国家互联网应急中心

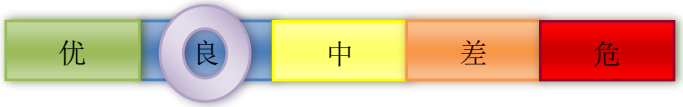
网络安全信息与动态周报

2018 年第 15 期

4 月 9 日-4 月 15 日

CNCERT/CC

本周网络安全基本态势

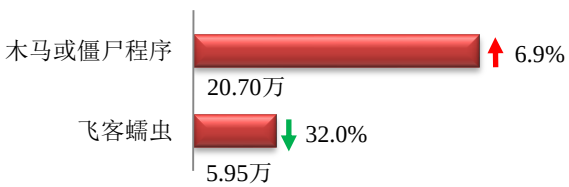


境内感染网络病毒的主机数量	•26.65万	5.2%
境内被篡改网站总数 其中政府网站数量	•976 •34	6.6% 13.3%
境内被植入后门网站总数 其中政府网站数量	•1147 •28	15.4% 154.5%
针对境内网站的仿冒页面数量	•1078	21.3%
新增信息安全漏洞数量 其中高危漏洞数量	•316 •113	91.5% 156.8%

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

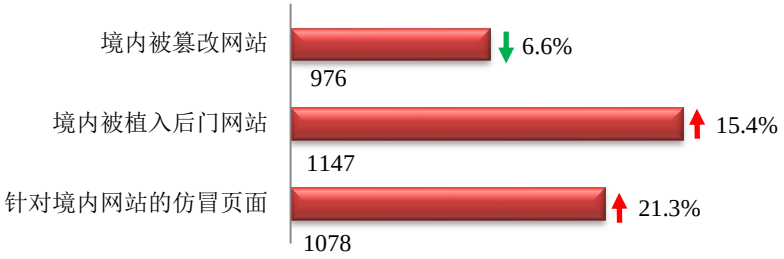
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 26.65 万个，其中包括境内被木马或被僵尸程序控制的主机约 20.70 万以及境内感染飞客（conficker）蠕虫的主机约 5.95 万。



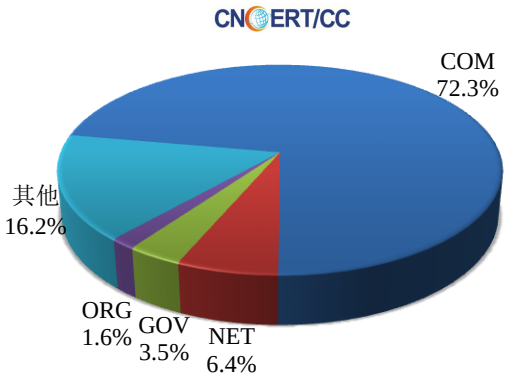
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 976 个；境内被植入后门的网站数量为 1147 个；针对境内网站的仿冒页面数量为 1078。

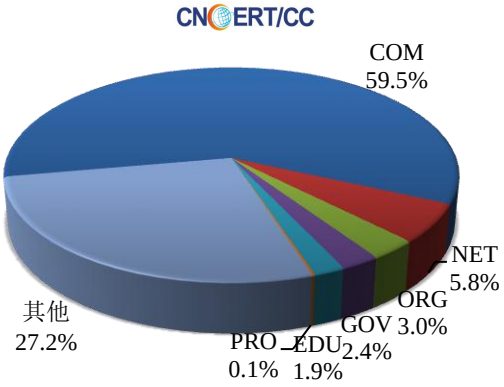


本周境内被篡改政府网站（GOV 类）数量为 34 个（约占境内 3.5%），较上周环比上升了 13.3%；境内被植入后门的政府网站（GOV 类）数量为 28 个（约占境内 2.4%），较上周环比上升了 154.5%；针对境内网站的仿冒页面涉及域名 458 个，IP 地址 180 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/9-4/15)

