国家互联网应急中心

网络安全信息与动态周报

2018 年第 41 期

10 月 8 日-10 月 14 日

CNCERT/CC

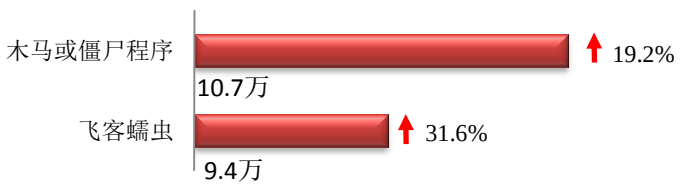
本周网络安全基本态势

境内感染网络病毒的主机数量	•20.1万	↑ 24.7%
境内被篡改网站总数 其中政府网站数量	•282 •20	↓ 31.7% ↓ 23.1%
境内被植入后门网站总数 其中政府网站数量	•587 •10	↑ 29.6% ↑ 25.0%
针对境内网站的仿冒页面数量	•2042	↑ 54.9%
新增信息安全漏洞数量 其中高危漏洞数量	•240 •85	↓ 36.0% ↓ 22.0%

═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

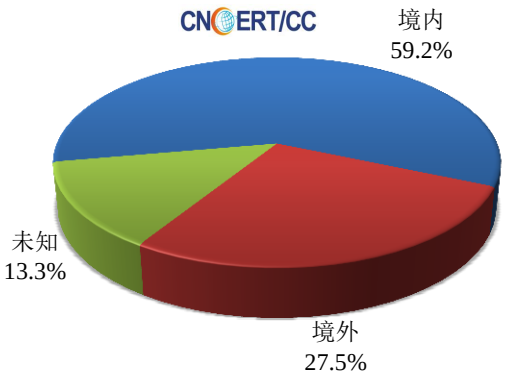
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 10.7 万以及境内感染飞客（conficker）蠕虫的主机约 9.4 万。

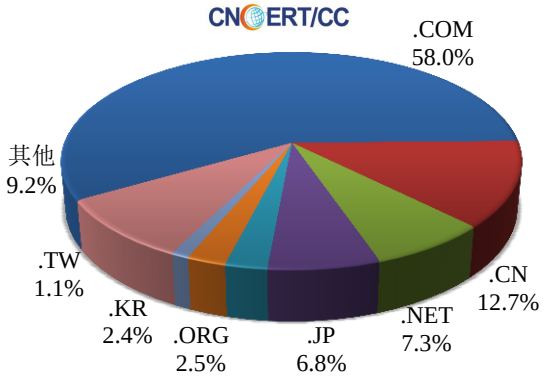


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 6411 个，涉及 IP 地址 65819 个。在 6411 个域名中，有 27.5%为境外注册，且顶级域为.com 的约占 58.0%；在 65819 个 IP 中，有约 31.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 485 个 IP。

本周放马站点域名注册所属境内外分布
(10/8-10/14)



本周放马站点域名所属顶级域的分布
(10/8-10/14)



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。

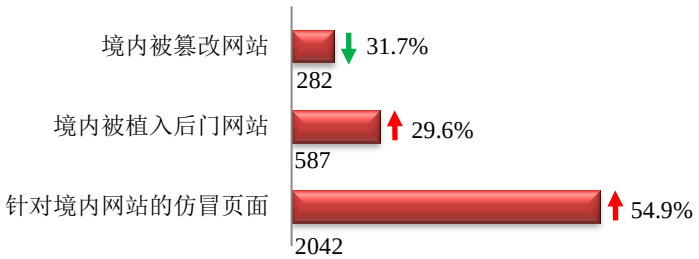
ANVA恶意地址黑名单发布地址

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。

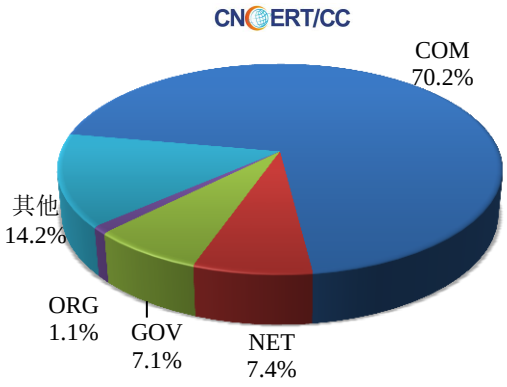
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 282 个；境内被植入后门的网站数量为 587 个；针对境内网站的仿冒页面数量为 2042。

