国家互联网应急中心

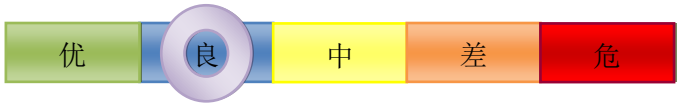
网络安全信息与动态周报

2016 年第 4 期

1 月 18 日-1 月 24 日

CNCERT/CC

本周网络安全基本态势

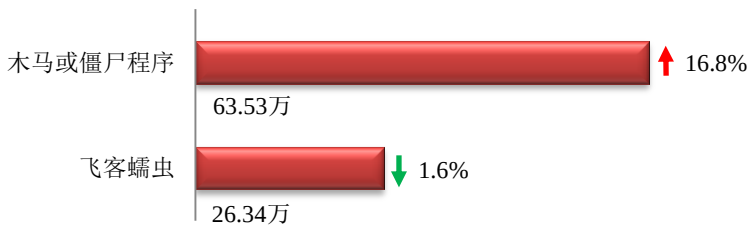


境内感染网络病毒的主机数量	•89.87万	↑ 10.7%
境内被篡改网站总数 其中政府网站数量	•4295 •72	↓ 5.3% ↓ 1.4%
境内被植入后门网站总数 其中政府网站数量	•1229 •49	↓ 40.8% ↓ 10.9%
针对境内网站的仿冒页面数量	•2859	↓ 58.5%
新增信息安全漏洞数量 其中高危漏洞数量	•165 •56	↑ 39.8% ↑ 40.0%

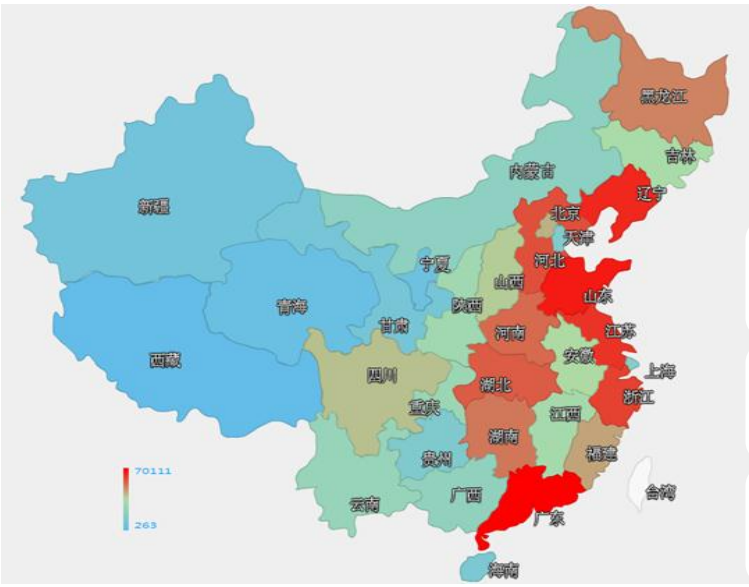
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 89.87 万个，其中包括境内被木马或被僵尸程序控制的主机约 63.53 万以及境内感染飞客（conficker）蠕虫的主机约 26.34 万。



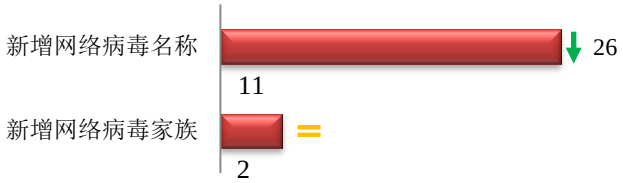
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和辽宁省。



TOP3

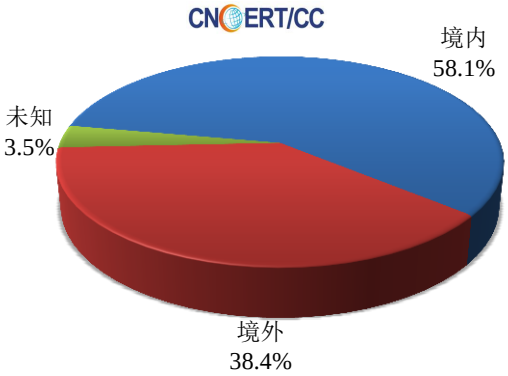
广东省	•约7.0万个（约占中国大陆总感染量的11.0%）
山东省	•约6.9万个（约占中国大陆总感染量的10.9%）
辽宁省	•约6.1万个（约占中国大陆总感染量的9.6%）

