**前言**

* **涉及范围**

本文主要针对360虚拟化安全管理系统轻代理产品P004U2B17H07版本的技术问题进行解答；仅为内部人员学习、参考使用，文档内涉及产品设计理念以及实现原理，**请同学们切勿对外传播推广**；

* **期望读者**

期望通过FAQ能快速排查,解决P004U2B17H07版本的问题,提高认知和解决问题的能力；

* **注意事项**

如FAQ无法满足您的需要,或您有任何意见,可直接联系虚拟化安全相关负责人；

目录

[一、 病毒查杀 3](#_Toc47964956)

[1.1 与扫描相关 3](#_Toc47964957)

[1.2 与隔离区相关 4](#_Toc47964958)

[1.3 与流行木马库相关 5](#_Toc47964959)

[二、 Webshell扫描 5](#_Toc47964960)

[2.1 与隔离区相关 5](#_Toc47964961)

[2.2 与webshell自定义扫描相关 5](#_Toc47964962)

[三、 安全基线 5](#_Toc47964963)

[四、 防暴力破解 5](#_Toc47964964)

[4.1 防爆力破解 5](#_Toc47964965)

[五、 虚拟化加固 6](#_Toc47964966)

[5.1 虚拟化加固黑名单 6](#_Toc47964967)

[六、 网卡流量统计 7](#_Toc47964968)

[七、 升级管理 7](#_Toc47964969)

[八、 资产管理 8](#_Toc47964970)

[九、 防火墙 9](#_Toc47964971)

[十、 入侵防御 10](#_Toc47964972)

[10.1 规则攻击汇总 10](#_Toc47964973)

[10.2 IPS日志 13](#_Toc47964974)

[十一、 日志与报表 14](#_Toc47964975)

[11.1 主机日志 14](#_Toc47964976)

[十二、 主机策略 14](#_Toc47964977)

[12.1 分组策略 14](#_Toc47964978)

[12.2 黑白名单 15](#_Toc47964979)

[十三、 系统配置 16](#_Toc47964980)

[13.1 系统设置 16](#_Toc47964981)

[13.2 系统工具 20](#_Toc47964982)

[十四、 其它 20](#_Toc47964983)

# 病毒查杀

## 1.1 与扫描相关

* **病毒查杀的扫描日志存放位置**

Windows：C:\Program Files (x86)\360\360Safe\deepscan\Log\VirusScanLog

Linux: /opt/360safe/log/ScanLog

* **压缩包大小和层数限制与扫描方式关系**

win和linux一致：快速扫描、全盘扫描、自定义路径扫描均受压缩包层数限制；

快速扫描、全盘扫描均受压缩包大小限制，自定义路径扫描不受压缩包大小限制；

* **快速扫描都扫描哪些路径**
* windows快扫项目跟路径相关的如下：

1、文件和系统内存，如一个黑文件起了一个黑进程，快扫是能够报出的，处理方式是结束进程，隔离文件、修改注册表等；

2、启动项：注册表中RUN键下指向的路径；这里可能会牵扯到Program Files里的文件，不会遍历子目录；

3、易感染区 ：具体目录视环境而定，这里会扫描到所有用户的桌面目录，不会遍历子目录

4、环境变量PATH中的所有目录；

环境变量中的PATH 目录扫描需要满足条件：

1. 非x64系统，也就是在X86上才会有效果;
2. Path路径中指向的目录下，存在跟c:\windows\system32下相同名称的文件才会被扫描；

5、所有用户目录

6、系统关键路径：windows如下，会遍历子目录：

1. "C:\Windows" 以及windows下的所有子目录；
2. 桌面以及桌面上的所有子目录；
* linux系统快速扫描下相关路径：

/home,

/root,

/etc/rc.d,

/usr/local/bin,

/usr/sbin,

/usr/bin,

/sbin,

/bin

## 1.2 与隔离区相关

* **Windows病毒查杀隔离区位置以及大小限制**

Windows隔离区目录是：C:\$360Section；

隔离区大小就是磁盘剩余空间的大小，没有保护机制；

* **Linux病毒查杀隔离区位置以及大小限制**

Linux隔离区目录是：/opt/360safe/backup；

隔离区大小：以系统磁盘剩余空间乘以10%作为参考数据，若参考数据<500M，则设定隔离区大小为500M，若参考数据>2G，则设定隔离区大小为2G，若500M<参考数据<2G，则直接设定隔离区大小为参考数据；当待隔离文件超出隔离区剩余空间时，隔离失败；

