SANGFOR

综合风险报表

时间范围：2016-06-04至2016-06-04

生成时间： 2016-06-04 04:20:35

业务系统域名/IP： 全部

用户终端IP： 全部

一、安全风险概况

1.1 整体安全

时间范围：2016-06-04至2016-06-04

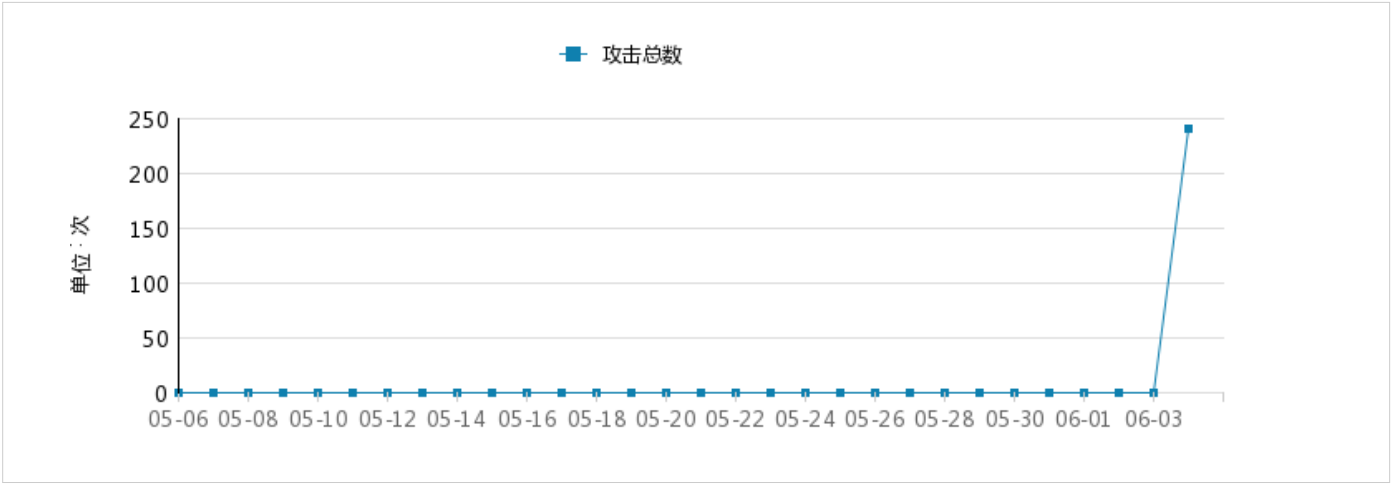
综合网络安全态势　　防护后综合网络安全态势

开启下一代防火墙策略后，整体网络状况得到提升，网络安全态势评级为：**良**
如果未开启策略，将遭受如下攻击：

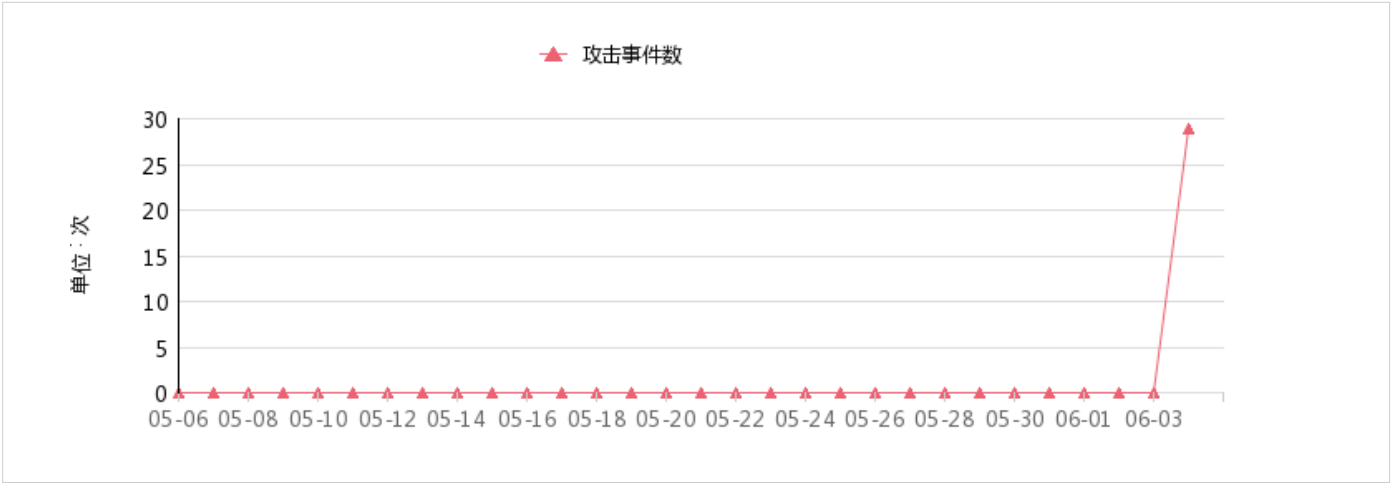
风 险	192.168.88.6、192.168.88.8、192.168.88.7等共11个服务器已被入侵 192.168.88.22、192.168.88.19共2个主机已被感染	**建议：** 请参考对应业务、用户风险详情中的安全加固建议进行处理，避免造成严重的业务损失
黑 链	192.168.88.6已被挂10个黑链 192.168.88.8已被挂10个黑链 192.168.88.7已被挂10个黑链	**建议：** 1. 清除对应页面黑链内容 2. 下载主机安全检测工具，对网站进行全面扫描
攻 击	共遭受攻击者攻击241次	**结论：** 虽然当前网络整体情况较差，但大部分攻击已被防火墙防护
漏 洞	共发现漏洞数22个，其中高危漏洞22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 攻击趋势

攻击总数：防火墙检测到攻击者对防护区域发起的所有攻击行为；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

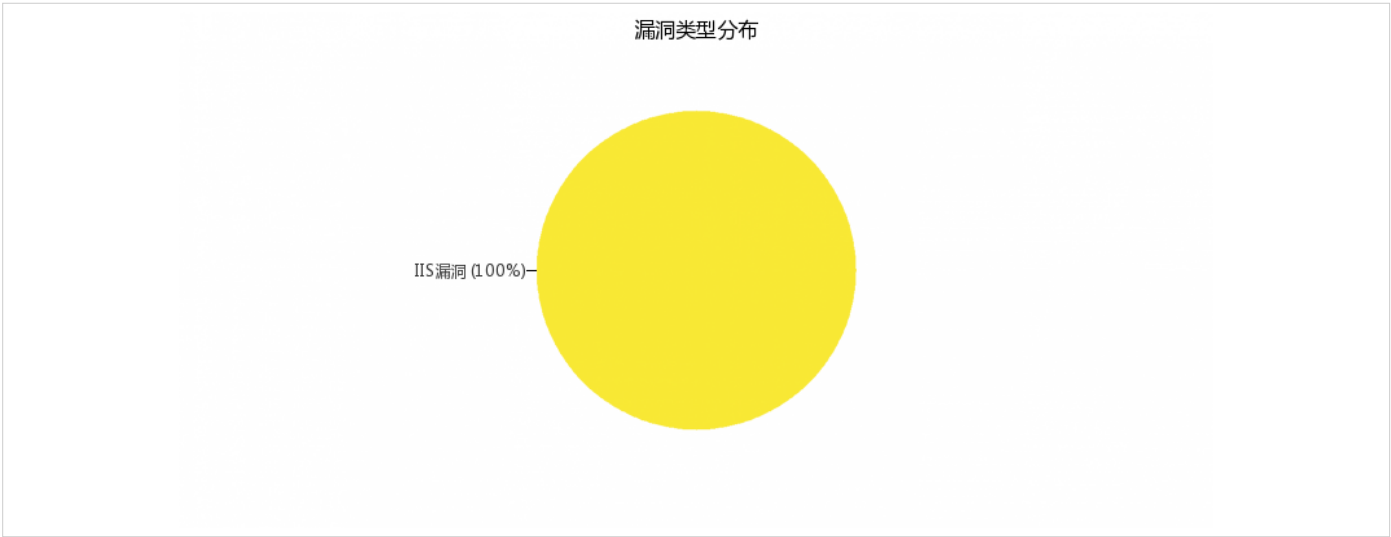


攻击事件：通过对多维攻击日志进行处理，结合攻击链分析技术，提炼出最关键的安全事件；攻击事件数越多，说明针对性攻击的次数越多，被防护区域的业务系统或主机被渗透的可能性越大，网络安全风险越高

