SANGFOR

综合风险报表

时间范围：2016-08-01至2016-08-07

生成时间： 2016-08-06 11:22:57

域名： www.sangfor.com

一、安全风险概况

整体安全

时间范围：2017-06-22至2015-06-31

综合**网站安全态势**评级: 差

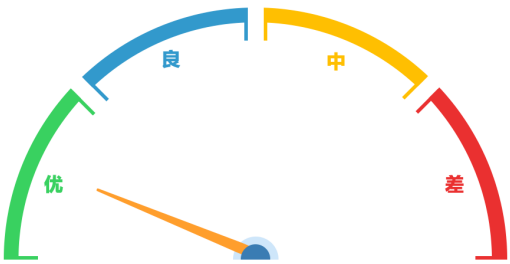
防护前：中

综合网站安全态势

开启

下一代防火墙

防护后：优



防护后综合网站安全态势

开启下一代防火墙策略后，整体网站状况得到提升，网站安全态势评级为：优

如果未开启策略，将遭受如下攻击：

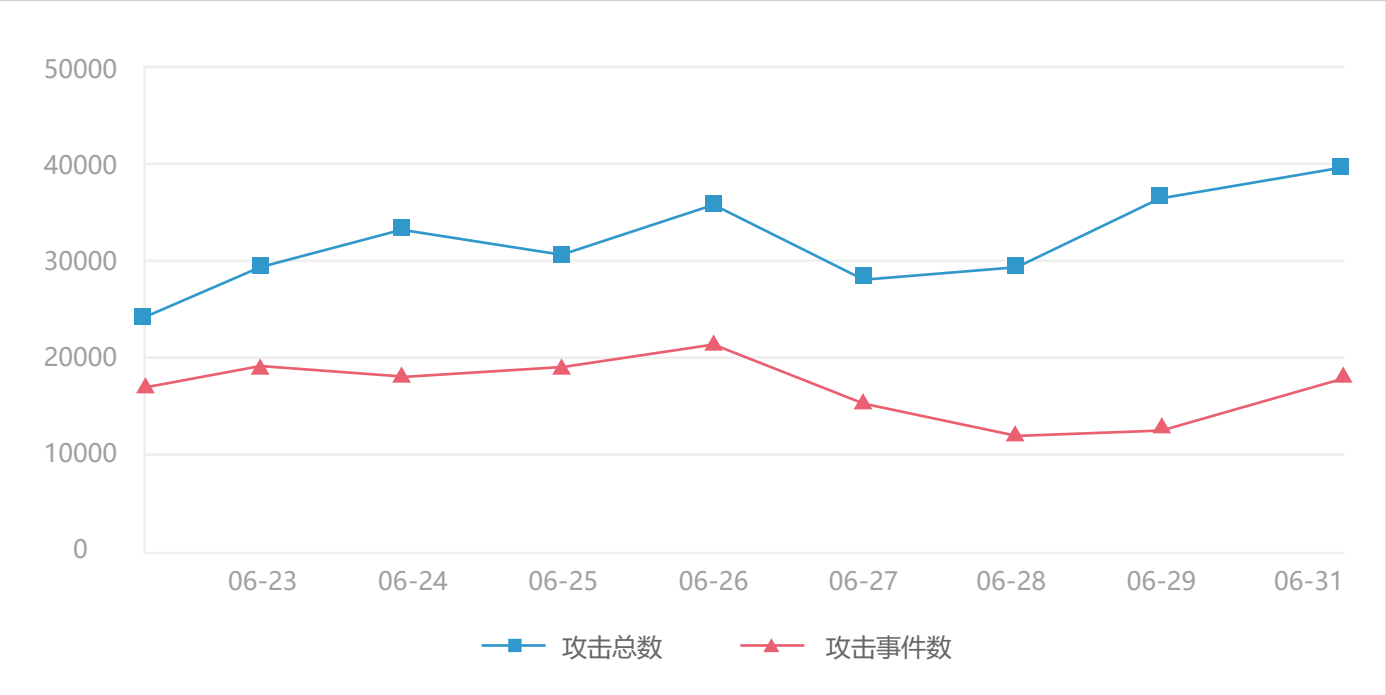
风 险	测试系统（180.170.170.11）	建议： 请参考对应业务，用户风险详情中的安全加固建议进行处理，避免造成严重的业务损失
黑 链	新闻发布主站（www.test.com）已被挂一个黑链	建议： 1、清除对应页面黑链内容 2、下载主机安全检测工具，对网站进行全面扫描
攻 击	共遭受攻击者攻击3215次	结论： 虽然当前网站整体情况较差，但大部分攻击已被防火墙防护
漏 洞	共发现漏洞553个，其中高危漏洞101个，共发现被利用的漏洞21个	结论： 当前业务系统整体脆弱性较高，请参考防火墙，运行状态>实时漏洞风险>查看完整报表，找到对应的漏洞解决方案，进行修复

