深信服智安全
SANGFOR SECURITY

2017 年安全威胁分析报告

网络安全篇

深信服智安全·千里目安全实验室

2018 年 1 月 22 日

1. 网站安全

1.1 网站安全整体解读

在 2017 年的调查中发现，对比 2016 年的保守防御方式，有接近三分之一的企业和组织对安全警报和事件的态度逐渐发生改变，**从以前的被动响应逐渐转变为主动寻找网站风险**，从根本上解决网站安全隐患。

深信服安全服务平台在 2017 年授权检测网站 30 余万个。

（1）深信服安全平台对全国 30 余万个授权域名（或 IP）进行安全检测，共发现 386952 个高危漏洞，网站安全依然不容乐观；

（2）深信服安全平台共拦截攻击 86.2 亿次，封锁恶意攻击 IP 15.9w 个，境内外攻击形势依旧非常严峻；

（3）网站入侵情况依然严重，共发现篡改事件 75094 次。

1.2 网站安全检测情况

1.2.1 漏洞行业分布

2017 年 1 月 1 日开始到 12 月 31 日截止，深信服安全服务平台对全国 11 个行业（其中包括政府、教育、医疗、金融、企业、能源等）30 余万个域名（或 IP）监测发现：

网站监测中除了大企业类网站，占比最多的是政府和教育类网站，政府类网站有 52062 个，教育类网站有 49025 个。

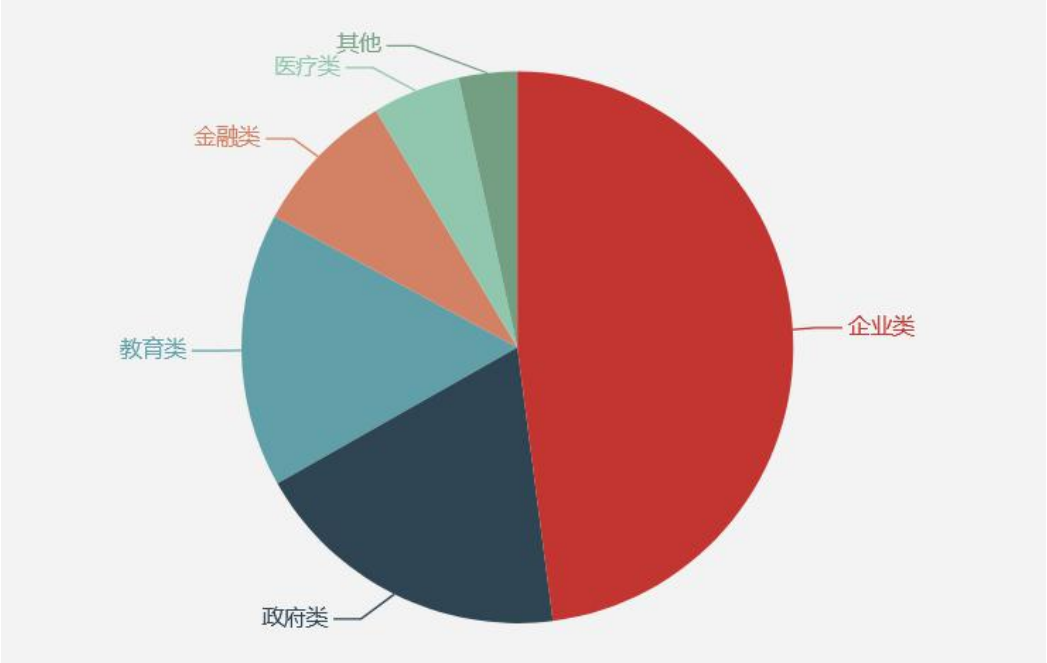


图 2.2.1-1

由此可见，政府和教育类网站管理者安全意识逐渐增强，即使在不具备安全能力的情况下，也在积极寻求安全协助，保障网站安全。

1.2.2 漏洞类型分类

2017 年 1 月 1 日开始到 12 月 31 日截止，深信服安全服务平台对全国 11 个行业（其中包括政府、教育、医疗、金融、企业、能源等）30 余万个域名（或 IP）监测发现：

高危漏洞统计分析：在监测的 30 余万个域名（或 IP）中，发现有 46246 个网站存在高危漏洞，占网站总数的 15.1%。

根据漏洞类型的不同，在所有网站中共发现高危漏洞 386952 个，其中，XSS 注入 160926 个、SQL 注入 84130 个、配置不当 52470 个、命令执行 24060 个、代码执行 20460 个、拒绝服务 19264 个、弱密码 12640 个、未授权访问 8368 个、认证绕过 6050 个。

