国家互联网应急中心

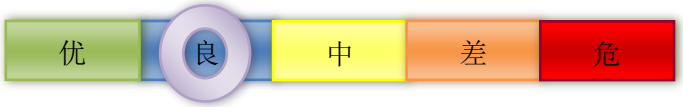
2017 年第 6 期

1 月 30 日-2 月 5 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

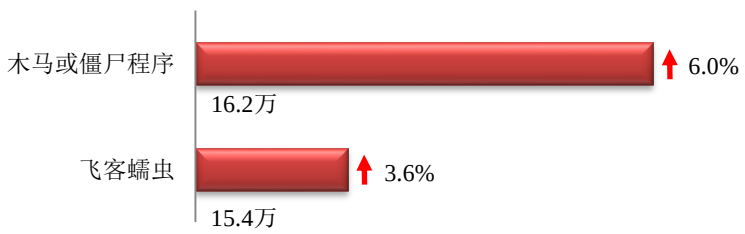


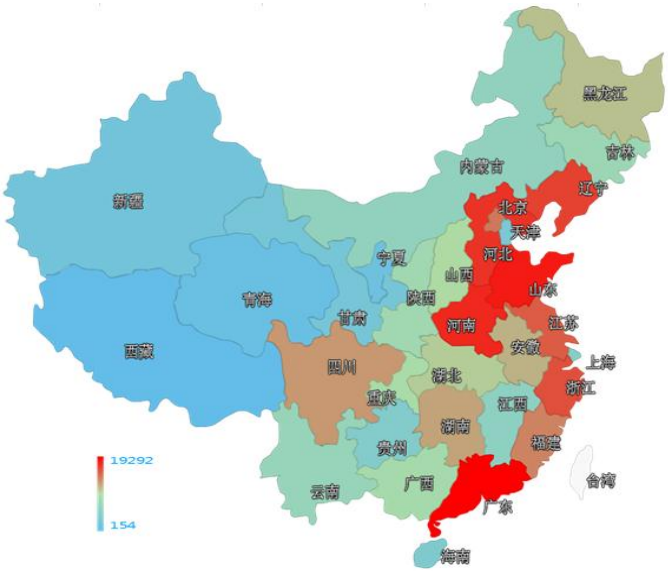
境内感染网络病毒的主机数量	•31.6万	↑ 4.8%
境内被篡改网站总数 其中政府网站数量	•2892 •63	↑ 1.5% ↓ 31.5%
境内被植入后门网站总数 其中政府网站数量	•1108 •11	↓ 0.6% ↑ 22.2%
针对境内网站的仿冒页面数量	•119	↓ 21.2%
新增信息安全漏洞数量 其中高危漏洞数量	•170 •44	

═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 31.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.2 万以及境内感染飞客（conficker）蠕虫的主机约 15.4 万。





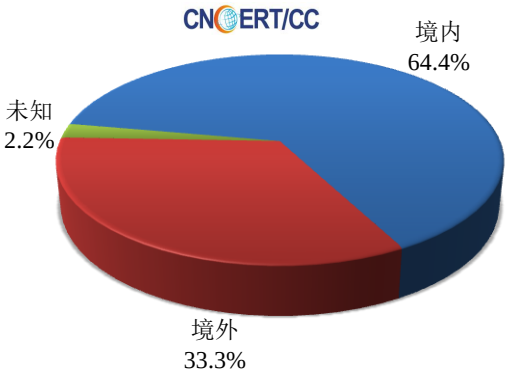
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和河南省。

TOP3

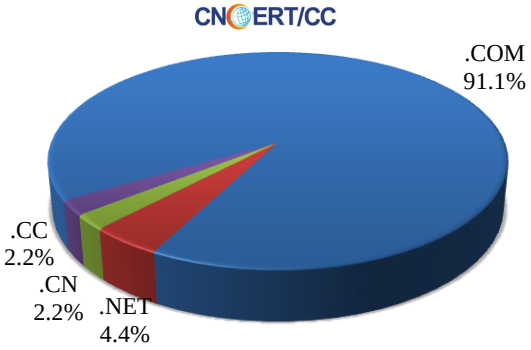
广东省	•约1.9万个（约占中国大陆总感染量的11.9%）
山东省	•约1.7万个（约占中国大陆总感染量的10.2%）
河南省	•约1.1万个（约占中国大陆总感染量的6.9%）

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 45 个，涉及 IP 地址 94 个。在 45 个域名中，有 33.3%为境外注册，且顶级域为.com 的约占 91.1%；在 94 个 IP 中，有约 4.3%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 6 个 IP。

本周放马站点域名注册所属境内外分布
(1/30-2/5)



本周放马站点域名所属顶级域的分布
(1/30-2/5)