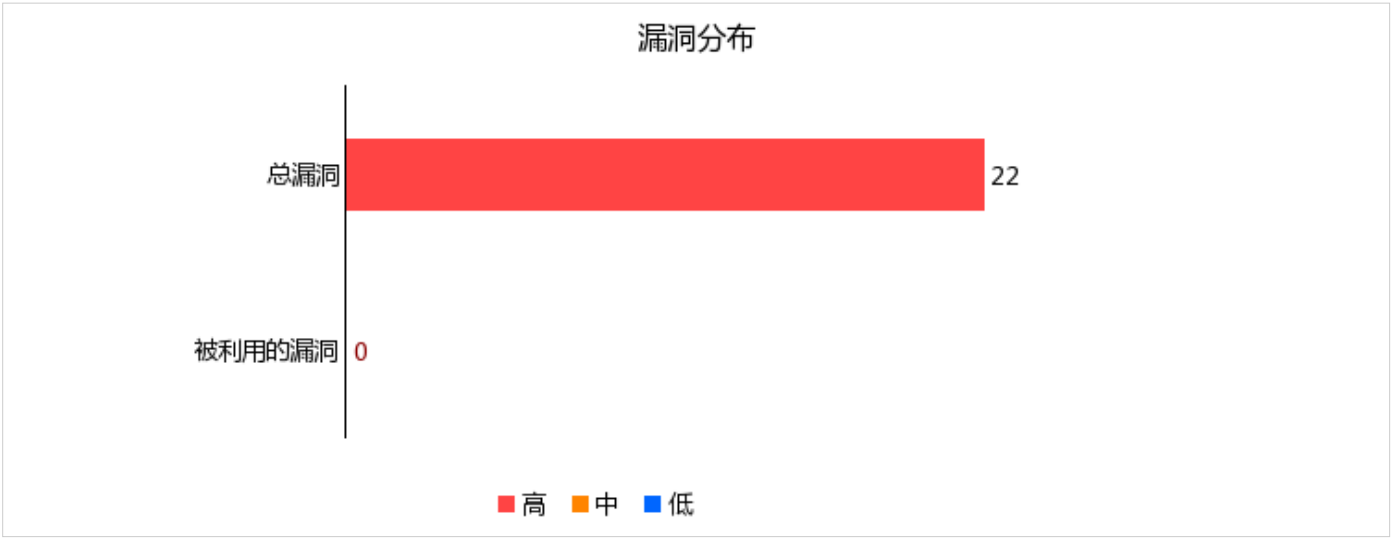


1.3 漏洞安全

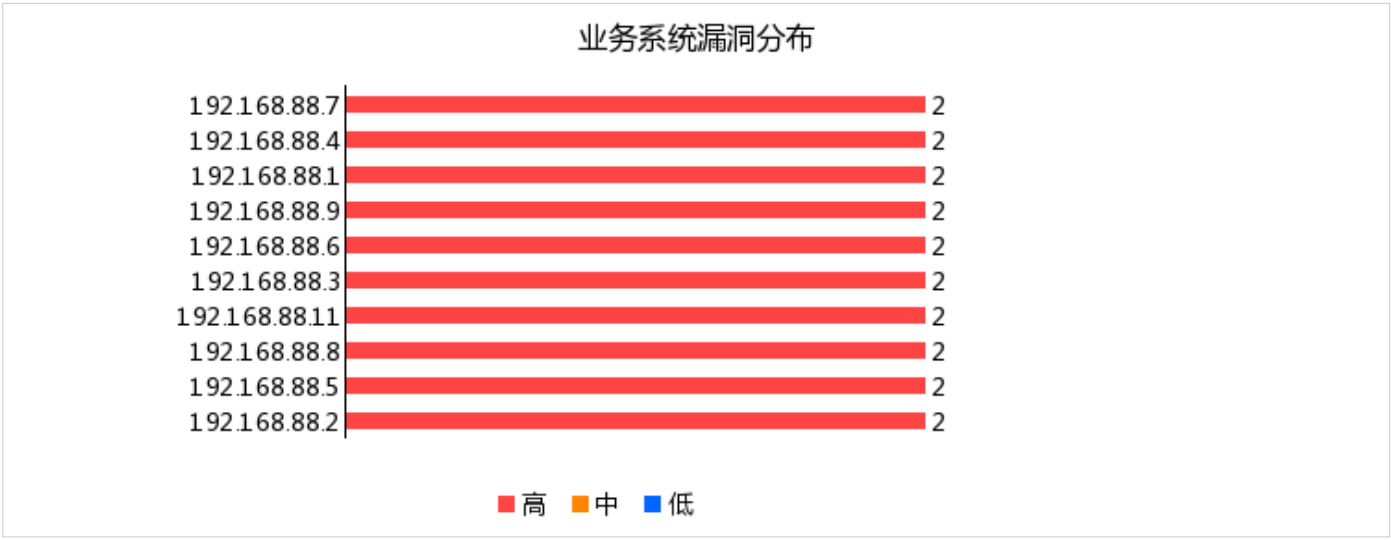
发现被防护区域漏洞类型分布如下：



共发现22个漏洞，22个高危漏洞，未发现有漏洞被攻击者利用



按漏洞严重等级统计，影响最大的业务系统分布如下：



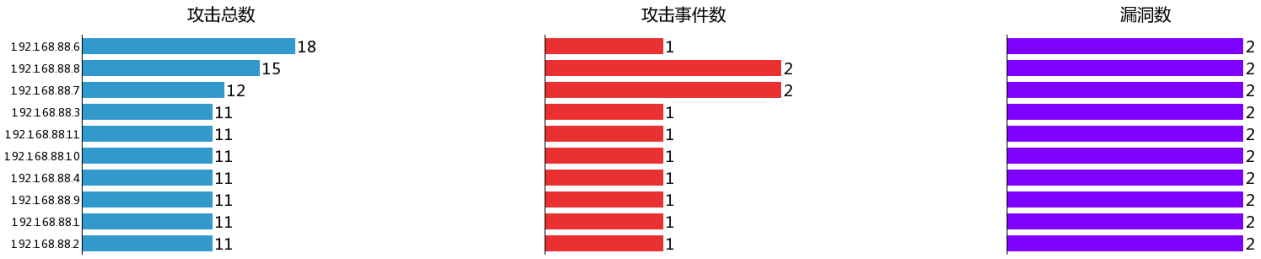
1.4 业务安全

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	拦截次数	拦截率
1	未处理	192.168.88.6	-	已被入侵（5级）	2016-06-04 03:41:47	18	1	5.56%
2	未处理	192.168.88.8	-	已被入侵（5级）	2016-06-04 03:54:04	15	1	6.67%
3	未处理	192.168.88.7	-	已被入侵（5级）	2016-06-04 03:45:00	12	1	8.33%
4	未处理	192.168.88.3	-	已被入侵（5级）	2016-06-04 03:16:22	11	1	9.09%
5	未处理	192.168.88.11	-	已被入侵（5级）	2016-06-04 04:06:21	11	1	9.09%

