国家互联网应急中心

2015 年第 35 期

8 月 24 日-8 月 30 日

# 网络安全信息与动态周报

## 本周网络安全基本态势

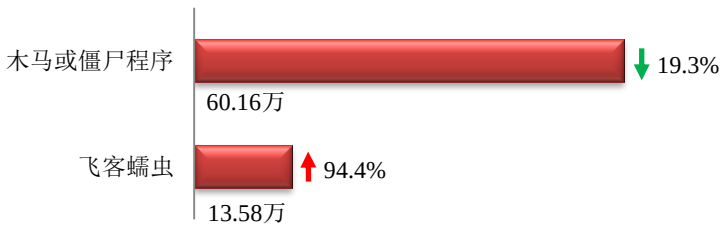
优 | 良 | 中 | 差 | 危

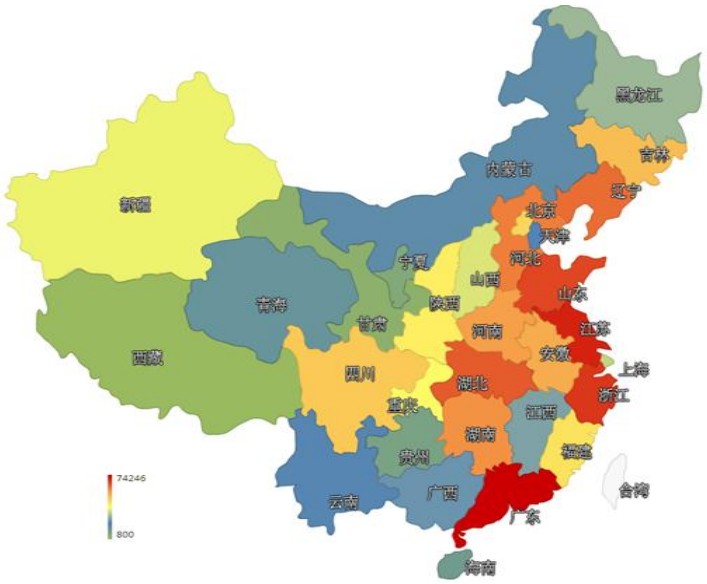
| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •73.74万 | 9.6% |
| 境内被篡改网站总数<br>其中政府网站数量 | •2816<br>•46 | 36.6%<br>7.0% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •3937<br>•173 | 23.1%<br>2.4% |
| 针对境内网站的仿冒页面数量 | •4503 | 23.4% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •219<br>•65 | 19.7%<br>23.5% |

*表示数量与上周相同　表示数量较上周环比增加　表示数量较上周环比减少*

## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 73.74 万个，其中包括境内被木马或被僵尸程序控制的主机约 60.16 万以及境内感染飞客（conficker）蠕虫的主机约 13.58 万。



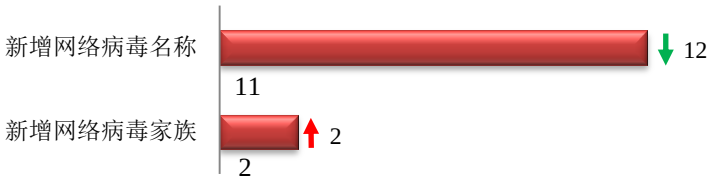



木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。

TOP3

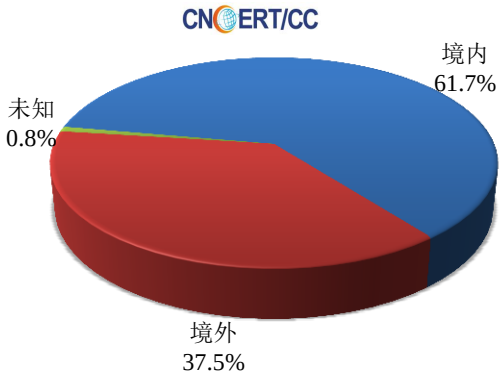
| | |
|---|---|
| 广东省 | •约7.4万个（约占中国大陆总感染量的12.3%） |
| 江苏省 | •约5.6万个（约占中国大陆总感染量的9.2%） |
| 浙江省 | •约5.2万个（约占中国大陆总感染量的8.6%） |

