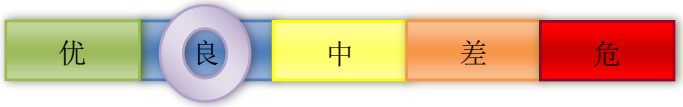
国家互联网应急中心

2018 年第 5 期

1 月 29 日-2 月 4 日

网络安全信息与动态周报

本周网络安全基本态势

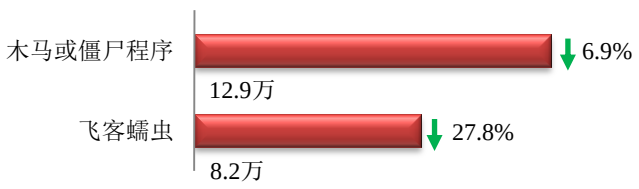


境内感染网络病毒的主机数量	• 21.1万	↓ 16.3%
境内被篡改网站总数 其中政府网站数量	• 1992 • 30	↑ 129.8%
境内被植入后门网站总数 其中政府网站数量	• 758 • 14	↓ 6.7% ↓ 17.6%
针对境内网站的仿冒页面数量	• 318	↓ 17.2%
新增信息安全漏洞数量 其中高危漏洞数量	• 382 • 101	↑ 58.5% ↓ 7.3%

= 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

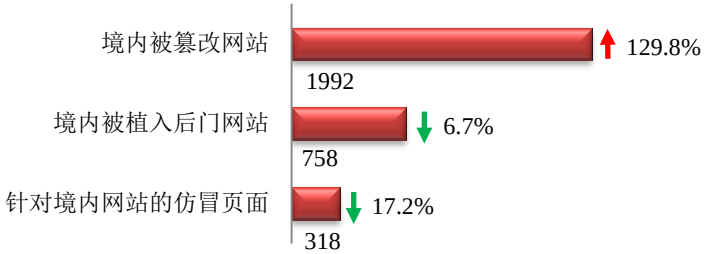
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.9 万以及境内感染飞客（conficker）蠕虫的主机约 8.2 万。



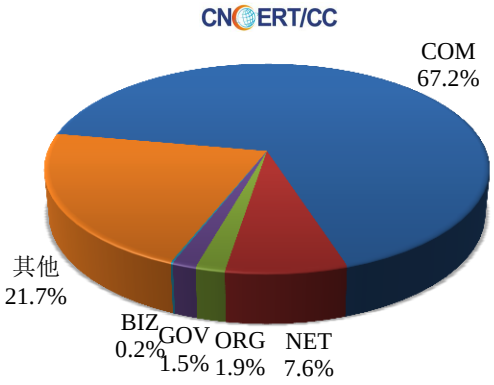
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1992 个；境内被植入后门的网站数量为 758 个；针对境内网站的仿冒页面数量为 318。

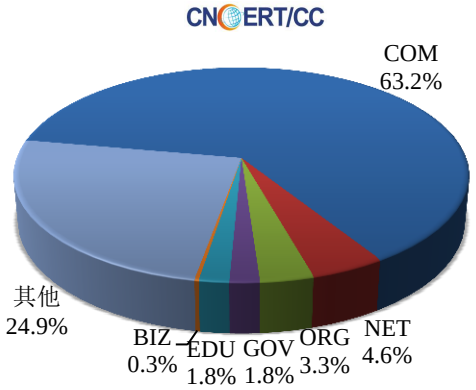


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 1.5%）；境内被植入后门的政府网站（GOV 类）数量为 14 个（约占境内 1.8%），较上周环比下降了 17.6%；针对境内网站的仿冒页面涉及域名 241 个，IP 地址 99 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/29-2/4)

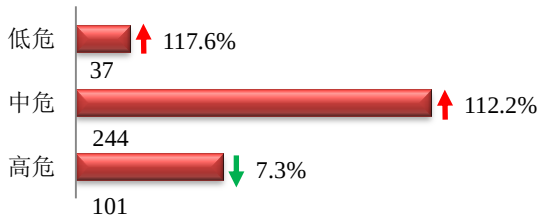


本周我国境内被植入后门网站按类型分布
(1/29-2/4)

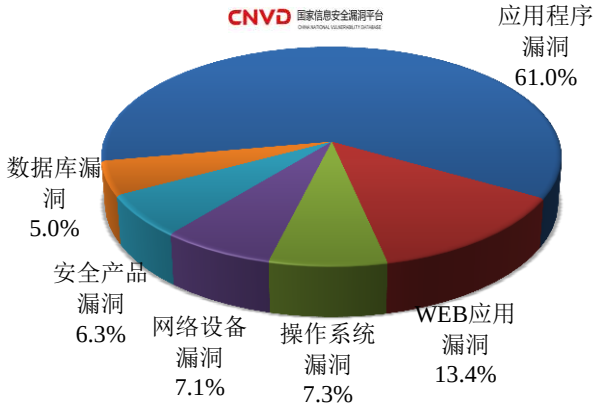


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 382 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
(1/29-2/4)



