国家互联网应急中心

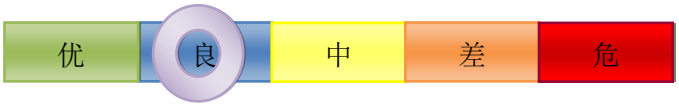
网络安全信息与动态周报

2019 年第 52 期

12 月 23 日-12 月 29 日

CNCERT/CC

本周网络安全基本态势

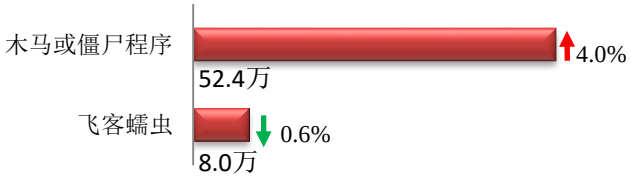


境内感染网络病毒的主机数量	•60.5万	↑ 3.4%
境内被篡改网站总数 其中政府网站数量	•6419 •23	↓ 10.1% ↓ 11.5%
境内被植入后门网站总数 其中政府网站数量	•2775 •22	↓ 4.0% ↑ 10.0%
针对境内网站的仿冒页面数量	•1266	↓ 36.4%
新增信息安全漏洞数量 其中高危漏洞数量	•203 •67	↓ 11.7% ↓ 13.0%

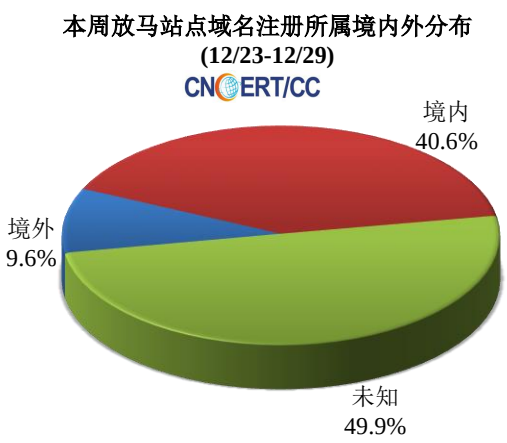
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

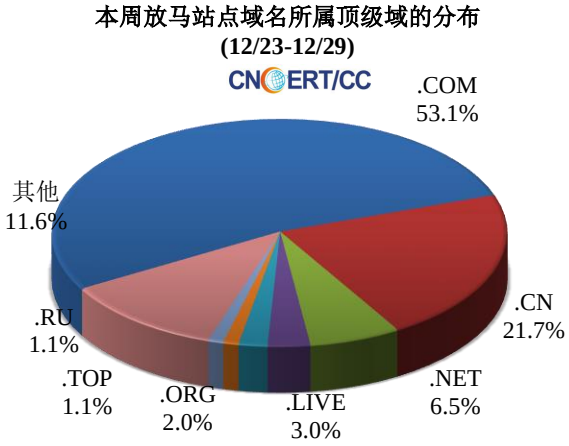
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 60.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 52.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.0 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 836 个，涉及 IP 地址 2035 个。在 836 个域名中，有 9.6%为境外注册，且顶级域为.com 的约占 53.1%；在 2035 个 IP 中，有约 25.1%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 151 个 IP。





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。

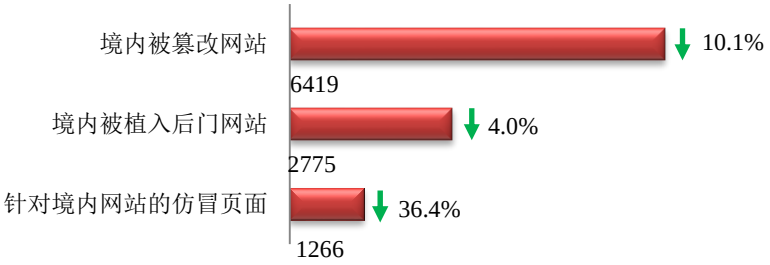
ANVA恶意地址黑名单发布地址

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。

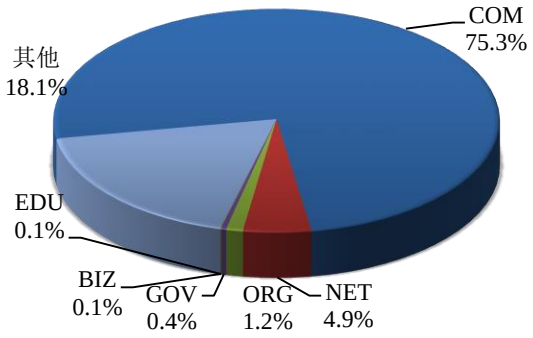
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 6419 个；被植入后门的网站数量为 2775 个；针对境内网站的仿冒页面数量 1266 个。

