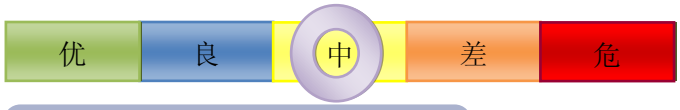
国家互联网应急中心

2013 年第 12 期

3 月 18 日-3 月 24 日

网络安全信息与动态周报

本周网络安全基本态势

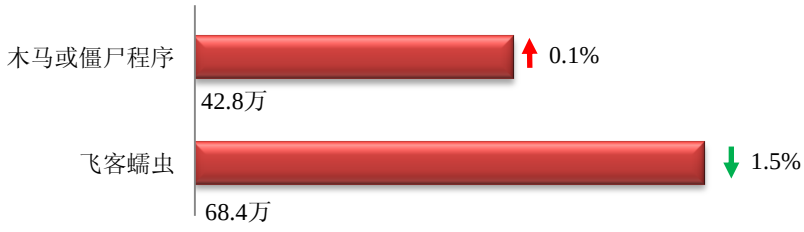


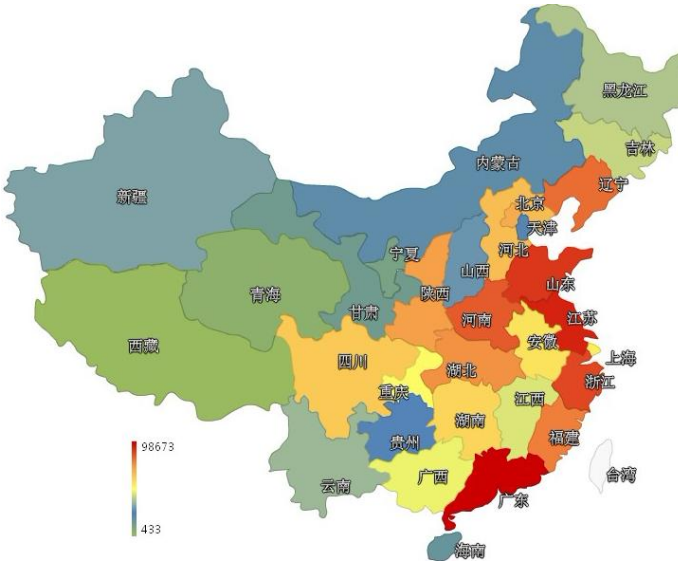
境内感染网络病毒的主机数量	• 111.2 万	↓ 0.9%
境内被篡改网站总数 其中政府网站数量	• 6266 • 487	↓ 2.0% ↑ 2.5%
境内被植入后门网站总数 其中政府网站数量	• 1979 • 104	↓ 4.5% ↓ 1.0%
针对境内网站的仿冒页面数量	• 1156	↑ 29.0%
新增信息安全漏洞数量 其中高危漏洞数量	• 118 • 50	↓ 4.8% ↓ 7.4%

= 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 111.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 42.8 万以及境内感染飞客（conficker）蠕虫的主机约 68.4 万。



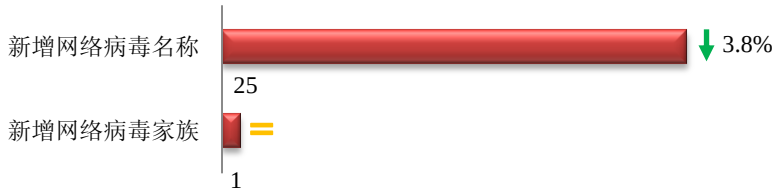


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和山东省。

TOP3

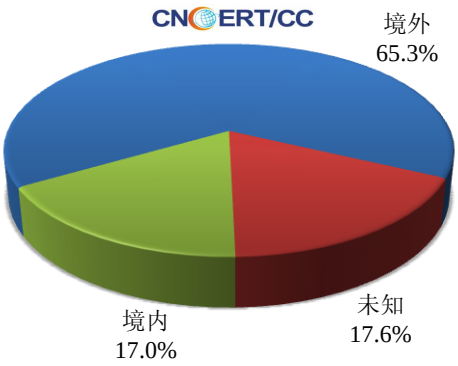
广东省	•约9.9万个（约占中国大陆总感染量的23.0%）
江苏省	•约3.1万个（约占中国大陆总感染量的7.3%）
山东省	•约2.8万个（约占中国大陆总感染量的6.6%）

