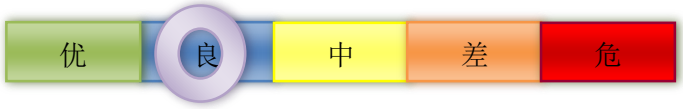
国家互联网应急中心

网络安全信息与动态周报

2020 年第 1 期
12 月 30 日-1 月 5 日

CNCERT/CC

本周网络安全基本态势

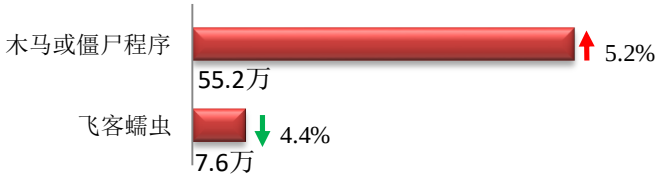


境内感染网络病毒的主机数量	•62.8万	↑ 3.9%
境内被篡改网站总数 其中政府网站数量	•9829 •34	↑ 53.1% ↑ 47.8%
境内被植入后门网站总数 其中政府网站数量	•2796 •17	↑ 0.8% ↓ 22.7%
针对境内网站的仿冒页面数量	•1620	↑ 28.0%
新增信息安全漏洞数量 其中高危漏洞数量	•215 •85	↑ 5.9% ↑ 26.9%

= 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

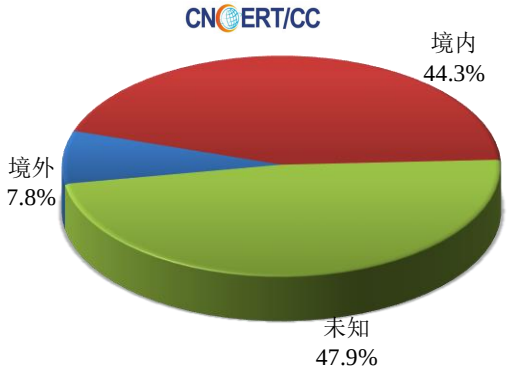
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 62.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 55.2 万以及境内感染飞客（conficker）蠕虫的主机约 7.6 万。

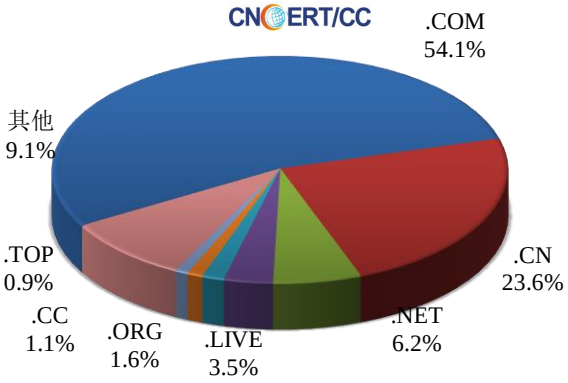


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1095 个，涉及 IP 地址 2417 个。在 1095 个域名中，有 7.8%为境外注册，且顶级域为.com 的约占 54.1%；在 2417 个 IP 中，有约 25.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 205 个 IP。

本周放马站点域名注册所属境内外分布
(12/30-1/5)



本周放马站点域名所属顶级域的分布
(12/30-1/5)



