深信服智安全
SANGFOR SECURITY

2016 年安全威胁分析报告

深信服智安全 • 千里目安全实验室

2017 年 1 月 3 日

目 录

一、2016 年安全威胁总体概述

经研究分析， 2016 年安全威胁的整体态势相比 2015 年更加严峻，总体情况如下：

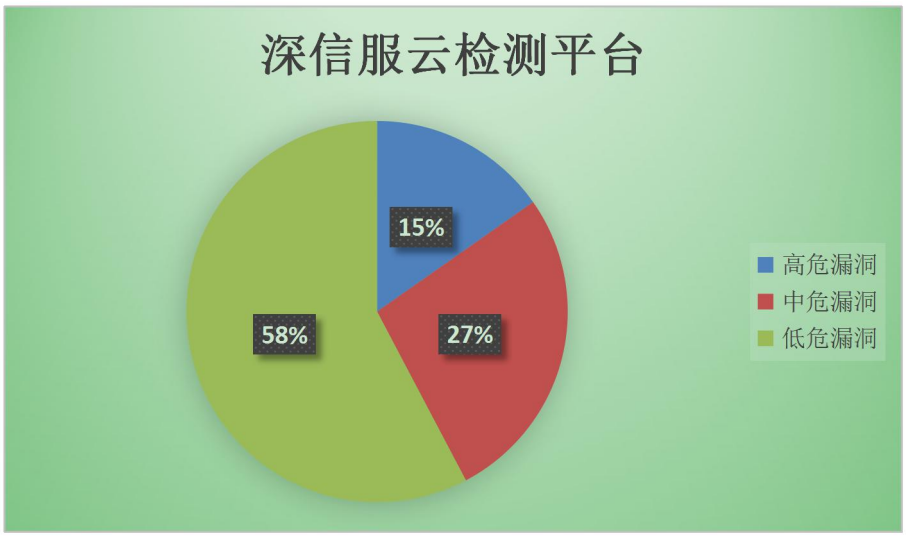
- 国内网站安全情况不容乐观，75.7%的网站存在安全漏洞。政府网站有 89.6%存在漏洞，在所有行业分类中漏洞比例最高
- XSS 注入漏洞和 SQL 注入漏洞在所有漏洞类型中占比最高；同一地区的区县政府和中小学网站更喜欢使用相同建站框架，安全风险极高
- 大型企业对网站安全关注度最高，平均漏洞修复时期为 10 天，政府方面对网站安全关注度最低，平均漏洞修复时期为 3 个月，最长达 1 年以上
- 2016 年发现并拦截网站攻击 56.36 亿次，其中 DDoS 攻击次数最多，占总攻击量的 27.7%；来自广东地区的攻击流量最高，占总攻击量的 23%
- 2016 年发现网站安全事件 10.6 万起，网站仿冒钓鱼事件最多，占总事件的 46%
- 2016 年共监测到恶意程序感染主机/服务器 IP 有 156898 个，其中受僵尸网络感染最多，占总感染数 37.6%

二、网站安全监测情况

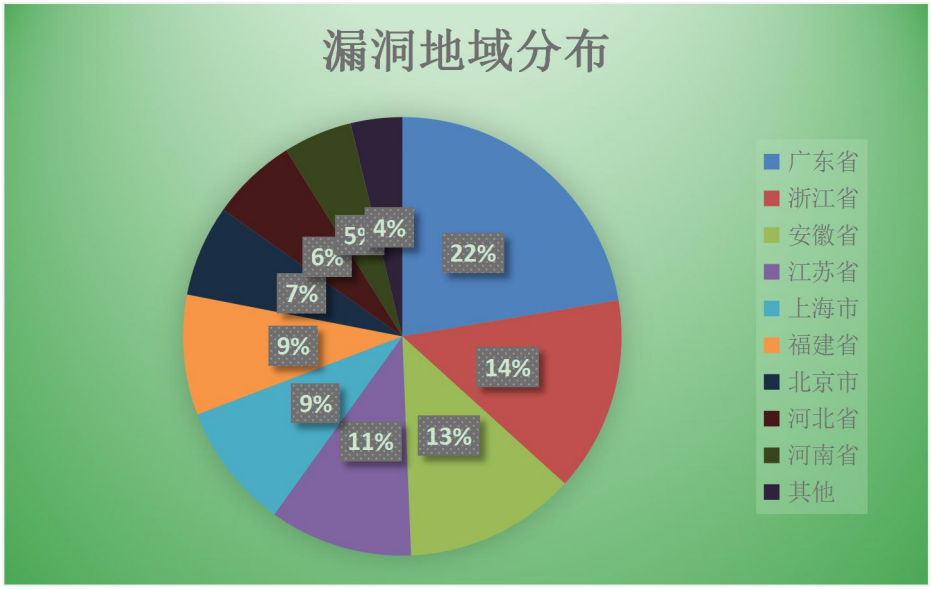
1. 网站漏洞整体解读

2016 年（1 月 1 日到 12 月 25 日），千里目云检测平台对全国 14 个取样省份 25.9 万网站进行授权安全检测，其中有 19.6 万个网站存在安全漏洞，占总检测网站的 75.7%。相比 2015 年增长 45.2%。

在 25.9 万取样网站中，共发现 50.3 万个漏洞，在所有漏洞风险等级中，高危漏洞有 9.2 万个，占漏洞总数的 15.2%，具体分布如下图：

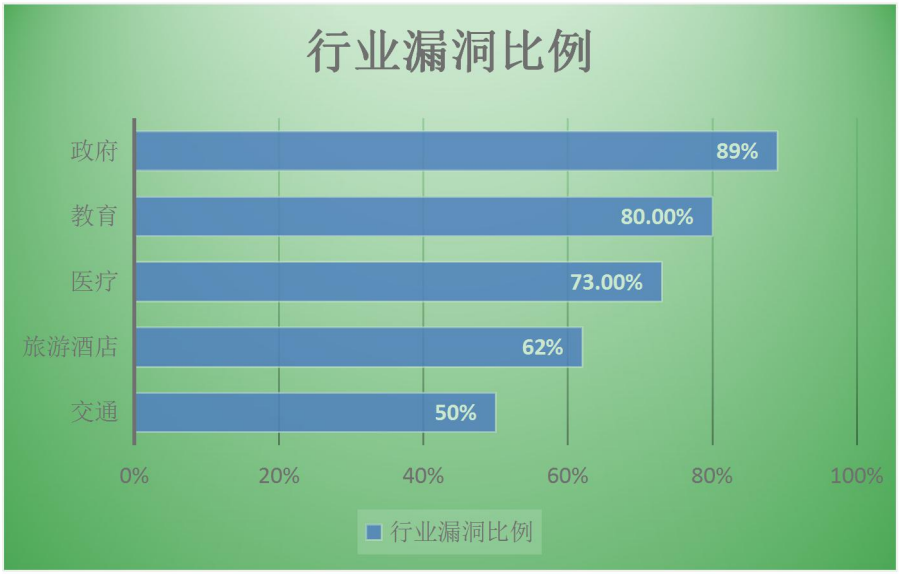


在本次 14 省漏洞检测过程中，广东省网站共监测到漏洞有 11 万个，占总漏洞数 22%，在全国范围内网站安全隐患最高，下面给出所有地区漏洞占比情况，如下图所示：



2. 网站漏洞行业分析

本次进行安全检测的 25.9 万个网站涉及各行各业，其中，存在漏洞比例最高的是政府类网站，其次是教育行业和医疗行业。漏洞占比最高的行业 TOP5 统计如下图：



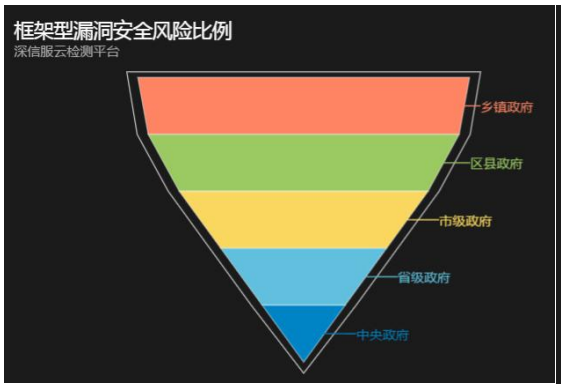
上图可以看出，政府、教育、医疗、酒店等行业的网站系统安全意识较为薄弱，网站运维人员大多数不具备专业的安全能力，导致网站安全事故频发。政府、教育、医疗等又是掌握各类敏感信息的重要行业，网站安全整体状况急需整改。

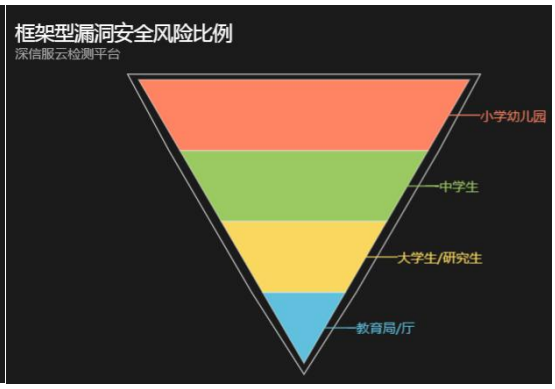
3. 网站漏洞类型分析

在研究过程中，我们发现数量占比最大的漏洞是 XSS 注入、SQL 注入等漏洞。以下是危害网站安全的漏洞 TOP10：

不同类型的漏洞对网站影响不同，XXS 注入漏洞是跨站脚本漏洞的简称，此漏洞在本年度所有网站安全漏洞中占比最高，黑客可利用该漏洞在网页中插入任意恶意代码，以达到盗取用户 Cookie、隐蔽运行网页木马等目的。

本年度安全漏洞统计中，共发现框架通用型漏洞 523 个，涉及重要框架 159 个，受影响网站多达 3263 个。框架型通用漏洞具有影响范围广、破坏性强等特点。框架通用型漏洞在政府类网站与教育类网站中应用最为广泛，如下图所示：