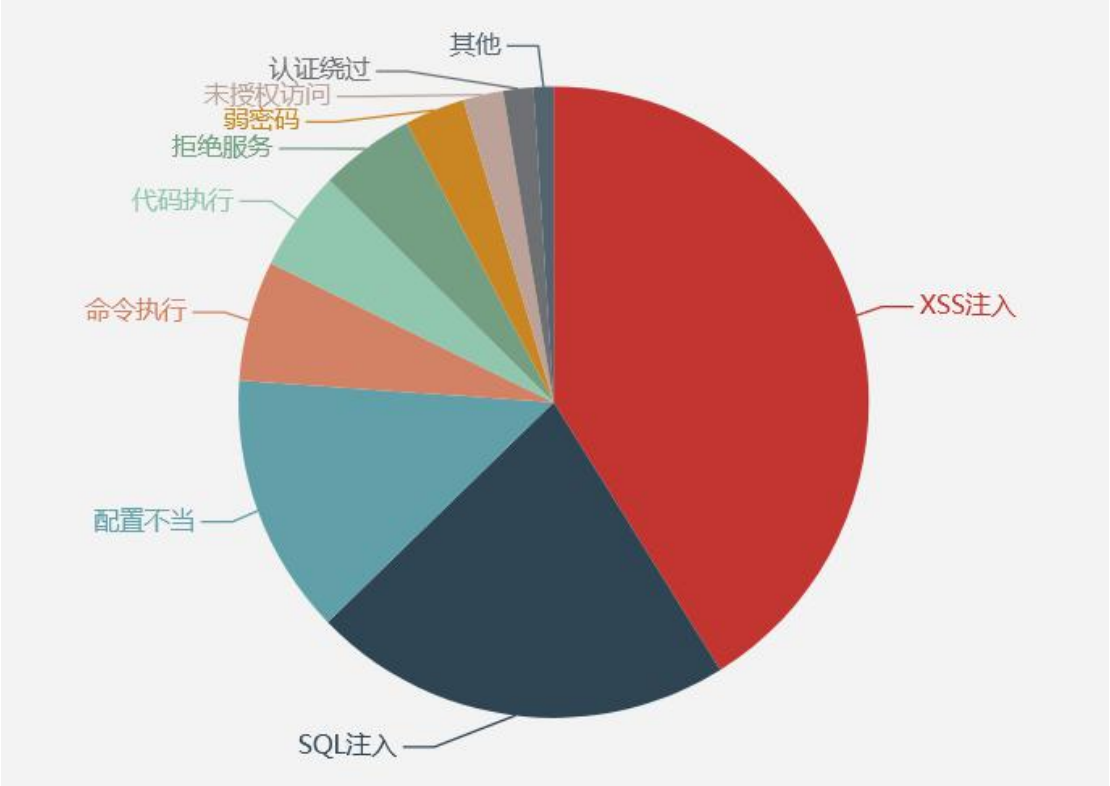


图 2.2.2-1

由上图可见，常规漏洞 XSS 注入、SQL 注入等依然是危害网站安全的重大杀手。除此之外，由于网站管理员不安全操作导致的配置错误，也是引发网站风险的重要因素。针对这些漏洞，我们建议在网站开发和运维中，采取下述手段降低安全隐患：

- 对网站开发人员进行安全编码培训；
- 请专业安全人员对网站架构和源代码做全面的安全审计，修复安全漏洞；
- 网站运营中，及时升级，包括操作系统、数据库、中间件等；
- 对网站各个组件、服务进行排查，关闭无用的服务和组件，修改默认配置及密码，并使用强度较高的密码；
- 采取备份手段，并时常备份网站的关键业务数据；
- 对敏感信息加密，包括敏感信息的存储和传输；
- 采用专业的 Web 应用安全产品。

1.2.3 漏洞修复周期

信服云眼在2017年期间检测网站多达30余万个，在此期间，挑选存在漏洞的政府（.gov）网站，教育（.edu）网站，企业网站各1000个，进行漏洞修复监测。其中发现，在所有网

站中，高危漏洞修复效率最高，从漏洞检测通告到修复平均用时 30 天左右。在监测中发现，大型企业对网站安全的关注度最高，中低危漏洞在检测发布后也在持续减少，教育行业网站建设存在安全隐患最多，且修复周期最长。以下给出三个典型行业的修复周期图：

