国家互联网应急中心

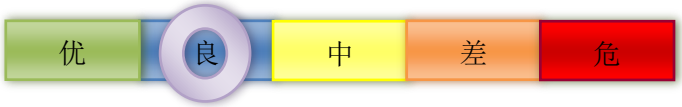
2018 年第 48 期

11 月 26 日-12 月 2 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

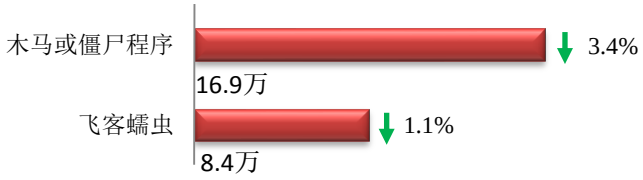


境内感染网络病毒的主机数量	•25.3万	2.7%
境内被篡改网站总数 其中政府网站数量	•836 •42	3.4% 7.7%
境内被植入后门网站总数 其中政府网站数量	•769 •18	34.2% 100.0%
针对境内网站的仿冒页面数量	•1297	34.4%
新增信息安全漏洞数量 其中高危漏洞数量	•213 •45	39.2% 26.2%

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

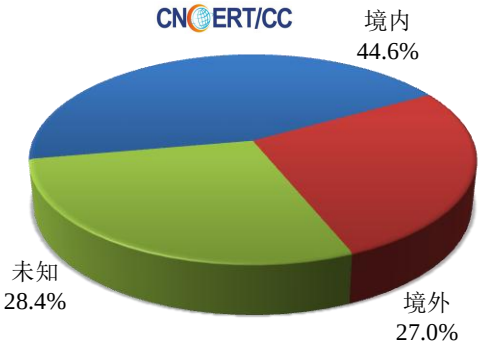
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.9 万以及境内感染飞客（conficker）蠕虫的主机约 8.4 万。

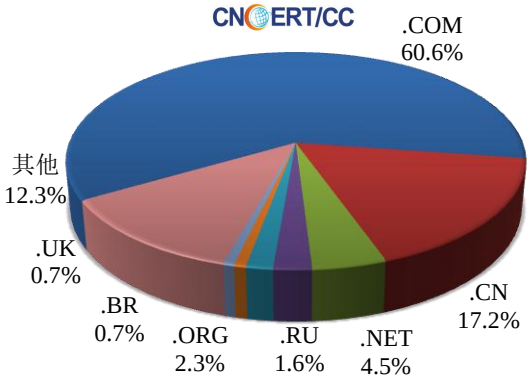


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 4443 个，涉及 IP 地址 6685 个。在 4443 个域名中，有 27.0%为境外注册，且顶级域为.com 的约占 60.6%；在 6685 个 IP 中，有约 70.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 627 个 IP。

本周放马站点域名注册所属境内外分布
(11/26-12/2)



本周放马站点域名所属顶级域的分布
(11/26-12/2)



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。

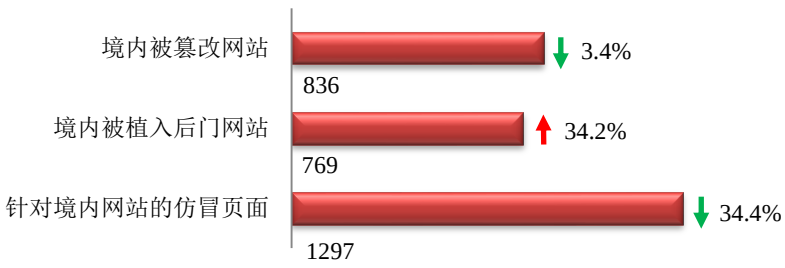
ANVA恶意地址黑名单发布地址

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。

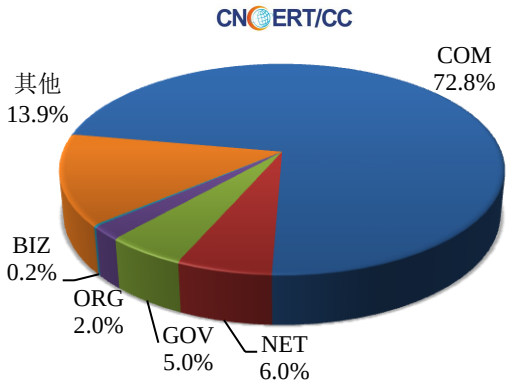
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 836 个；境内被植入后门的网站数量为 769 个；针对境内网站的仿冒页面数量为 1297 个。

