国家互联网应急中心

网络安全信息与动态周报

2019 年第 13 期

3 月 25 日-3 月 31 日

CNCERT/CC

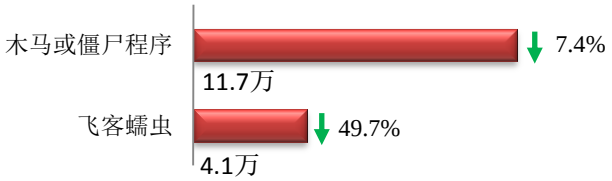
本周网络安全基本态势

境内感染网络病毒的主机数量	•15.8万	↓23.9%
境内被篡改网站总数 其中政府网站数量	•526 •26	↓17.2% ↓21.2%
境内被植入后门网站总数 其中政府网站数量	•633 •3	↓46.8% ↓86.4%
针对境内网站的仿冒页面数量	•2649	↓8.7%
新增信息安全漏洞数量 其中高危漏洞数量	•269 •93	↑37.2% ↑72.2%

=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

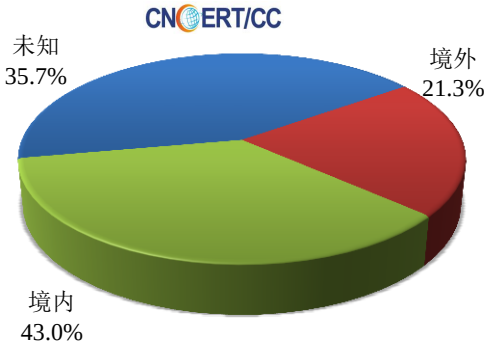
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 15.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.7 万以及境内感染飞客（conficker）蠕虫的主机约 4.1 万。

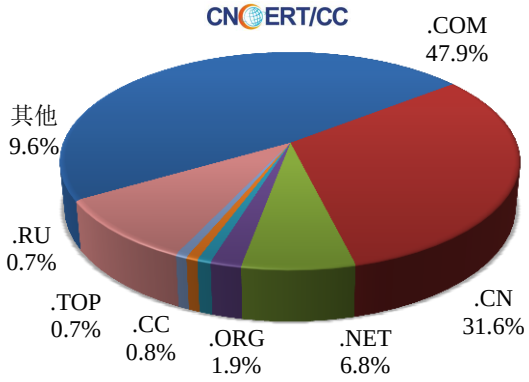


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1536 个，涉及 IP 地址 2995 个。在 1536 个域名中，有 21.3%为境外注册，且顶级域为.com 的约占 47.9%；在 2995 个 IP 中，有约 47.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 323 个 IP。

本周放马站点域名注册所属境内外分布
(3/25-3/31)



本周放马站点域名所属顶级域的分布
(3/25-3/31)



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。

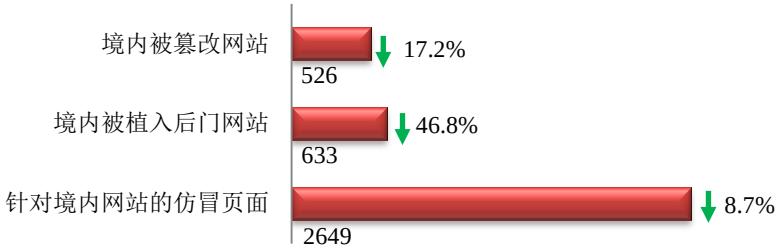
ANVA恶意地址黑名单发布地址

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。

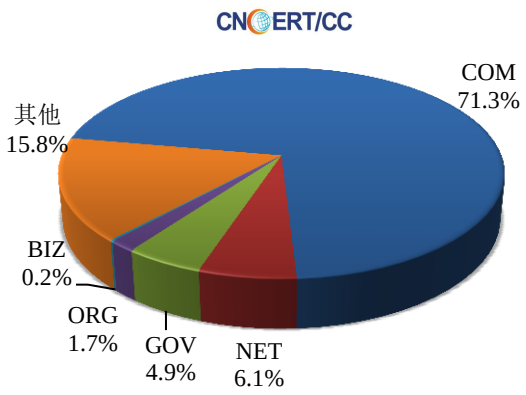
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 526 个；境内被植入后门的网站数量为 633 个；针对境内网站的仿冒页面数量 2649 个。