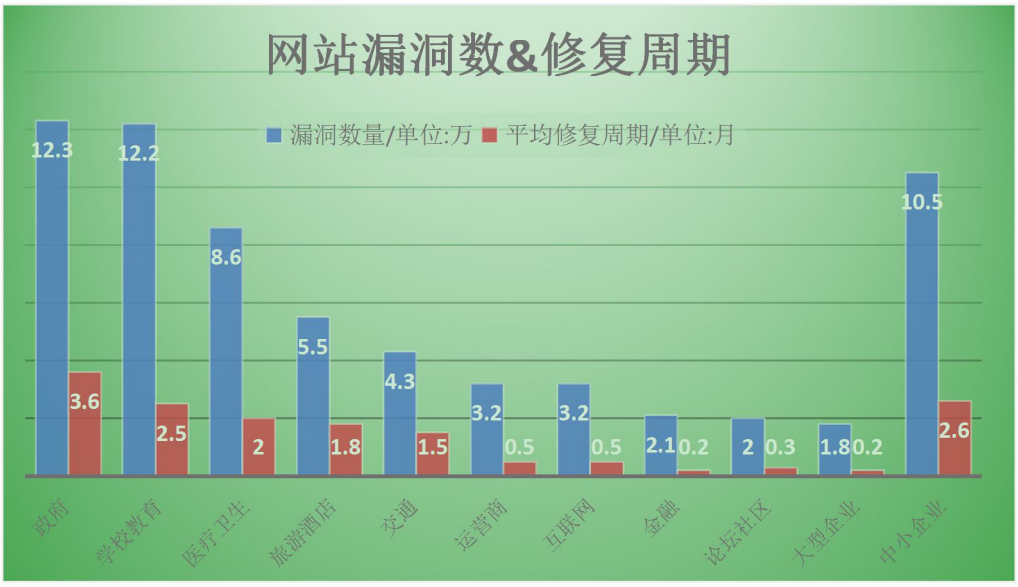
通过上图可发现，政府类网站中，区县及乡镇政府使用不安全框架较多，而更高行政级别的政府类网站使用框架型建站较少，安全风险相对较低。教育类网站中，中小学、幼儿园使用不安全框架较多，大学、教育厅等使用较少，风险明显较低。

此外，我们在网站安全检测过程中还发现，区县、乡镇政府网站、中小学幼儿园网站不仅偏爱使用同一套建站系统，而且为了节约成本、方便管理，还经常将网站搭建在同一个服务器上。2016 年各地政府逐渐推行政务云项目，将网站迁移到云上，区县、乡镇政府网站建设出现更多共用服务器的情况。如果其中一个网站被成功入侵，将影响同一个服务器上的所有网站。因此，网站分级管理，风险平摊，降低整体安全隐患，是区县乡镇政府以及中小学网站整改的重要方向。

4. 网站漏洞修复周期

千里目云监控平台对所有存在漏洞的网站同时进行一年以上安全监控，在此过程中发现，

大型企业对网站安全的关注度最高，从通知到修复平均用时 10 天左右。区县、乡镇政府对网站安全关注度最低，平均用时 3 个月以上，最长时间多达 12 月以上。以下是各行业漏洞爆发及平均漏洞修复周期图：



从上图可以看出，政府、学校教育、中小型企业网站安全与漏洞修复效率双低，急需提高安全意识，保障网络安全。造成网站修复率底的原因除了管理员安全意识不足外，还有以下几点：

（1）用户单位没有专业安全人员，不具备修补安全漏洞的能力；

（2）第三方厂商担心影响公司荣誉，有意忽略漏洞，不发布安全补丁；

（3）缺乏统一漏洞推送机制，网站发布安全补丁或者升级服务很多都会直接在官网发布，而不会定向推送给网站使用者；

（4）开发者定制开发的网站系统难以与发布的安全补丁相匹配，影响网站修复速度。

三、网站攻击流量分析

1. 网站攻击整体解读

2016 年（1 月 1 日到 12 月 25 日），深信服安全防护设备共发现并拦截攻击 56.36 亿次，平均每天拦截攻击 1544.1 万次。其中 8 月攻击流量达到最大值，每天拦截攻击多达 3966.7 万次，如下图所示：

从被攻击网站的数量来看，2016 年共有 77.9 万使用深信服防护设备的网站遭遇网络攻击，平均每月有 6.4 万网站受到攻击。其中 9 月是网络攻击最频繁的一个月，平均每天有 4278 个网站遭到攻击，具体统计图如下：

从上图可以看出，无论是总体攻击流量，还是受攻击的网站数，都在 7-9 月达到顶峰。此期间正值我国在杭州举办 G20 峰会，互联网调查也显示，峰会期间多数网站尤其是政府网站频繁受到攻击。

习近平总书记提出“没有网络安全，就没有国家安全”。事实上，网络攻击活动与国家政治动态也有着直接关联性，网络安全已经全面上升到国家战略层面。

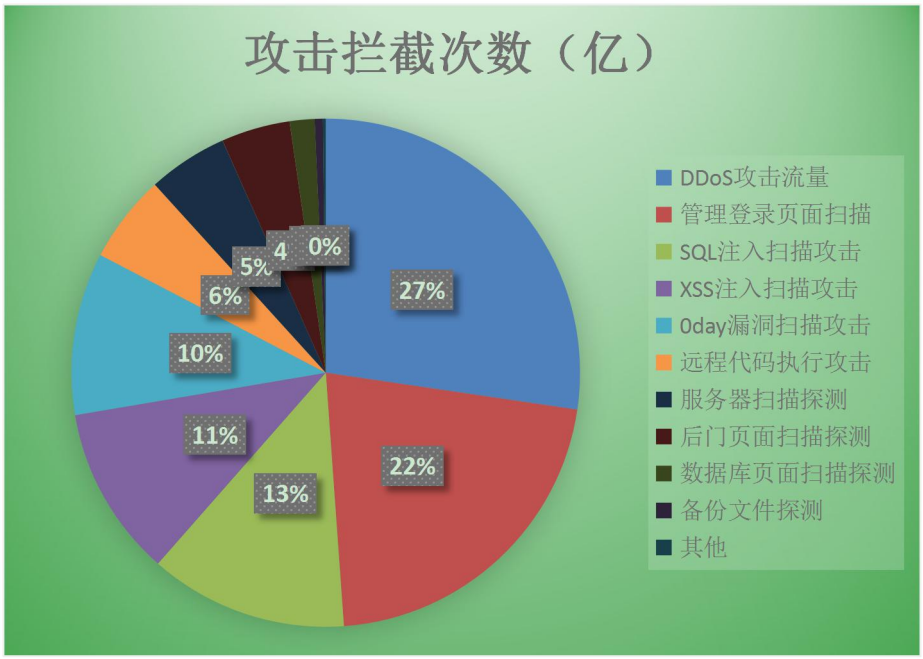
2. 网站攻击特征分析

我们通过对 56.36 亿次拦截的攻击流量进行特征分析发现，大部分攻击流量为自动化探测工具发送，其中常见的 Web 漏洞、服务器漏洞、0Day 漏洞扫描探测、管理登录页面、后门页面、数据库页面爬取以及 DDoS 攻击流量占比最高，各类攻击拦截次数

TOP10 如下图所示：

排名	攻击类型	拦截次数（单位：亿）
1	DDoS 攻击	15.6
2	管理登录页面扫描	12.3
3	SQL 注入扫描攻击	7.2
4	XSS 注入扫描攻击	6.2
5	0Day 漏洞扫描攻击	5.9
6	远程代码执行攻击	3.2
7	服务器扫描探测	2.9
8	后门页面扫描探测	2.5
9	数据库页面扫描探测	0.9
10	备份文件探测	0.3

其中攻击拦截类型分布占比情况如下图所示：

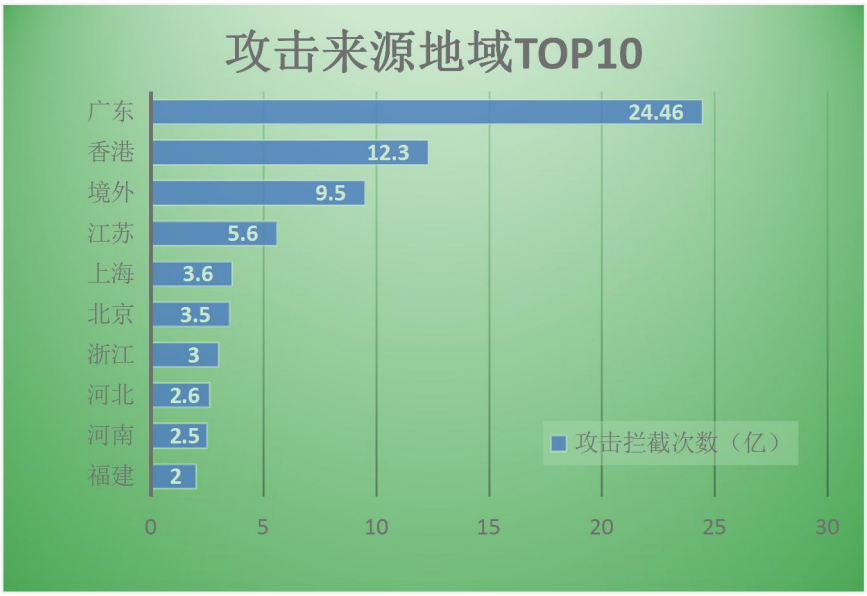


经研究发现，高居首位的 DDoS 攻击可用自动化程序瞬间发动成千上万肉鸡对目标进行攻击，攻击成本极小，但是对被攻击的目标来说，轻则与外界通信不畅，服务无法及时响应，重则造成宕机等严重后果。排名第二的管理登录页面扫描攻击是黑客常用的攻击方式，几乎所有扫描工具都会对管理页面进行探测，以达到暴力破解获取系统权限的目的。

如今市面上种类繁多的自动化攻击工具，极大的降低了攻击成本，技术能力较差的人员也能够使用自动化工具对网站进行扫描或其他攻击。自动化攻击或探测工具是目前网络攻击流量的最主要来源。

3. 网站攻击流量来源分析

千里目安全实验室对所有攻击 IP 进行统计，发现广东地区是攻击流量的主要直接来源地， 达到 24.46 亿次，占总攻击流量的 23%。其次是香港和境外（美国、日本等地）。攻击流量来源地 TOP10 如下图所示：