* **病毒隔离区空间大小限制**

病毒隔离区的所在磁盘的剩余空间大小必须不能小于20%，否则当前设置的隔离区就会失效，当进行病毒扫描的时候，程序会选择上一个有效的隔离区进行病毒隔离，如果不存在有效的隔离区，则隔离失败；

若磁盘剩余空间小于20%，手动清理磁盘空间，使剩余空间大于20%，需重新下发该策略，或等待1小时后，当前设置的隔离区方可生效。

## 1.3 与流行木马库相关

流行木马库功能上无需特殊配置，只需要云查询模式选择“通过控制中心代理连接到云安全鉴定中心”即可开启；流行木马库在功能使用上无感知，也没有其余配置项；

# Webshell扫描

## 2.1 与隔离区相关

* **隔离区位置**

Windows：C:\Program Files (x86)\360\360Safe\webshell\Quarantine

Linux： /opt/360safe/ThirdPath/webshell/Quarantine

## 2.2 与webshell自定义扫描相关

B17H01版本新增webshell自定义扫描功能，windows客户端升级主程序和webshell引擎后，webshell自定义扫描功能不生效；因为不同的库间依赖关系导致，请对不生效的客户端再次下发升级主程序任务，待任务结束1分钟后，重新下发webshell自定义扫描任务即可；

# 安全基线

暂无

# 防暴力破解

## 4.1 防爆力破解

* **Linux防暴力破解不生效**

打开主机的ssh配置文件，检查UsePAM yes是否被注释，若被注释，则去掉该注释重启ssh服务后再进行测试。或检查 /etc/pam.d/sshd 是否为空，若为空，则功能不生效；

* **部分Windows没有远程连接选项**

打开该链接<https://github.com/stascorp/rdpwrap>，下载软件，安装成功后，即可开启远程链接；

安装过程需关闭360软件；

* **防暴力破解功能不生效**

请检查是否设置了入侵防御白名单，该项功能会影响防暴力破解功能不生效，请谨慎设置。

# 虚拟化加固

## 5.1 虚拟化加固黑名单

* **虚拟化加固黑名单一次性添加多个文件是否有限制**

文件上传大小限制与浏览器及操作系统都有关系，不同的操作系统不同的浏览器下大小限制不一样，多个文件上传时chrome下所有文件名称总和不超过256个字符，转化后大小为不超过32k 火狐中这个数值会大点，取决于浏览器自身特性。

* **终端虚拟化加固日志存放路径**
* Windows虚拟化加固日志存放位置及文件格式为：

C:\ProgramData\360Skylar6\EntCloudfasten.ext.log；

* Linux虚拟化加固日志存放位置及文件格式：

/opt/360safe/log/libEntCloudFastenPlugin.so.log；

# 网卡流量统计

暂无

# 升级管理

* **如何在客户端查看主程序、病毒库、webshell引擎、入侵防御规则库、漏洞库的版本号**

Linux查看位置：/opt/360safe/modularize 中，通过more module\_config.ini 进行查看；

Windows查看位置：C:\Program Files (x86)\360\360Safe\EntClient\Modularize中，查看module\_config.ini ；

* **Windows客户端主程序升级的时候，为什么会出现短暂断网**

Windows客户端主程序升级的同时会对网卡驱动进行升级，会出现安装新驱动，卸载旧驱动的动作，在安装和卸载的时候，会出现短暂断网，这是正常现象，30秒左右即可恢复正常。

