国家互联网应急中心

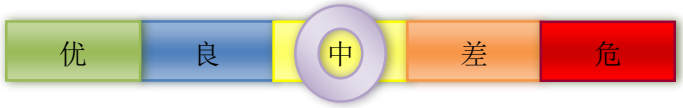
网络安全信息与动态周报

2020 年第 19 期

5 月 4 日-5 月 10 日

CNCERT/CC

本周网络安全基本态势

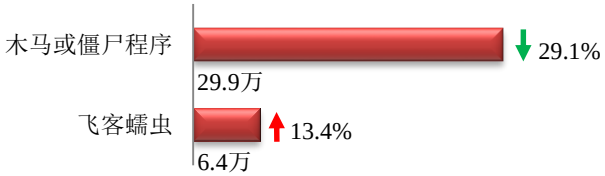


境内感染网络病毒的主机数量	•36.3万	↓ 24.0%
境内被篡改网站总数 其中政府网站数量	•7363 •31	↑ 1.3% ↓ 16.2%
境内被植入后门网站总数 其中政府网站数量	•1794 •6	↓ 2.8% ↑ 50.0%
针对境内网站的仿冒页面数量	•629	↑ 126.3%
新增信息安全漏洞数量 其中高危漏洞数量	•715 •331	↑ 91.2% ↑ 106.9%

= 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

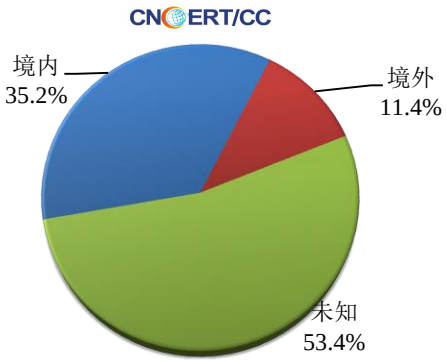
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 36.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 29.9 万以及境内感染飞客（conficker）蠕虫的主机约 6.4 万。

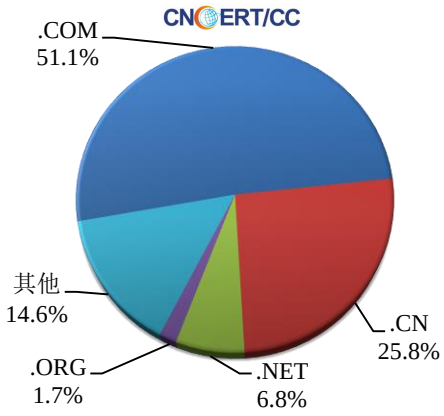


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1149 个，涉及 IP 地址 4646 个。在 1149 个域名中，有 11.4%为境外注册，且顶级域为.com 的约占 51.1%；在 4646 个 IP 中，有约 48.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 402 个 IP。

本周放马站点域名注册所属境内外分布
(5/4-5/10)



本周放马站点域名所属顶级域的分布
(5/4-5/10)



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。

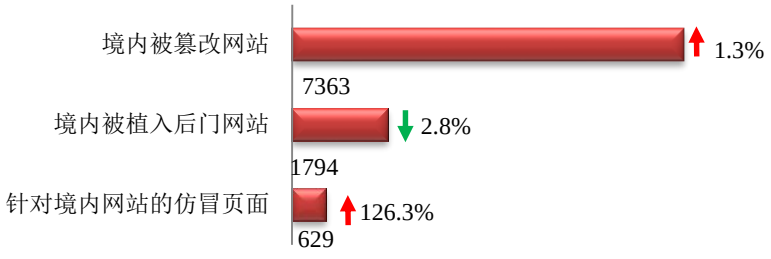
ANVA恶意地址黑名单发布地址

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。

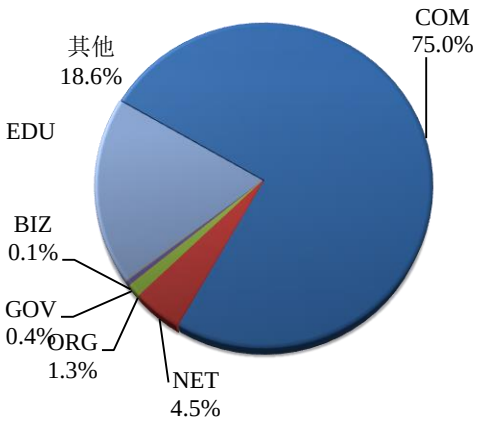
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7363 个；被植入后门的网站数量为 1794 个；针对境内网站的仿冒页面数量 629 个。