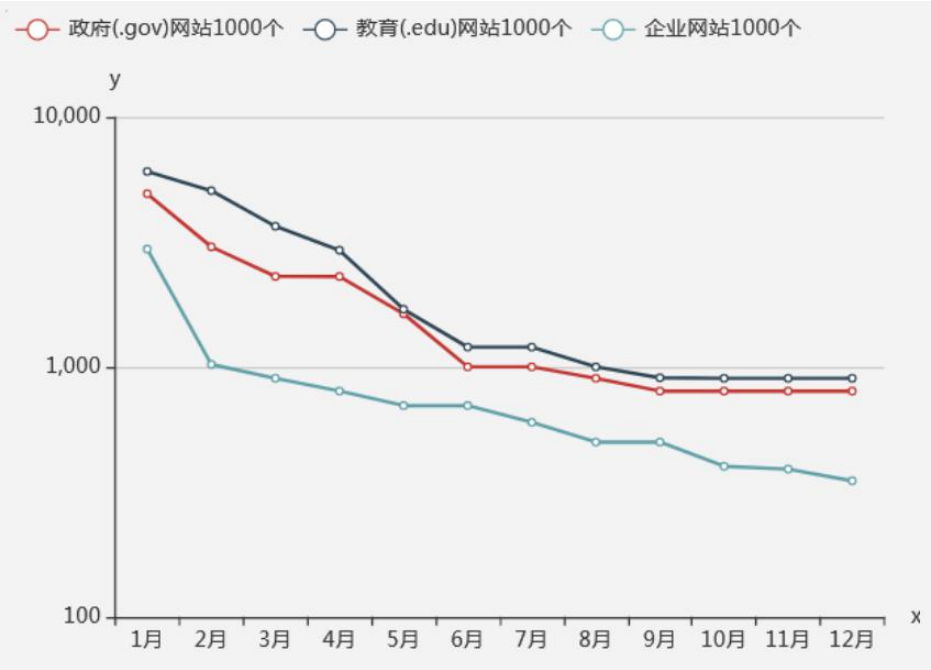


图 2. 2. 3-1

从上图可以看出，政府类网站和教育类网站修复效率较低，且对于中低危漏洞通常不关注，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：

- 用户单位没有专业安全人员，不具备修补安全漏洞的能力；
- 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；
- 缺乏统一漏洞推送机制，厂商发布安全补丁或者升级服务通常都会直接在官网发布，不会定向推送给网站使用者；
- 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。

1. 3 网站篡改情况

2017 年 1 月 1 日开始到 12 月 31 日截止，深信服安全实验室持续监控互联网中已被入侵篡改的网站，共涉及政府，医疗，教育，金融，大中小企业等篡改案例多达 75094 例。数据主要来源于深信服多款安全产品，信服云眼，互联网搜索引擎，各大中小黑客论坛/网站等。

1.3.1 网站篡改分类

从篡改表象来看，我国被篡改的网站主要有以下六种类型：1、被植入赌博网页/关键字/链接；2、被植入色情网页/关键词/链接；3、被植入游戏私服网页/关键字/链接；4、被植入违法交易产品信息（办假证/枪支等）页面；5、被植入涉政言论（诋毁党政国家）；6、黑客炫耀技术，植入个人信息增加圈内知名度。

从深信服安全实验室采集到的网站篡改样本来看，以获取经济利益为目的的赌博、色情、游戏私服类篡改占所有篡改总数的 80%以上，是网站篡改的常见内容，具体分布如下图所示：