其中针对境外攻击流量，目前国内有效的追踪手段较为缺乏，因此，通过国外流量进行攻击备受黑客青睐。经研究，境外攻击流量的原因有两点，一是国内攻击有意使用境外 IP 做跳板，逃避电子取证法律追究；二是来自境外有组织有计划的攻击行动。无论哪种原因，都对我国网络安全造成严重威胁。

4. 网站攻击行业特点分析

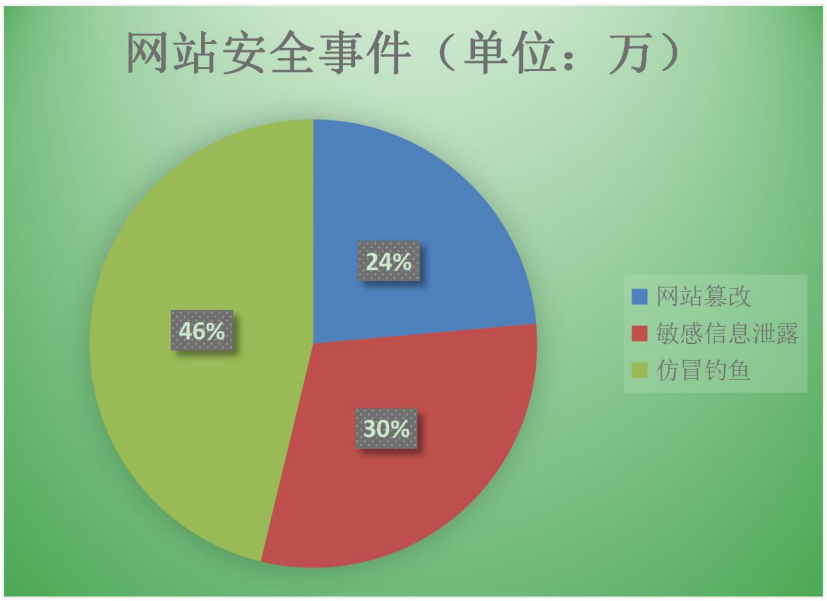
从深信服安全防护设备拦截的攻击来看，金融、医疗、教育行业的网站是平均被攻击次数最多的网站类型。一般来说，一个网站遭遇的攻击量越大，也就意味着网站对攻击者价值越高，下图是各行业网站 2016 年全年遭遇网络攻击的情况：

从上图可以看出，掌握大量敏感信息的网站备受黑客青睐，恶意攻击者可以对网站数据进行盗取后贩卖获取利益或直接对受害者进行诈骗获利。因此，掌握更多重要信息的行业更应该重视网站安全防护。

四、网站安全事件分析

1. 网站安全事件整体分析

2016 年（1 月 1 日到 12 月 25 日），千里目云检测平台共检测到网站安全事件 10.6 万起，其中包括网站篡改事件 2.5 万起，敏感信息泄露事件 3.2 万起，网站仿冒钓鱼事件 4.9 万起。整体分布图如下：

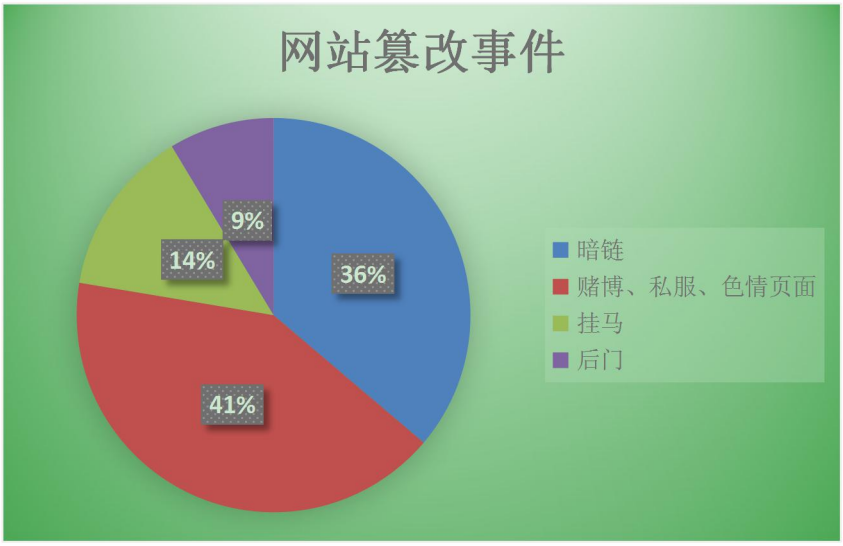


从每月监测情况来看，11 月数量最多，其次是 6 月和 1 月，每月检测出的网站事件统计图如下所示：

从上图可以看出，我国农历春节前期（11 月到 1 月）是网站安全事件高发期，也是不法分子的活跃期，这与现实生活中的生存环境的安全态势成正比，可以说，网络安全已深入到生活中的方方面面，网络安全也成为生命财产安全的一部分。

2. 网站篡改事件分析

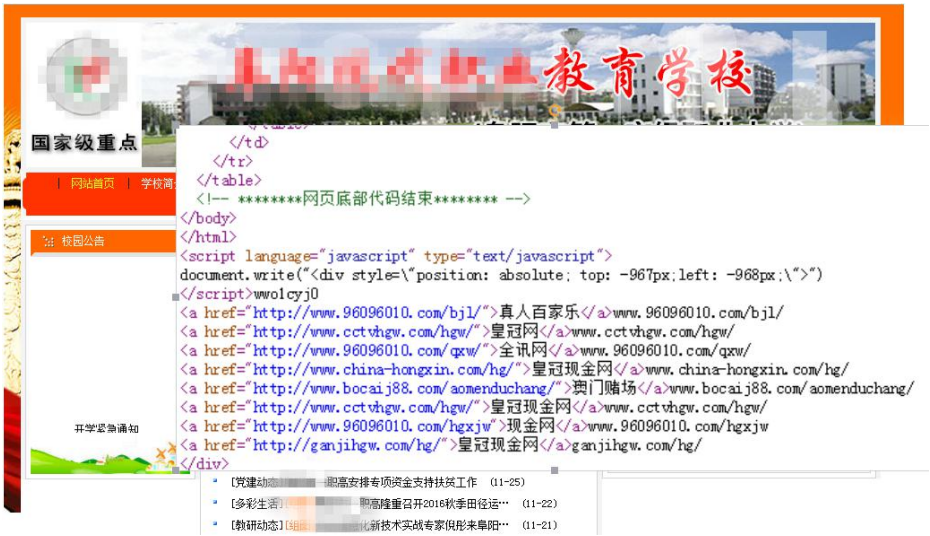
黑客成功入侵网站后，会对网站源码进行恶意篡改，这些篡改主要包含网站暗链植入，赌博、私服、色情页面植入，网站挂马，植入后门等来获取利益。所有网站篡改类别所占比例如下图所示：



- **网站暗链篡改**

暗链，即看不见的链接，是网站篡改的基本形式。暗链在网站中的链接做的非常隐蔽，不易被肉眼发现，但是它和网站友情链接相似容易被搜索引擎索引，所以可以有效的提高搜索权重值。提高网站搜索权重值即大大增加网站在搜索引擎中的排名。下面是典型的暗链植入页面：

某学校官网，从表面上看无任何异常，但是点击查看源码功能会发现大量与页面无关的内容，这些内容有“赌博”、“百家乐”、“皇冠现金网”等，如下图：



- **赌博、色情、私服页面植入**

同样用于提高网站权重值，增加网站知名度，赌博、色情、私服页面植入篡改就显得直接的多。以政府网站为例，在搜索引擎中就可以直接找到大量被篡改的页面，如下图：

打开其中一个页面，已被深信服上网行为管理拦截，但仍然能够看到其他恶意悬浮广告信息，如下图：

- **网页挂马**

黑客入侵网站后，通常会在网页中植入木马，又称“网马”。网马主要指把一个木马程序嵌入网页，所有浏览此网页的用户直接被下载并安装木马，从而电脑受到黑客控制。

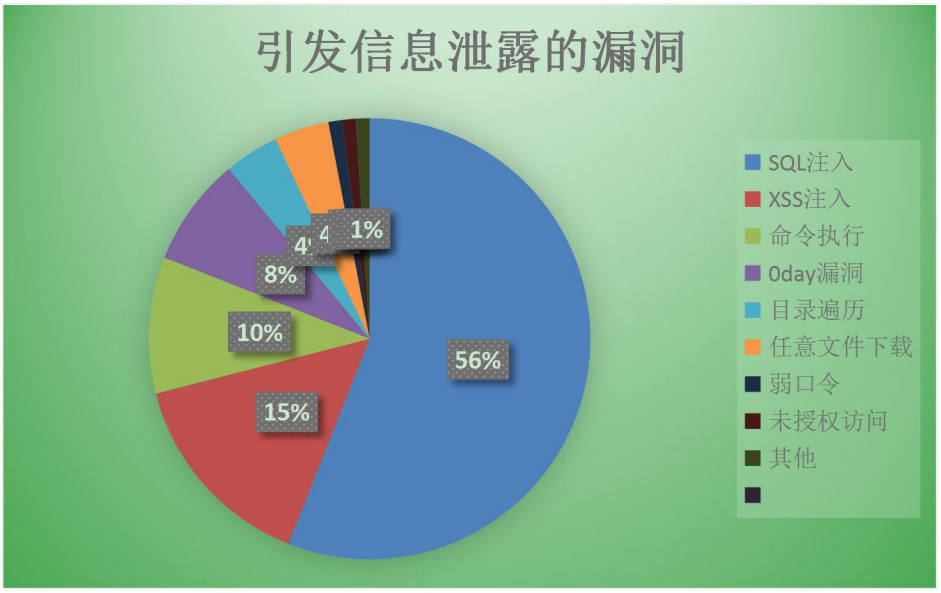
- **网站后门**

网站后门也是网站木马的一种，之所以称之为后门，主要是黑客为了悄悄控制网站而留下的木马，后门一般设有密码，防止被别的黑客使用自己留下的木马。但是黑客通常留下的密码都非常简单，其中 cmd、123 等密码出现频率极高。

