Situation of Information Security in 2016

13331233 孙中阳

概述

刚刚结束的第二届世界互联网大会，以互联网安全为主题，全世界互联网专家领导都在关心这一话题。在世界互联网大趋势下，网络安全问题成为首要问题。没有任何可靠地技术能够保证对所有网络犯罪或对针对性攻击免疫，但提前做好最坏的准备能够对部分攻击进行有效的防御。

安全事件

节选自《2016十大安全事件》和“ifanr”网站

OpenSSL“心脏出血”

2016年3月，全球有三分之二的网站服务器用的开源的加密工具OpenSSL爆出新的安全漏洞“水牢漏洞”，这一漏洞允许“黑客”攻击网站，并读取密码、信用卡账号、商业机密和金融数据等加密信息，对全球网站产生巨大的安全考验。我国有十万余家网站受到影响。

思科“方程式”0day漏洞

8月份思科安全产品被发现漏洞，据称，漏洞存在于IKEv1包处理代码中，利用该漏洞可致远程、未认证的攻击者获取存储内容（memory contents），84万思科系统受到影响。

WIFI安全漏洞

消费者权益保护日当天，央视315晚会曝光公共WIFI有安全漏洞，不法分子可提取登录用户手机中包括手机号码、家庭住址、身份证号甚至银行卡号等个人隐

私信息。一旦个人隐私信息被盗取，将会被不法分子利用，进行个人钱财转移或盗取操作，造成巨大的人身财产损失。

MySpace及雅虎等邮箱信息泄露

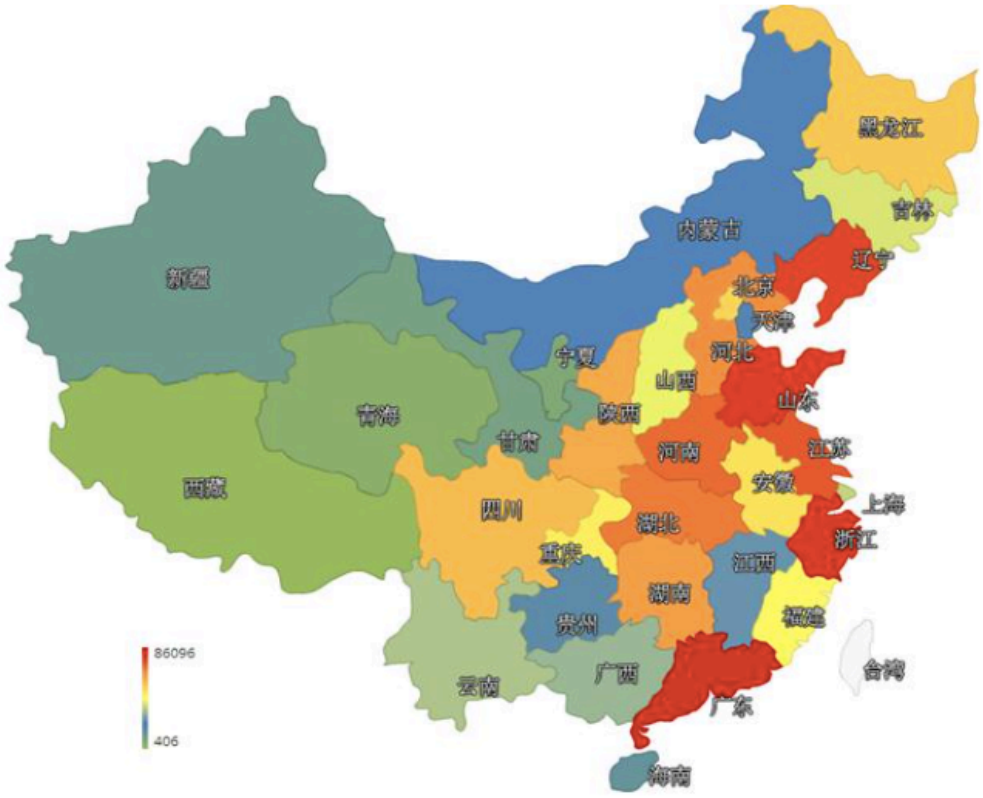
5月发生了两起恶性信息窃取事件：俄国黑客盗取了2.723 亿邮箱信息，其中包括 4000 万个雅虎邮箱、3300 万微软邮箱以及 2400 万个谷歌邮箱；黑客利用漏洞，盗取3亿6000万MySpace用户的电子邮件地址以及密码。