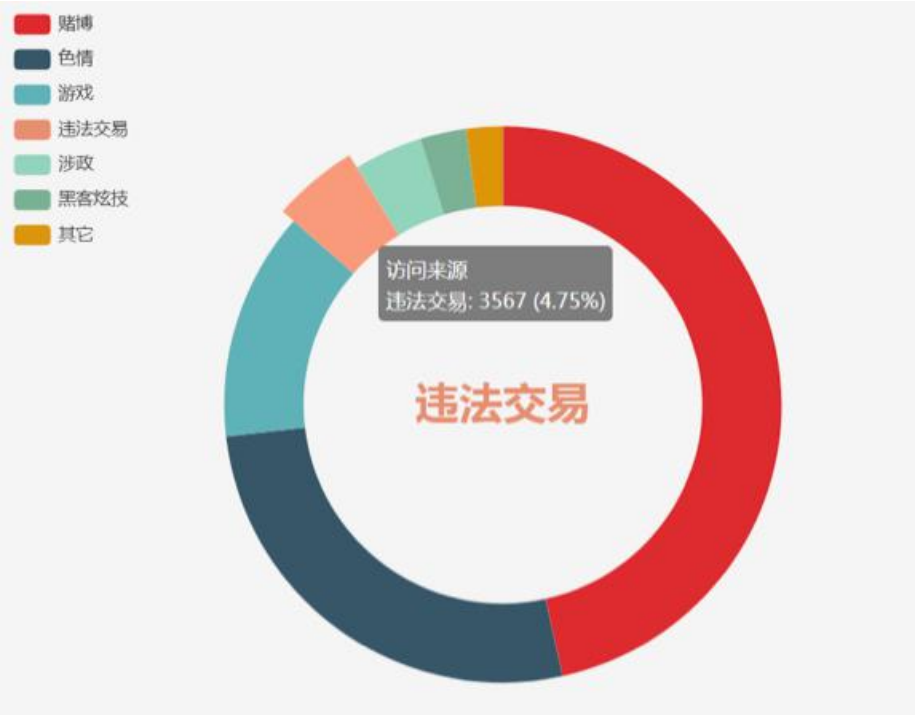


图 2.3.1-1

通过对被篡改网站进行收集发现，除了国外黑客组织基于政治目的小规模网站篡改，国内黑客组织大多利用黑客技术入侵网站，在正常的网页中植入赌博/色情/游戏/购物等关键词和网站链接，用来达到提高网站搜索排名的经济利益目的。被入侵的网站轻则沦为黑客获利的工具，被黑站引流，重则系统遭到破坏，数据丢失，网站内容被恶意更改，损坏客户利益和对外公开形象。