6	未处理	192.168.88.10	-	已被入侵（5级）	2016-06-04 04:02:28	11	1	9.09%
7	未处理	192.168.88.4	-	已被入侵（5级）	2016-06-04 03:20:19	11	1	9.09%
8	未处理	192.168.88.9	-	已被入侵（5级）	2016-06-04 03:59:07	11	1	9.09%
9	未处理	192.168.88.1	-	已被入侵（5级）	2016-06-04 03:07:11	11	1	9.09%
10	未处理	192.168.88.2	-	已被入侵（5级）	2016-06-04 03:11:40	11	1	9.09%

各业务风险分布



攻击事件

通过对多维攻击日志进行处理，结合攻击链分析技术，提炼出最关键的安全事件

- 已被入侵（业务系统被攻击者攻陷，已被挂马或篡改）
- 僵尸受控（终端/服务器已被攻击者远程控制沦为“肉鸡”）
- 尝试入侵（攻击者对业务系统发起的针对性攻击，但并未有数据证明已被攻击者攻陷）

序号	事件	详情分析
1	已被入侵	共11台服务器已被攻陷，192.168.88.6、192.168.88.8、192.168.88.7等共10台服务器检测到被挂载WEBSHELL后门，192.168.88.6、192.168.88.8、192.168.88.7等共11台服务器存在黑链
2	僵尸受控	共2台主机已经被控制沦为“肉鸡”，其中包含192.168.88.8、192.168.88.7
3	尝试入侵	1）192.168.88.6共遭受了8次攻击，主要攻击类型包括：WEBSHELL后门、弱口令类型-长度小于等于8位字典序、弱口令类型-长度小于等于6位仅数字和字母、弱口令类型-弱口令列表、弱口令类型-长度小于等于8位纯数字，其中来自188.188.208.108（比利时）的攻击8次

全网攻击源

以下为发起攻击最多的攻击源，建议登录控制台，配置：系统>全局放行与封堵>封堵名单

序号	IP	攻击类型	攻击次数	拦截次数	拦截率	IP归属地

1	188.188.208.108	WEBSHELL后门(10) SQL 注入(10) WEBSHELL上传(10) WEB登录弱口令防护(10) XSS 攻击(6)	69	50	72.46%	比利时
2	192.168.88.29	mail漏洞攻击(3) web漏洞攻击(3) system漏洞攻击(3) shellcode漏洞攻击(2)	11	9	81.82%	内部地址
3	192.168.88.35	SQL 注入(4)	4	0	0%	内部地址
4	192.168.88.36	敏感信息防护(3)	3	3	100%	内部地址
5	192.168.88.30	口令暴力破解攻击(1)	1	1	100%	内部地址

海外攻击源

以下为发起攻击最多的海外攻击源，建议登录控制台，配置：系统>全局放行与封堵>封堵名单

序号	IP	攻击类型	攻击次数	拦截次数	拦截率	IP归属地
1	188.188.208.108	WEBSHELL后门(10) SQL 注入(10) WEBSHELL上传(10) WEB登录弱口令防护(10) XSS 攻击(6)	69	50	72.46%	比利时

1.5 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	最近活跃时间	检测	拦截次数	拦截率
1	未处理	192.168.88.22	lan	已被感染（8级）	2016-06-04 03:09:05	2	0	0%
2	未处理	192.168.88.19	lan	已被感染（8级）	2016-06-04 03:09:05	1	0	0%
3	未处理	192.168.88.35	lan	很可能感染（7级）	2016-06-04 03:09:06	4	0	0%
4	未处理	192.168.88.36	lan	很可能感染（7级）	2016-06-04 03:09:06	3	3	100%
5	未处理	192.168.88.30	lan	很可能感染（7级）	2016-06-04 03:09:06	1	1	100%
6	未处理	192.168.88.29	lan	很可能感染（6级）	2016-06-04 03:09:05	11	9	81.82%
7	未处理	192.168.88.15	lan	很可能感染（6级）	2016-06-04 03:09:05	1	1	100%

8	未处理	192.168.88.14	lan	很可能感染（6级）	2016-06-04 03:09:05	1	1	100%
9	未处理	192.168.88.16	lan	很可能感染（6级）	2016-06-04 03:09:05	1	0	0%
10	未处理	192.168.88.13	lan	很可能感染（5级）	2016-06-04 03:09:05	8	0	0%

潜在恶意文件

云端沙盒分析平台检测到0day漏洞利用的恶意文件如下：

序号	样本md5	病毒名	严重性	受感染主机	受感染主机数	检测	拦截次数	拦截率	最近检测时间
1	0770ee8cb619-b3d090ad3282-c600b020	W97M/Marke-r.GB	高	192.168.88.1(2)	1	2	0	0%	2016-06-04 03:09:03
2	0220570b61f5-e7e33ca1447ff-bcaabea	Win32/Packe-d.MoleboxVS.A	高	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03
3	2d6f2e8293cb-18524a2e9e4b-2319224a	Win32/Agent.-WFY	高	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03
4	36e3743b17c3-3b1fa901a432-57e6ed37	Win32/Wapo-mi.O	高	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03
5	2858b8632c1f-2dd8de76e329-0b471b7d	SF/Exploit.Ag-ent.RAO	高	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03

恶意网址

云端沙盒分析平台检测到0day漏洞利用的恶意网址如下：

序号	网址	类别	访问主机	访问主机数	检测	拦截次数	拦截率	最近活跃时间
1	202.115.144.196/Upl-oadFiles/HtmlEditor/-201452092334955.zip	恶意网页	192.168.88.1(2)	1	2	0	0%	2016-06-04 03:09:03
2	www.sh198.com/por-tal.php	恶意网页	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03
3	122.224.34.201:1898-9/mainapp.dll	恶意网页	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03
4	sync.ad-stir.com/	非法的博彩网站	192.168.88.2(1)	1	1	0	0%	2016-06-04 03:09:03
5	www.sh1121.com/%-C6%BB%B9%FB%CE-%A2%B1%E4.rar	恶意网页	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03
6	www.fzzyue.com/	恶意网页	192.168.88.1(1)	1	1	0	0%	2016-06-04 03:09:03

建议：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除（工具下载地址：http://sec.sangfor.com.cn/apt）

1.6 总体安全加固建议

1、请按照防火墙管理系统首页的“待处理事件”建议进行处理和修复
2、对发现的漏洞，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
3、建议把以上攻击源IP加入黑名单，拦截其访问攻击，配置：系统>全局放行与封堵>封堵名单
4、其它解决方案请查看各业务、用户风险详情的“安全加固”章节

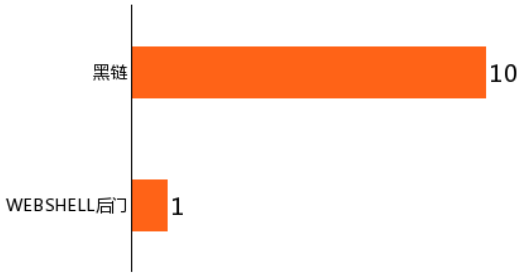
二、业务风险详情分析

2.1 192.168.88.6风险详情（未处理）

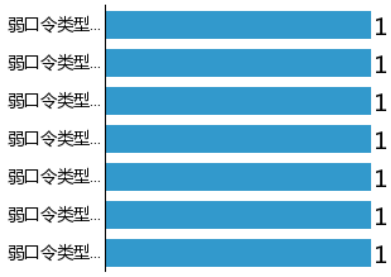
192.168.88.6总体风险评级为：严重（已被入侵）

192.168.88.6服务器已被攻击者控制。共发现攻击18次，探测到漏洞2个
网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门

