国家互联网应急中心

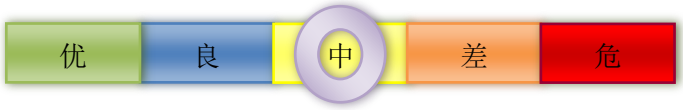
网络安全信息与动态周报

2019 年第 47 期

11 月 18 日-11 月 24 日

CNCERT/CC

本周网络安全基本态势

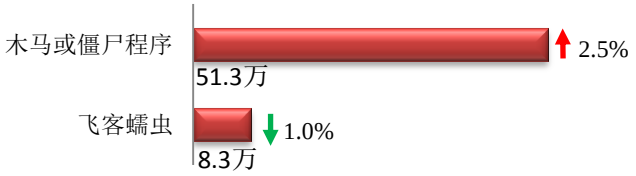


境内感染网络病毒的主机数量	•59.59万	↑2.0%
境内被篡改网站总数 其中政府网站数量	•6312 •24	↓27.3% ↑26.3%
境内被植入后门网站总数 其中政府网站数量	•3494 •44	↑16.9% ↓27.9%
针对境内网站的仿冒页面数量	•485	↓42.6%
新增信息安全漏洞数量 其中高危漏洞数量	•494 •147	↓8.7% ↑3.5%

═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

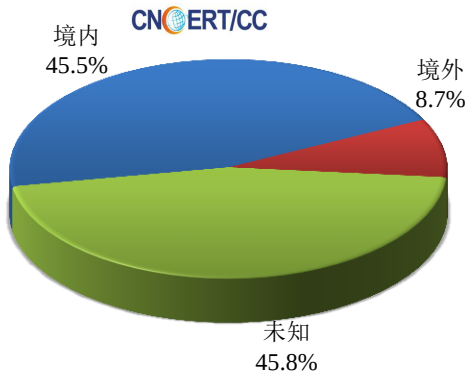
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 59.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.3 万以及境内感染飞客（conficker）蠕虫的主机约 8.3 万。

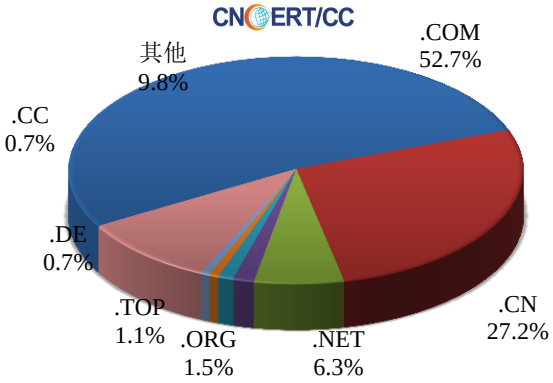


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1204 个，涉及 IP 地址 2048 个。在 1204 个域名中，有 8.7%为境外注册，且顶级域为.com 的约占 52.7%；在 2048 个 IP 中，有约 36.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 293 个 IP。

本周放马站点域名注册所属境内外分布
(11/18-11/24)



本周放马站点域名所属顶级域的分布
(11/18-11/24)