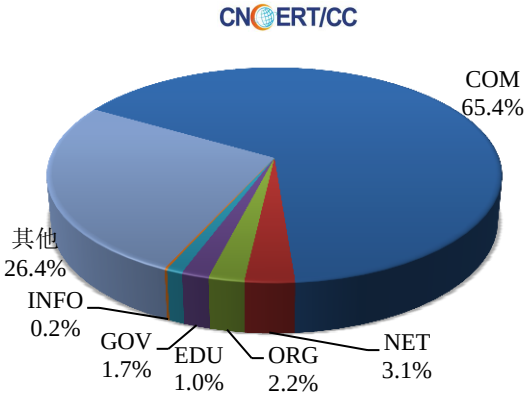


本周境内被篡改政府网站（GOV 类）数量为 20 个（约占境内 7.1%），较上周环比下降了 23.1%；境内被植入后门的政府网站（GOV 类）数量为 10 个（约占境内 1.7%），较上周环比上升了 25.0%；针对境内网站的仿冒页面涉及域名 694 个，IP 地址 5272 个，平均每个 IP 地址承载了约 0 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/8-10/14)

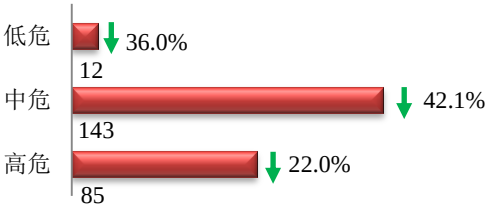


本周我国境内被植入后门网站按类型分布
(10/8-10/14)

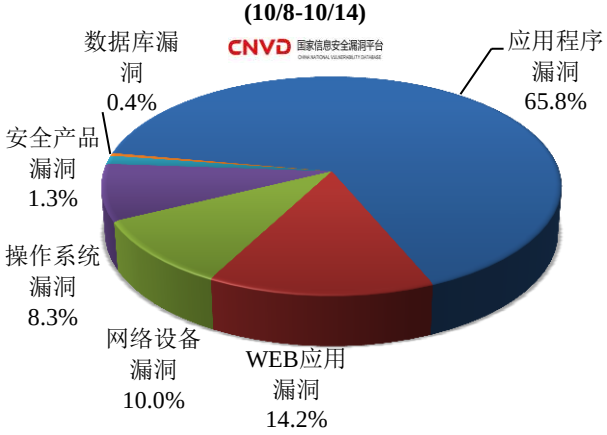


本周重要漏洞情况

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收录漏洞按影响对象类型分布
(10/8-10/14)



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

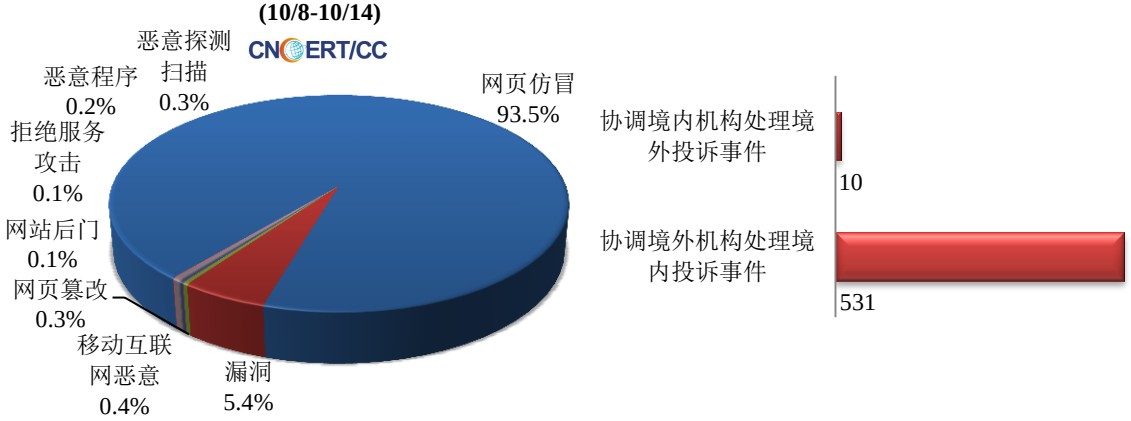
http://www.cnvd.org.cn/webinfo/list?type=4