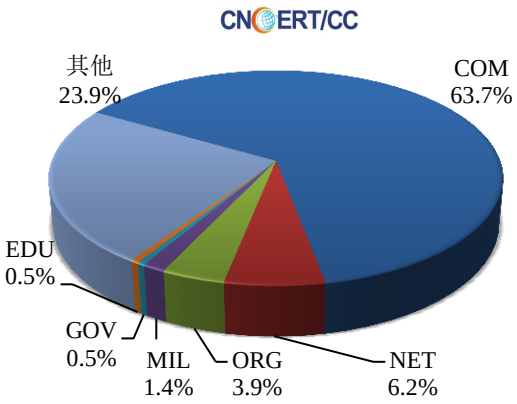


本周境内被篡改政府网站（GOV 类）数量为 26 个（约占境内 4.9%），较上周环比下降了 21.2%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.5%），较上周环比下降了 86.4%；针对境内网站的仿冒页面涉及域名 938 个，IP 地址 361 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/25-3/31)

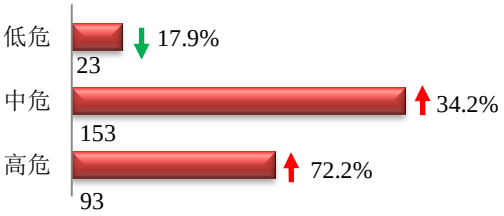


本周我国境内被植入后门网站按类型分布
(3/25-3/31)

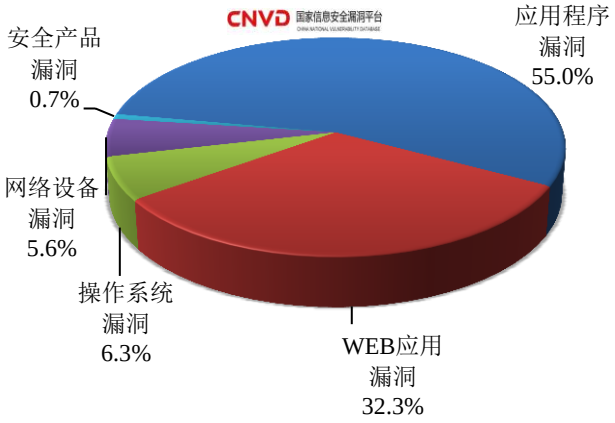


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 269 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
(3/25-3/31)



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

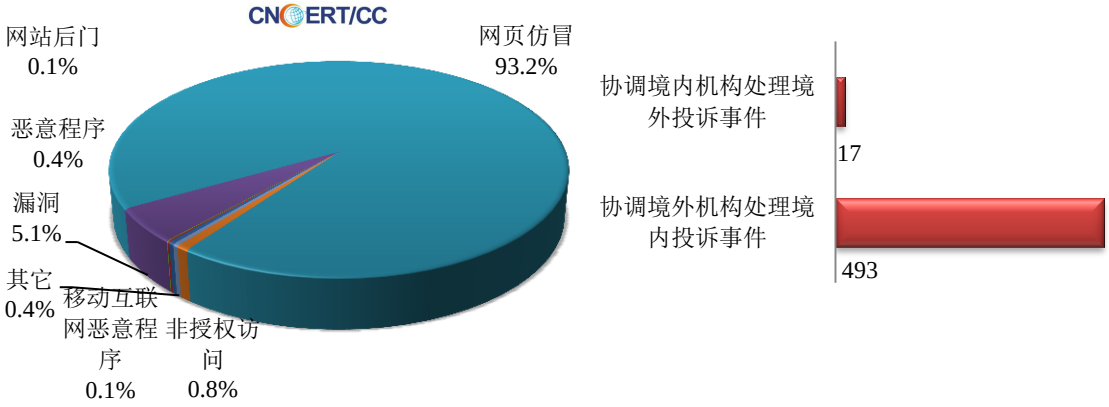
http://www.cnvd.org.cn/webinfo/list?type=4

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

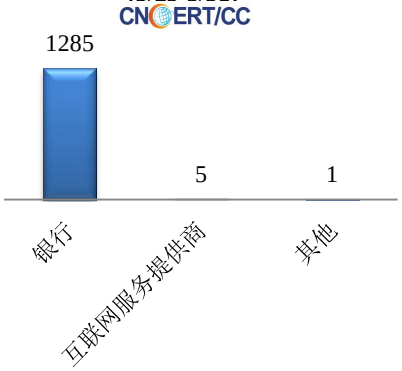
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1385 起，其中跨境网络安全事件 510 起。

本周CNCERT处理的事件数量按类型分布 (3/25-3/31)

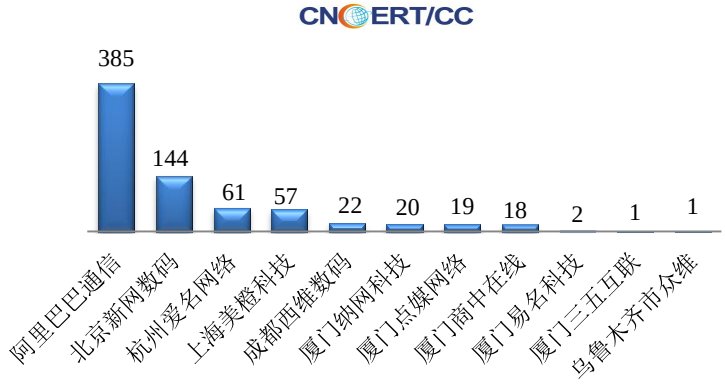


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1291 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1285 起和互联网服务提供商事件 5 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/25-3/31)

