国家互联网应急中心

网络安全信息与动态周报

2018 年第 43 期

10 月 22 日-10 月 28 日

CNCERT/CC

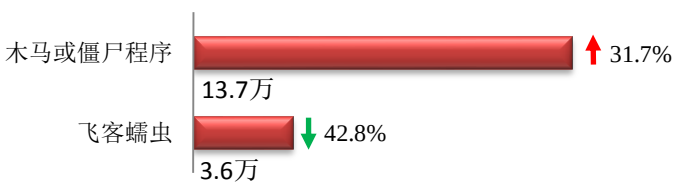
本周网络安全基本态势

境内感染网络病毒的主机数量	•17.3万	3.5%
境内被篡改网站总数 其中政府网站数量	•81 •14	80.4% 46.2%
境内被植入后门网站总数 其中政府网站数量	•931 •14	20.4% 40.0%
针对境内网站的仿冒页面数量	•1070	1.7%
新增信息安全漏洞数量 其中高危漏洞数量	•200 •79	18.0% 21.8%

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 17.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.7 万以及境内感染飞客（conficker）蠕虫的主机约 3.6 万。



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。

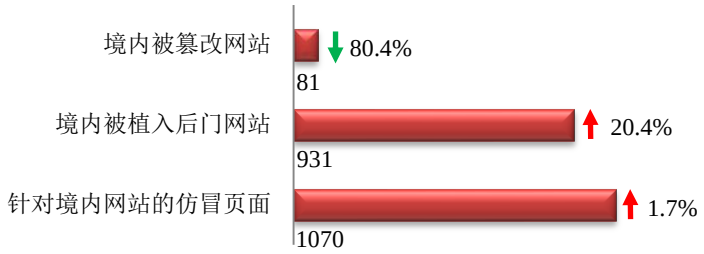
ANVA恶意地址黑名单发布地址

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。

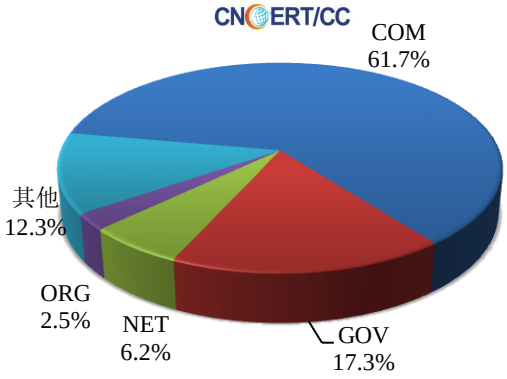
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 81 个；境内被植入后门的网站数量为 931 个；针对境内网站的仿冒页面数量为 1070。

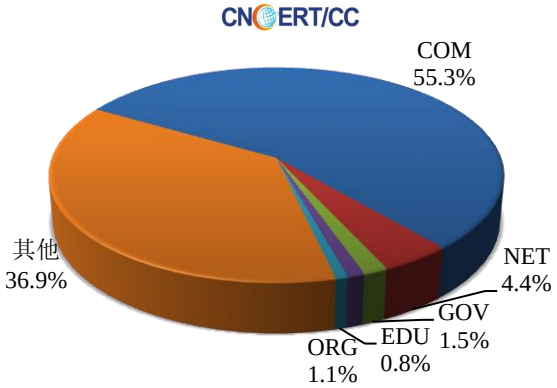


本周境内被篡改政府网站（GOV 类）数量为 14 个（约占境内 17.3%），较上周环比下降了 46.2%；境内被植入后门的政府网站（GOV 类）数量为 14 个（约占境内 1.3%），较上周环比上升了 40.0%；针对境内网站的仿冒页面涉及域名 278 个，IP 地址 213 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/22-10/28)

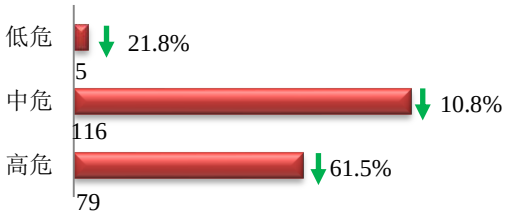


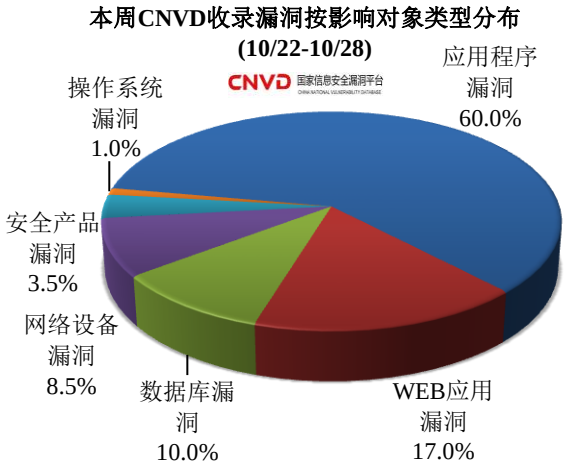
本周我国境内被植入后门网站按类型分布
(10/22-10/28)