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 11 个，按网络病毒家族统计新增 2 个。

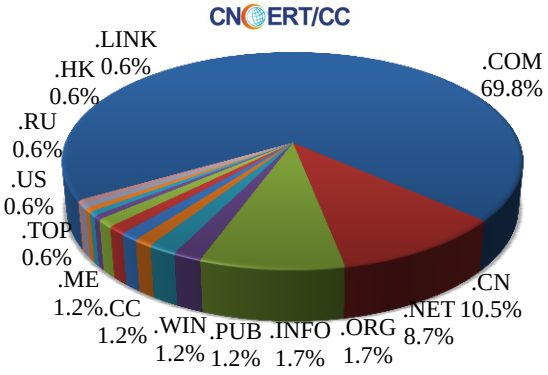


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 172 个，涉及 IP 地址 353 个。在 172 个域名中，有约 38.4%为境外注册，且顶级域为.com 的约占 69.8%；在 353 个 IP 中，有约 12.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 48 个 IP。

本周放马站点域名注册所属境内外分布
(1/18-1/24)



本周放马站点域名所属顶级域的分布
(1/18-1/24)



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。

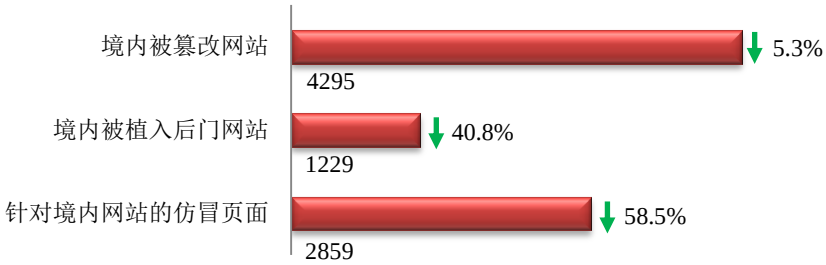
ANVA恶意地址黑名单发布地址

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。

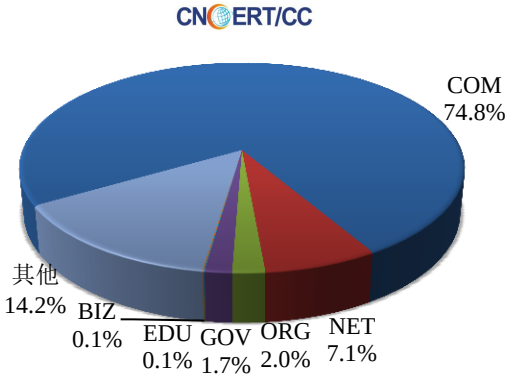
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4295 个；境内被植入后门的网站数量为 1229 个；针对境内网站的仿冒页面数量为 2859。

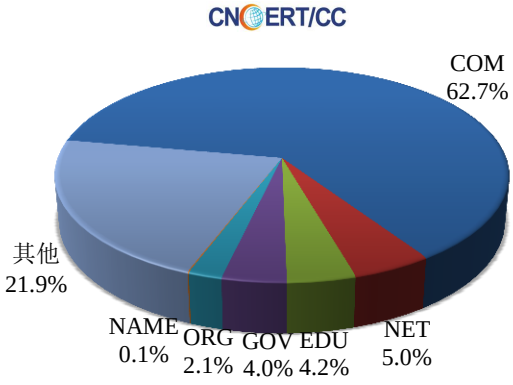


本周境内被篡改政府网站(GOV 类)数量为 72 个（约占境内 1.7%），较上周环比下降了 1.4%；境内被植入后门的政府网站(GOV 类)数量为 49 个（约占境内 4.0%），较上周环比下降了 10.9%；针对境内网站的仿冒页面涉及域名 2413 个，IP 地址 767 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/18-1/24)

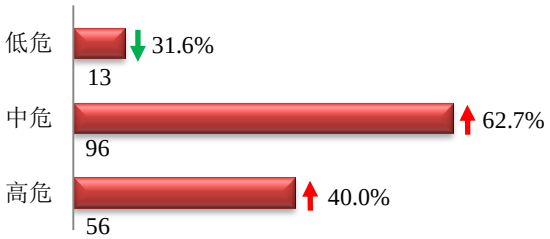


本周我国境内被植入后门网站按类型分布
(1/18-1/24)