1.2 攻击概述

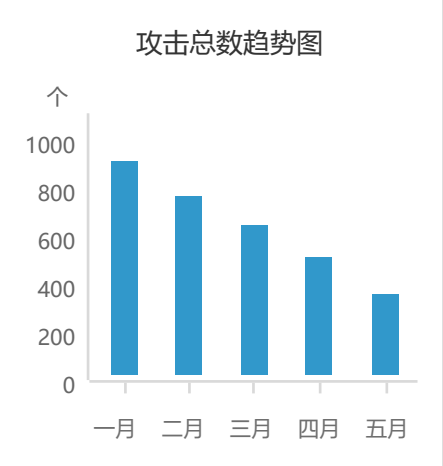
攻击趋势

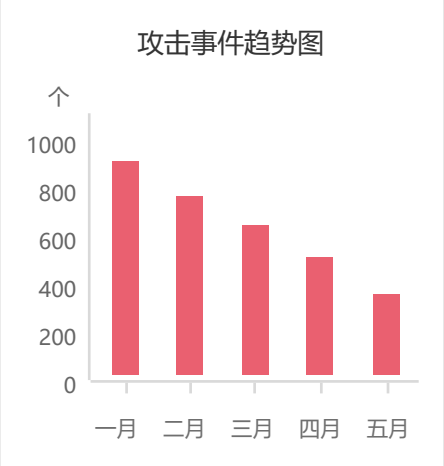
攻击总数：攻击数越多，说明网络环境遭受信息收集或攻击的次数越多，网络环境越不安全

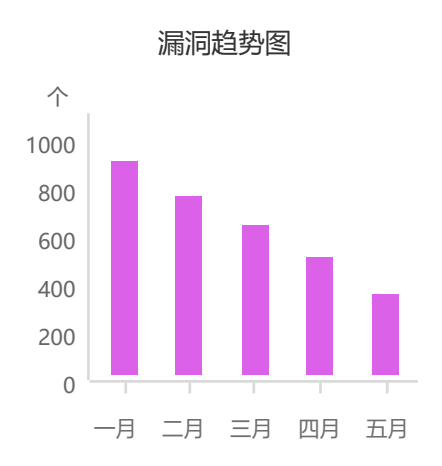
攻击事件：拦截数越多，说明配置的防火墙防护策略防护效果越好，被防护区域业务系统被控制的可能性越低