1.3.2 网站篡改技术手段

2017 年深信服千里目安全实验室一直在关注和搜集公网中被篡改的网站，除了基于政

治目的的恶意诋毁篡改，和基于炫耀目的的挂黑页篡改以外，其他篡改手段都是基于黑帽SEO技术手段实施。本章节主要针对几类不同的篡改技术手段作出说明。

篡改手段一、直接篡改网页文本、链接和图片（较低级）

直接篡改网页内容在网站表象中极为明显,非常容易被发现,这种篡改是大众所熟知的,通过技术手段入侵网站后台或者服务器，修改网页文字/图片，达到篡改目的。

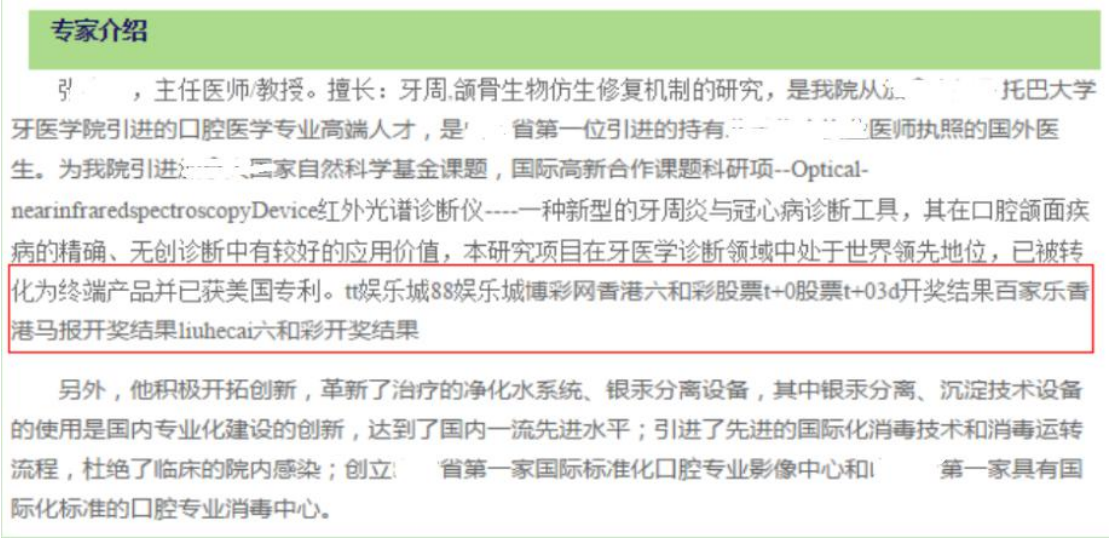


图 2.3.2-1

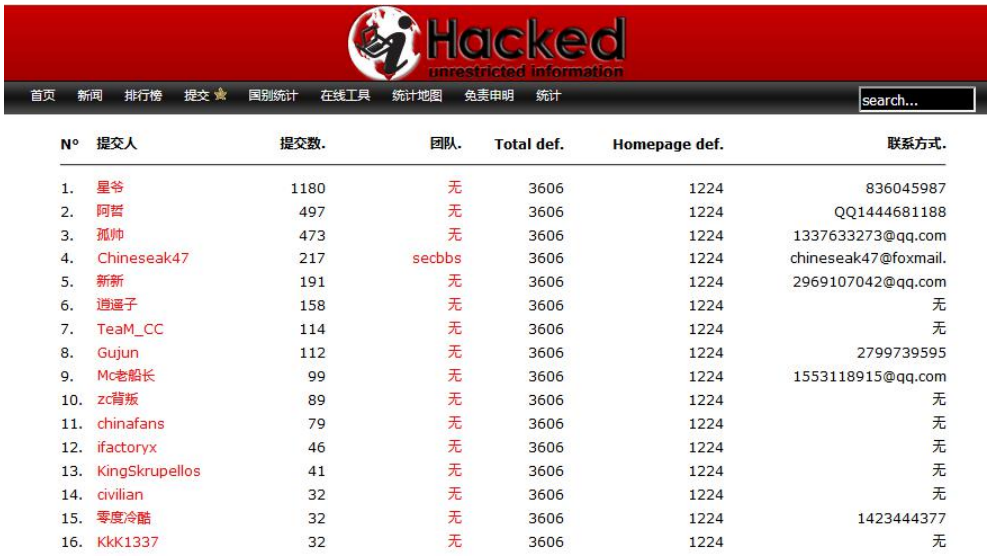
此类篡改对黑客技术要求不高，只需要修改文本即可，多以恶作剧为主。网站管理员面对此类修改需要删除篡改关键字，修改后台密码，同时全站检查后门的漏洞。

篡改手段二、植入单个篡改网页

相比于手段一，植入单个篡改网页极为简单粗暴，深受广大黑客初学者喜爱，精心制作黑酷炫彰显个性的页面，加上自己的黑客圈内 ID，用来在互联网中寻找存在感。

图 2.3.2-2

与其说这些黑客在网站挂黑页是为了秀技术、刷存在感，不如说他们是为了知名度而战。基于黑客这种绞尽脑汁获取知名度的行为，“被黑站点”统计平台应运而生，黑客的排名在一定程度上代表了他们的技术水平，排名靠前黑客更容易收到“徒弟”，得到“学费”的同时更方便组建自己的黑产团队，在互联网黑产中获取大量利益。



N°	提交人	提交数.	团队.	Total def.	Homepage def.	联系方式.
1.	星爷	1180	无	3606	1224	836045987
2.	阿哲	497	无	3606	1224	QQ1444681188
3.	孤帅	473	无	3606	1224	1337633273@qq.com
4.	Chineseak47	217	secbbs	3606	1224	chineseak47@foxmail.
5.	新新	191	无	3606	1224	2969107042@qq.com
6.	逍遥子	158	无	3606	1224	无
7.	TeaM_CC	114	无	3606	1224	无
8.	Gujun	112	无	3606	1224	2799739595
9.	Mc老船长	99	无	3606	1224	1553118915@qq.com
10.	zc背叛	89	无	3606	1224	无
11.	chinafans	79	无	3606	1224	无
12.	ifactoryx	46	无	3606	1224	无
13.	KingSkrupellos	41	无	3606	1224	无
14.	civilian	32	无	3606	1224	无
15.	零度冷酷	32	无	3606	1224	1423444377
16.	KkK1337	32	无	3606	1224	无

图 2.3.2-3

这种篡改手段在实现上并不需要特别高深的技术手段，黑客通常利用寄生虫工具获取互联网中被黑的网站，抹去其他黑客的印记，批量植入后门和黑页，变成自己的所有品。

对于这种篡改手段，网站管理员直接删除服务器上的黑页即可，随后还需要对网站进行全站检查，清除后门，修补漏洞。

篡改手段三、DNS 劫持

DNS 劫持又叫域名劫持，说到域名劫持，很多人都不会陌生，经常在上网的时候，打开一个网址，却访问到一个“不可描述”的网页。这种现象极有可能是网站发生了 DNS 劫持。

DNS 劫持是互联网攻击的一种方式，通过攻击域名解析服务器（DNS），或伪造域名解析服务器（DNS）的方法，把目标网站域名解析到错误的地址从而实现用户无法访问目标网站的目的。

