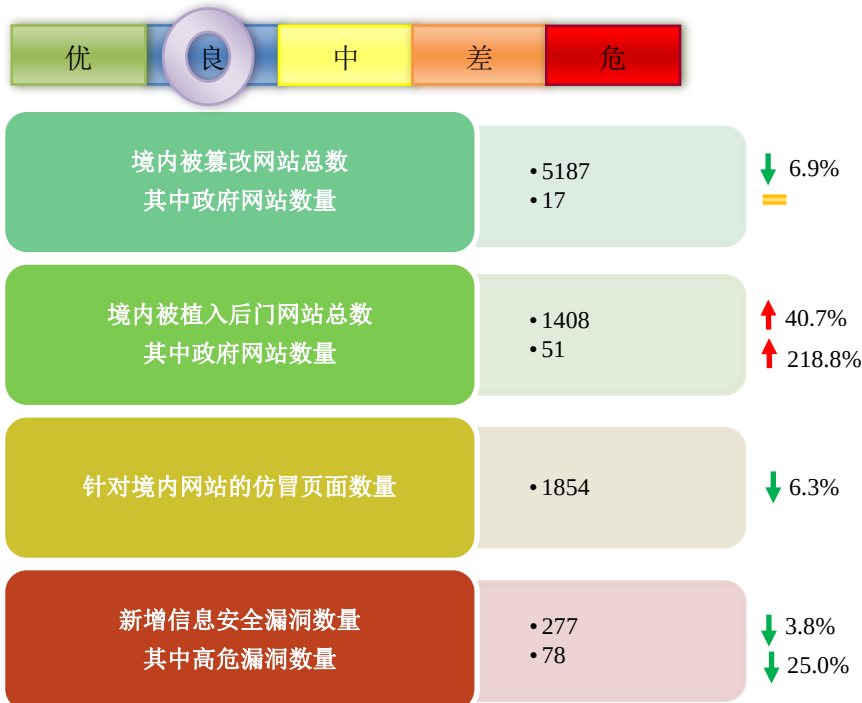


网络安全信息与动态周报

本周网络安全基本态势



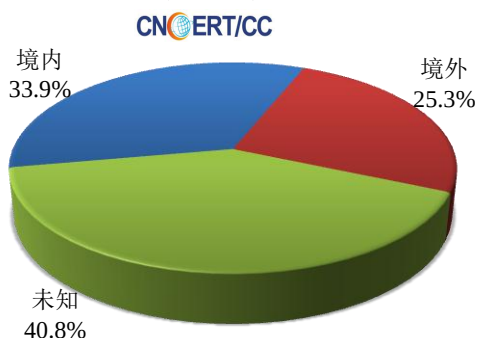
— 表示数量与上周相同

↑ 表示数量较上周环比增加

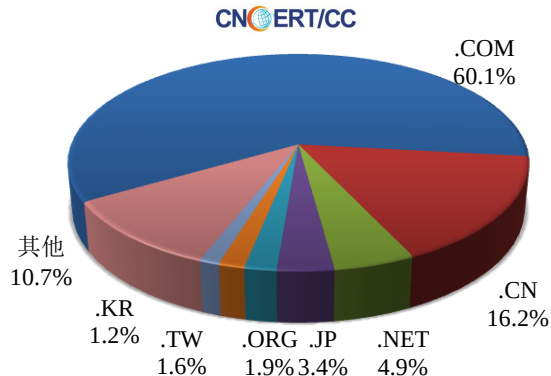
↓ 表示数量较上周环比减少

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 5470 个，涉及 IP 地址 4154 个。在 5470 个域名中，有 25.3% 为境外注册，且顶级域为 .com 的约占 60.1%；在 4154 个 IP 中，约有 55.3% 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 531 个 IP。

本周放马站点域名注册所属境内外分布
(5/6-5/12)



本周放马站点域名所属顶级域的分布
(5/6-5/12)



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。

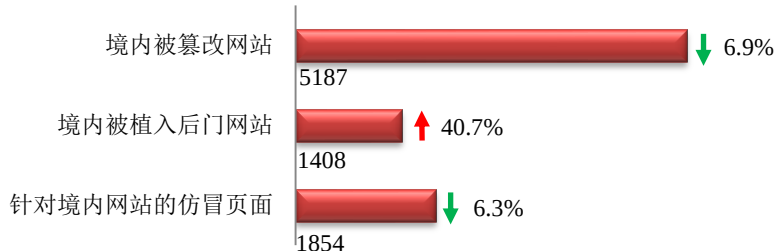
ANVA 恶意地址黑名单发布地址

<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

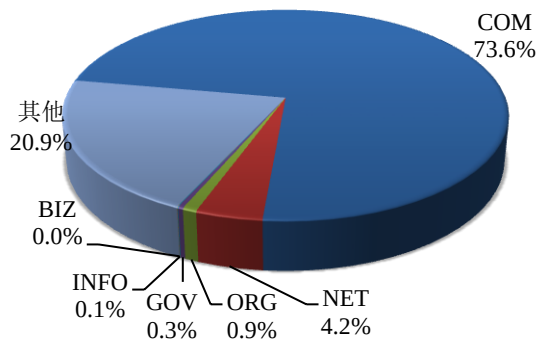
本周 CNCERT 监测发现境内被篡改网站数量 5187 个；境内被植入后门的网站数量为 1408 个；针对境内网站的仿冒页面数量 1854 个。