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。

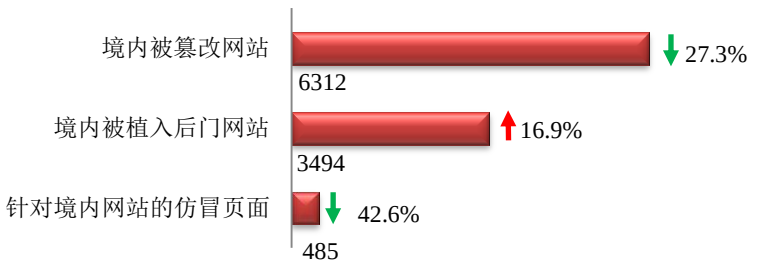
ANVA恶意地址黑名单发布地址

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。

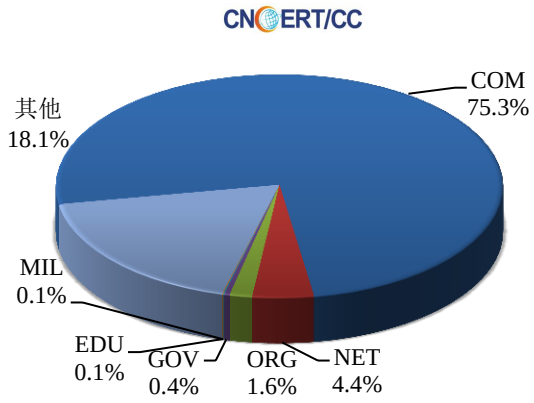
本周网站安全情况

本周 CNCERT 监测发现境内境内被篡改网站数量 6312 个；被植入后门的网站数量为 3494 个；针对境内网站的仿冒页面数量 485 个。

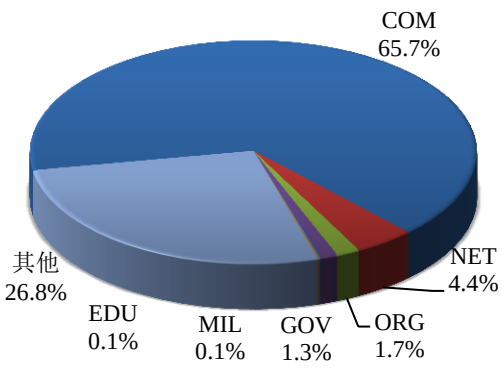


本周境内被篡改政府网站（GOV 类）数量为 24 个（约占境内 0.4%），较上周环比上涨了 26.3%；境内被植入后门的政府网站（GOV 类）数量为 44 个（约占境内 1.3%），较上周环比下降了 27.9%。

本周我国境内篡改网站按类型分布
(11/18-11/24)

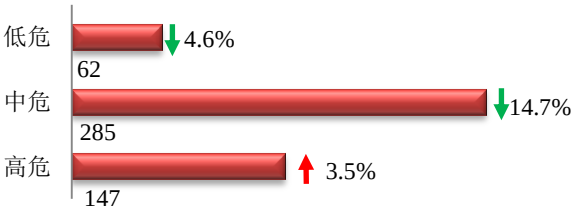


本周我国境内被植入后门网站按类型分布
(11/18-11/24)

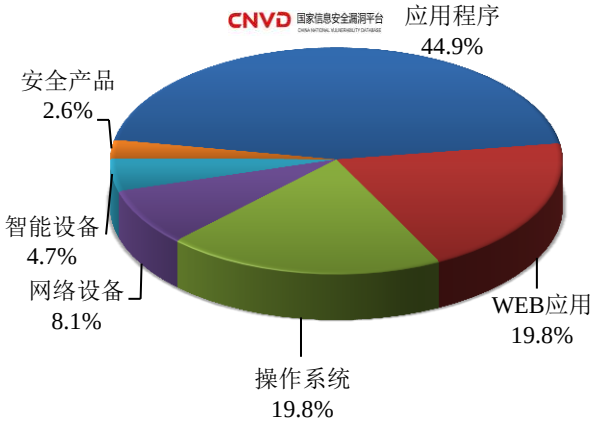


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 494 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
(11/18-11/24)



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

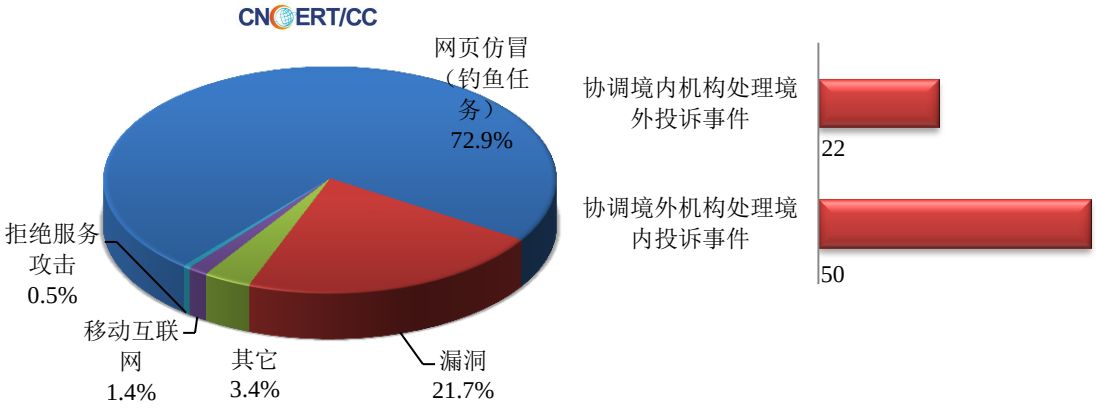
http://www.cnvd.org.cn/webinfo/list?type=4