攻击趋势图

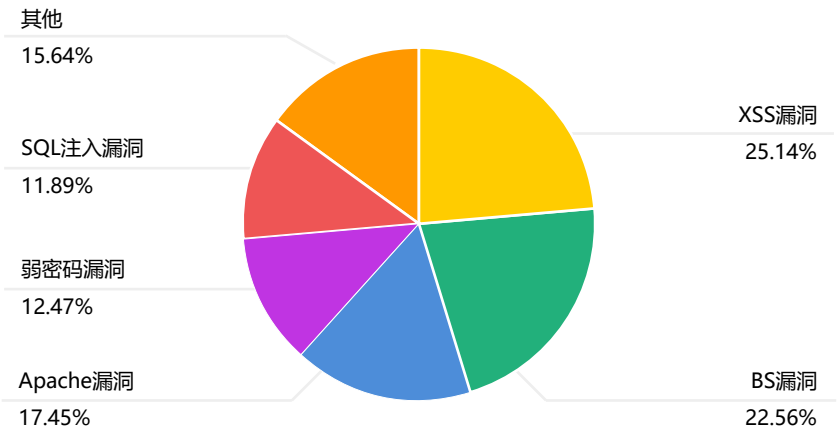




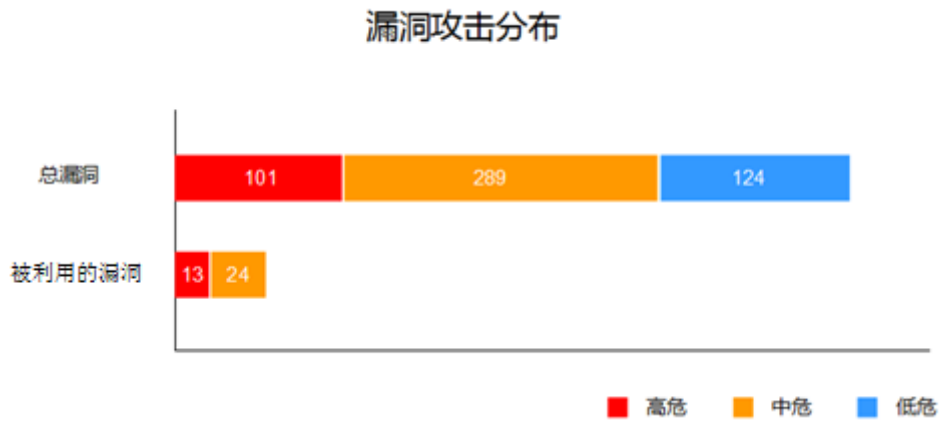


安全漏洞

发现防护区域漏洞类型分布如下：



共发现514个漏洞，其中37个漏洞被攻击者利用，且已被云WAF防护，其中高危漏洞13个，中危漏洞24个



二、风险详情分析

业务安全

遭受攻击最严重的业务系统如下：

序号	处理状态	被褥入侵的服务器	业务组	综合严重级别	最近检测时间	攻击次数
1	未处理	58.49.248.121	测试系统	已被入侵（5级）	2017-06-31 10：24：12	56
2	已处理	182.11.8.33.7	财务系统	已被入侵（5级）	2017-06-31 10：24：12	54
3	未处理	193.107.88.186	研发代码服务器	已被入侵（5级）	2017-06-31 10：24：12	54
4	未处理	5.39.251.4	邮件服务器	已被入侵（5级）	2017-06-31 10：24：12	50
5	未处理	180.170.170.21	ERP	已被入侵（5级）	2017-06-31 10：24：12	46
6	未处理	180.170.170.24	BBS	已被入侵（5级）	2017-06-31 10：24：12	43
7	未处理	180.170.170.12	host.sangfor.com	已被入侵（5级）	2017-06-31 10：24：12	42
8	未处理	221.238.195.113	CRM系统	已被入侵（5级）	2017-06-31 10：24：12	34
9	已处理	193.107.88.186	BBS	已被入侵（5级）	2017-06-31 10：24：12	24
10	已处理	5.39.251.4	新闻发布主站	已被入侵（5级）	2017-06-31 10：24：12	15

2.1.2 篡改监测

www.sangfor.com网站已被篡改10次，具体详情如下:

域名	时间	动作
www.sangfor.com	2016.08.01 18:00:00	异常：网页图片被替换，具体图片为： www.sangfo.com/images/pymx.gif www.sangfo.com/images/ontop6.gif www.sangfo.com/images/common6.gif 已联系管理员
www.sangfor.com	2016.08.01 18:00:00	异常：网站首页被非法篡改，请立即前往www.sangfor.com查看并恢复。 已联系管理员