本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 11 个，按网络病毒家族统计新增 2 个。

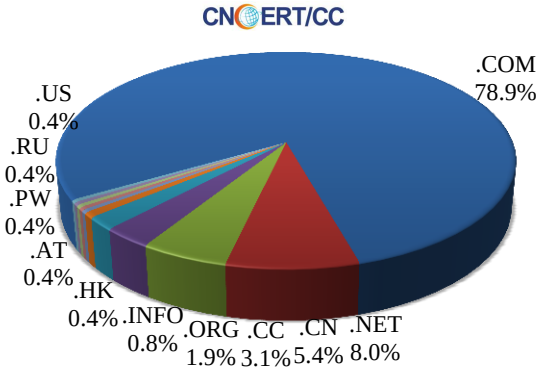



放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 261 个，涉及 IP 地址 456 个。在 261 个域名中，有约 37.5%为境外注册，且顶级域为.com 的约占 78.9%；在 456 个 IP 中，有约 24.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 80 个 IP。

**本周放马站点域名注册所属境内外分布**
**(8/24-8/30)**




**本周放马站点域名所属顶级域的分布**
**(8/24-8/30)**




针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

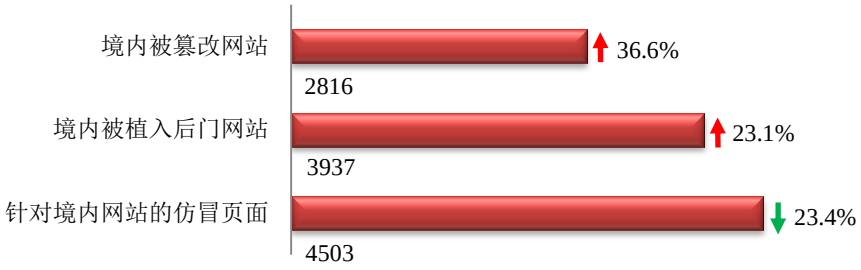
**ANVA恶意地址黑名单发布地址**

http://www.anva.org.cn/virusAddress/listBlack

*中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。*

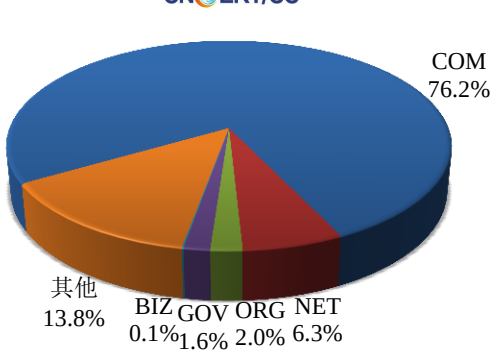
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2816 个；境内被植入后门的网站数量为 3937 个；针对境内网站的仿冒页面数量为 4503。

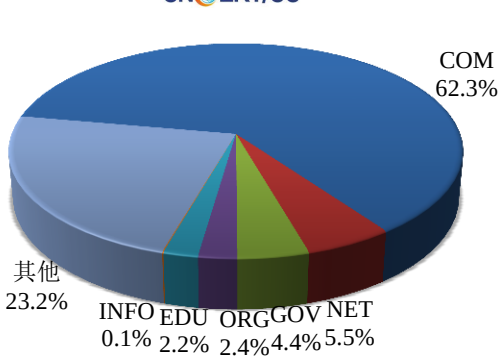



本周境内被篡改政府网站(GOV 类)数量为 46 个（约占境内 1.6%），较上周环比上升了 7.0%；境内被植入后门的政府网站(GOV 类)数量为 173 个（约占境内 4.4%），较上周环比上升了 2.4%；针对境内网站的仿冒页面涉及域名 3766 个，IP 地址 785 个，平均每个 IP 地址承载了约 6 个仿冒页面。

