国家互联网应急中心

2013 年第 13 期

3 月 25 日-3 月 31 日

网络安全信息与动态周报

CNCERT/CC

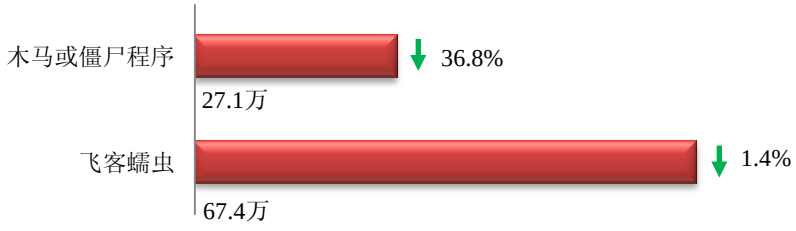
本周网络安全基本态势

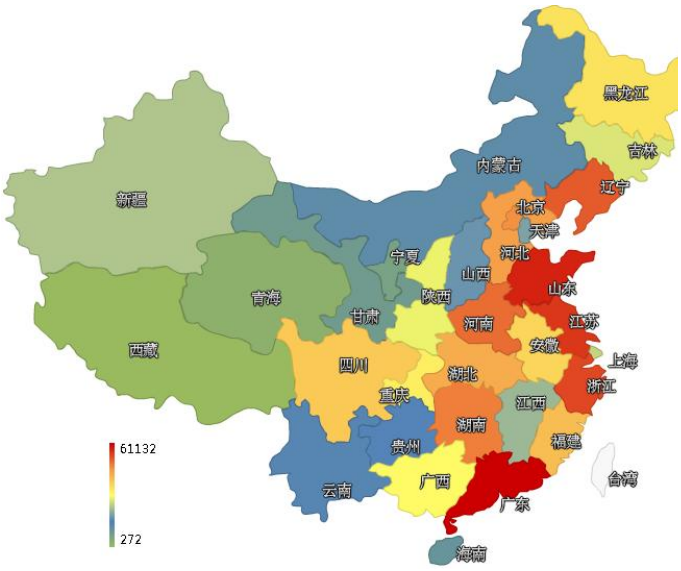
境内感染网络病毒的主机数量	•94.5 万	15.0%
境内被篡改网站总数 其中政府网站数量	•6121 •479	2.3% 1.6%
境内被植入后门网站总数 其中政府网站数量	•1446 •65	26.9% 37.5%
针对境内网站的仿冒页面数量	•836	27.7%
新增信息安全漏洞数量 其中高危漏洞数量	•160 •50	35.6% =

= *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 94.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 27.1 万以及境内感染飞客（conficker）蠕虫的主机约 67.4 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、山东省和江苏省。

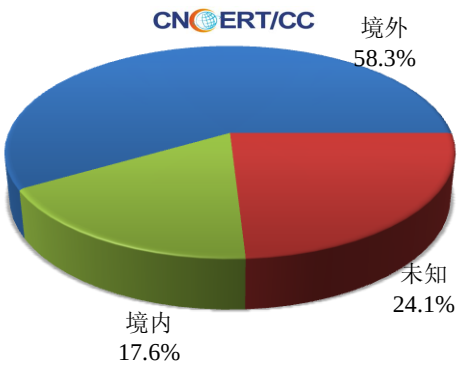
TOP3

广东省	•约6.11万个（约占中国大陆总感染量的22.6%）
山东省	•约1.73万个（约占中国大陆总感染量的6.4%）
江苏省	•约1.67万个（约占中国大陆总感染量的6.2%）

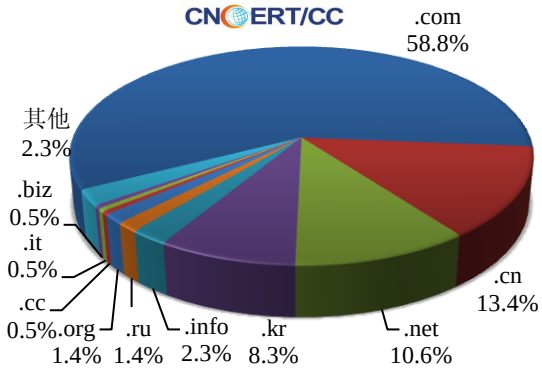
本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 44 个，按网络病毒家族统计无新增。