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。

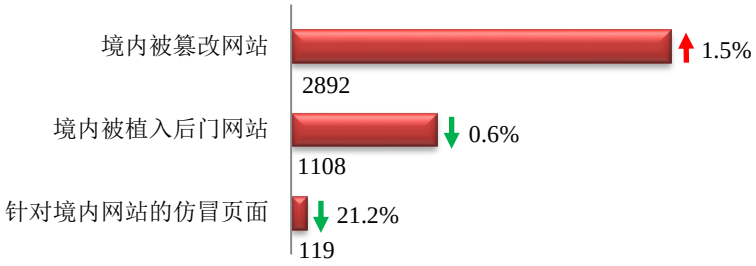
ANVA恶意地址黑名单发布地址

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。

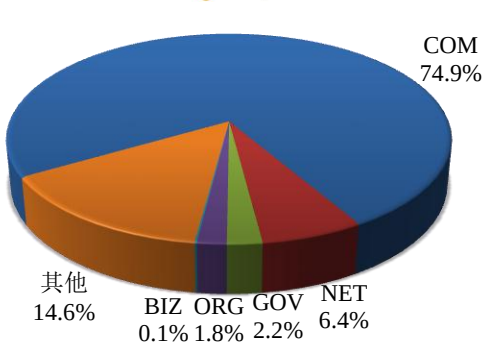
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2892 个；境内被植入后门的网站数量为 1108 个；针对境内网站的仿冒页面数量为 119。

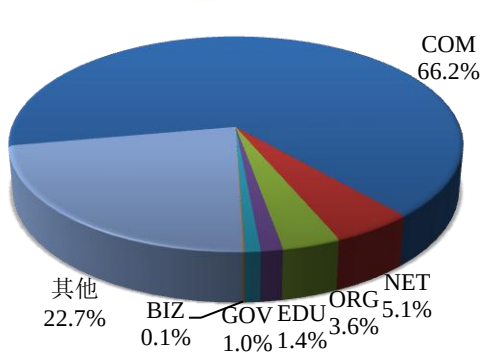


本周境内被篡改政府网站（GOV 类）数量为 63 个（约占境内 2.2%），较上周环比下降了 31.5%；境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 1.0%），较上周环比上升了 22.2%；针对境内网站的仿冒页面涉及域名 102 个，IP 地址 61 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/30-2/5)



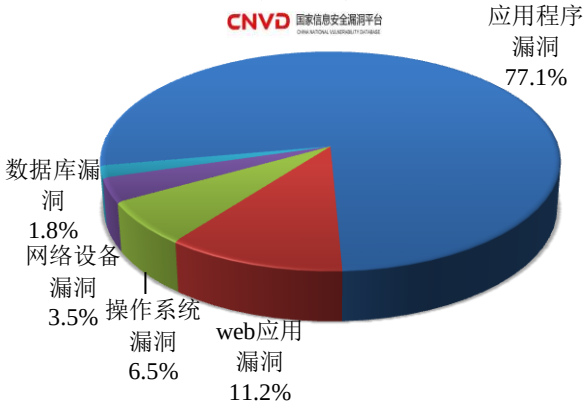
本周我国境内被植入后门网站按类型分布
(1/30-2/5)



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 170 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
(1/30-2/5)



