国家互联网应急中心

2018 年第 52 期
12 月 24 日-12 月 30 日

网络安全信息与动态周报

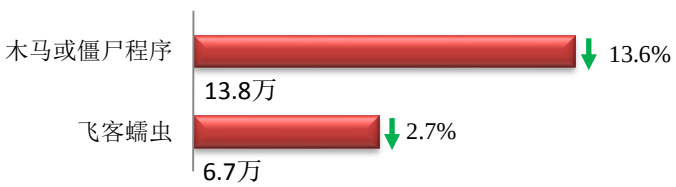
本周网络安全基本态势

境内感染网络病毒的主机数量	•20.5万	↓ 10.3%
境内被篡改网站总数 其中政府网站数量	•736 •54	↓ 8.3% ↑ 20.0%
境内被植入后门网站总数 其中政府网站数量	•659 •5	↑ 1.1% ↑ 25.0%
针对境内网站的仿冒页面数量	•1612	↑ 30.3%
新增信息安全漏洞数量 其中高危漏洞数量	•414 •166	↑ 17.6% ↑ 21.2%

=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

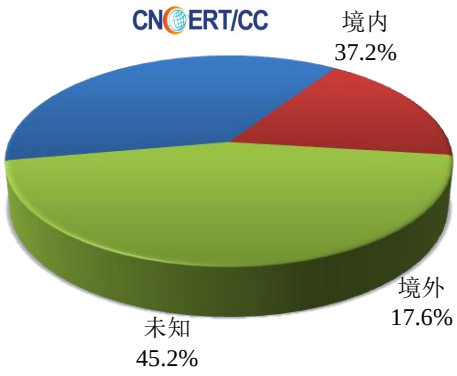
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.8 万以及境内感染飞客（conficker）蠕虫的主机约 6.7 万。

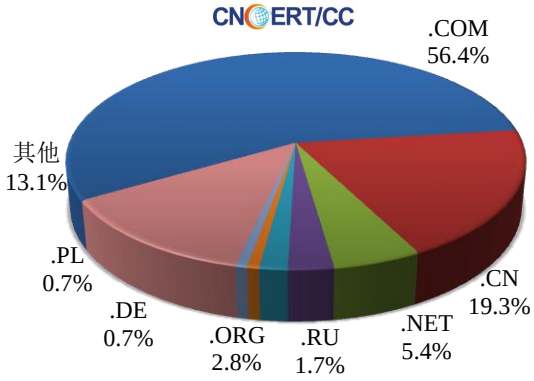


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3302 个，涉及 IP 地址 4999 个。在 3302 个域名中，有 17.6%为境外注册，且顶级域为.com 的约占 56.4%；在 4999 个 IP 中，有约 52.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 669 个 IP。

本周放马站点域名注册所属境内外分布
(12/24-12/30)



本周放马站点域名所属顶级域的分布
(12/24-12/30)



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。

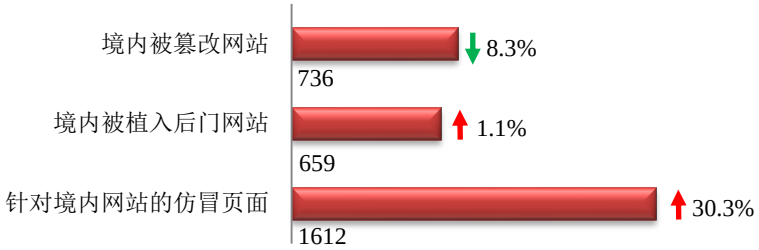
ANVA恶意地址黑名单发布地址

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。

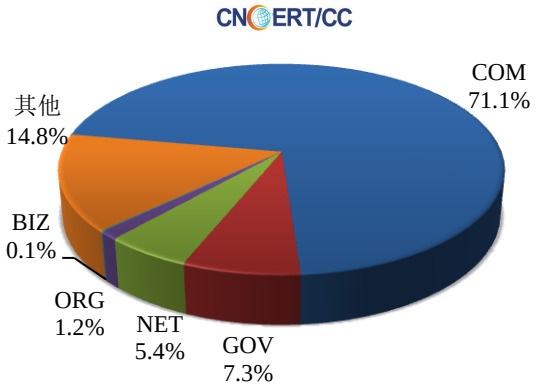
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 736 个；境内被植入后门的网站数量为 659 个；针对境内网站的仿冒页面数量 1612 个。