已被入侵攻击数



已遭受攻击分布



2.1.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.6已经被挂10个黑链
攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.6已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

2.1.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.1.3 攻击源

以下是攻击192.168.88.6的主要攻击源，遭受攻击共18次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	弱口令类型-用户名和密码相同(1) 弱口令类型-长度小于等于8-位字典序(1) 弱口令类型-长度小于等于8-位纯数字(1) 弱口令类型-长度小于等于8-位纯字母(1) 弱口令类型-长度小于等于6-位仅数字和字母(1)	比利时	8	1	12.5%

2.1.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙WEB应用防护策略，并将“检测攻击后操作>动作”配置为“拒绝”

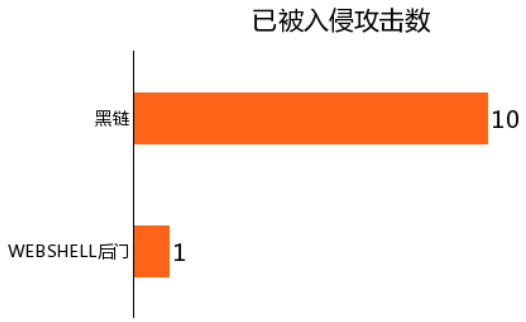
3. 攻击源IP黑名单

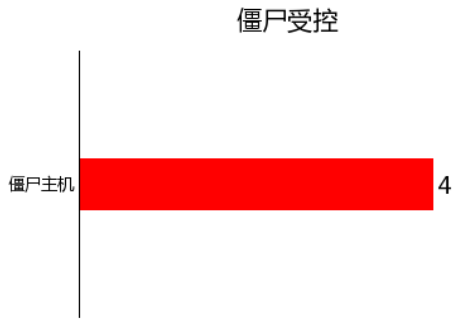
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.2 192.168.88.8风险详情（未处理）

192.168.88.8总体风险评级为：严重（已被入侵）

192.168.88.8服务器已被攻击者控制。共发现攻击15次，探测到漏洞2个
网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门





2.2.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.8已经被挂10个黑链
攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.8已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

事件类型	僵尸受控
事件详情	192.168.88.8已被攻击者远程控制沦为“肉鸡”
攻击举证	2016-06-04 03:09:04 试图短时间内解析如下僵尸网络C&C服务器tmiqqddnca.com的地址，该主机-可能已中飞客蠕虫病毒，详细威胁请查看风险详情 （2次） 2016-06-04 03:09:04 试图短时间内解析如下僵尸网络C&C服务器cobum.net的地址，该主机可能已-中飞客蠕虫病毒，详细威胁请查看风险详情 （2次）

2.2.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.2.3 攻击源

以下是攻击192.168.88.8的主要攻击源，遭受攻击共15次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.2.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙WEB应用防护策略，并将“检测攻击后操作>动作”配置为“拒绝”

3. 僵尸受控

- 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除（工具下载地址：http://sec.sangfor.com.cn/apt ）

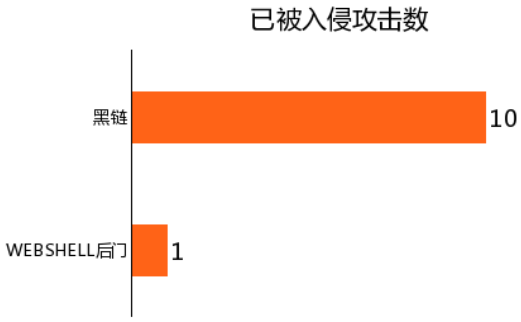
4. 攻击源IP黑名单

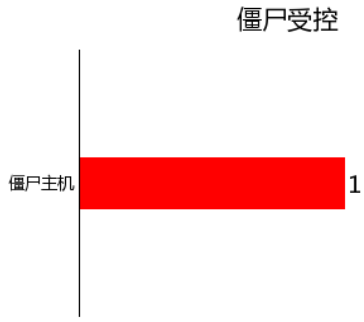
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.3 192.168.88.7风险详情（未处理）

192.168.88.7总体风险评级为：严重（已被入侵）

192.168.88.7服务器已被攻击者控制。共发现攻击12次，探测到漏洞2个
网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门





2.3.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.7已经被挂10个黑链
攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.7已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

事件类型	僵尸受控
事件详情	192.168.88.7已被攻击者远程控制沦为“肉鸡”
攻击举证	2016-06-04 03:09:04 主机100.100.88.176访问了virustotal等机构提供的C&C通信地址:screen.baidu-home.com/screen/checkupdate.txt,可能感染了Virus.Win32病毒 （1次）

2.3.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.3.3 攻击源

以下是攻击192.168.88.7的主要攻击源，遭受攻击共12次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.3.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙WEB应用防护策略，并将“检测攻击后操作>动作”配置为“拒绝”

3. 僵尸受控

- 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除（工具下载地址：http://sec.sangfor.com.cn/apt ）

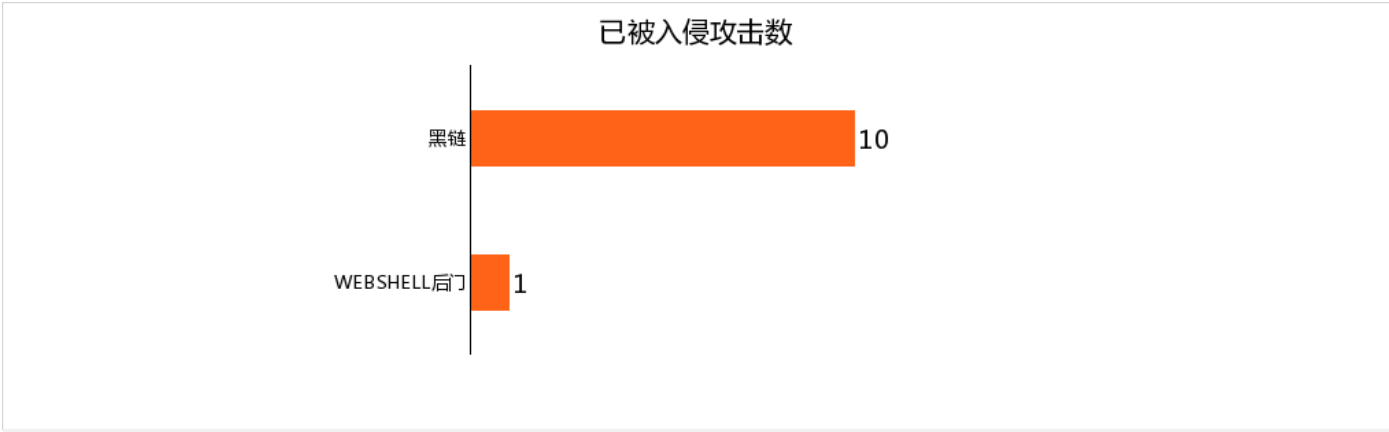
4. 攻击源IP黑名单

- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.4 192.168.88.3风险详情（未处理）

192.168.88.3总体风险评级为：严重（已被入侵）

192.168.88.3服务器已被攻击者控制。共发现攻击11次，探测到漏洞2个
网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门