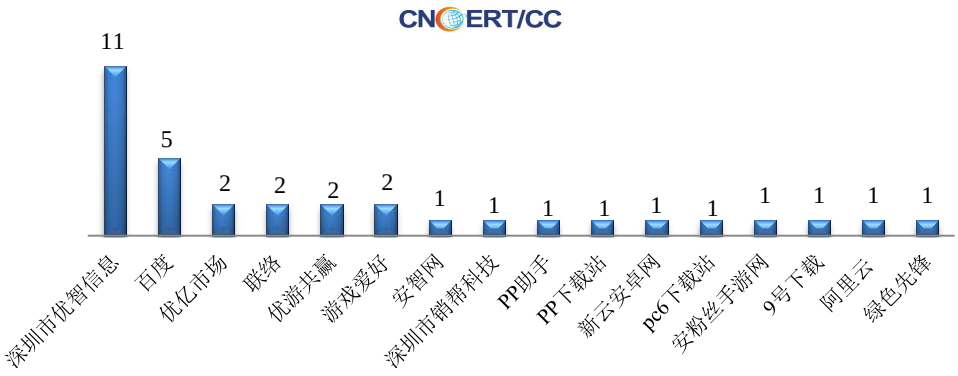


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (3/25-3/31)



本周，CNCERT 协调 16 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 34 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 (3/25-3/31)



业界新闻速递

1、欧洲议会批准互联网版权新规

人民网 3 月 28 日消息 欧洲议会 26 日以 348 票支持、274 票反对、36 票弃权的表决结果，通过新的互联网版权法规，让原创内容提供者和新闻出版商与互联网巨头谈判时底气更足。新法规规定，互联网平台必须与从事音乐、表演、文学和新闻等内容创作的人士事先签署特许协议，方能使用他们的作品。新法规旨在确保欧洲联盟长期以来施行的版权保护法规同样应用于互联网领域。

2、华盛顿州正在制定全面隐私法

安全内参 3 月 30 消息 华盛顿州即将成为继《加州消费者隐私法案》之后，美国第二个通过全面隐私法的州。起草该法令是一个两年多的过程，在此过程中《加州消费者隐私法案》（CCPA）已经通过，《欧盟通用数据保护条例》（GDPR）已经生效。华盛顿提出的隐私法与这两个隐私制度有许多共同的基本原则，但它也有显著的区别。重要的是，它代表了其他国家在起草自己的全面隐私法时考虑的一种新模式。众议院法案目前正在通过委员会的程序，委员会正在考虑修正案--一些重要的修正案，如增加私人行动权。当众议院通过该法案的版本时，它将领导一个会议委员会来协调两院通过的法案之间的任何分歧。众议院创新、技术和经济发展委员会上周发表了一份比较文件，概述了参议院法案和目前在委员会面前的众议院法案修正案之间的差异。

3、美国联邦应急管理局泄露了 230 万灾难幸存者的个人信息

E 安全 3 月 25 日消息 美国联邦应急管理局（FEMA）没有保护好约 230 万飓风幸存者的个

人信息，非法向一家联邦承包商提供了这些私人数据。2017 年，受哈维、玛利亚、厄玛飓风和加利福尼亚的野火和飓风影响的居民获得了政府提供的过渡性庇护援助（TSA）。但联邦应急管理局没有保证幸存者的信息安全，导致他们很容易遭受身份盗窃和欺诈。公开的资料包括：申请人的名字、申请人的中间名、申请人的姓、出生日期、灾难数量、过渡性庇护援助批准书、受援助开始日期、受援助结束日期、序列号、联邦应急管理局注册号码、申请人的住户数目、申请人社会保障号的最后四位数字。

4、韩国加密货币交易所遭黑客攻击

安全内参 3 月 31 消息 总部位于韩国的加密货币交易所 Bithumb 承认，黑客于 3 月 29 日从 Bithumb 窃取了价值近 1900 万美元的加密货币。黑客成功侵入了 Bithumb 的一些热门 EOS 和 XRP 钱包，并将大约 300 万 EOS（约 1300 万美元）和 2000 万 XRP（约 600 万美元）转移到了新创建的账户中。然后，黑客通过 ChangeNow（一个不需要 KYC/account 的非托管密码交换平台）将所盗的资产分散转移到他在其他加密货币交易所（包括 Huobi、HitBTC、WB 和 EXmo）上创建的不同账户。

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：李世淙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158