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。

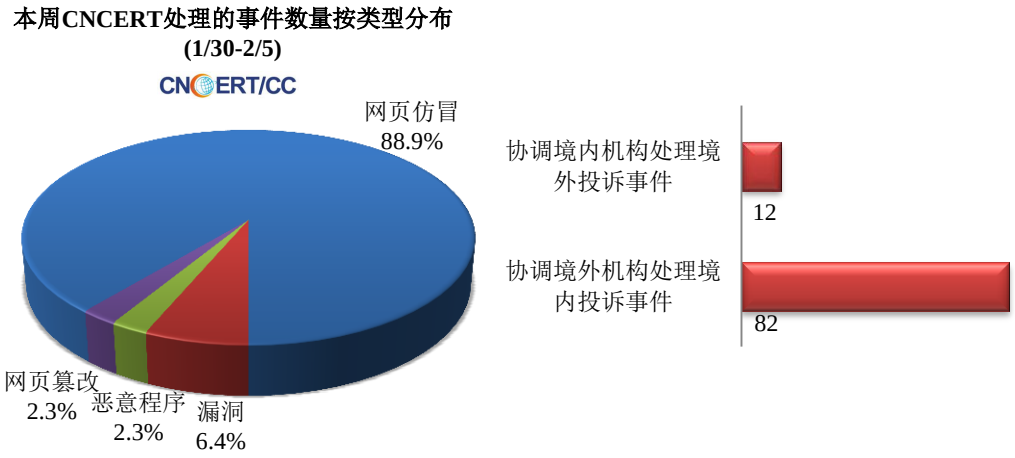
CNVD漏洞周报发布地址

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

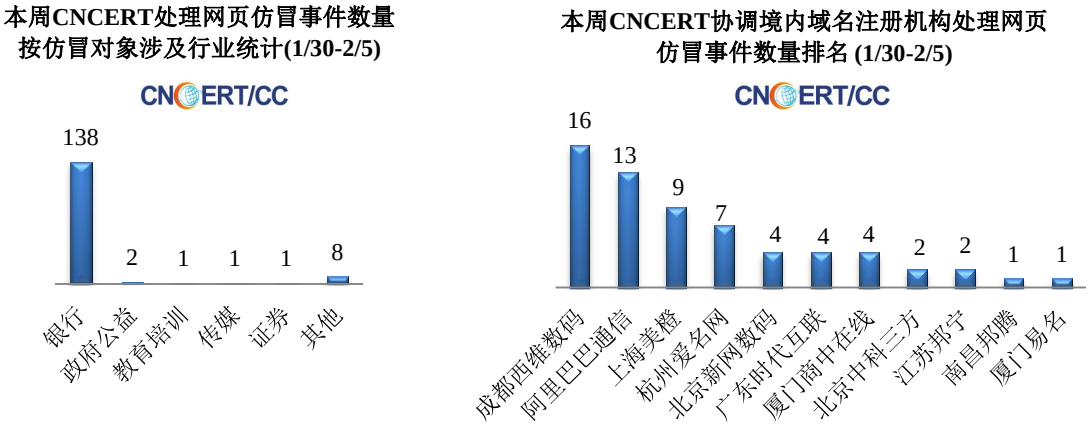
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 171 起，其中跨境网络安全事件 94 起。

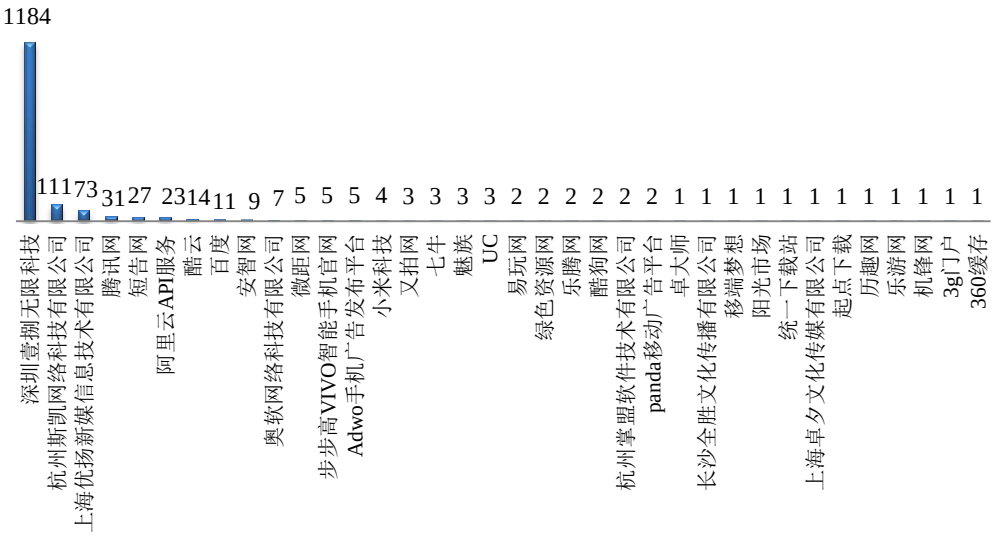


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 151 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 138 起和政府公益仿冒事件 2 起。



本周，CNCERT 协调 36 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 1545 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 (1/30-2/5)



业界新闻速递

1、工信部发布《信息通信网络与信息安全规划（2016-2020）》

中国网信网 1 月 30 日消息 为指导信息通信行业开展“十三五”期间网络信息安全工作，更好地服务网络强国建设和全面建成小康社会的目标要求，服务国家安全和社会稳定的大局，依据《网络安全法》、《中华人民共和国国民经济和社会发展第十三个五年规划纲要》和《国家网络空间安全战略》，近日，工业和信息化部制定印发了《信息通信网络与信息安全规划（2016-2020 年）》（以下简称《规划》）。《规划》围绕贯彻落实习近平总书记关于网络安全和信息化工作的系列重要讲话精神，立足信息通信行业网络与信息安全管理职责，紧扣“十三五”期间行业网络与信息安全工作面临的重大问题，对“十三五”期间行业网络与信息安全工作进行统一谋划、设计和部署，是“十三五”时期信息通信行业网络与信息安全工作的指导性文件。《规划》全面总结了“十二五”期间行业网络与信息安全工作取得的成效，并从国家层面安全工作要求、行业管理改革大局、信息通信技术业务创新发展、国内网络反恐维稳严峻态势、网络空间用户权益保障、国际网络空间竞合复杂形势等六个方面系统分析了“十三五”面临的形势。《规划》明确了以网络强国战略为统领，以国家总体安全观和网络安全观为指引，坚持以人民为中心的发展思想，坚持“创新、协调、绿色、开放、共享”的发展理念，坚持“安全是发展的前提，发展是安全的保障，安全和发展要同步推进”的指导思想；提出了创新引领、统筹协调、动态集约、开放合作、共治共享的基本原则；确定了到 2020 年建成“责任明晰、安全可控、能力完备、协同高效、合作共享”的信息通信网络与信息安全保障体系的工作目标。此外，《规划》共提出了 9 个方面的重点任务，从