**本周我国境内被篡改网站按类型分布**
**(8/24-8/30)**

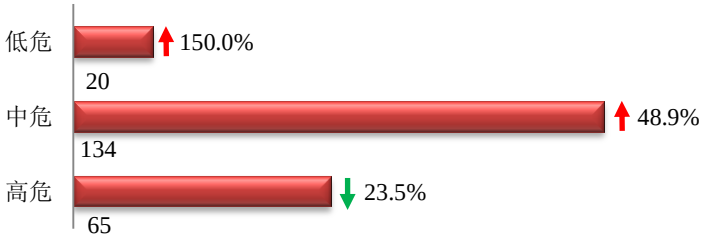



**本周我国境内被植入后门网站按类型分布**
**(8/24-8/30)**

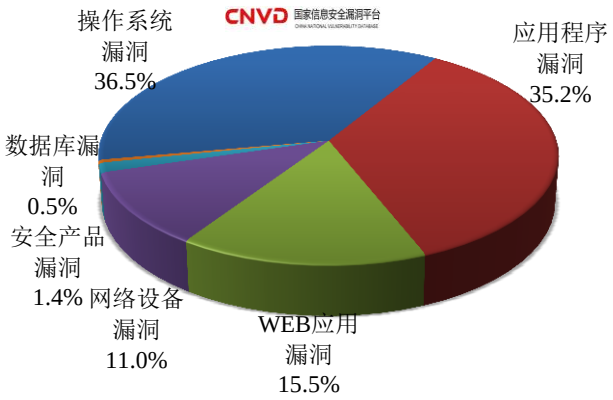



## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 219 个，信息安全漏洞威胁整体评价级别为中。



**本周CNVD收录漏洞按影响对象类型分布**
**(8/24-8/30)**




本周 CNVD 发布的网络安全漏洞中，操作系统漏洞占比最高，其次是应用程序漏洞和 WEB 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

**CNVD漏洞周报发布地址**

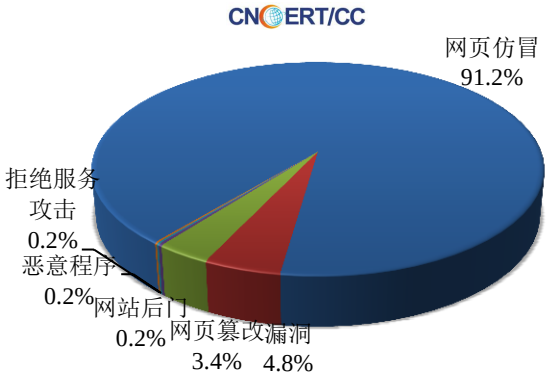
http://www.cnvd.org.cn/webinfo/list?type=4

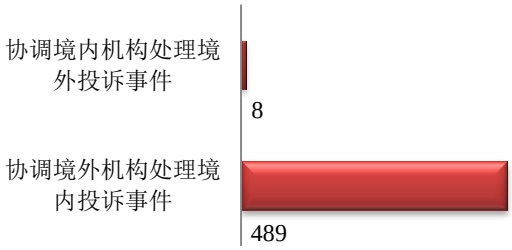
*国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。*

## 本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1224 起，其中跨境网络安全事件 497 起。

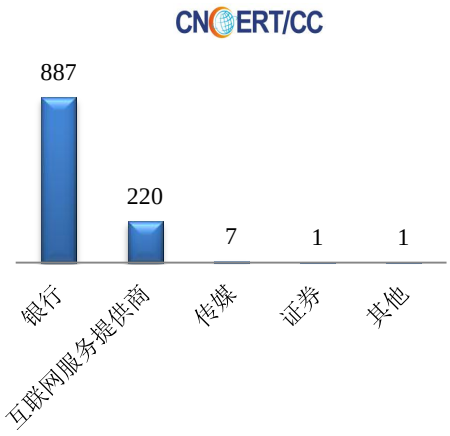
**本周CNCERT处理的事件数量按类型分布**
**(8/24-8/30)**