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 216 个，涉及 IP 地址 341 个。在 216 个域名中，有约 58.3%为境外注册，且顶级域为.com 的约占 58.8%；在 341 个 IP 中，有约 57.2%位于境内，约 42.8%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 123 个 IP。

本周放马站点域名注册所属境内外分布
(3/25-3/31)



本周放马站点域名所属顶级域的分布
(3/25-3/31)



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。

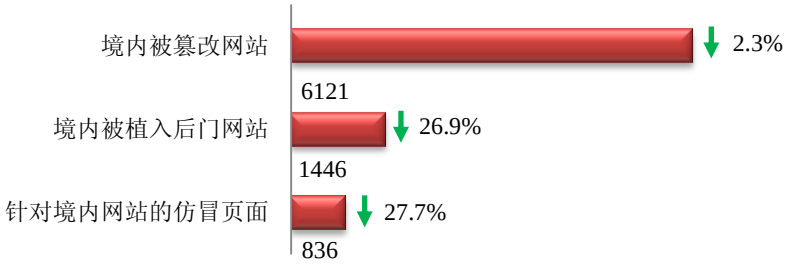
ANVA恶意地址黑名单发布地址

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。

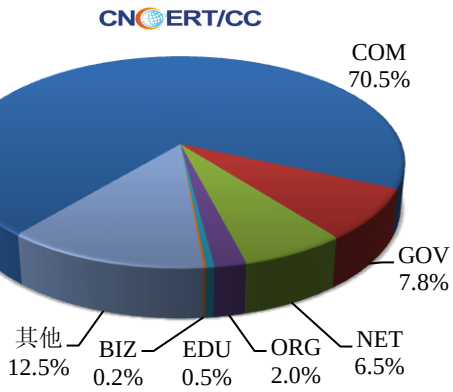
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 6121 个；境内被植入后门的网站数量为 1446 个；针对境内网站的仿冒页面数量为 836 个。

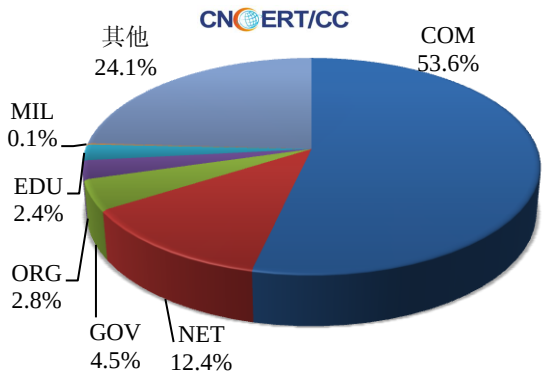


本周境内被篡改政府网站(GOV 类)数量为 479 个（约占境内 7.8%），较上周环比下降了 1.6%；境内被植入后门的政府网站(GOV 类)数量为 65 个（约占境内 4.5%），较上周环比大幅下降了 37.5%；针对境内网站的仿冒页面涉及域名 582 个，IP 地址 290 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/25-3/31)

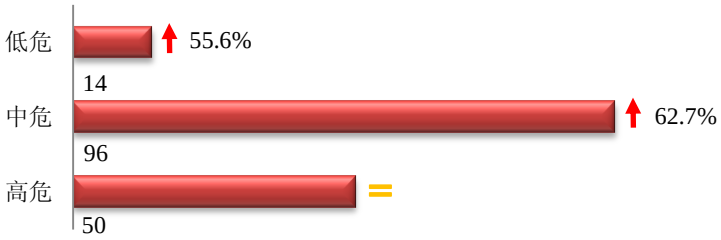


本周我国境内被植入后门网站按类型分布
(3/25-3/31)