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。

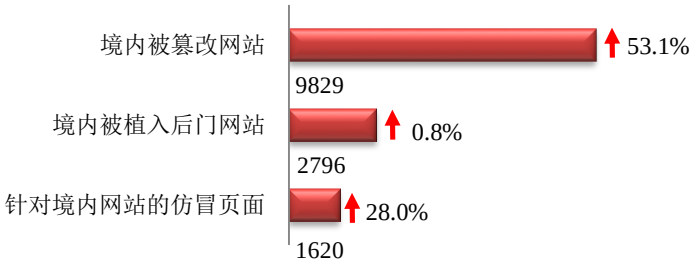
ANVA恶意地址黑名单发布地址

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。

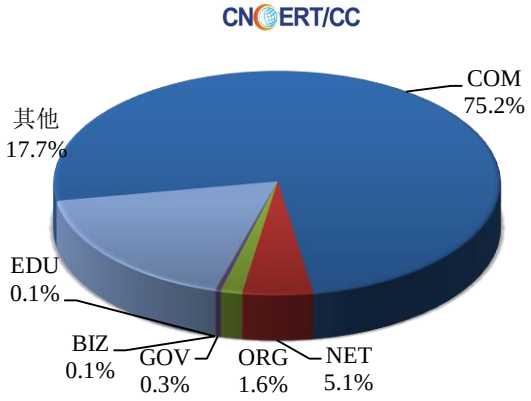
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 9829 个；被植入后门的网站数量为 2796 个；针对境内网站的仿冒页面数量 1620 个。

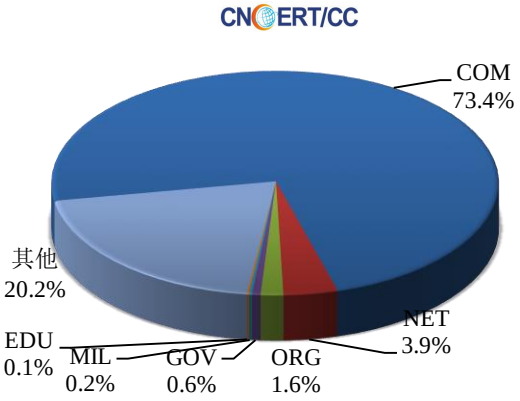


本周境内被篡改政府网站（GOV 类）数量为 34 个（约占境内 0.3%），较上周上涨了 47.8%；境内被植入后门的政府网站（GOV 类）数量为 17 个（约占境内 0.6%），较上周下降了 22.7%。

本周我国境内篡改网站按类型分布
(12/30-1/5)

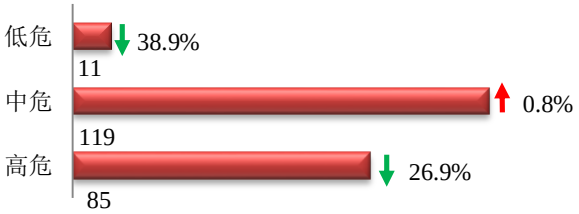


本周我国境内被植入后门网站按类型分布
(12/30-1/5)

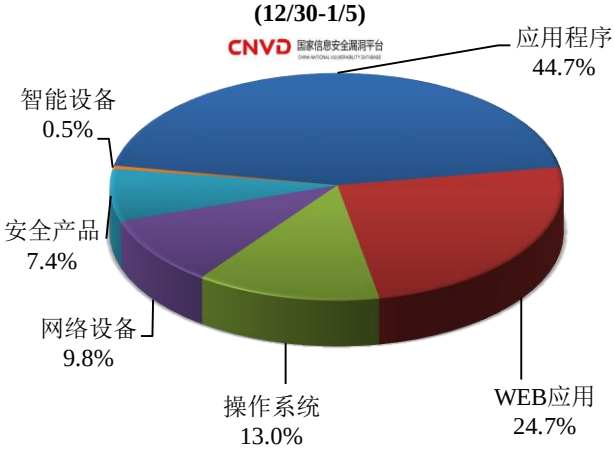


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 215 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
(12/30-1/5)



