2011-2012中国互联网网站

安全报告

KNOWNSEC

知 道 创 宇

北京知道创宇信息技术有限公司

2012.3

目 录

1. 声明

本报告包含的信息代表北京知道创宇信息技术有限公司 (中文简称知道创宇，英文简称 Knownsec) 对 2011 年所关注的互联网安全领域的总结。

本报告仅用于提供信息之目的。其资料由知道创宇互联网监控中心统一提供，本报告仅针对中国大陆地区 2011 年检测到网站资料进行统计、研究和分析。知道创宇 (Knownsec) 对于本报告中的信息不做任何明示、暗示或法定的担保。如若本报告阐述之状况、数据与其它机构研究结果有差异，请使用方自行辨别，本公司不承担与此相关的一切法律责任。

2. 相关术语

- **挂马源** 是指网马攻击代码所在的页面或 URL，黑客使用挂马源对外进行挂马传播。
- **挂马网站** 是指受到挂马源感染的网站，黑客利用网站存在的漏洞，将挂马源嵌入到正常网页中，当用户浏览这些网页就有可能受到来自挂马源的恶意攻击。
- **挂马 SITE** 在本报告中“SITE”表示受挂马影响的网站站点。例如 report.org、a.report.org。
- **挂马 URL** 由于挂马方式的特点，针对普通 URL 的后缀信息来进行挂马也已经是一种流行的常规的做法，因此，也就存在被挂马 URL。例如 http://flc.zjgsu.edu.cn/snow.htm。
- **监控网站数** 以站点 (SITE) 为基本单位进行统计的由知道创宇互联网监控中心监控所得的数值。
- **挂马网站数** 同样以站点 (SITE) 为基本单位但只对存在挂马的网站站点进行统计的数值。
- **网站挂马率** 由知道创宇互联网监控中心统计出来的存在挂马的网站站点数与被监控的网站站点总数的比值。
- **监控域名数** 在网站域名为基本单位进行统计的由知道创宇互联网监控中心提供的数值。需要重点说明的是，网站域名一般都有子域名的存在，所以，本报告中的监控域名数也包含了各主网站域名下的子域名数。
- **挂马域名数** 同样以网站站点为基本单位但只对存在挂马的域名进行统计的数值。
- **域名挂马率** 由知道创宇互联网监控中心统计出来的存在挂马的网站域名数与被监控的网站域名总数的比值。
- **暗链** 在这里通俗的说，网站链接中的一种，也称为黑链。如果再通俗的说一点“暗链”就是看不见的网站链接，“暗链”在网站中的链接做的非常 隐蔽，短时间内不易被搜索引擎察觉。它和友情链接有相似之处，可以有效地提高 PR 值。但要注意一点 PR 值是对单独页面，而不是整个网站。

3. 2011 年中国互联网挂马与暗链情况综述

根据知道创宇互联网监控中心 2011 年挂马检测资料统计，中国互联网 2011 年整体挂马情况仍普遍存在。同时，挂马的方式方法也变得比较复杂和多样化。根据知道创宇互联网监控中心所收集到的数据显示，全国的所有省份都存在程度不一的挂马现象。对于关系到国家重点部门以及重点行业的网站进行检测时，也发现存在比较严重的挂马问题。

从数据上看存在挂马比较严重的情况发生在 2011 年的 11 月份。同时，这也是 2011 年年网站挂马率最高的时期。根据数据显示，在整个 2011 年期间，中国整体互联网网站数量为 5,533,092，其中挂马量为 20,368，由于国家对于互联网安全问题的日益重视并加大了监管的力度，2011 年中国互联网整体挂马率 0.4% 与 2010 的 1% 相比已有了巨大的下降，显现出一种较稳定的保持趋势，与些同时，由于神州八号的发射、世界游泳锦标赛、世界大学生运动会等重大活动的举行，使得国家主要监管部门对于互联网安全的关注度非常高，这些因素综合一起使得中国互联网整体挂马情况得到了很大的改善。

以上只是对 2011 年中国互联网挂马状况做了一个说明。对于所收集到的信息进行更多细致的分类和划分后，又得到了很多具有特点的数据结果。

通过对挂马网站按行业来划分，不但可以就国家重点行业的网站被挂马的情况有一个准确的了解，同时，也可以清楚国家各个地区的网站被挂马的情况。同时，对于政府、教育、金融、电信等有关国计民生的网站的检测，也可以掌握 2011 年这类网站的挂马情况，详细数据请查看本报告相关内容。

同时，通过按地区区分，并进行数据对比，可以详细的了解全国各个地区的挂马状况。从数据可以得出，越是信息活动与经济发达、商业行为频繁的地区，其挂马状况就越严重。通过相关数据进行排名，全国挂马情况比较严重的地区前三名分别是北京、江苏和广东。这主要是因为此类地区，其商业网络化应用的程度非常高。日常的各种经济活动都需要在互联网上进行，因此，通过挂马这种传播非常快速、简单实用的恶意网络攻击行径，就可以在非常短的时间内，从互联网上得到巨大的物质利益。因此，只要有效的掌握了这些信息，就可以有效的对挂马行为进行有效监管和打击。

本报告除以上内容外，还在 2011 年度被挂马最多网站、域名、IP 地址、挂马源、最流行使用的漏洞以及受挂马影响的网站系统与软件、重大安全事件回顾等几个方面，进行了类型划分和数据分析以便更加全面、准确的展现出 2011 年中国互联网整体挂马、暗链等的安全情况。

为了使本报告在互联网安全整体情况上更加全面，本报告所关注的领域将不再只局限于网站挂马行为，同时也开始关注比网站挂马行为更加隐蔽、不易发觉的新的恶意行为，暗链的行为发生。在数据统计和分析中，也借鉴了对于网站挂马行为的一些统计手法。通过使相类似的数据统计方法，可以比较挂马与暗链之间的共通以及不同之处，同时，也就暗链行为在未来可能的一个发展趋势提供一个参考和借鉴。

以供国家各有关部门或机构进行参考。关于此类数据的详细信息，都可以本报告中查找。

4. 2011 年挂马网站疫情概要

2011 年全国挂马疫情概要所示数据由知道创宇互联网监控中心提供。基于监控中心所示数据，2011 年度中国互联网挂马疫情资料如下。

4.1. 2011 年各项挂马数据分析

4.1.1. 2011 年全国挂马状况趋势

根据知道创宇互联网监控中心 2011 年挂马检测资料统计，我们统计了 2011 年度中国互联网网站挂马整体趋势。为了更直观地表现出 2011 年度挂马情况，我们以 2011 年逐月挂马网站数为基础，制作了 2011 年挂马网站趋势图，如图 1 所示。

