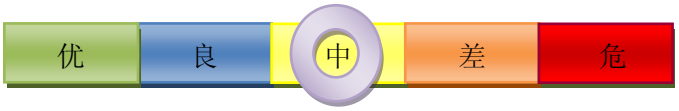
CNCERT/CC
国家互联网应急中心

CNCERT互联网安全威胁报告

2012 年 10 月　　总第 22 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。

2012 年 10 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为550万余个；
- 境内被篡改网站数量为1898个，其中被篡改政府网站数量为151个；境内被植入后门的网站数量为7366个，其中政府网站有380个；针对境内网站的仿冒页面数量为10347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洞665个，其中，高危漏洞237个，可被利用来实施远程攻击的漏洞有606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

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

2012 年 10 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，除我国境内感染“飞客”蠕虫的主机数量和被篡改网站数量、新发现信息系统安全漏洞数量较上月有所下降外，其他各类网络安全事件数量均有不同程度的增长。总体上，10 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

2012 年 10 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主要内因。本月，监测发现境内被篡改政府网站数量为 151 个，较上月的 186 个下降 18.8%，占境内被篡改网站比例由 8.9%减少到 8.0%；境内被植入后门的政府网站数量为 380 个，较上月的 270 个增长 40.7%，占境内被植入后门网站比例则由 6.2%减少到 5.2%；针对境内网站的仿冒页面数量为 10347 个，较上月的 1375 个大幅增长 652.5%，这些仿冒页面绝大多数是仿冒我国金融机构和著名社会机构。

本月，国家信息安全漏洞共享平台（CNVD[1]）共协调处置了共协调处置了 39 起涉及我国政府部门以及银行、民航等重要信息系统部

注1：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。

门以及电信、传媒、公共卫生、教育等相关行业的漏洞事件。这些事件大多数是网站程序存在 SQL 注入、弱口令以及权限绕过等漏洞，也有部分是信息系统采用的应用软件存在漏洞，可能导致获取后台系统管理权限、信息泄露、恶意文件上传等危害，甚至会导致主机存在被不法分子远程控制的风险。此外，“FirePass SSL VPN 'refreshURL' 参数 URI 重定向漏洞”、“VAM Shop SQL 注入漏洞”、“QQ Player 'quartz.dll'堆缓冲区溢出漏洞”、“BSW Gallery 'uploadpic.php'任意文件上传漏洞”等 0day 漏洞影响较为严重，互联网上已经出现针对上述漏洞的攻击代码。

◆ 公共网络环境安全

2012 年 10 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[2]活动情况方面，境内感染网络病毒的终端数为 550 万余个，较上月大幅增长 52.8%，这主要是由于 CNCERT 于 9 月底扩大了木马和僵尸程序的监测范围；在捕获的新增网络病毒文件[3]中，按网络病毒名称[4]统计新增 522 个，较上月增长 44.6%，按网络病毒家族[5]统计新增 5 个，较上月增加 1 个；各安全企业报送的网络病毒捕获数量中，瑞星公司截获的病毒数量较上月下降 38.8%，新增病毒数量较上月大幅增长 194.5%；安天公司捕获的样本总数较上月下降 0.8%，新增病毒种类较上月下降 30.8%；金山公司报送的计算机病毒事件数量较上月大幅增长 644.6%。②网站安全

注2：一般情况下，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。10 月，CNCERT 在对恶意代码进行抽样监测时，对 405 种木马家族和 85 种僵尸程序家族进行了抽样监测。

注3：网络病毒文件是网络病毒的载体，包括可执行文件、动态链接库文件等，每个文件都可以用哈希值唯一标识。

注 4：网络病毒名称是通过网络病毒行为、源代码编译关系等方法确定的具有相同功能的网络病毒命名，完整的命名一般包括：分类、家族名和变种号。一般而言，大量不同的网络病毒文件会对应同一个网络病毒名称。