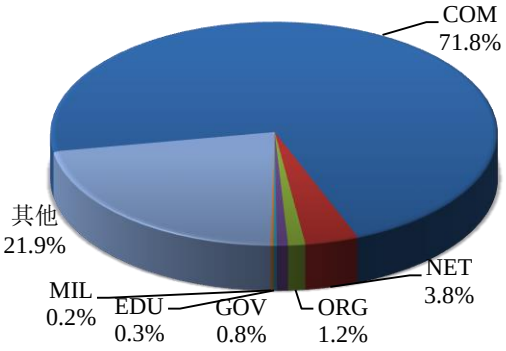


本周境内被篡改政府网站（GOV 类）数量为 23 个（约占境内 0.4%），较上周下降了 11.5%；境内被植入后门的政府网站（GOV 类）数量为 22 个（约占境内 0.8%），较上周上涨了 10.0%。

本周我国境内篡改网站按类型分布
(12/23-12/29)

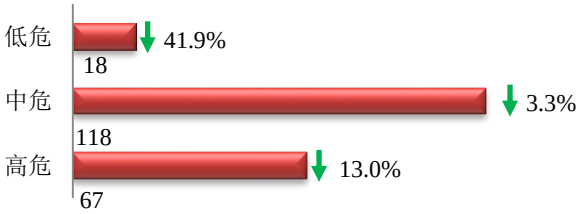


本周我国境内被植入后门网站按类型分布
(12/23-12/29)

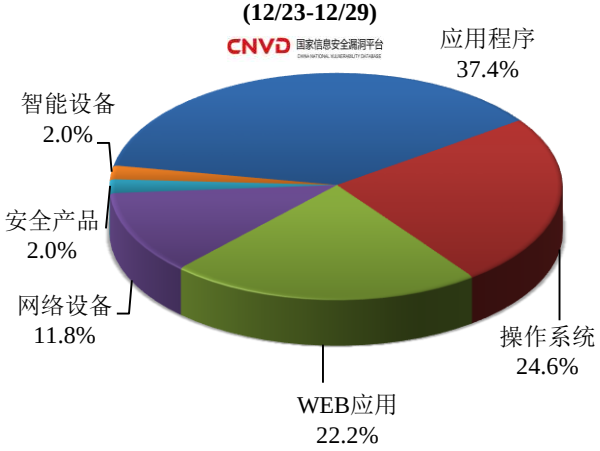


本周重要漏洞情况

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
(12/23-12/29)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统和 WEB 应用。

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

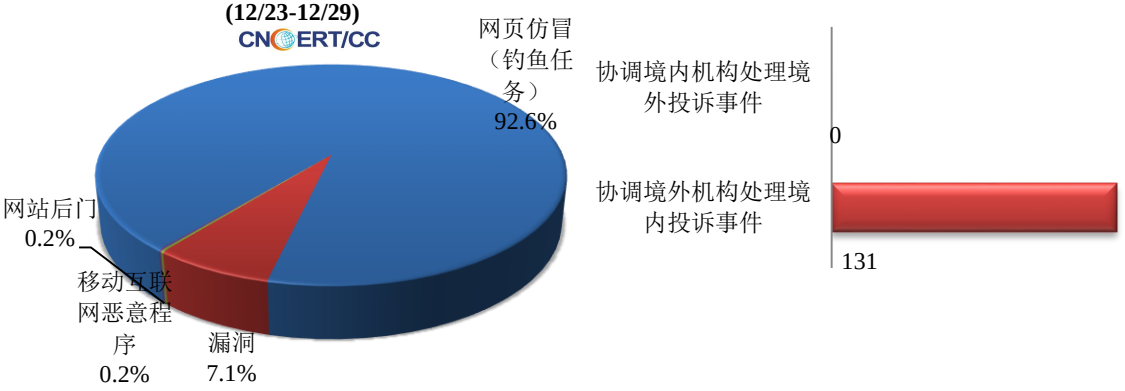
http://www.cnvd.org.cn/webinfo/list?type=4

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

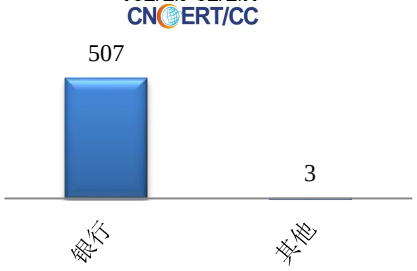
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 551 起，其中跨境网络安全事件 131 起。

本周CNCERT处理的事件数量按类型分布 (12/23-12/29)

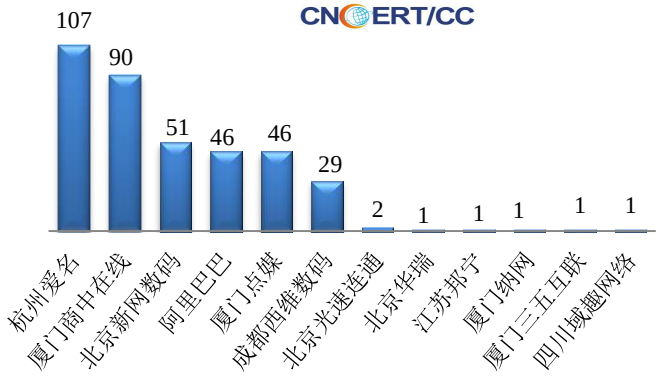


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 510 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 507 起和其他事件 3 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (12/23-12/29)

