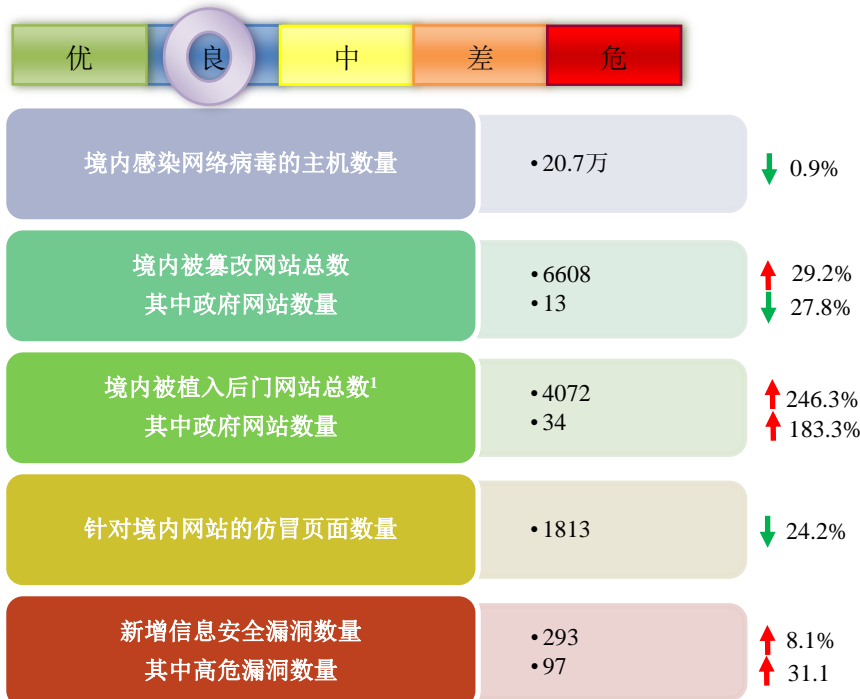


网络安全信息与动态周报

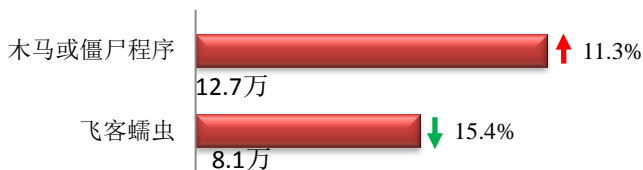
本周网络安全基本态势



▬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

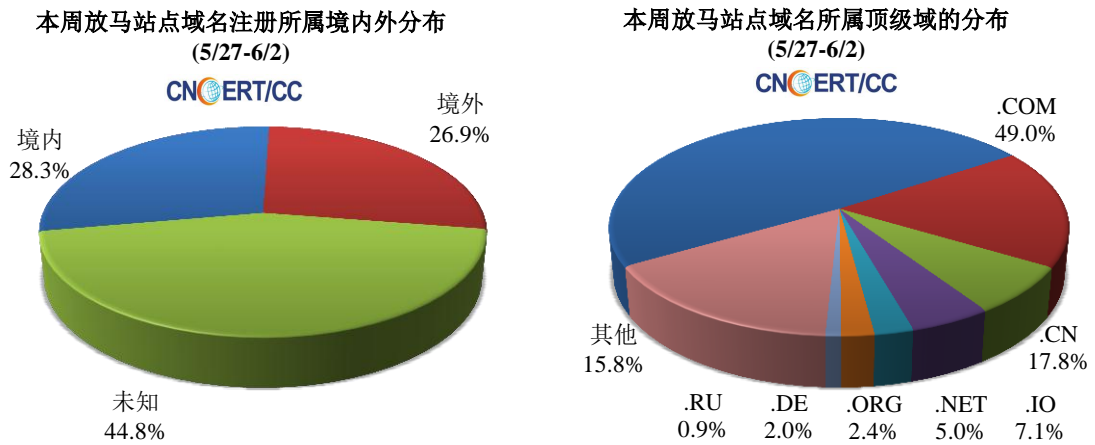
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.7 万以及境内感染飞客（conficker）蠕虫的主机约 8.1 万。