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

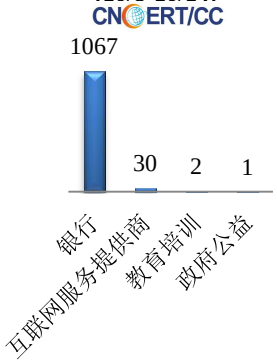
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1177 起，其中跨境网络安全事件 541 起。

本周CNCERT处理的事件数量按类型分布 (10/8-10/14)

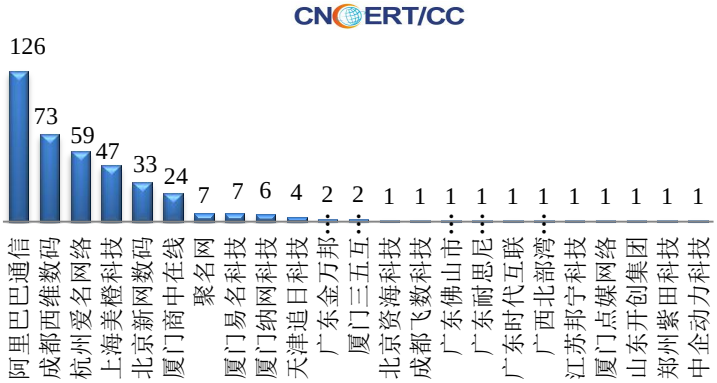


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1100 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1067 起和互联网服务提供商仿冒事件 30 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (10/8-10/14)

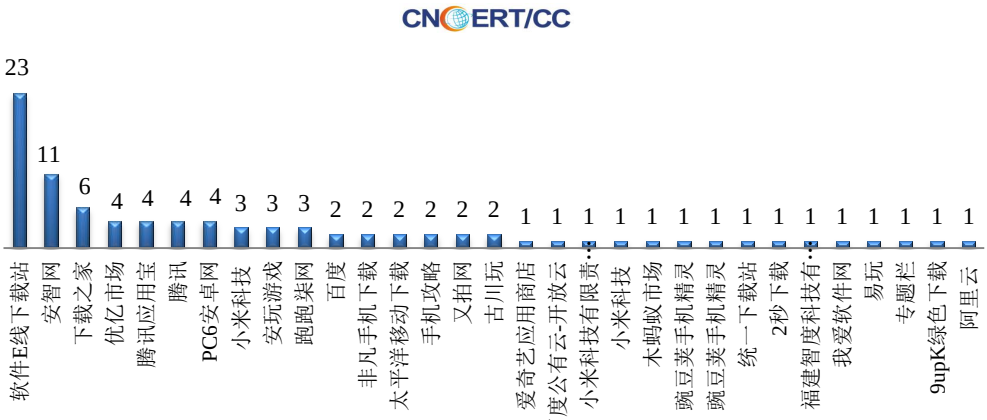


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/8-10/14)



本周，CNCERT 协调 31 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 92 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
(10/8-10/14)