2.4.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.3已经被挂10个黑链
攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.3已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

2.4.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.4.3 攻击源

以下是攻击192.168.88.3的主要攻击源，遭受攻击共11次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.4.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙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

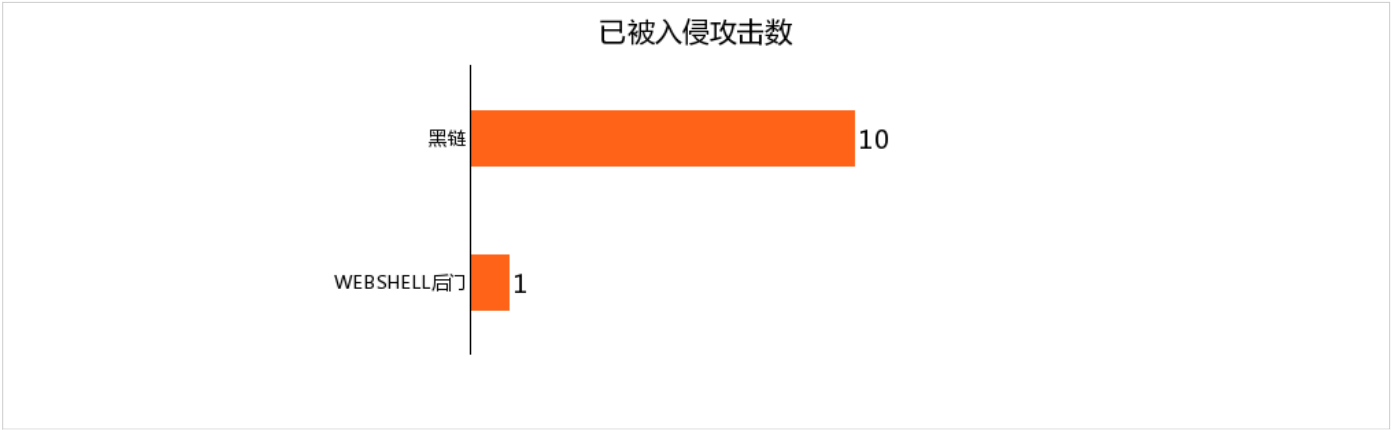
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.5 192.168.88.11风险详情（未处理）

192.168.88.11总体风险评级为：严重（已被入侵）

192.168.88.11服务器已被攻击者控制。共发现攻击11次，探测到漏洞2个

网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门



2.5.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.11已经被挂10个黑链
攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.11已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

2.5.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.5.3 攻击源

以下是攻击192.168.88.11的主要攻击源，遭受攻击共11次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.5.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙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

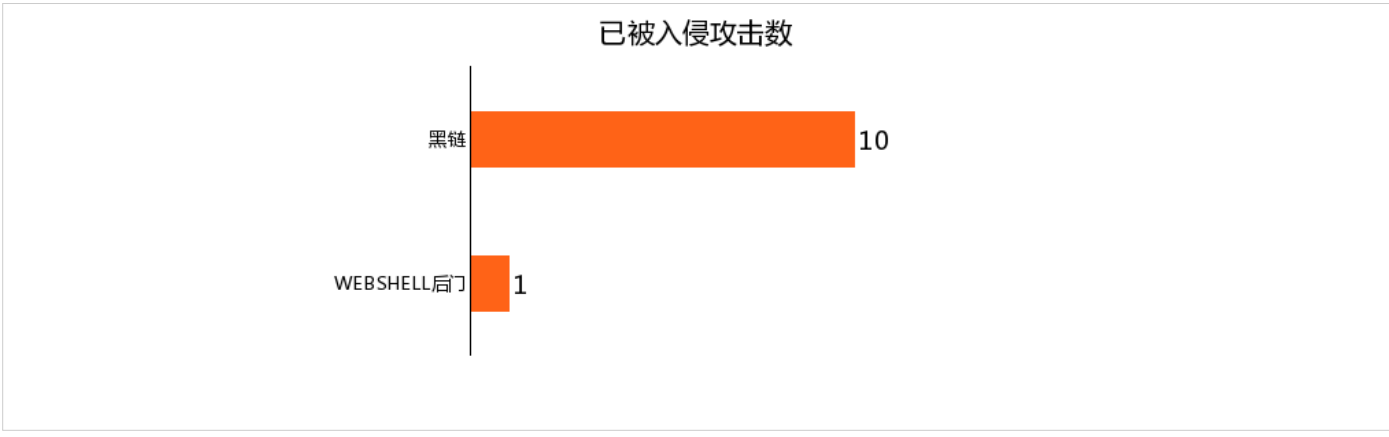
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.6 192.168.88.10风险详情（未处理）

192.168.88.10总体风险评级为：严重（已被入侵）

192.168.88.10服务器已被攻击者控制。共发现攻击11次，探测到漏洞2个

网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门



2.6.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.10已经被挂10个黑链
攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.10已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

2.6.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.6.3 攻击源

以下是攻击192.168.88.10的主要攻击源，遭受攻击共11次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.6.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙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

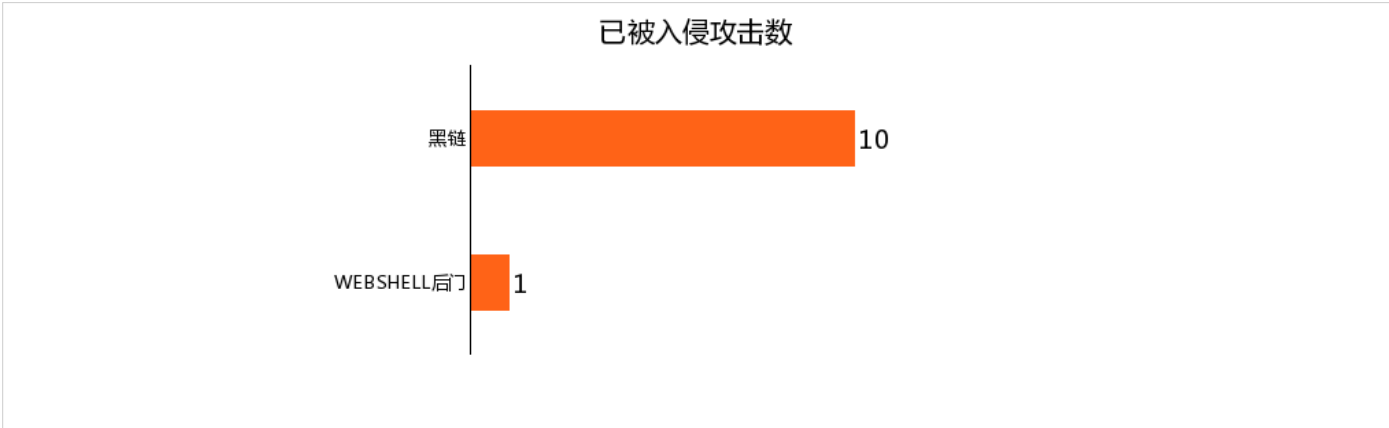
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.7 192.168.88.4风险详情（未处理）

192.168.88.4总体风险评级为：严重（已被入侵）

192.168.88.4服务器已被攻击者控制。共发现攻击11次，探测到漏洞2个

网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门



2.7.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.4已经被挂10个黑链

攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.4已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

2.7.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.7.3 攻击源

以下是攻击192.168.88.4的主要攻击源，遭受攻击共11次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.7.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙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

