国外的事件报告有 155 件。

在 1344 件事件报告中 , 排名前三位的安全事件分别是漏洞、网页仿冒、恶意代码。

◆ 事件处理情况

对国内外通过电子邮件、热线电话、传真等方式报告的网络安全事件 , 以及自主监测发现的网络安全事件 , CNCERT 每日根据事件的影响范围和存活性、涉及用户的性质等因素 , 筛选重要事件进行协调处理。

2011 年 6 月 , CNCERT 总部以及各省分中心共同协调处理了 882 件网络安全事件。各类事件处理数量中漏洞和恶意代码类事件处理数量较多 , 本月网页仿冒和网页篡改类事件也是处置的重点。

◆ 本月网络安全重点事件

开展木马和僵尸网络专项处置行动

为营造建党 90 周年庆祝活动的良好网络环境 , 6 月 22 日 , CNCERT 组织基础电信运营企业以及域名服务机构开展了一次木马和僵尸网络专项处置行动。本次专项要求基础电信运营企业及时通知僵尸网络控制端 IP 的相关用户完成主机病毒清理 , 对不配合的、无法联系的则暂停接入 24 个小时 , 同时对涉嫌大规模传播网络病毒的恶意域名要求立即停止域名解析。至 6 月 23 日上午 10 时 , 中国电信、中国联通反馈完成全部 47 个 IP 的处置 , 境内域名服务机构希网网络、易名中国、新网数码、万网志成、花生壳、新网互联、三五互联、江

苏邦宁、爱民网完成全部 170 个域名的处置。

开展高校网站安全专项保障行动

6 月，随着全国高等院校招生工作的陆续展开，高等院校网站成为考生及家长重点关注的网站。根据工作部署，CNCERT 组织开展高校网站安全专项保障行动，重点监测针对高校网站的网页挂马和网页篡改事件，同时组织通信行业通报工作成员单位报送自主发现的高校网站安全事件。CNCERT 共向相关主管部门以及教育网管理部门通报 50 起高校网站安全事件，其中涉及南京大学、北京交通大学、南开大学、厦门大学、中国矿业大学、云南大学、中南大学、华侨大学、暨南大学等多所部属或省属重点高校。

通报处理重要用户感染飞客蠕虫事件

自 2009 年以来在中国大陆地区大肆传播的飞客蠕虫至今仍在活跃，CNCERT 持续对其感染我国政府和重要信息系统部门主机系统的情况进行监测。6 月中旬，根据监测结果，CNCERT 向某重要部门通报了 11 起重要用户感染飞客蠕虫的事件，并提供处置技术支援。根据当前监测情况，飞客蠕虫危害情况仍需引起各部门、各单位的高度重视。

针对黑客组织“LulzSec”的全球攻击加强我国政府网站的漏洞处置

6 月，CNCERT 密切关注国外黑客组织“LulzSec”对全球政府部门网站的攻击情况，并与境外网络安全组织相互协作，加强我国政府部门网络安全事件的处置。6 月 28 日，根据澳大利亚 CERT 组织的通报，CNCERT 协调多个分中心对涉及 www.shuangliu.gov.cn、www.ykzzb.gov.cn、jsfgj.yeda.gov.cn、www.investhg.gov.cn、www.ahshx.gov.cn、www.ccpitzj.gov.cn 等多个境内政府部门网站存在的 SQL 注入等漏洞事件进行了验证和处置。同时，上述事件也对我国政府部门网站安全提出重要警示。

与 Phishlabs 密切协作严厉打击恶意代码传播活动

6 月 CNCERT 监测发现，某 IP 地址的主机长期被控制用于大规模传播恶意代码。其中，黑客还在 .info 域名上大量注册二级动态域名，通过域名传播大量恶意 URL。6 月 27 日，CNCERT 将有关情况通报国外网络安全组织 Phishlabs。Phishlabs 对相关域名进行了技术跟踪，至 7 月 1 日完成了 144 个恶意域名的处置，有力地打击了黑客传播恶意代码的势头。

域名系统软件 BIND 9 存在安全漏洞

6 月，CNVD 获知域名解析服务器软件 BIND 9 披露的一个中危漏洞，该漏洞可用于发起远程攻击，在特定条件下会导致采用 BIND 9 软件的递归服务器拒绝服务。受影响的 BIND 9 版本包括：9.4-ESV-R3 及之后版本、9.6-ESV-R2 及之后版本、9.6.3、9.7.1 及之后版本、9.8.0 及之后版本，其中 9.6.2-P3 不受影响。CNVD 建议升级 BIND 软件版本到 9.4-ESV-R4-P1、9.6-ESV-R4-P1、9.7.3-P1、9.8.0-P2 等已知安全版本。