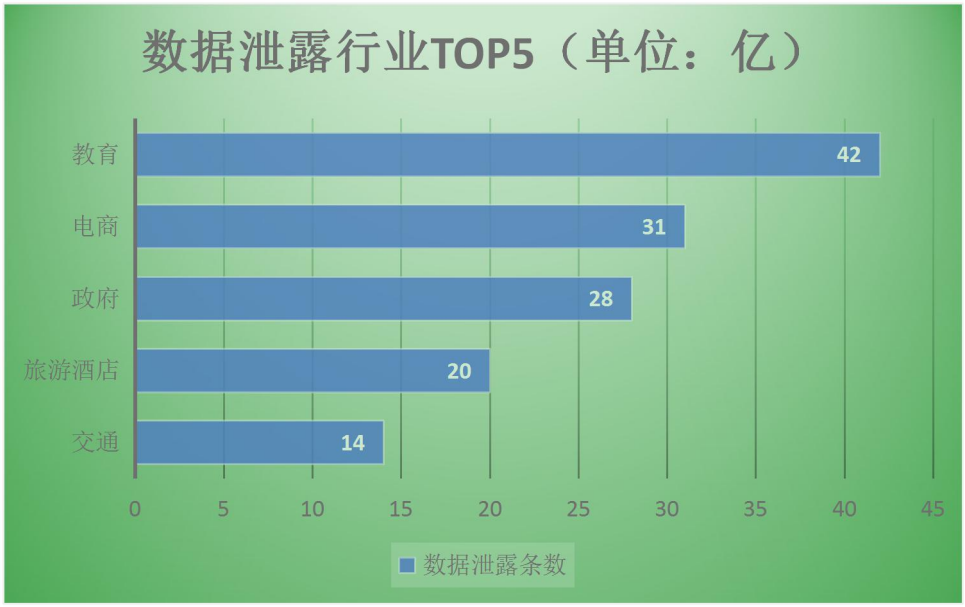
3. 网站敏感信息泄露事件分析

今年 8 月，山东准大学生徐玉玉事件就是典型的网站敏感信息泄露造成的诈骗案件。在此案件中 18 岁黑客杜天禹坦言:“网站存在漏洞,我通过上传木马下载 60 万考生信息获利”。

2016 年，千里目云检测平台统计发现由各类漏洞引发的网站敏感信息泄露事件共计 3.2 万起，其中 SQL 注入引发的数据泄露高达 56%，其次是 XSS 注入，命令执行等。引发网站敏感信息泄露的漏洞比例统计如下图所示：



通过对数据泄露行业进行分析对比发现，教育行业是黑客首选目标网站，全年发生数据泄露事件 42 亿条，其次是电商行业和政府行业，分别是 31 亿条、28 亿条（数据来源于互联网公开数据）。信息泄露行业 TOP5 如下图所示：



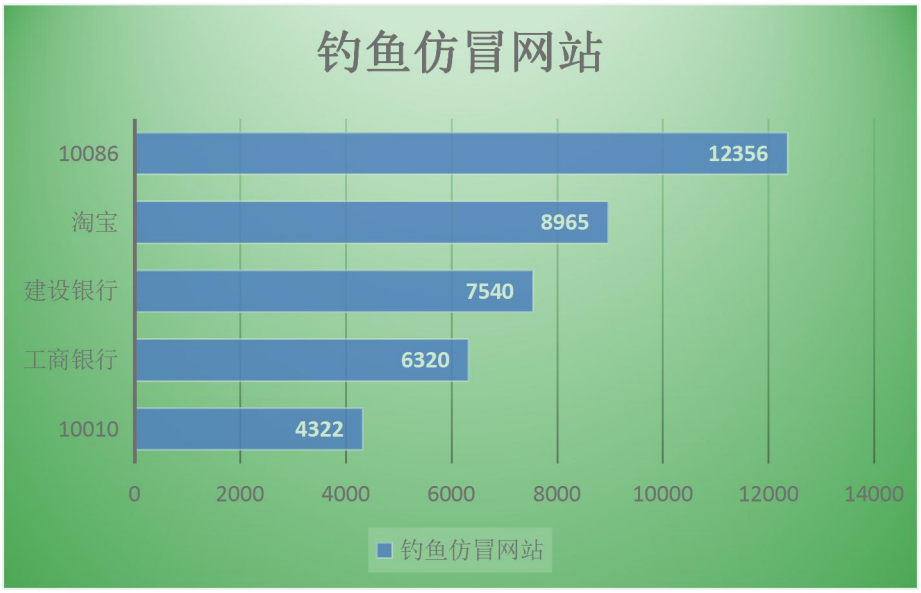
教育行业泄露的主要是学生信息，其中包括姓名、身份证号、学号、成绩、奖学金、教育经历等；电商行业主要泄露的信息有收货信息、购物订单等；政府行业主要泄露公民的社保信息、住房登记信息、公积金缴纳信息等。这些信息又可以组成完整的社工库，针对个人

进行精准的诈骗。

4. 网站仿冒钓鱼事件分析

网络钓鱼指的是黑客发送虚假电子邮件或模仿可信赖网站，来获取个人用户信息的一种犯罪行为。今年轰动全球的美国大选，希拉里“邮件门”事件就是由一封钓鱼邮件和一个高仿的钓鱼网站引发的，最终导致大选结果出现戏剧性反转。

2016 年（1 月 1 日到 12 月 25 日），千里目云检测平台共检测到网站仿冒钓鱼事件 4.9 万起，其中钓鱼网站主要以网银网站、淘宝等电商网站、10086 等运营商网站、公检法机关网站为主要仿冒对象。本年度监控到的钓鱼邮件 TOP5 分别是 10086 仿冒钓鱼网站 12356 例，淘宝仿冒钓鱼网站 8965 例、建设银行仿冒钓鱼网站 7540 例、工商银行仿冒钓鱼网站 6320 例、10010 仿冒钓鱼网站 4322 例，统计结果如下图所示：



钓鱼网站通常与所仿冒的网站高度相似，第一时间很难分辨真伪。

一个高仿的钓鱼网站首先都有一个极度相似的域名，这里展示的钓鱼网站域名为 http://wap.l0086xxf.com/。打开域名，跟真实网站并无不同，首页一个猫腻的地方就是在未登录情况下就有积分兑换人民币项目，如下图所示：

点击兑换人民币后会发现银行卡信息输入窗口：

不仅需要输入银行卡号、身份证号、手机号，甚至还要求输入银行卡密码。千里目安全实验室技术团队对此钓鱼网站进行技术破解，进入网站后台，发现一天时间内就有上百用户中招，如下图所示：

钓鱼网站通常通过短信、邮件、通讯软件、陌生网页进行传播，下面我们对钓鱼网站的主要传播方式进行梳理：

（1）伪基站之钓鱼短信

伪基站顾名思义就是假基站，设备一般由主机和笔记本电脑组成，通过短信群发器、短信发信机等相关设备，利用 2G 网络单向鉴权的漏洞，搜寻到一定半径范围内的手机卡信息，“劫持”用户的手机信号，模拟成任意手机号码向用户发送短信。

虽然号码可以伪装，但还是可以从内容找到猫腻：1、发送信息的时间和服务中心都与正常运营商短信不同。2、后边附带的链接一定会引诱用户下载 APP，从而达到控制受害者手机的目的。

（2）鱼叉式网络钓鱼

鱼叉式网络钓鱼源于亚洲与东欧，这种手法主要是针对特定人群目标的钓鱼攻击，比如企业高层，特定的政府部门以及其他敏感的企业。

（3）重定向钓鱼

重定向是指当使用者浏览某个网址时，将他导向另一个网址的技术。这种类型的钓鱼一般是将较长的网站网址转换成较短网址。当要传播某网站的网址时，常常因为网址太长，不好记忆；又有可能由于更换了网路的免费网页空间，网址又必须要变更，需要使用网路上的转址服务。这个技术使一个网页能够通过不同的统一资源定位符（URL）进行访问。

（4）克隆钓鱼

克隆钓鱼，顾名思义，就是将某个网站克隆下来，将其中的某环节篡改，然后将受害者引导至钓鱼页面；或者是制作一个 UI 界面一样的可执行程序，以此来让用户上当。克隆钓鱼基本上会采取 web、exe、URL 等方式。

（5）图片钓鱼

图片钓鱼顾名思义是黑客利用图片来进行钓鱼，这些图片通常看起起来比较模糊，利用人们的猎奇心理，当你点击放大图片时即中招，正在浏览的网页已经悄悄变成钓鱼网站。

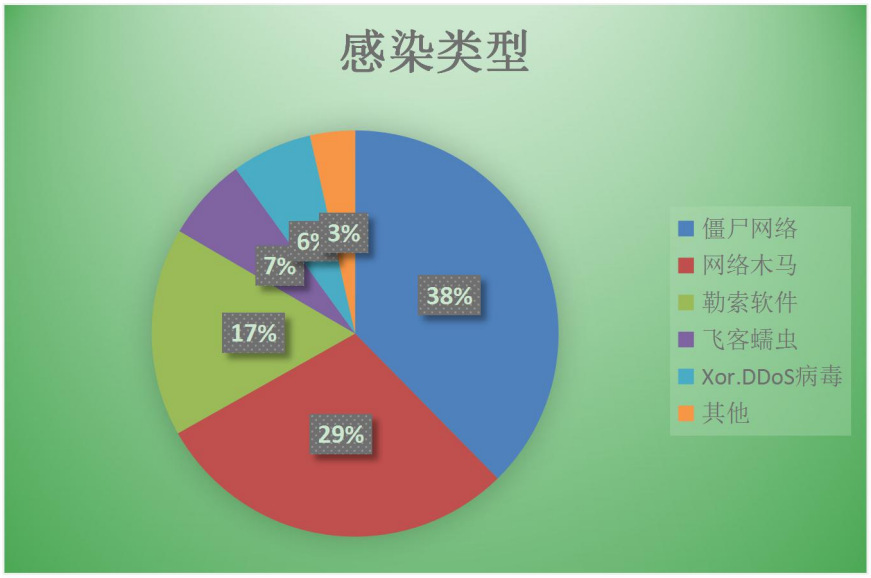
总结：如今钓鱼攻击已经成为非常严重的网络威胁。对抗钓鱼攻击，不再是单一用户或某个企业、行业单独面临的问题，而是成了大家共同关注的焦点。只有大家一致行动，建立多方协作的平台，才能最大限度的减少钓鱼攻击造成的损失。

