国家互联网应急中心

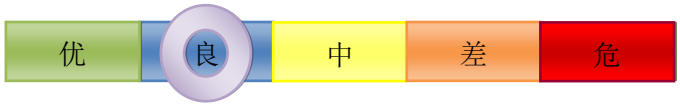
# 网络安全信息与动态周报

**2016 年第 12 期**

**3 月 14 日-3 月 20 日**

CNCERT/CC

## 本周网络安全基本态势

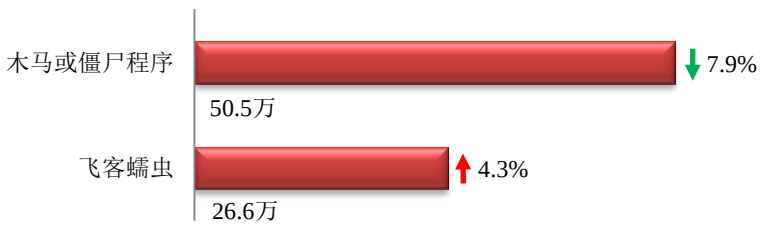


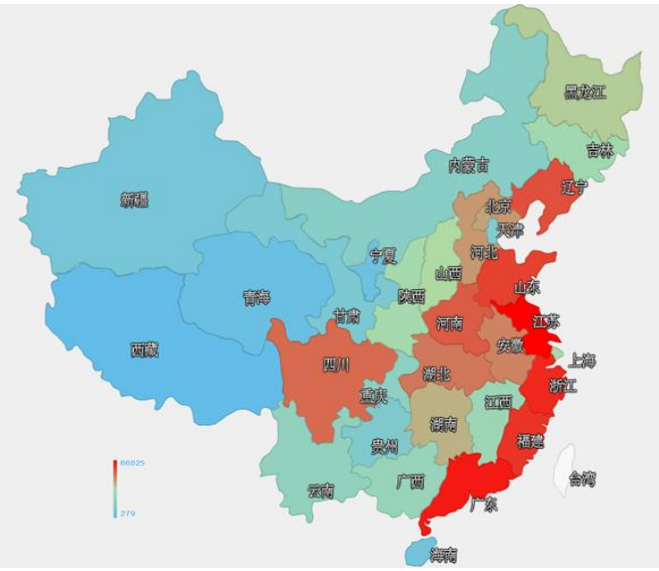

| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •77.1万 | 4.1% |
| 境内被篡改网站总数<br>其中政府网站数量 | •3762<br>•62 | 6.4%<br>10.1% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •1885<br>•99 | 6.7%<br>22.2% |
| 针对境内网站的仿冒页面数量 | •4159 | 2.9% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •143<br>•71 | 20.2%<br>4.4% |

*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 77.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.5 万以及境内感染飞客（conficker）蠕虫的主机约 26.6 万。



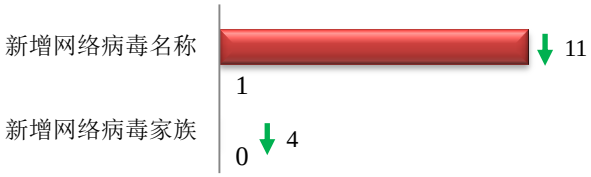



木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是江苏省、广东省和浙江省。

TOP3

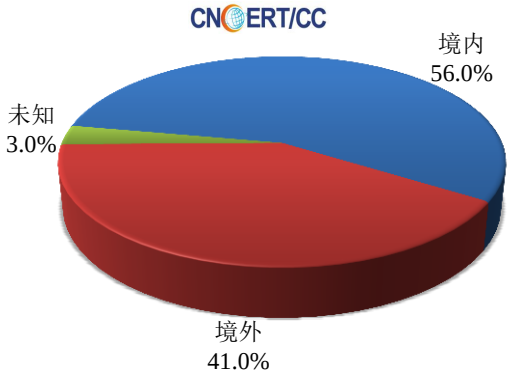
| | |
|---|---|
| 江苏省 | •约6.7万个（约占中国大陆总感染量的13.2%） |
| 广东省 | •约4.9万个（约占中国大陆总感染量的9.6%） |
| 浙江省 | •约4.2万个（约占中国大陆总感染量的8.4%） |