注 5：网络病毒家族是具有代码同源关系或行为相似性的网络病毒文件集合的统称，每个网络病毒家族一般包含多个变种号区分的网络病毒名称。

方面，本月境内被篡改网站数量为 1898 个，较上月下降 9.4%；境内被植入后门的网站数量为 7366 个，较上月大幅增长 70.0%；针对境内网站的仿冒页面有 10347 个，较上月大幅增长 652.5%；各安全企业报送的网页挂马情况中，浪潮公司报送的网页挂马事件数量较上月下降 20.8%，安天公司报送的网页挂马事件数量与上月持平，奇虎 360 公司报送的网页挂马事件较上月大幅增长 415.5%。③安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 665 个，较上月下降 2.5%。其中高危漏洞 237 个，较上月增长 7.2%；可被利用来实施远程攻击的漏洞有 606 个，较上月下降 4.9%。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 6702 件垃圾邮件事件举报，较上月增长 43.0%。⑤事件受理方面，CNCERT 接收到网络安全事件报告 1729 件，较上月增长 12.2%。数量最多的分别是网页仿冒类事件 770 件、漏洞类事件 699 件。

本月重点网络安全信息

◆ 发现开源邮件服务软件 Exim 存在高危漏洞

10 月 26 日，CNVD 收录了一款互联网上应用广泛的开源邮件服务软件 Exim 存在的一个高危漏洞（CNVD-2012-15485），攻击者利用漏洞可以发起针对邮件服务器的远程攻击，构成信息泄露和运行安全风险。

Exim 是由英国剑桥大学的研究组织开发的一款开源邮件服务软件，主要用于搭建邮件服务器或用作接收和发送邮件的客户端代理程序。该软件由于配置简单，功能灵活，可运行于大多数类 UNIX 系统上,如：Solaris、AIX、Linux 等，近年来在国内外应用较为广泛。漏洞存在于 Exim 默认安装下集成启用的用于支持 DKIM（域名密钥识邮件标准）的功能模块中，由于该模块未能正确处理相应参数，存在堆缓冲区溢出漏洞。攻击者可以向服务器发起远程攻击，严重的可以获得服务器主机管理权限。受影响的软件版本包括 Exim 4.7x 以及 Exim 4.80 版本。

在该漏洞公告披露前，CNCERT/CNVD 获知了漏洞安全补丁即将发布的情况，并对互联网上安装使用 Exim 的服务器进行技术探测。截至 26 日 16 时的探测结果显示，有 4249 个域名对应的 5943 个服务器 IP 采用 Exim，将受到漏洞的直接威胁：按版本区分，4.72、4.80、4.69 版本使用数量排前三位；按服务器 IP 所在国家或地区分，位于中国、俄罗斯、美国的数量排前三位；按顶级域名分，.ru、.com、.net 的域名数量排前三位，其中.cn 域名的有 8 个。

Exim 开发组织在披露信息的同时提供了用于修复漏洞的软件升级版本——Exim 4.80.1。CNCERT 建议相关用户及时下载软件最新版本，完成可用性测试后做好升级部署。如因业务关系暂时无法升级的，可以通过临时禁用支持 DKIM 功能来防范漏洞攻击威胁。

◆ CNCERT 组织开展恶意程序专项打击行动

10 月 26 日至 10 月 31 日，根据工业和信息化部《木马和僵尸网络监测与处置机制》，CNCERT 组织 31 个省分中心开展了一次木马和僵尸网络专项处置行动。本次专项处置主要对危害较大的远控类木马、僵尸程序控制服务器 IP 地址和受控主机 IP 地址进行了打击，共处置完成控制服务器 IP 地址 108 个和受控主机 IP 地址 1174 个，各项处置率分别达到 95.58%和 86.39%。

本月网络安全主要数据

◆ 网络病毒监测数据分析

2012 年 10 月，境内感染网络病毒的终端数为 550 万余个。其中，境内被木马或僵尸程序控制的主机 IP 为 290 万余个，环比大幅增长 369.8%，这主要是由于 CNCERT 于 9 月底扩大了木马和僵尸程序的监测范围；境内感染飞客蠕虫的主机 IP 为 260 万余个，环比下降 12.8%。

