国家互联网应急中心

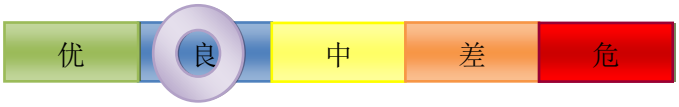
网络安全信息与动态周报

2019 年第 50 期

12 月 9 日-12 月 15 日

CNCERT/CC

本周网络安全基本态势

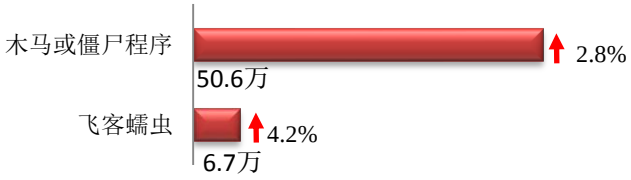


境内感染网络病毒的主机数量	•57.3万	↑ 3.0%
境内被篡改网站总数 其中政府网站数量	•1491 •4	↑ 223.4% =
境内被植入后门网站总数 其中政府网站数量	•3119 •11	↑ 6.3% ↓ 59.3%
针对境内网站的仿冒页面数量	•1260	↑ 3.6%
新增信息安全漏洞数量 其中高危漏洞数量	•327 •133	↓ 32.0% ↓ 39.5%

= 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

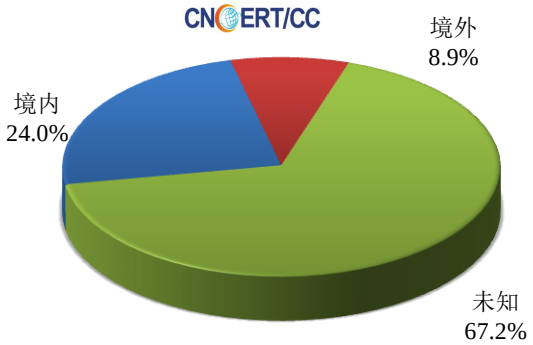
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 57.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.6 万以及境内感染飞客（conficker）蠕虫的主机约 6.7 万。

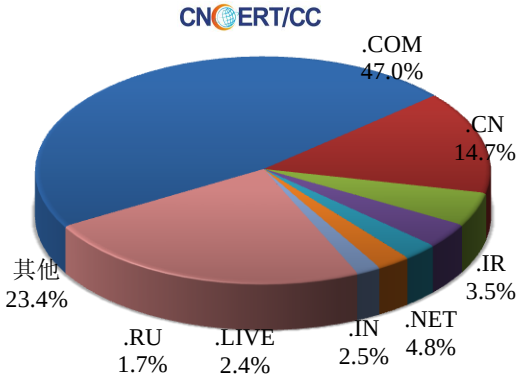


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1501 个，涉及 IP 地址 2481 个。在 1501 个域名中，有 8.9%为境外注册，且顶级域为.com 的约占 47.0%；在 2481 个 IP 中，有约 56.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 175 个 IP。

本周放马站点域名注册所属境内外分布
(12/09-12/15)



本周放马站点域名所属顶级域的分布
(12/09-12/15)



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。

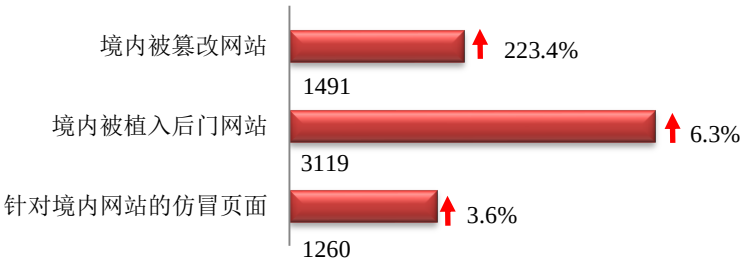
ANVA恶意地址黑名单发布地址

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。

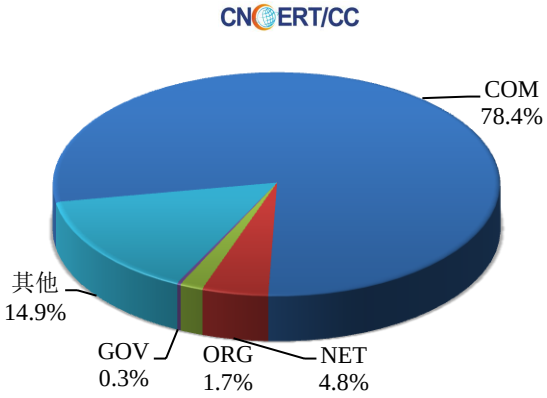
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1491 个；被植入后门的网站数量为 3119 个；针对境内网站的仿冒页面数量 1260 个。