网站内容管理系统软件 TurboCMS 存在安全漏洞

根据中国电力科学研究院信息安全实验室报告，CNVD 获知北京泰得文通科技有限公司生产的 TurboCMS Java 内容管理系统存在四个安全漏洞，这些漏洞可被利用发起钓鱼攻击或窃取敏感信息，严重的可被利用获得系统管理员权限及网站管理控制权限。根据泰得文通公司提供的客户信息，一些中央企业、电力系统单位、地方政府部门和金融机构采用了该版本软件。但根据 CNVD 检测结果以及泰得文通公司提供的项目实施情况，上述部门对其系统后台访问权限均进行了限制，未对互联网用户开放，暂未发现可利用的攻击入口。截止 6 月底，泰得文通公司已发布其中三个漏洞的升级补丁，并将于 7 月中旬发布最后一个漏洞的升级补丁。在补丁发布前，建议相关单位加强内部用户访问情况的审计，防范可能存在的内部攻击或通过内部局域网发起的跳板攻击情况。

H3C ER 系列路由器存在安全漏洞

6 月，CNVD 获知杭州华三通信技术有限公司（简称华三公司）生产的 H3C ER 系列企业级路由器存在验证绕过漏洞，攻击者可以利用漏洞发起远程攻击，查看系统配置等敏感信息，甚至可修改配置，重启设备，对相关企业、个人用户网络安全构成威胁。根据华三公司公布的信息，该系列产品主要用于以太网/光纤/ADSL 接入的 SMB 市场和政府、企业机构、网吧等网络环境。截止 6 月 24 日，华三公司仍无法提供技术细节，也未明确漏洞补丁具体发布时间及如何做好客户应急服务的计划。CNVD 建议各相关单位和用户自行联系华三公司，要求其提供补丁或解决方案；同时加强对路由器访问的安全策略，只允许系统管理员使用的 IP 访问后台管理界面。

新浪微博跨站漏洞被利用大量传播恶意链接事件

2011 年 6 月 28 日晚 9 时许，许多新浪微博用户在其微博页面上收到附有恶意链接的私信，且在短时间内呈迅速蔓延之势。根据 CNVD 监测情况，该事件是新浪微博网站页面存在的跨站漏洞被黑客利用、通过恶意代码发起钓鱼攻击引起。截至 6 月 29 日 16 时，CNVD 向新浪公司确认了漏洞情况并验证其相关页面的跨站漏洞已经修复。由于微博这一互联网社交网络的特殊性，该漏洞被用于发起的钓鱼攻击效果被迅速放大，进而造成了广泛的影响。此次事件还体现了互联网黑色地下产业由破坏性转向趋利性的特点。CNVD 建议各微博网站应以此为鉴，加强对注入、跨站、信息泄露等常见的、可利用的网站安全漏洞的自查；加强与国内外域名注册机构、基础电信运营企业、网络安全组织的协作，坚决清除黑客传播非法内容、发起钓鱼攻击使用的恶意域名和主机 IP；加强行业自律，提高用户安全意识。

网赢企业网络营销平台存在高危安全漏洞

CNVD 获知广东天拓资讯科技有限公司（简称天拓公司）旗下产品网赢企业网络营销平台存在 SQL 注入漏洞。攻击者可以利用漏洞发起远程攻击，取得网站管理操作权限，甚至获得网站服务器主机管

理权限。根据天拓公司官方网站公布的客户列表，该产品用户包括国内保险、证券、银行、民航、家电、体育、消费品、电子商务等行业知名企业。CNVD 联系天拓公司后其仍未能按 CNVD 处置流程要求提供技术细节，也未能明确漏洞修补时间以及如何做好客户应急服务的计划。CNVD 建议相关用户自行联系天拓公司，要求其针对漏洞情况提供临时解决方案；相关用户也可以自行对网站进行 web 常规漏洞的检测，对存在 SQL 注入漏洞的 URL 进行参数过滤。

