国家互联网应急中心

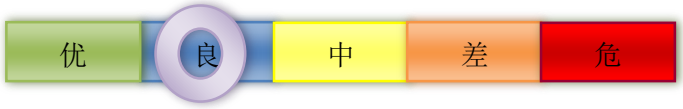
网络安全信息与动态周报

2020 年第 3 期

1 月 13 日-1 月 19 日

CNCERT/CC

本周网络安全基本态势

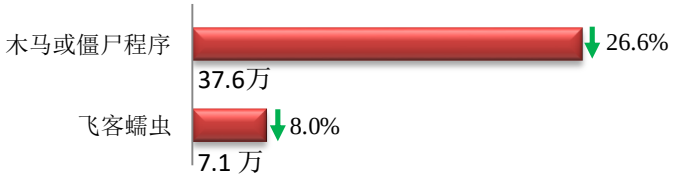


境内感染网络病毒的主机数量	•44.7万	↓24.2%
境内被篡改网站总数 其中政府网站数量	•8128 •30	↓7.4% ↓6.3%
境内被植入后门网站总数 其中政府网站数量	•2378 •11	↓14.4% ↓38.9%
针对境内网站的仿冒页面数量	•1236	↓16.4%
新增信息安全漏洞数量 其中高危漏洞数量	•354 •160	↑20.0% ↑20.3%

= 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

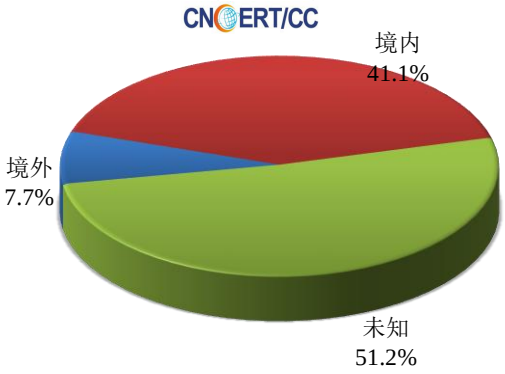
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 44.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 37.6 万以及境内感染飞客（conficker）蠕虫的主机约 7.1 万。

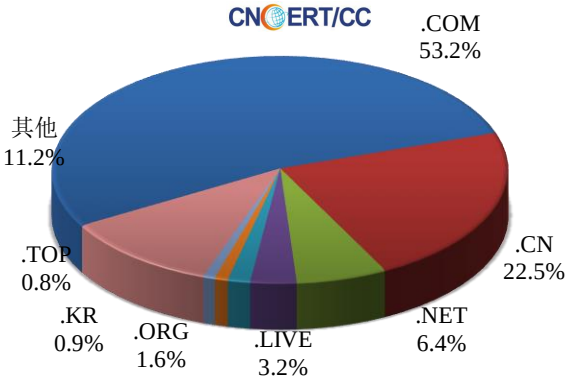


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1078 个，涉及 IP 地址 2589 个。在 1078 个域名中，有 7.7%为境外注册，且顶级域为.com 的约占 53.2%；在 2589 个 IP 中，有约 22.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 282 个 IP。

本周放马站点域名注册所属境内外分布
(1/13-1/19)



本周放马站点域名所属顶级域的分布
(1/13-1/19)



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。

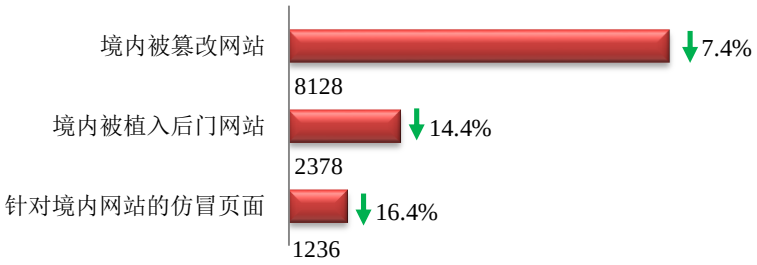
ANVA恶意地址黑名单发布地址

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。

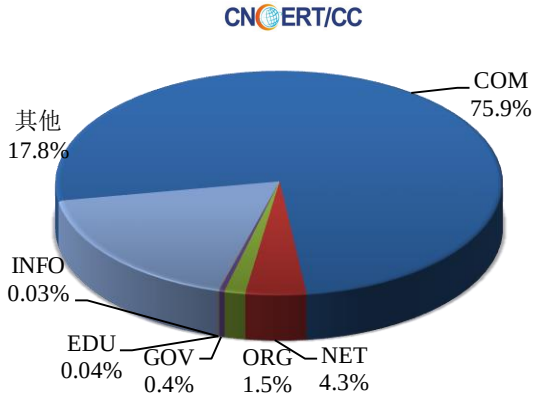
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 8128 个；被植入后门的网站数量为 2378 个；针对境内网站的仿冒页面数量 1236 个。

