国家互联网应急中心

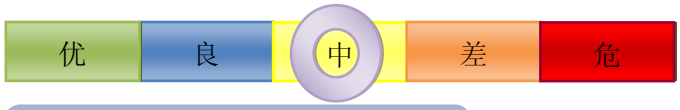
网络安全信息与动态周报

2013 年第 14 期

4 月 1 日-4 月 7 日

CNCERT/CC

本周网络安全基本态势

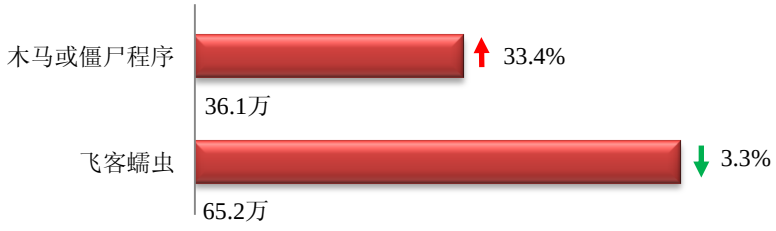


境内感染网络病毒的主机数量	•101.3 万	↑ 7.2%
境内被篡改网站总数 其中政府网站数量	•6178 •558	↑ 0.9% ↑ 16.5%
境内被植入后门网站总数 其中政府网站数量	•2450 •114	↑ 69.4% ↑ 75.4%
针对境内网站的仿冒页面数量	•1113	↑ 33.1%
新增信息安全漏洞数量 其中高危漏洞数量	•101 •33	↓ 36.9% ↓ 34.0%

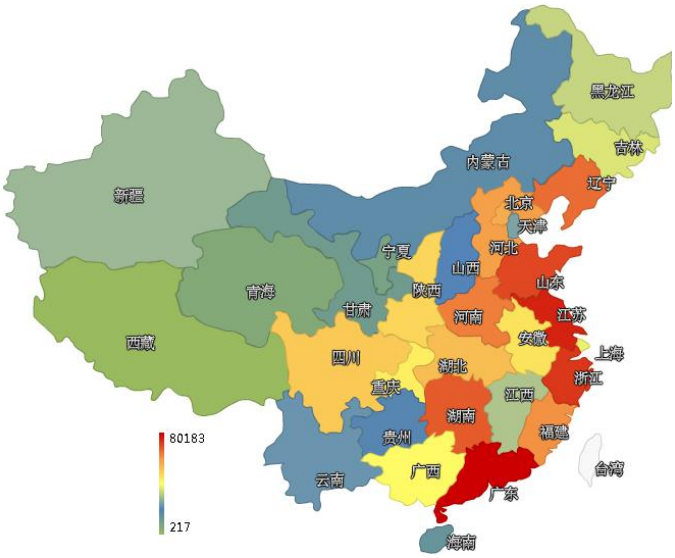
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

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 101.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 36.1 万以及境内感染飞客（conficker）蠕虫的主机约 65.2 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。



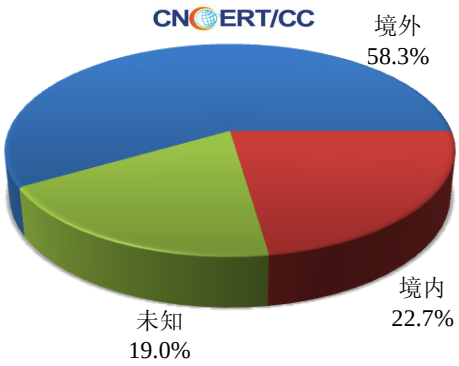
TOP3

广东省	•约8.0万个（约占中国大陆总感染量的22.2%）
江苏省	•约2.8万个（约占中国大陆总感染量的7.7%）
浙江省	•约2.1万个（约占中国大陆总感染量的5.7%）

