国家互联网应急中心

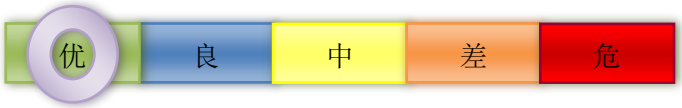
网络安全信息与动态周报

2019 年第 5 期

1 月 28 日-2 月 3 日

CNCERT/CC

本周网络安全基本态势

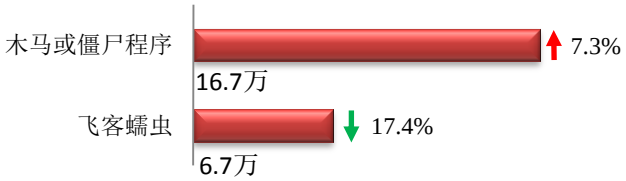


境内感染网络病毒的主机数量	•23.3万	↓1.2%
境内被篡改网站总数 其中政府网站数量	•618 •34	↓11.8% ↓19.0%
境内被植入后门网站总数 其中政府网站数量	•424 •5	↓29.3% ↑66.7%
针对境内网站的仿冒页面数量	•320	↓74.6%
新增信息安全漏洞数量 其中高危漏洞数量	•205 •51	↑15.8% ↓21.5%

=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

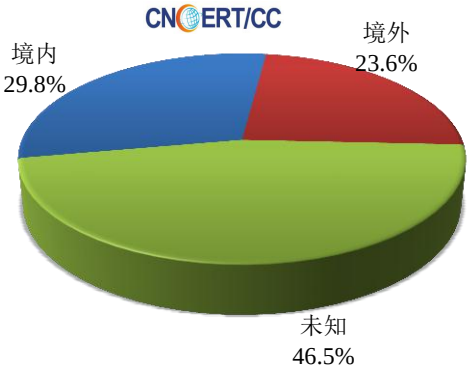
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 23.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.7 万以及境内感染飞客（conficker）蠕虫的主机 6.7 万。

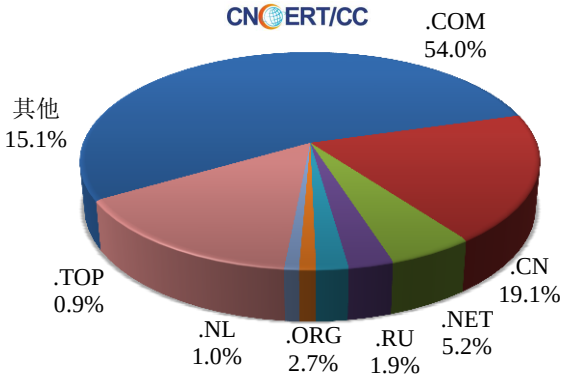


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2275 个，涉及 IP 地址 4517 个。在 2275 个域名中，有 23.6%为境外注册，且顶级域为.com 的约占 54.0%；在 4517 个 IP 中，有约 50.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 421 个 IP。

本周放马站点域名注册所属境内外分布
(1/28-2 /3)



本周放马站点域名所属顶级域的分布
(1/28-2/3)