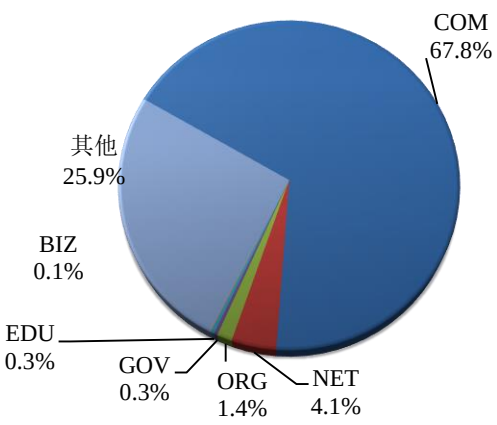


本周境内被篡改政府网站（GOV 类）数量为 31 个（约占境内 0.4%），较上周下降了 16.2%；境内被植入后门的政府网站（GOV 类）数量为 6 个（约占境内 0.3%），较上周上涨了 50.0%。

本周我国境内篡改网站按类型分布
(5/4-5/10)

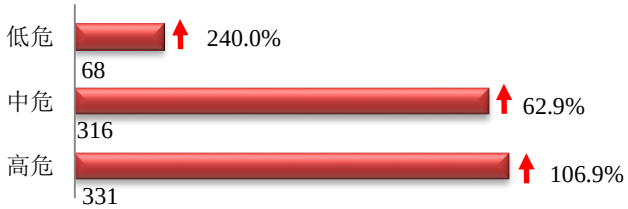


本周我国境内被植入后门网站按类型分类
(5/4-5/10)

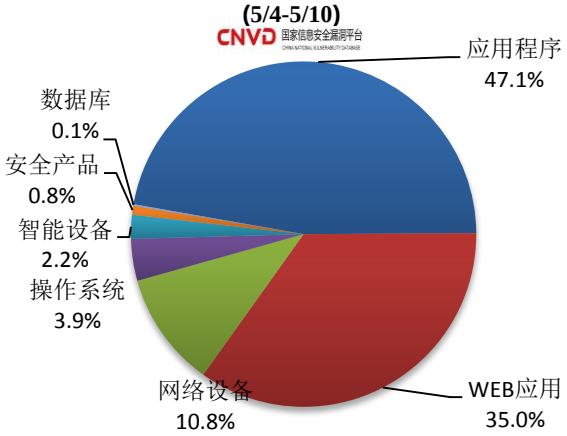


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 715 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分布
(5/4-5/10)



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

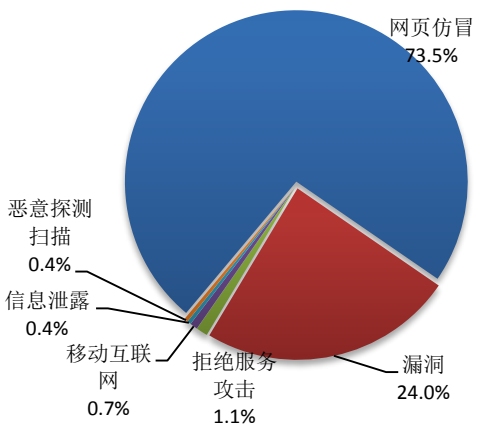
http://www.cnvd.org.cn/webinfo/list?type=4

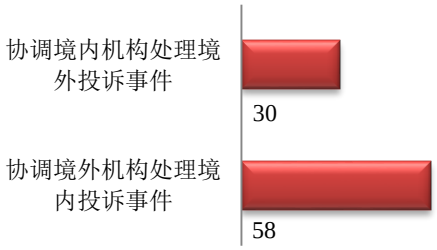
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 279 起，其中跨境网络安全事件 88 起。

