国家互联网应急中心

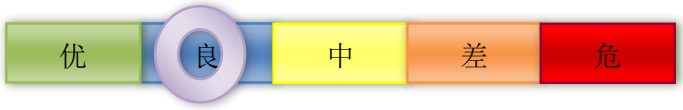
网络安全信息与动态周报

2019 年第 51 期

12 月 16 日-12 月 22 日

CNCERT/CC

本周网络安全基本态势

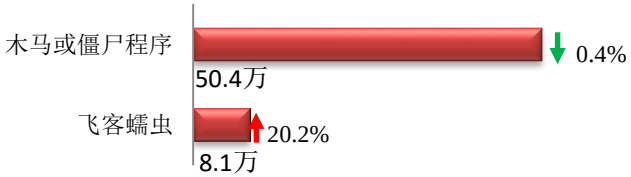


境内感染网络病毒的主机数量	•58.5万	↑ 2.0%
境内被篡改网站总数 其中政府网站数量	•7138 •26	↑ 378.7% ↑ 22 个
境内被植入后门网站总数 其中政府网站数量	•2891 •20	↓ 7.3% ↑ 9 个
针对境内网站的仿冒页面数量	•1992	↑ 58.1%
新增信息安全漏洞数量 其中高危漏洞数量	•230 •77	↓ 29.7% ↓ 42.1%

= 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

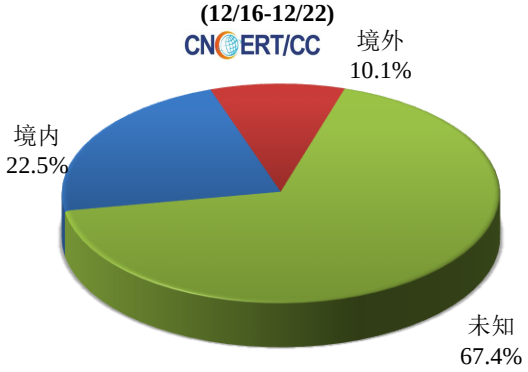
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 58.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.1 万。

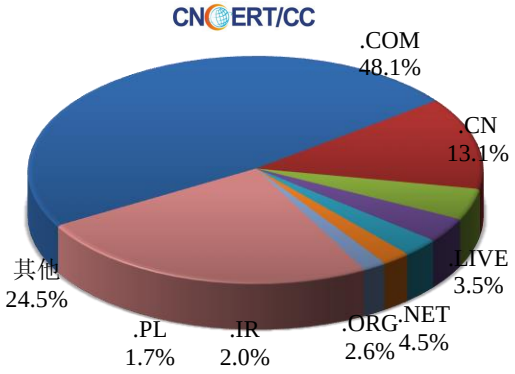


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1369 个，涉及 IP 地址 2164 个。在 1369 个域名中，有 10.1%为境外注册，且顶级域为.com 的约占 47.0%；在 2164 个 IP 中，有约 48.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 165 个 IP。

本周放马站点域名注册所属境内外分布
(12/16-12/22)



本周放马站点域名所属顶级域的分布
(12/16-12/22)



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。

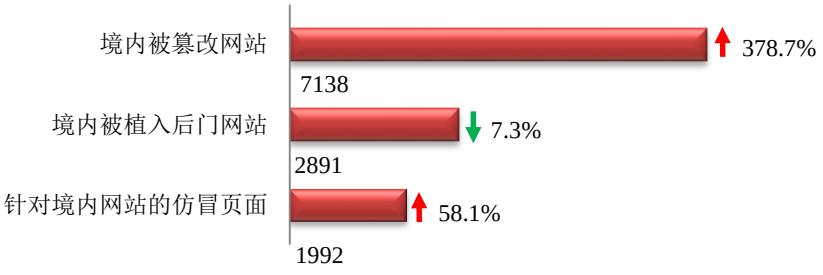
ANVA恶意地址黑名单发布地址

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。

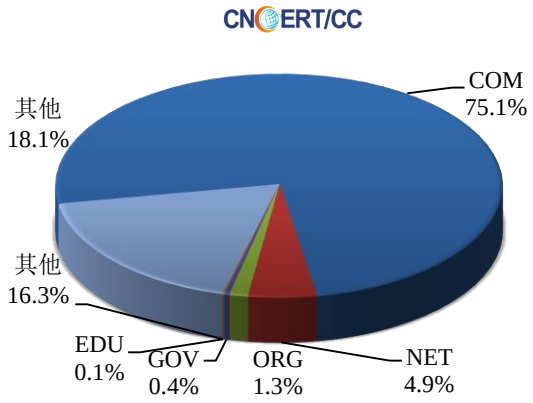
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7138 个；被植入后门的网站数量为 2891 个；针对境内网站的仿冒页面数量 1992 个。

