国家互联网应急中心

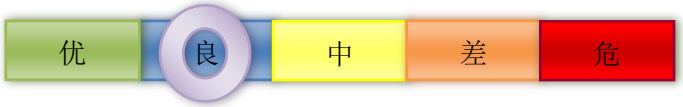
网络安全信息与动态周报

2018 年第 44 期

10 月 29 日-11 月 4 日

CNCERT/CC

本周网络安全基本态势

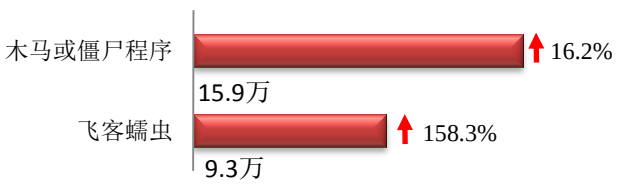


境内感染网络病毒的主机数量	•25.2万	↑ 45.9%
境内被篡改网站总数 其中政府网站数量	•245 •20	↑ 202.5% ↑ 42.9%
境内被植入后门网站总数 其中政府网站数量	•885 •9	↓ 4.9% ↓ 35.7%
针对境内网站的仿冒页面数量	•1290	↑ 20.6%
新增信息安全漏洞数量 其中高危漏洞数量	•203 •90	↑ 1.5% ↑ 13.9%

═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

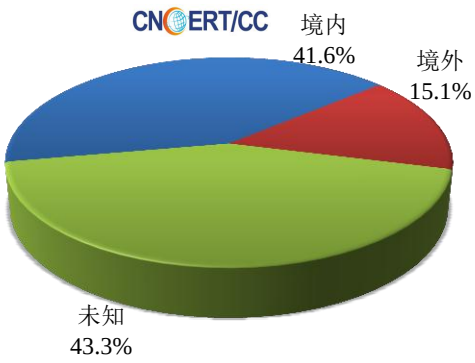
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.9 万以及境内感染飞客（conficker）蠕虫的主机约 9.3 万。

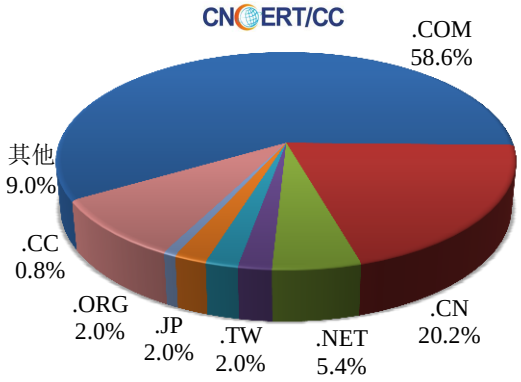


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 4577 个，涉及 IP 地址 5590 个。在 4577 个域名中，有 15.1%为境外注册，且顶级域为.com 的约占 58.6%；在 5590 个 IP 中，有约 49.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 551 个 IP。

本周放马站点域名注册所属境内外分布
(10/29-11/4)



本周放马站点域名所属顶级域的分布
(10/29-11/4)



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。

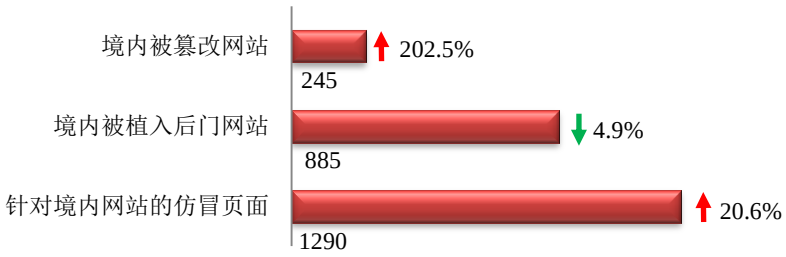
ANVA恶意地址黑名单发布地址

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。

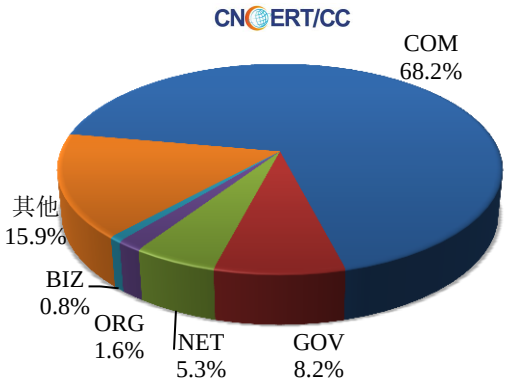
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 245 个；境内被植入后门的网站数量为 885 个；针对境内网站的仿冒页面数量为 1290 个。