¹本期境内被植入后门总数受监测数据范围扩大影响，波动较大

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 3396 个，涉及 IP 地址 5191 个。在 3396 个域名中，有 26.9% 为境外注册，且顶级域为 .com 的约占 49.0%；在 5191 个 IP 中，有约 57.8% 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 574 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

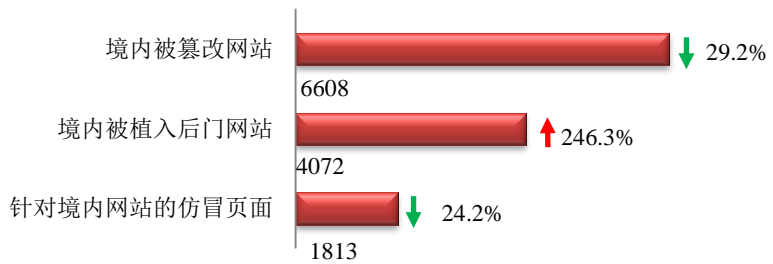
<http://www.anva.org.cn/virusAddress/listBlack>

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

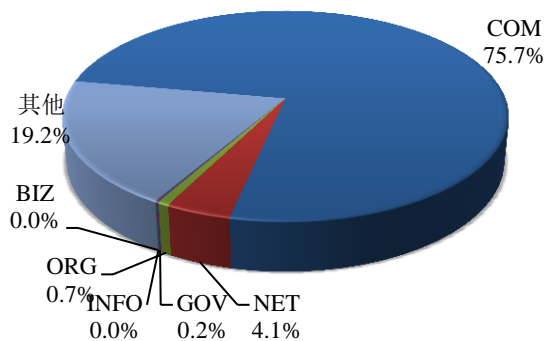
本周 CNCERT 监测发现境内被篡改网站数量 6608 个；境内被植入后门的网站数量为 4072 个；针对境内网站的仿冒页面数量 1813 个。



本周境内被篡改政府网站（GOV 类）数量为 13 个（约占境内 0.2%），较上周环比下降 27.8%；境内被植入后门的政府网站（GOV 类）数量为 34 个（约占境内 0.8%），较上周环比上升 183.3%；针对境内网站的仿冒页面涉及域名 544 个，IP 地址 295 个，平均每个 IP 地址承载了约 6 个仿冒页面。

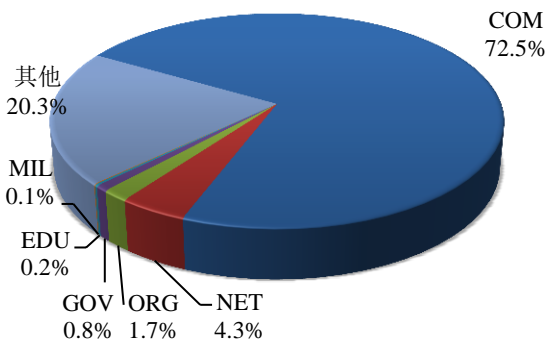
本周我国境内被篡改网站按类型分布
(5/27-6/2)

CNERT/CC



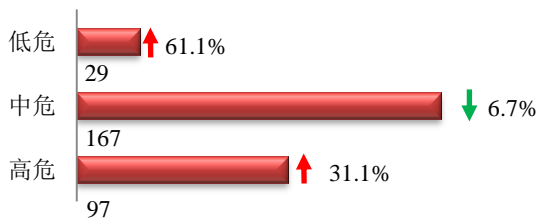
本周我国境内被植入后门网站按类型分布
(5/27-6/2)