图 1 2011 年受挂马攻击网站趋势图

相关分析：

从图 1 中可以看出，在于 11 月份之前网站挂马整体上都处于一个比较稳定的状态，遇有一些波折但都在一定的区间内反复。但到了 11 月则达到了年度网站被挂马网站次数最高时刻 15,840，之后在但快速的呈下降的趋势走向。知道创宇的研究团队注意到，在此期间正好发生了一些重大的互联网安全事件，一些重要的系统与软件出现了安全漏洞或安全问题（如：wordpress 插件，Discuz!，phpcms 等），这也正好与挂马数据突然高升相吻合。但与此同时，由于国家对于互联网信息安全的重视以及相关部门出台了诸多关于互联网信息安全的法律、法规等文件以后，加大了监管以及打击各种利用互联网进行非法活动的力度，在随后的 12 月期间，挂马网站次数非常快速的下降，回落到了原有的稳定状态。

2011 年全国主要地区（省级）挂马分布图。

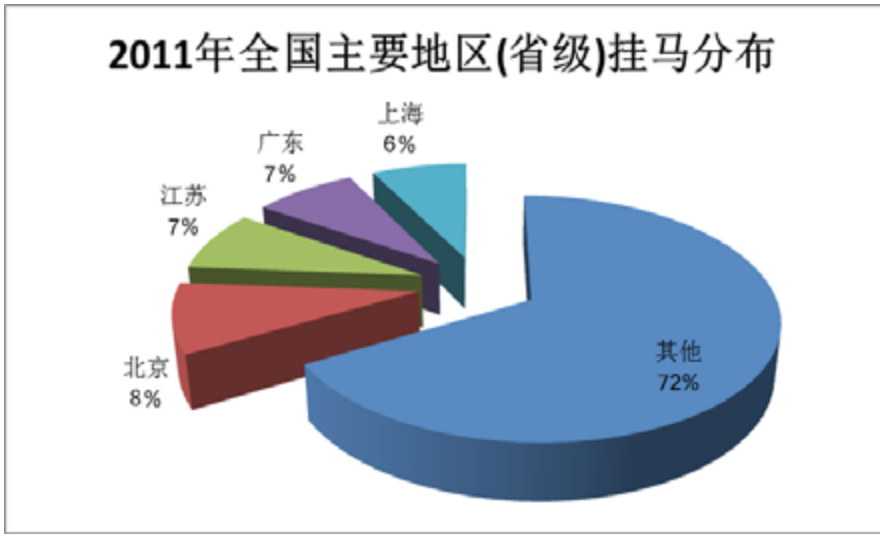

图 2　2011 年全国主要地区（省级）挂马分析图

从图 2 中可以看出 2011 年度全国主要地区网站的挂马情况。对于我们了解挂马行为在全国各地区的分布情况，提供了一个很好的参考。通过上图所展现的资料，我们给出了一个挂马网站次数前十名的地区排名表。如图 3 所示。

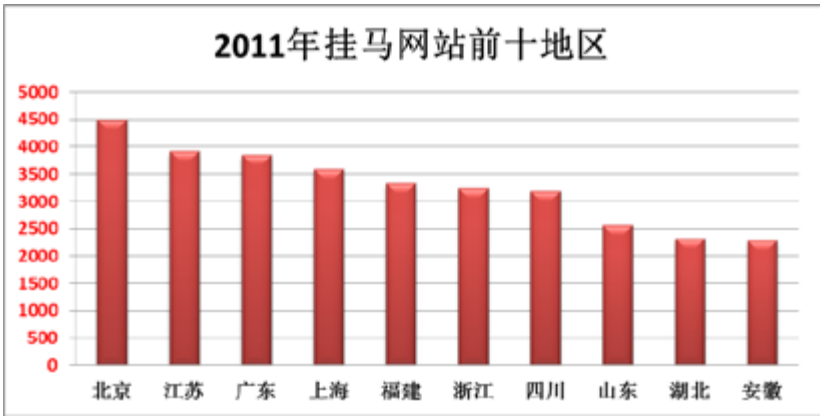

图 3　2011 年挂马网站前十地区

从图 3 中可以看出，北京、江苏、广东、（北京占 8%、江苏占 7%、广东占 7%）等地的挂马问题远领先于全国其他地区。另外，我们也可看出，前十位中一半以上都为南方地区，且随着地区经济愈发达，挂马数量愈发增多，这也说明了经济发达程度对于挂马行为的影响力是非常大的。

4.1.2. 2011 年度全国重点行业挂马状况分析

重点行业网站的安全问题对于国家经济建设、国家行业信息秘密来说有着非常重要的意义。所以，针对这些重点网站的挂马情况，我们也在这里做了一个统计。以下为全国重点行业网站的挂马状况做了一个统计。

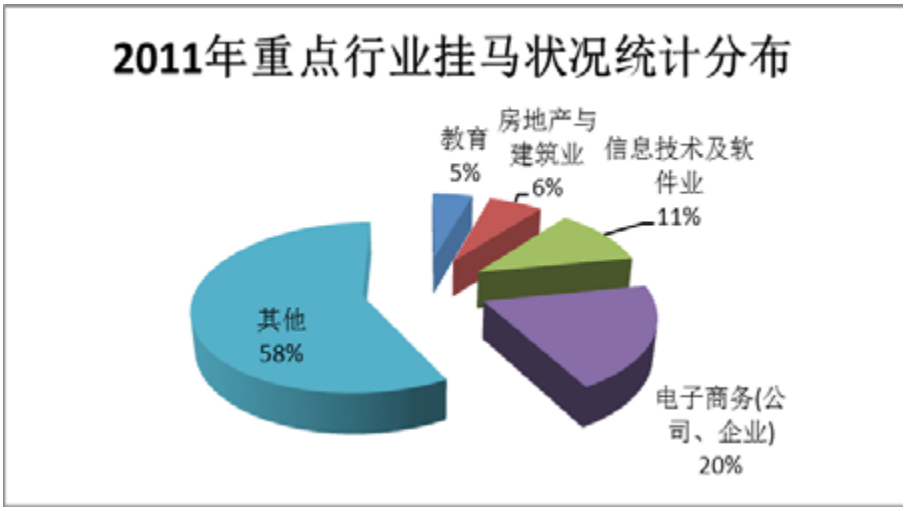

图 4　2011 年重点行业挂马状况统计分布

4.1.3. 2011 年重点网站域名挂马分析

知道创宇互联网监控中心，也对目前互联网应用中主要的域名类型进行了挂马检测，并得出了 2011 年各类型域名的挂马情况。通过排名可以看到，排名前三位的基本上也是应用最多的域名类型，分别为：.com、. cn、.com. cn，分别占到了 22%、8%、9%，如图 5 所示。