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

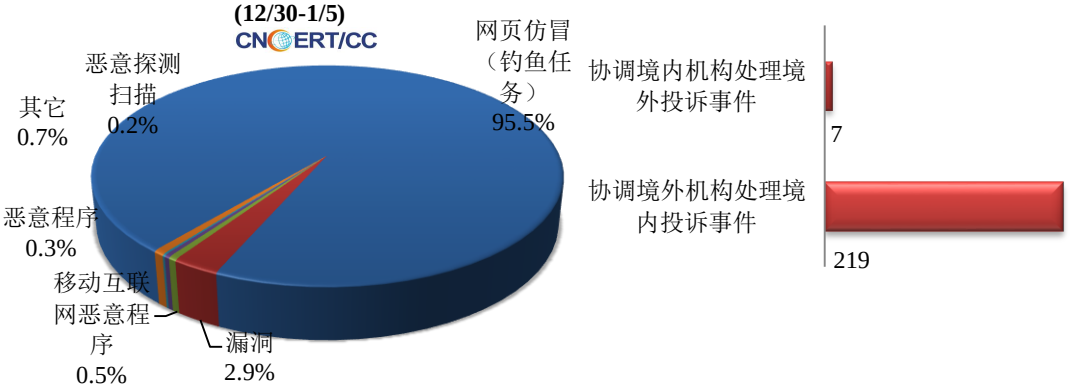
http://www.cnvd.org.cn/webinfo/list?type=4

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

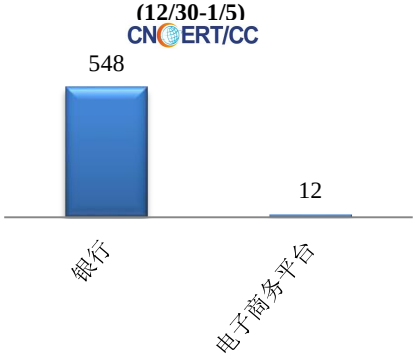
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 594 起，其中跨境网络安全事件 226 起。

本周CNCERT处理的事件数量按类型分布 (12/30-1/5)

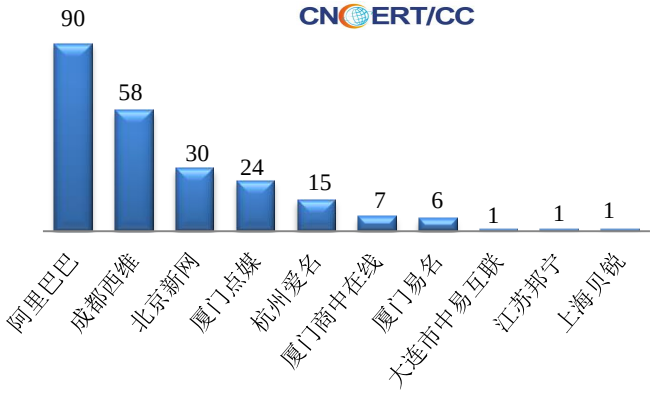


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 567 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 548 起和其他事件 12 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (12/30-1/5)

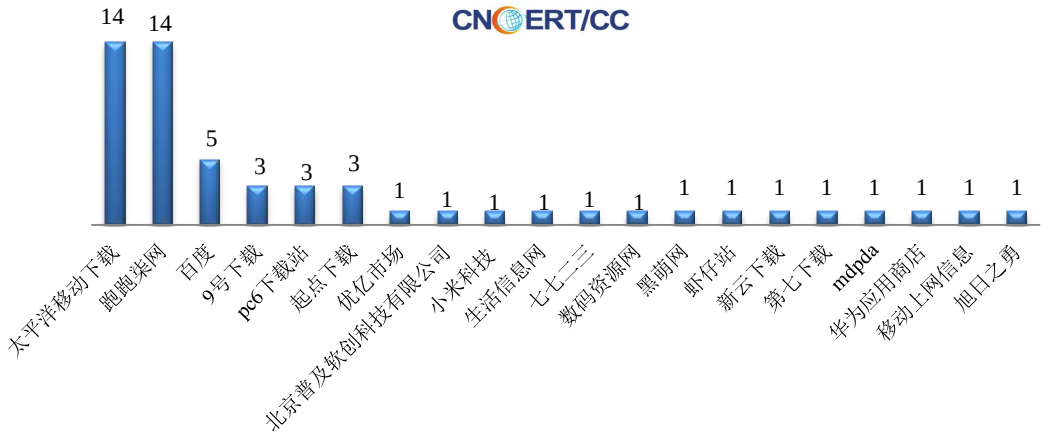


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (12/30-1/5)



