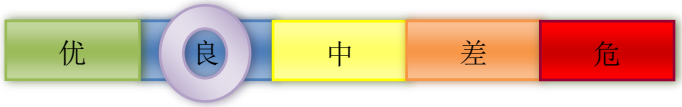
国家互联网应急中心

2018 年第 49 期

12 月 3 日-12 月 9 日

网络安全信息与动态周报

本周网络安全基本态势

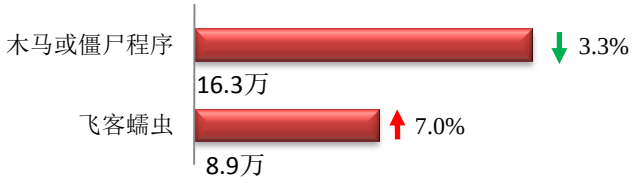


境内感染网络病毒的主机数量	•25.3万	↑0.1%
境内被篡改网站总数 其中政府网站数量	•856 •50	↑2.4% ↑19.0%
境内被植入后门网站总数 其中政府网站数量	•638 •17	↓17.0% ↓5.6%
针对境内网站的仿冒页面数量	•969	↓25.3%
新增信息安全漏洞数量 其中高危漏洞数量	•244 •108	↑14.6% ↑140.0%

=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

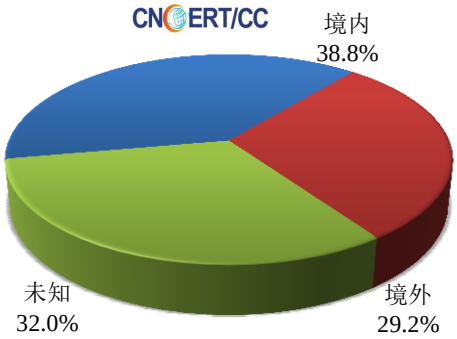
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.3 万以及境内感染飞客（conficker）蠕虫的主机约 8.9 万。

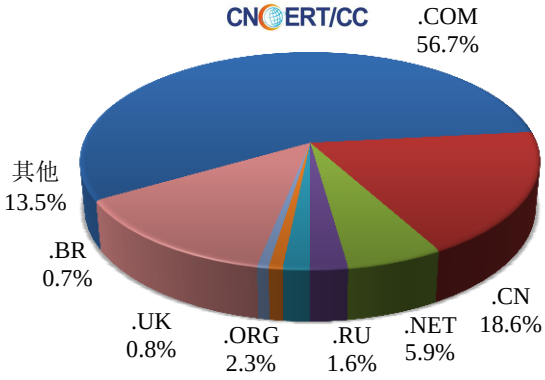


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 4896 个，涉及 IP 地址 7509 个。在 4896 个域名中，有 29.2%为境外注册，且顶级域为.com 的约占 56.7%；在 7509 个 IP 中，有约 52.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 727 个 IP。

本周放马站点域名注册所属境内外分布
(12/3-12/9)



本周放马站点域名所属顶级域的分布
(12/3-12/9)



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。

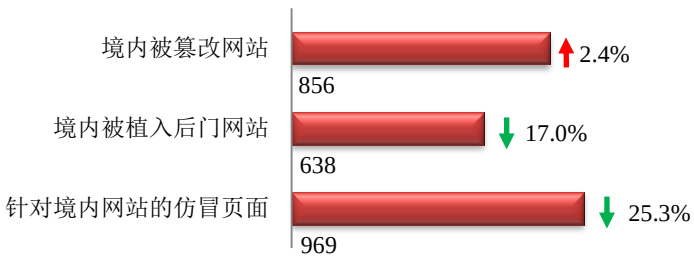
ANVA恶意地址黑名单发布地址

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。

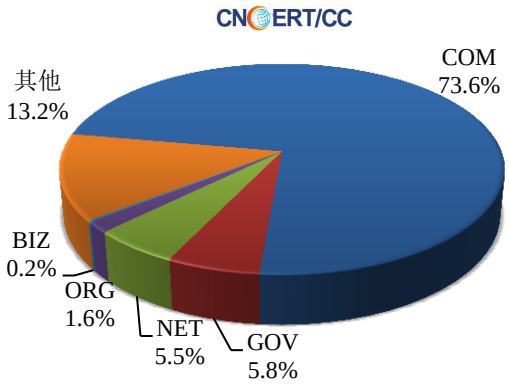
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 856 个；境内被植入后门的网站数量为 638 个；针对境内网站的仿冒页面数量 969 个。