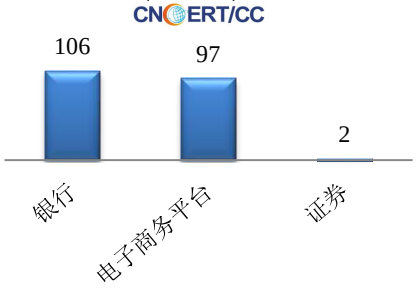
本周CNCERT处理的事件数量按类型分布
(5/4-5/10)





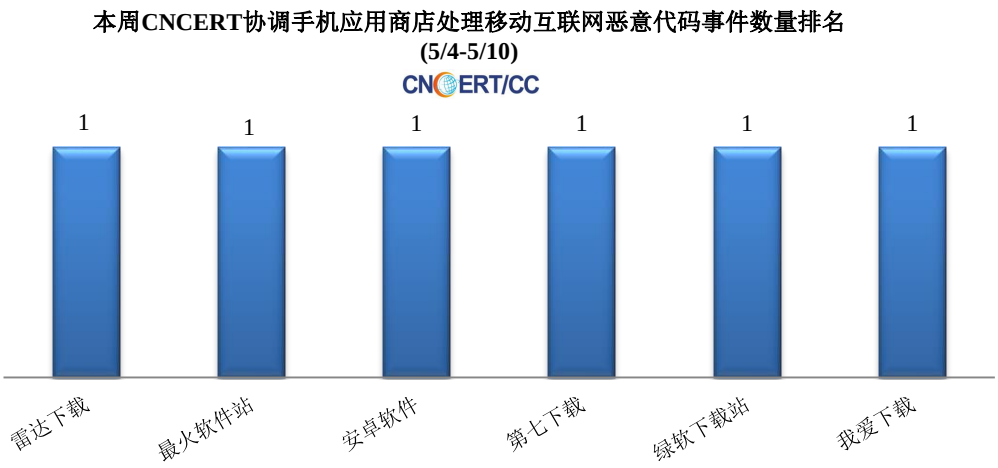
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 205 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 106 起、电子商务平台 97 起和证券仿冒事件 2 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(5/4-5/10)



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 (5/4-5/10)

本周，CNCERT 协调 6 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 6 个。



业界新闻速递

1、 26 项网络安全国家标准获批发布

根据 2020 年 4 月 28 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020 年第 8 号），全国信息安全标准化技术委员会归口的 GB/T 20281-2020《信息安全技术 防火墙安全技术要求和测试评价方法》等 26 项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1.	GB/T 20281-2020	信息安全技术 防火墙安全技术要求和测试评价方法	GB/T 20010-2005, GB/T 20281-2015, GB/T 31505-2015, GB/T 32917-2016	2020-11-01
2.	GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南	GB/T 22240-2008	2020-11-01
3.	GB/T 25066-2020	信息安全技术 信息安全产品类别与代码	GB/T 25066-2010	2020-11-01
4.	GB/T 25067-2020	信息技术 安全技术 信息安全管理体系审核和认证机构要求	GB/T 25067-2016	2020-11-01
5.	GB/T 28454-2020	信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作	GB/T 28454-2012	2020-11-01
6.	GB/T 30284-2020	信息安全技术 移动通信智能终端操作系统安全技术要求	GB/T 30284-2013	2020-11-01
7.	GB/T 34953.4-2020	信息技术 安全技术 匿名实体鉴别 第4部分：基于弱秘密的机制		2020-11-01
8.	GB/T 38625-2020	信息安全技术 密码模块安全检测要求		2020-11-01
9.	GB/T 38626-2020	信息安全技术 智能联网设备口令保护指南		2020-11-01
10.	GB/T 38628-2020	信息安全技术 汽车电子系统网络安全指南		2020-11-01
11.	GB/T 38629-2020	信息安全技术 签名验签服务器技术规范		2020-11-01
12.	GB/T 38631-2020	信息技术 安全技术 GB/T 22080 具体行业应用 要求		2020-11-01
13.	GB/T 38632-2020	信息安全技术 智能音视频采集设备应用安全要求		2020-11-01
14.	GB/T 38635.1-2020	信息安全技术 SM9 标识密码算法 第1部分：总则		2020-11-01
15.	GB/T 38635.2-2020	信息安全技术 SM9 标识密码算法 第2部分：算法		2020-11-01
16.	GB/T 38636-2020	信息安全技术 传输层密码协议（TLCP）		2020-11-01
17.	GB/T 38638-2020	信息安全技术 可信计算 可信计算体系结构		2020-11-01
18.	GB/T 38644-2020	信息安全技术 可信计算 可信连接测试方法		2020-11-01
19.	GB/T 38645-2020	信息安全技术 网络安全事件应急演练指南		2020-11-01
20.	GB/T 38646-2020	信息安全技术 移动签名服务技术要求		2020-11-01
21.	GB/T 38647.1-2020	信息技术 安全技术 匿名数字签名 第1部分：总则		2020-11-01
22.	GB/T 38647.2-2020	信息技术 安全技术 匿名数字签名 第2部分：采用群组公钥的机制		2020-11-01
23.	GB/T 38648-2020	信息安全技术 蓝牙安全指南		2020-11-01
24.	GB/Z 38649-2020	信息安全技术 智慧城市建设信息安全保障指南		2020-11-01
25.	GB/T 38671-2020	信息安全技术 远程人脸识别系统技术要求		2020-11-01
26.	GB/T 38674-2020	信息安全技术 应用软件安全编程指南		2020-11-01

