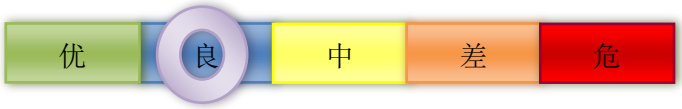
国家互联网应急中心

2019 年第 16 期
4 月 15 日-4 月 21 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

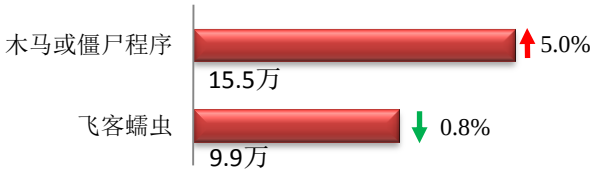


境内感染网络病毒的主机数量	•25.4万	↑2.6%
境内被篡改网站总数 其中政府网站数量	•1054 •8	↑105.9% =
境内被植入后门网站总数 其中政府网站数量	•1321 •35	↑25.0% ↑600.0%
针对境内网站的仿冒页面数量	•2641	↓6.8%
新增信息安全漏洞数量 其中高危漏洞数量	•230 •96	↑70.4% ↑104.3%

=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

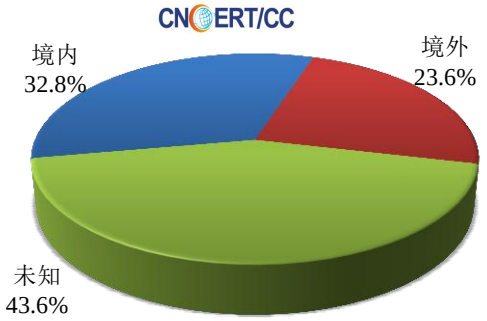
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.5 万以及境内感染飞客（conficker）蠕虫的主机约 9.9 万。

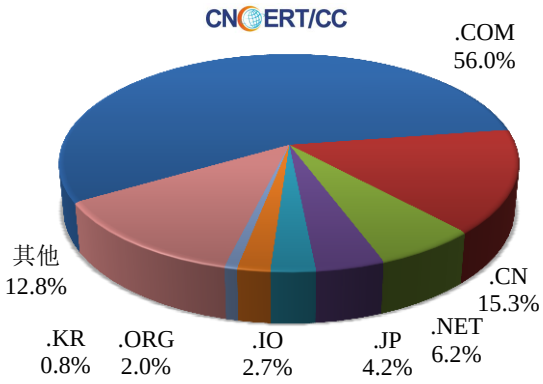


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3885 个，涉及 IP 地址 3672 个。在 3885 个域名中，有 23.6%为境外注册，且顶级域为.com 的约占 56.0%；在 3672 个 IP 中，有约 40.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 405 个 IP。

本周放马站点域名注册所属境内外分布
(4/15-4/21)



本周放马站点域名所属顶级域的分布
(4/15-4/21)



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。

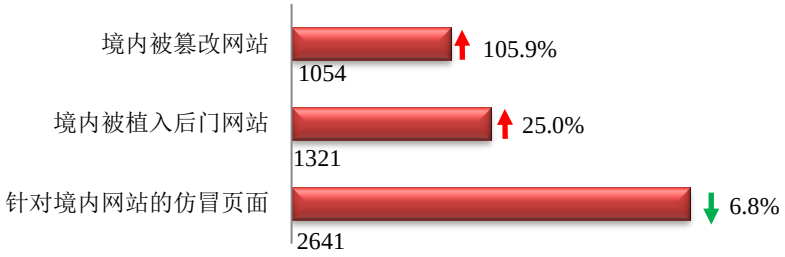
ANVA恶意地址黑名单发布地址

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。

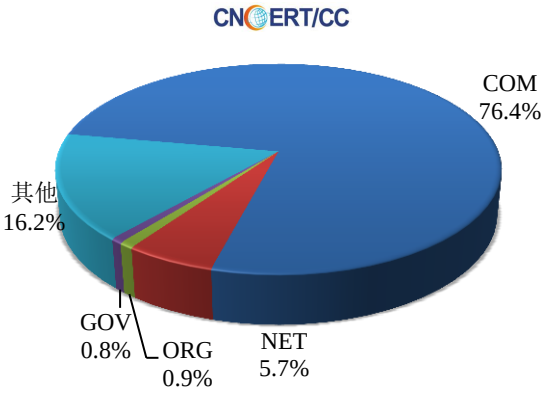
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1054 个；境内被植入后门的网站数量为 1321 个；针对境内网站的仿冒页面数量 2641 个。