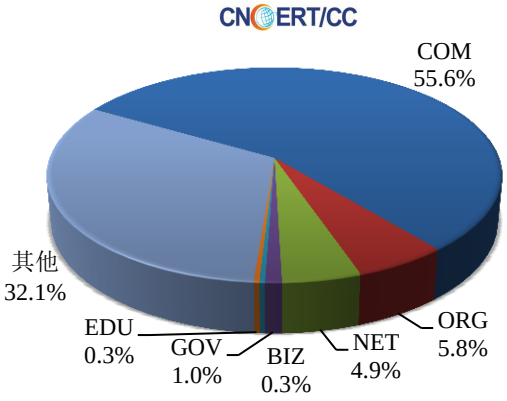


本周境内被篡改政府网站（GOV 类）数量为 20 个（约占境内 8.2%），较上周环比上升了 42.9%；境内被植入后门的政府网站（GOV 类）数量为 9 个（约占境内 1.0%），较上周环比下降了 35.7%；针对境内网站的仿冒页面涉及域名 403 个，IP 地址 228 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/29-11/4)

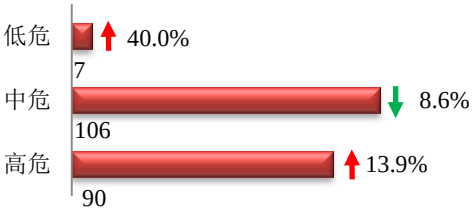


本周我国境内被植入后门网站按类型分布
(10/29-11/4)

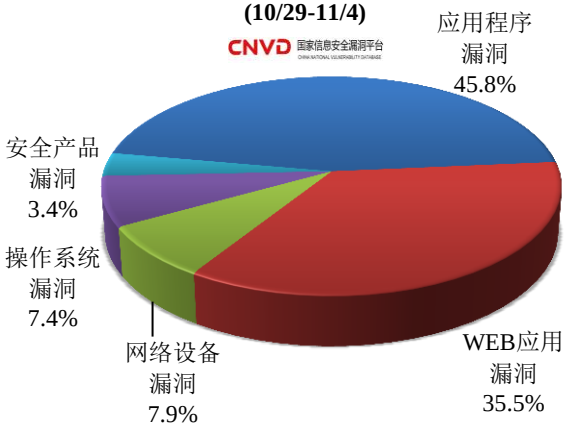


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 203 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
(10/29-11/4)



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 应用漏洞和网络设备漏洞。

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

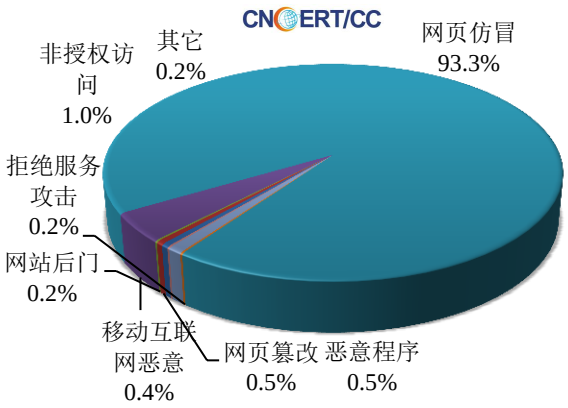
http://www.cnvd.org.cn/webinfo/list?type=4

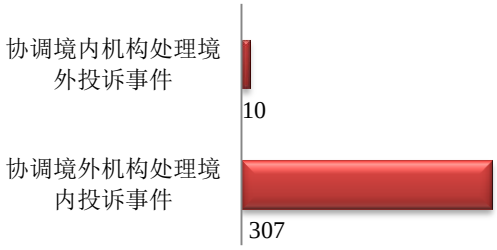
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 630 起，其中跨境网络安全事件 317 起。

本周CNCERT处理的事件数量按类型分布 (10/29-11/4)