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 1 个，按网络病毒家族统计无新增。

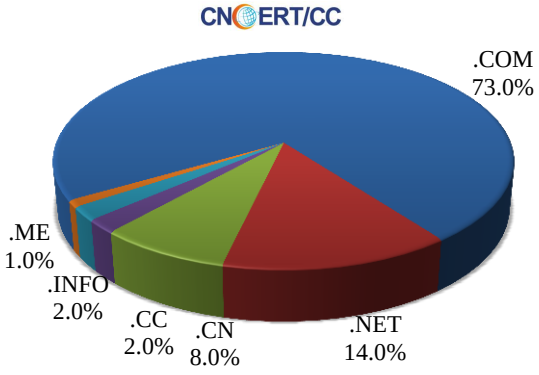



放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 100 个，涉及 IP 地址 232 个。在 100 个域名中，有约 41.0%为境外注册，且顶级域为.com 的约占 73.0%；在 232 个 IP 中，有约 7.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 28 个 IP。

**本周放马站点域名注册所属境内外分布**
**(3/14-3/20)**




**本周放马站点域名所属顶级域的分布**
**(3/14-3/20)**



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。

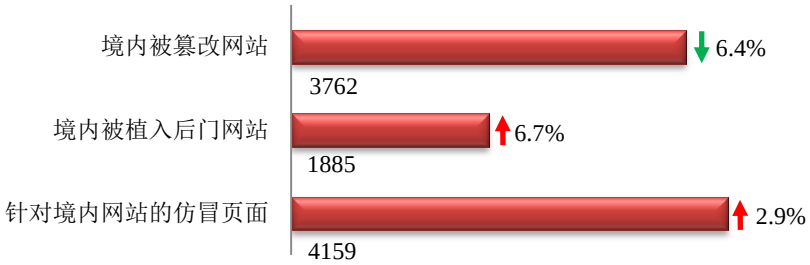
**ANVA恶意地址黑名单发布地址**

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。*

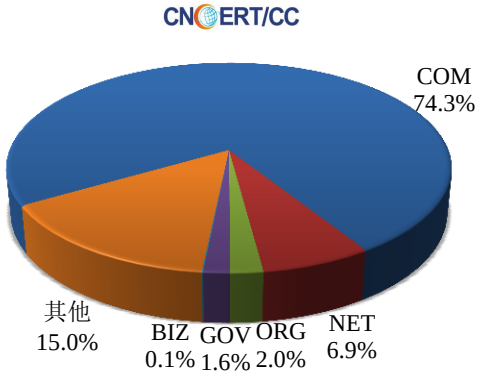
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3762 个；境内被植入后门的网站数量为 1885 个；针对境内网站的仿冒页面数量为 4159。

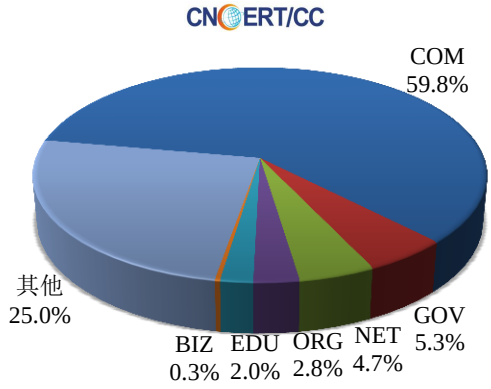



本周境内被篡改政府网站(GOV 类)数量为 62 个（约占境内 1.6%），较上周环比下降了 10.1%；境内被植入后门的政府网站(GOV 类)数量为 99 个（约占境内 5.3%），较上周环比上升了 22.2%；针对境内网站的仿冒页面涉及域名 3484 个，IP 地址 1102 个，平均每个 IP 地址承载了约 4 个仿冒页面。