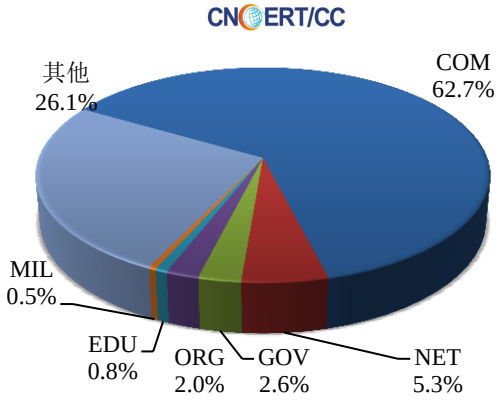


本周境内被篡改政府网站（GOV 类）数量为 8 个（约占境内 0.8%），较上周环比持平；境内被植入后门的政府网站（GOV 类）数量为 35 个（约占境内 2.6%），较上周环比上升了 600.0%；针对境内网站的仿冒页面涉及域名 803 个，IP 地址 434 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/15-4/21)

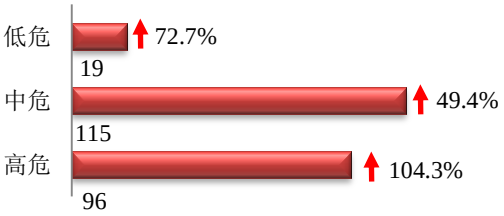


本周我国境内被植入后门网站按类型分布
(4/15-4/21)

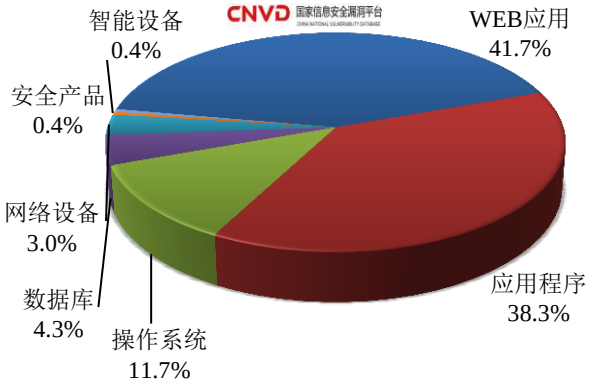


本周重要漏洞情况

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
(4/15-4/21)



本周 CNVD 发布的网络安全漏洞中，WEB 应用漏洞占比最高，其次是应用程序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

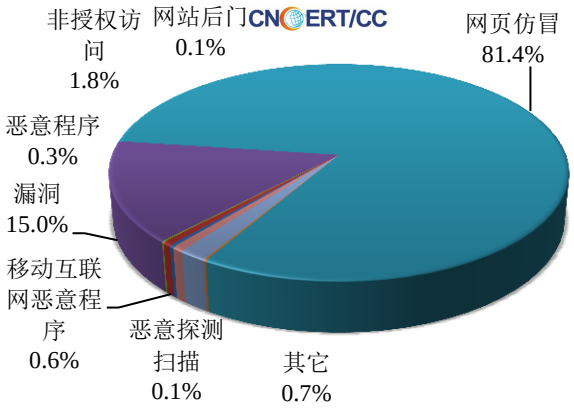
http://www.cnvd.org.cn/webinfo/list?type=4

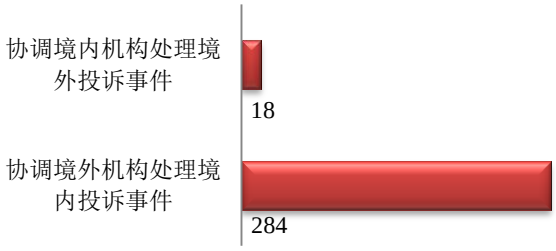
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 681 起，其中跨境网络安全事件 302 起。

本周CNCERT处理的事件数量按类型分布 (4/15-4/21)

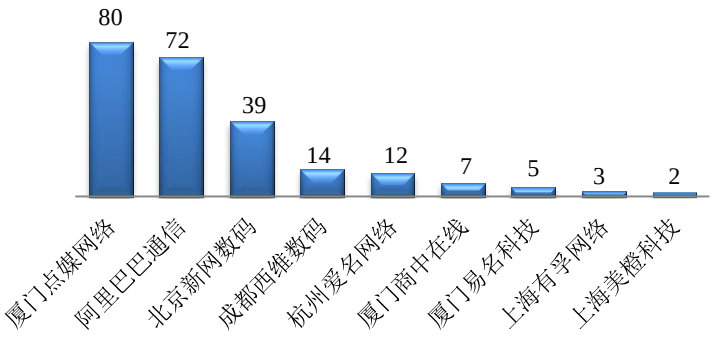




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 554 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 554 起。