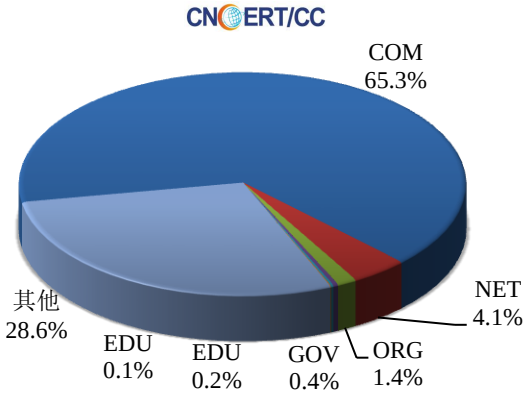


本周境内被篡改政府网站（GOV 类）数量为 4 个（约占境内 0.3%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 0.4%），较上周环比下降了 59.3%。

本周我国境内篡改网站按类型分布
(12/09-12/15)

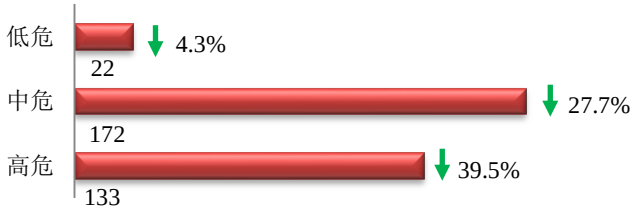


本周我国境内被植入后门网站按类型分布
(12/09-12/15)

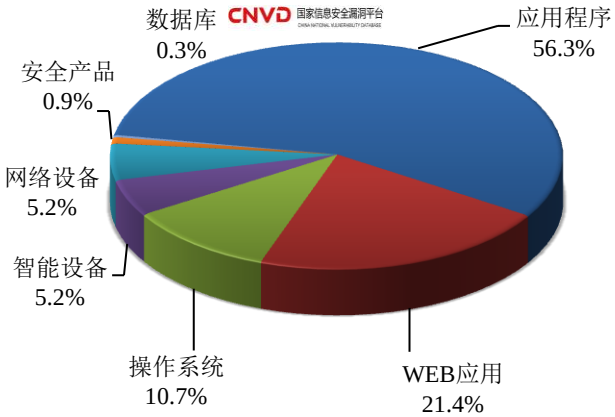


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 327 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
(12/09-12/15)



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 应用和操作系统。

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

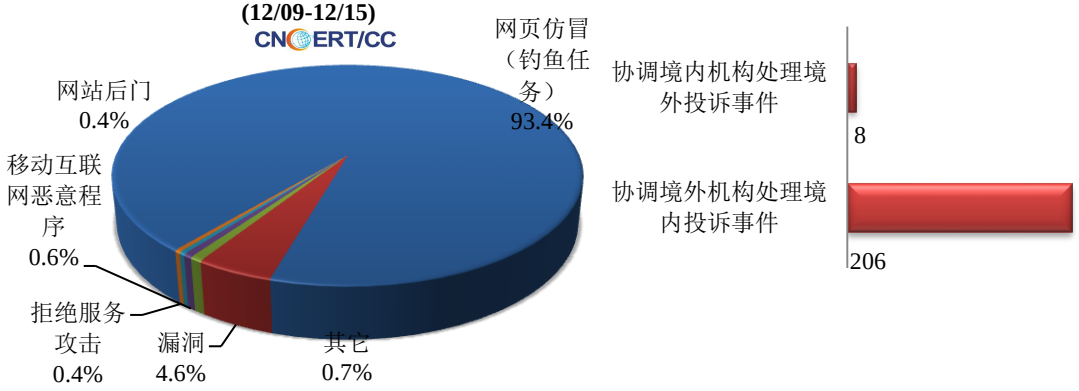
http://www.cnvd.org.cn/webinfo/list?type=4

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

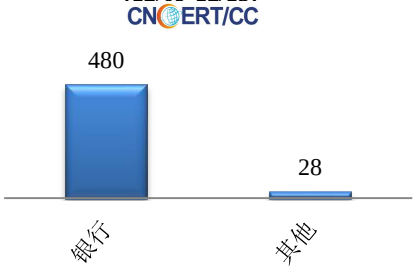
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 544 起，其中跨境网络安全事件 214 起。

本周CNCERT处理的事件数量按类型分布 (12/09-12/15)

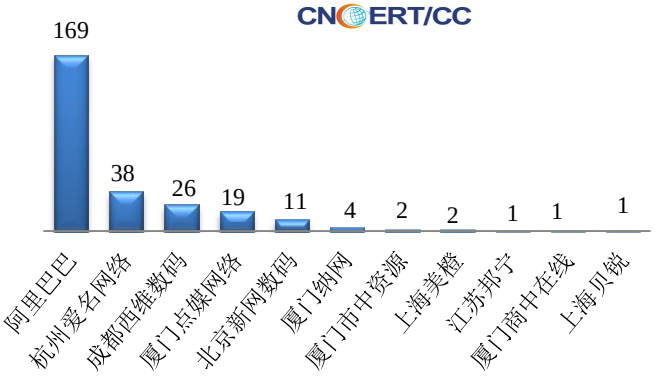


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 508 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 480 起和其他事件 28 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (12/09-12/15)