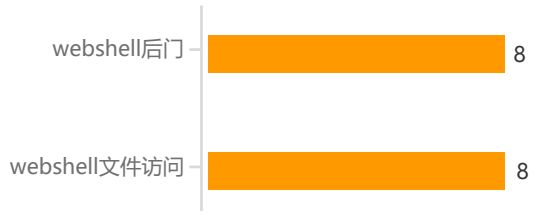
建议：您可以访问网站 www.sangfor.com进行验证,并清除篡改文件

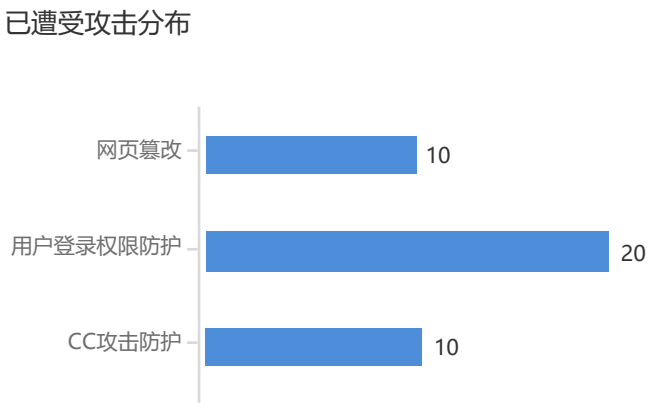
2.2 防护服务

测试系统（180.170.170.11）总体风险等级评级为：**严重**（已被入侵）

180.170.170.11服务器已被攻击者控制，共发现攻击56次，探测到漏洞3个

系统存在8个Webshell后门，系统被挂的Webshell已被黑客访问了8次





90.0.0.100（未处理）

总体综合风险等级评级为：**严重**（已被感染）

90.0.0.100共遭受威胁270次，目前处于命令控制与通信阶段,该阶段表示主机感染了恶意软件并且和黑客建立了控制通道

用户安全

僵尸主机

遭受威胁最严重的主机如下：

序号	处理状态	受感染主机	区域	综合严重级别	最近检测时间	检测次数
1	未处理	58.49.248.121	WAN	已被感染（9级）	2017-06-31 10：24：12	56
2	已处理	182.11.8.33.7	WAN	已被感染（8级）	2017-06-31 10：24：12	54
3	未处理	193.107.88.186	WAN	已被感染（8级）	2017-06-31 10：24：12	54
4	未处理	5.39.251.4	WAN	已被感染（8级）	2017-06-31 10：24：12	50
5	未处理	180.170.170.21	WAN	已被感染（8级）	2017-06-31 10：24：12	46
6	未处理	180.170.170.24	WAN	已被感染（8级）	2017-06-31 10：24：12	43
7	未处理	180.170.170.12	WAN	很可能感染（7级）	2017-06-31 10：24：12	42
8	未处理	221.238.195.113	WAN	很可能感染（7级）	2017-06-31 10：24：12	34
9	已处理	193.107.88.186	WAN	很可能感染（7级）	2017-06-31 10：24：12	24
10	已处理	5.39.251.4	WAN	很可能感染（7级）	2017-06-31 10：24：12	15

2.2.1.2 攻击源

www.sangfor.com遭受攻击共7923次，以下为主要攻击源

序号	攻击来源	IP归属地	攻击次数
1	58.49.248.121	中国，湖北，武汉	2999
2	182.11.8.33.7	中国，河南	630
3	193.107.88.186	波兰	470
4	5.39.251.4	英国	133

安全加固

当前业务系统已被入侵，建议按照以下建议进行安全加固

1、未处理状态

- 根据具体业务系统风险详情添加对应防火墙防护策略之后，再登录防火墙“运行状态>安全状况>入侵风险”标记对应业务系统为“已处理”状态

2、Webshell后门

- 下载主机安全检测清除工具，对网站被植入的webshell进行检测和清除
  （工具下载地址：http://sec.sangfor.com,cn/apt ）
- 开启应用防火墙的WEB应用防护策略，并将“检测攻击后操作>动作”配置为“拒绝”

3、攻击源IP黑名单

- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

安全加固

1、未处理状态

- 根据具体主机威胁详情添加对应防火墙防护策略之后，再登录防火墙“运行状态>安全状况>入侵风险”标记对应主机为“已处理”状态

2、已被感染

- 当前主机已被感染，请下载主机安全检测清除工具，对受感染的主机进行僵尸病毒检测和清楚
  （工具下载地址：http://sec..sangfor.com.cn/apt ）

2.2.2 篡改事件

2.2.2.1 篡改事件详情

事件类型	尝试入侵
事件详情	www.sangfor.com遭受来自-（未知区域）的攻击2次，其中网页篡改2次
攻击举证	篡改详情： GET /pagead/show_ads.js HTTP/1.1 Host: pagead2.googlesyndication.com Connection: keep-alive Cache-Control: max-age=0 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 Accept: */* Referer: http://www.w3school.com.cn/php/php_file_create.asp Accept-Encoding: gzip, deflate, sdch Accept-Language: zh-CN,zh;q=0.8 If-None-Match: 14124271275959182453