五、恶意程序传播和活动情况

1. 恶意程序传播活动整体检测

2016 年（1 月 1 日到 12 月 25 日），千里目安全实验室共监测到受恶意程序感染的主机/服务器 IP 地址 156898 个，其中感染主机/服务器数量在 10 月达到全年最高点，每月恶意程序活动情况如下图所示：

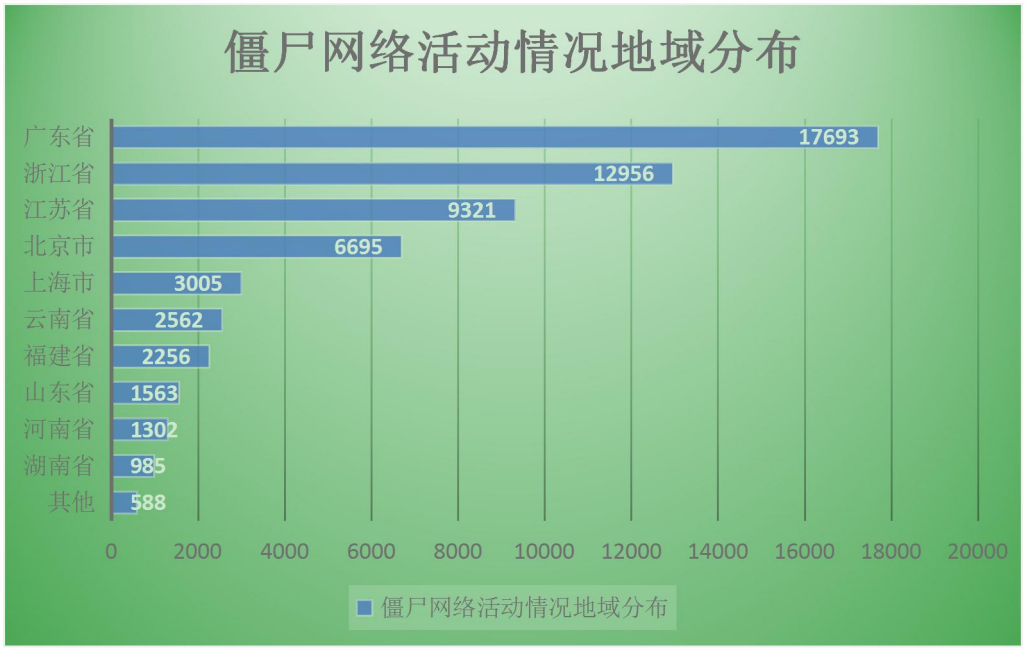
受感染主机的感染类型主要有僵尸网络、网络木马、勒索软件、飞客蠕虫、Xor.DDoS 病毒等，其中受僵尸网络感染的主机数量最多，共 58962 台。具体分布如下：



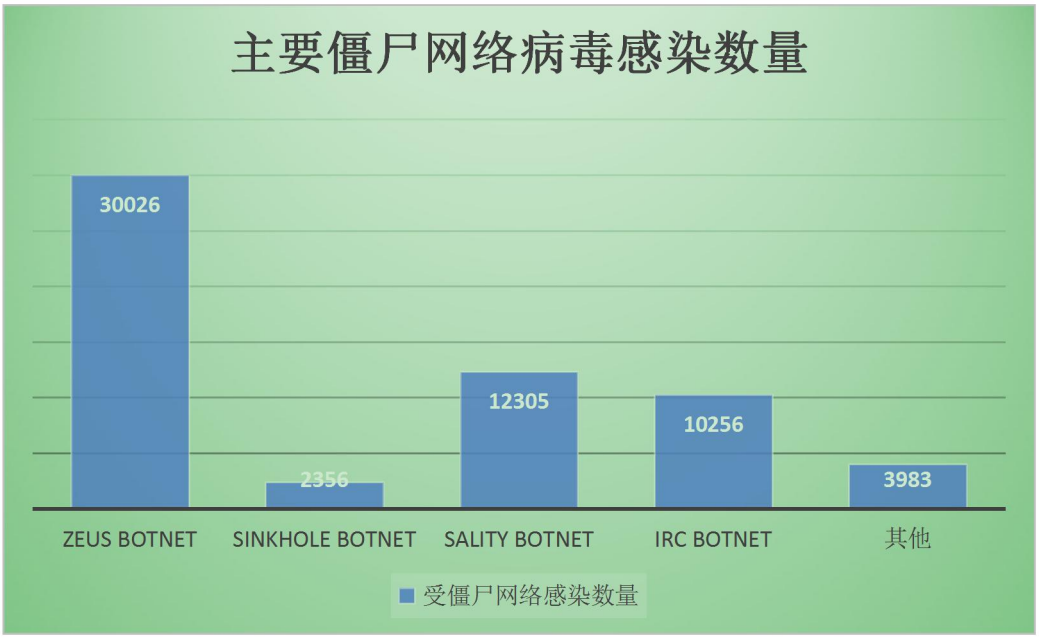
2. 僵尸网络监测情况

2016 年 10 月，导致半个美国网络瘫痪的元凶就是 Mirai 僵尸网络发起的 DDoS 攻击。僵尸网络，从字面上理解就像僵尸一样没有意识，受人指挥，被人利用。僵尸网络一般由成百上千个僵尸主机组成，受人控制，执行任意命令。

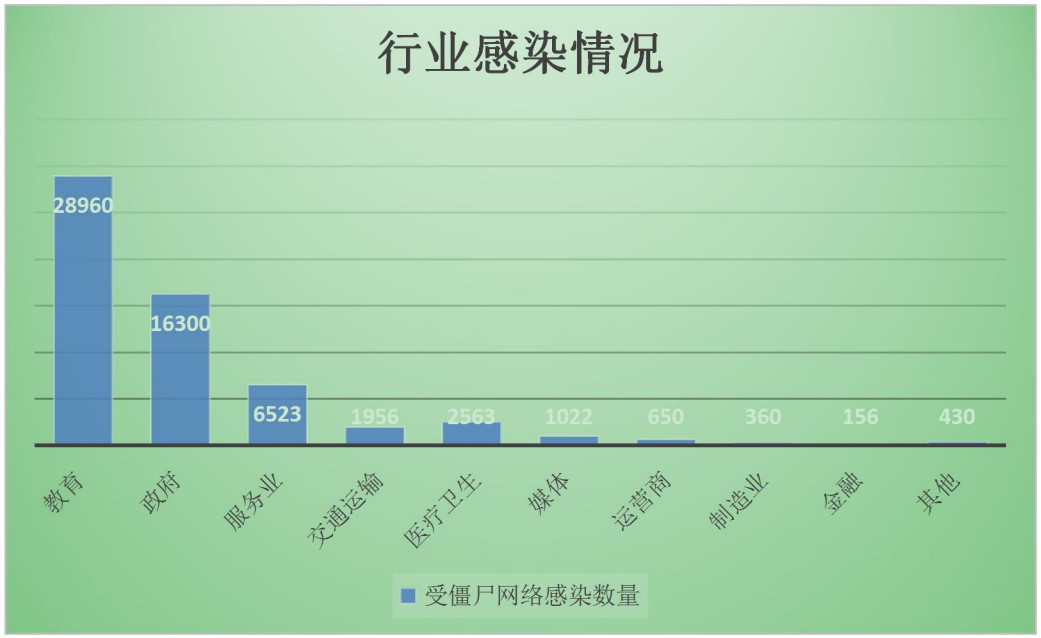
2016 年千里目安全实验室共监测到受僵尸网络感染的主机/服务器 IP 有 58926 个，比 2015 年同期增长 56%。我国境内僵尸程序控制的主机/服务器 IP 地址最多的三个地区分别是广东省、浙江省、江苏省。具体分布如下图所示：



其中最为活跃的僵尸网络病毒有 Zeus Botnet、Sinkhole Botnet、Sality Botnet、IRC Botnet 等，具体受感染用户主机/服务器 IP 数量如下图所示：



受僵尸网络感染的主机/服务器以教育行业为主，教育行业受感染主机/服务器 IP 数共有 28960 个，具体行业受感染情况如下图所示：



从上图统计中可以看出，教育、政府类网络受僵尸病毒感染最多，安全防护最弱。在加固网络安全防护的同时，应注意以下几个方面：

（1）网站漏洞发现与修复；

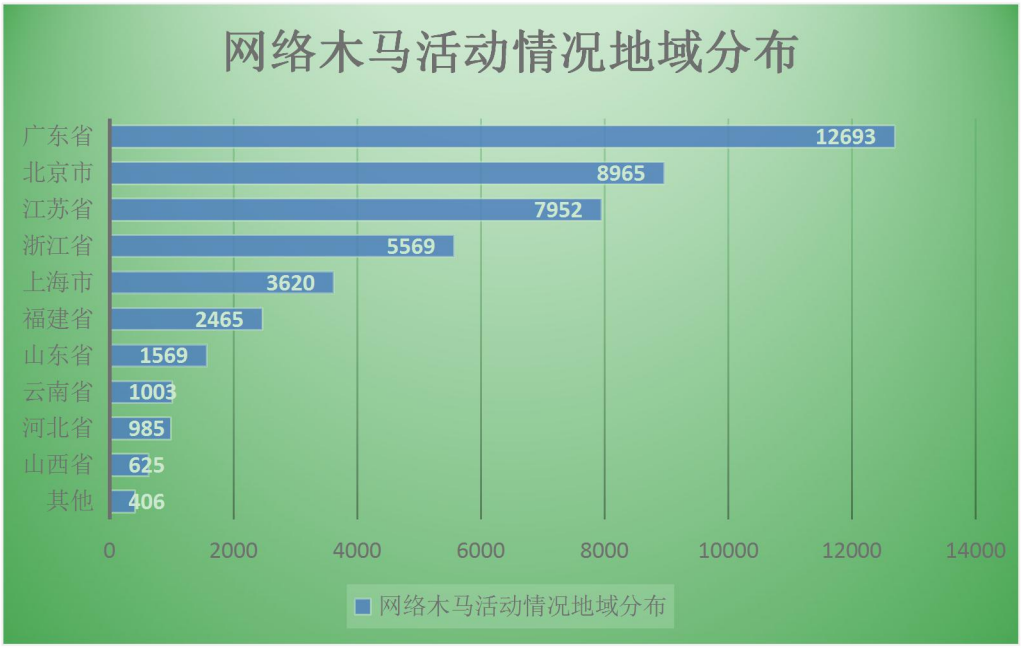
（2）定期对企业资产进行梳理和安全检查；

（3）培养员工网络安全意识，避免由个人操作失误造成的企业利益损失。

3. 网络木马监测情况

2016 年，千里目安全实验室共监测到受网络木马感染的主机 IP 有 45690 个，比 2015 年同期增长 23%。在我国境内受网络木马感染的主机/服务器 IP 地址最多的三个地区分别是