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 25 个，按网络病毒家族统计新增 1 个。

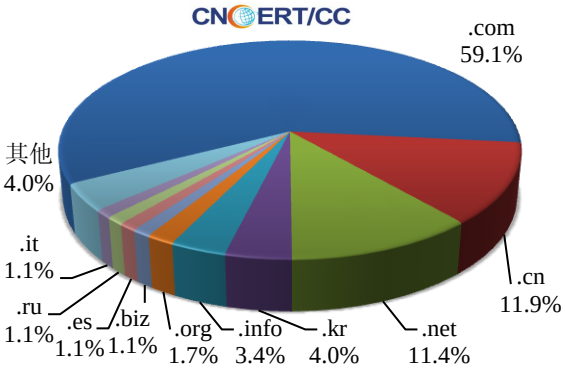


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 176 个，涉及 IP 地址 284 个。在 176 个域名中，有约 65.3%为境外注册，且顶级域为.com 的约占 59.1%；在 284 个 IP 中，有约 58.7%位于境内，约 41.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 100 个 IP。

本周放马站点域名注册所属境内外分布
(3/18-3/24)



本周放马站点域名所属顶级域的分布
(3/18-3/24)



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。

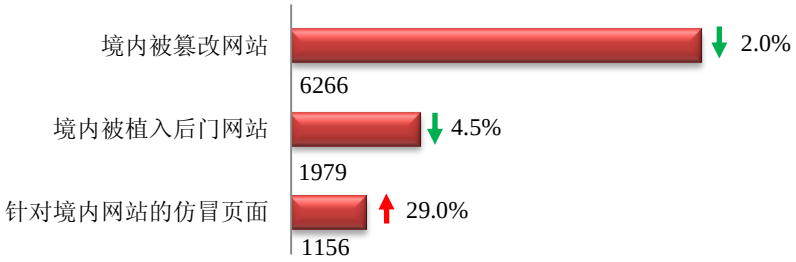
ANVA恶意地址黑名单发布地址

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。

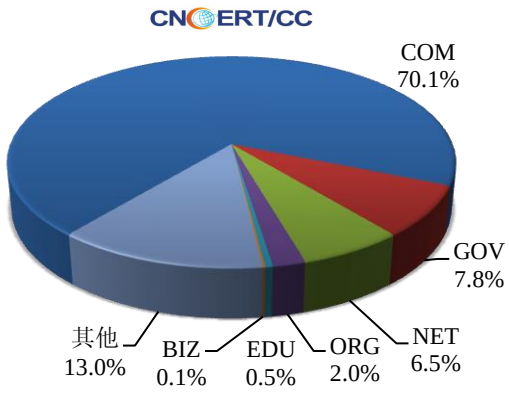
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 6266 个；境内被植入后门的网站数量为 1979 个；针对境内网站的仿冒页面数量为 1156 个。

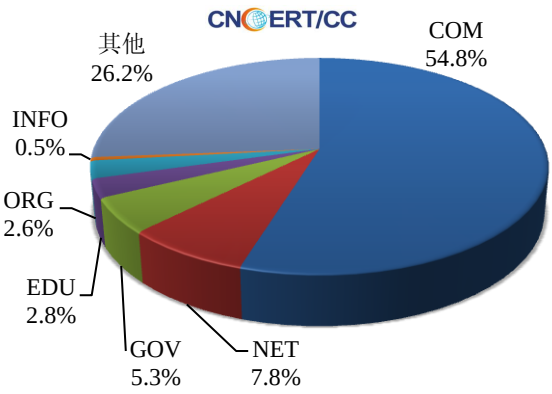


本周境内被篡改政府网站(GOV 类)数量为 487 个（约占境内 7.8%），较上周环比上升了 2.5%；境内被植入后门的政府网站(GOV 类)数量为 104 个（约占境内 5.3%），较上周环比减少了 1%；针对境内网站的仿冒页面涉及域名 737 个，IP 地址 318 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/18-3/24)

