国家互联网应急中心

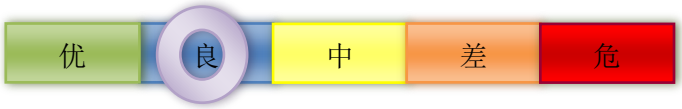
网络安全信息与动态周报

2019 年第 12 期

3 月 18 日-3 月 24 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	•20.8万	↑11.7%
境内被篡改网站总数 其中政府网站数量	•635 •33	↓1.2% ↓25.0%
境内被植入后门网站总数 其中政府网站数量	•1189 •22	↓34.3% =
针对境内网站的仿冒页面数量	•2903	↑147.9%
新增信息安全漏洞数量 其中高危漏洞数量	•196 •54	↓44.0% ↓22.9%

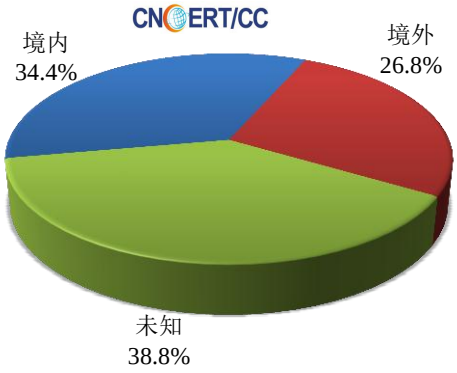
=表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

本周网络病毒活动情况

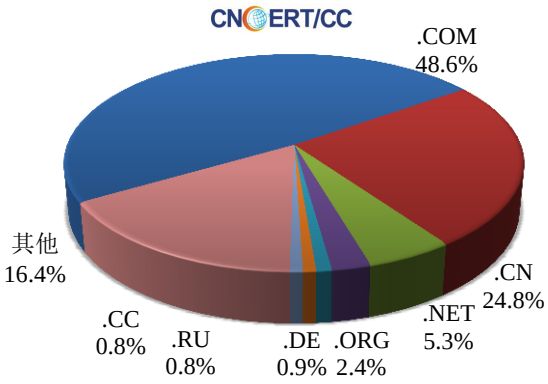
本周境内感染网络病毒的主机数量约为 20.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.7 万以及境内感染飞客（conficker）蠕虫的主机约 8.1 万。

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 2037 个，涉及 IP 地址 3434 个。在 2037 个域名中，有 26.8% 为境外注册，且顶级域为.com 的约占 48.6%；在 3434 个 IP 中，有约 52.9 %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 378 个 IP。

本周放马站点域名注册所属境内外分布
(3/18-3/24)



本周放马站点域名所属顶级域的分布
(3/18-3/24)



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。

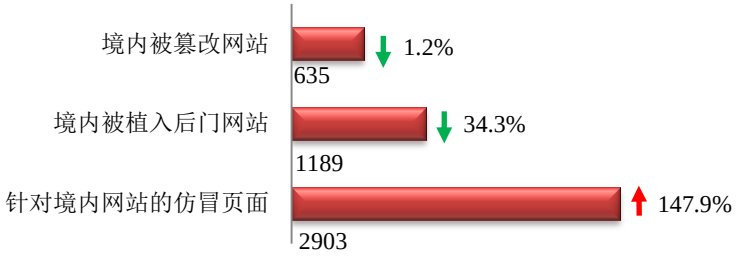
ANVA恶意地址黑名单发布地址

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。

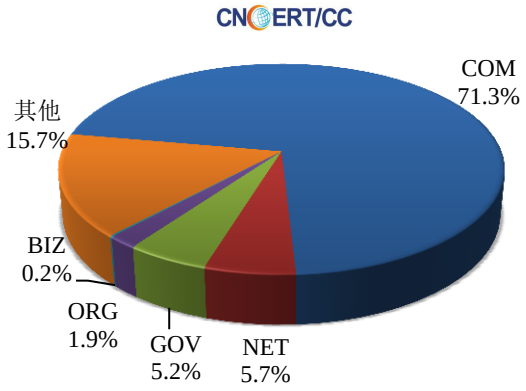
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 635 个；境内被植入后门的网站数量为 1189 个；针对境内网站的仿冒页面数量 2903 个。