➢ *木马僵尸网络监测数据分析*

2012 年 10 月，CNCERT 监测发现境内 290 万余个 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广东省、山东省、江苏省。

木马或僵尸网络控制服务器 IP 总数为 59139 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 25923 个，按地区分布数量排名前三位的分别为广东省、江苏省和浙江省。境外木马或僵尸网络控制服务器 IP 数量为 33216 个，主要分布于摩洛哥、美国、印度。其中，位于美国的控制服务器控制了境内 1938926 个主机 IP，控制境内主机 IP 数量居首位，其次是位于德国和瑞士的 IP 地址，分别控制了境内 334797 个和 137739 个主机 IP。

➢ *飞客蠕虫监测数据分析*

2012 年 10 月，CNCERT 监测到全球互联网 2182 万余个主机 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、印度。

境内感染飞客蠕虫的主机 IP 为 260 万余个，按地区分布感染数量排名前三位的分别是广东省、江苏省、浙江省。

➢ *网络病毒捕获和传播情况*

CNCERT 捕获了大量新增网络病毒文件，其中按网络病毒名称统计新增 522 个，按网络病毒家族统计新增 5 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。2012 年 10 月，CNCERT 监测发现排名前十的活跃放马站点域名和活跃放马站点 IP 如表 1 所示。

表 1： 2012 年 10 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	www.2sidks.com	1	113.107.108.5
2	download.cpudln.com	2	220.181.19.75
3	hn.cnysfl.com	3	173.208.198.210
4	down1.chedan8.com	4	122.224.8.109
5	www.flggcm.com	5	117.21.227.119
6	msn.xuexue123.com	6	142.4.101.140
7	dl.bj-gct.com	7	60.191.143.116
8	www.tssgdam.com	8	173.208.202.196
9	wsdl13.yunpan.cn	9	60.190.218.167
10	hardertolocate.ru	10	122.226.167.20

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。2012 年 10 月，CNCERT 监测发现的放马站点中，通过域名访问的共涉及有 990 个域名，通过 IP 直接访问的共涉及有 433 个 IP。在 990 个放马站点域名中，于境内注册的域名数为 186 个（约占 18.8%），于境外注册的域名数为 646 个（约占 65.2%），未知注册商所属境内外信息的有 158 个（约占 16.0%）。放马站点域名所属顶级域名排名前 5 位的具体情况如表 2 所示。

表 2： 2012 年 10 月活跃恶意域名所属顶级域名

排序	顶级域名（TLD）	类别	恶意域名数量
1	.COM	通用顶级域名（gTLD）	553
2	.INFO	通用顶级域名（gTLD）	104
3	.CN	中国顶级域名（ccTLD）	61
4	.NET	通用顶级域名（gTLD）	59
5	.KR	韩国顶级域名（ccTLD）	46

◆ 网站安全数据分析

➢ *境内网站被篡改情况*

2012 年 10 月，境内被篡改网站的数量为 1898 个，与上月的 2095 个相比下降 9.4%，其中代号为“D.H.T”、“NoEntryPhc”和“ZoRRoKiN”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福建省、北京市、广东省。按网站类型统计，被篡改数量最多的是 COM 域名类网站，其多为商业类网站；值得注意的是，被篡改的 GOV 域名类网站有 151 个，占境内被篡改网站的比例为 8.0%。

截至 10 月 31 日仍未恢复的部分被篡改政府网站[6]如表 3 所示。

表 3： 截至 10 月 31 日仍未恢复的部分政府网站

被篡改网站	所属部门或地区
zgsxsf.gov.cn	安徽省淮北市
www.xxsjj.gov.cn	安徽省宿州市
da.whx.gov.cn	安徽省芜湖市
www.lpnyxxw.gov.cn	广西壮族自治区桂林市
sxdjw.gov.cn	湖北省宜昌市
hnan.anxiang.gov.cn	湖南省常德市
clyouth.zjjcl.gov.cn	湖南省张家界市
www.txdjw.gov.cn	宁夏回族自治区吴忠市