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 240 个，信息安全漏洞威胁整体评价级别为中。





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 应用漏洞和数据库漏洞。

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

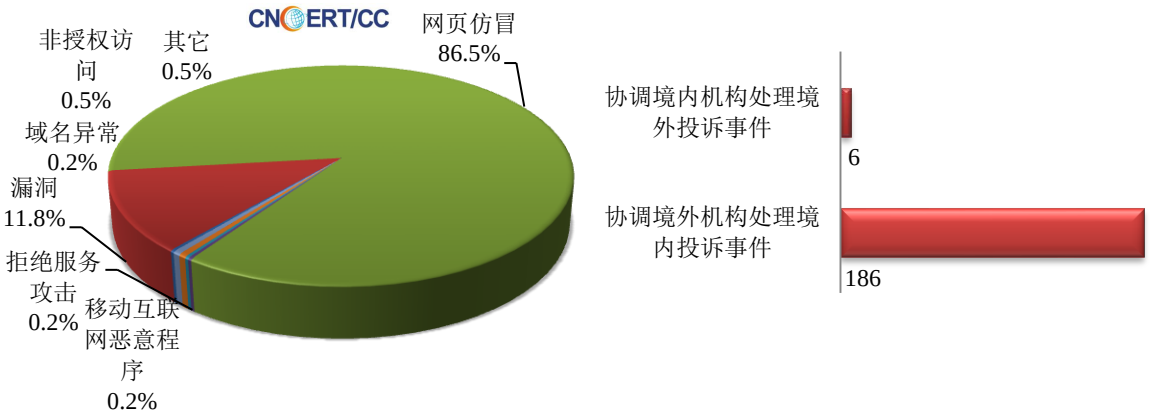
http://www.cnvd.org.cn/webinfo/list?type=4

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

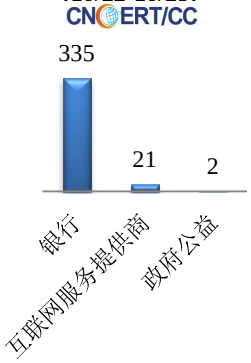
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 414 起，其中跨境网络安全事件 192 起。

本周CNCERT处理的事件数量按类型分布
(10/22-10/28)



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 358 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 335 起和互联网服务提供商仿冒事件 21 起。

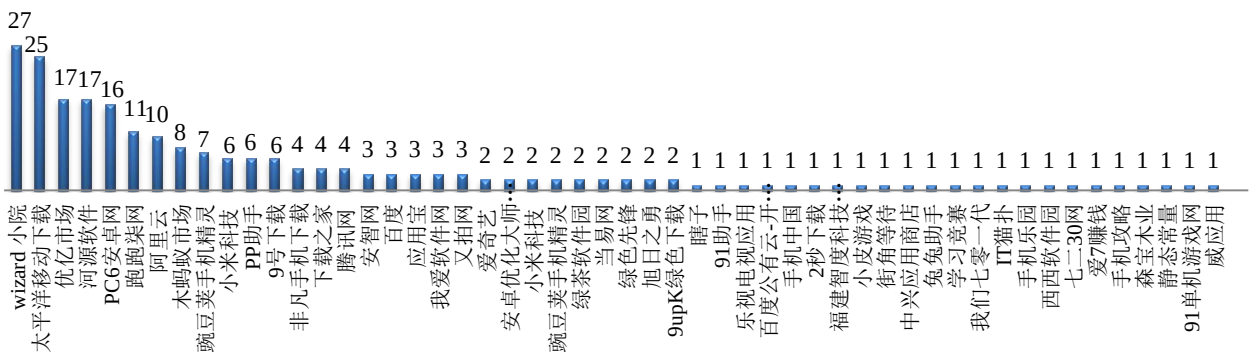
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(10/22-10/28)



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 (10/22-10/28)

本周，CNCERT 协调 52 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 224 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
(10/22-10/28)



业界新闻速递

1、央行发布声纹识别安全应用技术标准 适用手机银行、第三方支付

cnBate10月25日消息 10月9日,《移动金融基于声纹识别的安全应用技术规范(标准编号:JR/T 0164-2018)》由中国人民银行正式发布，即日起实施。近日，《关于发布金融行业标准规范声纹识别技术金融应用的通知（文件编号：0001-2018-S-000-005057）》已随该标准的印刷版一同下发给全国各大银行及各类金融机构，标准的电子版也将择日公布。据了解，该标准由中国建设银行、清华大学、北京得意音通技术有限责任公司发起，历时3 年研证，由央行批准颁布。标准修订期间，在央行科技司主导下，发起单位联合工、农、中、交等国内各大银行，国家级测评机构及第三方支付平台等共同对标准报批稿进行了进一步完善。这是央行颁布的我国金融行业第一个生物识别技术标准。本标准将声纹作为一种独立认证因子进行规范，实际应用中可根据不同场景的安全等级需要，独立采用动态声纹密码完成认证，或与其他认证因子组合完成认证。随着国际上对移动支付安全性和个人隐私保护等问题的日益重视，本标准将安全性和个人隐私保护摆到了突出位置。此外，在本标准中不仅参考了 2017 年 6 月开始实施的《网络安全法》、2017 年 12 月颁布的金融行业标准《移动终端支付可信环境技术规范》，还纳入了 2018 年 5 月刚刚实施的国家标准《信息安全技术个人信息安全规范》等最新文件的要求。