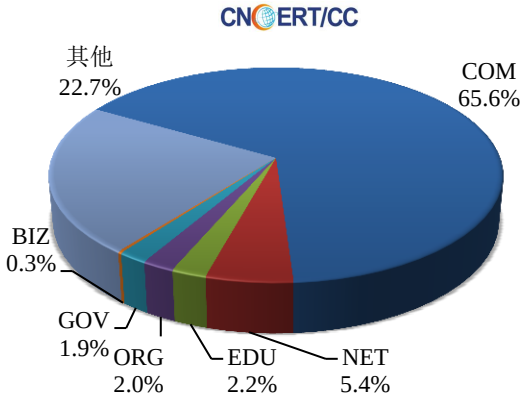


本周境内被篡改政府网站（GOV 类）数量为 33 个（约占境内 5.2%），较上周环比下降了 25.0%；境内被植入后门的政府网站（GOV 类）数量为 22 个（约占境内 1.9%），较上周环比持平；针对境内网站的仿冒页面涉及域名 584 个，IP 地址 327 个，平均每个 IP 地址承载了约 9 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/18-3/24)

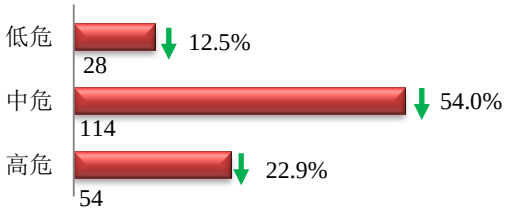


本周我国境内被植入后门网站按类型分布
(3/18-3/24)

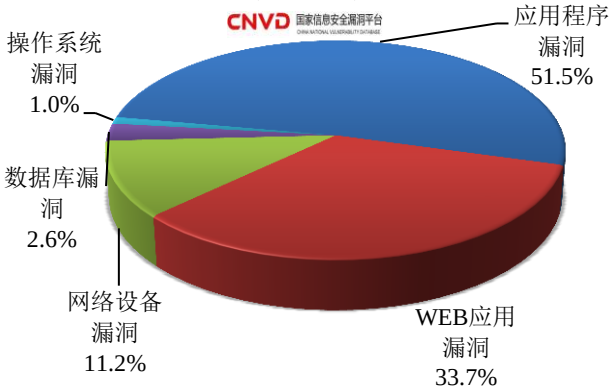


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 196 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
(3/18-3/24)



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 应用漏洞和网络设备漏洞。

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

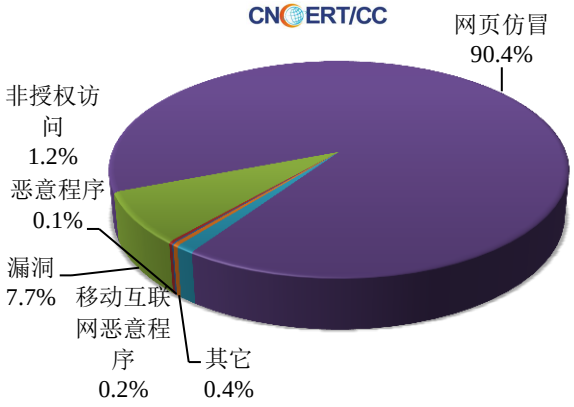
http://www.cnvd.org.cn/webinfo/list?type=4

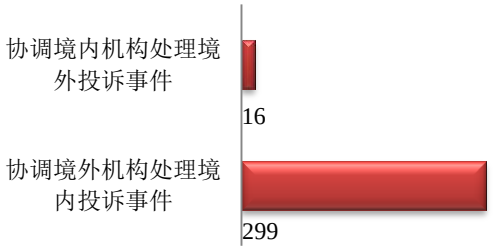
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 831 起，其中跨境网络安全事件 315 起。