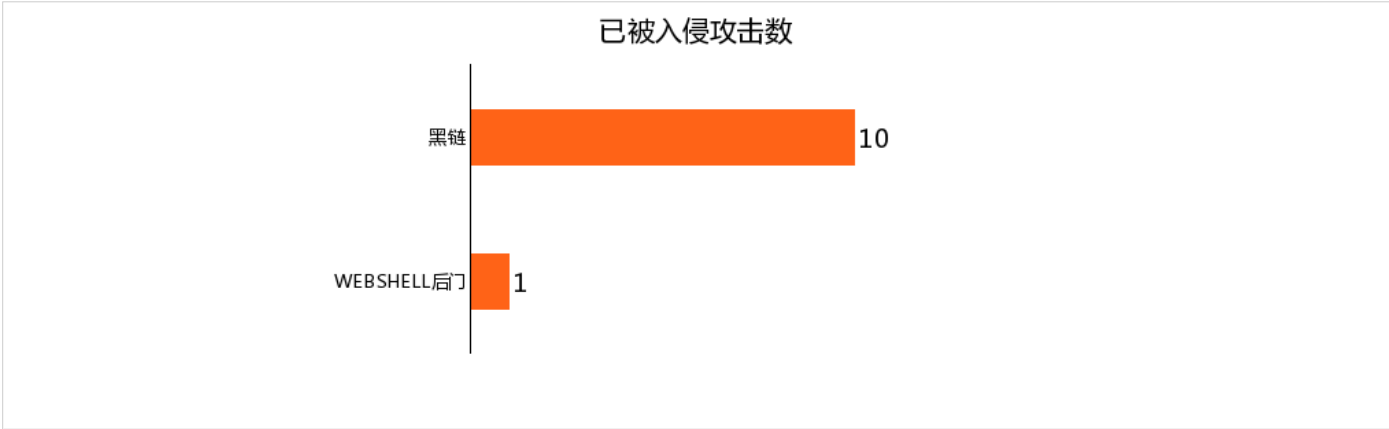
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.8 192.168.88.9风险详情（未处理）

192.168.88.9总体风险评级为：严重（已被入侵）

192.168.88.9服务器已被攻击者控制。共发现攻击11次，探测到漏洞2个

网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门



2.8.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.9已经被挂10个黑链

攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.9已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL)：** 200.200.88.93/b.html

2.8.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.8.3 攻击源

以下是攻击192.168.88.9的主要攻击源，遭受攻击共11次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.8.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙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

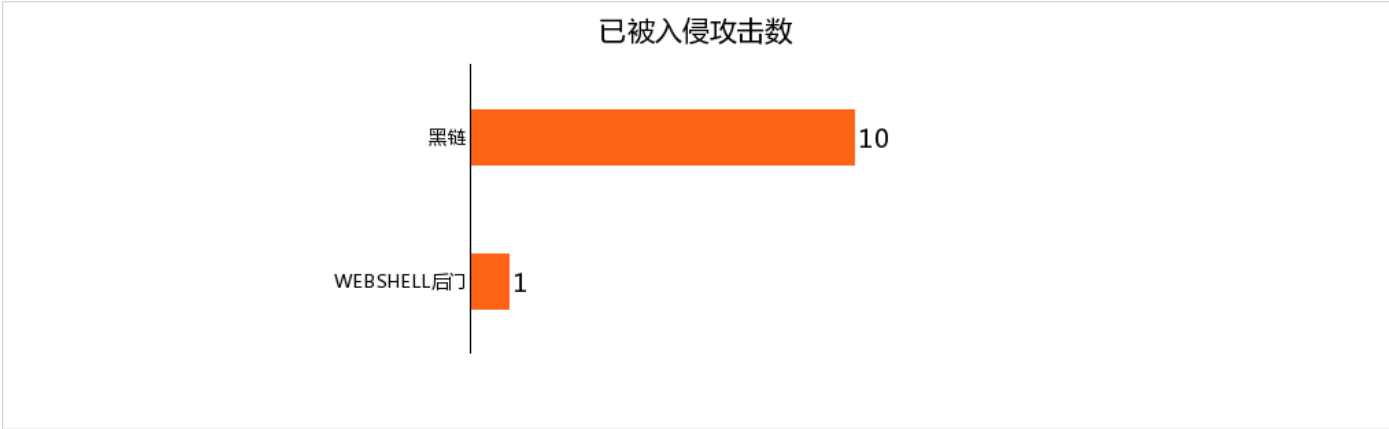
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.9 192.168.88.1风险详情（未处理）

192.168.88.1总体风险评级为：严重（已被入侵）

192.168.88.1服务器已被攻击者控制。共发现攻击11次，探测到漏洞2个

网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门



2.9.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.1已经被挂10个黑链

攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.1已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

2.9.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.9.3 攻击源

以下是攻击192.168.88.1的主要攻击源，遭受攻击共11次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.9.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙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

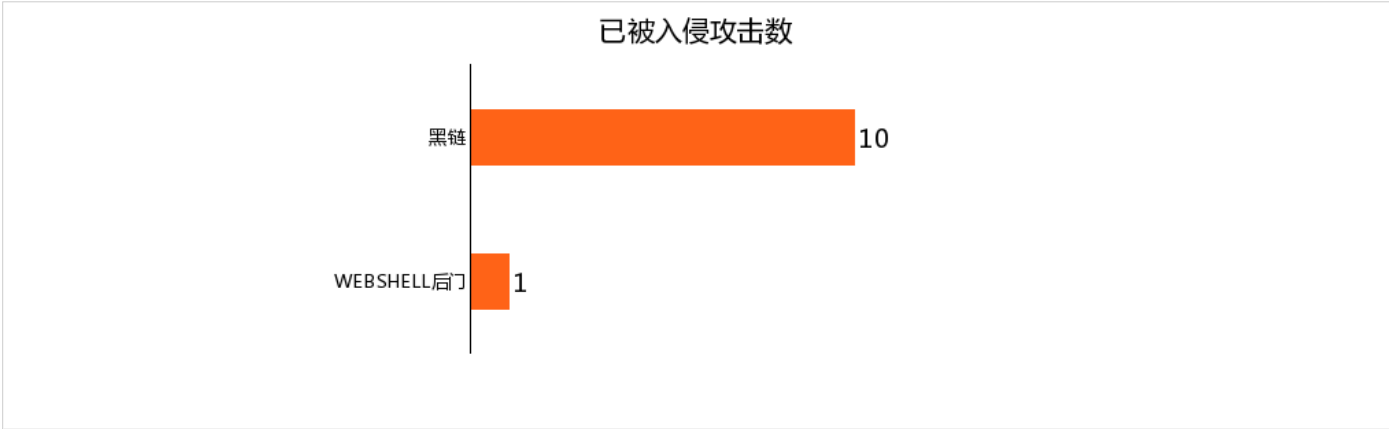
- 建议把以上主要攻击源IP加入黑名单，拦截其攻击

2.10 192.168.88.2风险详情（未处理）

192.168.88.2总体风险评级为：严重（已被入侵）

192.168.88.2服务器已被攻击者控制。共发现攻击11次，探测到漏洞2个

网页被挂10个黑链，涉及色情、成人内容、赌博等链接和内容，系统被挂1个WEBSHELL后门



2.10.1 攻击事件

事件类型	已被入侵（黑链）
事件详情	192.168.88.2已经被挂10个黑链

攻击举证	**该服务器已经被上传以下黑链：** v.baidu.com/kan/dmW9 类型：游戏 内容：小游戏 100.100.88.40/%3Cscript%3Ealert(xxx):%3C/script%3E 类型：反动及其他非法内容 内容：法轮功 100.100.88.40/0618crnr2.html 类型：成人内容 内容：延时药 v.baidu.com/kan/dmmN/d9q8 类型：色情 内容：小游戏 100.100.88.40/0618ffyw4.html 类型：非法药物 内容：海洛因