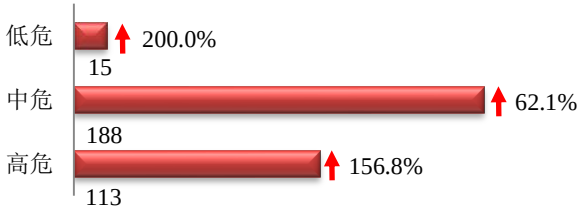


本周我国境内被植入后门网站按类型分布
(4/9-4/15)

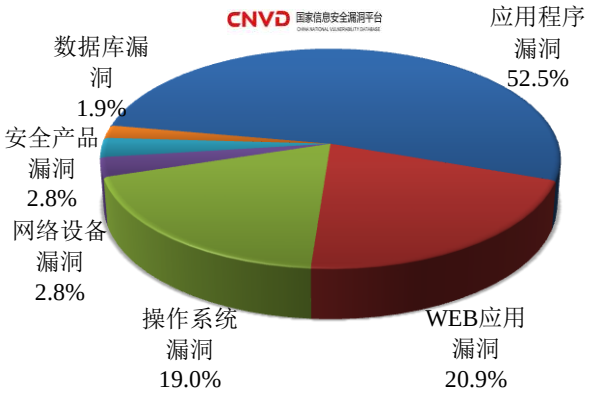


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 316 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
(4/9-4/15)



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

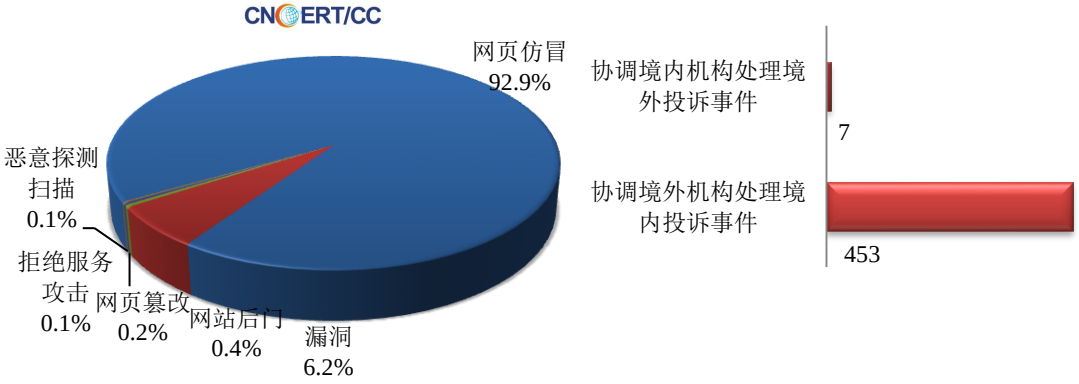
http://www.cnvd.org.cn/webinfo/list?type=4

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

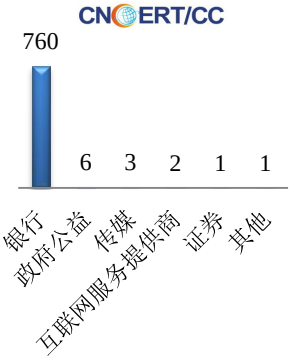
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 833 起，其中跨境网络安全事件 460 起。

本周CNCERT处理的事件数量按类型分布
(4/9-4/15)

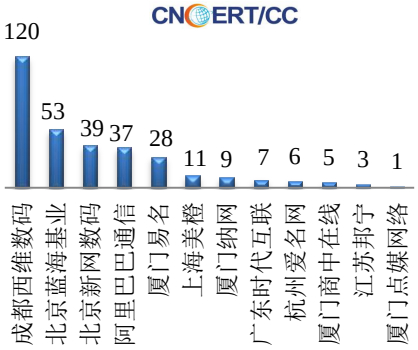


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 773 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 760 起和政府公益仿冒事件 6 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/9-4/15)

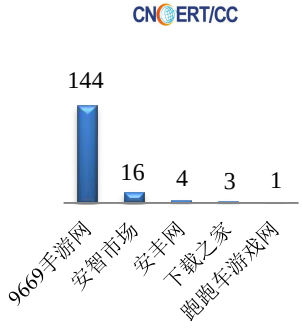


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/9-4/15)