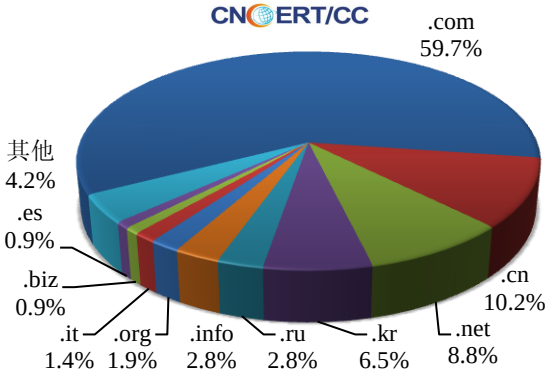
本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 36 个，按网络病毒家族统计新增 1 个。

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 216 个，涉及 IP 地址 374 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 59.7%；在 374 个 IP 中，有约 55.1%位于境内，约 44.9%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 136 个 IP。

本周放马站点域名注册所属境内外分布
(4/1-4/7)



本周放马站点域名所属顶级域的分布
(4/1-4/7)



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。

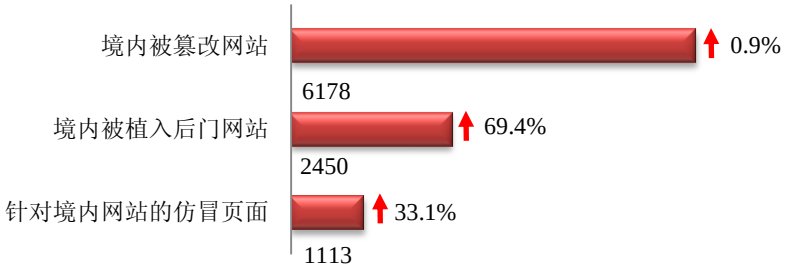
ANVA恶意地址黑名单发布地址

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。

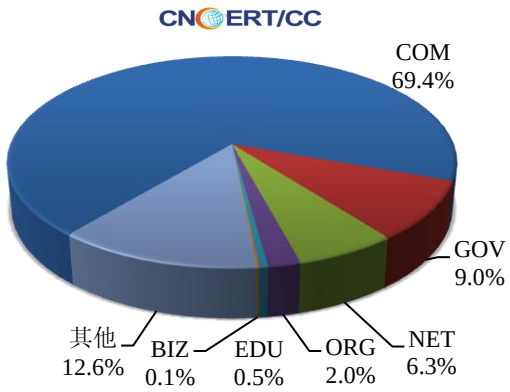
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 6178 个；境内被植入后门的网站数量为 2450 个；针对境内网站的仿冒页面数量为 1113 个。

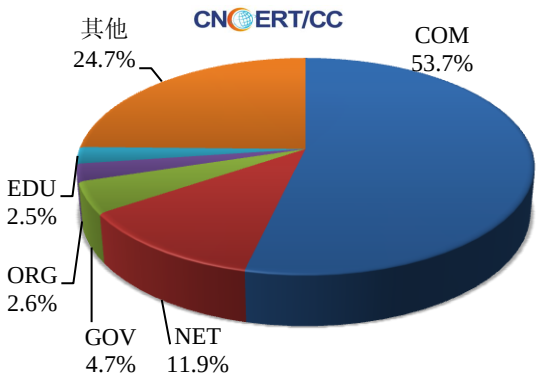


本周境内被篡改政府网站(GOV 类)数量为 558 个（约占境内 9.0%），较上周环比上升了 16.5%；境内被植入后门的政府网站(GOV 类)数量为 114 个（约占境内 4.7%），较上周环比大幅上升了 75.4%；针对境内网站的仿冒页面涉及域名 771 个，IP 地址 297 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/1-4/7)

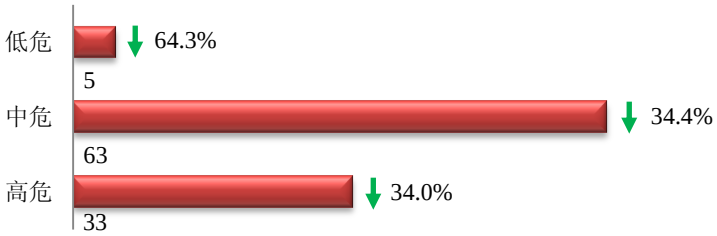


本周我国境内被植入后门网站按类型分布
(4/1-4/7)