注6：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.bxfgj.gov.cn	山东省滨州市
www.jxjtw.gov.cn	山东省日照市
www.scpcgt.gov.cn	四川省达州市

➢ *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 10 月 31 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 10 月 31 日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.gzbjfda.gov.cn	贵州省毕节市
www.lgzj.gov.cn	河北省石家庄市
xw.yuanjiang.gov.cn	湖南省沅江市
www.sdlzfda.gov.cn	山东省莱州市
www.lzrc.gov.cn	山东省莱州市
www.lzldbz.gov.cn	山东省莱州市
www.ytny.gov.cn	山东省烟台市
www.ytgt.gov.cn	山东省烟台市
www.ytgh.gov.cn	山东省烟台市
www.ytfda.gov.cn	山东省烟台市
www.yantaiepz.gov.cn	山东省烟台市
phdm.pinghu.gov.cn	浙江省平湖市

➢ *境内网站被植入后门情况*

2012 年 10 月，境内被植入后门的网站数量为 7366 个。境内被植入后门的网站数量按地区分布排名前三位的分别是北京市、上海市、江苏省。按网站类型统计，被植入后门数量最多的是 COM 域名类网站，其多为商业类网站；值得注意的是，被植入后门的 GOV 域名类网站有 380 个，占境内被植入后门网站的比例为 5.2%。

2012 年 10 月，境外 9942 个 IP 地址通过植入后门对境内 6652 个网站实施远程控制。其中，境外 IP 地址主要位于中国台湾、美

国和中国香港等国家或地区。从境外 IP 地址通过植入后门控制境内网站数量来看，位于韩国的 IP 地址共向境内 1569 个网站植入了后门程序，侵入网站数量居首位，其次是位于美国和位于乌克兰的 IP 地址，分别向境内 1292 个和 1124 个网站植入了后门程序。

➢ *境内网站被仿冒情况*

2012 年 10 月，CNCERT 共监测到针对境内网站的仿冒页面有 10347 个，涉及域名 2664 个，IP 地址 753 个，平均每个 IP 地址承载近 14 个仿冒页面。在这 753 个 IP 中，境外占 97.9%，主要位于美国和中国香港。

◆ 漏洞数据分析

2012 年 10 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 665 个。其中，高危漏洞 237 个，可被利用来实施远程攻击的漏洞有 606 个。受影响的软硬件系统厂商包括 Adobe、Cisco、Google、IBM、Linux、Microsoft、Mozilla、Oracle、WordPress 等。

根据 CNVD 的代码验证结果，本月共出现了 231 个 0day 漏洞，其中影响较为严重的是“FirePass SSL VPN 'refreshURL'参数 URI 重定向漏洞”、“VAM Shop SQL 注入漏洞”、“QQ Player 'quartz.dll'堆缓冲区溢出漏洞”、“BSW Gallery 'uploadpic.php'任意文件上传漏洞”。互联网上已经出现针对上述漏洞的攻击代码，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。

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。

◆ 网络安全事件接收与处理情况

➢ *事件接收情况*

2012 年 10 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 1729 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 211 件。

在 1729 件事件报告中，排名前三位的安全事件分别是网页仿冒、漏洞、拒绝服务攻击。

➢ *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。

2012 年 10 月 ,CNCERT 总部以及各省分中心共同协调处理了 1976 件网络安全事件。各类事件处理数量中网页仿冒、漏洞类事件处理数量较多。

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。

- 恶意程序

恶意程序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。恶意程序分类说明如下：

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[7]、网银木马[8]、窃密木马[9]、远程控制木马[10]、流量劫持木马[11]、下载者木马[12]和其它木马七类。

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

注7：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8：网银木马是用于窃取用户网银、证券等账号的木马。

注9：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10：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11：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12：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。

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,如可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。

- 网站后门

网站后门事件是指黑客在网站的特定目录中上传远程控制页面从而能够通过该页面秘密远程控制网站服务器的攻击事件。

- 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。