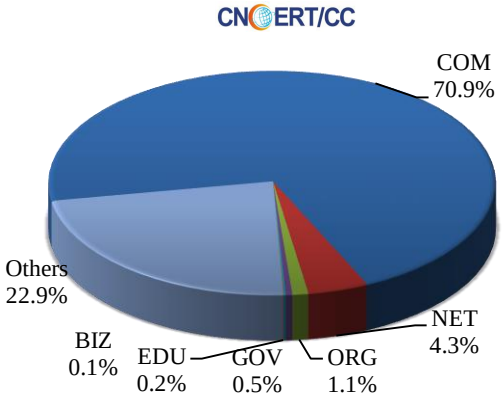


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 0.4%），较上周下降了 6.3%；境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 0.5%），较上周下降了 38.9%。

本周我国境内篡改网站按类型分布
(1/13-1/19)

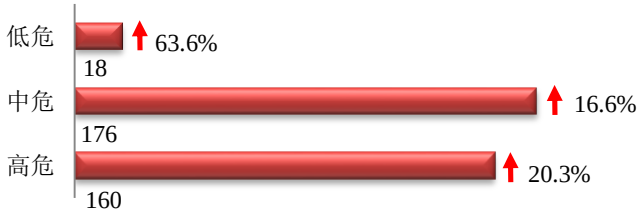


本周我国境内被植入后门网站按类型分布
(1/13-1/19)

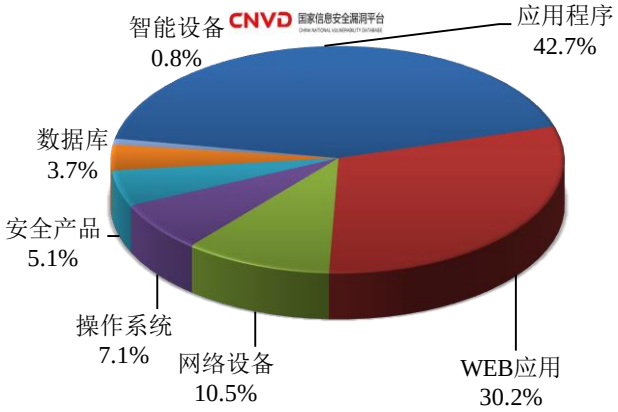


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 354 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
(1/13-1/19)



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 应用和网络设备。

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

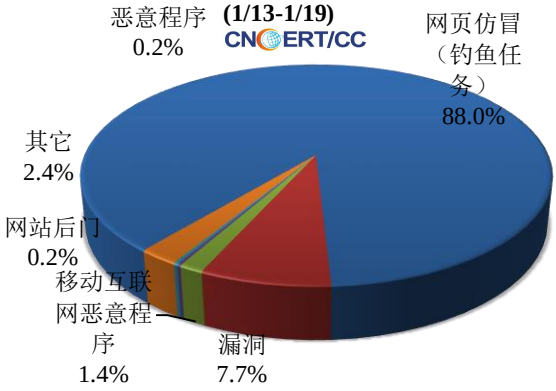
http://www.cnvd.org.cn/webinfo/list?type=4

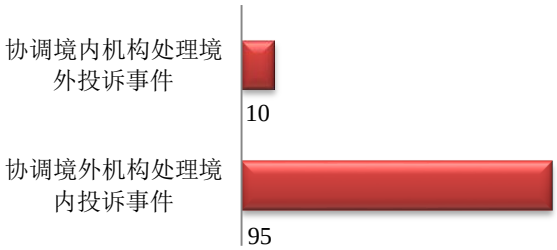
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 417 起，其中跨境网络安全事件 105 起。

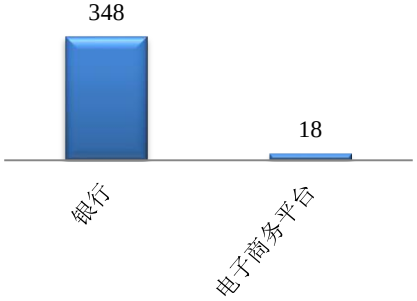
本周CNCERT处理的事件数量按类型分布 (1/13-1/19)



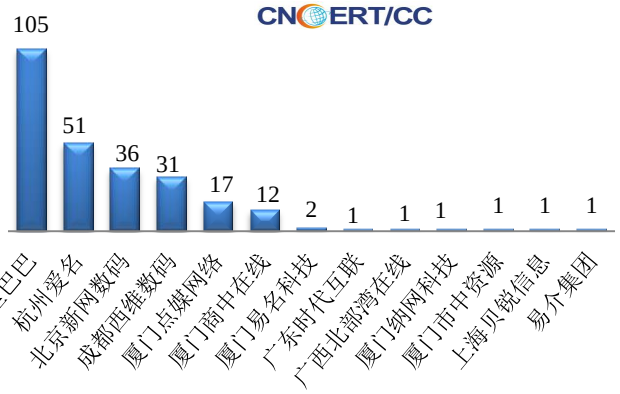


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 366 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 348 起和电子商务平台仿冒事件 18 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (1/13-1/19)