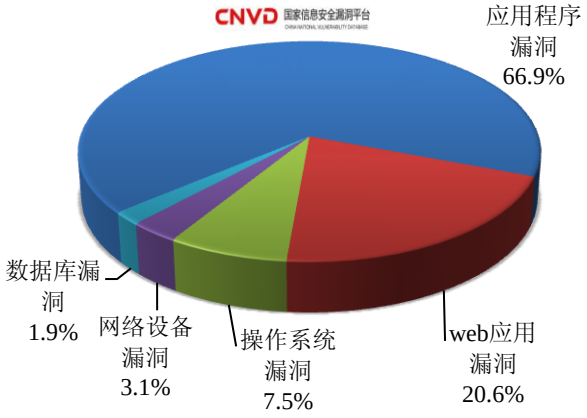


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 160 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
(3/25-3/31)



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 Web 应用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

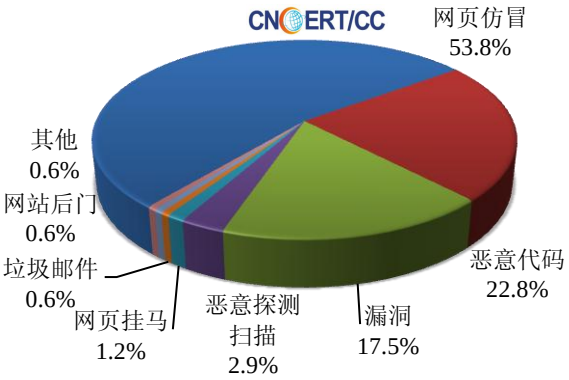
http://www.cnvd.org.cn/publish/main/47/index.html

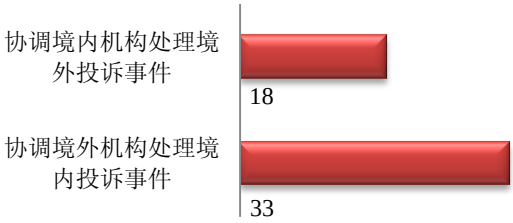
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 171 起，其中有跨境网络安全事件 51 起。

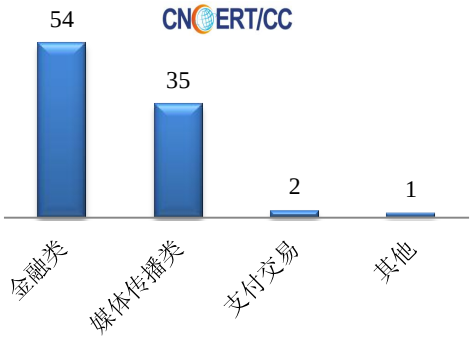
本周CNCERT处理的事件数量按类型分布
(3/25-3/31)



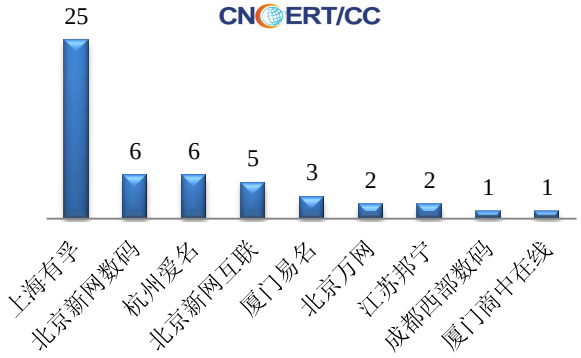


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 92 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包含工商银行等金融类仿冒事件 54 起、央视等媒体传播类仿冒事件 35 起、淘宝等支付交易类仿冒事件 2 起和其他仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/25-3/31)

