国家互联网应急中心

2018 年第 51 期

12 月 17 日-12 月 23 日

网络安全信息与动态周报

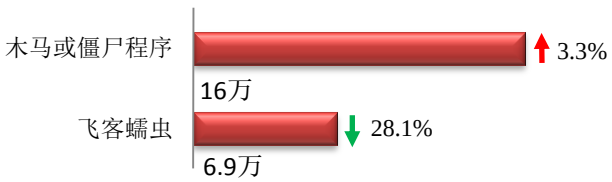
本周网络安全基本态势

境内感染网络病毒的主机数量	•22.9万	↓ 8.7%
境内被篡改网站总数 其中政府网站数量	•803 •45	↓ 0.4% ↓ 11.8%
境内被植入后门网站总数 其中政府网站数量	•652 •4	↑ 9.0% =
针对境内网站的仿冒页面数量	•1237	↓ 18.5%
新增信息安全漏洞数量 其中高危漏洞数量	•352 •137	↑ 77.8% ↑ 93.0%

=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

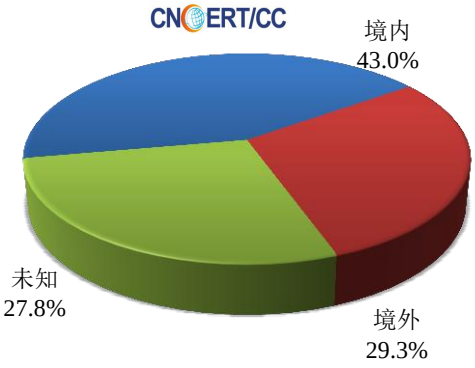
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 22.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.0 万以及境内感染飞客（conficker）蠕虫的主机约 6.9 万。

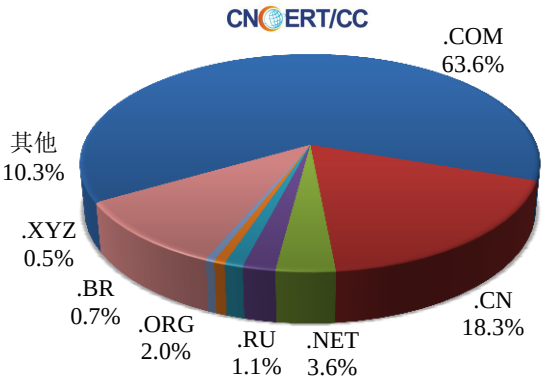


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 4484 个，涉及 IP 地址 5811 个。在 4484 个域名中，有 29.3%为境外注册，且顶级域为.com 的约占 63.6%；在 5811 个 IP 中，有约 60.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 761 个 IP。

本周放马站点域名注册所属境内外分布
(12/17-12/23)



本周放马站点域名所属顶级域的分布
(12/17-12/23)



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。

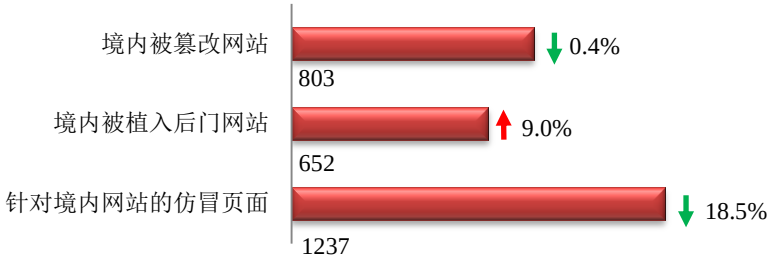
ANVA恶意地址黑名单发布地址

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。

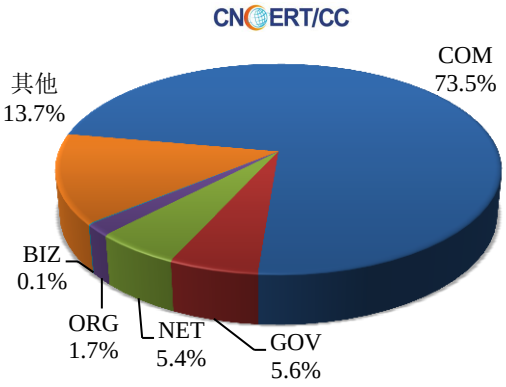
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 803 个；境内被植入后门的网站数量为 652 个；针对境内网站的仿冒页面数量 1237 个。

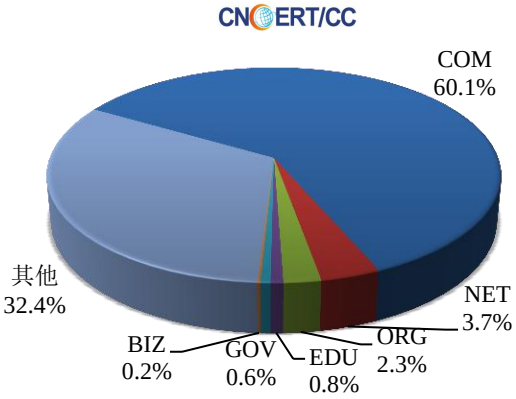


本周境内被篡改政府网站（GOV 类）数量为 45 个（约占境内 5.6%），较上周环比下降了 11.8%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.6%），较上周环比无变化；针对境内网站的仿冒页面涉及域名 426 个，IP 地址 240 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/17-12/23)

