1. 需求列表

|  |
| --- |
| 能够智能识别木马上传行为，支持自定义上传文件的大小、后缀名。 |
| 用户可自定义对上传脚本文件的处理方式：直接拦截，智能识别。 |
| 支持木马上传日志，记录上传时间，源地址，目的地址，目的URL，拦截原因。支持将木马文件直接下载至本地进行人工分析。 |
| 可根据用户设置与云端联动，可疑文件上传云端检测 |

1. 时序图





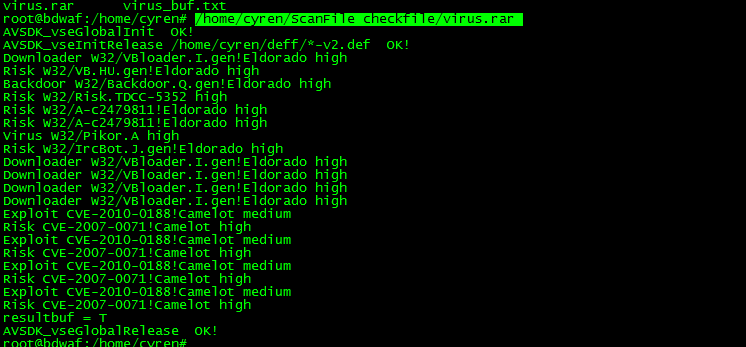
1. 开发方案
   1. nginx及扫描工具
      1. 扫描工具
         1. 安装工具

安装目录为/home/cyren

扫描工具目录为:/home/cyren/ScanFile

病毒文件存放目录/usr/local/bluedon/checkFile/viruesFile

* + - 1. 扫描方式



resultbuf = T 为有木马或病毒

* + - 1. 定时升级

4小时检查一次升级，即

vi /etc/crontab

追加一行

\* \*/4 \* \* \* root /home/cyren/src/avdeff\_update\_online/avdeff\_update\_online

* + 1. nginx

此需求仅适用于反向代理，透明桥接因框架性原因，无法处理报文体。

该需求仅考虑全局性配置，不适用于站点组模式

nginx通过配置modsecurity.conf,包括uploadfile.conf，uploadfile.conf内容为：

SecRule REQUEST\_METHOD "!^POST$" "phase:2,id:'800100',t:none,nolog,pass,skipAfter:END\_UPLOAD\_PROTECTION\_CHECK"

SecRule FILES "\.(jpg|png)$" "phase:2,id:'800101',t:none,log,deny,msg:'uploadfile block:time=%{time}|::|uri=%{request\_uri}|::|tmpname=%{files\_tmpnames}|::|realname=%{files}|::|size=%{files\_sizes} '"

SecRule REQUEST\_BODY "@gt 5242880" "phase:2,id:'800102',t:none,nolog,pass,skipAfter:END\_POST\_CONTENT\_MONITOR\_CHECK"

SecRule &FILES "@eq 1" "phase:2,id:'800103',t:none,log,pass,msg:'uploadfile block:time=%{time}|::|uri=%{request\_uri}|::|tmpname=%{files\_tmpnames}|::|realname=%{files}|::|size=%{files\_sizes} '"

SecMarker END\_UPLOAD\_PROTECTION\_CHECK

* 1. python
     1. 修改反向代理模板
* 当开启上传文件过滤时，生成的modsecurity.conf, 需要包含uploadfile.conf（include位置在"敏感词警告"功能之前)。
* 规则库无需添加这四条规则.
* 当"敏感词警告"或“智能木马检测”两者有一项功能启用时，打开modsecurity.conf以下开关：

SecUploadKeepFiles On

或者

SecUploadKeepFiles RelevantOnly

* + 1. 添加上传文件日志表

至少包含以下字段：

ID、时间、URI、文件名、处理方式(按后缀拦截、扫描)、威胁等级、扫描信息、保存路径

* + 1. 添加日志的处理
       1. 800100

上传文件仅为post请求，非post跳过下面的800101，800102，800103

* + - 1. 800101

该规则为上传文件触发指定后缀后，被拦截。日志格式见附件

msg 包含：时间、URI、临时文件名、实际文件名、文件大小；各字段以|：：|分隔

流程见：**上传文件指定后缀过滤流程**

**备注：**

**1、该拦截日志，不记入侵日志表，另记上传文件数据表。**

* + - 1. 800102

800102判断文件大小：大于配置的大小跳过800103

* + - 1. 800103

该规则为上传文件没有触发指定后缀后，通知python上传文件信息。日志格式见附件



msg 包含：时间、URI、临时文件名、实际文件名、文件大小；各字段以|：：|分隔

流程见：**上传文件扫描流程**

**备注：**

**1、该拦截日志，不记入侵日志表，另记上传文件数据表**

* + 1. 保存文件定期清理

**/usr/local/bluedon/checkFile/viruesFile默认只保存10G，隔清清理最旧的**

* 1. php
     1. 添加配置页面

包括以下功能：

是否启用上传文件分析

自定义指定拦截的文件后缀(如JPG、PNG)

设置最大的文件分析大小(默认5M)

* + 1. 添加上传文件日志界面

参考2.6.1，

增加处理方式(按后缀拦截、扫描)，

严重等级为低中高的，可供下载