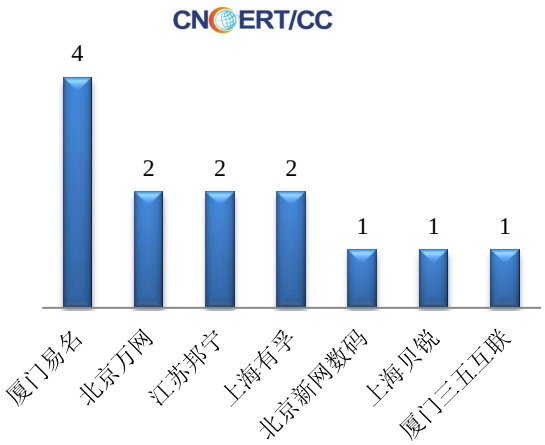


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (3/25-3/31)

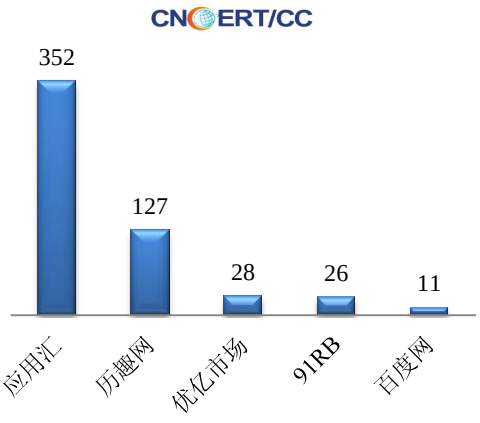


本周，CNCERT 协调 1 家基础电信运营企业、7 家境内域名注册机构及 5 家手机应用商店开展恶意代码处理工作，共处理传播恶意代码的域名 14 个，传播移动互联网恶意代码的恶意 URL 链接 544 个。

本周CNCERT协调境内域名注册机构处理恶意代码事件数量排名 (3/25-3/31)



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 (3/25-3/31)



业界新闻速递

1、日美将举行首次网络安全一揽子对话

中国日报 3 月 28 日消息 日本共同社 3 月 28 日援引多名消息人士的话报道说，日美两国政府已达成一致，定于 5 月份在东京举行有关网络安全问题的首次一揽子对话。日美两国政府将共同强化举措，通过建立跨部门对话框架，从经济和国家安全等多个角度磋商针对网络攻击的合作方案。首次对话将在就日美两国目前对网络攻击威胁的认识进行讨论后，从国家安全、企业信息、基础设施保护、官民合作等多个层面交换信息，并将其反映在今后的对策上。据了解，在去年 4 月举行的日美首脑会议上，日本前首相野田佳彦与美国总统奥巴马就举行网络领域的日美对话达成一致。目前，日美双方正在就于 5 月中旬举行一揽子对话进行协调，相关会议今后将有可能定期举行。

2、韩国继续调查黑客攻击事件

人民网 3 月 26 日消息 韩国警察厅 3 月 25 日发布消息称，此前针对韩国多家电视台和金融机构的黑客攻击来自美国和欧洲地区共 4 个国家。据警察厅调查显示，导致计算机网络瘫痪的恶意代码 IP 源地址分别显示为这 4 个国家，警察厅已要求上述国家予以协助调查。据悉，3 月 20 日，韩国三家主流电视台和六家金融机构的计算机网络因黑客攻击而全面瘫痪，3.2 万余台电脑和服务器在攻击中受损。为此，韩国军方将情报作战防卫级别上调一级，政府特别发布网上危机注意警报，召集紧急会议，成立联合应对小组，还临时启动了国家安全室开展工作。经过调查，韩国政府证实瘫痪是由于向计算机补丁管理系统中植入恶意代码所致，基础设备未受影响。韩方还将继续调查此事件。为防范类似事件再次发生，韩方政府层级已对网络安全高度重视。在 3 月 25 日举行的记者会中，青瓦台发言人金杏表示，为了更好地应对网络攻击，政府有关部门正讨论制定相应的法律法规，其中包括“通讯社和电视台在遭受网络攻击时应第一时间向政府汇报，否则将被处以罚款”，并对此前舆论提及的“在国家安全室新设网络安全秘书一职”之事予以否认。