协调处置多起仿冒银行网站的钓鱼事件

6 月，CNCERT 对自主监测和投诉受理工作中发现的多起仿冒银行网站的钓鱼事件进行了处置，分别涉及建设银行、工商银行、农业银行、兴业银行、香港银行等。这些钓鱼网站使用了极具迷惑性的域名对上述银行网站进行仿冒，对用户帐户安全构成严重威胁。经验证分析，CNCERT 协调仿冒域名所属的境内外注册机构，暂停了仿冒域名的解析服务。

协调处置多起仿冒韩国政府部门网站的事件

6 月，CNCERT 接到韩国网络安全组织投诉，称在境内注册的域名为 seoulspok.net 的网站仿冒韩国警察厅网站，域名为 cybspob.com、cybspob.net、cybspok.com、cybspok.net 和 cyspo.com 的网站仿冒韩国法院网站，对韩国政府的声誉和民众获取真实信息的渠道构成威胁。经验证核实后，CNCERT 协调域名注册机构西部数据公司暂停了被举报的全部仿冒域名的解析服务。

协调处理仿冒赛尔网络公司的事件

6 月 20 日，CNCERT 接到中国教育网应急组织（CCERT）举报，称域名为 www.saier13800.com 的网站仿冒中国教育和科研计算机网主办的赛尔网络公司网站，对广大教育网用户安全构成威胁。经验证核实后，CNCERT 协调境内域名服务机构江苏邦宁公司，暂停了被举报的仿冒域名的解析服务。

附：术语解释

● 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

● 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

● 恶意代码

恶意代码是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。恶意代码分类说明如下：

1. 特洛伊木马 (Trojan Horse)

特洛伊木马 (简称木马) 是以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意代码。由于它像间谍一样潜入用户的电脑，与战争中的“木马”战术十分相似，因而得名木马。按照功能，木马程序可进一步分为：盗号木马⁴、网银木马⁵、窃密木马⁶、远程控制木马⁷、流量劫持木马⁸、下载者木马⁹和其它木马六类。

2. 僵尸程序 (Bot)

僵尸程序是用于构建大规模攻击平台的恶意代码。按照使用的通信协议，僵尸程序可进一步分为：IRC 僵尸程序、Http 僵尸程序、P2P 僵尸程序和其它僵尸程序四类。

3. 蠕虫 (Worm)

蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的

注4：盗号木马是用于窃取用户电子邮箱、网络游戏等账号的木马。

注5：网银木马是用于窃取用户网银、证券等账号的木马。

注6：窃密木马是用于窃取用户主机中敏感文件或数据的木马。

注7：远程控制木马是以不正当手段获得主机管理员权限，并能够通过网络操控用户主机的木马。

注8：流量劫持木马是用于劫持用户网络浏览的流量到攻击者指定站点的木马。

注9：下载者木马是用于下载更多恶意代码到用户主机并运行，以进一步操控用户主机的木马。

恶意代码。按照传播途径，蠕虫可进一步分为：邮件蠕虫、即时消息蠕虫、U 盘蠕虫、漏洞利用蠕虫和其它蠕虫五类。

4. 病毒 (Virus)

病毒是通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的恶意代码。

5. 其它

上述分类未包含的其它恶意代码。

随着黑客地下产业链的发展，互联网上出现的一些恶意代码还具有上述分类中的多重功能属性和技术特点，并不断发展。对此，我们将按照恶意代码的主要用途参照上述定义进行归类。

- 僵尸网络

僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为，如同时对某目标网站进行分布式拒绝服务攻击，或发送大量的垃圾邮件等。

- 拒绝服务攻击

拒绝服务攻击是向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

- 网页篡改

网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

- 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人秘密信息（如银行帐号和帐户密码）。

- 网页挂马

网页挂马是通过在网页中嵌入恶意代码或链接，致使用户计算机在访问该页面时被植入恶意代码。

- 垃圾邮件

垃圾邮件是将不需要的消息（通常是未经请求的广告）发送给众多收件人。

包括：(一)收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；(二)收件人无法拒收的电子邮件；(三)隐藏发件人身份、地址、标题等信息的电子邮件；(四)含有虚假的信息源、发件人、路由等信息的电子邮件。

- 域名劫持

域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假 IP 地址或使用户的请求失败。

- 非授权访问

非授权访问是没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序 (Exploit) 来获取信息系统访问权限。

- 路由劫持

路由劫持是通过欺骗方式更改路由信息，以导致用户无法访问正确的目标，或导致用户的访问流量绕行黑客设定的路径，以达到不正当的目的。