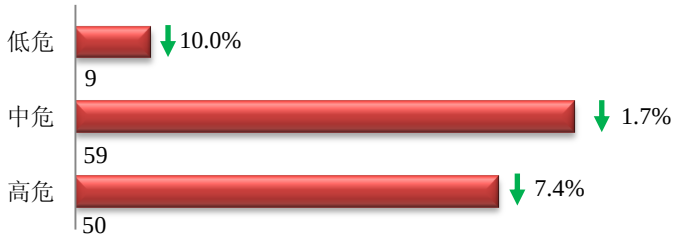


本周我国境内被植入后门网站按类型分布
(3/18-3/24)

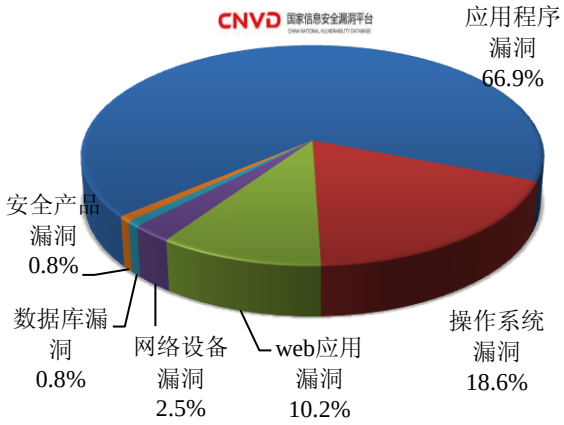


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 118 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
(3/18-3/24)



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

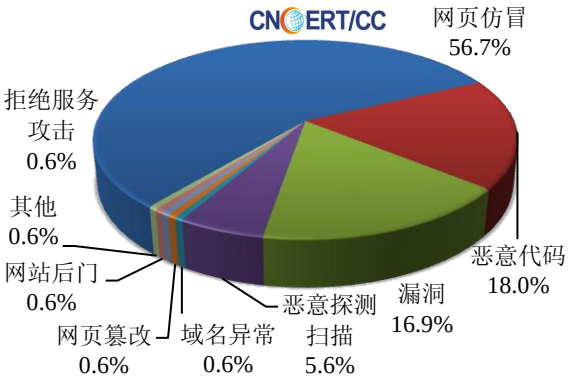
http://www.cnvd.org.cn/publish/main/47/index.html

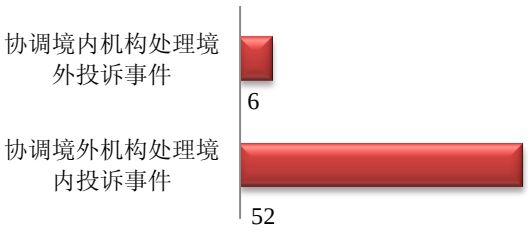
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 178 起，其中有跨境网络安全事件 58 起。

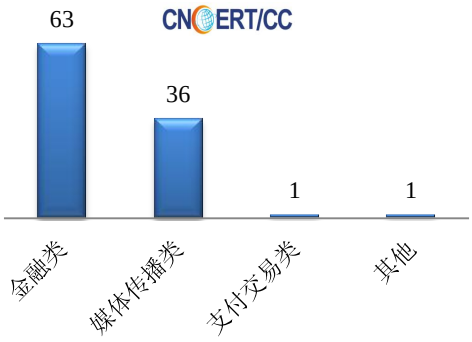
本周CNCERT处理的事件数量按类型分布
(3/18-3/24)



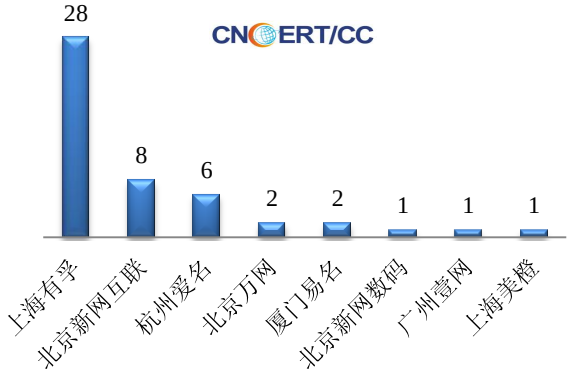


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 101 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包含工商银行等金融类仿冒事件 63 起、央视等媒体传播类仿冒事件 36 起、淘宝等支付交易类仿冒事件 1 起和其他仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(3/18-3/24)