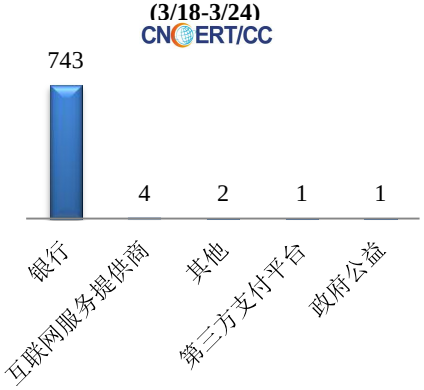
本周CNCERT处理的事件数量按类型分布 (3/18-3/24)



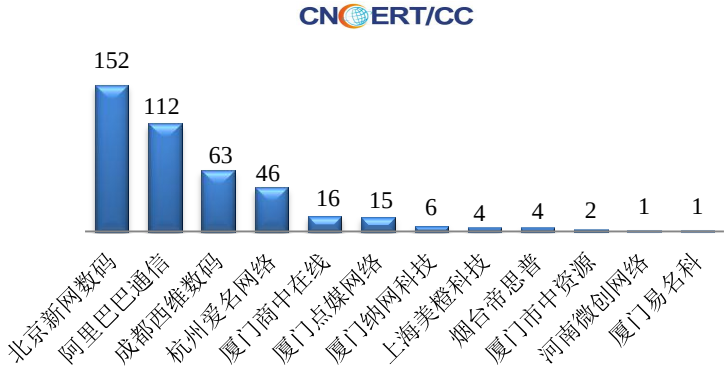


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 751 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 743 起和互联网服务提供商事件 4 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/18-3/24)

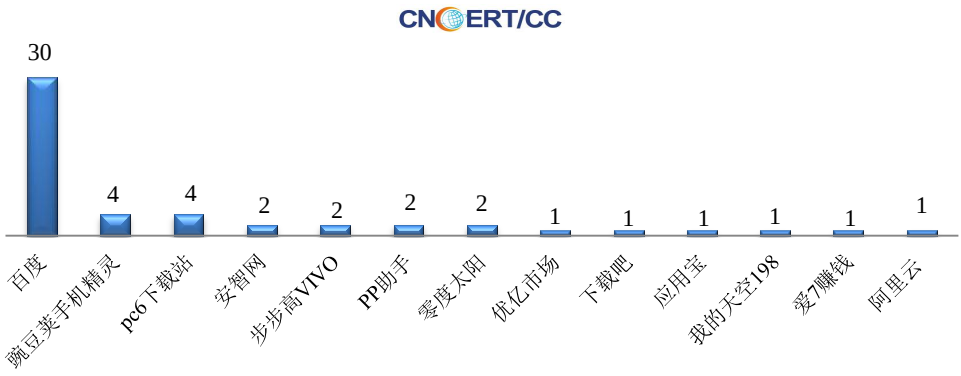


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (3/18-3/24)



本周，CNCERT 协调 13 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 52 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
(3/18-3/24)



业界新闻速递

1、澳大利亚发布政府数据共享临时指导原则

安全内参 3 月 24 日消息 据报道，澳大利亚联邦政府发布了联邦机构数据共享临时性指导原则。由于先前拟议的《数据共享和发布法案》细节仍在制定之中，因此，19 日发布的数据共享指导原则将作为立法准备期间的临时措施。《数据共享和发布法案》的总体目标是，以一致和适当的方式保护数据的发布和共享；增强数据系统的完整性；建立对使用公共数据的信任；建立体制安排；促进更好地公共部门数据共享。