* **为什么控制台升级后入侵防御规则库版本显示为空**



控制台升级完成后，客户端仍然是旧版本，而旧版的客户端并没有入侵防御规则库版本，所以版本一列显示为空。

在升级管理界面，升级客户端主程序，完成版本升级，即可显示入侵防御规则库版本的显示。

* **病毒库和主程序的升级次序**

控制台覆盖升级前，需先将病毒库升级到最新版本，然后再进行控制台覆盖升级；

控制台覆盖升级后，若病毒库需要升级，此时，应先将客户端主程序升级到最新版本；

* **Windows客户端webshell自定义扫描功能不生效**

Windows客户端已经升级过主程序和webshell引擎库，但webshell自定义功能依然没有生效（设置的自定义目录下的后门文件未被检出）；

因为不同的库间依赖关系导致，请对不生效的客户端再次下发升级主程序任务，待任务结束1分钟后，重新下发webshell自定义扫描任务即可；

# 资产管理

* **为什么主机发现功能，Windows操作系统显示未知**



Windows在关闭“启动文件和打印机共享”功能的情况下，nmap无法识别出操作系统；控制台在执行主机发现和远程安装功能，Windows需要先打开“启动文件和打印机共享”。



# 防火墙

* **为何linux操作系统配置icmp允许策略，一直ping时只产生一条日志**

Linux开启状态防火墙后，iptables会对已经建立连接的请求直接放行，所以建立连接以后就没有日志了，这个是防火墙的正常行为；

PS：TCP长连接也会有此现象；

* **在保障防火墙功能的前提下，如何关闭日志上报功能**

修改对应的防火墙规则的日志开关状态即可。



# 入侵防御

## 10.1 规则攻击汇总

* **Linux IPS攻击规则和方法汇总**

|  |  |  |
| --- | --- | --- |
| 分类 | Rule | 方法 |
| WEB攻击 | rule\_id: 301005name: DELETED WEB-ATTACKS /bin/ps command attempt  | 攻击方法:1、安装apacheYum –y install httpd2、开启httpdService httpd start3、确保HTTP：80端口开放/sbin/iptables -I INPUT -p tcp --dport 80 -j ACCEPT /etc/rc.d/init.d/iptables save /etc/init.d/iptables restart4、在攻击机浏览器中访问http://<配置策略的主机> /bin/ps |
| 其他攻击 | rule\_id: 301001name: PROTOCOL-FTP ADMw0rm ftp login attempt  | 攻击方法：1、在靶机上安装vsftpYum –y install vsftpd2、开启vsftpService vsftpd start3、确保FTP：21端口可达/sbin/iptables -I INPUT -p tcp --dport 21 -j ACCEPT /etc/rc.d/init.d/iptables save /etc/init.d/iptables restart4、打开winSCP新建FTP连接，用户名w0rm，密码随便，链接登录，观察是否触发日志 |
| 获取权限 | rule\_id: 308463、303469name:  MALWARE-BACKDOOR w00w00 attempt  | 攻击方法：1、安装telnet服务Yum –y install telnet-serverYum –y install telnet2、修改配置文件vi /etc/xinetd.d/telnet将disable=yes改为disable=no3、重启telnetService xinetd restart4、添加端口23vi /etc/sysconfig/iptables增加：-A INPUT -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT重启iptablesService iptables restart5、检查是否在监听netstat -tnl | grep 23tcp    0   0 :::23    :::\*    LISTEN6、远程用w00w00用户登录，密码随意，观察是否触发日志 |
| 木马后门 | rule\_id:301169name: BLACKLIST URI request for known malicious URI - greenherbalteagirlholdingcup  | 攻击方法：1、  准备另外一台win机器，安装HFS2、  新建文件，命名：“sgreenherbalteagirlholdingcup1.gif”并放入HFS下载目录里3、  在测试机上访问：Curl [http://win](http://win/)机器ip:8080 /sgreenherbalteagirlholdingcup1.gif观察是否触发日志； |
| 网络扫描 | rule\_id: 308250name: INDICATOR-SCAN [Proxyfire.net](http://proxyfire.net/) anonymous proxy scan  | 攻击方法：1、配置策略的主机搭建web服务远端用浏览器访问2、curl http://< 配置策略的主机> /[proxyfire.net/fastenv](http://proxyfire.net/fastenv) |
| 拒绝服务 | rule\_id: 310536name: SERVER-OTHER Apache ActiveMQ shutdown command denial of service attempt  | 攻击方法：Curl <http://192.168.126.193/shutdown> |
| 缓冲区溢出 | rule\_id: NULLname: INDICATOR-SHELLCODE x86 OS agnostic unicode mixed encoder  | 改规则P005版本已删除 操作同上<http://192.168.126.193/YAZBABABABABkMAGB9u4JB> |