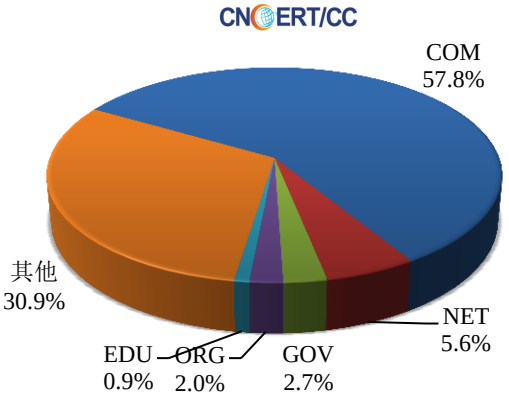


本周境内被篡改政府网站（GOV 类）数量为 50 个（约占境内 5.8%），较上周环比上升了 19.0%；境内被植入后门的政府网站（GOV 类）数量为 17 个（约占境内 2.7%），较上周环比下降了 17.0%；针对境内网站的仿冒页面涉及域名 346 个，IP 地址 215 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/3-12/9)

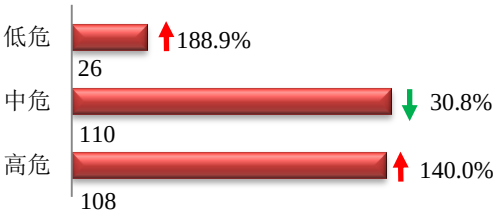


本周我国境内被植入后门网站按类型分布
(12/3-12/9)

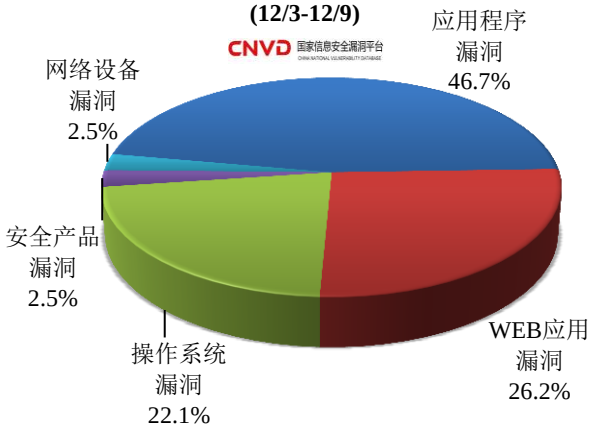


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 244 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
(12/3-12/9)



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

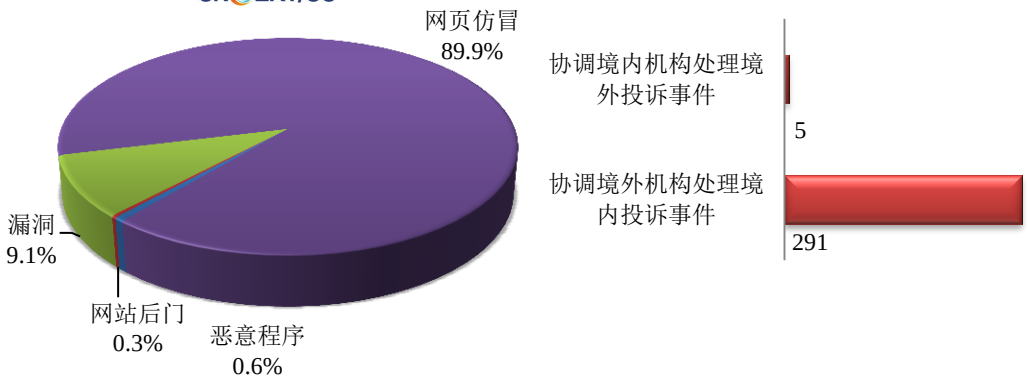
http://www.cnvd.org.cn/webinfo/list?type=4

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 658 起，其中跨境网络安全事件 296 起。

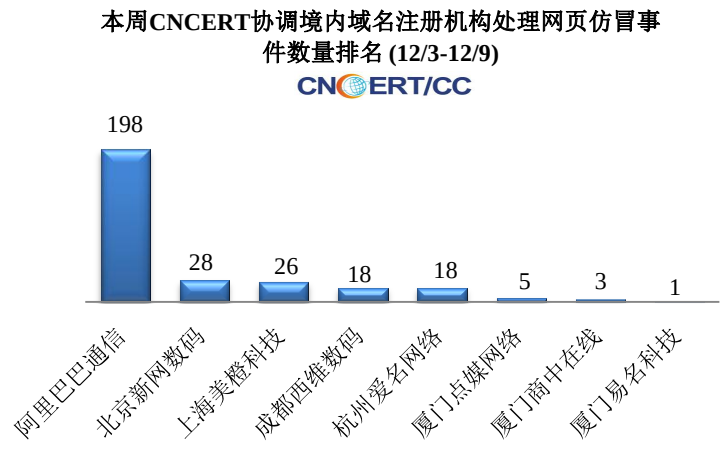
本周CNCERT处理的事件数量按类型分布 (12/3-12/9)