2、美修改部分版权规定：为维修电子设备可合法破解 DRM 保护

cnBate10 月 27 日消息 美国国会图书馆员与美国版权局近日针对美国版权法规-DMCA 数字千年版权法第1201 条批准了数项豁免，美国消费者和独立第三方可以因修复电子设备的目的，合法地绕过内嵌软件的数字保护（如 DRM）机制，而且该项豁免适用的电子设备是宽泛的，包括智能手机、汽车、智能家用电器等诸多设备。这一破天荒的法律豁免标志着“修理权利”运动的胜利。这意味着美国民众和第三方可以合法地绕过 DRM 修复电子设备。包括越狱和修改各种智能语音助手设备；解锁新旧（智能）手机；维修智能手机、家电、家庭系统享有一般豁免；允许自行修改软件来维修汽车、卡车和其他陆上机动车；允许其他第三方代表设备所有者进行此类维修。

3、欧洲议会要求全面审计 Facebook：评估个人数据安全性

新浪科技 10 月 26 日消息 据美国科技媒体 TechCrunch 报道，在 Facebook 出现一系列数据泄露丑闻之后（包括此前“剑桥分析”事件），欧洲议会提出要对 Facebook 进行全面审计。之前 Facebook 有 870 万用户的数据被不正当获取及滥用，为此欧洲议会成员正在敦促该公司允许欧盟机构进行全面审计，以评估数据保护和用户个人数据的安全性。在决议中，他们还建议 Facebook 调整其应对选举干预问题的做法——并坚称该公司不但辜负了欧洲用户的信任，还“违反了欧盟法律”。最近，英国的一个议会委员会敦促政府优先考虑民主流程面临的数字风险并据以调整选举法。不过至今为止，政府对此的态度依旧是较为谨慎，称还在通过审查该问题的不同方面以收集证据。与此同时，Facebook 也在一些地区推出了针对政治广告商的监测系统——包括英国。但是议会成员国显然认为这家公司需要采取更多措施。

4、黑客入侵与 HealthCare.gov 交互的系统

E 安全 10 月 23 日消息 美国医保与医助服务中心（CMS）宣布黑客入侵了与 HealthCare.gov 交互的计算机系统。据美国医保与医助服务中心称，黑客入侵了与 HealthCare.gov 交互的计算机系统，盗取约 75000 人的敏感个人数据。专家发现该入侵后，立即关闭了系统，IT 人员正紧急恢复系统正常运行。据美联社报道，“官方消息称其已关闭受感染系统，技术人员正对其进行紧急修复，以期在 11 月 1 日，即《可负担医疗费用法案（Affordable Care Act）》规定的医疗保险注册时间前恢复其运行”。“受感染系统为保险代理人及保险经纪人用以直接帮助客户进行登记的系统。其他注册系统皆正常工作”。根据“奥巴马医改”（即《可负担医疗费用法案》），约 1 千万美国公民在私营保险公司购买保险之后，可向政府申请补贴，但需要提供社会安全号码、个人收入、公民身份或合法移民身份等大量个人信息。自 11 月 1 日起，公民可登陆 HealthCare.gov，填写申请表，加入 2019 年健康计划交易市场。

5、雅虎将为史上最大安全漏洞案支付 5000 万美元赔偿金

新浪科技 10 月 24 日消息 雅虎已经同意支付 5000 万美元的赔偿金，并向美国和以色列的约 2 亿名用户提供两年的免费信用监控服务，此前这些用户的电子邮件地址及其他个人信息在有史以来最大的安全漏洞案中被盗。上述赔偿需在联邦法庭批准周一提交的和解协议后才会生效，这项和解协议是就一桩已经进行了两年的诉讼案而达成的，原告方要求雅虎为 2013 年到 2014 年间发生的数字窃案负责，该公司直到 2016 年才披露了用户数据被盗的信息。在这桩窃案中，约 30 亿个雅虎账号被黑客盗取，其中包括与俄罗斯之间存在关联的一些黑客。上述和解协议是在旧金山法庭达成的，覆盖了约 2 亿名用户拥有的 10 亿个账号。雅虎现在已是 Verizon 通信公司旗下子公司。

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：刘栋

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158