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

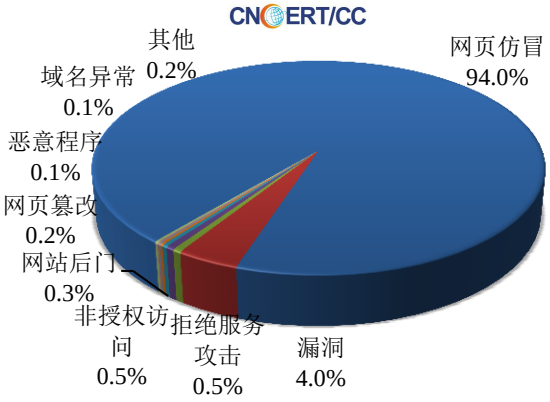
http://www.cnvd.org.cn/webinfo/list?type=4

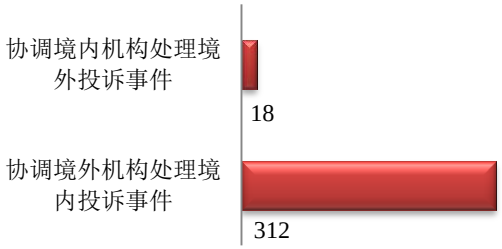
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 910 起，其中跨境网络安全事件 330 起。

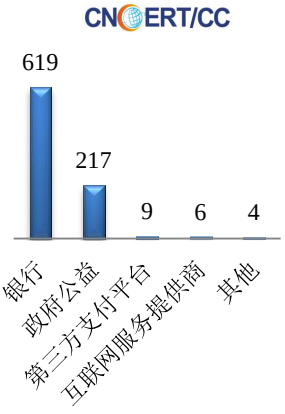
本周CNCERT处理的事件数量按类型分布
(1/29-2/4)



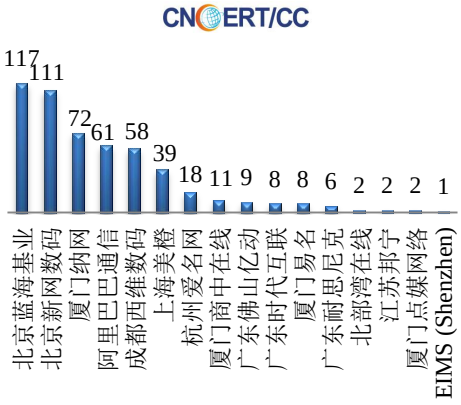


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 855 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 619 起和政府公益仿冒事件 217 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(1/29-2/4)

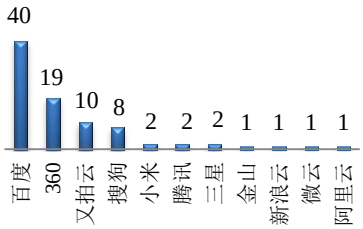


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/29-2/4)



本周，CNCERT 协调 11 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 87 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 (1/29-2/4)



业界新闻速递

1、印度政府计划成立顶尖网络犯罪协调中心

HackerNews.cc1 月 31 日消息 外媒 1 月 28 日报道，为了处理金融诈骗、传播色情内容等各种网络犯罪行为，印度政府计划成立一个顶尖的网络犯罪协调中心，并且印度政府还发放 83 亿卢比，用于在各州设立网络法证培训实验室和警察培训中心。目前该网络犯罪协调中心将在德里建立，用于与州政府和工会领地进行协调，并密切关注网络空间和社交媒体。除此之外，那些蔑视印度法律并传播儿童色情内容以及种族敏感内容的网站也会通过该中心及时阻止。根据印度官员的说法，目前网络犯罪案件种类繁多，比如政府网站的入侵、在线金

融欺诈、网络病毒、恶意代码、DDoS 攻击、追踪骚扰以及数据盗窃等，所以在调查技术、法律、行政等方面加强体制建设是非常重要的。据悉，印度不仅计划建设网络犯罪协调中心和警察培训中心，还试图成立网络和移动法庭实验室，用于确定网络空间特定领域的研究和开发需求。

2、英国将对网络安全失当的企业处以最高 1700 万英镑的罚款

cnBeta.COM1 月 30 日消息 去年爆发的“WannaCry”勒索病毒给全球带来了深重的灾难，而英国政府显然不愿往事重演。据 Engadget 报道，为了敦促各企业妥善落实网络安全防护措施，有关部门将对处置不当的企业苛以最高 1700 万英镑（约 1.51 亿 RMB）的罚款。这项惩罚制度，其实是对欧盟 2016 年 8 月通过的 NIS 指令的回应，旨在确保各成员国对新型网络攻击做好准备。据悉，英国政府将把 NIS 指令引入该国的法律体系，以保护健康、能源、交通和数字基础设施。鉴于企业与相关监管机构合作采取补救措施、以及其它可能被违反的法律条款的程度，罚款将保留为“最后的手段”。其实早在去年 8-9 月份，英国政府就已经咨询过这套方案。针对不同的行业，其适用的“基础运营服务”也不尽相同。至于更多细节，英国政府会在正式条文中列明。