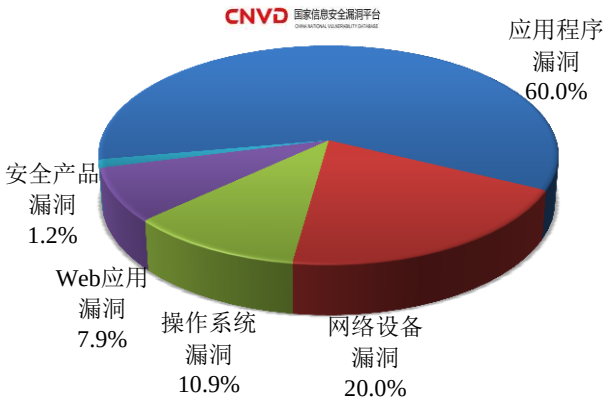


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 165 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
(1/18-1/24)



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

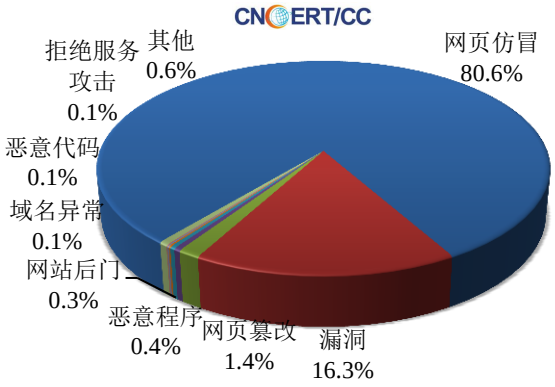
http://www.cnvd.org.cn/webinfo/list?type=4

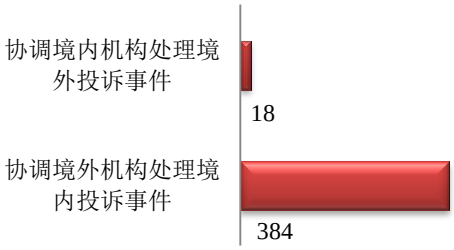
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 2129 起，其中跨境网络安全事件 402 起。

本周CNCERT处理的事件数量按类型分布
(1/18-1/24)

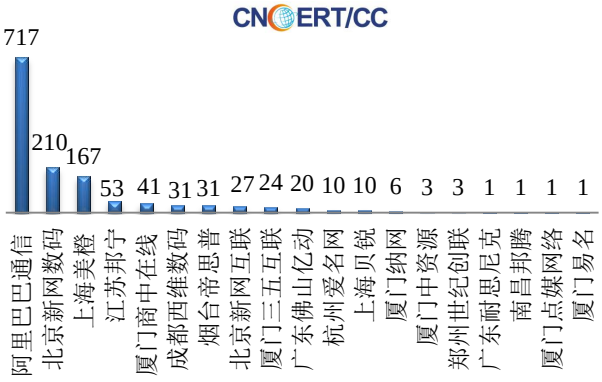




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1716 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 1453 起和互联网服务提供商仿冒事件 250 起。

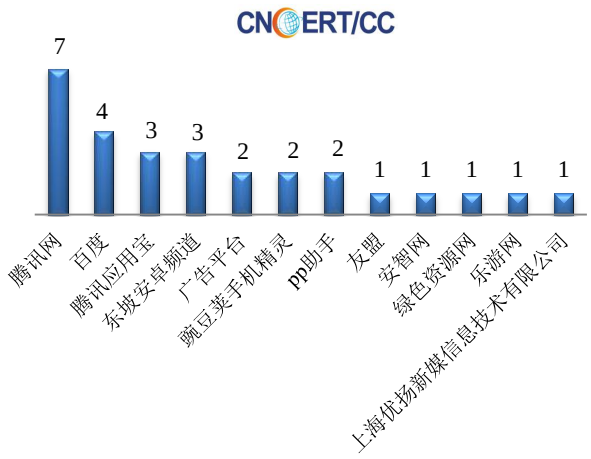
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(1/18-1/24)

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 (1/18-1/24)



本周，CNCERT 协调 12 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 28 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 (1/18-1/24)