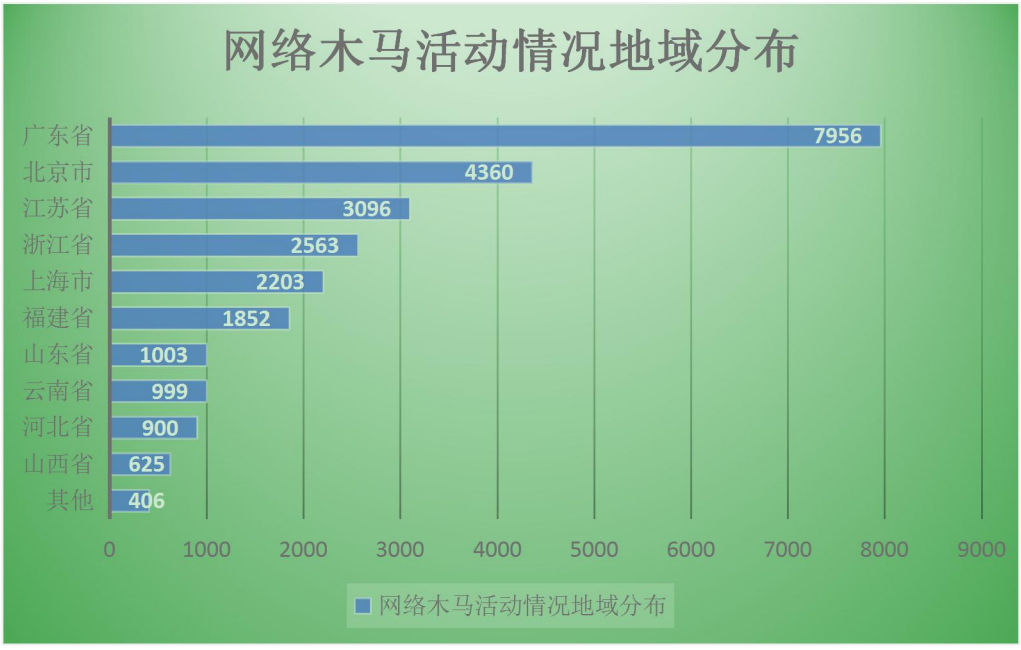
广东省、北京市、江苏省，具体分布图如下：



4. 勒索软件监测情况

2015 年底到 2016 期间，勒索软件数量暴增。因其低成本、高产出的攻击特性，而备受黑客喜爱，2016 年各产业都曾遭受到勒索软件的攻击，受害者一旦中招，基本上只有支付赎金才能安全找回数据。

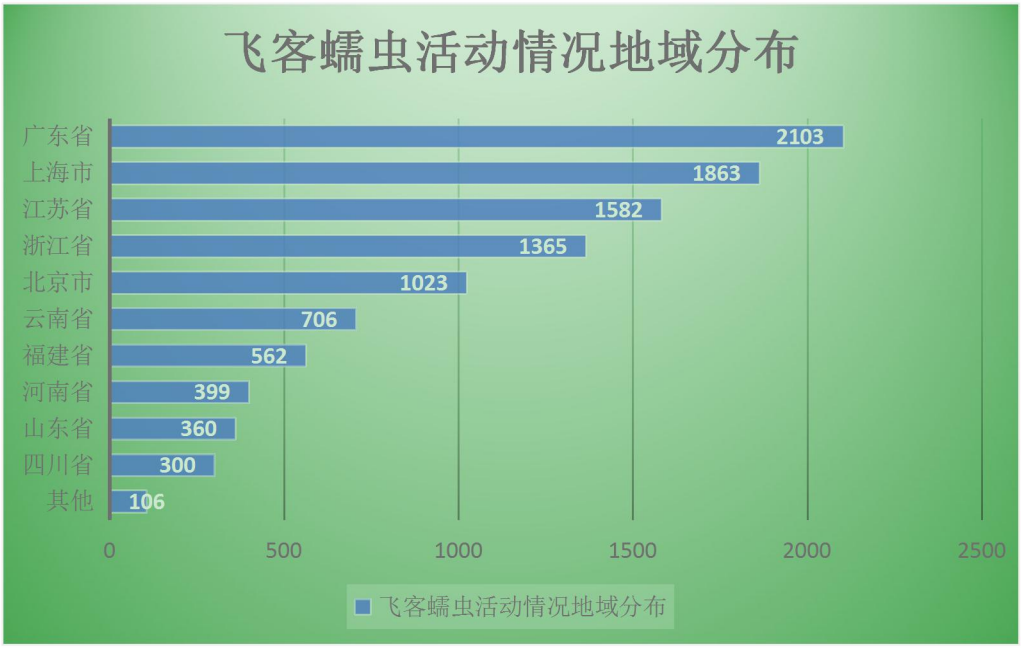
2016 年千里目安全实验室共监测到受勒索软件感染的主机/服务器 IP 有 25963 个，比 2015 年同期增长 406%。在我国境内受网络木马感染的主机/服务器 IP 地址最多的三个地区分别是广东省、北京市、江苏省，具体分布图如下：



5. 飞客蠕虫监测情况

飞客蠕虫是一种针对 Windows 操作系统的蠕虫病毒，最早出现在 2008 年。飞客蠕虫是一个利用微软 MS08-067 高危漏洞入侵暴露在公网中的主机/服务器。通过局域网、U 盘等方式进行快速传播，并且会停用受感染主机的所有 Windows 服务。

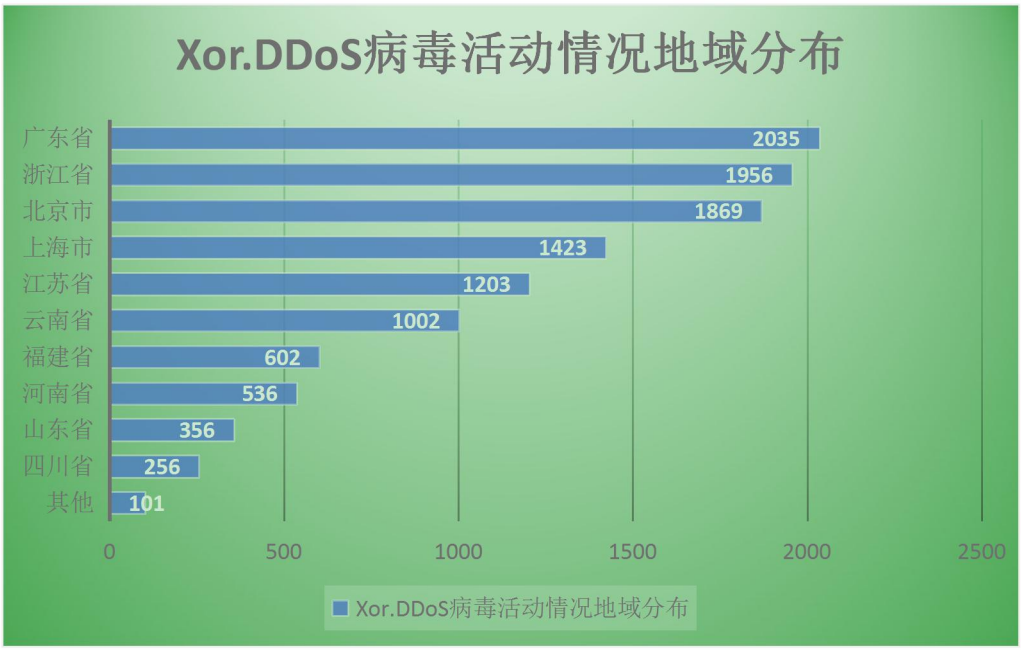
2016 年千里目安全实验室共监测到受勒索软件感染的主机/服务器 IP 有 10369 个，比 2015 年同期减少 9%。在我国境内受飞客蠕虫感染的主机/服务器 IP 地址最多的三个地区分别是广东省、上海、江苏省，具体分布图如下：



6. Xor.DDoS 病毒监测情况

Xor.DDoS 起源于中国，是一种专门感染 Linux 操作系统的病毒，用来组建实施 DDoS 攻击的僵尸网络。自 2014 年 10 月被安全研究人员首次曝光之后，Xor.DDoS 病毒就在 Linux 系统僵尸网络中异常活跃，不断对网络进行入侵和攻击，扩大僵尸网络规模。

千里目安全实验室在 2016 年监测到 106 起 Xor.DDoS 病毒感染事件，受感染主机/服务器 IP 多达 11339 个，比 2015 年同期增长 22%，在我国境内受 Xor.DDoS 病毒感染的主机/服务器 IP 地址最多的三个地区分别是广东省、浙江省、北京市，具体分布图如下：



Xor.DDoS 的 DDoS 攻击带宽已经从每秒数十亿字节提升到每秒 150 亿字节以上，可造成巨大的破坏力。Xor.DDoS 僵尸网络每天至少瞄准 20 个网站，且将近 90% 的目标站点位于亚洲，游戏行业是其主要的攻击目标，其次是教育机构。