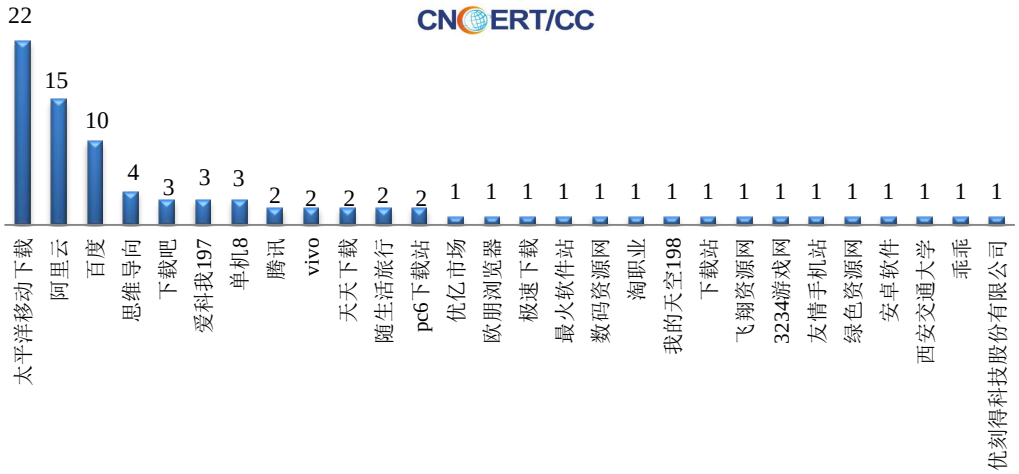


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/13-1/19)



本周，CNCERT 协调 28 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 86 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
(1/13-1/19)



业界新闻速递

1、 中央政法工作会议强调：2020 年防控新型网络安全风险将成为重中之重

1 月 17 日至 18 日，中央政法工作会议在京召开。会上强调，2020 年要把防控新型网络安全风险摆在突出位置来抓，提升网络社会综合治理能力，不断健全网络社会综合防控体系。一是构筑打击遏制网络犯罪的“新高地”。要抓住群众反映强烈的网络贩枪、网络黄赌毒、网络传销、电信网络诈骗、网络套路贷等新兴网络犯罪，完善线索快速落查、跨区域协作和跨境执法司法合作机制，深化打击整治行动，坚决打掉网络黑灰产业链，遏制网络犯罪高发势头。二是构筑大数据安全的“防护罩”。要把大数据安全作为贯彻总体国家安全观的基础性工程，依法严厉打击侵犯公民隐私、损坏数据安全、窃取数据秘密等违法犯罪活动。三是构筑新业态风险的“隔离带”。要坚持鼓励创新与确保安全相统一，对新技术、新产业、新业态、新模式，既留足发展空间又坚守安全底线。

2、 六家银行 App 遭点名 监管开出罕见数据治理罚单

1 月 13 日，国家计算机病毒应急处理中心在“净网 2020”专项行动中通过互联网监测发现，多款违法、违规有害移动应用存在隐私不合规行为，违反《网络安全法》相关规定，涉嫌超范围采集个人隐私信息。25 款应用被点名，其中 22 款“未向用户明示申请的全部隐私权限，涉嫌隐私不合规”。在金融领域有 6 款应用被点名，民生银行、兴

业银行两家股份制银行，以及内蒙古三家银行和海峡银行。在被点名后，兴业银行、内蒙古银行和鄂尔多斯银行于 1 月 13 日当日立刻更新其用户隐私政策。民生银行也于翌日更新其隐私政策。

3、 美国国家安全局发现 Win10 漏洞 影响全球数十亿用户

1 月 17 日，据外媒报道，美国国家安全局（NSA）发现 Windows 10 中存在一个严重漏洞 CVE-2020-0601，该漏洞可能会使用户遭受监视或严重数据泄露。该漏洞是在一个名为 crypt32.dll 的 Windows 组件中发现的，该组件主要用于处理“证书和加密消息传递功能”，可能会影响 Windows 台式机和服务器上的身份验证、Microsoft 的 Internet Explorer 和 Edge 浏览器上的敏感数据以及许多第三方应用程序。黑客还可以使用其进行中间人攻击以解密受害者的通信、伪造恶意代码签名。对此，微软发布了一月份安全公告，警告数十亿用户有 49 个漏洞需要更新，并发布了补丁程序。

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：吕利锋

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315