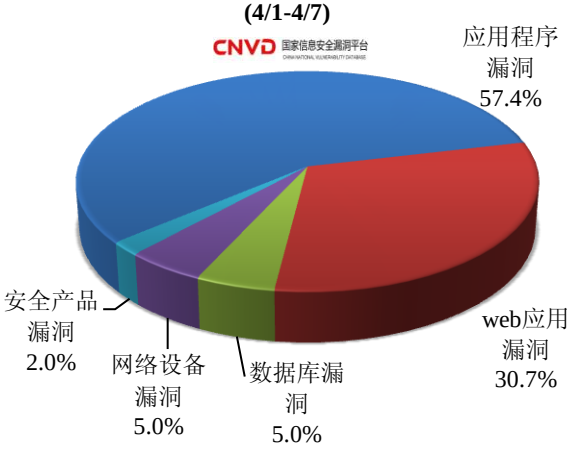


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 101 个，信息安全漏洞威胁整体评价级别为低。



本周CNVD收录漏洞按影响对象类型分布
(4/1-4/7)



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 应用漏洞和数据库漏洞。

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

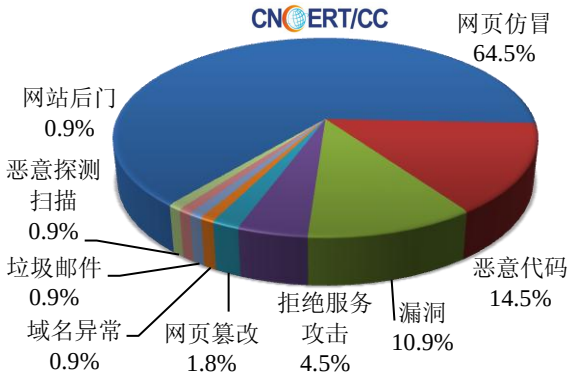
http://www.cnvd.org.cn/publish/main/47/index.html

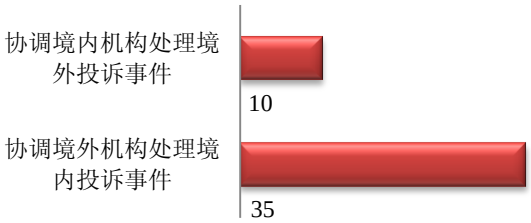
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 110 起，其中有跨境网络安全事件 45 起。

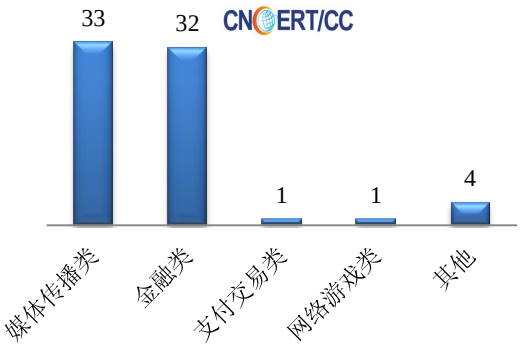
本周CNCERT处理的事件数量按类型分布
(4/1-4/7)





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 71 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包含央视等媒体传播类仿冒事件 33 起、工商银行等金融类仿冒事件 32 起、阿里巴巴等支付交易类仿冒事件 1 起、忘仙等网络游戏类仿冒事件 1 其和其他仿冒事件 4 起。

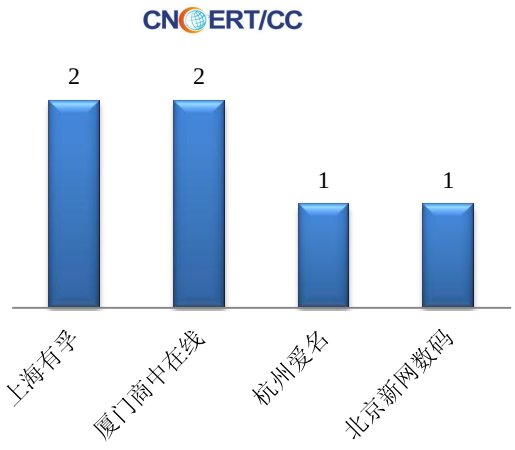
本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(4/1-4/7)