2、谷歌 Facebook 等公司被曝在政府网站上追踪欧盟用户

新浪科技讯 3 月 19 日消息 丹麦浏览器分析公司 Cookiebot 公布研究报告称，欧盟各国政府将允许包括谷歌和 Facebook 在内的 100 多家广告公司在敏感的公共部门网站上秘密跟踪公民，而这显然是违反欧盟数据保护规则的。Cookiebot 在欧盟 25 个成员国的官方政府网站上发现了可记录用户位置、设备和广告主浏览行为的广告追踪工具，其中法国政府网站上的广告追踪工具数量最多，共有 25 家不同公司在其网站上跟踪用户行为。在 22 个主要政府网站的前五大追踪域名中，谷歌、YouTube 和谷歌旗下 DoubleClick 广告平台占据了三席。研究人员还对欧盟公共卫生服务机构的网站进行了研究，结果发现在接受分析的网站中，就堕胎、艾滋病毒和精神疾病等敏感话题寻求健康建议的人而言，他们在超过一半的网站上都遇到了商业广告追踪工具。Cookiebot 对爱尔兰卫生服务网站的 15 个页面进行了扫描，发现其中近四分之三页面都含有广告追踪工具；而就法国政府有关流产服务的一个页面而言，有 21 家不同的公司正在对这个页面

进行监控。一个有关产假的德国网页遭到了 63 个追踪工具的监控，而在提供艾滋病病毒症状、精神分裂症和酒精中毒相关信息的卫生服务网页上则发现了谷歌 DoubleClick 追踪工具。

3、Facebook 再爆隐私丑闻 6 亿用户密码可被员工随意读取

cnBeta.COM3 月 22 日消息 据网络安全记者发布的一份报告称，Facebook 存储了多达 6 亿个没有加密的用户帐户密码。这些账户密码可以作为纯文本，给该公司成千上万的公司员工查看。Facebook 在一篇博文中证实了这一报道。Facebook 股价下跌不到 1%。6 亿用户占 Facebook 全球 27 亿人口用户的 22%。该公司表示，计划开始通知受影响的用户，以便他们可以更改密码。作为 1 月例行安全审查的一部分，Facebook 发现一些用户密码以可读格式存储在我们的内部数据存储系统中。由于多起隐私和安全丑闻，Facebook 一直受到严密的审查，这些丑闻使公司受到客户的批评，以及来自多个监管机构（尤其是欧盟）的问询和罚款。但 Facebook 的丑闻并没有显著削弱该公司的日常活跃用户数量，上个季度的社交媒体活动有所增加。毫无疑问，这一事件将引发爱尔兰数据保护专员的审查，该专员负责执行欧盟新的通用数据保护条例（GDPR）。GDPR 规则允许给予公司 72 小时的时间，来通知受隐私泄露影响的用户，并且要求公司安全地存储密码。

4、新加坡又有数据泄露事件，政府职员邮箱密码在暗网出售

E 安全 3 月 22 日消息 据外媒报道，网上公开了新加坡多家政府机构和教育机构员工的电子登录信息，以及新加坡多家银行的 1.9 万多张被盗银行卡的详细信息。根据 Group-IB 发布的一份新闻稿，信息被盗的组织包括新加坡政府科技局（GovTech）、和新加坡警察部队，以及新加坡国立大学。Group-IB 首席技术官兼威胁主管表示，被泄露的信息可能被用于网络犯罪和间谍活动。政府的用户账户要么在地下论坛上出售，要么被用于进行针对政府机构的网络攻击。即使被泄露的账户只有一个，也可能导致内部中断或政府机密泄露。

5、英国警察联合会遭遇勒索软件，近 12 万警察信息被加密

安全内参 3 月 22 日消息 消息英格兰和威尔士警察联合会（PFEW）遭受了严重的勒索软件攻击，此次攻击涉及英格兰和威尔士 43 支警察部队中的 11.9 万名警察的信息。PFEW 代表声明，能够在恶意软件扩散到其他分支机构之前将其隔离。损害的全部程度仍未公布，公告部分指出，一些数据库和系统受到了影响。备份数据已被删除并已加密，电子邮件服务被禁用，文件无法访问。PFEW 正在继续与专家合作，以恢复系统并将损害降至最低。

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：陈阳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158