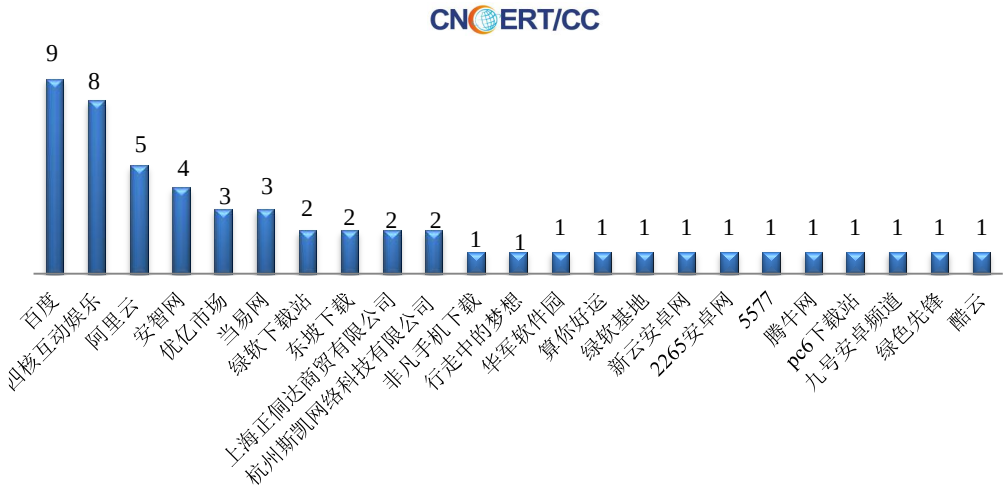
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (4/15-4/21)

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 (4/15-4/21)



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
(4/15-4/21)

本周，CNCERT 协调 23 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 53 个。



业界新闻速递

1、 四部门抓紧推进 App 违法收集使用个人信息专项治理

新华社消息，中央网信办、工信部、公安部、市场监管总局指导成立 App 违法违规收集使用个人信息专项治理工作组以来，组织开展的 App 收集使用个人信息评估工作取得阶段性进展。记者从工作组负责人处获悉，截至 4 月 16 日，举报信息超过 3480 条，涉及 1300 余款 App。对于 30 款用户量大、问题严重的 App，工作组已向其运营者发送了整改通知。

2、民法典人格权编草案：加大未成年人信息保护

新浪司法 4 月 20 日消息 民法典人格权编草案已提请十三届全国人大常委会第十次会议进行二次审议。草案二审稿首次对人体基因、人体胚胎等有关的医学和科学研究进行了规范，并围绕个人信息保护等问题增加规定。二审稿作出规定，对收集使用未成年人等无民事行为能力人或者限制民事行为能力人的个人信息的，增加规定应当征得其监护人同意，但是法律、行政法规另有规定的除外。针对公务人员在履职过程中知悉的个人信息的保密义务，也增加了规定：国家机关及其工作人员对于履行职责过程中知悉的自然人隐私、个人信息，应当予以保密，不得泄露或者非法向他人提供

3、欧盟通过提高在线平台公平性和透明度的新法规

安全内参 4 月 17 日消息 欧洲议会批准了《关于提高在线平台交易的公平性和透明度规则》，

旨在为企业和交易者在使用在线平台时建立一个公平，可信和创新驱动的环境。该法规将来还须得到欧盟理事会的正式批准，一旦获得批准，将在官方公报上公布 12 个月后生效。该法规采取共同监管方式，要求在线平台中介机构和在线搜索引擎遵守法律义务，并鼓励其采取自愿的补充措施。

4、Facebook 承认员工可获取数百万 Instagram 用户的明文密码

cnBeta.COM4 月 19 日消息 Facebook 公司员工可在一个内部数据库中看到数以百万计的 Instagram 用户密码，这些密码以可搜索的格式存储在数据库中。公司员工可以看到数亿 Facebook Lite 用户、数千万 Facebook 用户、以及数万 Instagram 用户的密码。公司在进行内部调查后确定，这些密码并未“被滥用或不正当地访问”。数千名 Facebook 员工可看到这些密码，此事在今年 3 月被首次曝光以来，Facebook 一直都没有提供调查的最新信息。

5、阿桑奇被捕后 厄瓜多尔政府和机构网站遭到 4000 万次攻击

cnBeta.COM4 月 18 日,据外媒报道,由于厄瓜多尔现任总统莫雷诺撤回了外交庇护，维基解密创始人朱利安·阿桑奇（Julian Assange）藏身厄瓜多尔驻英大使馆将近 7 年之后被抓。厄瓜多尔资讯与通讯科技部副部长表示在阿桑奇遭到逮捕之后，已经受到了大规模针对该国的网络攻击。在撤销对维基解密（WikiLeaks）创办人阿桑奇的政治庇护以来，该国的政府和机构网站遭到了 4000 万次的网络攻击。这些攻击始于 4 月 11 日，不仅来自厄瓜多尔国内，而且还来自于美国、巴西、荷兰、德国、罗马尼亚、法国、奥地利及英国地区。

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：王适文

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158