业界新闻速递

1、中央政法委：构建维护网络安全新格局

央广网 1 月 22 日消息 中共中央政治局委员、中央政法委书记孟建柱今天在中央政法工作会议上分析，我国面临的安全风险不少来自网络，网络安全对国家不少领域安全具有牵一发动全身的意义，没有网络安全就没有国家安全。中央政法委要求按照建设网络强国的要求，坚持网上治理和网下管理相统一、专门力量和社会力量相统筹，构建维护网络安全新格局。孟建柱强调，要健全工作机制，及时发现、打击编造和恶意传播谣言违法犯罪活动。督促互联网企业落实主体责任，第一时间发现、处理有害信息。孟建柱分析，当前，传统违法犯罪不断向网上蔓延，网络黄赌毒、金融诈骗、贩枪、传授制爆技术等违法犯罪明显增多，严重影响公共安全。要加强网站“网安警务室”建设，加强网警网上公开巡查执法，健全网上网下一体化打防管控机制，提高对网络违法犯罪的发现、处置能力。针对网络犯罪分子跨地域作案等特点，司法机关要形成打击网络犯罪合力。加强与银行、电信及互联网企业的合作，加大对网络违法犯罪产生链打击力度，从根本上遏制网络违法犯罪高发势头。孟建柱指出，我国信息技术产品国产化率比较低，不少缺少必要的安全防护手段，易受网络攻击；窃取、泄露单位和个人信息等案事件时有发生，侵犯公民隐私权，影响国家安全。要加大对窃取、泄露单位、个人信息和企业商业秘密违法犯罪打击力度，维护公民、企业合法权益。

2、美国国安局局长：美国即将部署先进网络武器

中新网 1 月 22 日消息 据美媒报道，美国网络司令部司令罗杰斯（音译，Mike Rogers）上将 21 日称，美军已经花了五年时间开发先进的网络武器和数字作战能力，可能很快会对这些武器和能力进行更为公开的部署。罗杰斯表示，美国决策者已大体上就何时可动用网络武器进行防御的交战规则达成一致。他同时还兼任美国国家安全局局长。不过，对于何时应动用网络武器实施“攻击”，例如针对某个组织或外国发动攻击，目前仍无定论。罗杰斯称，可以说美国现在已处在转折点上。他表示，这些网络作战能力已开始上线，一些相当有形的能力已开始发挥作用。他强调，美军将开始扩大这些网络作战力量的部署范围。不过，罗杰斯并未透露未来几个月如何对上述网络作战力量进行部署的细节。他表示，与其他作战形式一样，决策者已在研究制定适用于应对网络攻击的相关标准。罗杰斯还表示，美国国家安全局将启动机构重组，以便更好地融合该局的两项职能，一项是开展数字间谍和信息收集工作，另一项职能是保护信息安全。

3、日产日本与美国官网遭黑客攻击 被迫关停

环球网 1 月 18 日消息 据美国媒体 leftlanenews1 月 16 日消息，日产公司日本与美国的官方网站近日受到黑客组织 Anonymous 的攻击。日产现已主动关停了上述网站。据悉，此次 Anonymous 黑客组织的组织者以“OpWhales”为名，目的是为了呼吁人们停止狩猎鲸鱼和海豚为食的残忍做法。现在在全球范围内只有日本，挪威和冰岛是捕鲸的合法国家，而该组织也针对包括日本和冰岛的政府网站、日本首相安倍晋三的个人网站在内的多个目标发起网络攻击。目前尚不知晓日产和捕鲸、捕猎海豚有什么联系。绝大部分情况下，匿名者组织都是将攻击矛头指向涉及捕杀鲸鱼和海豚的日本官方站点的，而针对日产官网的攻击则表明匿名者组织的攻击

方向在发生变化。日产主动关闭旗下网站也是确保手中顾客的资料不会泄露。Anonymous 是一个横跨全球，结构松散的黑客组织，任何人都可以宣称代表该组织或属于该组织。福克斯新闻网将该组织称为“对世界网络威胁最大的组织”。该组织曾经报道过巴黎的枪击事件，以及在美国警方屠杀手无寸铁的非裔美国人等事实。

4、乌克兰空中交通管制系统受到有针对性的网络攻击

网易 1 月 19 日消息 据路透社报道，在上周末基辅机场受到网络攻击之后，乌克兰正在全面审查政府电脑系统。在此之前，乌克兰的电力系统也受到恶意软件攻击，最终成功导致停电。令人担忧的是，这次遭遇袭击的基辅机场空中交通管制系统和电力系统在同一个网络上运行。不过，相关报告显示，基辅机场安全人员及时发现了攻击，因此没有造成任何实质性损害。在分析此前袭击电力系统的恶意软件之后，有迹象表明，俄罗斯黑客可能是背后偷袭的黑手，目前，乌克兰官方没有证实或者否认这一说法。乌克兰网络安全响应单位，建议遭遇袭击系统的管理员彻底检查日志文件和流量来源。

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：王新镇

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158