本周，CNCERT 协调 5 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 168 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 (4/9-4/15)



业界新闻速递

1、第 3 届“香港—内地网络安全论坛”在港举行

人民网 4 月 12 日消息 由国家互联网信息办公室网络安全协调局及香港特区政府资讯科技总监办公室（资科办）合办的第 3 届“香港—内地网络安全论坛”4 月 11 日在港圆满举行，约 180 名来自两地网络安全业界的管理及专业人员参会，就共同推动网络安全技术和产业发展进行深入交流。本届论坛主题为“安全的智慧互联—挑战与机遇”。特区政府资讯科技总监杨德斌致辞时表示，随着建设智慧城市引入各种新科技和新模式，网络攻击的层面及其复杂程度也会同时倍增，为网络安全带来新的挑战。论坛共设 4 个专题演讲，由不同范畴的网络安全专家就智慧互联所带来的挑战提供建议，包括保护基础设施及大数据安全的措施及策略。资科办也在论

坛上介绍了将于 2018 年下半年推出的网络安全资讯共享平台，该平台可有效提高香港整体应对网络攻击的防卫及复原能力。

2、英国网络犯罪局：将加密货币网络攻击列为严重威胁

新浪网 4 月 13 日消息 外媒 Btcmanager 报道，英国政府机构承认了加密货币网络攻击的兴起，并发布了一份报告，其中列出了英国互联网生态系统面临主要威胁。这份由英国国家网络安全中心（NCSC）于 4 月 10 日发布的报告强调了加密货币劫持的严重程度。在过去的几年里，黑客们已经将加密货币劫持作为一种收入手段。黑客可以通过使用受害者的计算能力来挖掘加密货币。

3、英国数码购物网站泄露数千名警方、军方、政府消费记录

E 安全 4 月 13 日消息 根据英国科技新闻网站 The Register 的报道，英国热门数码商品在线购物网站 DronesForLess.co.uk 在无意间泄露了数千名警方、军方、政府以及个人消费者的购买记录以及个人信息。导致事件发生的根本原因在于，该网站的交易数据库意外在线暴露并且没有得到加密保护，仅使用谷歌语句搜索就能够很轻松地找到这些数据。约有 13,000 条日期显示为 2015 年 10 月至 2018 年 3 月 31 日期间的购买记录被存储在 DronesForLess.co.uk 的网站服务器上，而这些数据并没有进行加密处理甚至没有设置密码保护。事件的严重性不言而喻，这种情况意味着任何人只要能够在网上找到这个网站服务器，就能够任意浏览上面的数据。根据报道的描述，这些购买记录还包含了消费者的详细个人信息，如姓名、地址、电话号码、电子邮箱地址、IP 地址、用于访问该网站的设备信息、所购买商品的详情、发卡银行以及支付卡号码的后四位。从购买记录来看，在这些消费者中不乏有来自警方、军方以及政府的工作人员。

4、全球超 15 亿敏感文件被曝光

开源中国 4 月 11 日消息据 digital shadows 报道，在三个月的时间内有超过 15 亿个敏感文件被公开在网上，其中包括专利申请、工资单、纳税申报单、患者名单、版权申请和源代码等。这些文件并不是被黑客违法曝光的，而是由配置错误的云存储、文件交换协议和文件共享服务导致的。此次被曝光数据量高达 12,000 TB，这些数据在公开的 Amazon S3 Bucket、Rsync、SMB、FTP 服务器、配置错误的网站或网络附加存储（NAS）驱动器上就可以轻易获得。其中来源于 Amazon S3 Bucket 的占了 7%，SMB 占了 33%，Rsync 占了 28%，FTP 占 26%。更加震惊的是，这些数据中有一些高度敏感的信息，例如安全审计报告、网络基础架构详细信息，甚至是渗透测试报告！Digital Shadows 称：“对这些被公开的文件进行分析表明，组织和个人在无意中暴露了大量的信息，这些数据会使具有恶意的攻击者受益，包括间谍和经济罪犯。”不论是个人还是组织，都应该尽快检查自己的信息安全状况。

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：王小群

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158