

互联网网络安全指数通报

(2009 年 10 月)

本月，互联网网络安全状况整体评价为**中**。我国未发生造成较大影响的网络安全事件，网络安全状况各项指标较上月各有增减。其中，本月我国境内木马和僵尸网络受控端的数量较上月有所下降，境外木马和僵尸网络控制服务器的数量较上月有大幅度下降，这说明国庆保障期间进行的木马和僵尸网络专项治理行动取得一定成效。本月我国境内被篡改网站的数量较上月有较大幅度增加。此外，本月公布的一些应用软件的高危安全漏洞以及网页挂马对互联网用户的威胁程度较高。

(1) 基础网络运行安全

本月，互联网基础网络运行基本正常，未出现全国或省级行政区域内造成较大影响的基础网络运行故障。针对境内互联网设备的主要网络攻击仍然是拒绝服务攻击。

依据辽宁、河北等地运营商的检测统计样本，拒绝服务攻击中一般流量¹攻击次数约占 86%，较大流量攻击次数约占 12%，大流量攻击次数约为 2%。运营企业通过配置 ACL 设置路由策略以及采取相关安全防护措施可以较好地抵御上述攻击。

(2) 公共互联网环境安全

本月，全国公共互联网大部分网络安全状况指标与上月相比各有增减，其中较为突出的是境外僵尸网络控制服务器数量继前几个月大幅增长之后出现大幅下降，我国大陆地区被篡改网站数

¹ 一般流量、较大流量、大流量攻击是指流量分别为小于 5Gb、大于 5Gb 但小于 15Gb、大于 15Gb 的攻击。

量继上月下降之后出现反增。CNCERT/CC 监测数据显示：①我国大陆地区有 2.2 万个 IP 地址所对应的主机被通过木马程序秘密控制，较上月下降 1.9%，境外木马控制端主机较上月下降 19.8%；②我国大陆地区约 10.8 万个 IP 地址对应的主机被僵尸网络控制，与上月相比下降 15.9%，境外控制服务器数量较上月大幅下降 56.9%；③我国大陆地区被篡改网站数量为 5793 个，较上月增长 39%，其中被篡改政府网站数量为 343 个，较上月的 256 个增长 34%，但占大陆被篡改网站的比例则由 7.29% 下降到 5.92%；④ CNCERT/CC 接收到的事件数量较上月下降 18%，其主要原因是垃圾邮件、网页恶意代码和网络仿冒事件报告数量均有不同程度的下降。

（3）网络安全风险

近几个月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。10 月，CNCERT/CC 接收到国内外安全组织报告的漏洞 38 个，其中高危漏洞 13 个，漏洞报告数量达到今年以来最高水平。受影响的软硬件系统包括 Cisco(思科)、Debian、Microsoft(微软)、Mozilla 和 VMware 等厂商。此外，病毒、木马等恶意代码威胁程度相对较高，其传播和扩散的途径往往是利用了已经公布的系统和应用软件漏洞。

（4）网络安全感知

本月，互联网用户感知最为强烈的事件仍然是网页挂马事件。此外，从 CNCERT/CC 接收国内外投诉事件情况看，垃圾邮件事件（占 61%）和网页挂马事件（占 31%）受用户关注度较高。

附：本月各指标具体情况

一级指标	二级指标	三级指标	值	环比
基础网络运行安全	IP 业务安全	一般事件数	18	+28.6%
	基础 IP 网络安全	一般事件数	6084	+98.6%
	域名系统服务安全	一般事件数	1	(-3)
	基础电信运营企业网上营业厅、移动 WAP 业务、门户网站等安全	一般事件数	0	(-5)
公共互联网环境安全	计算机病毒事件	一般事件数	351	-11.4%
		恶意代码样本捕获次数	30430	-23.4%
		恶意代码新样本捕获次数	446	-41.7%
	蠕虫事件	一般事件数	69	+156%
	木马事件	一般事件数	201	-63.3%
		境内被植入木马的 IP 地址数目	22154	-5.3%
		境内木马控制服务器的 IP 地址数目	47163	+10.7%
	僵尸网络	一般事件数	705	-80.3%
		境内被僵尸网络控制的 IP 地址数目	108222	-16.0%
		境内僵尸网络控制服务器的 IP 地址数目	400	-22.6%
	域名劫持	一般事件数	8	(+1)
		境内域名劫持事件数目	0	-

	网页篡改	一般事件数	24	-65.2%
		境内被篡改网站的总数	5793	+64.9%
		境内被篡改政府网站占境内被篡改网站总数的比例	5.92%	-18.8%
	网页挂马	一般事件数	28	-69.2%
	拒绝服务攻击	一般事件数	153	+28.6%
	后门漏洞事件	一般事件数	38	+72.7%
	非授权访问	一般事件数	4	(+4)
	垃圾邮件	一般事件数	11151	-10.7%
	网络仿冒	一般事件数	31	-3.1%
	其他网络安全事件	一般事件数	113	+21.5%
网络安全 风险	漏洞情况	网络传输设备高危漏洞数	0	-18.8%
		域名服务有关高危漏洞数	0	
		服务器系统高危漏洞数	2	
		个人操作系统高危漏洞数	8	
		应用软件高危漏洞数	3	
	预警情况	四级预警信息数	35	-10.3%
网络安全 感知	垃圾邮件举报	垃圾邮件举报总数	46132	+141%
	恶意代码举报	恶意代码举报总数	5	(+2)
	网页挂马举报	网页挂马举报总数	525	+34.0%

	拒绝服务攻击举报	拒绝服务攻击举报总数	2	—
	网络仿冒举报	网络仿冒举报总数	94	-28.2%

注：环比是指与上月相比。