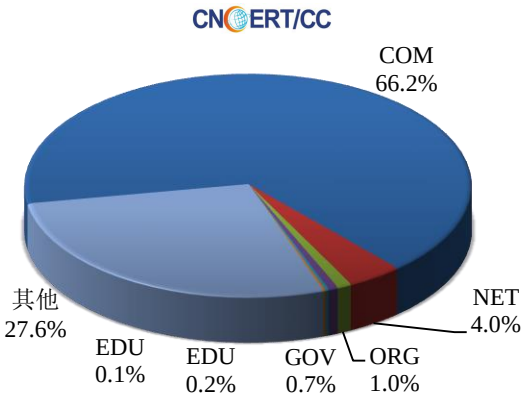


本周境内被篡改政府网站（GOV 类）数量为 26 个（约占境内 0.4%），较上周增长了 22 个；境内被植入后门的政府网站（GOV 类）数量为 20 个（约占境内 0.7%），较上周增长了 9 个。

本周我国境内篡改网站按类型分布
(12/16-12/22)

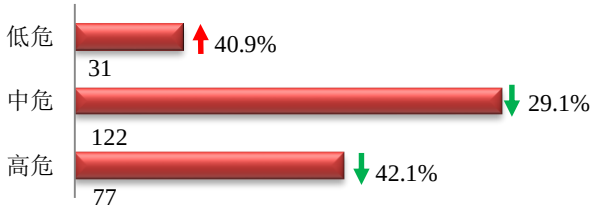


本周我国境内被植入后门网站按类型分布
(12/16-12/22)

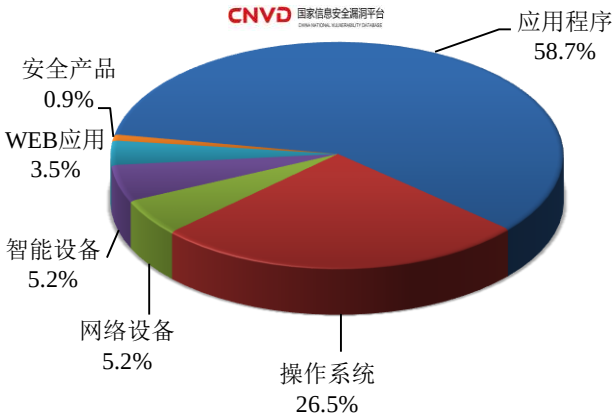


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 230 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
(12/16-12/22)



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

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

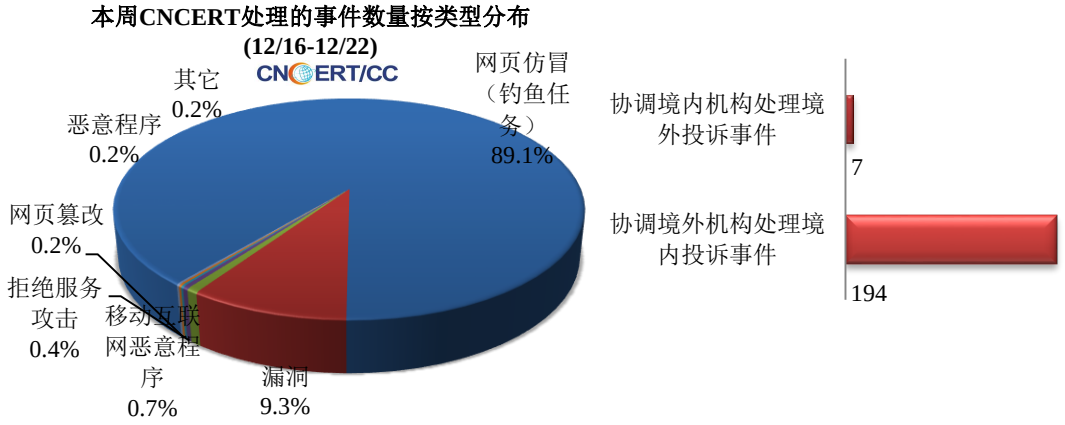
CNVD漏洞周报发布地址

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

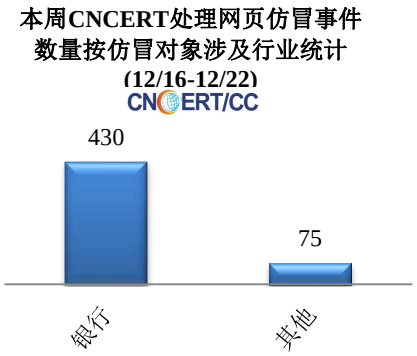
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

