防火墙开启防病毒功能后无法拦截病毒文件

AV防病毒 孔凡安 2022-08-18 发表

组网及说明

不涉及

问题描述

防火墙开启防病毒功能后无法拦截病毒文件
特征库版本最新，使用默认的防病毒配置，对FTP文件做过滤。
发现依然能通过防火墙FTP传输病毒文件。
病毒测试文件见链接：
https://blog.csdn.net/Mnky/article/details/65894

病毒测试文件

原创 Mnky 于 2011-07-07 08:54:16 发布 1190 收藏 1 版权
分类专栏： 病毒 文章标签： 测试 dos

病毒 专栏收录该内容 0 订阅 0 篇文章 订阅专栏

打开“记事本”，将下面一行文本copy进去，保存文件，文件类型选择“所有文件”，文件名为“EICAR.COM”。

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

如果开着文件实时监控，该文件不用执行即可被查出（在DOS下执行会出现“EICAR-STANDARD-ANTIVIRUS-TEST-FILE!”一行文字）。
该文件是欧洲反病毒发展研究所（EICAR）提供的“EICAR标准反病毒测试文件”，它是反病毒软件厂商在全世界范围内提供的用来检查反病毒软件安装的一个测试标准。**文件本身不是真的病毒！**

改为不可执行文件或对该 字符串 进行修改都不再被视为病毒（哪怕修改那串显示的字符串）。

p.s. 把这串字符贴到这里都会自动加上<a href="mailtomailto:>标签，也许是这里网站的防毒措施？呵呵

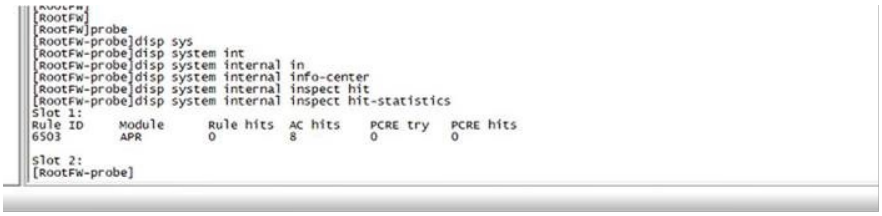
==========

原文时间：2005.07.22
原文地址：http://mnky.bokee.com/2347431.html

过程分析

首先查看应用层检测引擎的工作状态，显示正常。

其次查看，底层是否命中，发现并未有规则命中。



```
[RootFW]
[RootFW]probe
[RootFW-probe]disp sys
[RootFW-probe]disp system int
[RootFW-probe]disp system internal in
[RootFW-probe]disp system internal info-center
[RootFW-probe]disp system internal inspect hit
[RootFW-probe]disp system internal inspect hit-statistics
Slot 1:
Rule ID     Module      Rule hits  AC hits    PCRE try   PCRE hits
6503        APR         0          8          0          0

Slot 2:
[RootFW-probe]
```

解决方法

开启如下命令：

inspect md5-verify all-files命令用来配置应用层检测引擎对所有文件进行MD5哈希运算。

undo inspect md5-verify all-files命令用来恢复缺省情况。

【命令】

inspect md5-verify all-files

undo inspect md5-verify all-files

【缺省情况】

只对可执行文件、office文件和压缩文件等文件进行MD5哈希运算。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

vsys-admin

【使用指导】

开启此功能后，应用层检测引擎将对所有文件进行MD5哈希运算，并将生成的MD5值与特征库中的MD5规则进行匹配。如果匹配成功，则认为该文件携带病毒。

开启此功能后将对设备业务处理性能产生影响，请管理员根据设备实际情况进行配置。

【举例】

配置应用层检测引擎对所有文件进行MD5哈希运算。

<Sysname> system-view

[Sysname] inspect md5-verify all-files

【相关命令】

· display inspect md5-verify configuration