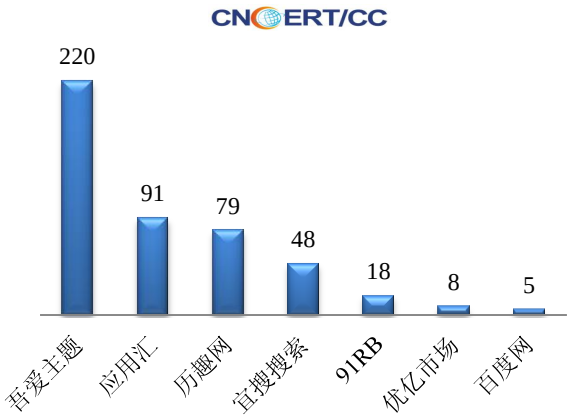


本周CNCERT协调境内域名注册机构处理
网页仿冒事件数量排名 (3/18-3/24)



本周，CNCERT 协调 1 家非经营性互联单位及 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域名 37 个、传播移动互联网恶意代码的恶意 URL 链接 469 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 (3/18-3/24)



业界新闻速递

1、北约五国联合启动赛博防御能力开发计划

新华网 3 月 18 日消息 据悉，3 月 14 日，在北约通信与信息局(NCIA)的支持下，加拿大联合丹麦、荷兰、挪威和罗马尼亚四国，启动了多国赛博防御能力开发计划(MNCD2)。多国赛博防御能力开发计划旨在促进赛博防御信息共享，将允许国与国之间共享威胁和攻击信息，并合作开发可改善信息共享的技术以及先进的赛博防御传感器。在北约通信与信息局的支持下，该计划将成为改善北约整体应变能力的重要环节。与每个国家独立发展网络防御能力相比，多国赛博防御能力开发计划可采用更加经济的方式实现目标，同时也鼓励北约各成员国之间网络安全的多样性。根据这一计划，各国可以将主要精力放在各自关注领域，其他国家都将从中受益，从而实现“人人为我，我为人人”的局面。该计划可通过联合研发和采购降低成本，能够大幅度节省长期投资，而且开发出的成果天然具有互操作性。

2、美开发无线网络防御技术 部分节点受损仍可运行

中新网 3 月 21 日电 据悉，美国国防先期计划研究局(DARPA)的军用通信专家表示，将启动无线网络防御项目，以确保在若干节点受损的情况下，语音和数据无线网络持续可用。DARPA 表示，将于 4 月 1 日上午 9 点到 12 点向工业界发布无线网络防御项目的相关简介。DARPA 无线网络防御项目旨在开发新的网络协议，确保个别节点出现无意的配置错误或受到攻击损毁的情况下，整个网络依然能够保持正常运行。无线网络防御项目经理 Wayne Phoel 表示，当前的安全工作重点主要关注单个电台或节点，而不是网络本身，致使如果单个节点配置错误或出现受损，就会致使整个网络效率降低。这就需要对控制无线网络的方式做出改变，通过开发基于一种网络的解决方案，在认识到网络中有可能存在损坏节点的前提下，可以绕过其进行组网。该项目将开发协议，以确定相邻节点间通信的可行性和可信性，并且自动对网络进行配置，以确保容错运行。该项目经理还表示，将吸收信用卡防盗刷机制的经验，利用多种参数来辨别节点的有效性。

3、CNCERT 发布《2012 年我国互联网网络安全态势综述》

CNCERT 网站消息，2013 年 3 月 19 日，国家互联网应急中心（CNCERT）在京举办了“2012 年我国互联网网络安全态势综述”（简称“态势综述”）发布会，对 2012 年我国互联网网络安全总体态势和主要特点进行了发布和说明。来自重要信息系统运行部门、基础电信运营企业、域名注册管理和服务机构、行业协会、互联网企业和安全厂商等 73 家单位的 97 位专家和代表出席了发布会。CNCERT 运行部周勇林主任对态势综述做了详细阐述和讲解，并回答了媒体提问。态势综述从 CNCERT 视角出发，结合 CNCERT 监测数据和通信行业报送信息，经归纳分析后，总结概括了 2012 年我国互联网网络安全威胁的新特点、新趋势，介绍了 CNCERT 在维护网络安全方面开展的相关工作，展望了 2013 年值得关注的网络安全威胁和热点问题，提出了若干对策建议。CNCERT 希望此态势综述能够帮助政府机构、重要信息系统部门、通信行业相关单位和广大网民了解掌握当前网络安全面临的主要威胁和发展形势，进一步提高网络安全意识，加强自身网络信息系统安全防护，共同维护我国互联网网络安全。