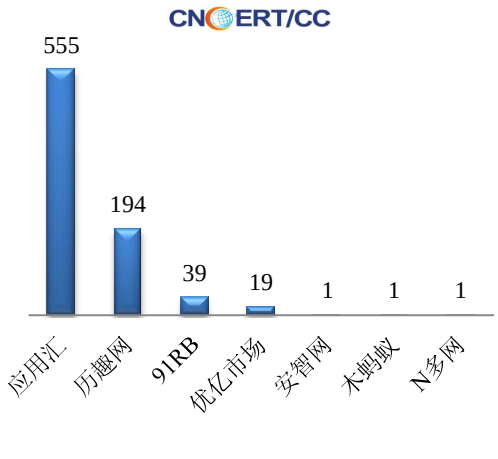
本周CNCERT协调境内域名注册机构处理
网页仿冒事件数量排名 (4/1-4/7)

本周，CNCERT 协调 4 家境内域名注册机构及 7 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恶意域名 6 个、传播移动互联网恶意代码的恶意 URL 链接 810 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 (4/1-4/7)



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 (4/1-4/7)



业界新闻速递

1、韩国防部拟新设网络政策总管科 研发网络战武器

中新网 4 月 2 日消息 据韩联社报道，韩国军方消息人士 4 月 2 日介绍称，目前韩军网络相关工作按功能被分散到军方网络司令部、联合参谋本部、国防部信息化企划官室、机要司令部等多个部门。韩国军方今年上半年将在国防部新设“网络政策总管科”，把这些功能整合在一起。新设部门将由上校级人士带领，主要负责网络防御性武器的相关研发政策、网络战争人力供给计划的制定工作等。这位消息人士表示，美国国防部下面设有网络政策决策部门。韩国也将在上半年新设负责国防网络政策的组织部门。他说，国防网络政策属于韩军固有领域，但有必要时，也会与美国开展合作。该政策的重点在于研发网络战争防御性武器，应对敌对势力对计算机网络的攻击等。韩国国防部计划在相关预算和扩大人力的条件成熟时，将网络战争人员增加到 1000 人以上。

2、墨西哥成立网警队伍 拟加强对网络犯罪监管

中国日报 4 月 4 日消息 日前，墨西哥联邦区公安部门正式成立网警部队，加强对科技化、网络化犯罪的监管。该部队目前由 30 名成员组成，绝大多数成员为系统工程师和网络专家。该部队的日常任务为维护墨西哥联邦区网络安全，同时预防和阻止以网络为平台的犯罪形式，如勒索、欺诈、身份资料窃取乃至网络团伙卖淫等等。对此，联邦区治安负责任赫苏斯·罗德里格斯表示了积极的评价和较高的期望。他对墨西哥联邦区网警部队未来将取得的成绩抱有极大信心。相信通过网警部队的努力，将会切实维护该地区乃至墨西哥网络用户的人身、财产安全和利益不受侵犯。据介绍，这次行动由墨西哥和韩国合作完成，这支队伍的所有成员此前均接受了韩国网警专家的相关培训。

3、美国防部要求陆军改善商用移动设备网络安全性

中新网 4 月 2 日消息 据一份来自美国国防部总检察长的报告显示，美国陆军首席信息官迄今为止，尚未针对商用移动设备(CMDs)实施有效的网络安全项目。商用移动设备的服务与其他网络一样，易受网络攻击且有可能泄露敏感数据。美国防部总检察长正在努力研究，以确定陆军是否存在一项能够监视并降低商用移动设备与移动媒介风险的有效网络安全项目。在对站点监察过程中，总检察长力图核实陆军官员是否正确地对商用移动设备进行了追踪、配置和审查。他同时透露了许多与商用移动设备网络攻击相关的实际问题，其中一个问题是陆军首席信息官在对存储的信息进行保护时，并未使用陆军指令，对商用移动设备安全地进行配置。特别强调的是，美国军事学院和美国陆军工程兵工程研究与开发中心的首席信息官们并未使用移动设备管理软件配置商用移动设备，以保护存储的信息。其他的网络攻击障碍涉及到陆军首席信息官失职的地方表现在：没有恰当地审核商用移动设备、没有控制做移动媒介用途的商用移动设备、没有进行必要的培训以及没有使用针对商用移动设备的专门协议。为补救目前的状况，陆军首席信息官应该提出清晰且完整的政策，包括报告所有商用移动设备的追踪需求，扩大对目前所使用的全部商用移动设备的信息保障需求。