主要威胁

根据《2015年中国互联网网络安全报告》，我国主要面临以下几个方面的安全威胁

木马和僵尸网络

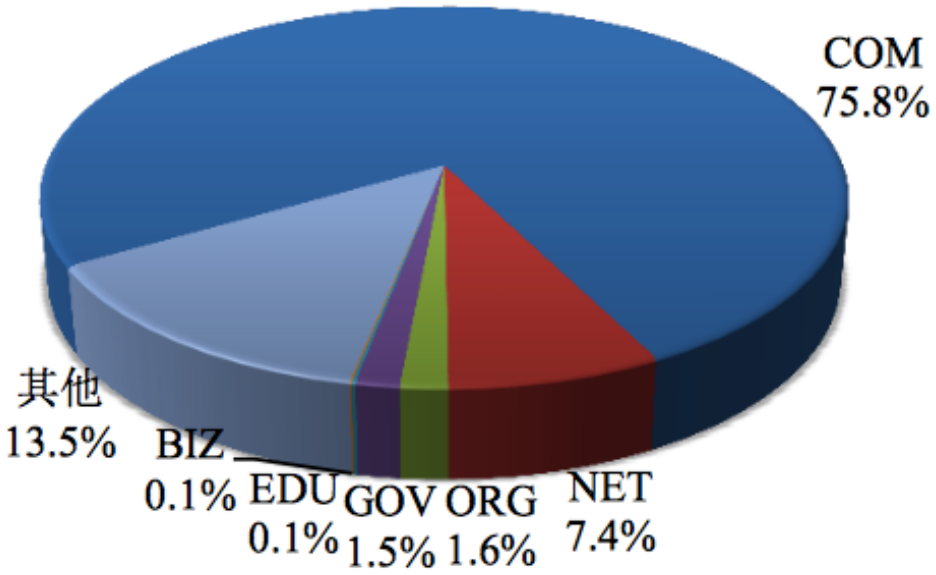
国家互联网应急中心网络安全信息与动态周报（2016年第38期）显示9月12日-9月18日境内感染网络病毒的主 机数量约为 61.9 万个,其中包括 境内被木马或被僵尸程序控制的 主机约 40.6 万以及境内感染飞客 (conficker)蠕虫的主机约 21.3 万。境外威胁数量高于境内，同时较去年同期（2015 9.14-9.20）的87.8 万个有明显减少。
木马或僵尸程序受控主机在我国大陆的分布情况如下图所示



网页仿冒和篡改

一周内CNCERT监测发现境内被篡改网站数量为2674个，较去年同期的3051个有所减少;境内被植入后门的网站数量为8683个，较去年同期的3996个大幅上升;针对境内网站的仿冒页面涉及域名852个,IP地址391个,平均每个IP地址承载了约2个仿冒页面，主要为诈骗网站，钓鱼网站等。