六、2016 年国内外安全漏洞和安全事件盘点

1. 重大安全漏洞盘点

漏洞一、Linux glibc 曝漏洞

✧ 漏洞编号：CVE-2015-7547

✧ 漏洞概述：

2016 年 2 月 17 日，网曝 GNU C Library (glibc)中存在严重的安全漏洞，可导致 Linux 软件被攻击者劫持，进而在 Linux 平台上执行任意代码，获取密码，监视用户，甚至控制计算机。

✧ 漏洞影响：Linux glibc2.9 之后的所有版本

✧ 修复情况：官方已发布补丁

漏洞二、OpenSSL DROWN 漏洞

✧ 漏洞编号：CVE-2016-0800

✧ 漏洞概述：

2016 年 3 月 1 日，OpenSSL 最新的安全公告（2016 年 3 月 1 日）中指出，OpenSSL SSLV2 协议 EXPORT 加密模块存在高危漏洞，研究者将该漏洞命名为 DROWN。攻击者可利用这个漏洞破坏网站加密体系，发起“中间人劫持攻击”，从而窃取 HTTPS 敏感通信，包括网站密码，信用卡帐号，商业机密，金融数据等。

✧ 漏洞影响：漏洞影响了全世界 33% 以上，多达 1100 万个 HTTPS 网站，其中包括雅虎，阿里巴巴，新浪微博，新浪网，360，BuzzFeed、Flickr，StumbleUpon 4Shared 和三星等知名网站。

✧ 修复情况：官方已发布安全补丁。

漏洞三、Struts2 方法调用远程代码执行漏洞

✧ 漏洞编号：CVE-2016-3081

✧ 漏洞概述：

2016 年 4 月 21 日，Struts2 官方发布两个 CVE，其中，Apache Struts method: prefix 任意代码执行漏洞，官方评级为高。主要原因是用户开启动态方法调用时，会被攻击者实现远程代码执行攻击。

✧ 漏洞影响：2.3.18~2.3.28 (除2.3.20.2 和 2.3.24.2)版本

✧ 修复情况：官方已发布安全补丁

漏洞四、ImageMagick 图像处理软远程代码执行漏洞

✧ 漏洞编号：CVE-2016-3714

✧ 漏洞概述：

2016 年 5 月 3 日，ImageMagick 的官方披露称，目前提供给用户使用的程序存在一处远程命令执行漏洞（CVE-2016–3714），当其处理的上传图片带有恶意攻击代码时，就可以远程执行任意代码&命令，获取服务器的操作权限。

✧ 漏洞影响：ImageMagick 6.9.3-9 以前是所有版本，包括 ubuntu 源中安装的 ImageMagick

✧ 修复情况：官方在 6.9.3-9 版本中对此漏洞没有进行完全的修复

漏洞五、Zabbix SQL 注入漏洞

✧ 漏洞编号：无

✧ 漏洞概述：

2016 年 8 月，Zabbix 监视系统被曝存在 SQL 注入安全漏洞，攻击者无需授权即可登录 Zabbix 管理系统，也可通过 script 等功能直接获取 Zabbix 服务器的操作系统权限。

✧ 漏洞影响：2.2.x，3.0.0-3.0.3版本

✧ 修复情况：3.0.4 版本已修复此漏洞

漏洞六、iOS 曝严重安全漏洞

✧ 漏洞编号：CVE-2016-4655，CVE-2016-4656，CVE-2016-4657

✧ 漏洞概述：

2016 年 8 月 26 日，美国苹果公司发布 3 个紧急安全漏洞，利用这三个漏洞，攻击者可对设备进行全面控制，还能获取设备中的数据，通过麦克风监听对话，检测 GPS 信号位置，追踪及时通讯应用的对话内容等。

✧ 漏洞影响：iOS 9.3.5之前版本

✧ 修复情况：官方已发布 iOS9.3.5 修补这些漏洞

漏洞七、方程式曝 0day 漏洞

✧ 漏洞编号：CVE-2016-6415

✧ 漏洞概述：

2016 年 9 月，美国 NSA 方程式组织被黑，曝出 0day 漏洞，影响思科大部分设备产品，利用该漏洞可致远程、未认证的攻击者获取存储内容。

✧ 漏洞影响：全球超过84万独立IP设备受此漏洞影响，美国受影响最大，其次是俄罗斯，

中国受影响排名第10。具体影响IOS XR版本4.3.x、5.0.x、5.1.x和5.2.x（5.3.0及更新版本不受影响），所有IOS XE，以及数个IOS版本

✧ 修复情况：官方已发布安全补丁并敦促用户修复

漏洞八、"脏牛漏洞"

漏洞编号：CVE-2016-5195

✧ 漏洞概述：

10 月 19 日，国外安全研究人员 Phil Oester 在 RedHat 官网的安全公告中发布了一个全版本 Linux 内核本地提权漏洞（CVE-2016-5195），被称为“脏牛漏洞”（Dirty Cow）。之所以称为 Dirty Cow，是因为 Linux 内核在进行内存管理时使用的写时复制（Copy on Write）机制存在条件竞争漏洞，从而引起内存破坏，导致权限提升。

✧ 漏洞影响： Linux 内核版本 >=2.6.22 的系统，都会受到该漏洞的影响

✧ 修复情况：官方未发布正式修复补丁

漏洞九、Debian-based Linux 版本的 Nginx 本地提权漏洞

✧ 漏洞编号：CVE-2016-1247

✧ 漏洞概述：

11 月 15 日，Dawid Golunski 发现 Nginx 存在本地提权漏洞，CVE 编号为 CVE-2016-1247。这个漏洞产生的原因是 Nginx 在新建日志目录时，使用了不安全的权限，导致本地恶意攻击者可以从 Nginx / Web 用户权限 (www-data) 提升到 root 权限。该漏洞影响基于 Debian 的 Linux 发行版的 Nginx 网站服务器。

✧ 漏洞影响：

Debian 系统：Debian 系统在 Nginx 1.6.2-5+deb8u3 中修复

Ubuntu 系统：Ubuntu 16.04 LTS：在 1.10.0-0ubuntu0.16.04.3 中修复；

Ubuntu 14.04 LTS：在 1.4.6-1ubuntu3.6 中修复；Ubuntu 16.10：在 1.10.1-0ubuntu1.1 中修复

除以上已修复或更高版本，其他 Nginx 服务器版本均受到该漏洞影响。

✧ 修复情况：

Debian 和 Ubuntu 已经在官方安全公告中说明该漏洞，可以直接使用系统更新命令，更新 Nginx 软件

全年重大安全漏洞总结

✧ 2016 年 4 月，Struts2 再次爆发高危漏洞，Struts2 在金融、政府行业使用广泛，导致大量行业私密数据被窃取，另外通过千里目云检测平台检测发现 Struts2 暴发新的高危漏洞的同时，针对以往 Struts2 的高危漏洞攻击也迅速增加，攻击者针对 Struts2 框架，制定了完整的攻击包，因此使用 Struts2 的用户需要注意安全防护，定期扫描监控发现威胁，并反复监视原有漏洞，确认修复效果。

✧ 本年度针对 Linux 系统的漏洞主要以本地提权为主，但是由于利用困难大，并未造成大规模危害。但是由于 Linux 多是部署在服务器上，大部分是企业重要数据系统，因此使用 Linux 用户需时刻关注 Linux 安全新动态。

✧ 针对使用量广泛的软件，越来越成为黑客挖掘的重点，今年爆出的 OpenSSL DROWN 漏洞、苹果 iOS 漏洞、思科设备漏洞，都是使用量巨大、影响广泛的漏洞。保护好通用基础应用的安全，是厂商及企业用户需要重点关注的方面。

2. 重大安全事件盘点

事件一、FortiGate SSH“后门”事件

2016 年 1 月 12 日凌晨四点钟,国外安全研究员爆料 FortiGate 防火墙存在一个后门,攻击者可以通过这个后门直接获取防火墙控制权限。此后门影响 FortiGate 防火墙 4.0 到 5.0.7 版本。在网络空间搜索引擎上发现全球有 64567 个 IP 使用 FortiGate 防火墙。目前在新版本中已删除后门。

事件二、以色列国家电网遭受有史最大规模网络攻击

继去年 12 月 23 号乌克兰电网遭遇历史上首例针对供电体系的恶意行为，导致当时成千上万乌克兰民众陷入无电可用的窘境之后，2016 年 1 月 25 日，以色列电力供应系统也受到重大网络攻击侵袭，且已经有多份报告表明勒索软件正是造成事故的直接原因。针对基础设施的网络攻击活动，能够导致发电站乃至整套能源供应链发生瘫痪，其中涵盖天然气、石油、汽油以及供水系统，并可能造成人员伤亡等严重后果。此次针对国家关键性基础设施的攻击活动规模极大，标志着第一次转折性恶意行为已经出现，未来网络攻击将不仅仅以经济损失或者声誉破坏为目标。

事件三、5000 万名土耳其公民个人信息在网上曝光

2016 年 4 月 3 日，土耳其发生了一次重大数据泄露事件，48,611,709 名土耳其公民个人数据牵涉其中。这些泄露数据被压缩成 1.5GB（数据容量 6.6GB）的文件储存在芬兰 IP 地址 185.100.87.84 下，人们可以通过 P2P 下载到他们感兴趣的数据。数据中包括了土耳其公民的名和姓、身份证号码(TC Kimlik No)、其父母的名字、性别、出生城市、生日、完整的住址及 ID 注册城市和地区。

事件四、2.7 亿 Gmail、雅虎和 Hotmail 账号泄露事件

2016 年 5 月，俄罗斯黑客成功的进行了一场大规模的数据窃取攻击。在此次攻击中，俄罗斯用户的 Gmail、雅虎及微软电邮 Hotmail 等 2.723 亿账号惨遭泄露，并在俄罗斯地下黑市进行交易。此次泄露数据列表中，删除重复的账户后，还包括至少 5700 万 Mail.ru，3300 万 Hotmail，4000 万雅虎以及 2400 万 Gmail 地址。此外，列表中还包括成千上万的中国和德国电子邮箱地址服务器的信息等。