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。

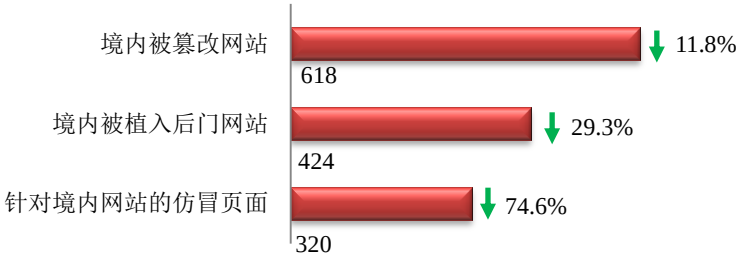
ANVA恶意地址黑名单发布地址

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。

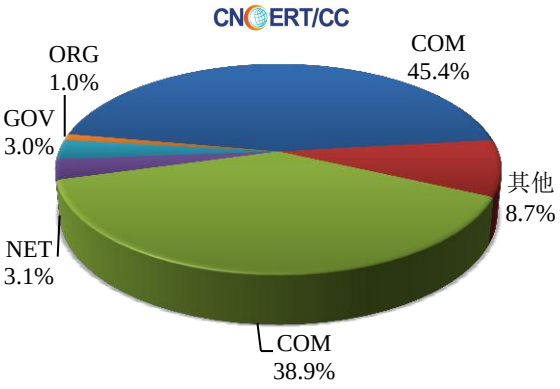
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 618 个；境内被植入后门的网站数量为 424 个；针对境内网站的仿冒页面数量 320 个。

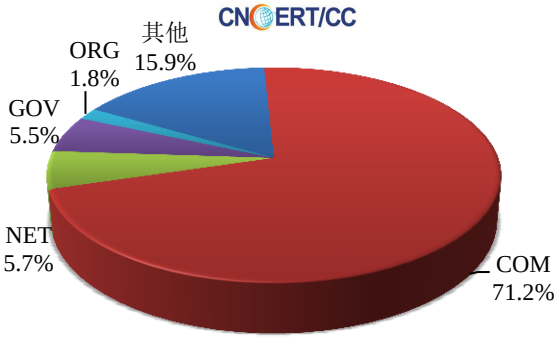


本周境内被篡改政府网站（GOV 类）数量为 34 个（约占境内 5.5%），较上周环比下降了 19.0%；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 1.2%），较上周环比上升了 66.7%；针对境内网站的仿冒页面涉及域名 174 个，IP 地址 120 个，平均每个 IP 地址承载了约 24 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/28-2/3)

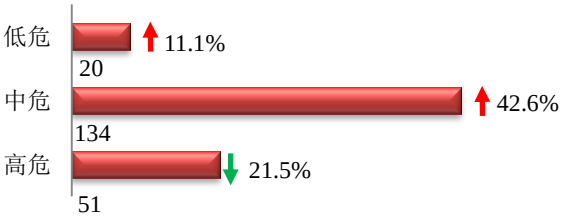


本周我国境内被植入后门网站按类型分布
(1/28-2/3)

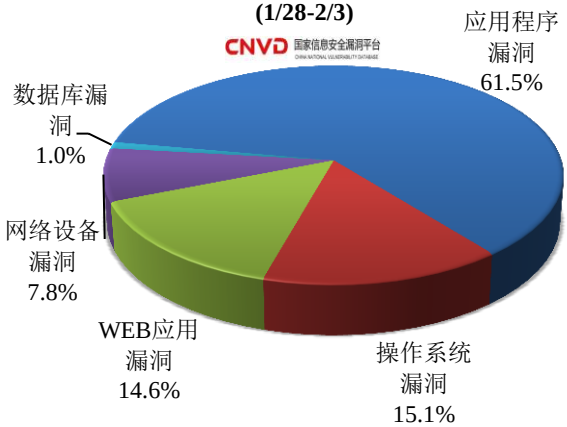


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 205 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
(1/28-2/3)



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

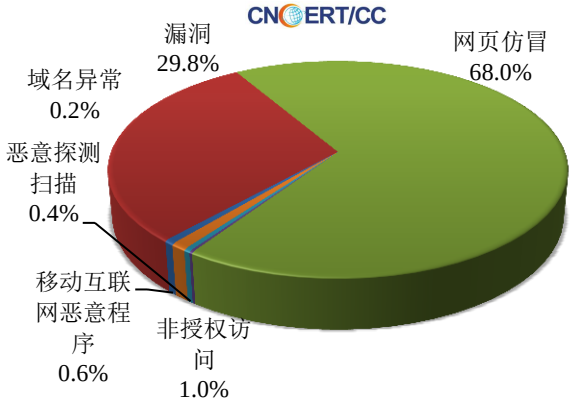
http://www.cnvd.org.cn/webinfo/list?type=4