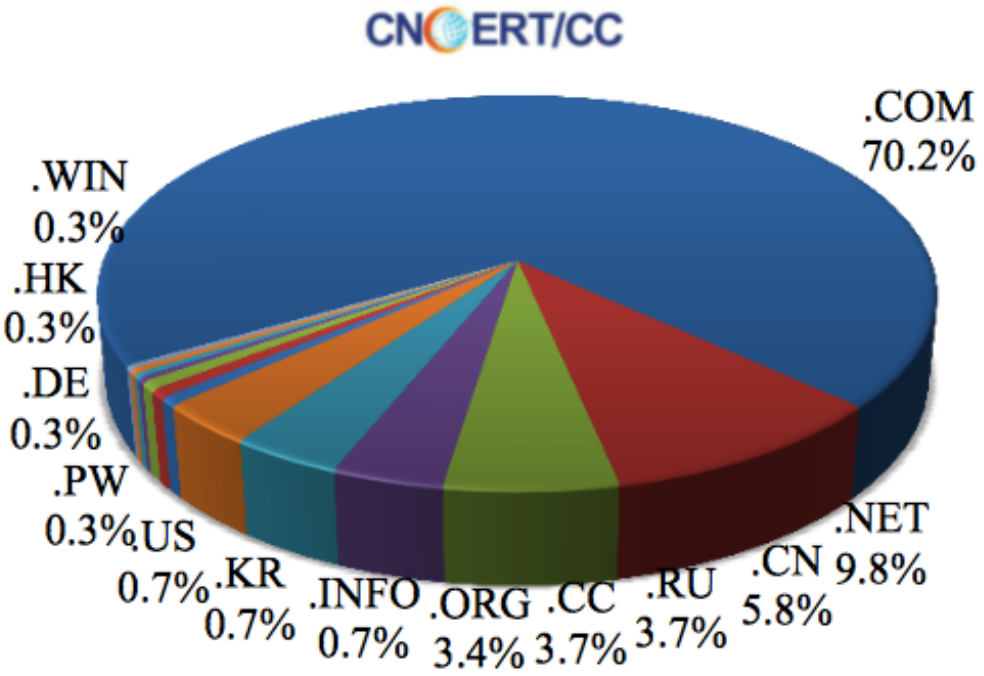
我国境内被篡改网站按类型分布：



计算机漏洞和病毒

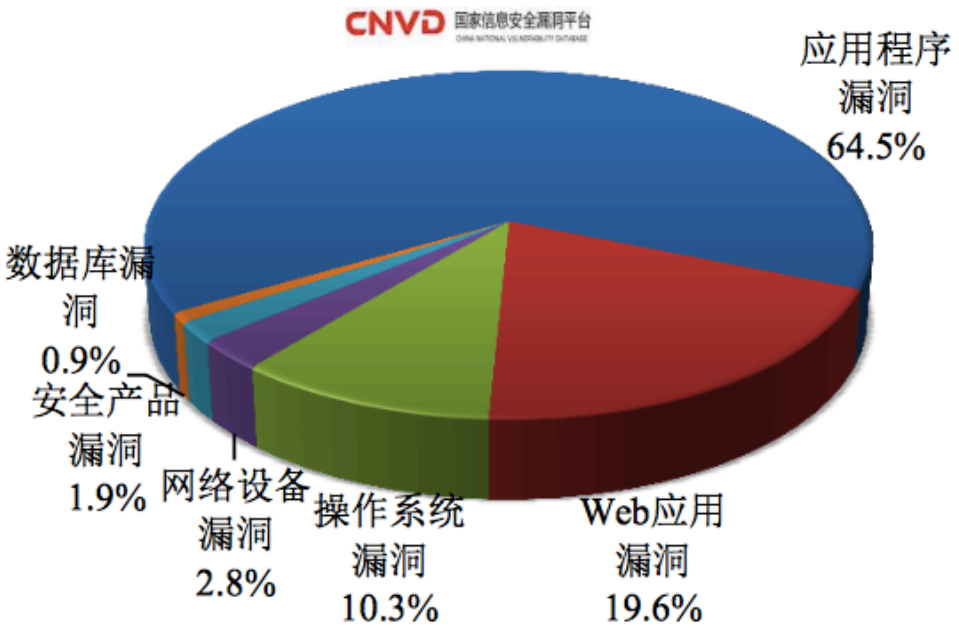
2015年CNCERT捕获了大量新增网络病毒文件,按网络 病毒名称统计新增177个,按 网络病毒家族统计新增55个。根据调查显示，放马站点是网络病毒传播的源头。另外，一周年日监测发现的放马站点共涉及域名295个,涉及IP地址479个。在295个域名中,有约34.6%为境外注册,且顶级域为.com的约占70.2%;在479个IP中,有约24.0%位于境外。