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

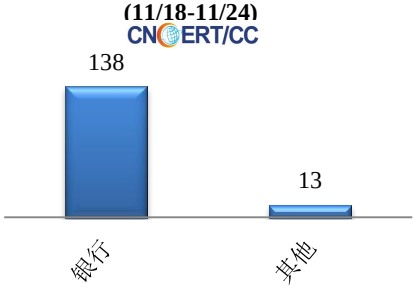
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 207 起，其中跨境网络安全事件 72 起。

本周CNCERT处理的事件数量按类型分布 (11/18-11/24)



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 151 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 138 起和其他事件 13 起。

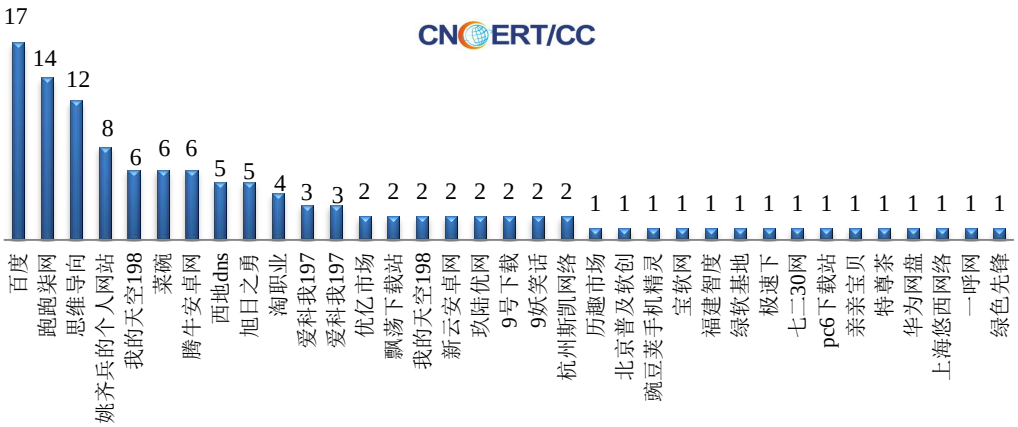
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (11/18-11/24)



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 (11/18-11/24)

本周，CNCERT 协调 35 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。

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
(11/18-11/24)



业界新闻速递

1、 国家网信办就《网络安全威胁信息发布管理办法（征求意见稿）》公开征求意见

11 月 20 日，中国国家互联网信息办公室发布《关于<网络安全威胁信息发布管理办法（征求意见稿）>公开征求意见的通知》。通知表示，为规范发布网络安全威胁信息的行为，有效应对网络安全威胁和风险，保障网络运行安全，依据《中华人民共和国网络安全法》等相关法律法规，国家互联网信息办公室会同公安部等有关部门起草了《网络安全威胁信息发布管理办法（征求意见稿）》，向社会公开征求意见。在通知发布的同时，国家网信办还发布了《国家互联网信息办公室有关负责人就<网络安全威胁信息发布管理办法（征求意见稿）>答记者问》，就《办法》的制定背景、依据等 9 个问题回答了记者提问。

2、 澳大利亚发布物联网安全实践准则草案

11 月 19 日，据 ZDNet 网站消息，澳大利亚发布物联网安全实践准则草案，并至 2020 年 3 月 1 日前公开征求意见。该准则将适用于澳大利亚所有可用的 IoT 设备，包括连接到互联网的日常智能设备，例如智能电视、手表和智能音箱等。该准则基于 13 条原则，其中前三条为最高优先级，包括：不使用重复的默认密码或弱密码；向设备制造商、服务提供商和 APP 开发人员提供漏洞披露政策，建立公共的访问、联系站点；确保软件和固件的安全更新。

3、 Oracle 电子商务套间存严重缺陷可导致上万企业面临风险

11 月 20 日，bleepingcomputer 网站消息，Oracle 电子商务套件（EBS）中发现的两个不当访问控制漏洞（CVE-2019-2638 和 CVE-2019-2633），可能使攻击者完全控制公司的整个企业资源计划（ERP）解决方案。Onapsis 研究实验室表示，全球超过 21000 个机构将 Oracle EBS 用于财务管理、客户关系管理（CRM）、供应链管理（SCM）、人力资本管理（HCM）、物流、采购等，由于受影响的组件存在于所有 EBS 安装中，因此所有使用 Oracle EBS 客户可能会面临风险。消息还显示，利用这些 Oracle EBS 安全问题进行的攻击还可能导致个人敏感信息和企业财务信息的泄露。这些严重的缺陷会影响企业 ERP 系统中信息的所有机密性、完整性和可用性。

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：温森浩

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315