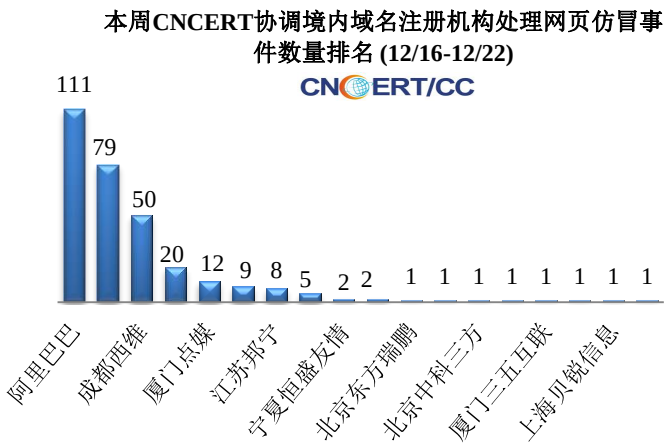
本周事件处理情况

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 567 起，其中跨境网络安全事件 201 起。



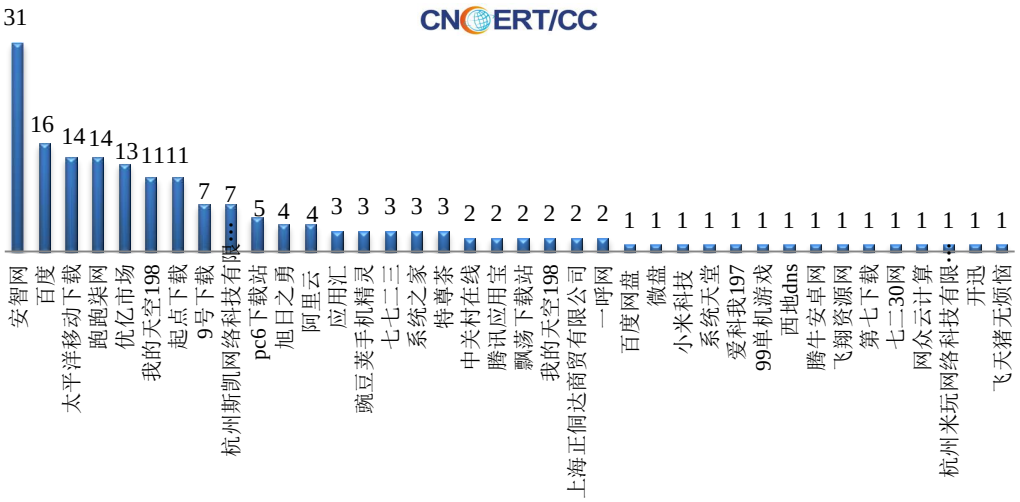
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 505 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 430 起和其他事件 75 起。





本周，CNCERT 协调 38 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 179 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
(12/16-12/22)



业界新闻速递

1、 国家网信办发布《网络信息内容生态治理规定》

12 月 20 日，国家互联网信息办公室发布了《网络信息内容生态治理规定》（以下简称《规定》），自 2020 年 3 月 1 日起施行。《规定》的出台，旨在营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益。

2、 工业和信息化部关于《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿）公开征求意见的公告

12 月 17 日，为贯彻落实《加强工业互联网安全工作的指导意见》，推动工业互联网安全责任落实，对工业互联网企业网络安全实施分类分级管理，提升工业互联网安全保障能力和水平，中华人民共和国工业和信息化部研究起草了《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿），向社会公开征求意见。

3、 美国 CISA 成立新的 ICT 供应链工作小组

12 月 20 日消息，美国网络安全与基础设施安全局（CISA）下属信息和通信技术（ICT）供应链风险管理（SCRM）工作组批准了一个新的工作小组，以研发 SCRM 框架和最佳实

践。该小组的目标是使整个 ICT 生态系统中的利益相关者有能力做出明智的决策，从而提高他们整个供应链的可信度。该小组将针对供应商风险、生命周期管理、网络安全等方面制定 SCRM 指南，以帮助组织应对供应链挑战。

4、 俄罗斯护网新动作，与全球断网检验应对外部威胁攻击能力

12 月 19 日，美国军事新闻媒体网站 Defense one 消息，俄罗斯通讯部近日表示，俄罗斯计划在 12 月 23 日断开与全球互联网的连接，对其国内互联网基础设施的可靠性进行测试，以检验其应对外部互联网威胁的能力。通讯部保证，威胁测试将会分阶段进行，不会影响普通的互联网用户。

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：郭晶

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315