4、美国运通遭网络攻击致运营瘫痪数小时

人民网 4 月 1 日消息 据纽约时报昨日（3 月 31 日）报道称，美国著名的金融公司美国运通公司当地时间周四遭到黑客组织的网络攻击，致使该公司持续数小时运营瘫痪。据报道，这次对美国金融企业的网络攻击技巧高超。黑客并非遵循传统利用一些个人电脑向每家银行发送网络流量，而是利用高级的恶意软件侵入强大的商业数据中心，命令它们同步向每一家银行展开攻击。研究这些攻击的安全专家表示，这和最近六个月导致摩

根大通、富国银行、美国银行和其他一些金融机构瘫痪的攻击是由同一批人发动的。一个自称卡桑网络战士的组织声称对之前那些攻击负责。纽约时报猜测，该名字或许为了纪念上世纪 30 年代著名巴勒斯坦反英人士阿兹丁·卡桑。该组织称，它是为了去年秋天上传到 YouTube 上的一段反伊斯兰教视频而实施报复。但美国情报官员和行业调查人员说，这个组织只是伊朗的一个理想掩护。它们之间的关系有多紧密，该组织的行动是否受命于伊朗政府，目前还不清楚。政府官员和银行的管理者也还没有拿出确切的证据。

5、黑客组织攻击朝鲜外宣网站 公布九千多名会员信息

国际在线 4 月 7 日消息 据韩国《东亚日报》4 月 6 日报道，一个名为“匿名者”的国际黑客组织继 3 月 4 日攻击朝鲜对外宣传网站“我们民族之间”，并公开该网站 9001 名会员的个人信息之后，4 月 6 日追加公开了 500 名该网站会员的个人信息。“我们民族之间”是朝鲜祖国和平统一委员会运营的网站，韩国禁止本国国民浏览，但仍有部分韩国网民通过特殊渠道访问该网站。此次对朝鲜对外宣传网站“我们民族之间”发动网络攻击的名为“匿名者”的黑客组织 2003 年成立于美国。该组织曾对美国中央情报局（CIA）、北大西洋公约组织（NATO）、苹果公司等机构与企业进行过网络攻击，获取对方的秘密情报或导致对方网络瘫痪。该组织 4 月 2 日曾公开表示，要求朝鲜停止开发核武器、停止核威胁，否则将发起网络战争。另据韩国媒体报道，韩国国家情报院已经着手调查被该黑客组织公开个人信息的会员名单。韩国国情院方面称，将会先确认会员名单中的韩国公民是否加入朝鲜组织，再判断这些人是否违反韩国《国家保安法》。

6、以色列多家政府网站遭黑客攻击 但损失不大

中新网 4 月 7 日电 据外电报道，以色列一位顶级网络专家 4 月 7 日称，以色列多家政府网站遭到黑客的网络攻击，但是损失并不大。多名黑客联合黑客组织“匿名者”攻击了以色列总理办公室、国防部、教育部与中央统计局等机构的网站，但所有的网站都运转正常。以色列财政部发布声明称，截至(当地时间)4 月 7 日中午(北京时间下午 5 点)，以色列政府机关网站对公众正常开放。声明称，教育部网站一度“由于技术故障”停止运转。据报道，“匿名者”4 月 6 日发布声明称将对以色列网络实施第二次大举进攻。2012 年 11 月，“匿名者”曾对以色列实施大规模网络攻击，当时 5000 多名以色列军官的个人信息被公诸于众，此前 7 万多家以色列网站遭袭，国防部和财政部也未能幸免。

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：王英

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990316