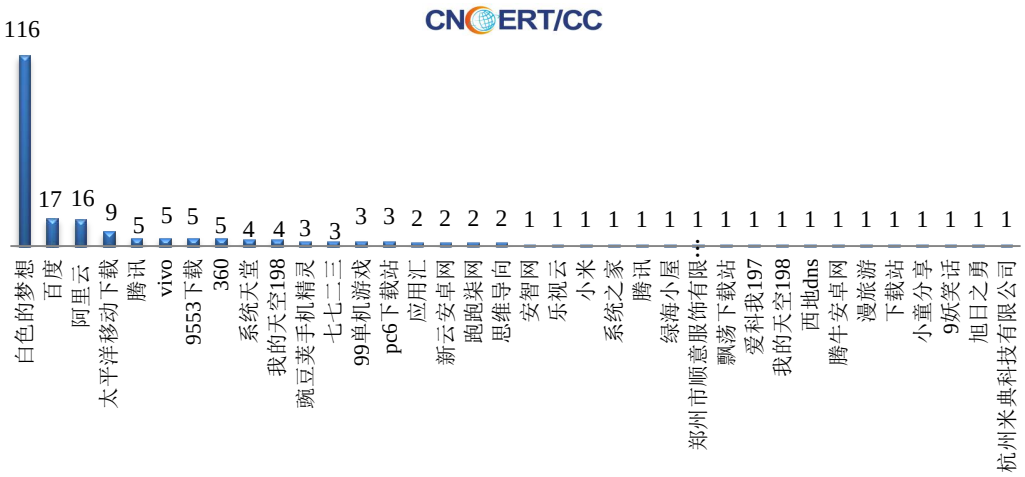


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (12/09-12/15)



本周，CNCERT 协调 36 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 224 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
(12/09-12/15)



业界新闻速递

1、 2019 年中国网络安全产业规模预计超 600 亿元

12 月 9 日，中新社消息，9 日在北京举行的 2019 年中国网络安全产业高峰论坛上，中国工业和信息化部网络安全管理局表示，2019 年中国网络安全产业规模预计超过 600 亿元人民币，年增长率超过 20%，明显高于国际 8%的平均增速，保持健康的发展态势。报道称，中国的网络安全产业结构日趋优化，既有防火墙、监测以及防病毒等传统产品，又有态势感知、数据防泄露等新兴产品，基本构成了覆盖防护、监测和应急的各个环节。据统计，截至 2019 年 11 月底，在公开融资方面，中国国内上市的网络安全企业达到了 23 家，创新孵化方面，有 100 多家创投机构在网络安全领域进行投资布局。

2、 美国《国防授权法案》增加保护电网不受网络攻击的立法

12 月 11 日，据美国数字媒体网 The Hill 报道，《美国国防授权法》（National Defense Authorization Act，NDAA）的最终版本中增加了保护国家电网免受网络攻击的立法，立法内容包括在国家实验室内建立为期两年的试点计划，帮助消除电网中的漏洞。美参议院表示，能源网为美国的金融交易、通信网络、医疗服务等提供动力。因此，如果这个关键的基础架构遭到黑客的入侵，美国将面临巨大的风险。国家情报局局长办公室进行的年度全球威胁评估发现，俄罗斯和中国都有能力攻击美关键基础设施，例如电网，并

造成“短暂的破坏性影响”。美国家基础设施咨询委员会向特朗普发送的报告草稿进一步强调了电网遭受网络攻击的危险。该报告呼吁采取“大胆的行动”，以应对包括能源网格在内的关键基础设施日益增加的网络威胁。

3、 Intel 公司确认并发布“骑士”漏洞

12 月 10 日，Intel 官方正式确认并发布了清华大学计算机系汪东升、吕勇强、邱朋飞和马里兰大学 Gang Qu 等发现的“VoltJockey”（骑士）漏洞。“骑士”漏洞将影响 Intel 公司第 6、7、8、9、10 代 Core™核心处理器，以及 Intel 至强处理器 E3 v5 & v6 和 Intel 至强 E-2100 和 E-2200 等系列处理器。“骑士”漏洞是我国研究团队发现的首个处理器硬件漏洞，该漏洞是因为现代主流处理器微体系架构设计时采用的动态电源管理模块 DVFS（Dynamic Voltage and Frequency Scaling）存在安全隐患造成的。来自英国和德国的团队也同期对此漏洞发现具有贡献。

4、 伊朗称击退大规模网络攻击

12 月 11 日，据伊朗法尔斯通讯社报道，伊朗通信和信息技术部长阿扎里·贾赫鲁米宣布，伊朗发现并击退了一个由外国政府组织的针对伊电子政务基础设施的大规模网络攻击。贾赫鲁米表示暂不能说明是哪个国家对其发动了攻击，稍后会公布一份报告。此前，贾赫鲁米于 10 月在慕尼黑安全会议网络安全峰会上发表讲话时说，过去一年，代号为“数字堡垒”的伊朗网络安全项目可能阻止了近 3300 万次网络攻击。

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：朱芸茜

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315