业界新闻速递

1.央行、银保监会、证监会联合发布《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》

经济日报-中国经济网北京 10 月 10 日讯 为规范互联网金融从业机构反洗钱和反恐怖融资工作，切实预防洗钱和恐怖融资活动，中国人民银行、中国银行保险监督管理委员会、中国证券监督管理委员会制定了《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》（以下简称《管理办法》），并于今日公布。《管理办法》的出台，旨在建立相关监管机制和监管规则。一是建立监督管理与自律管理相结合的反洗钱监管机制。明确中国人民银行、国务院有关金融监督管理机构协同监管和互金协会自律管理相结合，做到履职各有侧重，工作相互配合。同时，充分发挥互金协会和其他行业自律组织的管理作用，借助自律组织的力量，促使从业机构强化内控建设、增强反洗钱意识，提升监管有效性。二是建立对全行业实质有效的框架性监管规则。《管理办法》对从业机构需要履行的反洗钱义务进行原则性规定。同时，明确由互金协会协调其他行业自律组织制定行业规则，实现监管和自律管理的有效衔接。

2.欧盟隐私部门主管：首轮涉数据违规罚款或在年底实施

新浪科技讯 北京时间 10 月 10 日早间消息，据路透社报道，欧盟隐私部门主管表示，监管机构将依据新隐私法行使权力，对违规行为处以罚款甚至临时禁令，预计今年年底将实施第一轮制裁。《欧盟通用数据保护条例》（GDPR）于 5 月 25 日生效，被外界认定为欧盟二十多年来最大的数据隐私法规改革。新规允许消费者更好地控制他们的个人数据，并赋予监管机构权力，对违反规定的企业处以罚款，金额可高达其全球收入 4%或 2000 万欧元（约合 2300 万美元）。

3.重大系统故障袭击东京证券交易所

cnBeta.COM10 月 09 日消息 日本最大的证券交易所设法通过使用备用线路恢复交易，而正常交易预计将在周三恢复。然而，包括野村证券公司，SMBC 日兴证券和大和证券公司在内的大型经纪公司完全停止了订单处理，因为故障已经失控。与此同时，野村证券（Nomura Securities）周二下午开始恢复接受客户的订单。

4.Facebook 表示 2900 万人信息被黑客窃取 1400 万人被看光

cnBeta.COM10 月 14 日消息 近日，Facebook 表示，上月底宣布的安全漏洞影响的人数要比预期少的多，最初 Facebook 内部认为有 5000 万个账户受到影响，但核实后，Facebook 将这一数字削减到了 3000 万。Facebook 表示，黑客确实收集了这 3000 万个账号中的 2900 万个账户的个人信息，包括这 2900 万人的姓名、联系方式、电话号码与电子邮件。FBI 正在调查此次黑客入侵事件，Facebook 表示正在配合 FBI 进行调查，但仍未找到这名黑客究竟是谁。此次 Facebook 受攻击的原因是网站代码中有一个 View As 功能存在缺陷，View As 可以让用户了解其他人的个人资料与看法；攻击者利用 View As 的漏洞来窃取多达 5000 万个帐户的访问权限，使用该权限，其他人可以接管用户的 Facebook 会话并访问数据。

5.物联网僵尸网络“捉迷藏”新变种发现：Android 设备成新受害者

cnBeta.COM10 月 9 日消息 继今年 1 月发现首个物联网僵尸网络 Hide and Seek（HNS，捉迷藏）之后，近日 Bitdefender Labs 发布报告称已经发现新型变种。利用 Android 开发者调试之用的 Android Debug Bridge (ADB)功能中所存在的漏洞，该变种通过 WiFi 网络连接来感染 Android 设备，使之成为僵尸网络的一员。虽然并非所有 Android 都默认启用 ADB 功能，但部分 Android 手机厂商会默认自动启用，可以通过 5555 端口使用 WiFi ADB 远程连接就能轻松进行攻击。在连接至默认激活 ADB 的 Android 系统之后，允许攻击者以 root 级别获得 shell 访问，可以在受感染设备上运行和安装任何东西。

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：曹攀攀

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158