* **Windows IPS攻击规则和攻击方法汇总**
* 规则1：rule\_id = 121570

Drop tcp $EXTERNAL\_NET any -> $HOME\_NET 3389 (msg:"OS-WINDOWS Microsoft Windows RemoteDesktop new session flood attempt"; flow:to\_server,established; content:"|02 F0 80 7F 65|"; fast\_pattern; content:"|03 00|"; within:2; distance:-9; content:"|000000|"; within:17; distance:9; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop; reference:cve,2012-0002; reference:url,technet.microsoft.com/en-us/security/bulletin/ms12-020; classtype:attempted-admin; sid:121570; rev:8;)

攻击方法：python ms12-20.py 靶机IP

* 规则2：rule\_id = 126944
alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"MALWARE-CNC Win.Trojan.Post\_Show RAT beacon"; flow:to\_server,established; content:"GET"; depth:3; nocase; http\_method; content:"/post\_show.asp?"; fast\_pattern:only; http\_uri; content:"123456789"; http\_uri; metadata:impact\_flag red, policy balanced-ips drop, policy security-ips drop, service http; classtype:trojan-activity; sid:26944; rev:3;)
攻击方法：
    1) HTTP  GET 请求， 不区分大小写。
    2) 请求的RUI 中同时包含 "/post\_show.asp?"  和  "123456789".
* 规则3：rule\_id = 126943
alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"MALWARE-CNC Win.Trojan.Post\_Show RAT beacon"; flow:to\_server,established; content:"GET"; depth:3; nocase; http\_method; content:"/jp/admin.asp"; fast\_pattern:only; http\_uri; metadata:impact\_flag red, policy balanced-ips drop, policy security-ips drop, service http; classtype:trojan-activity; sid:26943; rev:3;)
攻击方法：
    1) HTTP  GET 请求， 不区分大小写。
    2) 请求的RUI 中包含 "/jp/admin.asp"。
* 规则4：rule\_id = 126942

alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"MALWARE-CNC Win.Trojan.PipCreat RAT beacon"; flow:to\_server,established; content:"GET"; depth:3; nocase; http\_method; content:"/adminweb/news.asp?id="; fast\_pattern:only; http\_uri; metadata:impact\_flag red, policy balanced-ips drop, policy security-ips drop, service http; reference:url,[www.cyberengineeringservices.com/login-exe-analysis-trojan-pipcreat/](http://www.cyberengineeringservices.com/login-exe-analysis-trojan-pipcreat/); classtype:trojan-activity; sid:26942; rev:3;)
攻击方法：
    1) HTTP  GET 请求， 不区分大小写。
    2) 请求的RUI 中包含  "/adminweb/news.asp?id="  。

