**${company}**

**${title}**

**（${dateRange}）**



**星海安全实验室**

**应用攻击阻断云平台社区版**

**${createTime}**

目录

[1. 安全风险概况 3](#_Toc6667)

[1.1. 安全趋势 3](#_Toc17786)

[1.2. 网站安全 3](#_Toc16231)

[2. 攻击类型详情分析 3](#_Toc6304)

[3. 攻击源TOP 10分析 4](#_Toc17640)

[4. 攻击区域详情分析 4](#_Toc12642)

[5. 安全建议须知 5](#_Toc3181)

# 安全风险概况

【防护时段】：${startMonth} 至 ${endMonth};

【防护范围】：(${host})等共${hostNum}个网站，其中${parseNum}个已解析，${noParse}个未解析；

【防护动态】：所有攻击均已被星海应用攻击阻断云防护系统拦截，网站共出现0起安全事件；

【整体安全趋势】：网站群共计受到攻击${attackNum}次；

在星海应用攻击阻断云防护系统提供的专业、稳定云防护服务下，网站所有攻击均被有效阻断，未造成攻击成功或篡改成功的安全事件，有效地保障网站安全、平稳地运行。

## 安全趋势

其中拦截到的攻击次数越多，表示网络环境遭受黑客攻击的次数越多，网络环境越不安全，黑客能成功入侵的可能性越大，使用星海应用攻击阻断云防护系统能有效抵御黑客利用已存在漏洞发起的攻击。

每日攻击趋势图：

${line1}

## 网站安全

站点累计遭受${attackNum}次攻击，主要攻击目标为${attackTop2}，以上攻击被有效阻断，未造成攻击成功或篡改成功的安全事件。

${pie1}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 站点 | 攻击类型 TOP5 | 攻击次数 | 攻击占比 |
| ${allSort} | ${allHosts} | ${allType} | ${allNum} | ${allScale} |

# 攻击类型详情分析

${TYPE\_BLOCK}

#### 2.1.${type\_block\_sort} ${type\_name}

【描述】${type\_describe}

【攻击详情】

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 站点 | 目的地址 TOP5 | 攻击次数 |
| ${type\_sort} | (${type\_host}) | ${type\_urls} | ${type\_num} |

${/TYPE\_BLOCK}

# 攻击源TOP 10分析

主要攻击源来自${ipTop3Str}，以上攻击均被有效阻断。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 攻击源IP | 攻击源区域 | 攻击域名及次数 | 攻击类型 |
| ${iptop\_sort} | ${iptop\_ip} | ${iptop\_region} | ${iptop\_host} | ${iptop\_type} |

# 攻击区域详情分析

根据风暴中心数据大脑安全分析，境外攻击源主要是通过肉鸡、跳板机对网站发起恶意攻击。若网站主要访问源集中在境内，建议打开区域访问控制，限制国外地区进行访问，保障网站安全，具体攻击区域分布见下图：

${pie2}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 区域 | 主要集中IP | 攻击次数 | 攻击占比 |
| ${regiontop\_sort} | ${regiontop\_region} | ${regiontop\_ip} | ${regiontop\_num} | ${regiontop\_scale} |

# 安全建议须知

安全建议：

1) 已接入星海应用攻击阻断云防护系统的网站域名禁用IP方式进行访问，或者做好访问控制，只允许星海应用攻击阻断云防护系统IP与源站进行请求响应；

2) 如带www的子域名网站接入星海应用攻击阻断云防护系统，不带www的根域名网站禁用访问；

3) 加强同IP的其他网站的安全防护，否则还可能存在通过其他网站的安全风险进行入侵网站服务器；

4) 加固网站服务器安全：加强网站服务器的日常维护，做好网站服务器的访问控制，限定开放访问IP白名单、限定开放高危端口/服务、定期对网站服务器进行安全体检、及时消除可能存在的安全隐患；

5) 加强网站弱点修复：定期对网站开展安全风险评估，及时消除网站的漏洞风险，提升网站本身的安全性；

6) 及时清理网页后门：网站发布、升级、迁移前和日常运维过程中都要对网站源文件进行网页后门扫描和彻底清理；

7) 加强管理账号管理：加强对网站管理后台账号、FTP/SSH/VNC/远程桌面等远程维护工具账号的管理，尽可能使用强密码，并保证定期更换新密码。