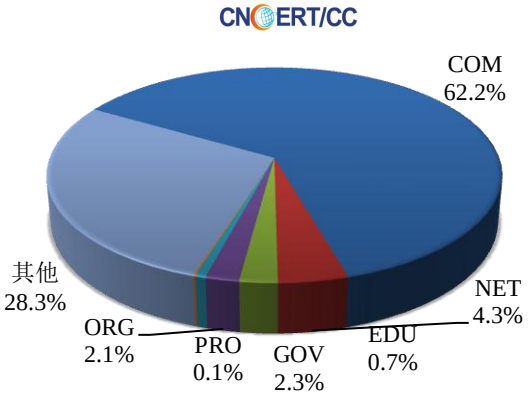


本周境内被篡改政府网站（GOV 类）数量为 42 个（约占境内 5.0%），较上周环比上升了 7.7%；境内被植入后门的政府网站（GOV 类）数量为 18 个（约占境内 2.3%），较上周环比上升了 100.0%；针对境内网站的仿冒页面涉及域名 414 个，IP 地址 234 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/26-12/2)

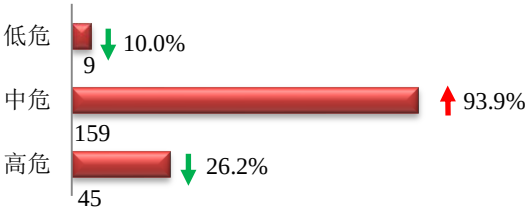


本周我国境内被植入后门网站按类型分布
(11/26-12/2)

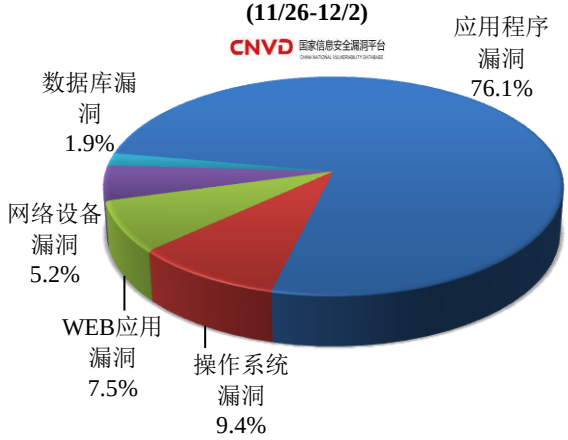


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 213 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
(11/26-12/2)



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

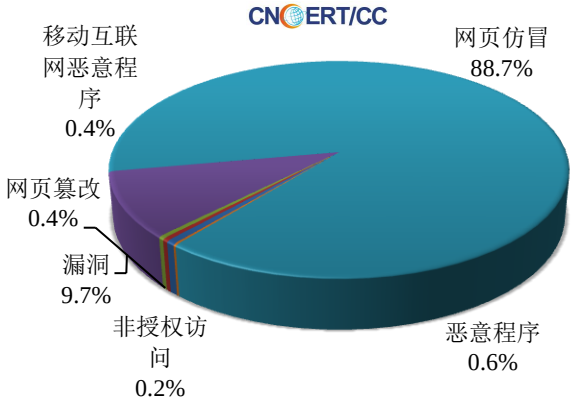
http://www.cnvd.org.cn/webinfo/list?type=4

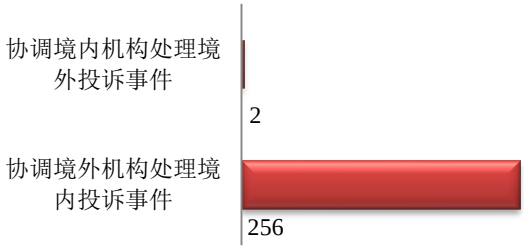
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 524 起，其中跨境网络安全事件 258 起。

本周CNCERT处理的事件数量按类型分布 (11/26-12/2)