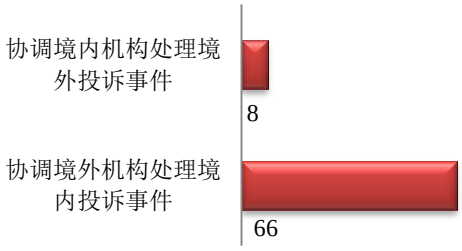
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 485 起，其中跨境网络安全事件 74 起。

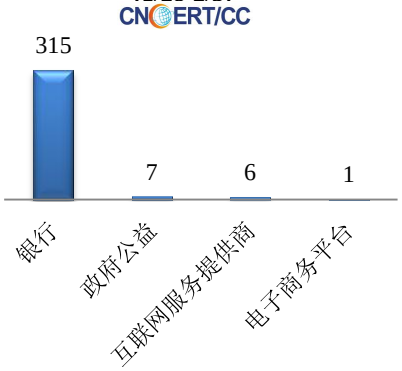
本周CNCERT处理的事件数量按类型分布 (1/28-2/3)



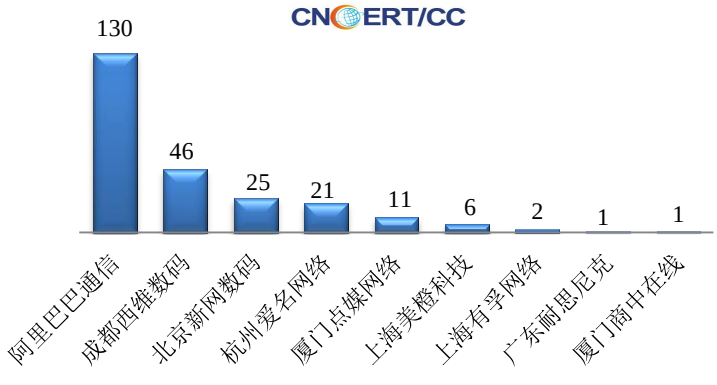


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 329 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 315 起和政府公益事件 7 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (1/28-2/3)

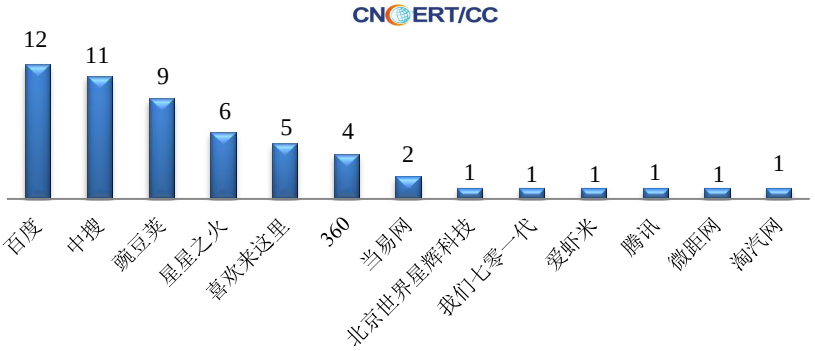


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/28-2/3)



本周，CNCERT 协调 13 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 55 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
(1/28-2/3)



业界新闻速递

1、国家互联网信息办公室发布《区块链信息服务管理规定》

中国网信网 1 月 28 日消息 国家互联网信息办公室 2019 年 1 月 10 日发布《区块链信息服务管理规定》（以下简称“《规定》”），自 2019 年 2 月 15 日起施行。国家互联网信息办公室有关负责人表示，出台《规定》旨在明确区块链信息服务提供者的信息安全管理责任，规范和促进区块链技术及相关服务健康发展，规避区块链信息服务安全风险，为区块链信息服务的提供、使用、管理等提供有效的法律依据。《规定》明确，本规定所称区块链信息服务，是指基于区块链技术或者系统，通过互联网站、应用程序等形式，向社会公众提供信息服务。本规定所称区块链信息服务提供者，是指向社会公众提供区块链信息服务的主体或者节点，以及为区块链信息服务的主体提供技术支持的机构或者组织。国家互联网信息办公室依据职责负责全国区块链信息服务的监督管理执法工作。省、自治区、直辖市互联网信息办公室依据职责负责本行政区域内区块链信息服务的监督管理执法工作。