曾经在处理一起应急响应事件中，发现某政府网站所有的二级域名都被“金沙娱乐”IP 所劫持。属于典型的泛域名解析劫持事件。

图 2.3.2-4

对于此类篡改事件，一般都是域名管理平台被黑客入侵，恶意修改解析 IP，将赌博网站解析到受害者域名。

对于站长来说，DNS 劫持危害严重，一方面可能影响用户的上网体验，用户被引到假冒的网站进而无法正常浏览网页，而用户量较大的网站域名被劫持后恶劣影响会不断扩大；另一方面用户可能被诱骗到冒牌网站进行登录等操作导致泄露隐私数据。

遇到此类篡改的网站管理员，需立即修改域名管理平台密码，加强密码复杂度。并将恶意解析的 IP 地址换成自己服务器的 IP 地址。

篡改手段四、网站前端劫持

网站前端劫持又称之为跳转劫持，其表象为用户输入地址 A，在浏览器中访问后跳转到地址 B。此类篡改通常是在网站的相应页面中插入 JS 脚本，通过 JS 来进行跳转劫持。

输入被劫持的网站时，浏览器会执行相应的 JS 脚本。跳转到需要引入流量做推广的网站，经典案例如下图所示：

图 2.3.2-5

随着网民安全意识越来越高，以上三种篡改手段带来的价值越来越低，由于篡改特征太过明显，通常篡改后不到几分钟就会被发现并删除。因此，黑客除了在网页中直接加入 JS 跳转代码外，通常还会加入附加条件。判断条件一般会根据 IP 归属地、user-agent 或 referer 进行判断。

加入附加条件后的网站篡改隐蔽性更高，例如下图篡改案例：

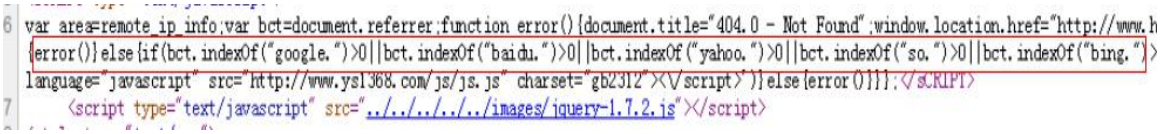


图 2.3.2-6

当判断使用“google”、“baidu”、“yahoo”、“so.”、“bing”等搜索引擎搜索词网站时呈现加载 JS 脚本，返回博彩、娱乐等页面；当人工正常访问网站时则呈现正常网站内容。

这种篡改手段对于正常的人工访问会返回正常的内容，所以导致这种网站很难发现、并且其存留时间相对较长，同时可被搜索引擎爬虫所收录，提高 SEO 搜索排名。

网站首页被植入 JS 跳转代码。针对这种篡改案例，需要清除网站页中 JS 跳转代码，同时全站查找后门，修复漏洞。

篡改手段五、网站服务器劫持

服务端劫持也称为全局劫持，此手法为修改网站动态语言文件，判断访问来源控制返回内容，从而达到网页劫持的目的。其特点往往是通过修改 asp/aspx/php 等后缀名文件，达到动态呈现网页内容的效果。

服务器劫持类篡改是在服务器上执行的，因此不像前端劫持那样可以分析加载的恶意 JS 脚本。很多时候，打开网站可以看到篡改标题或链接，但是打开对应文件准备清除恶意代码时却找不到对应内容。如下图所示（在服务器上找不到“传奇私服”关键字）：