## 10.2 IPS日志

* **终端IPS防护日志存放路径**

Windows入侵防御日志存放位置及文件格式：C:\ProgramData\360Skylar6\EntIPS.ext.log；

Linux入侵防御日志存放位置及文件格式：/opt/360safe/ThirdPath/ips/log/alert；

# 日志与报表

## 11.1 主机日志

* **主机日志中涉及离线统计的图表有那些**
1. ips日志-按主机统计-**每小时整点统计前1小时内攻击数据**，统计后更新图表；
2. ips日志-按规则统计-**每小时整点统计前1小时内攻击数据**，统计后更新图表；
3. ips日志-每日拦截次数趋势图-**每天凌晨00:05统计前1天内攻击数据**，统计后更新图表；
4. webshell日志-按主机统计-**每小时整点过5分统计前1小时内威胁数据**，统计后更新图表；
5. webshell日志-每日查杀后门数趋势图-**每天凌晨02:05统计前1天内威胁数据**，统计后更新图表，00:00~02:05之间数据存在异常；
6. firewall日志-按主机统计-**每小时整点过5分统计一次数据**，统计后更新图表，**但数据存在1小时延迟**（ 如05:05时开始统计3点~4点之间的攻击数据）；
7. firewall日志-按规则统计--**每小时整点过5分统计一次数据**，统计后更新图表，**但数据存在1小时延迟**（ 如05:05时开始统计3点~4点之间的攻击数据）；
8. firewall日志-每日拦截次数趋势图--**每天凌晨02:05统计前1天的攻击数据**，统计后更新图表，00:00~02:05之间数据存在异常；

# 主机策略

## 12.1 分组策略

* **分组策略下发后如何在客户端查看**
* win：

日志排查：debugview  get\_conf接口
本地策略文件：C:\ProgramData\360Skylar6\EntClientSvc.log

* linux：

日志排查： /opt/360safe/log/policycom.log
本地策略文件：/opt/360safe/Data /policydata.dat

## 12.2 黑白名单

* **Windows黑白名单不生效**

场景：覆盖升级---用户B09H07环境先升级病毒库（win客户端病毒库为1月16号），然后再覆盖升级B13，升级成功后，再升级win主程序，这种升级顺序会导致病毒黑白名单不生效；

原因分析：这种场景加载的还是以前的dll文件，导致bwver.dat和bwinfo.dat两个文件未生成，黑白名单不生效；

规避方法：重启客户端进程，加载新的dll文件；

备注：此问题属于偶发问题；若先B09H07覆盖升级B13——再升级win主程序——最后升级win病毒库，此时黑白名单是生效的；

* **Linux黑白名单不生效**

场景：中控先存在病毒黑白名单，此时卸载安装Linux客户端，或者重新安装新的Linux客户端，会导致Linux黑白名单不生效；

原因分析：新安装程序初始化时（杀毒模块未加载），心跳已经将版本号写入心跳数据库中，但此时杀毒模块没有起来，不会进行下载黑白名单操作，等杀毒模块加载成功后，心跳中版本号bw\_ver未更新，和心跳数据库中的版本号一样，因此不会再次触发下载操作，这样中控先存的黑白名单就无法下发到Linux客户端；

规避方法：更新中控病毒黑白名单（删除或者新增黑白名单）；

# 系统配置

## 13.1 系统设置

* **日志清除的处理逻辑**
1. 日志清理，比如保留1天，是保留的1月7日00:00:00以后的数据，清理的1月6日23:59:59之前的数据（也就是不算清理当天，往前保留1天（24小时））。
2. 保留1个月的逻辑是1个月\*30天=30天（不算当天，往前保留30天）。
3. 保留12个月的逻辑是12个月\*30天=360天（不算当天，往前保留360天）。
4. 定时清理和立即清理都是上边的逻辑，定时清理是凌晨4点开始。
* **中控日志清理日志位置**

定时/立即日志清理的日志的保存在下面文件中:

/opt/qihu360/hsmp/logs/php\_console\_logclear\_commands.log

* **访问控制失误添加授信IP**

授信IP添加错误,导致所在IP无法登录中控,出现如下如所示的情况;



有两种解决办法:

1. 通过修改redis来解除限制

[root@localhost ~]# redis-cli

127.0.0.1:6379> keys \*



127.0.0.1:6379> get "server\_access\_limit\_config"

"{\"type\":\"0\",\"ips\":{\"single\":[\"1.1.1.1\"],\"rangBe\_normal\":[],\"range\_cidr\":[]}}"

127.0.0.1:6379>

127.0.0.1:6379> set "server\_access\_limit\_config" "{\"type\":\"1\",\"ips\":{\"single\":[\"1.1.1.1\"],\"rangBe\_normal\":[],\"range\_cidr\":[]}}"