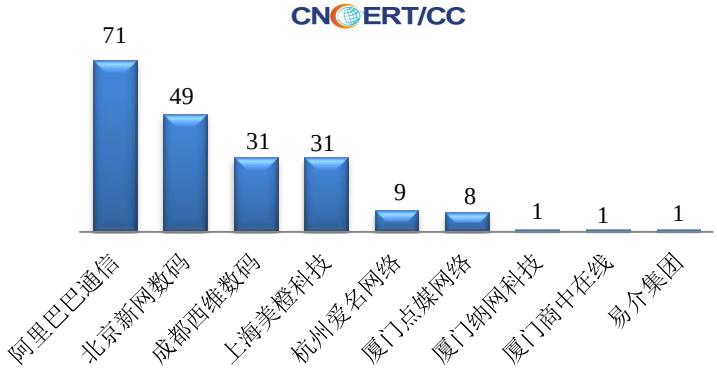




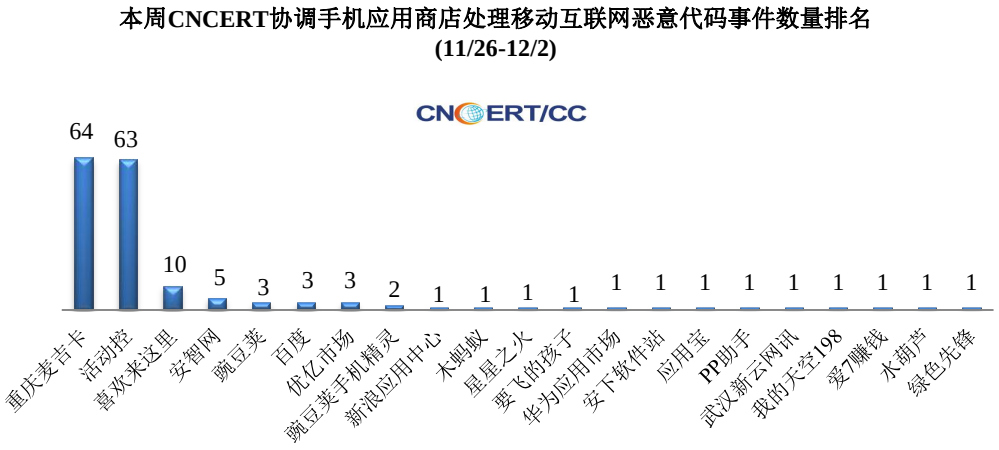
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 465 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 446 起和政府公益仿冒事件 15 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (11/26-12/2)

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 (11/26-12/2)



本周，CNCERT 协调 21 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 166 个。



业界新闻速递

1、2018 年度车联网安全年会暨第一届车联网安全攻防挑战赛在上海顺利举行

E 安全 11 月 28 日消息 由国家计算机网络应急技术处理协调中心主办，以“共生、共享、共赢”为主题的 2018 年度车联网安全年会暨第一届车联网安全攻防挑战赛在上海拉开帷幕。围绕“共建车联网信息安全新生态”，国家计算机网络应急技术处理协调中心云晓春副主任，中国标准化研究院巫小波副院长、国家市场监督管理总局缺陷产品管理中心王琰副主任、国家中心实验室副主任李政、上海国际汽车城荣文伟董事长等嘉宾分别发表了主题演讲，针对车联网日益严峻的网络信息安全风险等行业相关问题进行了深入的探讨。通过此次实战演练，不仅提升了安全人员的专业技术能力，还让各个队伍通过此次“交手”收获良多，彼此之间有了进一步的了解，共同为我国车联网安全事业的发展而努力。

2、万豪旗下喜达屋酒店数据库遭入侵 5 亿顾客信息或泄露

新浪科技讯 11 月 30 日消息 万豪国际酒店集团(Marriott International)今日宣布，旗下喜达屋酒店(Starwood Hotel)的一个顾客预订数据库被黑客入侵，可能有约 5 亿顾客的信息泄露。该消息公布后，万豪国际酒店股价在今日盘前交易中一度下跌逾 5%。目前，万豪国际酒店已采取了补救措施，但并未公布进一步的信息。万豪国际酒店称，这些可能被泄露的信息包括顾客的姓名、通信地址、电话号码、电子邮箱、护照号码、喜达屋 VIP 客户信息、出生日期、性别和其他一些个人信息。对于部分客户，可能被泄露的信息还包括支付卡号码和有效日期，但这些