本周，CNCERT 协调 20 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 56 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
(12/30-1/5)



业界新闻速递

1、 国家网信办等四部门联合印发《App 违法违规收集使用个人信息行为认定方法》

12 月 30 日，国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅联合发布<关于印发《APP 违法违规手机使用个人信息行为认定方法》的通知>（国信办秘字〔2019〕191 号）。通知指出，根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为认定 App 违法违规收集使用个人信息行为提供参考，落实《网络安全法》等法律法规，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定了《App 违法违规收集使用个人信息行为认定方法》（以下简称“认定方法”）。认定方法明确了六大类的 App 违法违规收集个人信息行为，并对每类行为进行了详细说明，包括未公开收集使用规则，未明示收集使用个人信息的目的、方式和范围，未经用户同意收集使用个人信息，违反必要原则收集与其提供的服务无关的个人信息，未经同意向他人提供个人信息，未按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息。

2、 工信部发布《关于下架第一批侵害用户权益 APP 名单的通报》

1 月 3 日，工信部发布“《关于下架第一批侵害用户权益 App 名单的通报》关于下架第一批侵害用户权益 App 名单的通报”，包括人人视频 4.3.3、4.3.4 版本、，春雨计步器

2.5.4 版本和，微唱-原创音乐 1.1.0 版本被下架。根据工信部官网消息，2019 年 12 月 19 日，工信部向社会通报了 41 家存在侵害用户权益行为 App 企业的名单。截至目前，经第三方检测机构核查复检，尚有 3 款 App 未按要求完成整改。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等法律和规范性文件要求，工信部组织对上述 App 进行下架。相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。已经完成整改的 App，应于 2020 年 1 月 6 日 12 点前，在相关渠道更新整改后的 App 版本。

3、 Facebook 因泄露用户信息被巴西处以高额罚款

12 月 30 日，据央视报道，巴西司法部宣布对美国 Facebook 处以 Facebook 因不正确的分享用户数据被巴西司法部罚款 160 660 万雷亚尔（约合人民币 1150 万元）的罚款，原因是该公司不当共享用户数据。万美元。巴西司法部消费者保护部门称，它发现 443,000 名 Facebook 用户的数据被提供给了 thisisyourdigitallife 应用的开发商，分享的意图是“可疑的”。Facebook 表示考虑上诉，称它已经做出了改变限制应用开发商能访问的信息。巴西政府称，它是在 2018 年的 Cambridge Analytica 丑闻之后展开调查的。巴西司法部发表声明称，自去年脸书公司陷入数据泄露丑闻后，巴西作为脸书在全球的第三大市场也随即就此事件展开调查。调查后发现，脸书允许应用开发者在用户不知情的情况下，访问并处理脸书上的用户个人信息。这是巴西政府今年来首次对脸书处以罚款。

4、 英国外汇兑换公司 Travelex 因遭到恶意软件攻击暂停服务

1 月 3 日，据外媒 Techcrunch 报道，英国外汇兑换公司 Travelex 证实在 12 月 31 日遭受恶意软件攻击，使其网站和在线服务系统都受到了影响。据悉，这家总部位于伦敦的公司在全球经营着 1500 多家门店。此次攻击使 Travelex 所服务的相关企业也受到了严重影响，其中乐购银行（Tesco Bank）的网上在线服务目前正处于脱机状态，特易购银行也表示其网络中断与 Travelex 的恶意软件攻击有关。攻击事件发生后，公司的某些服务已经暂停，但是目前为止没有迹象表明有数据遭到破坏。

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：胡俊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315