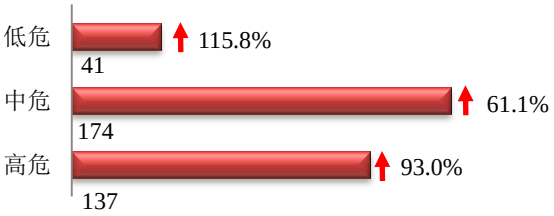


本周我国境内被植入后门网站按类型分布
(12/170-12/23)

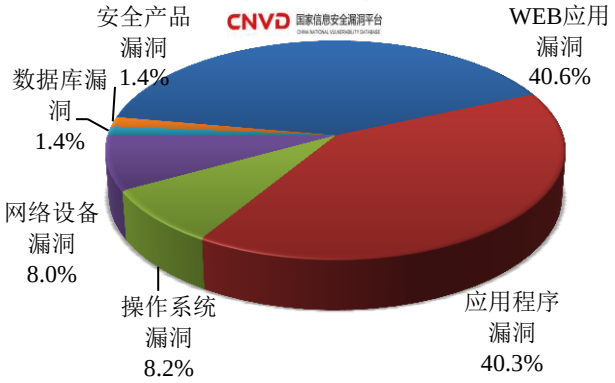


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 352 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
(12/17-12/23)



本周 CNVD 发布的网络安全漏洞中，WEB 应用程序漏洞占比最高，其次是应用程序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

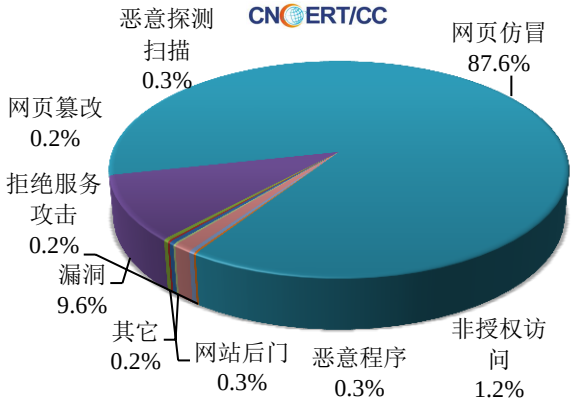
http://www.cnvd.org.cn/webinfo/list?type=4

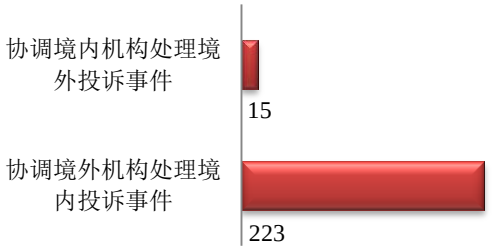
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 591 起，其中跨境网络安全事件 238 起。

本周CNCERT处理的事件数量按类型分布 (12/17-12/23)

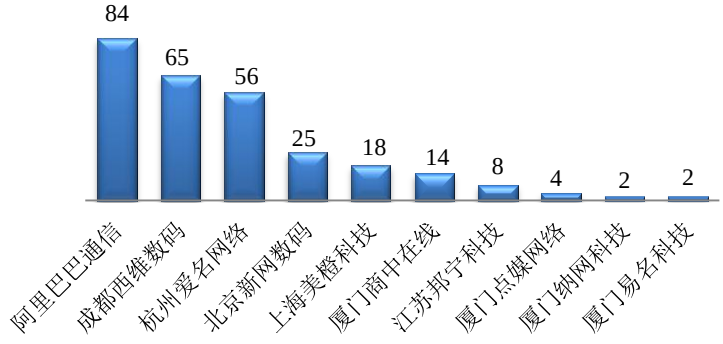




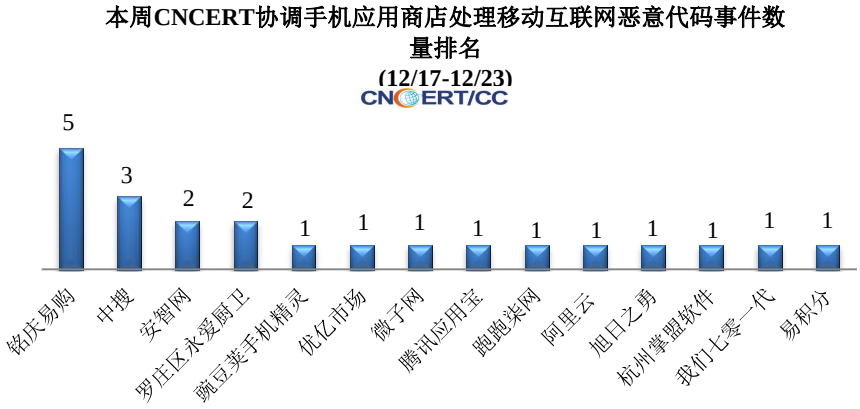
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 518 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒 500 起和互联网服务提供商事件 16 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (12/17-12/23)