数据是加密的。

3、300 万用户数据泄露 Uber 被英国和荷兰罚款 117 万美元

黑客视界 2018 年 11 月 28 日消息 据美媒 CNBC 报道，因 2016 年的数据泄露事件，周二英国和荷兰当局分别对 Uber 处以罚款，罚款总金额达 117 万美元。2016 年 10 月和 11 月，Uber 遭到网络攻击致使用户数据泄露，泄露的信息包括用户完整姓名、电子邮箱地址和电话号码。对此，英国信息专员办公室（ICO）宣布对 Uber 处以 38.5 万英镑（约 49.1 万美元），理由是公司“未能在网络攻击期间保护消费者个人信息”。荷兰数据保护局也针对该次数据泄露事故对公司处以 60 万欧元（约 67.9 万美元）罚款。隐瞒事故近一年后，Uber 于 2017 年 11 月份承认，黑客窃取了全球 5700 万用户和司机的个人信息。并且，为了删除数据和隐瞒数据泄露事故，Uber 还向黑客支付了 10 万美元。由于网络攻击发生于 2016 年，该次数据泄露事件不受今年 5 月份生效的欧盟“通用数据保护条例”的管辖。今年 9 月份，Uber 同意向美国各州和华盛顿特区支付 1.48 亿美元以解决与 2016 年数据泄露有关的诉讼。

4、巴西最大的专业协会发生大规模数据泄露

E 安全 11 月 28 日消息 巴西圣保罗州工业联合会（简称 FIESP）遭指控，称其在线泄露其三个数据库中数百万个人数据记录。FIESP 代表了约 13 万家公司，是巴西工业部门的最大企业实体。这些外泄记录包括：姓名、ID 与社会安全号码、完整住址信息以及电子邮件与电话号码。白帽黑客生态系统 Hacken Proof 的安全研究员鲍勃·迪亚琴科（Bob Diachenko）称其在 11 月 12 日发现了三个包含个人记录的数据库，可通过 Elasticsearch 搜索引擎访问这些记录。最大的数据源包含 3480 万个条目。关于该数据泄露事件，该研究员称其已试图警告 FIESP，但无济于事。Hacken Proof 在推特上首次公开该泄露事件后，一位巴西粉丝将该数据泄露事件告知了企业，企业这时才离线了数据库。巴西检察官办公室目前正对该数据泄露事件展开调查。巴西亟需执行自己的数据保护法案，相较于其他法案，该法案将旨在确保公共及私人企业对个人数据泄露事件负责。

5、黑客向热门 JavaScript 库注入恶意代码 窃取 Copay 钱包的比特币

cnBeta.COM11 月 27 日消息 尽管上周已经发现了恶意代码的存在，但直到今天安全专家才理清这个严重混乱的恶意代码，了解它真正的意图是什么。黑客利用该恶意代码获得(合法)访问热门 JavaScript 库，通过注射恶意代码从 BitPay 的 Copay 钱包应用中窃取比特币和比特币现金。这个可以加载恶意程序的 JavaScrip 库叫做 Event-Stream，非常受者欢迎，在 npm.org 存储库上每周下载量超过 200 万。但在三个月前，由于缺乏时间和兴趣原作者将开发和维护工作交给另一位程序员 Right9ctrl。Event-Stream，是一个用于处理 Node.js 流数据的 JavaScript npm 包。根据 Twitter、GitHub 和 Hacker News 上用户反馈，该恶意程序在默认情况下处于休眠状态，不过当 Copay 启动（由比特币支付平台 BitPay 开发的桌面端和移动端钱包应用）之后就会自动激活。它将会窃取包括私钥在内的用户钱包信息，并将其发送至 copayapi.host 的 8080 端口上。目前已

经确认 9 月至 11 月期间，所有版本的 Copay 钱包都被认为已被感染。今天早些时候，BitPay 团队发布了 Copay v5.2.2，已经删除 Event-Stream 和 Flatmap-Stream 依赖项。恶意的 Event-Stream v3.3.6 也已从 npm.org 中删除，但 Event-Stream 库仍然可用。这是因为 Right9ctrl 试图删除他的恶意代码，发布了不包含任何恶意代码的后续版本的 Event-Stream。建议使用这两个库的项目维护人员将其依赖树更新为可用的最新版本－Event-Stream 版本 4.0.1。此链接包含所有 3,900+ JavaScript npm 软件包的列表，其中 Event-Stream 作为直接或间接依赖项加载。

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：李佳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158