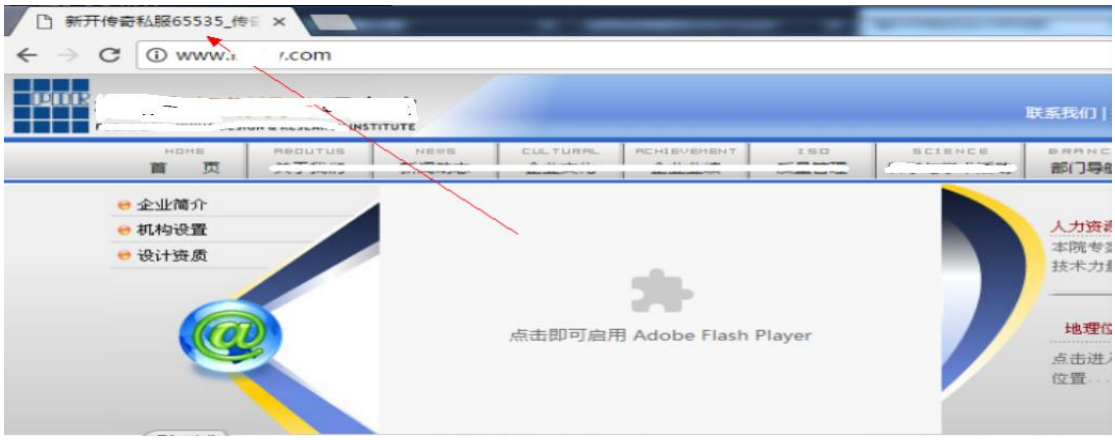


图 2.3.2-7

对于这种篡改情况，一般是在服务器段做了劫持，其需要在服务器上进行分析。一般检测都是要检测全局脚本文件，分析其是否被恶意修改。如 global.asax、global.asa、conn.asp、conn.php 这种比较特殊文件每次加载时都会加载的配置文件，如访问 x.php 时会加载 conn.php。这种文件一般情况下不会经常修改，因此可以使用文件完整性进行检测。初次配置好了以后生成其 MD5 或 HASH 值，并且周期性对比其 MD5 值是否变化。若变化则进行变化内容的分析与检测。

安全建议

以上 5 种篡改手段，除了 DNS 劫持外，其他 4 类篡改无一例外的属于网站被恶意入侵，文件遭到了非法修改。在对这些被篡改网站进行网络知名 webshell（如：g00nshell、CTT-Shell、Ekin0x-Shell、r57shell、php-webshell 等）进行探测，发现 10%网站依然存在后门。且 webshell 路径极其简单，非常容易被二次利用。因此，在修复网站篡改的同时，也要完全清除网站后门，才能避免二次篡改。因此，针对被篡改的网站，给出以下安全建议：

- 定期修改域名解析管理密码、网站后台管理密码，并保证密码复杂度；
- 定期检测网站漏洞，及时修复漏洞；
- 定期备份网站文件，并检查文件完整性，尤其是一些不常修改的配置文件；
- 对于已被入侵的网站，及时清理篡改和暗链，并在全站查找并清除后门，最后通过专业漏扫工具或安全渗透专员查找网站漏洞，完全修补漏洞。

1.4 攻击防护情况

1.4.1 网站攻击整体解读

2017 年是网络攻击达到高峰的一年，各种安全事件频发，攻击工具泛滥，导致 2017 年的攻击流量比 2016 年多出 52%。

2017 年 1 月 1 日开始至 12 月 31 日截止，深信服下一代防火墙、信服云盾等安全防护产品对全国 11 个行业（其中包括政府、教育、医疗、金融、企业、能源等）超过 10w 个域名（或 IP）做安全防御，共拦截网络攻击 86.2 亿次。封锁恶意攻击 IP 15.9w 个。每月拦截攻击次数，封锁 IP 个数走势图如下：

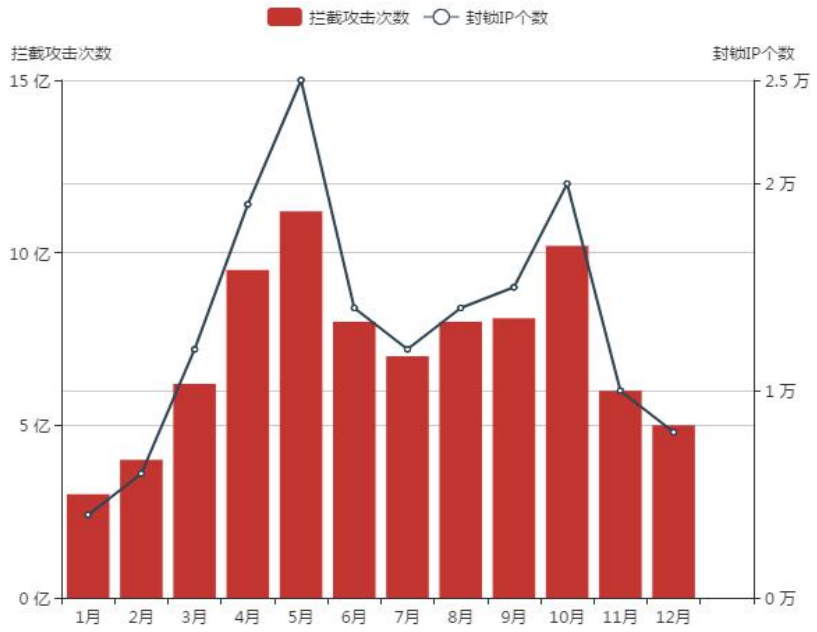


图 2.4.1-1

从被攻击流量数据来看，2017 年中攻击流量最多的三个月分别是 4 月、5 月和 10 月。由此可以看到，在重大安全事件爆发时期，以及国家重大会议活动期间，黑客活动猖獗。因此，网络安全工作时刻不能松懈，在特殊时期更应该加固网络防护，避免中招。