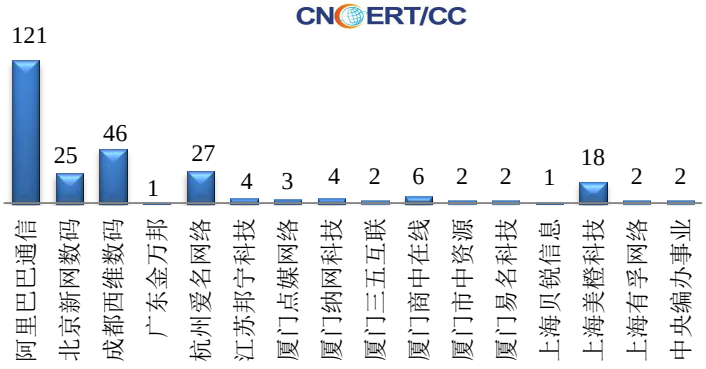




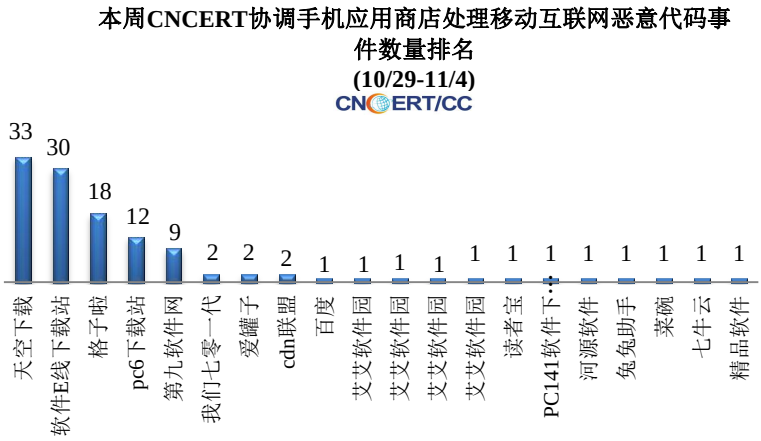
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 588 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 553 起和互联网服务提供商仿冒事件 32 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (10/29-11/4)

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 (10/29-11/4)



本周，CNCERT 协调 20 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 120 个。



业界新闻速递

1、中国区块链生态联盟发布《区块链行业自律倡议书》

新浪财经 10 月 31 日讯 中国区块链生态联盟在京发布《区块链行业自律倡议书》，参与发布会的包括赛迪（青岛）区块链研究院、华为、360、太一云、众享比特、信任度科技等多家联盟成员单位。《区块链行业自律倡议书》是根据工业和信息化部信息化和软件服务业司相关会议精神和工作部署，为构建区块链行业发展良好氛围，推动区块链行业健康有序发展，中国区块链生态联盟与区块链行业内重要机构和组织共同起草形成的。倡议书倡议行业区块链企业认真履行企业主体责任，配合监管，抵制利 用区块链概念进行各种违法违规活动，促进区块链与实体经济深度融合。

2、《公安机关互联网安全监督检查规定》今起施行

新京报 11 月 1 日讯《公安机关互联网安全监督检查规定》自 11 月 1 日起施行。根据规定，公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对互联网服务提供者和联网使用单位开展监督检查。《规定》明确，公安机关开展监督检查，可以采取进入营业场所、机房、工作场所、要求监督检查对象的负责人或者网络安全管理人员对监督检查事项作出说明、查阅、复制与互联网安全监督检查事项相关的信息、查看网络与信息安全保护技术措施运行情况等措施。

3、网络攻击暴露法国核电站敏感数据

E 安全 11 月 4 日讯 据外媒报道，法国公司 Ingerop 受到了黑客攻击。黑客对法国公司 Ingerop

发起网络攻击，窃取与法国核电站计划相关的机密文件。早在六月，该黑客就已窃取逾 65G 文件，这些文件包括核电站计划，和监狱及有轨电车网络的蓝图等内容。这些敏感文件包含一座法国戒备森严的监狱摄像机的位置、计划置于法国东北部的核废料倾倒场等核电站的细节信息。黑客还窃取了千余名 Ingerop 工作人员的个人信息。有报道称，部分文件与法国最早的核电站费森海姆核电站（ Fessenheim ）相关，该核电站位于德国边境，将于 2022 年关闭。

4、丽笙集团顾客数据被一锅端 旗下 1100 家酒店一个没跑

cnBate.COM 11 月 3 日讯 丽笙酒店集团的丽笙奖励项目（Radisson Rewards）被黑客来了个“七进七出”，发送给受影响顾客的数据安全事故通知显示，大量顾客（未公布具体数字）的个人信息已经惨遭黑手。丽笙奖励项目会为该酒店集团分布在全球 1100 多家酒店的顾客提供多项服务和权益，因此此次数据泄露事件受害者数目必然会相当庞大，绝对是一场无妄之灾。当然，坏消息过后也有“好消息”，那就是此次数据泄露事件中黑客并没有盗走任何信用卡或密码信息。

5、苹果与三星因“计划性淘汰”获数百万罚款

E 安全 10 月 29 日讯 因“计划性淘汰”其智能手机，苹果与三星分别被意大利竞争局（AGCM）处以 500 万欧元与 1000 万欧元罚款。经长期调查，意大利竞争局（AGCM）向苹果开具 500 万欧元（即 580 万美元）罚单、向三星开具 1000 万欧元（即 1150 万美元）罚单，因两者“计划性淘汰”其智能手机。据意大利竞争局透露，这两家技术巨头公司为其设备提供无法完全支持的软件更新，且未告知消费者准确、正确的信息，亦不允许任何后续的卸载。这两家公司均涉嫌为刺激用户购买新机而降低其旧款手机运行速度。

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：杨凯

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158