**本周我国境内被篡改网站按类型分布**
**(3/14-3/20)**



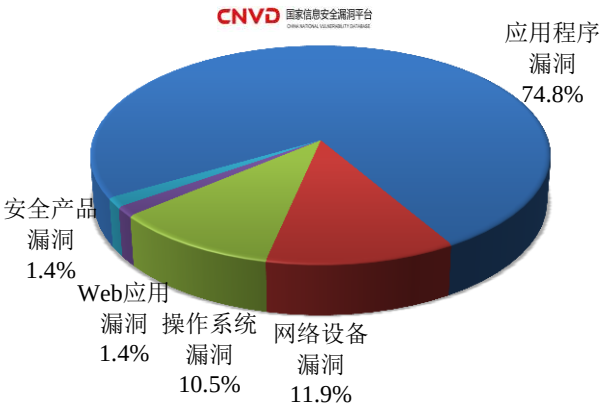

**本周我国境内被植入后门网站按类型分布**
**(3/14-3/20)**



## 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 143 个，信息安全漏洞威胁整体评价级别为高。


**本周CNVD收录漏洞按影响对象类型分布**
**(3/14-3/20)**




本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和操作系统漏洞。

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**

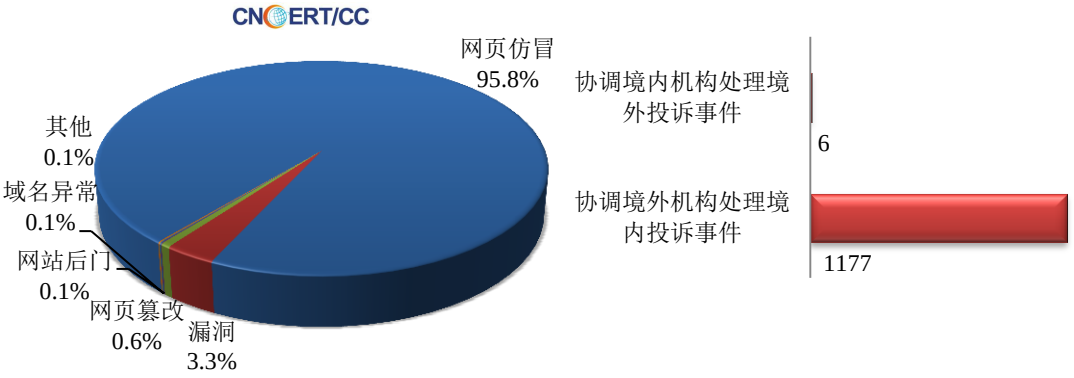
http://www.cnvd.org.cn/webinfo/list?type=4

*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 3349 起，其中跨境网络安全事件 1183 起。

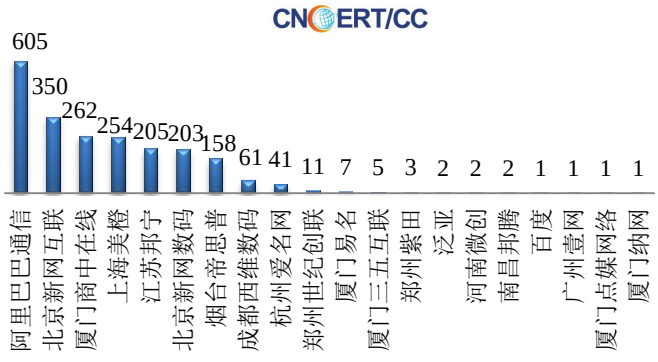
**本周CNCERT处理的事件数量按类型分布**
**(3/14-3/20)**




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 3209 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 2790 起和互联网服务提供商仿冒事件 407 起。

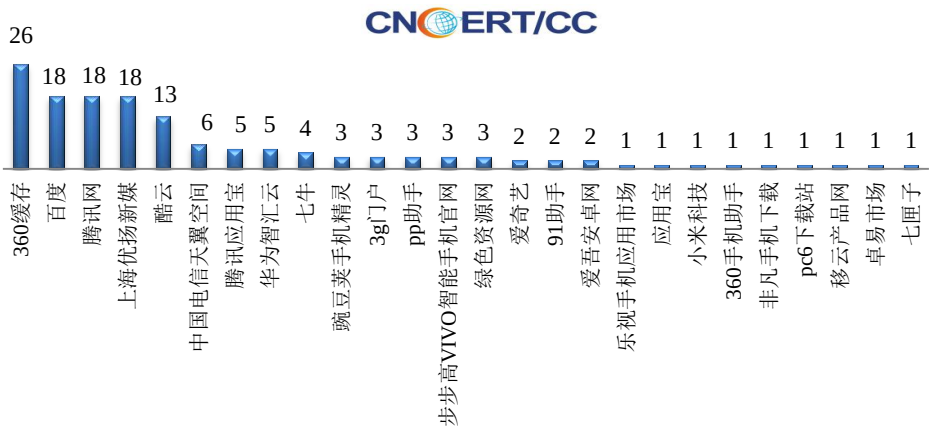
**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/14-3/20)**