强化组织机构建设、加强资金保障、建设新型智库、强化人才队伍、加强宣传教育、规划组织实施等 6 个方面提出了保障措施。

2、我国将建立网络数据安全管理体系 强化用户个人信息保护

新华网 1 月 30 日消息 工信部近日印发《信息通信网络与信息安全规划（2016－2020）》，提出重点从建立网络数据安全管理体系、强化用户个人信息保护、建立完善数据与个人信息泄露公告和报告机制三个方面大力强化网络数据和用户信息保护。工信部提出，将推动建立健全网络与信息安全法律法规制度，构建新型网络与信息安全治理体系，全面提升网络与信息安全技术保障水平。此外，工信部还将加强基础资源信息安全管理、强化增值电信业务信息安全监管、深化互联网新技术新业务信息安全评估、积极营造清朗网络生态环境，同时推动网络安全服务市场发展。据悉，工信部已在全国范围内对互联网网络接入服务市场开展清理规范工作。

3、美法院要求谷歌提交储存在海外服务器的邮件数据

cnBeta.COM2 月 5 日消息 据外媒报道，日前，看起来谷歌不得不遵守由法官 Thomas Rueter 下达的客户邮件搜查令。据悉，该搜查令针对的是谷歌储存在海外服务器的数据。根据法官最新作出的判决，谷歌将需要提交其储存在美国之外的客户邮件数据，以便 FBI 展开一起欺诈案的调查工作。Rueter 法官指出，虽然这种要求谷歌提供海外服务器数据的行为可能涉及到隐私问题，但真正的隐私侵犯只出现在在美国境内公开的时候。谷歌方面表示将对这一判决结果展开上诉，特别是微软先前得到的是一个完全相反的结果。去年 7 月，纽约美国第二巡回上诉法院作出判决，政府机构不能强制要求微软上交其储存在都柏林服务器的数据。几周前，该判决结果再度得到院方肯定。据了解，谷歌已经有在向政府提交其储存在美国境内数据中心的数据，当然前提是要有来自法院的搜查令。

4、黑客通过政府金融监管机构入侵多家波兰银行

E 安全 2 月 5 日消息 根据波兰媒体报道，上周多家波兰银行着手调查黑客入侵活动，而这批黑客在过去三个月中已经入侵了波兰多家金融机构。值得注意的是，恶意软件的感染途径似乎经由波兰金融监管局（简称 KNF）的内部服务器——而该机构本身恰好负责对银行业内的安全标准实施工作进行监督。黑客们并未窃取任何资金。相反，根据波兰媒体所报道，他们泄露了大量尚未识别的加密数据。目前尚不清楚这批黑客的真实身份。根据分析，此次黑客活动已经成为波兰历史上最为严重的攻击行为，且这一复杂入侵所使用的恶意软件无疑是由某个资源丰富的团队所设计并部署。尽管各系统可能自 2016 年 10 月以来就已经受到入侵，但各家银行在大约一个星期之前才发现入侵活动，当时其意识到已经有来自多台工作站的大量加密数据及未知加密可执行文件流出。波兰金融监管局于本周五公开承认攻击活动的存在，暂没有发布任何细节信息。

5、匿名者组织攻陷五分之一“暗网”

cnBeta.COM2 月 4 日消息 近日，大量基于 Tor 网络连接的暗网网站被黑客攻击，超过 1 万个暗网页面被黑客替换成含有警告信息的页面。某隶属于匿名者组织的黑客小组声称对此攻击行为负责，涉及此次攻击的暗网站点采用主流的 Tor 连接 Freedom Hosting II 主机服务，Freedom Hosting II 主机服务彻底被该黑客组织攻破，据安全专家介绍，涉及站点约占暗网组成的五分之一。该黑客组织披露，被攻破的这些暗网站点数据中，超过

半数涉及儿童色情，还有一些比特币担保交易服务，庞氏骗局信息和黑客论坛。黑客向 Freedom Hosting II 主机服务提出可用 0.1 比特币（约为 100 美元）交换泄露数据。Freedom Hosting 初代主机服务在 2013 年被执法部门攻破，当时该主机服务组成了半数暗网访问流量，泄露出大量非法儿童色情数据。

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：郭禹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158