放马站点域名分布:



漏洞和系统风险

另外国家信息安全漏洞共享平台(CNVD)近期新收录网络安全漏洞107个,信息安全漏洞威胁整体评价级别为低。 在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。
详细占比如下:



发展趋势

根据黄海峰《网络信息安全2016年呈现五大发展趋势》，云安全、数据安全、APT 攻击防御、未知威胁、智能制造安全等5个领域，将成为2016年网络安全技术重点发展方向。他提到

> 在云安全方面,云模式的防御产品是 发展方向。通过云端服务器,其可以实现 样本广泛采集、高速分析和实时全网应对;提供虚拟化安全、数据安全等体系化 解决方案成趋势,突破单一产品局限;以 云基础设施、云网络、云应用构成的三层 安全结构逐渐确立,专业厂商、云服务提 供商可为用户提供定制化安全服务。在数据安全方面,业界逐步加强敏感 信息识别审计、数据加密脱敏、泄露监测 等技术突破和集成;在APT攻击防御方面,监测、防御、追溯并重。业界在加强深度沙箱监测、自学习安全基线、历史数据回溯和关联分析等技术创新和联动。 在应对未知威胁方面,以大数据分析为基础的威胁情报分析和安全态势感知 被认为是应对位置威胁的有效途径,逐渐 受到重视。在智能制造安全方面,智能设 备领域全生命周期安全设计、轻量级安全 成趋势;在智能系统领域,安全防护、监 测等关键技术将实现突破。

另外，赛门铁克安全情报团队针对2016年及未来的重大安全预测进行整合。以下为赛门铁克公司针对2016年的主要安全趋势预测

> 1.对提高物联网设备安全的需求变得更加迫切
> 2.将会有越来越多针对苹果设备的攻击
> 3.勒索软件犯罪团体和恶意软件分发网络之间的战争将会愈演愈烈
> 4.网络攻击与数据泄露将会推动对网络保险的需求
> 5.针对关键基础设施的攻击将更加严重
> 6.更多更强的加密需求
> 7.生物识别安全系统将会达到临界点
> 8.安全游戏机制和安全模拟将帮助用户应对安全意识的挑战

应对方法

基础通信网络安全防护

OSI框架中基础的五层承担重要的网络安全责任，电信产业对网络安全的投入对信息安全的总体态势起到重要作用。对于提供信息接入和传达服务的电信服务商，须有系统化、规范化和常态化的核准，检查和评级的手段，对不合格或者不合规的体系、制度和技术方案采取措施。如交换机的招标采购，代码审核等须严格规范，避免“棱镜门”或者8月思科“0day”漏洞造成的影响。

方程式再曝0day漏洞：超84万思科设备受影响

责任编辑：editor007 作者：欧阳洋葱 | 2016-09-22 22:00:46 本文摘自：FreeBuf.COM

前一阵的NSA方程式组织被黑事件，可能受影响最大的还不是美国政府，而是思科——因为这次事件中，公布了大量针对思科安全产品的漏洞利用工具，思科不得不一个个去调查研究，确认漏洞存在与否，发布安全公告，着手漏洞修复。

我们已经对其中的ExtraBacon利用工具，和涉及到的相关漏洞进行了一波分析。在之前描述ExtraBacon的文章中，我们带到过另一款漏洞利用工具，即BenignCertain。这款工具专门针对思科的PIX防火墙家族产品，此工具可用于解密VPN流量。