3、北约合作网络防御卓越中心（CCDCOE）将负责协调北约所有机构网络防御行动训练

HackerNews.cc2 月 1 日消息 据外媒报道，北约合作网络防御卓越中心（CCDCOE）被选定来协调联盟内所有网络防御行动领域的教育和培训解决方案。CCDCOE 是一家总部位于爱沙尼亚，由 20 个不同国家组成的知识中心。从技术上讲，这是一个军事组织，它的任务是为盟友提供 360 度的网络防御，并且输送技术、战略、行动和法律方面的专业知识。除上述功能之外，CCDCOE 还扮演了一个新的角色——作为网络防御作战教育和训练纪律的负责人，这一新角色由北约两个战略指挥部门之一的最高盟军指挥部（SACT）授予，主要职责是与位于美国弗吉尼亚州诺福克的盟军司令部密切合作。另外，CCDCOE 也是“塔林手册 2.0”的发源地（该手册是关于国际法如何适用于网络运营的综合指南）、组织了世界上最大最复杂的国际技术性现场网络防御演习。

4、荷兰三大银行频繁遭受 DDoS 攻击，致其互联网银行服务瘫痪

HackerNews.cc1 月 31 日消息 据外媒报道，荷兰三大银行（荷兰银行、荷兰合作银行以及 ING 银行）于 1 月 29 日表示其网络系统在过去一周内不断遭受分布式拒绝服务（DDoS）攻击，导致网站和互联网银行服务瘫痪。荷兰银行在上周共遭受 7 次袭击（周末就发生了 3 次），其中包含安全人员在周日晚上观察到的分布式拒绝服务（DDoS）攻击。荷兰合作银行发言人 Margo van Wijgerden 周一称因网络系统受到 DDoS 攻击，导致网络服务业务下滑。ING 银行表示，在 DDoS 攻击期间，因为数据流量导致服务器超载，网上银行的可用性承受了巨大压力。此外，荷兰税务局也遭受了类似攻击，不过其网络服务很快就恢复了运作。根据相关媒体报道，目前三家银行的一些网络服务已恢复正常运营，并且其官方承诺客户的银行业务细节不会受到损害。

5、日本第二大虚拟货币在线交易所 Coincheck 遭黑客攻击 损失惨重

央视网 1 月 29 日消息 近日，日本第二大虚拟货币在线交易所 Coincheck 遭黑客攻击，价值约 580 亿日元，约合 34 亿元人民币的虚拟货币新经币去向不明。该交易所 12 月 28 日宣布，将对持有新经币的约 26 万人以日元形式补偿其虚拟货币的损失。据报道，这家交易所 26 日发布消息称，当天该机构价值约 580 亿日元的新经币因非法访问流向了外部，去向不明。事发后，交易所立即叫停了所有虚拟货币和日元取款等服务。目前，该交

易所服务仍未恢复，用户已无法提取自己的资产。28 日，这家交易所表示，将通过自有资金返还顾客损失的大部分数额，补偿金额约为 88.5 日元乘以新经币的持有数，赔偿总金额将达到 460 亿日元，约合 27 亿元人民币。据悉，遭黑客攻击的交易所成立于 2012 年，总部位于东京，其保管新经币的帐户通常与互联网连接，与不联网的离线管理相比安全性较低。

6、澳大利亚最大汽车共享服务公司遭入侵，数万名会员个人信息泄露

E 安全 2 月 1 日消息 本周三，澳大利亚规模最大的汽车共享服务公司 GoGet 向其客户发出警告，称他们的车辆预定系统在去年遭到了黑客的入侵，在去年 7 月 27 日之前注册的会员个人信息已经遭到泄露。泄露信息的多少取决于 GoGet 用户在填写会员登录表时录入的具体个人资料内容，这可能包括：姓名、家庭住址、电子邮箱地址、电话号码、出生日期、驾驶执照详细信息、就业单位、紧急联系人的姓名和电话号码以及 GoGet 管理帐户详细信息。GoGet 表示，他们的 IT 团队在去年 6 月 27 日发现了这起入侵活动，并立即展开了全面的内部调查。同时，也向新南威尔士州警察局网络犯罪小组进行了报告。根据当时警方的建议，GoGet 并没有选择立即将这件事情公开。GoGet 和新南威尔士州警方都强调，目前没有直接的证据表明嫌疑人已经将窃取的信息进行销售或通过其他途径传播。

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 2016 年，CNCERT 与 69 个国家和地区的 185 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：何世平

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158