2、 4400 万巴基斯坦移动用户详细信息在线泄漏

5 月 5 日，据外媒报道，有 4400 万巴基斯坦移动订户的详细信息在线泄漏。上月底，一名黑客试图以折合 210 万美元的比特币的价格出售一个包含 1.15 亿巴基斯坦移动用户记录的软件包。目前，某外媒已获得了两个数据软件包的副本，其中一个软件包包含 4400 万条记录，另一个软件包包含 5500 万条用户记录的样本。根据对数据集的分析，研究人员认为，两者的基本内容是相同的。数据包的信息内容包括：用户全名、家庭住址（城市，地区，街道名称）、国家身份证号（CNIC）、手机号码、座机号码和巴基斯坦用户的公司详细信息。此外，泄露的用户公司详细信息与公司网站上列出的公共记录和公用电话号码是相匹配的。

3、 欧洲警察拆除“ Infinity Black”黑客组织

5 月 5 日，据外媒 ZDNet 报道，欧洲刑警组织宣布逮捕了 Infinity Black 黑客组织的五名波兰黑客。据悉，该集团成立于 2018 年底，主要以运营 Infinity[.]black 网站，并在网站上出售用户凭证为盈利方式。目前，由于 Infinity Black 黑客组织给瑞士公民造成了财务损失，瑞士当局开始对该组织的运营进行调查。对此欧洲刑警组织表示，目前损失估计为 5 万欧元，但黑客获得的账户总金额有可能已经超过了 61 万欧元。

据了解，瑞士警方将调查升级至由欧洲刑警组织和欧洲司法组织协助，最终于 2020 年 4 月 30 日在波兰逮捕 5 人。同时，波兰警方没收了价值约 10 万欧元的电子设备，外部硬盘驱动器和硬件加密货币钱包。警察还查封了两个在线平台，这两个平台的数据库包含超过 1.7 亿个被盗的用户凭证。同时，该黑客组织的主要负责人也已经被捕，这表明该组织几乎已经被瓦解。

4、 印度最大在线教育平台 Unacademy 发生大规模数据泄露

5 月 5 日，印度最大的在线教育平台 Unacademy 承认发生数据泄露事件，暴露了大约 1100 万用户的个人详细信息。网络安全情报公司 Cyble 表示已收购了一个包含近 2200 万个 Unacademy 用户账户的数据库（Unacademy 在声明中指出自己只有 1100 万用户），该数据库在 darkweb 上的售价为 2,000 美元。泄漏的数据包括用户 ID、名称和用户名、加密密码、电子邮件地址、加入日期和上次登录时间。Cyble 透露，数据泄露发生于 2020 年 1 月。迄今为止，安全研究人员无法确认是否还有其他人可以访问已泄露数据。

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 2019 年，CNCERT 已与 78 个国家和地区的 260 个组织建立了“CNCERT 国际合作伙伴”关系。CNCERT 还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

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：高川

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315