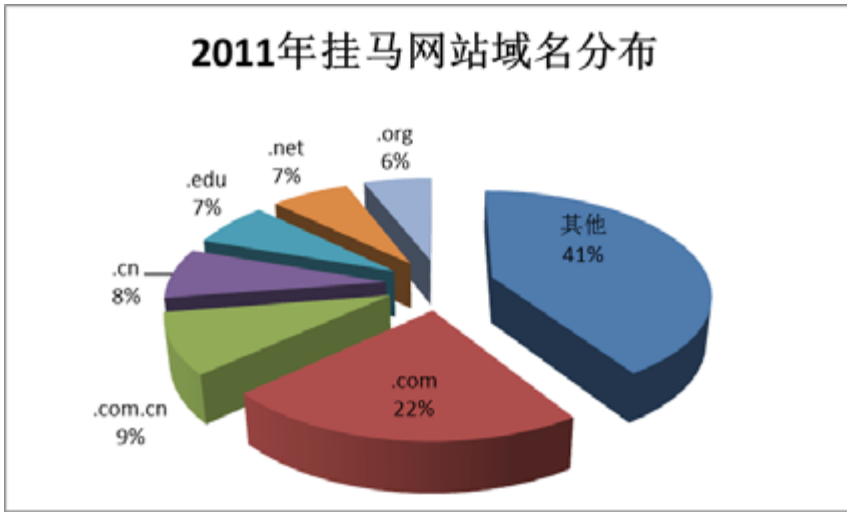

图 5　2011 年挂马网站域名分布

4.1.4. 2011 年十大被挂马最多网站排名

通过知道创宇互联网监控中心资料统计，得出 2011 年十大被挂马次数最多网站说明：一个网站在一定时间内（本文按 12 个月进行计算）被嵌入带有木马程序的恶意代码的次数总和，如表 1 所示。

表 1　2011 年年十大被挂马最多网站排名

网站	网站标题	ip	被挂马次数
www.china-indo.com	深圳市印都印刷器材有限公司	115.28.83.40	3390
www.alouhang.com	欧航铝业有限公司	59.36.99.19	3135
66w66.com	深圳市珍真实业有限公司	61.139.126.20	2595
media.ce.cn	中国经视--中国经济网	219.143.233.45	2490
www.znrs.cn	中年人生欢迎您！	218.240.43.69	2475
www.feitengdog.com	成都飞腾宠物	222.73.37.80	2280
sfe168.com	深圳市胜丰电子有限公司	58.215.76.171	2265
www.fec-edu.com	富源教育中心	114.112.59.58	2220
bus.xyqiye.com	公交车查询系统	202.102.233.199	2175
denisen.com.cn	德尼森 - 首页	211.144.136.88	2130

4.1.5. 2011 年主要流行挂马源分析

根据知道创宇互联网监控中心所得资料，列出 2011 年排名前十的挂马源。挂马源是指网马攻击代码所在的页面或 URL，恶意网络攻击多使用挂马源来进行对外挂马传播。根据挂马源传播的特点，可分为两类型。以 URL 挂马源为一类型；以 SITE（站点）挂马源为一类型。

URL 挂马源前十名见表 2。

表 2　URL 挂马源前十名

url 挂马源	传播次数	IP 地址	IP 所在地域
http://static.nimp.org/jews.wmv	535	80.65.228.132	法国
http://www.china-indo.com/en/superlink/Ajax.htm	485	202.106.195.30	北京市
http://www.china-indo.com/en/superlink/PPS.htm	422	202.106.195.30	北京市
http://www.china-indo.com/en/superlink/Bfyy.htm	383	202.106.195.30	北京市
http://static.nimp.org/lm.pdf	370	80.65.228.132	法国
http://cheaton9.com/tt13/06014.htm	348	61.63.42.77	台湾省
http://www.china-indo.com/en/superlink/vip.htm	252	202.106.195.30	北京市
http://flc.zjgsu.edu.cn/xi.htm	242	124.160.64.198	浙江省宁波
http://www.zjqykf.com/1/i1.htm	231	64.74.223.73	美国
http://www.znrs.cn/flash/ad/ec1.htm	222	218.240.43.69	北京市

SITE 挂马源前十名见表 3。

表 3 SITE 挂马源前十名

site 挂马源	传播次数	ip	ip 所在地域
down1.5ga.info	330	76.73.125.188	加拿大
ewang.jneol.com	272	203.148.15.187	北京市
up.spiritsoft.cn	248	117.79.94.164	北京市
allweb.com.cn	244	184.82.232.22	美国
blogtuzi.dyndns-blog.com	223	188.65.208.45	俄罗斯
officelbgp.dyndns-office.com	222	188.65.208.45	俄罗斯
officeityh.dyndns-office.com	218	78.159.100.253	德国
officejuzi.dyndns-office.com	217	78.159.100.253	德国
www.wuli-e.com	216	61.155.154.120	江苏省苏州市
officeuinw.dyndns-office.com	213	78.159.100.253	德国

分析：从表 2 和表 3 中可以看出来，国内以北京市为挂马源传播重点地区，特征显著，同时国外 IP 地址非常的多，这同时也表明国内监管的力度已经取得了非常明显的效果。当然，IP 地址本身会有误报的可能性存在，但如此多的 IP 地址都指向同一地域那么误报的可能性基本上可以排除。