OK

127.0.0.1:6379>

修改type为1即可



1. 清除psql中的记录,此方法较为暴力,会清除中控所有设置,慎用

登录数据库 psql –U hsmp

然后输入密码：hsmp!@#cl0ud



select \* from config where key = ‘sys\_setting’





删除该条记录，即恢复到中控安装后的状态



刷新redis缓存



* **密码错误次数超限,账号被锁定**

中控打开用户安全开关,如下图



用户输入密码错误次数超限,将会出现下图所示



可以使用下面方法进行解决:

1. 进入/opt/qihu360/hsmp/application目录下,执行命令 php yii clean-login-err/clean-account xxx



1. 然后刷新中控登录页面,输入正确密码后即可成功登录

## 13.2 系统工具

* **B13版本及之前版本备份的数据，在B15版本上进行数据恢复，出现部分数据恢复失败**

B15版本，进行数据存储和查询的优化，更改了数据存储格式，所以B13版本及之前版本备份的数据在B15上恢复，出现失败是正常现象。

建议用户不要在高版本上恢复低版本备份的数据。

# 其它

* **查看中控安装时间**

more /opt/qihu360/hsmp/ INSTALL



* **查看中控版本**

more /opt/qihu360/hsmp/VERSION



* **Windows静默安装方法**
1. 中控下载Windows客户端360-wins(10.95.46.66\_8080\_8090).exe；
2. 客户端cmd中添加参数运行360-wins(10.95.46.66\_8080\_8090).exe /S，如下图：



* **Windows开启界面方法**
1. Windows界面默认隐藏，对外测试不建议开启界面；
2. 若有需要显示界面，方法如下:
3. 中控界面关闭Windows自我保护；
4. 客户端修改修改注册表

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\360Safe\360Ent]—show\_main\_ui设置为1；

1. 客户端上双击应用图标，即可显示界面；
* **重启控制中心的服务命令**

进入/opt/qihu360/hsmp目录下，执行命令：

supervisorctl -s unix:///opt/qihu360/hsmp/logs/supervisor.sock restart all



* **控制台忘记登录密码，如何修改密码**

在安装目录/opt/qihu360/hsmp/bin下面有个control.sh ，进到 /opt/qihu360/hsmp/bin(命令 cd /opt/qihu360/hsmp/bin)

然后运行下面命令： bash control.sh reset-pass 新密码（为重置后的密码）



* **多用户登录server2003sp2x64系统**

Server2003sp2x64系统支持同时登录多个用户，若在此系统上安装客户端端，则多用户登录后，会出现多个360tray进程；

* **远程安装Windows客户端，客户端已安装成功，但中控为什么显示安装失败**

远程安装Windows客户端，客户端安装成功，心跳正常，进程正常，但中控一直未返回安装成功，可查看中控日志/opt/qihu360/hsmp/logs/deploy\_client\_stdout.log，中控一直在等待，等到10分钟超时之后，中控返回安装失败，报未知错误，此时可在主机发现中下发同步任务，安装成功的客户端将显示已安装；

* **普通管理员登录控制中心，主机管理中为什么没有文件分发功能**

文件分发功能目前只支持超级管理员使用，不支持普通管理员使用，因此在创建普通管理员时，权限分配中不包括文件分发，所以普通管理员登录控制中心，主机管理中没有文件分发功能；

* **SuspendMonitor.exe进程自保问题**

SuspendMonitor.exe进程的自保问题目前仅在64位的windows操作系统（所有server2003\_x64除外）上有效；在32位的系统上自保不支持该进程；

若该进程意外退出或被杀掉，360EntClient.exe进程正常的状态下会在10s内将该进程启动；

* **控制中心与Linux客户端部署在同一Linux系统下，会相互干扰吗？**

存在相互干扰的可能性。在同一台Linux系统下，先部署控制中心，再部署Linux客户端，可能会造成控制中心与Linux客户端的部分通信混乱，最终导致控制中心部分服务异常；

若误操作造成这种情况，先卸载Linux客户端，再重启控制中心的所有服务，控制中心即可恢复正常；