事件五、美国国家安全局（NSA）内部黑客团队方程式组织（Equation Group）被黑事件

2016 年 8 月，美国国家安全局（NSA）内部黑客团队方程式组织（Equation Group）被黑。The Shadow Brokers（国内媒体翻译为影子经纪人）黑客组织将其入侵所得文件和工具以 100 万比特币（约 5.68 亿美元买）拍卖，为证明文件和工具的有效性，影子经纪人在 Github 给出了方程式组织攻击防火墙设备利用的攻击脚本和工具。从泄露的资料看，有 5 家防火墙公司的产品受到威胁，分别是华为、天融信、Fortigate、Cisco、Juniper，但也不排除其他厂商不会受到影响。

事件六、徐玉玉信息泄露遭诈骗事件

2016 年 8 月 21 日，山东准大学生徐玉玉因被诈骗电话骗走上大学的费用 9900 元，伤心欲绝，不幸离世。随后公安机关通缉抓获 3 名诈骗罪犯。隐私泄露源头追踪中顺藤摸瓜抓获 18 岁天才黑客杜天禹，杜天禹坦言：网站存在漏洞，我通过上传木马下载 60 万考生信息

获利。

事件七、Mirai 僵尸网络，造成半个美国网络瘫痪

2016 年 10 月 21 日，黑客操控感染了恶意软件 Mirai 的物联网设备对 DNS 服务提供商 Dyn 发起了 DDOS 攻击，影响波及 Twitter、Reddit、GitHub 等知名网站，强大的攻击流量甚至使域名服务商 DYN 多地网络服务直接中断。Mirai 预计已经感染了超过 50 万台设备，被 Mirai 感染的设备中，约有 10%参与了本次 DDoS 攻击。Mirai 通过感染那些存在漏洞或内置有默认密码的物联网设备，像“寄生虫”一样存在设备中，操控它们，针对目标网络系统发起定向攻击。网络监控摄像头、DVRs、路由器等其它家用网络设备都可能成为 Mirai 僵尸网络的“猎物”，据 ISP 服务商 Level3 调查，全球受 Mirai 感染的 IoT 设备达 50 万，其中：美国 29%，巴西 23%，哥伦比亚 8%。

事件八、希拉里邮件门事件

2016 年 11 月，美国大选倒计时时刻，作为最有希望出任总统的希拉里无论从政治权利还是国内支持率都以压倒性的优势完胜川普，不出意外的话，希拉里很有可能当选新一任的美国总统。然而原本已经十拿九稳坐上总统宝座的希拉里，由于私密邮件遭黑客曝光，邮件几乎涉及希拉里从政期间的各种丑闻，深陷“邮件门”的希拉里支持率暴跌，最终与总统之位失之交臂。“邮件门”的起因要追溯到 3 月 19 日，希拉里竞选团队竞选经理 John Podesta 收到了一封伪装成谷歌的钓鱼邮件。在这个伪装的长链接中，包含了 30 个字符的加密字符串，这些信息包括 Podesta 邮箱地址和姓名等。Podesta 无意点击了邮件中的恶意链接，造成了个人信息的泄露，黑客通过钓鱼链接窃取 Podesta 邮箱密码，获取希拉里通信隐私内容。

事件九、雅虎发声明称 10 亿账户数据被泄露

2016 年 12 月 15 日，雅虎发布声明称其发现了新的安全漏洞，并表示此次数据泄露与 2016 年 9 月的 5 亿用户数据泄露“并无关联”，据雅虎官方说明，本次信息泄露可追溯至 2013 年 8 月，该漏洞造成至少 10 亿用户的姓名、电邮和密码被盗。

被窃的用户账号信息可能包括姓名、电子邮件地址、电话号码、出生日期以及密码。雷锋网(公众号：雷锋网)发现，据美国《纽约时报》网站报道，新披露的袭击涉及更多敏感的用户信息，包括没有加密的安全问题。雅虎正在让这些安全问题失效，同时强行要求所有受影响的用户修改自己的密码。

全年重大安全事件总结

- ✧ 全球重大安全事件盘点中，共有 50%内容涉及公民信息泄露，可见信息泄露已成为危害全球的首要安全大事。不提信息泄露造成的多起诈骗致死事件，单单是每日的垃圾邮件，骚扰电话/短信，就已经严重影响着个人的日常生活。因此，信息泄露已成为影响公民人身财产安全的重要杀手之一。无论是信息管理者还是个人，都应该时刻关注各种针对信息窃取的攻击行为。
- ✧ 此外，本年度爆发多起防火墙安全漏洞事件，针对安全防护设备的攻击有明显增加，安全厂商在做安全防护产品的同时也应同样注意自身产品安全建设。
- ✧ 网络安全已经开始渗入方方面面，从公民个人隐私到国家之间的对抗，每个人，每个国家都很难独善其身，我国也把网络安全提升到国家重要战略地位，相继出台了重要的政策法规。没有网络安全，就没有国家安全，未来我们需要花费更多精力时间提升公民安全意识，提升整个国家网络安全建设。

七、网络安全现状及攻击应对措施

1. 个人层面

网络调查显示，针对企业的攻击事件56%是从企业员工进行攻击，攻击方式有钓鱼邮件、社工、管理员账号窃取等方式。网站曝出漏洞后，有58%的管理员由于没有造成实际危害而无任何作为。

针对个人层面造成的网络攻击，千里目安全实验室给出如下建议：

（1）在办公环境下禁止外来陌生网页访问，慎点未经确认的各类链接；

（2）使用专业的密码管理软件来存储办公环境中的各类账号和密码；

（3）时刻注意关机锁屏，尽量不用生日、身份尾号、手机号等作为开机密码；

（4）重视安全防护设备/软件的报警信息；

（5）网站管理人员应尤其注意网站漏洞通报信息，并及时验证修复。同时在日常网站运维时期，应定期做漏洞监控和扫描，及时发现网站风险。在漏洞修复后同样应该反复监视，确认修复效果。有些漏洞有可能会出现反复修复的现象，例如2014年OpenSSL心血漏洞，当时厂商提供的补丁没有对漏洞进行完全的修复，后续几个月内，业内又公开了几种新的漏洞利用方式，导致该漏洞带来新的风险。

2. 企业层面

深信服专注企业用户的信息安全。深信服经调研统计发现，拥有专业安全团队的单位不足15%，拥有网络安全制度及网络安全事故应急响应流程机制的单位不足20%。且大量单位使用第三方开源建站系统，然而使用第三方建站系统的单位有23%左右不能正确的管理和配置这些网站，导致网站存在大量安全隐患。统计中还发现，公司人员安全意识不足同样是导致企业网络发生安全事故的重要因素。针对以上现状，深信服科技针对企业层面给出以下安全建议：

（1）邀请专业的安全专家不定期培养企业内部人员安全意识，减少因为非技术因素造成的安全损失；

（2）建立完善的网络安全制度明确安全管理人员工作职责，定期对企业资产进行梳理，排查安全隐患，做出目标、内容、考核三个执行标准；

（3）建立网络安全事故应急响应机制，从漏洞爆发、漏洞验证、漏洞修补、安全加固、漏洞预防等五个方面来执行；

（4）通过黑白名单的方式，严格规范企业员工上网行为，避免由于个人操作失误给全公司带来经济损失；

（5）预设黑名单和白名单的方式协助运维人员进行网站威胁发现，在监测的顺序上建议先采用黑名单拦截过滤检测，然后再用白名单正常访问行为进行检测；

（6）对网站安全威胁源进行封禁。虽然在攻防技术上攻击者完全可以更换攻击源来持续对目标进行攻击，但是在攻防中，有效对抗攻击行为，可以使攻击者的攻击时间成本与技术成本上升，这样部分攻击者会因为攻击阻断和封禁措施，停止攻击，转向攻击成本低的目标；

（7）对企业网络安全事件按照事前、事中、事后三维度进行管理，构建事前预警、事中防御、事后溯源的能力；

3. 法律法规

2016 年 11 月 7 日，全国人大常委会正式表决通过《中华人民共和国网络安全法》，该法规第二十一条提出：“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。在此项法规中，不仅明确了网络安全负责人责任，而且对计算机病毒、网络攻击和入侵等危害网络安全行为等违法行为进行定性。

《网络安全法》在个人信息保护内容中强调“任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息”。明确个人信息应受到保护的权利。

在互联网高速发展的现在，黑客攻击行为屡禁不止的今天，《网络安全法》展示了我国网络安全工作的基础性法律框架，不仅规范了企业行为，明确其责任，还加大网络犯罪打击力度，为保护公民和企业在互联网中安全生存提供法律依据。

八、网络安全威胁未来趋势

针对 2016 年网站安全情况以及网络攻击情况分析，千里目安全实验室对 2017 年攻击趋势做出如下几方面预测：

1、数据泄露问题是企业关注的焦点。从近两年的安全事件来看，企业级的信息泄露事件都会造成巨大影响。智能硬件的普及，个人信息数字化，导致存有敏感信息企业防护压力越来越大，而这些地方往往也是黑客青睐的攻击对象。

2、社工工程学攻击效果会更加明显。今年勒索软件席卷全球，很多攻击都是通过恶意邮件，恶意链接，钓鱼邮件，以及诈骗、冒充身份等方式进行，这些攻击手段非常普遍，技术难度不高，但是效果明显，所以安全意识提升对于企业来说也安全建设的一个重大问题。

3、云计算、物联网等新技术带来的安全隐患。比如企业业务上云、物联网以及近两年流行的大数据分析、机器学习，人工智能等技术，在飞速发展的同时，也给了黑客更多可用的攻击方法，所以威胁也变的更加智能，攻击效率越来越高，防御难度也会加大。

综上，我们认为 2017 年，企业用户最应该关注的安全问题分别是数据泄露、社工工程学攻击、攻击智能化三个方面。

九、千里目安全实验室介绍

千里目是深信服旗下第一安全实验室，主要专注于网络安全攻防技术研究，利用黑客视角解决网络安全问题，为企业安全赋能。

千里目取自王之涣《登鹳雀楼》“欲穷千里目，更上一层楼”；寓意站得高、看得远，学无止境，勇攀高峰。在网络安全攻防技术研究领域精勤钻研，不断提高专业技术造诣，抵御更多的网络安全威胁。同时千里目更希望做网络空间的一双眼睛，拥有更加敏锐长远的眼光（Further eye），深度洞察网络安全威胁，解读前沿安全技术。

。