域名系统建设

作为网络体系重要基础设施的域名系统，必须严格确保域名的合理使用。域名系统的疏漏可造成违规网站泛滥，钓鱼网站欺诈，DDos攻击等网络安全事件。域名相关操作应尽可能通过域名实名认证，注册地点管理等手段对域名进行规范，例如我国最近征求意见的的《域名管理办法》（修订稿）就明确提到“内网络接入的域名应有境内域名注册服务机构提供服务”等具体实施细节，可有力提升我国域名安全的管理水平。

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

搜索

工业和信息化部 新闻动态 信息公开 在线办事 公众参与 专题专栏 工信数据

首页 > 工业和信息化部 > 机构设置 > 政策法规司 > 工作动态 > 正文

公开征求对《互联网域名管理办法（修订征求意见稿）》的意见

发布时间：2016-03-25 来源：政策法规司

为了规范互联网域名服务活动，落实《国务院关于取消和调整一批行政审批项目等事项的决定》（国发〔2014〕27号）等有关规定，我部起草了《互联网域名管理办法（修订征求意见稿）》，现向社会公开征求意见，请于2016年4月25日前反馈意见。

联系人：工业和信息化部政策法规司

电 话：010-68205072（传真）

电子邮箱：law@miit.gov.cn

地 址：北京市西城区西长安街13号工业和信息化部政策法规司（邮编：100804），请在信封上注明"规章征求意见"。

工业和信息化部

2016年3月25日

附件：互联网域名管理办法（修订征求意见稿）

工业互联网安全

工业互联网安全直接关系到信息系统安全性的问题。2015年12月,因遭到网络攻击,乌克兰境内近三分之一的地区发生断电事故。据 分析,此次网络攻击利用了一款名为“黑暗力量”的恶意程序。随着工业信息化发展，工业生产对信息技术的依赖加大，如果出现安全事故，将造成直接的经济损失和巨大的不稳定因素。我国已组建相关网络安全，通信安全部队，防止针对工业信息系统的有组织攻击。

新闻中心 新闻中心 > 正文

沙特以色列被曝欲开发"超级震网"病毒破坏伊朗核计划

2013年12月03日14:17 国际在线 微博

国际在线专稿：据俄罗斯RT电视台网站12月2日报道，伊朗半官方的法尔斯通讯社披露称，沙特与以色列情报机构摩萨德正在密谋共同开发更具破坏性的新型"超级震网"电脑病毒，以破坏伊朗核计划。

与沙特情报机构关系密切的消息人士证实："沙特情报主管班达尔王子（Bandar bin Sultan bin Abdulaziz Al Saud）与以色列摩萨德主管塔米尔·巴德（Tamir Bardo）曾派代表于11月24日在维也纳会面，双方欲在情报工作、破坏伊朗核计划方面加强合作。"双方探讨的主要合作内容是"开发比'震网'更强大的恶意软件"。

用户角度安全建设

个人认为，以下几点使得用户安全得到了长足的提升

> 1.操作系统升级，恶意软件活动空间缩小
> 如之前XP系统权限管理并不成熟，后在WIN7中得到改善。
> 2.软件市场成熟，正规软件逐渐抢占更多市场
> 记得以前很多人安装盗版的Office 2003，易被安插恶意代码，不过后来逐渐被WPS所取代，珊瑚虫QQ，雨林木风等也类似。
> 3.流氓软件活动更加隐匿，不易被察觉
> 流氓软件的开发需要成本，需要闷声发大财。
> 4.用户有价值信息逐渐转移到互联网上，主机作用下降
> 互联网取得良好发展，恶意软件制作者在主机端的投入下降。
> 5.杀毒软件成熟，下载站审核更加严格，应用商店的出现
> MSE，360都有足以满足一般杀毒需求的能力，360有应用商店。同时软件的获取渠道相比之前更为正规，如官网下载等。
> 6.故意制作恶意软件受到舆论压力
> 如360、3721、百度全家桶，最终用户用脚投票。