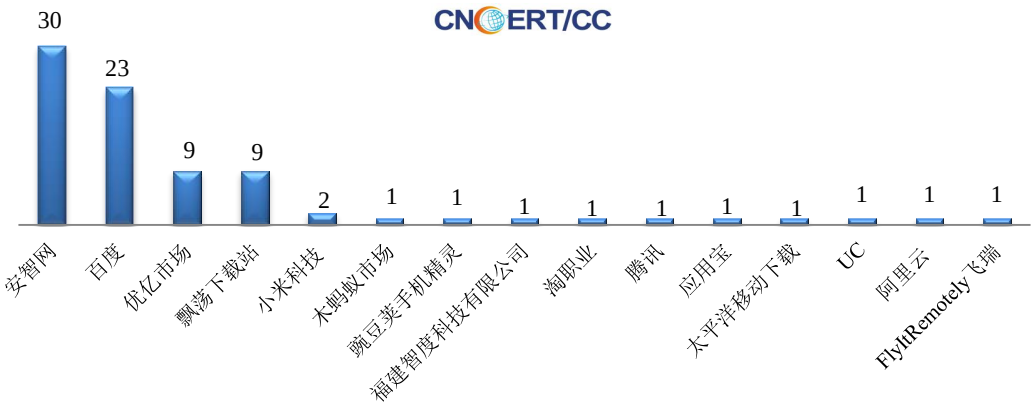


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (12/23-12/29)



本周，CNCERT 协调 15 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 83 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
(12/23-12/29)



业界新闻速递

1、 全国人大常委会法工委：2020 年将制定个人信息保护法、数据安全法

12 月 20 日，据中新网消息，在全国人大常委会法工委举行的第三次记者会上，全国人大常委会法工委发言人表示，中国明年将制定个人信息保护法、数据安全法等。在记者会上，谈及全国人大常委会 2020 年的立法工作安排情况，发言人介绍，按照立法法的规定，全国人大常委会都要编制年度立法工作计划，围绕党和国家中心任务，回应人民群众关切，统筹安排立法工作，具体工作由法工委负责。并称，立法工作计划已经全国人大常委会第四十四次委员长会议原则通过，对明年的立法工作作出预安排。

2、 最高法修改《民事诉讼证据规定》，完善电子数据证据规则体系

12 月 25 日，最高人民法院发布公告称，《最高人民法院关于修改<关于民事诉讼证据的若干规定>的决定》已于 2019 年 10 月 14 日由最高人民法院审判委员会第 1777 次会议通过，自 2020 年 5 月 1 日起施行；并颁布了修改后的《关于民事诉讼证据的若干规定》，进一步补充、完善了电子数据范围的规定，明确了电子数据的审查判断标准。

3、 俄罗斯成功断开全球互联网

12 月 23 日，据“ZDNet”网站报道，俄罗斯政府周一宣布，它完成了一系列测试，成功地切断了与全球互联网的连接。测试从上周开始，持续了数天，涉及俄罗斯政府机构、本地互联网服务提供商和俄罗斯本地互联网公司。此举的目的是测试俄罗斯的国家互联网基础设施（RuNet）是否可以在不接入全球 DNS 系统和外部互联网的情况下正常运行。俄罗斯政府没有透露有关测试的任何技术细节以及测试的具体内容，只表示政府测试了几种断开连接的场景，包括模拟来自外国的恶意网络攻击的场景。据悉，俄罗斯的《互联网主权法》，赋予俄罗斯政府这一权力：以“国家安全”为由，基本上不需要解释就可以随意将该国与互联网的其余部分断开。

4、 联合国大会批准俄罗斯打击网络犯罪决议草案

12 月 29 日，据环球网报道，联合国近日通过了一项俄罗斯此前提交的旨在打击网络犯罪的决议草案。该协议草案由俄罗斯和其他 47 个国家联合起草，最终以 79 票赞成、60 票反对、33 票弃权的结果通过。报道称，该决议呼吁联合国大会成立一个代表世界各地的专家委员会，以制定一项全面的国际公约，用于打击信息和通信技术犯罪行为。不过，这项决议却遭到美国及其盟友的强烈反对，这些国家认为这项草案实际上是损害而非加强打击网络犯罪。对此，莫斯科方面表示，该决议旨在巩固全球打击网络犯罪的努力，赋予了每个国家对其网络空间的主权。

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 2018 年，CNCERT 与 76 个国家和地区的 233 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：朱天

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315