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 590 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 395 起和政府公益仿冒事件 167 起。

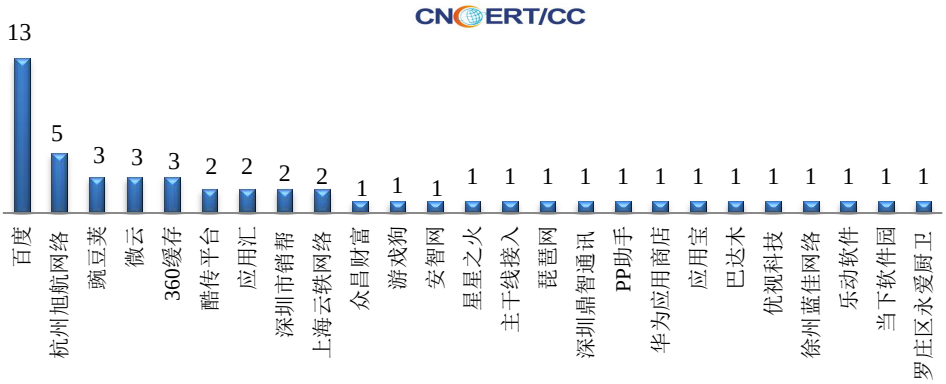
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (12/3-12/9)

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 (12/3-12/9)



本周，CNCERT 协调 25 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 51 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 (12/3-12/9)



业界新闻速递

1、工业和信息化部将开展移动恶意程序专项治理工作

cnBeta.COM12 月 3 日消息 工业和信息化部将开展移动恶意程序专项治理工作下一步，工业和信息化部将积极指导各基础电信运营企业做好 5G 系统试验的基站部署，开展好 5G 系统基站与同频段、邻频段卫星地球站等其他无线电台站的干扰协调工作，确保各类无线电业务兼容共存，促进我国 5G 产业的健康快速发展。

2、美共和党全国委员会确认在今年中期选举期间遭到网络攻击

cnBeta.COM12 月 5 日消息 据外媒报道，美国共和党全国国会委员会(NRCC)在今年美国中期选举期间遭到黑客攻击。Politico 最新报道了这起攻击事件。另外，NRCC 还向负责调查了 2016 年民主党全国委员会网络攻击事件的网络安全公司 CrowdStrike 报告了这起黑客攻击事件。同样的，这家公司也没有立即作出回应。NRCC 没有就此次攻击以及为何等到选举日之后才公开此事的做法作出解释。

3、澳通过全球最严反加密法 FB 等将被迫上交隐私数据

新浪科技 2018 年 12 月 6 日消息，据彭博社报道，澳大利亚下议院通过了全球最为严苛的反加密法律，进一步推进该国为强制 Facebook(141.85, 4.43, 3.22%)等其他科技巨头协助警方调查恐怖主义和有组织犯罪解密聊天信息而制定法律。据悉，该立法还需要由议会委员会审查 12 个月。新的权力仅适用于处理极端犯罪行为。并且，针对所谓的“技术能力通知”——即强制

公司修改其服务协助警方获取数据的通知——也会受到严密监管。

4、Quora 披露巨大漏洞，1 亿用户受其影响

E 安全 12 月 5 日消息 最大的问答门户网站 Quora 表示，黑客通过访问其服务器，窃取了约一亿用户的信息，约占该网站总用户数的一半。该公司昨日披露了该入侵（事件），但称是在上周五发现的该事件。Quora 仍在调查该事件，但其称已确定黑客窃取了用户以下几类信息：账户信息（例如：姓名、电子邮件地址、加密密码、经用户授权联网导入的数据），公开内容与操作（例如：提问、回答、评论、点赞），非公开内容与操作（例如：回答请求、不赞成、直接消息）。

5、巴西 Sky Brasil 公司泄露 32.7 万用户信息

黑客视界 12 月 4 日消息 巴西最大的订阅电视服务公司 Sky Brasil 泄露了 32.7 万用户的信息，包括 28.7GB 的日志文件和 429.1GB 的 API 数据，这些数据显示姓名，家庭住址，电话号码，出生日期，客户端 IP 地址，付款方式和加密密码。虽然 Castro 发现了这一事件后通知了 Sky Brasil，公司随后也对数据库进行了密码保护。但其服务器至少从 10 月中旬就开始在 Shodan 上被编入索引，目前还不清楚数据库的访问者数量。

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：狄少嘉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158