4.2. 2011 年受挂马影响的系统与软件分析

4.2.1. 2011 年 Web 服务器软件应用总量以及被挂马数量

根据知道创宇互联网监控中心统计的资料，我们依据各网站所使用的服务器软件、常见 Web 应用等方面做了统计，如图 6 所示。

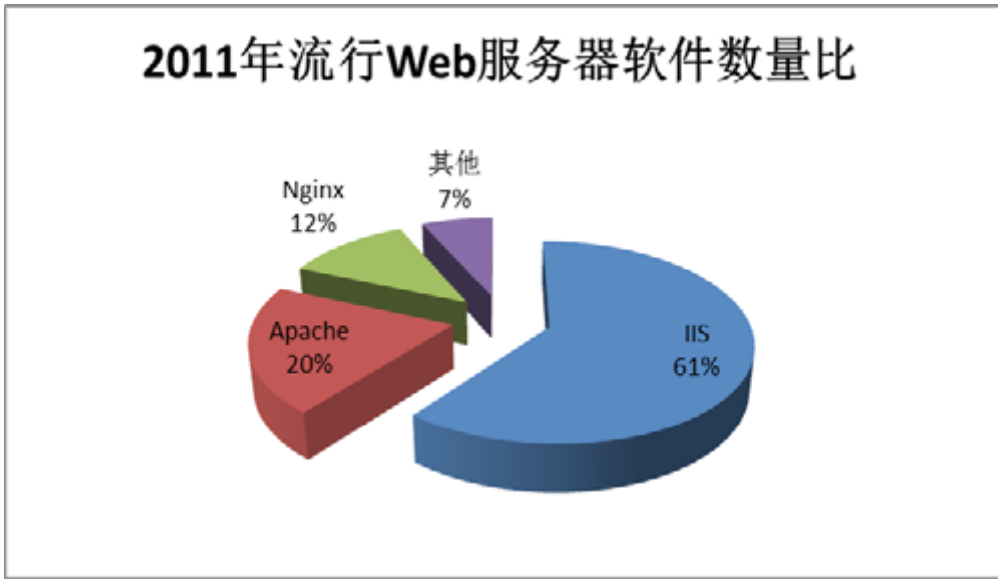

图 6 2011 年流行 Web 服务器软件数量比

根据统计到的十大服务器软件，我们对各自全年挂马数量亦做了统计，如图 7 所示。

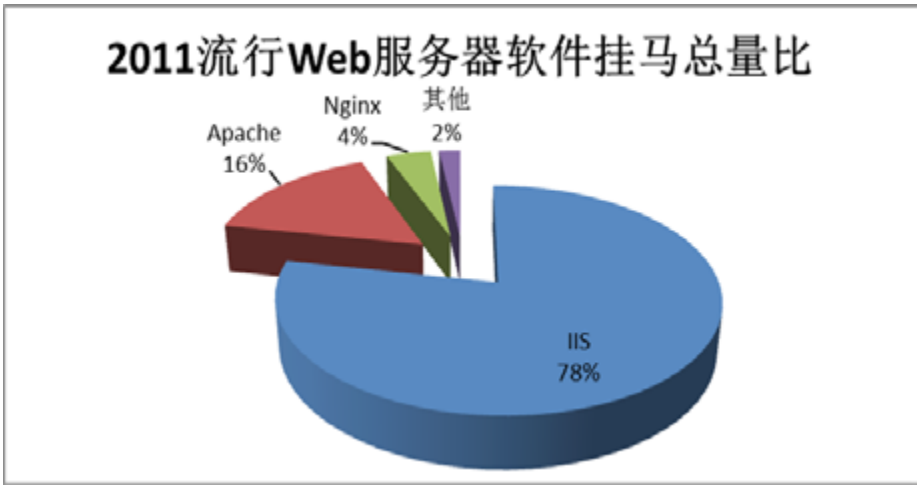

图 7 2011 流行 Web 服务器软件挂马总量比

根据各 Web 服务器的挂马情况，我们得出了各 Web 服务器的挂马比例

表 4 Web 服务器挂马比例

类型	使用数量	挂马数量	挂马比例
IIS	1343580	89867	6.7%
Apache	457520	18379	4%
Nginx	261583	4578	1.7%
Gnws	18402	13	0
Lighttp	33920	82	0
Resin	29152	66	0.2%
Bea weblogic server	17421	0	0
GFE	15967	0	0
IBM_HTTP_SERVER	25077	25	0
Tomcat	27192	31	0

从统计结果可以看出，无论从挂马数量，还是从挂马比例上来看，IIS 均已经成为最易受挂马影响的服务器软件。

4.2.2. 受挂马影响的开源 Web 应用

由于目前众多中小型网站选择使用开源 Web 应用做为首选建站，因此我们特别对目前知道创宇挂马监控平台所监控的 550 多万网站中可做出 Web 应用判断的网站，进行了安装数量、挂马情况等做出了统计，如表 5 和图 8 所示。

表 5 受挂马影响的开源 Web 统计

Web 应用名称	统计总数	挂马数量	挂马占比
Discuz!	89496	2318	2.5%
Phpwind	7892	66	0.08%
Wordpress	4968	789	0.15%
PHP168	896	56	0.63%
DEDECMS	654	23	0.03%
BBSMAX	233	5	0.02

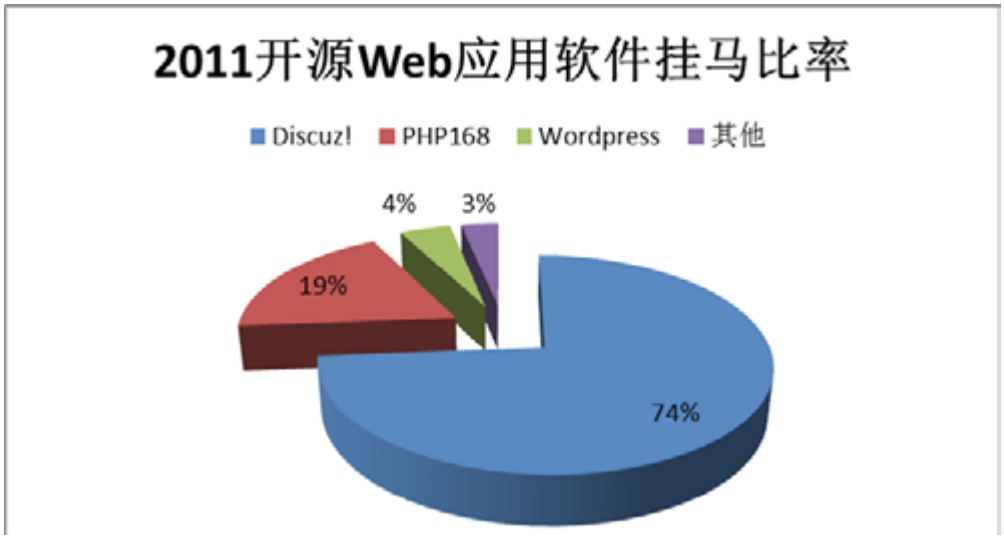

图 8 2011 开源 Web 应用软件挂马比率

由图 8 我们可以看出，在开源的 Web 应用中，Discuz! 所占市场份额较大，但同时挂马也最为严重。

5. 2011 年网站暗链情况综述

继 2010 年暗链攻击大规模爆发以来，众多网站深受其害，知道创宇在 2011 年对暗链攻击做了持续跟踪，根据知道创宇 2011 年以来对全国数百万互联网网站的暗链检测来看，2011 年，暗链攻击并没有停止，在没有受到普遍关注的情况下，被暗链攻击的网站数目急剧上升，2011 年 12 月较 1 月增长 76%，如图 9 所示。给受黑客攻击的网站植入暗链，已经成为黑客在攻陷网站后最常使用的方法了。