3、反垃圾邮件组织 Spamhaus 遭史上最大 DDoS 攻击

腾讯科技 3 月 28 日消息 北京时间 3 月 28 日消息，据国外媒体报道，旨在帮助电子邮箱服务供应商过滤垃圾邮件和其他不受欢迎的内容的非营利性反垃圾信息组织 Spamhaus 最近封杀了荷兰网站 Cyberbunker 的一些服务器，而引发了黑客对 Spamhaus 域名系统服务器的报复性 DDoS 攻击，对更大范围的互联网造成了影响。Spamhaus 的首席执行官史蒂夫林福特（Steve Linford）称，这次的网络攻击的规模是空前的，其攻击的最大强度达到了 300GB/s，而平时所说的针对重要银行的网络攻击强度也只有 50GB/s 左右。目前已有 5 个国家的网络警察机构开始对这些网络攻击展开调查。

4、网游软件成移动互联网安全重灾区

新华网 3 月 28 日消息 移动互联网已进入快速发展期，也日益成为网络安全事件的重灾区。日前，国家计算机网络应急技术处理协调中心公布的《2012 年第四季度中国移动互联网应用安全检测与分析报告》显示，移动互联网十大恶意应用软件下载量排行榜的前七名均为游戏软件。去年第四季度，我国移动互联网应用商店恶意软件下载量合计超过 1100 万次，主要集中在游戏类和常用工具类，七款游戏类应用排名靠前，下载量最多达 400 万次。2012 年我国手机网民数量超过了使用台式电脑接入互联网的网民数量，达到 4.2 亿，移动互联网的安全问题得到越来越被人们所关注。据了解，网络游戏恶意软件会在手机后台释放应用程序损害手机系统，自

动访问网络消耗用户流量以及拦截电话、短信泄露用户隐私。对此，专家建议，用户要养成安全使用手机的习惯，不要轻易越狱手机，尽量下载官方发布或认证的应用，同时安装防病毒软件以减少手机病毒的感染。

5、支付宝交易现泄露漏洞

网易 3 月 29 日消息 3 月 27 日晚上，支付宝曝出重大漏洞，用户使用谷歌等搜索引擎可以搜索出大量的支付宝用户交水电煤等生活服务类的交易记录，其中包括付款账户、收款账户、姓名、日期甚至地址等信息。据悉，只要在搜索引擎中输入“site:shenghuo.alipay.com”等，则可以看到数百条支付宝相关交易记录。其中，谷歌搜索在五六页以后全部变为付款记录。一些备注中，还有付（收）款人的姓名、电话和地址，这些信息中有些是淘宝交易的付款记录，也有普通的支付宝转账。幸好，该记录只有账户名、交易时间、用途等，并没有密码等核心数据。一位搜索方面相关负责人表示，这些结果被搜索抓取披露，有可能是支付宝的非授权访问出现了问题，后台验证不严的漏洞使得外部的搜索能看到半公开的页面，使得用户不登录支付宝账户也可以看到别人的交易记录。3 月 28 日，支付宝的官方微博对此事回应称，支付宝生活助手转账付款结果页面一般用于支付双方展示支付结果，不含用户真实姓名、密码等重要信息。这一页面链接加具了安全保护，正常情况下任何搜索引擎都无法抓取。支付宝称已将用户付款页面做部分信息隐藏。

6、苹果被爆重大安全漏洞：可轻易更改他人密码并绑架账户

新浪 3 月 25 日消息 据美国《洛杉矶时报》报道，一个科技新闻网站宣称发现一个网络教学影片。影片告诉使用者如何通过修改后的苹果网址进入别人的苹果账户并重置密码。基于安全考虑，该网站未公布教学影片链接，但建议使用者启动苹果账户的两步安全验证机制，以保护账号。不幸的是，部分尝试启动两阶段验证机制的用户称，信息显示他们必须等候 3 天，机制才会启动。这项验证机制目前只有美国、英国、澳大利亚、爱尔兰、新西兰用户可用，其他国家用户无法通过这项措施保护账号。苹果发言人穆勒告诉表示：“苹果非常重视客户隐私。我们已了解这个问题，正在进行修复。”

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（英文简称是 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。国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

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：刘军

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990316