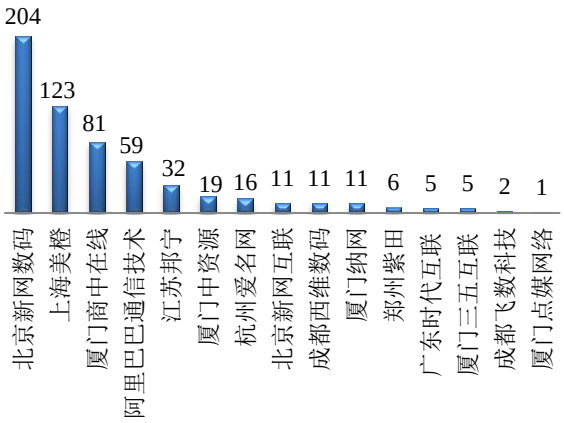




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1116 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 887 起和互联网服务提供商仿冒事件 220 起。

**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/24-8/30)**

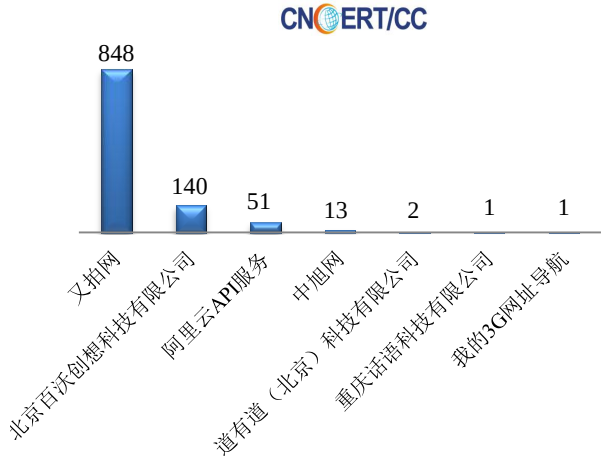



**本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/24-8/30)**




本周，CNCERT 协调 7 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 1056 个。

**本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名 (8/24-8/30)**




## 业界新闻速递

### 1、中国刑法修正案（九）草案 维护信息网络安全

环球网 8 月 30 日消息 8 月 29 日，备受关注的刑法修正案（九）由十二届全国人大常委会第十六次会议审议通过。刑法修正案（九）特别重视打击网络犯罪，将网络视为打击犯罪活动的重要“战场”。一是，为进一步加强对公民个人信息的保护，修改出售、非法提供因履行职责或者提供服务而获得的公民个人信息犯罪的规定，扩大犯罪主体的范围，同时，增加规定出售或者非法提供公民个人信息的犯罪。二是，针对一些网络服务提供者不履行网络安全管理义务，造成严重后果的情况，增加规定：网络服务提供者不履行网络安全管理义务，经监管部门通知采取改正措施而拒绝执行，致使违法信息大量传播的，致使用户信息泄漏，造成严重后果的，或者致使刑事犯罪证据灭失，严重妨害司法机关追究犯罪的，追究刑事责任。三是，对为实施诈骗、销售违禁品、

管制物品等违法犯罪活动而设立网站、通讯群组、发布信息的行为，进一步明确规定如何追究刑事责任；针对在网络空间传授犯罪方法、帮助他人犯罪的行为多发的情况，增加规定：明知他人利用信息网络实施犯罪,为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助,情节严重的，追究刑事责任。四是，针对开设“伪基站”等严重扰乱无线电秩序，侵犯公民权益的情况，修改扰乱无线电通讯管理秩序罪，降低构成犯罪门槛，增强可操作性。五是，针对在信息网络或者其他媒体上恶意编造、传播虚假信息，严重扰乱社会秩序的情况，增加规定编造、传播虚假信息的犯罪。此外，还对单位实施侵入、破坏计算机信息系统犯罪规定了刑事责任。