事件类型	已被入侵（WEBSHELL后门）
事件详情	192.168.88.2已经被挂WEBSHELL后门
攻击举证	**该服务器已经被上传以下网站后门（WEBSHELL）：** 200.200.88.93/b.html

2.10.2 漏洞

序号	漏洞名称	漏洞总数	是否被攻击	防护状态	风险等级
1	IIS漏洞	2	否	已防护	高

说明：

- 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。

2.10.3 攻击源

以下是攻击192.168.88.2的主要攻击源，遭受攻击共11次。建议配置黑名单拒绝其访问攻击

序号	攻击来源	攻击类型	IP归属地	攻击次数	拦截次数	拦截率
1	188.188.208.108	WEBSHELL后门(1)	比利时	1	1	100%

2.10.4 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. 黑链攻击

- 查看以上被植入黑链的页面源代码，清除所有被篡改的内容，更多黑链请查看下一代防火墙>首页>待办事项
- 下载主机安全检测工具，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 ）

2. WEBSHELL攻击

- 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 ）
- 开启应用层防火墙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

三、用户风险详情分析

3.1 192.168.88.22风险详情（未处理）

总体综合风险级别评级为：严重（已被感染）

192.168.88.22共遭受威胁2次，目前处于C&C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

3.1.1 威胁详情

事件类型	C&C通信
事件详情	主机存在使用HFS协议进行通信的行为，主机被黑后有时会被黑客上传HFS软件用于远程控制
攻击举证	2016-06-04 03:09:05 主机11.11.88.214访问了HFS服务器，可能已被黑客攻破 （2次）

3.1.2 安全加固

- 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除（工具下载地址：http://sec.sangfor.com.cn/apt）

3.2 192.168.88.19风险详情（未处理）

总体综合风险级别评级为：严重（已被感染）

192.168.88.19共遭受威胁1次，目前处于C&C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

3.2.1 威胁详情

事件类型	C&C通信
事件详情	主机有浏览动态域名的行为
攻击举证	2016-06-04 03:09:05 经深信服威胁引擎检测，主机访问的经深信服威胁引擎检测，主机访问的check-ip.dyndns.org为恶意动态域名，可能是恶意软件通信的C&C服务器地址为恶意动态域名，可能是恶意-软件通信的C&C服务器地址 （1次）

3.2.2 安全加固

- 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除（工具下载地址：http://sec.sangfor.com.cn/apt）

3.3 192.168.88.35风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.35共遭受威胁4次，目前处于数据/资产发现阶段，该阶段表示受感染主机扫描到内网服务器，并尝试对服务器进行暴力破解、SQL注入等攻击

3.3.1 威胁详情

事件类型	数据/资产发现
事件详情	受感染主机扫描到内网服务器，并尝试对服务器进行SQL注入攻击
攻击举证	2016-06-04 03:09:06 检测到网站攻击！攻击类型：SQL 注入 （4次）

3.3.2 安全加固

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

3.4 192.168.88.36风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.36共遭受威胁3次，目前处于数据泄漏阶段，该阶段表示已有证据证明受感染主机已拿到服务器上敏感信息，并正在或即将进行数据泄密

3.4.1 威胁详情

事件类型	数据泄漏
事件详情	主机已拿到服务器上的敏感信息，并正在或即将进行数据泄密

攻击举证	2016-06-04 03:09:06 匹配到的敏感信息组合策略为: rrr\\ 内容为: mpserver.com/en/donations.php">Donate -
\\ \\\\ Alter Way
\\ \\&l... （1次） 2016-06-04 03:09:06 匹配到的敏感信息组合策略为: rrr\\ 内容为: able Web Application (DVWA) is a RandomStorm OpenSource project</p>
\\ \\18824649828
\\ \\13225456786
\\ \\303822@qq.com
\\ \\</div> <!-- end align div -->&... （1次） 2016-06-04 03:09:06 匹配到的敏感信息组合策略为: rrr\\ 内容为: ges/RandomStorm.png" /> -->
\\ \\
\\ \\ Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
\\ \\18824649828
\\ \\13225456786&a... （1次）

3.4.2 安全加固

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

3.5 192.168.88.30风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.30共遭受威胁1次，目前处于数据/资产发现阶段，该阶段表示受感染主机扫描到内网服务器，并尝试对服务器进行暴力破解、SQL注入等攻击

3.5.1 威胁详情

事件类型	数据/资产发现
事件详情	受感染主机扫描到内网服务器，并尝试对服务器进行暴力破解攻击
攻击举证	2016-06-04 03:09:06 发现某个用户频繁登录FTP服务器失败信息，可能存在暴力破解攻击。 （1次）

3.5.2 安全加固

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

3.6 192.168.88.29风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.29共遭受威胁11次，目前处于横向移动阶段，该阶段表示受感染主机扫描同网内其他在线主机及服务，通过漏洞攻击等方式将恶意软件传播给它们

3.6.1 威胁详情

事件类型	横向移动
事件详情	主机存在利用漏洞攻击其他主机的行为
攻击举证	2016-06-04 03:09:05 GUN Glibc 存在一个基于堆的缓冲区溢出漏洞，在__nss_hostname_digits_dots函数中允许攻击者利用gethostbyname或gethostbyname2函数存在的漏洞执行任意代码，Exim Mail服务器通过HELO或EHLO命名远程利用此漏洞。 （3次） 2016-06-04 03:09:05 Microsoft Windows是微软发布的常流行的操作系统。Windows的Workstation服务组件中存在栈溢出漏洞，远程攻击者可能利用此漏洞在服务器上执行任意指令。在Workstation服务名为wkssvc.dll的模块中，NetpManageIPCConnect函数以未经检查的缓冲区数据调用了swprintf，而输入缓冲区是远程攻击者可控的。 （1次） 2016-06-04 03:09:05 微软的Windows存在一个远程代码执行漏洞，将影响到Windows Server上的RPC(远程过程调用)服务。针对这个漏洞存在许多自动化攻击工具。攻击者可以利用这个漏洞以SYSTEM-level权限执行任意代码，成功的攻击者将完全控制受害主机。 （2次） 2016-06-04 03:09:05 （2次） 2016-06-04 03:09:05 Struts2是基于Java EE Web应用的Model-View-Controller设计模式的应用框架。Apache Struts 2.3.16.1 之前的版本的参数过滤器允许远程攻击者通过传递给getClass方法的class参数操纵ClassLoader，从而可以执行任意代码。 （3次）

3.6.2 安全加固

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

3.7 192.168.88.15风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.15共遭受威胁1次，目前处于C&C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

3.7.1 威胁详情

事件类型	C&C通信
事件详情	主机存在已知恶意软件关联的通信特征
攻击举证	2016-06-04 03:09:05 PcShare是一款强大的远程控制软件，采用HTTP反向通信，屏幕数据线传输，-驱动隐藏端口通信过程等技术，达到了系统级别的隐藏。 （1次）

3.7.2 安全加固

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

3.8 192.168.88.14风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.14共遭受威胁1次，目前处于C&C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

3.8.1 威胁详情

事件类型	C&C通信
事件详情	主机存在已知恶意软件关联的通信特征
攻击举证	2016-06-04 03:09:05 WanRemote 3.0是一个后门程序。攻击者通过垃圾邮件、网页木马等方式向受-害者主机植入后门程序，进而利用这个后门程序绕过计算机的安全控制机制，非法访问受害者主机。该-事件表明WanRemote 3.0正在与攻击者进行通信。 （1次）