2.2.2.2 攻击源

www.sangfor.com遭受篡改共10次，以下为主要攻击源

序号	攻击来源	IP归属地	攻击次数
1	58.49.248.121	中国，湖北，武汉	2999
2	182.11.8.33.7	中国，河南	630

2.2.3 漏洞事件

2.2.3.1 漏洞详情

序号	漏洞名称	影响的域名/IP	漏洞总数	是否被利用	风险等级	防护状态
1	SQL注入漏洞	www.tongji.edu.com	1	是	高	已防护

2.2.3.2 安全加固

1、SQL注入漏洞

- 页面存在传SQL语句安全漏洞，建议修改服务器端代码，严格限制用户输入参数

2、IIS漏洞

- 升级到 Apache 2.0.50 或者更高的版本

三、风险评估模型&危害说明

3.1 风险评估说明

网站风险是通过对防护站点的所有入侵风险日志进行综合关联分析得到的，其中严重等级分为已被入侵、曾被攻击、曾被收集信息、存在漏洞；具体评级规则如下：

当整体网站状况评级为**差**：

- 网站严重等级评级为**严重**(已被入侵)

当整体网站状况评级为**中**：

- 网站严重等级评级为**高危**(曾被攻击)
- 网站严重等级评级为**中危**(曾被收集信息)

当整体网站状况评级为**良**：

- 网站严重等级评级为**低危**(存在漏洞)

当整体网站状况评级为**优**：

- 网站不存在漏洞且未受到攻击；或者网站不存在任何风险

3.2 危害说明

3.2.1 黑链

黑链是SEO(搜索引擎优化)手法中相当普遍的一种手段，笼统地说，它就是指一些人用非正常的手段获取的其它网站的反向链接，最常见的黑链就是通过各种网站程序漏洞获取搜索引擎权重或者PR较高的网站的webshell，进而在被黑网站上链接自己的网站，其性质与明链一致，都是属于为高效率提升排名，而使用的作弊手法。如果网站内容被篡改成包含如赌博、游戏、色情等非法及不良信息，存在被监管部门通报的风险

攻击演示：http://www.sangfor.com/xingxiao/heilian.html

解决方案：

- 查看被植入黑链的页面的源代码，清除所有被篡改的内容
- 下载网站安全检测工具，对网站进行全面的黑链检测和清除（工具下载地址：http://sec.sangfor.com.cn/apt）

3.2.2 Webshell后门

在已知WEB系统漏洞情况下，攻击者利用WEB系统漏洞将WEBSHELL页面成功植入到WEB系统中，攻击者通过WEBSHELL页面访问数据库，执行系统命令并长期的操控WEB系统

攻击演示：http://www.sangfor.com/xingxiao/webshell.html

解决方案：

- 下载网站安全检测清除工具，对网站被植入的webshell进行检测和清除（工具下载地址：http://tool.sangfor.com）

3.2.3 尝试入侵

以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为，利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。 这种行为往往经过长期的经营与策划，并具备高度的隐蔽性。攻击手法在于隐匿自己，针对特定对象，长期、有计划性和组织性地窃取数据，这种发生在数字空间的偷窃资料、搜集情报的行为，就是一种网络间谍的行为

- SQL注入：攻击者利用此漏洞盗取数据库中数据，导致WEB业务信息泄漏，危及数据库账户信息安全
- 口令暴力破解攻击：服务器开放了基于密码认证的服务，攻击者可以使用暴力破解工具对服务器进行暴力破解；一旦暴力破解成功，可以通过服务器做任何操作
- XSS攻击：攻击者利用此漏洞盗取用户COOKIE信息，伪造用户身份登录WEB系统，当盗取的是普通用户的COOKIE时，普通用户的个人安全受到威胁，当盗取的是管理员或者特殊用户的COOKIE时，威胁到整个WEB系统的安全

攻击演示：http://www.sangfor.com/xingxiao/attack.html