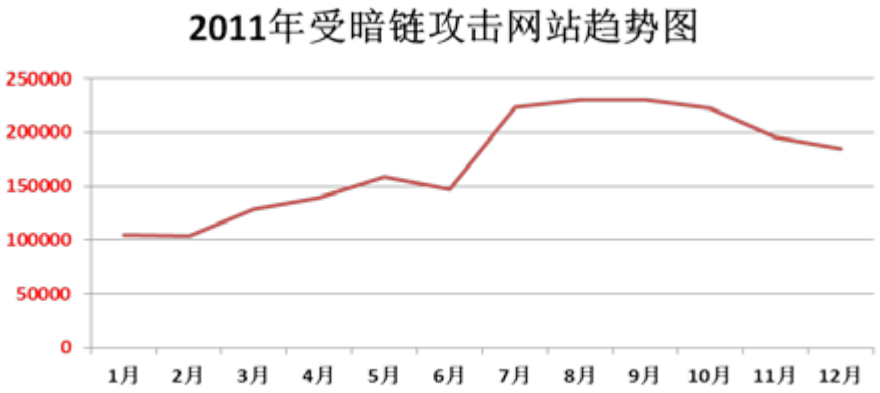

图 9　2011 年受暗链攻击网站趋势图

整个 2011 年，暗链网站数总的来说是持续上升的，其中在 7 月到 10 月达到本年度最高，暗链的隐藏性，是加剧这一增长的因素之一，正是由于常期不为网站管理人员所知，导致暗链能够长期潜伏在网站中，窃取网站访问量，而受暗链攻击的网站本身数据已经不再安全。

5.1. 2011 年暗链攻击类型分析

知道创宇网站安全检测中心对监控到的所有存在暗链植入的网站进行分析后，针对被植入的暗链接将暗链攻击进行了筛选和分类，统计出了 2011 年植入暗链的类型统计概况。我们将一些比较集中的暗链记录进行了分类，其中私服、医疗、博彩类成为 2011 年暗链攻击前三甲，而私服类网站的总量，接近于其它类型的总和，而医疗类本次名列第二，主要是医疗器械、医院等网站的链接，关键词主要集中在“医疗器械回收、糖尿病治疗、癌症治疗等”，如图 10 所示。

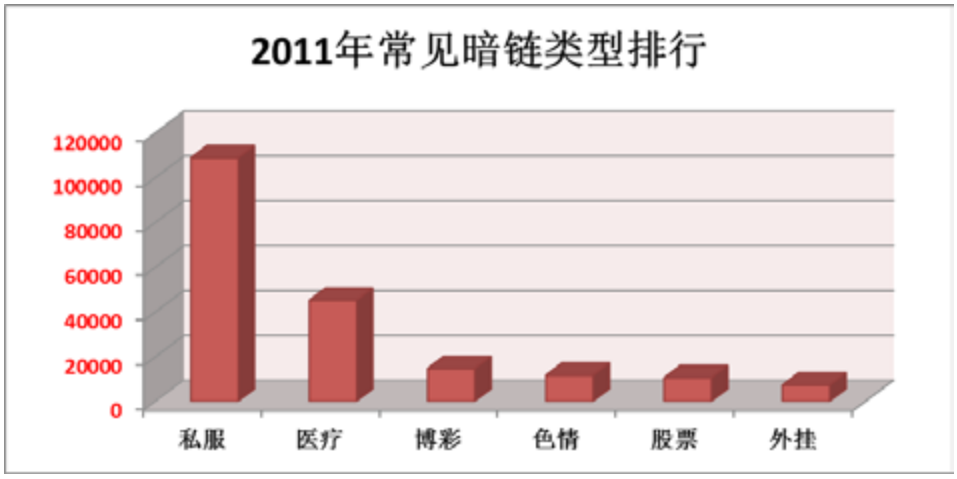

图 10　2011 年常见暗链类型排行

5.2. 2011 年各地区受暗链攻击网站统计

根据知道创宇数据网站安全检测中心监控到的数据，我们对监测到的暗链攻击情况按省份进行了分类，并总结出了各地区暗链数量前十名，数据如表 6 所示。

表 6　2011 年各地区受暗链攻击网站统计

地区	数量	较 2010 年上升
北京	112455	137%
上海	106896	184%
山东	34068	183%
浙江	30141	92%
广东	26979	199%
天津	25908	259%
四川	24582	68%
河北	23205	165%
河南	23103	-33%
江苏	22746	-34%

通过上面的统计我们可以看出，在 Top10 中，北京和上海再次成为暗链攻击的重灾区，这二个地区的受暗链攻击的网站数目是 Top10 中仅有的两个突破十万数量大关的地区，在增长率上，北京上海也非常突出。

5.3. 2011 年主要网站域名暗链分析

知道创宇数据网站安全检测中心，在对目前互联网应用中心主要的域名类型进行了暗链检测，并得出了 2011 年全年常见类型域名暗链情况。通过排名，我们可以看出，2011 年，仅从数量上来看，被植入暗链的网站数与各个域名的市场占有率相当，表 7 所示为是各个主要类型域名被植入暗链的数据。

表 7　2011 年主要网站域名暗链比率

域名类型	暗链网站数量	暗链率
.com	412549	17%
.cn	128320	14%
.net	48758	20%
.com.cn	45597	23%
.org	17582	17%
.gov.cn	29991	33%
.edu.cn	6396	32%

通过排名，我们可以看出，虽然在数量上暗链网站数量与域名市场占有率排名直接关系，但在暗链率上政府类网站与教育类网站成为受暗链攻击的重灾区，暗链率明显高于其他类型网站，经过知道创宇安全中心分析，造成