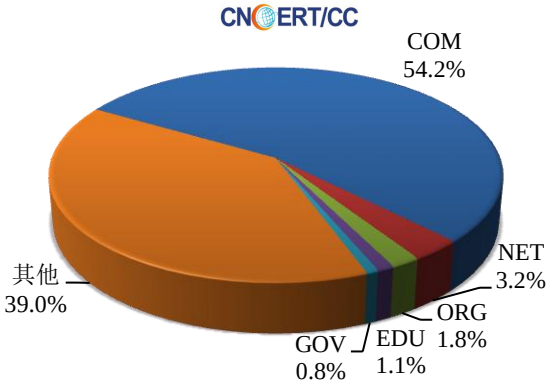


本周境内被篡改政府网站（GOV 类）数量为 54 个（约占境内 7.3%），较上周环比上升了 20.0%；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 0.8%），较上周环上升了 25.0%；针对境内网站的仿冒页面涉及域名 568 个，IP 地址 194 个，平均每个 IP 地址承载了约 8 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/24-12/30)

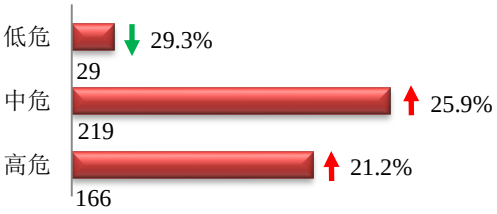


本周我国境内被植入后门网站按类型分布
(12/24-12/30)

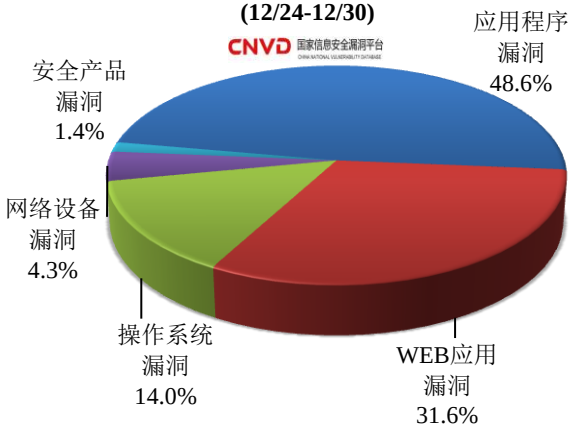


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 414 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
(12/24-12/30)



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

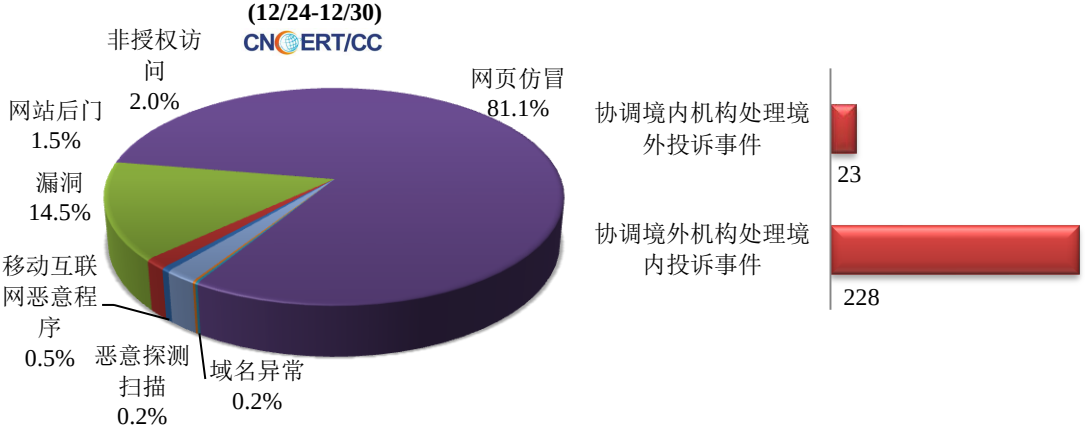
http://www.cnvd.org.cn/webinfo/list?type=4

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

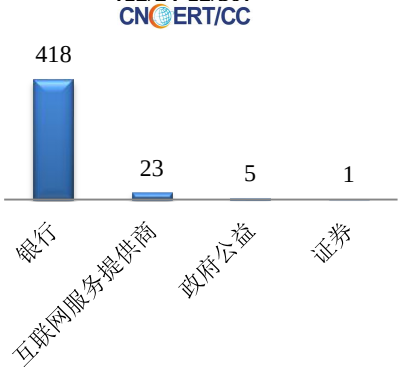
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 551 起，其中跨境网络安全事件 251 起。

本周CNCERT处理的事件数量按类型分布 (12/24-12/30)

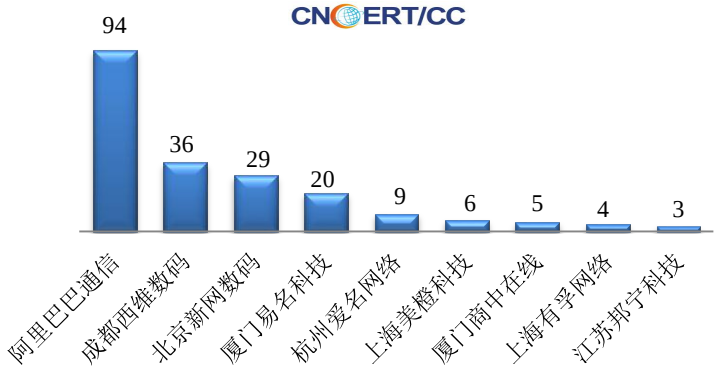


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 447 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒 418 起和互联网服务提供商事件 23 起。