4、我国协助调查发现 韩国多家广播电视台及银行遭受攻击来自韩国境内而非中国

CNCERT 网站消息，3 月 20 日，CNCERT 从互联网、FIRST 组织和 APCERT 组织了解到韩国主要广播电视台 KBS、MBC、YTN，以及韩国新韩银行（ShinNan Bank）、农协银行（NongHyup Bank）等部分金融机构

疑似遭受黑客攻击，相关网络与信息系统突然出现瘫痪。CNCERT 立即联系韩国国家级应急响应组织 KrCERT 了解具体情况。3 月 21 日，CNCERT 从互联网得知，韩国民官军联合应对小组证实，向韩国多家广播电视台及银行等金融机构植入恶意代码的 IP 来自中国。CNCERT 再次迅速联系了 KrCERT。据 KrCERT 称，通过对农协银行的计算机系统进行分析后发现，黑客经由我国的 IP 地址（101.106.25.105）攻击韩国部分电视台和金融公司的杀毒软件管理服务器，并植入了恶意程序。然而，经 CNCERT 的深入调查和分析，发现此 IP 自去年 8 月起已停用。CNCERT 立即于 22 日向 KrCERT 进行了反馈，并要求韩方提供攻击分析报告及相关证据线索。韩国民官军联合应对小组经过再次调查发现，农协银行一直使用私自设立的 IP 地址，而这恰好与中国的 IP 地址一致。参加此次调查的相关负责人在对遭到黑客攻击的农协银行内部电脑进行分析时，误认为这是国际公认的中国 IP 地址。韩国民官军联合应对小组于 3 月 22 日下午 16 时在韩新社正式发布消息称，3 月 20 日导致韩国部分电视台和金融公司计算机网络全面瘫痪的恶意代码来自韩国境内电脑，而不是中国。

5、BBC 多个 Twitter 账户遭"叙利亚网络军团"黑客攻击

国际在线 3 月 22 日消息 据英国广播公司 3 月 21 日报道，英国广播公司（BBC）多个 Twitter 账户被自称“叙利亚网络军团”的黑客攻击，包括 BBC 天气、阿拉伯语和阿尔斯特电台（Radio Ulster）。报道称，从 3 月 21 日下午开始，BBC 天气 Twitter 账户发布了一系列中东国家假的天气情况信息。此前，BBC 阿拉伯语和阿尔斯特电台的 Twitter 账户也遭到劫持。阿拉伯语节目总编法里斯 库里（Faris Couri）说：“账户被劫持后，发布了多条亲叙利亚政权信息。我们谴责这种行为，并向所有观众道歉。”BBC 方面表示，现在他们已经重新控制了上述三个账户，所有不合适的内容都已被删除。一个自称“叙利亚网络军团”的组织宣称对此负责，该组织发布支持叙利亚总统巴沙尔 阿萨德（Bashar-al-Assad）的信息。3 月 21 日下午，BBC 工作人员还被要求警惕一种网络钓鱼电子邮件，它能将 BBC 的电子邮件帐户发送出去。目前尚不清楚这两起事件是否存在关联。网络钓鱼电子邮件中有一个链接，如果点击就可能暴露密码信息。

6、Mac OS X 出现新的恶意插件 肆意显示网页广告

凤凰网 3 月 21 日消息 Mac OS X 平台最近出现一种恶意的广告插件，可在受攻击的 Mac 肆意显示网页广告，这款恶意插件的开发者也就能从中牟利。这一木马称之为 Trojan.Yontoo.1，增长速度较快。这种病毒植入 Mac 的途径很多，但最有趣的是通过几个特制的“电影预告片”。预告片将会以普通的方式弹出对话框，如果用户点击“安装插件”，恶意广告插件将立即安装到用户的 Mac 中。其他传播途径还包括媒体播放器、视频画质增强器、加速器等。弹出的对话框提示用户安装“Free Twit Tube”，因此用户在安装软件的过程中发现弹窗需警惕，目前发现 Safari、Chrome 和 Firefox 无法拦截这一恶意插件。虽然黑客最初的目标是 OS X，但很快有可能就会瞄准 Windows 平台。

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：苏燕谨

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990316