1.4.2 网站攻击特征分析

我们通过对 86.2 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 如下表所示：

排名	攻击类型	拦截次数（单位：亿）
1	DDoS 攻击	20.6
2	管理登录页面探测	12.3

3	SQL 注入扫描攻击	10.2
4	XSS 注入扫描攻击	10.2
5	0DAY 漏洞扫描攻击	9.9
6	远程代码执行攻击	7.2
7	服务器探测	3.9
8	网站后门探测	3.5
9	数据库探测	2.9
10	备份文件探测	2.3

表 2.4.2-1

其中攻击拦截类型分布占比情况如下图所示：

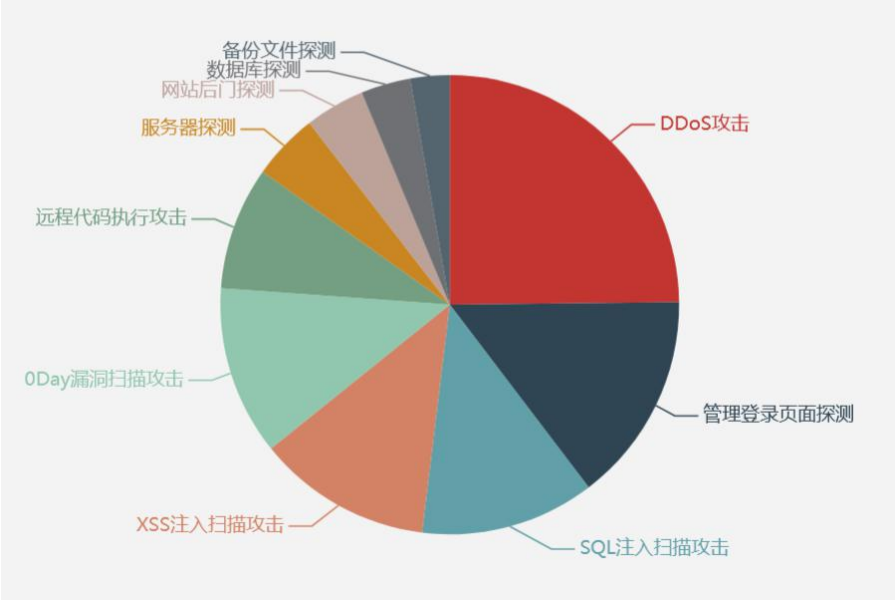


图 2.4.2-2

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。

1.4.3 网站攻击流量来源分析

千里目安全实验室对被封锁的 15.9w 恶意 IP 进行统计，发现广东地区是攻击流量的主要直接来源地，其中有 3.2w 恶意 IP 归属地为广东，总攻击达到 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：

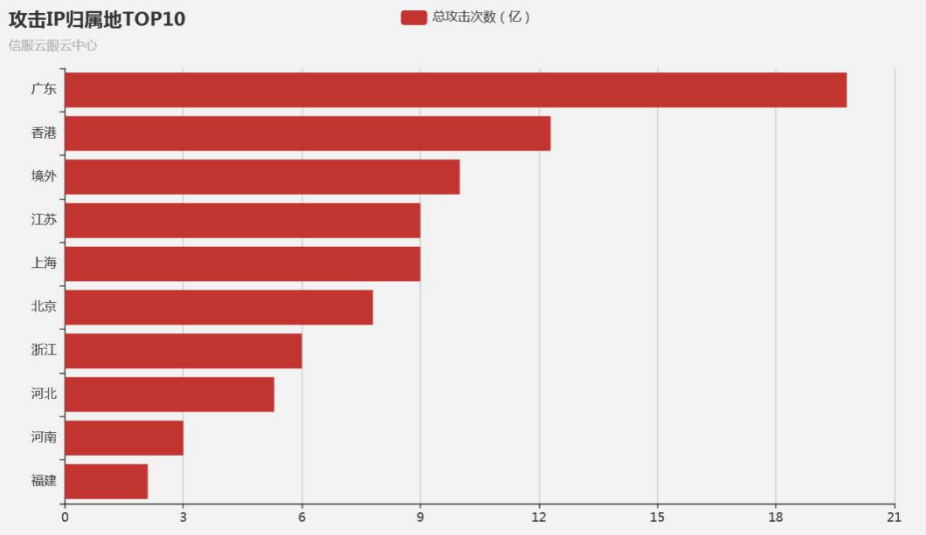


图 2.4.3-1

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。