本周境内被篡改政府网站 (GOV 类) 数量为 17 个 (约占境内 0.3%)，较上周环比持平；境内被植入后门的政府网站 (GOV 类) 数量为 51 个 (约占境内 3.6%)，较上周环比上升 218.8%；针对境内网站的仿冒页面涉及域名 612 个，IP 地址 361 个，平均每个 IP 地址承载了约 5 个仿冒页面。

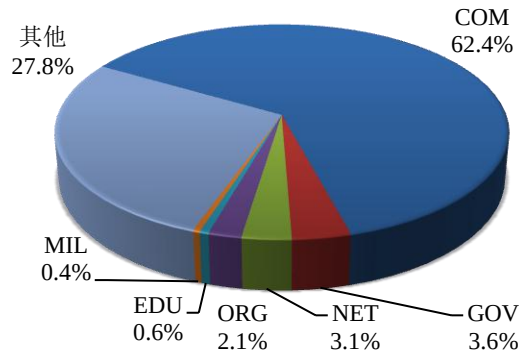
本周我国境内被篡改网站按类型分布
(5/6-5/12)

CNERT/CC



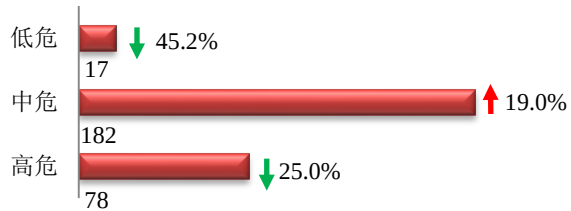
本周我国境内被植入后门网站按类型分布
(5/6-5/12)

CNERT/CC



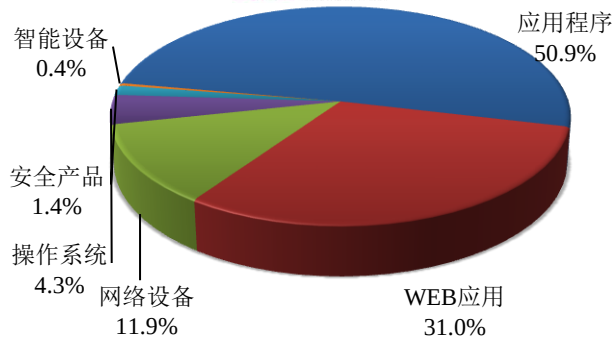
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 277 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
(5/6-5/12)

CNVD 国家信息安全漏洞平台



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 应用漏洞和网络设备漏洞。

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

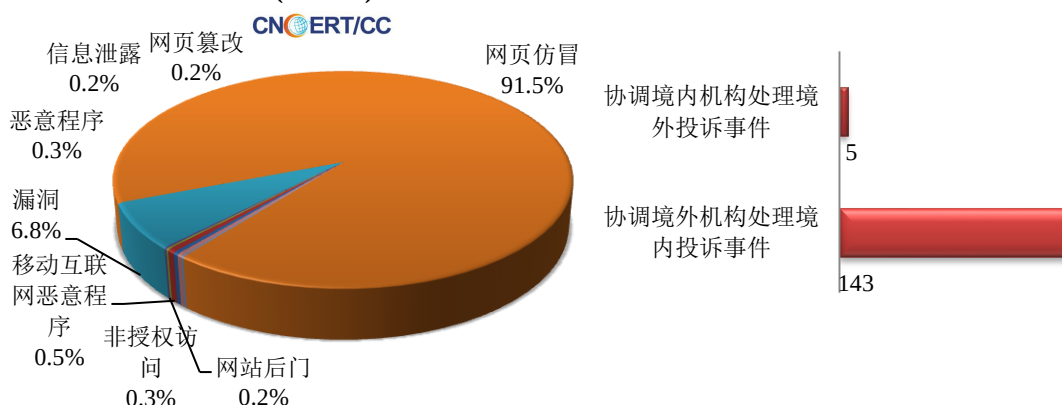
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

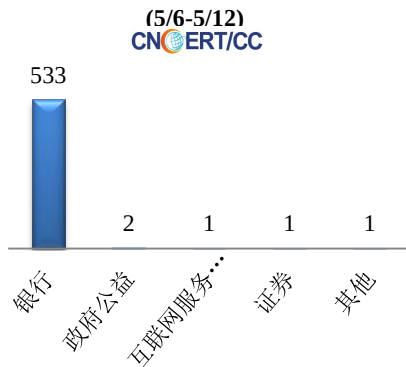
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 322 起，其中跨境网络安全事件 148 起。

本周CNCERT处理的事件数量按类型分布
(5/6-5/12)