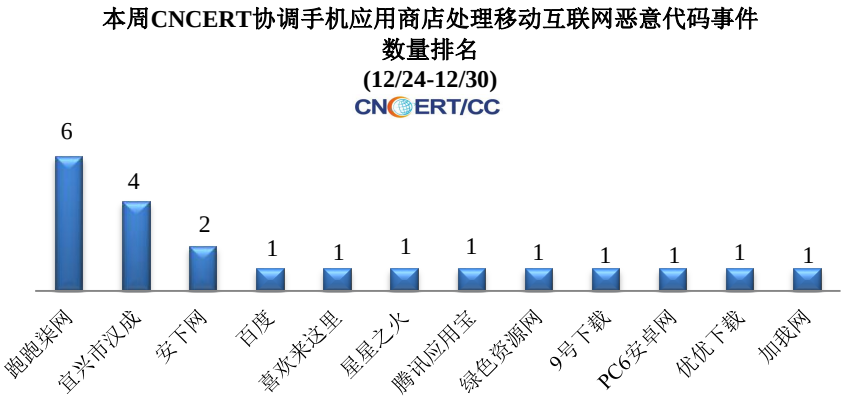
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (12/24-12/30)



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 (12/24-12/30)



本周，CNCERT 协调 12 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 21 个。



业界新闻速递

1、国家网信办发布《金融信息服务管理规定》

网信办 12 月 26 日消息 为加强金融信息服务内容管理，提高金融信息服务质量，促进金融信息服务健康有序发展，保护自然人、法人和非法人组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定《金融信息服务管理规定》。

2、欧盟将为 14 个开源项目漏洞赏金计划支付赏金

E 安全 12 月 29 日消息 欧盟议员 Julia Reda 上周宣布，欧盟将为 14 个开源项目的漏洞赏金计划支付赏金。这 14 个项目可按字母顺序排列为 7-zip、Apache Kafka、Apache Tomcat、Digital Signature Services （DSS）、Drupal、Filezilla、FLUX TL、GNU CLibrary （glibc）、KeePass、midPoint、Notepad++、PuTTY、the Symfony PHP framework、VLC Media Player 与 WSO2。该漏洞赏金计划是作为第三版免费和开源软件审计（FOSSA）项目的一部分发起的。欧盟当局于 2015 年首次批准了 FOSSA，一年前，安全研究人员在 OpenSSL 库中发现了高危安全漏洞，OpenSSL 库是许多网站用以支持 HTTPS 连接的开源项目。

3、科威特国家银行应用 Ripple 新汇款服务

E 安全 12 月 29 日消息 为提高跨境汇款速度，科威特国家银行（NBK）加入 Ripple 基于区块链的支付网络。该银行周四宣布，推出了一项名为“NBK Direct Remit”的新汇款服务，该服务利用 Ripple 技术实现了基于区块链的“即时”支付。全球有越来越多的金融公司就基于区块链的支付服务与 Ripple 结成合作关系，科威特国家银行也成了其中之一。最近，马来西亚银行集团 CIMB、韩国加密货币交易所 Coinone、美国银行巨头

PNC 以及汇款公司阿联酋交易所也成为这些金融公司中的一员。

4、美国电信运营商 CenturyLink 停电致各地 911 服务受影响

网易新闻 12 月 29 日消息 由于电信供应商 CenturyLink 出现线路问题，导致美国全国范围内出现网络中断，主要受影响的是西部各州。该情况从美国东部时间周四（27 日）上午 8 点 18 分开始，直到周五（28 日）晚上才基本恢复。更严重的是，由于 CenturyLink 为一些地区的 911 提供服务，这一故障导致多地的 911 呼叫电话无法使用。据波士顿当地媒体，受影响的地区有马萨诸塞州、密苏里州、爱达荷州、亚利桑那州和华盛顿州的部分地区。

5、近千名脱北者身份受网络攻击影响

E 安全 12 月 28 日消息 据韩国统一部称，黑客窃取了 997 名脱北者的个人数据。某官员称，这是朝鲜历史上脱北者遭遇的最大的个人数据失窃事件。12 月 19 日在 Hana 中心计算机中发现了恶意代码。进一步调查显示，有人窃取了包含脱北者个人数据的文件，而此人并非其员工。目前尚未发现其他受感染计算机。总共约有 30000 名脱北者已逃至韩国。韩国境内有 25 家类似的再定居中心，这些再定居中心试图帮助脱北者成功在别国定居，并开启新生活。

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：温森浩

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158