CNERT/CC

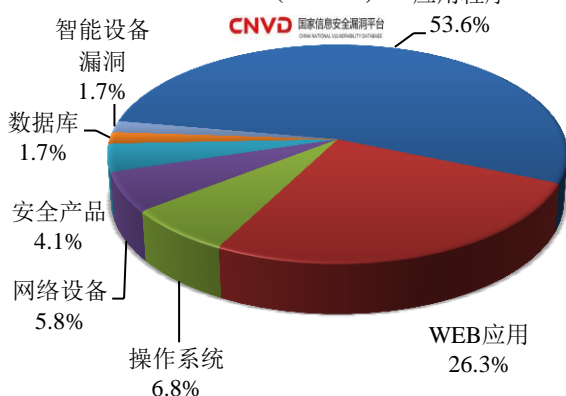


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 293 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
(5/27-6/2)



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

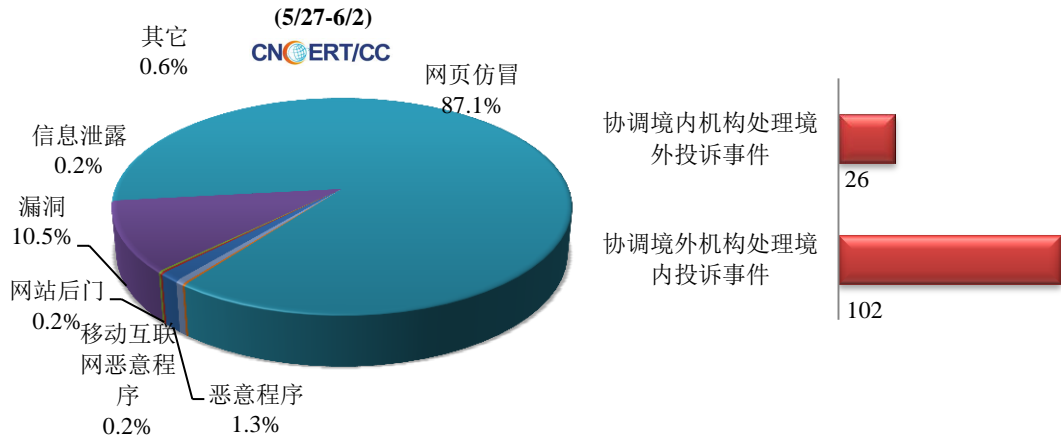
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

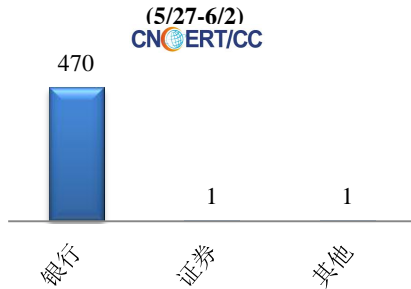
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 543 起，其中跨境网络安全事件 128 起。

本周CNCERT处理的事件数量按类型分布

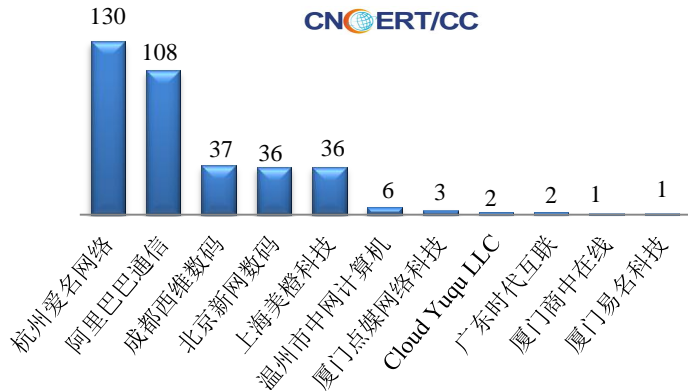


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 472 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 470 起和证券仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计



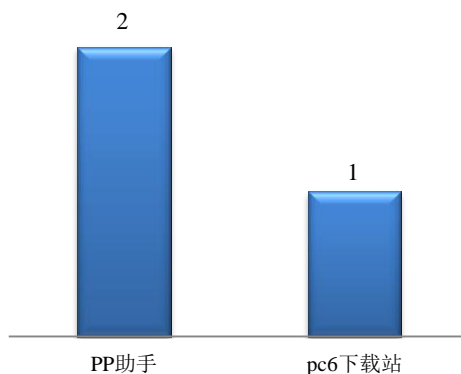
本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名(5/27-6/2)