**2、美上诉法院推翻 NSA 监听项目违法判决：证据不足**

凤凰网 8 月 29 日消息 据路透社报道，8 月 28 日，美国哥伦比亚地区上诉法院推翻了下级法院的判决。该裁定本可以阻止美国国家安全局（NSA）在一个备受争议的项目下收集手机元数据。这一数据收集项目已引发隐私担忧。上诉法院表示，下级法院作出的初步禁令缺乏足够的证据。对于隐私拥护者来说，上诉法院的裁定是一大挫折，但它尚未涉及到一个更大问题，那就是 NSA 的行为是否合法。上诉法院的裁定意味着，NSA 大规模收集和存储电话记录的项目将不受影响地继续进行，直到该项目在 11 月底终止。根据美国国会在 6 月份通过的《美国自由法案》，NSA 的监听项目获准继续开展 180 天，直到旨在解决隐私问题的新规定生效。白宫发言人约什·厄尼斯特表示：“这一判决与政府此前的表态一致，我们确信这些行为是符合宪法的。”对 NSA 监听项目发起诉讼的保守派律师拉里·克莱曼表示，他将向最高法院提起上诉。“我们对胜诉充满信心，”他说。NSA 和美国国家情报主任办公室（ODNI）发言人均对裁定不予置评。

**3、黑客组织入侵泰国 6 个政府网站 声称来自突尼斯**

环球网 8 月 24 日消息 据香港“东网”8 月 24 日报道，泰国 6 个政府网站，24 日遭黑客入侵，并在网页上张贴缅甸罗兴亚族逃亡及在炸弹袭击中受害的穆斯林儿童照片。6 个遭入侵的网站包括北部南奔府、中部信武里府、沙缴府、来兴府等政府网站。黑客声称来自突尼斯黑客组织 FallagGassrini& Dr. Lamouchi，自称为回教徒，呼吁他人尊重他们。据指，该黑客组织曾于法国《查理周刊》杂志社遭回教枪手血洗后，入侵数个以色列及法国网站。泰国信息及通讯科技部官员指，黑客使用 Linux 系统在全球同步发动攻击，现正调查其服务器所在地。

**4、Ziggo 服务器连续两天遭黑客攻击 60%以上用户网络全断**

C114 中国通信网 8 月 24 日消息 Ziggo 是荷兰知名网络提供商。昨晚他们的主要服务器 DNS 受到黑客攻击，致使许多用户无法连接网络。然而，这并不是 Ziggo 第一次遭遇黑客攻击，就在本周二晚上，他们就已经受到不明黑客的严重攻击。那次攻击使得全国范围内，60%的 Ziggo 用户无法连接上网络，约有 320 万用户受到影响。Ziggo 发言人表示，昨天晚上，黑客主要攻击了他们的 DNS 服务器。这个服务器是管理所有用户 IP 地址的，所以使得用户无法使用网络。他们表示，周二的那次攻击比周三的更加严重，但是他们也已经成功修复了网络，积攒了对付此问题的经验。发言人还表示，今后他们会重强网络服务器的防固，也会着重预防此类黑客的攻击，保障用户们有一个安全快速的网络环境。在今早凌晨 4 点，服务器已完全被修复，用户们皆可正常使用网络。部分用户可能需要重启他们的调解器，才可以顺利连接上网络。

**5、网络诈骗每年花费企业三百七十万美元**

8 月 27 日，据 SC Magazine 报道，有新的报告表明，每年企业花在网络诈骗的耗资达三百七十万美元，不过通过适当的员工训练，该数字可以减少一百八十万美元。由 Wombat 发起，Ponemon 实施的“网络诈骗耗资和员工训练价值”报告，有超过 375 家 IT 和 IT 安全相关企业参与。报道称生产上的损失超过一百八十万美元，包括人事上消耗、机器被黑等。其他的损失来源包括信誉损失、恶意软件等。员工训练可以帮助其发现攻击和相关威胁，以减少近 2 百万的损失。Wombat 的 CEO，Ferrara 建议企业采用一种持续循环的训练方法帮助员工强化正确的操作和知识，以帮助从业者不断改进，识别诈骗，以减少相关损失。

## 关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2014 年，CNCERT 与 63 个国家和地区的 144 个组织建立了“CNCERT 国际合作伙伴”关系。

## 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：赵慧

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82991373