政府及教育部分暗链率普遍较高的原因可能是这类网站长期缺乏有效管理以及这类网站往往拥有较高的搜索引擎权重，以致于更容易被黑客所关注。

为了使结果更加明了清晰，我们将上面的统计制作成了柱状分布图，如图 11 所示。

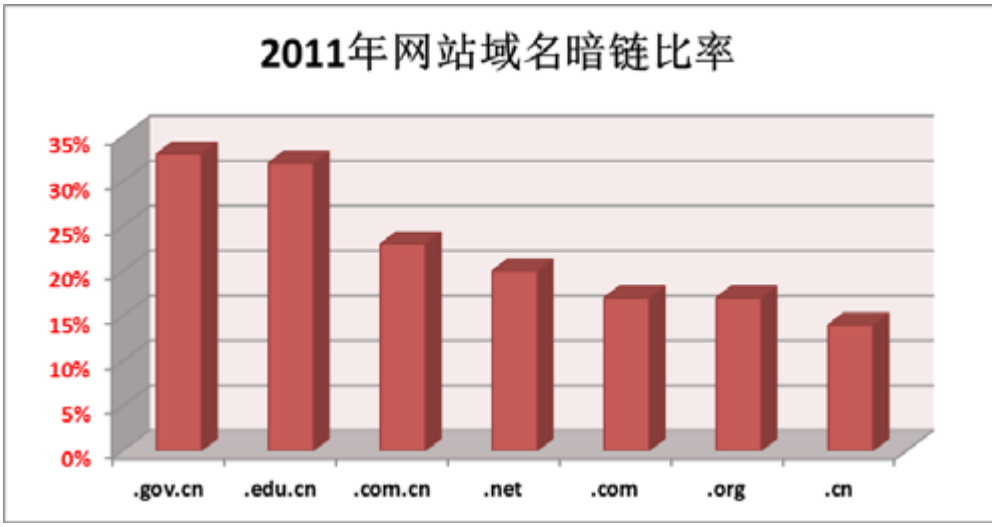

图 11　2011 年网站域名暗链比率

与往年相比，类型前三名中，仍然是 gov.cn、edu.cn、com.cn，不过名次上稍有变化，gov.cn 超越 edu.cn 成为本年度受暗链攻击最严重的网站类型。

5.4. 2011 年受暗链攻击十大重点网站

知道创宇安全中心在对 2011 年暗链数据进行统计过程中，我们发现很多大型网站同样成为暗链攻击的受害者，在此，我们特别筛选出一些影响力比较广泛的网站进行列举，以下排名无先后顺序，如表 8 所示。

表 8　2011 年受暗链攻击十大重点网站

站名	网址	暗链关键字
古城热线	www.xaonline.com	私服
北京大学科学传播中心	www.csc.pku.edu.cn	色情、博彩、私服
中国红十字基金会紧急救援基金	crcf.chinajjjy.gov.cn	私服、色情
中国人民银行--宜春市中心支行	pbc.yichun.gov.cn	私服、医疗
赛迪网博客	Blog.ccidnet.com	私服
宁波国家司法考试网	www.lzschool.org	彩票
核工业航测遥感中心	www.cn-arcn.com	私服
山西省电子商务协会	sxec.org.cn	刻章
大庆市人民政府网	www.daqing.gov.cn	二手车
中国国家地理网	www.dili360.com	双色球

5.5. Web 安全

历数 2011 年的泄密事件便会发现，这些泄密的站点中，十之八九是因为其前端 Web 的漏洞被利用，从而导致进一步的用户信息被窃取，这可以说是众多互联网产生用其惨痛的代驾给广大网民上了一课：Web 是不安全的！

而与此同时，还有一件看起来“不痛不痒”的事件却也让众多互联网企业见识了跨站脚本攻击[1]的威力，这就是新浪微博跨站脚本蠕虫事件。新浪微博对此次事件的响应速度很快，但影响用户仍然超过了 7 万，因此，这也引起了人们对 SNS（Social Networking Services，即社会性网络服务）站点的安全引发了普遍的关注和热议。

根据知道创宇 2011 年对部分授权网站长期安全跟踪检测得到的数据显示，2011 年全年存在漏洞的网站数量数量基本平稳，我们在将网站统计后，针对网站存在漏洞的安全性，得出以下分布。

5.5.1. 2011 年中国互联网网站安全情况分布

经过下图我们可以看出，65% 的网站存在不同程度的安全隐患，其中约 26% 的网站存在高危漏洞，极有可能被恶意网络攻击入侵。

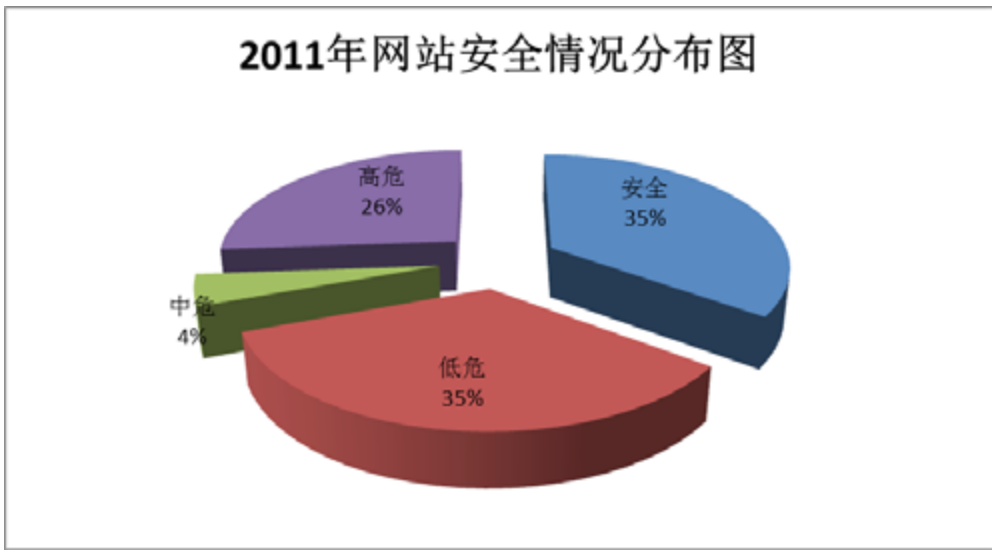

图 12 2011 年网站安全情况分布图

5.5.2. 2011 年网站漏洞类型分布

根据知道创宇安全中心统计到的数据，2011 年网站存在的漏洞最主要的仍是 XSS[1] 漏洞，几乎大多数被检测到漏洞的网站均不同程度存在 XSS 漏洞。

1. 跨站脚本攻击，缩写为 CSS (Cross Site Script)，但因为 CSS 的写法与级联样式表（Cascading Style Sheet）简写相同，因此常被简写为 XSS。