**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 (3/14-3/20)**




本周，CNCERT 协调 26 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 143 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**
**(3/14-3/20)**




## 业界新闻速递

### 1、上海发布金融信息安全技术指引 保护金融消费者权益

新华网 3 月 15 日消息 上海金融信息行业协会 3 月 15 日发布《互联网金融网络与信息安全技术指引》，指导企业信息安全建设、规范行业自律，加强金融消费者权益保护。上海市互联网金融信息安全公共服务平台也同时启动。“随着金融信息行业规模和影响逐渐扩大，企业金融数据和客户信息的安全保护就显得日益重要。金融信息行业企业也要提升自律经营意识，切实保障金融消费者的合法权益。”上海金融信息行业协会会长邢波说。尤其值得注意的是，在各项指标中，与金融消费者安全与权益保护有关、与管理相关的指标占到了 30%，这更适合目前互联网金融行业“消费者信任度减弱”，亟待提升消费者信心的现实需求；也将有效地缓解目前互联网金融行业网络与信息安全标准缺失导致的行业风险。例如，在金融消费者信息安全及权益保护方面，指引不仅要求金融信息企业在技术上严格把关，更要求企业在制度保障、人员安全、事件处置、风险提示等方面均要“与时俱进”，全方位保护金融消费者权益。据介绍，指引将首先在上海 20 多家传统金融机构及互联网企业试点施行。同期，上海市互联网金融信息安全公共服务平台启动，旨在通过整合情报系统、在线测评、实时观测以及各类个性化安全服务，建立行业信息安全共享和漏洞解决机制，提升上海市金融信息行业的风险防范能力。

### 2、德国总统 3 月 20 日起访华 中德网络安全协议有望定稿

网易 3 月 17 日消息 应国家主席习近平邀请，德国总统约阿希姆高克将于 3 月 20 日至 24 日对中国进行国事访问，而根据去年中德双方的约定，中德网络安全协议有望于阿希姆高克访华期间定稿。德国总理默克尔访华期间与中国总理李克强达成一致，筹备一份中德网络安全协议，按照约定，这份协议将于今年年中中德政府磋商期间定稿。过去几年间，针对德国企业的网络攻击数量大幅上升，尤其网络间谍的出现令我们很担忧。习近平总书记在中央网络安全和信息化领导小组第一次会议上提出，网络安全是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我

国建设成为网络强国。发展国产顶尖信息安全核心技术并确保重要领域信息系统及数据的安全可控已受到高层特殊关注。此外，中国首部《互联网安全法》有望加速出台，将成为中国互联网安全环境建设的里程碑。目前《网络安全法草案》已通过全国人大审议并完成公开征求意见，根据我国立法的三审制度，两会之后有望迎来第二次审议。在多重政策的大力推动下，网络安全有望在未来 10 年迎来黄金发展期。当前我国在网络安全方面的投入占整个 IT 比重仅为 2%左右，远低于欧美国家 10%左右的水平，潜在发展空间将达千亿级别。正如习近平总书记所指出的，建设网络强国，要有自己的技术，有过硬的技术。