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 (5/27-6/2)

CNCERT/CC

本周，CNCERT 协调 2 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 3 个。



业界新闻速递

1、国家互联网信息办公室关于《儿童个人信息网络保护规定（征求意见稿）》公开征求意见的通知

中国网信网 5 月 31 日消息 国家互联网信息办公室发布《儿童个人信息网络保护规定（征求意见稿）》（下称《征求意见稿》）公开向社会征求意见。《征求意见稿》规定，网络运营者收集、使用儿童个人信息的，应当征得儿童监护人的明示同意。《征求意见稿》规定，网络运营者收集、存储、使用、转移、披露儿童个人信息的，应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并设立个人信息保护专员或者指定专人负责儿童个人信息保护。网络运营者不得收集与其提供的服务无关的儿童个人信息，不得违反法律、行政法规的规定和用户协议的约定收集儿童个人信息。网络运营者收集、使用儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的明示同意。明示同意应当具体、清楚、明确，基于自愿。

2、信通院发布《欧盟 GDPR 合规指引》

中国信息通信研究院 5 月 29 日消息 据报道，欧盟《通用数据保护条例》（以下简称“GDPR”）于 2018 年 5 月 25 日全面实施，被称为“史上最严格的数据保护法”。5 月 28 日在贵阳举办的 2019 年中国国际大数据产业博览会“人工智能产业与数据跨境业务的法律监管国际论坛”上，中国信息通信研究院安全研究所联合对外经济贸易大学数字经济与法律创新研究中心、北京大学法治与发展研究院、奋迅律师事务所、科文顿 柏灵律师事务所、京东集团，共同发布《欧盟 GDPR 合规指引》，为深入理解 GDPR 提供了有益思路。指引共分四章，分别包括 GDPR 概述、合规体系、疑难点及合规建议，以及 GDPR 与我国法律的比较及冲突应对。

3、Flipboard 发安全通告：内部系统遭黑客攻击 推荐所有用户重置密码

cnBeta.COM 5 月 29 日消息 新闻聚合服务和移动新闻应用 Flipboard 发布安全通告，公司内部多个系统遭到黑客攻击，已经持续超过 9 个月时间。援引外媒 ZDNet 掌握的多封电子邮件，Flipboard 表示黑客获得了存储客户信息的服务器访问权限。在该服务器上存储了用户名、哈希值、加密密码，以及和第三方服务捆绑的 Flipboard 个人资料。

4、美国汉堡连锁品牌 Checkers 遭黑客攻击 102 家门店 POS 机被感染

cnBeta.COM 5 月 31 日消息 美国快餐连锁品牌 Checkers & Rally's 遭遇恶意程序攻击，15% 的美国门店 POS 机被感染，导致严重的数据泄露。Checkers 是美国境内最大的免下车汉堡连锁餐馆之一，总部位于佛罗里达州坦帕市，目前已经在美国 28 个州开拓业务。黑客攻击了 Checkers 的支付系统，并且在 100 多家线下门店的 POS 系统中植入了恶意软件。这些恶意软件会收集支付卡磁条上的数据，包括持卡人姓名、支付卡号、卡验证码以及到期日期等等。

5、谷歌云服务宕机 YouTube 和 Gmail 等大量服务中断

新浪科技 6 月 2 日消息 据美国财经媒体 CNBC 报道，在经历了数小时的中断之后，基于谷歌云技术的 YouTube、Gmail 和 Snapchat 等服务已恢复正常。美国当地时间周日，YouTube、Snapchat、Gmail、Nest、Discord，以及其他许多网络服务均陷入无法访问状态，包括使用谷歌技术的苹果 iMessage 和 iCloud 等服务。据悉，此次故障的原因是谷歌云计算服务出现了故障。据谷歌称，此次故障始于美国东部时间 6 月 2 日下午 3 点 25 分，主要影响美国东海岸的用户，但欧洲许多地区的 YouTube 和 Gmail 用户也表示受到了影响。

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 2017 年，CNCERT 与 72 个国家和地区的 211 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：韩志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315