全球知名的开放式 Web 应用程序安全项目（OWASP，Open Web Application Security Project）每三年会统计出网络上流行的十大 WEB 安全隐（OWASP TOP 10），而 XSS 在最新的 OWASP TOP 10 中，XSS 排在第二位，仅次于注入攻击（Injection flaw）。

根据图 13 所示，我们不难看出，超过一半的网站不同程度存在 XSS 跨站漏洞，XSS 跨站漏洞最常见的利用方式就是被恶意网络攻击利用进行钓鱼挂马等，可见 XSS 漏洞不容忽视，而由于在 2011 年中，大多开源 Web 应用产品暴出漏洞，而大量网站未能及时更新补丁，导致应用漏洞占有不小的比例。

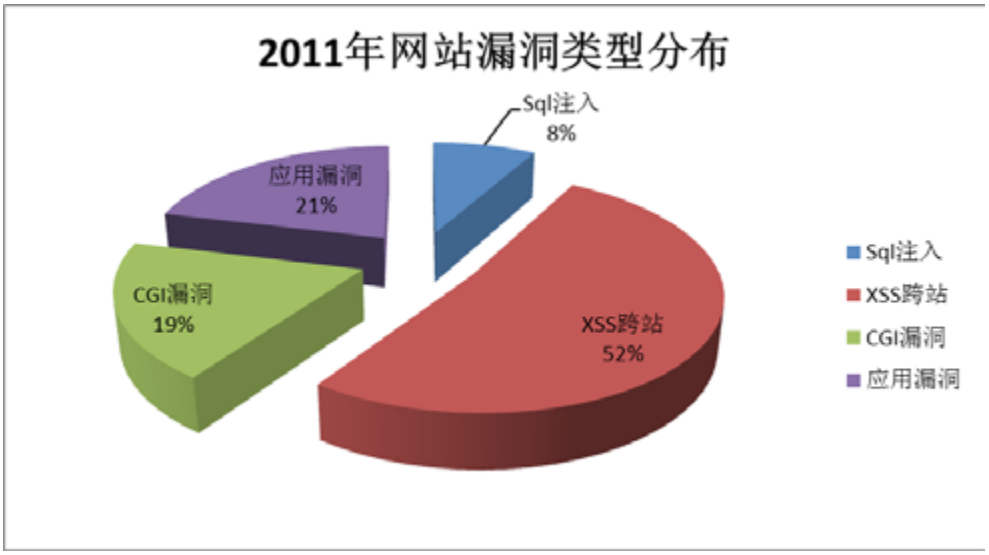

图 13　2011 年网站漏洞类型分布图

6. 2011 年安全大事记

在信息安全的道路上，每一年都是相似的，但每一年也都是不平凡的。

2011 年，对于信息安全来说，却尤为不同，因为在这一年里，电话里曾经一度的问候语都变成了 —— 你的密码改了吗?

这一年，有两个关键字是不得不提的：Anonymous、泄密。

6.1. 重大入侵事件

Anonymous 是什么?

这里的 Anonymous 不是 FTP 服务器的匿名登录账户名，而是一个松散的黑客组织，成立于 2003 年，声明大振于 2011 年，在这一年里，Anonymous 对索尼、HBGary Federal[3]、Facebook 等全球知名的公司实施了效果显著的一系列攻击，并且在攻击中多有收获到一些公司内部的敏感信息，甚至对某些内部系统获得了控制权限。

在此，我们就以 HBGary Federal 被入侵事件为起点，我们对 Anonymous 这个组织在 2011 年的一些大事记进行一个简单的梳理，以加强对这个组织的认识。

6.1.1. 2 月 入侵 HBGary Federal

由于 Anonymous 在 2010 年一系列的攻击和入侵行为，导致身为安全公司的 HBGary Federal 决定开始对该组织的成员进行调查，并将调查结果出售给相关的执法部门，因此，就导致了 Anonymous 对 HBGary 的入侵行动。

根据 Anonymous 自己对外公布的消息来看，这一次入侵行动以 SQL 注入作为开端，通过注入过程中获取到了一些散乱的信息，随后，通过一些列举的技术和非技术手段（如：社会工程学），最终获取了 HBGary CEO 的账户密码。

6.1.2. 4 月 攻击并入侵索尼 PSN

目前，PSN 被攻击及入侵事件是否由 Anonymous 所为，并无确切的定论。

这一事件起始于 4 月中下旬，首先是有不明身份的黑客对索尼 PSN（PlayStation Network）发起攻击，导致索尼关闭 PSN 服务，而在随后几天内，索尼又发现有黑客入侵了 Station.com 网站，这次入侵导致接近 1 亿的用户信息被窃取。

在事件发生后，索尼宣称此次事件为 Anonymous 所为，原因是索尼的技术人员在他们的服务器上发现了一个名为 Anonymous 的文件，文件里面写有“We are Legion”的字样。

而 Anonymous 对索尼所发布的消息也做了响应的回复：Anonymous 没有参与本次事件。

但是，在事件三周后，在索尼还无法提供正常服务的情况下，Anonymous 再次发布声明，宣称“未策划本次事件，但不排除是团队内成员的个人行为”。

6.1.3. 6 月 攻击 Policia.es

Policia.es 是西班牙的国家警察官方站点，Anonymous 组织在 6 月份的时候对该站点发起了攻击，迫使该站点下线。

Anonymous 宣称，这次攻击是因为西班牙警方逮捕了攻击索尼网站的嫌疑犯 —— 但这和之前 Anonymous 所发表的“未参与攻击索尼的行动”又有所冲突，而结合 12 月份 Anonymous 以“索尼支持 SOPA（禁止网络盗版法案）”为由对索尼发出威胁一事来看，多数人还是怀疑 Anonymous 早先确实参与了对索尼的一系列攻击和入侵行动的。

6.1.4. 7 月 入侵 Mantech International

ManTech 是一家提供信息系统、国防和航天技术方面解决方案的供应商，同时，ManTech 也是美国军方的服务提供商。

在 7 底，Anonymous 发布消息称“已经攻破 ManTech 网站”，并在其 Twitter 上公布了来自该公司的机密信息，而 ManTech 方面则对此事拒绝发表任何评论。