### 3、2015 年日本 27 家单位遭网络攻击蒙受损失

环球网 3 月 18 日消息 日本警察厅 3 月 17 日发布数据称，2015 年全年确认至少有日本年金机构、早稻田大学、石油联盟等 27 家单位（较上年增加 22 个）在遭到目标型病毒邮件、非法入侵等网络攻击后信息外泄，创下有可查数据的 2013 年以来的新高。据日本共同社 3 月 17 日报道，目标型病毒邮件攻击多达 3828 起（较上年增加 2105 起），也刷新了纪录，尤其是恶意利用附件及“Word”文件的案例骤增至 2038 起(增加 2004 起)。这些数据再次暴露出网络攻击的隐蔽化及造成损失日益严重的现状。此外，2015 年 9 月以来，日本成田机场、中部机场、和歌山县太地町等 58 家单位确认受到自称国际黑客组织“匿名者”发动的“DDoS 攻击”（短时间内发送大量访问请求），导致网站一度瘫痪。发生 125 万条个人信息外泄的日本年金机构等 12 家单位受到目标型邮件的攻击。2011 年针对三菱重工的网络攻击曝光后，这一手法受到关注。针对网站漏洞的非法入侵等导致 15 家单位蒙受损失。据相关人士透露，确认发生信息外泄的还有日本证券、日本动物园水族馆协会（JAZA）、东京商工会议所、名城大学、长野县小诸市政府等。但防卫产业、运输等重要基础行业未发现蒙受损失。

### 4、谷歌披露用户数据加密情况 77%网络流量已被加密

腾讯网 3 月 16 日消息 据外电报道，谷歌周二发布统计数据，详尽的披露了在该公司努力对用户所有的网络活动数据进行加密之后，多少谷歌搜索引擎和其他服务的流量已受到保护，免于被黑客获取。谷歌提供的数据显示，谷歌目前对全球发往谷歌数据中心 77%的请求进行了防护，比例高于 2013 年年底时的 52%。这一数据包含了除用户数量超过 10 亿的 YouTube 视频网站之外的谷歌所有服务。谷歌计划从今年年底开始披露 YouTube 流量的加密情况。加密是一种混乱了传输数据的安全措施，当第三方拦截传输数据时，将无法掌握真确的信息。自美国国家安全局（NSA）前雇员爱德华·斯诺登（Edward Snowden）在 2013 年曝光 NSA 及其他情报机构监控用户通信数据，并一直通过互联网收集用户传输的个人数据之后，谷歌开始强调需要对用户网络行为进行加密的问题。美国国家安全局的监控利用了未加密网站的漏洞。谷歌提供的数据显示，目前用户使用 Gmail 账户相互发送的电子邮件已完全被加密，而 Gmail 与其他电子邮件服务之间的邮件通讯则不一定被加密。谷歌排名第二的加密服务为谷歌地图，已有 83%的流量被加密；排名第三的是广告服务，已有 77%的流量被加密，比例高于 2013 年时的仅仅 9%。谷歌新闻服务流量的加密比例为 60%，谷歌财经流量的加密比例为 58%。

### 5、Android 多媒体库又现新漏洞 2.75 亿部设备受影响

腾讯网 3 月 19 日消息 以色列软件研究公司 NorthBit 今日发布报告称，由于 Android 系统的媒体服务器和多媒体库 Stagefright 中存在安全漏洞，上亿部 Android 设备可能会遭到黑客攻击。这并非 Stagefright 首次被发现存在安全漏洞，早在去年 10 月时，就有媒体报道称超过 10 亿部 Android 设备可能会因为 Stagefright 中的一

个安全漏洞而被入侵。从那以后，谷歌陆续发布了多个补丁，但是 Stagefright 的安全问题始终没有得到解决。NorthBit 称，运行 2.2 至 4.0 版 Android 系统以及 5.0 和 5.1 版 Android 系统的设备可能都会受到这个新发现的漏洞的影响。NorthBit 估计运行上述版本 Android 系统的设备大约有 2.75 亿部，但是很难说清到底有多少设备可能会受到影响。NorthBit 称，运行常规 ROM 的 Nexus 5 设备最有可能受到攻击，公司成功攻破的其他手机还包括 HTC One、LG G3 和三星 S5。幸运地是，黑客利用这个新漏洞发动攻击并不是一件容易的事。据 NorthBit 称，利用 Stagefright 中的这个新漏洞发动攻击需要具备一定水平的社会工程学技术，因此黑客不太容易成功。如果不能诱骗用户点击恶意链接并在目标网页上停留足够长的时间，攻击者就不能绕过用户设备的安全系统，整个攻击过程耗时在数秒钟到两分钟之间。因此，在谷歌发布针对 Stagefright 的下一个补丁之前，Android 用户上网时最好还是小心谨慎一点。

## 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 2015 年，CNCERT 与 66 个国家和地区的 165 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：刘锦亮

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158