3.8.2 安全加固

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

3.9 192.168.88.16风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.16共遭受威胁1次，目前处于C&C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

3.9.1 威胁详情

事件类型	C&C通信
事件详情	主机存在已知恶意软件关联的通信特征
攻击举证	2016-06-04 03:09:05 恶意广告软件是指未经用户允许，下载并安装或与其他软件捆绑通过弹出式广-告或以其他形式进行商业广告宣传的软件，甚至有些会集成间谍软件 ，如键盘记录软件和隐私入侵软-件等。该事件表明检测到广告软件NewDotNet正在运行。 （1次）

3.9.2 安全加固

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

3.10 192.168.88.13风险详情（未处理）

总体综合风险级别评级为：高危（感染可能性：高）

192.168.88.13共遭受威胁8次，目前处于C&C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

3.10.1 威胁详情

事件类型	C&C通信
事件详情	主机具有疑似进行反弹连接的行为
攻击举证	2016-06-04 03:09:05 SSH协议利用22端口进行反弹连接。 （8次）

3.10.2 安全加固

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

四、风险评估说明&危害说明

4.1 风险评估说明

业务风险是通过对防护区域内服务器的所有入侵风险日志进行综合关联分析得到的，其中严重等级共分为已被入侵、曾被攻击、曾被收集信息、存在漏洞；用户风险是通过对防护区域内主机的所有僵尸网络相关风险日志进行综合关联分析得到的，其中威胁等级共分为已被感染、感染可能性高、感染可能性中、感染可能性低；综合风险等级是通过综合分析业务安全风险和用户安全风险得到；具体评级规则如下：

当整体网络状况评级为**差**：

- 业务系统至少一个服务器严重等级评级为**严重**(已被入侵)；或者僵尸主机至少一个主机严重威胁为**严重**(已被感染)

当整体网络状况评级为**中**：

- 业务系统至少一个服务器严重等级评级为**高危**(曾被攻击)；或者僵尸主机至少一个主机严重威胁**高危**(感染可能性：高)
- 业务系统至少一个服务器严重等级评级为**中危**(曾被收集信息)；或者僵尸主机至少一个主机严重威胁**中危**(感染可能性：中)

当整体网络状况评级为**良**：

- 业务系统至少一个服务器严重等级评级为**低危**(存在漏洞)；或者僵尸主机至少一个主机严重威胁**低危**(感染可能性：低)

当整体网络状况评级为**优**：

- 业务系统不存在漏洞且未遭受攻击；或者主机不存在任何风险

4.2 危害说明

4.2.1 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://sec.sangfor.com.cn/attacks/4.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
- 下载主机安全检测工具，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 ）

4.2.2 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://sec.sangfor.com.cn/attacks/2.html

解决方案：

- 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）
- 开启应用层防火墙WEB应用防护策略，并将“检测攻击后操作>动作”配置为“拒绝”

4.2.3 僵尸受控

僵尸主机是指用户网络中因感染了蠕虫、木马等病毒而被攻击者控制的主机。攻击者可通过控制僵尸主机进行DoS攻击、APT攻击等各种类型的攻击，以达到致使用户网络或重要应用系统瘫痪、窃取用户机密业务数据等目的

攻击演示：http://sec.sangfor.com.cn/attacks/8.html

解决方案：

- 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除（工具下载地址：http://sec.sangfor.com.cn/apt）

4.2.4 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
- 系统命令注入：攻击者利用此漏洞执行系统命令，获取系统的运行信息，新增系统用户，开启远程连接并控制WEB系统所在主机

攻击演示：http://sec.sangfor.com.cn/attacks/1.html

解决方案：

- 开启应用层防火墙WEB应用防护策略，并将“检测攻击后操作>动作”配置为“拒绝
- 开启应用层防火墙IPS策略，并将“检测攻击后操作>动作”配置为“拒绝”

4.2.5 服务器风险说明

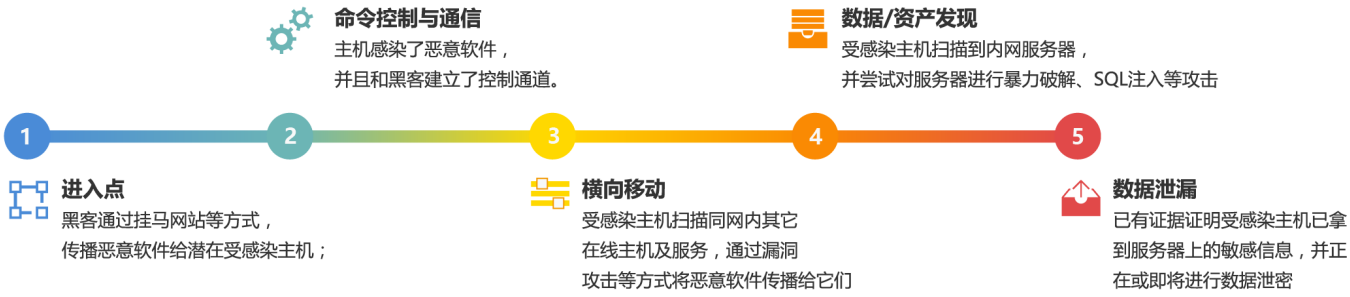
- 攻击阶段示意图

- 危险等级说明

序号	服务器严重性	严重性说明	等级值
1	已被入侵	已有数据证明服务器已被黑，如被挂WEBSHELL、黑链等	5
2	曾被攻击	无数据证明服务器被黑，但存在被攻击的证据：包括SQL注入、暴力破解、WEBSHELL-上传等攻击类型的日志	3-4
3	曾被收集信息	无数据证明服务器被黑，但存在被收集信息的证据	2
4	存在漏洞	无数据证明服务器被黑，无攻击记录，但服务器本事存在漏洞	1

4.2.6 僵尸主机威胁说明

- 攻击阶段示意图



- 危险等级说明

序号	主机严重性	等级	定义
1	**已被感染** 主机展现出了感染恶-意软件的明确行为	10	具有与已知恶意软件关联的URL、域名、IP地址等进行通信，同时存在数据泄漏或已危害数据库的主机
		9	具有与已知恶意软件关联的URL、域名、IP地址等进行通信，并且主机正在尝试向其他主机传播恶意文件
		8	具有与已知恶意软件关联的URL、域名、IP地址等进行通信的主机
2	**感染可能性：高** 主机展现出了感染恶-意软件的高可能性行为	7	具有对外发起DDOS攻击行为的主机，或者具有访问疑似飞客蠕虫类域名行为的主机
		6	被检测出存在已知恶意软件关联的通信数据包特征的主机，或者被检测出存在传播恶意s-hellcode行为的主机
		5	具有访问疑似DGA自动生成域名行为的主机，或者具有疑似进行反弹连接行为的主机
3	**感染可能性：中** 主机受到已知恶意软-件入侵，但尚未展示-出被感染的行为	4	具有下载恶意可执行文件、恶意PDF或挂马网页等行为的主机，但是无用户感染的迹象
		3	具有下载疑似恶意文件行为的主机，如文件后缀和文件名不符，但是无用户感染的迹象
4	**感染可能性：低** 主机展现出了感染恶-意软件的低可能性行为	2	主机正在使用可能被恶意软件用作通信协议的已知或未知协议，如IRC协议、HFS协议等-，主机访问疑似恶意软件通信使用的域名、IP
		1	检测出了中低威胁异常流量的主机，或者具有访问钓鱼、盗号等恶意网站或邮件行为的-主机，如SSL协议跑在非标准的443端口