2、上海网信办:将加强对 App 违法违规申请权限等行为监管

cnBeta.COM 2 月 3 日消息 2018 年 10 月，上海市网信办对本地最常用的 23 个 App 获取用户个人信息等权限申请情况开展安全抽查，并就抽查中发现的申请权限不合理、过度索取用户个人信息等问题依法对 23 家 App 运营企业进行约谈，要求切实做好整改工作，严格落实主体责任。近期，市网信办根据被约谈 App 计划完成整改的时间节点，对各 App 整改情况开展了“回头看”复测工作。根据安全抽查结果，结合运营企业发展实际，最终确定整改前的“不合理权限”数量为 164 项，“合理但存在风险权限”数量为 113 项。市网信办对各 App 运营企业的整改工作进行督促落实，要求各企业按照整改报告切实做好整改工作。截止 1 月中旬，各 App 共整改 158 个“不合理权限”和 98 个“合理但存在风险权限”。整改后剩余 6 个“不合理权限”因企业战

略调整等原因还未整改，但都已列出详细整改计划，剩余 15 个“合理但存在风险权限”因安卓系统的限制，无法完成“修改为一次性授权”的整改，但会对此类权限加强网络安全管控，严防个人信息泄露风险。

3、日本政府计划“入侵”公民的物联网设备

HackerNews.COM1 月 28 日消息 日本政府上周五批准了一项法律修正案，允许政府工作人员“入侵”人们的物联网设备，作为前所未有的不安全物联网设备调查的一部分。该调查将由日本国家信息通信技术研究所（NICT）的员工在总务省的监督下进行。这项计划是编制一个使用默认和易于猜测的密码的不安全设备列表，并将其交给当局和相关的互联网服务提供商，以便他们采取措施提醒消费者并保护设备。该调查计划于下个月启动，届时有关部门计划将测试超过 2 亿件物联网设备的密码安全性，从路由器和网络摄像头开始。人们家中和企业网络中的设备将进行相同的测试。

4、新加坡 1.4 万艾滋病患者个人健康信息遭泄露

黑客视界 1 月 31 日消息 新加坡卫生部（Ministry of Health，MOH）于本周一发布消息称，数千名被确诊为 HIV 阳性患者的新加坡人和外国人的医疗记录和联系方式现已经被公开发布在了网上，而他们正在与相关部门进行合作，以尽快删除这些信息。新加坡卫生部在其官方网站发布的一篇新闻稿中表示，此次个人健康信息遭到泄露的艾滋病病毒携带者大约有 14200 名。并表示，这些信息全都掌握在美国公民米基 •K •法雷拉 •布罗切兹（音译，Mikhy K Farrera Brochez）的手中。新加坡卫生部表示，遭泄露的个人健康信息部分属于 5400 名在 2013 年 1 月之前被确诊感染了艾滋病毒的新加坡人，部分属于 8800 名在 2011 年 12 月之前被确诊感染了艾滋病毒的的外国人。

5、纽约联邦储备银行协助孟加拉国诉讼黑客网络抢劫案

cnBeta.COM2 月 2 日消息 纽约联邦储备银行表示，它将就孟加拉国银行起诉一家菲律宾银行以挽回损失的做法提供“技术援助”。三年前，身份不明的黑客从该银行在美国中央银行的账户中偷走了 8100 万美元。纽约联邦储备银行和孟加拉国央行在一份联合声明中表示，这项援助包括“与菲律宾有关机构或政党联合召开会议，大力鼓励他们协助追回被盗资金”。在曼哈顿的美国地方法院，孟加拉国银行起诉菲律宾银行黎萨尔商业银行（RCBC），指控其和其他数十人，包括几位高管，参与“大规模”和“错综复杂的计划”的多年阴谋窃取他们的资金。

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。截至 2017 年，CNCERT 与 72 个国家和地区的 211 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：朱天

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158