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 (12/17-12/23)



本周，CNCERT 协调 14 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 22 个。



业界新闻速递

1、经印度政府授权，10 个安全机构可监控、拦截与解密公民数据

E 安全 12 月 23 日消息 10 个安全与情报机构经印度政府授权，可合法监控、拦截与解密储存在任何计算机上的数据、互联网流量及其他数据流。发布该指令是为确保机构在拦截、监控或解密任何信息时都合乎法律要求。任何违法的个人与团体都将面临 7 年的监禁或罚款。发布该指令，是为了确保任何通过计算机资源拦截、监控或解密信息的行为都是按照正常法律程序进行的。这也将防止任何机构、个人或中介机构在未授权的情况下滥用这些权力。任何个案都需得到内政部与州政府的提前批准。印度内政部并未将其权力下放至任何执法部门与安全机构。

2、NASA 服务器被黑客攻击 员工信息曝光

cnBeta.COM12 月 20 日消息 美国国家航空航天局（NASA）已确认旗下一台服务器在 10 月被黑客攻击，黑客从其中盗取了一些员工信息，包括社会安全号码等等。在 12 月 18 日发布的通知中，美国国家航空航天局表示，它目前正在通知那些可能因此受到损害的员工。调查已经开始，NASA 表示社会安全号码和其他个人身份信息存储在被黑的服务器上。美国宇航局及其联邦网络安全合作伙伴正在继续检查服务器，以确定潜在数据泄漏的范围，并识别可能受影响的个人。

3、非法放飞的无人机让英国第二大机场被迫关闭

2018 年 12 月 20 日消息 据英国《卫报》报道，英国第二大机场盖特威克机场在周三晚上和周四早上收到两架无人机在附近飞行的报告后关闭。在发现无人机之后，机场最初的航班在周三晚上 9 点暂停，虽然它在凌晨 3 点暂时重新开放，但在无人机航班恢复后 45 分钟后又被迫再次关闭。截至周四早上 11 点 45 分，往返机场

的航班仍然暂停。除了防止任何航班起飞外，暂停意味着必须将许多入境航班转移到伦敦地区的其他机场，包括卢顿，希思罗机场和斯坦斯特德机场，而其他航班则被迫降落在巴黎和阿姆斯特丹。总共有 760 个航班和 11 万名乘客受到影响，这些航班将于周四从盖特威克机场起飞或降落。

4、法国数据保护监管机构 CNIL 因 Uber 数据保护不力 向其开出 46 万美元罚单

cnBeta.COM12 月 21 日消息 欧洲各国已经开始进入“围殴”模式，一个接一个地向 Uber 开出罚单，以惩戒其处理 2016 年数据泄露的方式。今天，法国的数据保护监管机构 CNIL 宣布将对 Uber 开出 460000 美元（400000 欧元）的罚款。因早在 2016 年，Uber 的大规模数据泄露影响了 5700 万用户，其中包括法国的 140 万用户。根据 CNIL 的报告，黑客正使用来自这些泄露数据的登录名和密码连接到 Uber 的 GitHub 存储库，然后再设法连接到 Uber 的亚马逊网络服务帐户并下载用户数据，更夸张的是 AWS 登录信息以纯文本格式存储在 GitHub 上。对 Uber 来说，唯一好消息是欧盟 GDPR 来得晚了一点，目前，如果一家公司在 72 小时内没有向相关机构报告违规行为，他们最终可能会被罚款高达公司全球年营业额的 4%。

5、亚马逊发生重大监听事故

新浪科技 12 月 21 日消息，德国媒体《c't》报道称，由于亚马逊的人为错误，导致德国一位 Alexa 智能音箱用户接收到了 1700 份的陌生人录音。今年 8 月，这位用户根据《通用数据保护条例》要求亚马逊提供自己的个人活动语音数据时，没想到对方竟然发来了 1700 份陌生人录音。《c't》听取了其中部分录音发现，仅凭这些信息可以“拼凑”出一个人的生活细节和个人习惯。有些录音还有沐浴的声音。《c't》根据这些信息找到了不幸被泄露隐私的两位用户，其中一位表示震惊和愤怒。这不是亚马逊音箱第一次出现窃听问题。据澎湃报道，今年 5 月，美国俄勒冈州的一个家庭向媒体爆料称，其家中的亚马逊智能音箱 Echo 在未经许可的情况下将私人对话录音，并在主人不知情的情况下将音频发送给了联系人列表中的人。对此，亚马逊称是人工智能助手 Alexa 将用户对话内容误解成了指令。

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：何世平

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158