6.1.5. 8 月 攻击 BART

BART（Bay Area Rapid Transit，旧金山湾区捷运系统）是美国旧金山湾区捷运局经营的有轨大众捷运交通系统，

行驶线路涵盖旧金山湾区的大部分区域，主要用于解决旧金山湾区内各城市之间的运输需求。

在 7 月份，BART 警察曾向无家可归的流浪汉开枪射击，而由此引起民众示威，在示威中，BART 曾关闭旧金山四个地铁站内的手机基站信号以阻止示威。

在 8 月份，Anonymous 为对此事做出报复，发起了对 BART 的攻击行动，攻击行动中，Anonymous 篡改了 BART 对乘客提供服务的站点 myBART.org，从而迫使其下线。随后，Anonymous 还对 BART 的上级部门加州交通安全办公室发起了攻击。

6.1.6. 10 月 视频威胁墨西哥贩毒组织 Los Zetas

在 10 月份，Anonymous 在网络上发布视频威胁 Los Zetas —— 宣称 Zetas 若不释放在上个月绑架的 Anonymous 成员，将于 11 月 5 日开始对外逐步公布其组织的人员名单等信息，而这些信息主要来源于几个月前 Anonymous 破解的上万封邮件，这些邮件里包含了很多政府公务人员和墨西哥毒贩之间的交易信息。

视频发布后，立刻传遍网络，而 Los Zetas 也在 11 月 4 日释放了被绑架的成员。

6.1.7. 宣称 11 月 5 日对 Facebook 发起攻击

Anonymous 在 2011 年 8 月份曾发布声明称，将于 11 月 5 日对 Facebook 发起攻击。

因为该组织认为“Facebook 向政府机构出售信息，并使信息安全公司获得这些信息，帮助他们刺探全球用户”。但在该威胁被发布不久之后，Anonymous 成员又发布了截然相反的信息，宣称此次发布威胁只是为了引起网民对 Facebook 收集个人信息行为的关注，但却因某些原因导致计划改变，而放弃了此次攻击，对 Facebook 来说可谓虚惊一场。

6.1.8. 12 月 窃取美国安全智库 STRATFOR 资料

安全问题一直是美国安全智库 Stratfor 的主要研究领域，而颇具讽刺意味的是，在 2011 年的圣诞节期间，Anonymous 宣称已成功入侵该公司的系统，并获取了 Stratfor 大量的客户信息，其中也包括信用卡信息。Anonymous 成员说，之所以会对该公司发起攻击，为了“借用”公司客户的资金，用做圣诞捐款。而就在当天，一些 Stratfor 的客户证实，他们的信用卡出现了不明的转账。

但这并不是结束，而只是开始。在随后的几小时，Anonymous 在网络上公布了约 7.5 万名客户的信息，包括：客户姓名、电话、邮件、地址和信用卡信息。

而 Anonymous 的发言人称，他们的目标是 Stratfor 内部超过 300 万封的电子邮件，但目前这些邮件尚未被公布，因此外界也无法确认 Anonymous 是否已达到其目的。

6.2. 信息泄密事件

泄密对互联网来说已经是稀松平常的事情了，我们每天都能接到不同的类型的“骚扰”电话和短信，这正是泄密所带来的影响。但是，在 2011 年的年末，CSDN 却将泄密推向了一个新的巅峰 —— 以至于一时间，就连公交车上的问候语也都变成而来“你改密码了吗？”。

2011 年的泄密虽由 CSDN 事件而大噪，但这仅仅是这一年中泄密事件的冰山一角，在这一年里，索尼、花旗银行、百思买，就连专业安全公司 RSA 也遭受了 APT（高持续性渗透攻击）而导致大量的数据被窃。

6.2.1. 索尼，7700 万

索尼绝不会是 2011 年最先被入侵并丢失数据的厂商，但索尼的大名加上 7700 万的泄密数量，绝对是 2011 年的一个标志性事件，而正是这样的一个事件，也更多的吸引了普通民众对互联网安全的关注。

6.2.2. Epsilon，殃及池鱼

营销公司 Epsilon 的数据有 2% 失窃，其中包括大量的私人敏感信息，涉及到了 Walgreens、百思买、摩根大通、Kroger 连锁超市等。

关于这次失窃事件，Epsilon 并没有过多的细节。

6.2.3. 花旗银行，36 万信用卡数据

花旗集团承认有黑客侵入并有超过 36 万用户的信用卡数据被黑客盗取。这起黑客入侵事件为花旗集团造成了 270 万美元的损失。

6.2.4. RSA 资料被窃

RSA 是双因素身份验证的领航者，但是在 2011 年，RSA 也未能幸免。

RSA 在 3 月份遭受了 APT（高持续性渗透攻击）攻击后，其 SecureID 产品的相关资料被窃。而在不久后，有使用 SecureID 的用户反馈称“遭受黑客攻击”，因此有人怀疑在 RSA 被窃资料中可能包含其 SecureID 的种子文件。

6.2.5. CSDN，600 万用户密码

2011 年虽然国内外出现很多的数据失窃事件，但并未引起国内网友的普遍重视，而就再大家认为将要平静的度过 2011 年之际，在 12 月底，网络上突然有爆料称“CSDN 数据被窃，丢失用户数据 600 万，其中包含用户的明文密码”，在消息出现后，即有网站提供了这 600 万用户数据的下载，并且经大部分网友证实了这些数据的真实性。

一时间，问候用于都变成了“你改密码了吗？”，但是，这仅仅是一个开始。

6.2.6. 天涯社区，4000 万用户密码

CSDN 的 600 万密码锁带来的愁云惨雾还未消去，天涯社区却紧随其后。

网络上曝出的天涯社区 4000 万带有用户邮箱和明文密码的数据后不久，天涯官网对此进行了证实，官方称，被窃取的明文密码均为 2009 年的备份数据，天涯社区的密码在 2010 后改为加密存储。

天涯社区注册用户在 6000 万左右，此次失窃的数据超过其总用户数量的 60%。

6.2.7. 京东用户资料泄露

12 月 27，乌云平台上报告京东站点上存在用户权限控制不严格而导致任意用户登录后，可访问任意其他用户的信息，这些信息包括：姓名、地址、电话和 E-Mail 等。

京东以较快的速度响应了该漏洞，但仍有网友在网上发布消息称“京东泄密用户资料导致我的京　被盗”。

6.2.8. 当当网，数据不详

京东漏洞曝出第二天后，网络上即流出“当当网 1200 万用户数据”，但当当官方回应称，这些数据只有极小部分属实。

北京知道创宇信息技术有限公司 www.knownsec.com

O +86 (10) 51295887
F +86 (10) 52723966
E sec@knownsec.com
w weibo.com/knownsec
A 北京市海淀区蓝靛厂南路55号金威大厦803室 100097
香港德辅道中173号南丰大厦1609D2室