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 538 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 533 起和政府公益事件 2 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
(5/6-5/12)



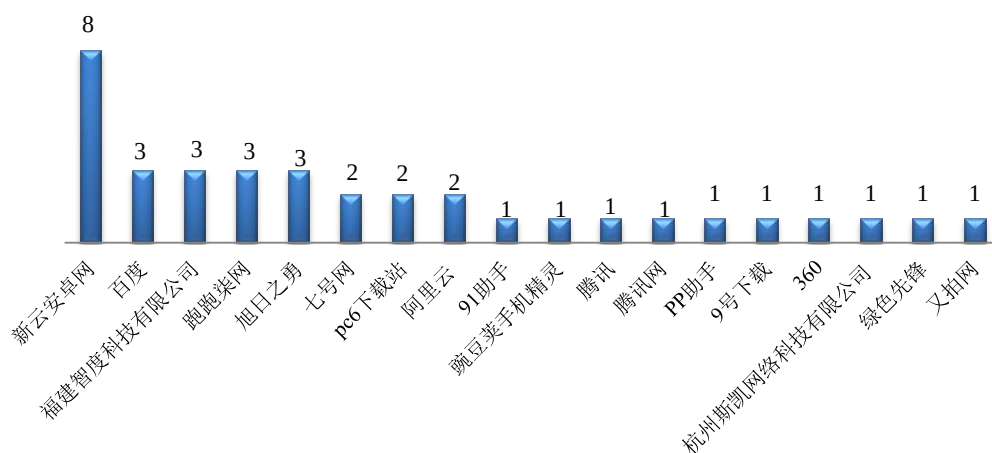
本周CNCERT协调境内域名注册机构处理网页仿冒事
件数量排名 (5/6-5/12)



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
(5/6-5/12)

CNCERT/CC

本周，CNCERT 协调 18 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 36 个。



业界新闻速递

1、《国务院 2019 年立法工作计划》公布 密码法草案、关键信息基础设施安全保护条例等在列

央视网 5 月 11 日消息 国务院办公厅发布《国务院 2019 年立法工作计划》（以下简称“计划”），计划中明确的与网络安全相关的立法项目有：密码法草案（密码局起草）、未成年人网络保护条例（网信办起草）、公共安全视频图像信息系统管理条例（公安部起草）、关键信息基础设施安全保护条例（网信办、工业和信息化部、公安部起草）等。

2、黑客组织 Fxmsp 攻击了 3 家美国反病毒公司

腾讯网 5 月 11 日消息黑客组织 Fxmsp 声称他们已经入侵了三家反病毒公司，并从这些公司的反病毒软件、人工智能和安全插件中提取了源代码。黑客组织窃取了与这些公司的软件开发相关的源代码，并向数据被盗的公司要价 30 多万美元买回这些源代码以及网络访问权。

3、著名加密货币交易所遭黑客入侵，超 7000 枚比特币被盗

E 安全 5 月 9 日消息 2019 年 5 月 9 日,据外媒报道,全球五大加密货币交易所之一 Binance（币安）遭黑客攻击，7000 多枚比特币被盗。Binance 5 月 7 日宣布网站出现安全漏洞，黑客使用网络钓鱼、病毒等攻击来获取 API 密钥、2FA 码以访问用户帐户，窃取了逾 7000 枚比特币，价值近 4100 万美元。黑客在 Binance 的热钱包中进行了 7074 比特币的巨额交易。

4、黑客入侵多个亚马逊供应商账户窃取资金

E 安全 5 月 10 日消息 电子商务和科技公司亚马逊遭遇了网络攻击，黑客侵入了 100 多家供应商的账户，并通过欺诈手段窃取了账户资金。据报道，攻击发生在 2018 年 5 月至 10 月之间，黑客对 Prepay 和 Barclay 等金融机构的亚马逊供应商账户实施攻击。黑客将账户信息修改后，资金会进入到黑客控制的银行账户。亚马逊尚不清楚黑客成功获取多少资金，但据信，一切都始于网络钓鱼，黑客欺骗亚马逊供应商提供登录凭证和财务信息等详细账户信息。

5、涉及 2.75 亿条印度公民信息的 MongoDB 数据库被曝光和公开索引

cnBeta.COM 5 月 10 日消息 外媒 Security Discovery 报道，他们发现了一个未经保护和公开索引的 MongoDB 数据库，其中包括了涉及印度公民的个人身份信息的 275,265,298 条记录。这些信息中包括姓名、电子邮件地址、性别、教育水平和专业领域、专业技能和职称、手机号码、就业经历和当前雇主、出生日期以及当前的薪资水平。在这个曝光的数据库中并没有泄露源或者从属关系的标签。这个 MongoDB 数据库本身是托管在亚马逊 AWS 基础架构上的，反向 DNS 也没有显示任何结果。数据库中的结构和名称暗示这个曝光的数据库仅仅只是黑客大规模手机数据中的一部分。根据 Shodan 的历史数据，MongoDB 于 2019 年 4 月 23 日首次被索引。

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：贾子骁

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158