7 防毒墙与杀毒软件

防毒墙实质就是一个防病毒【恶意代码】软件，但针对的主要是 HTTP、HTTPS、FTP、SMTP、POP、TELNET 之类的防护，基本上是在应用层。

内部访问外部的网络时，不把外部的恶意代码引入内部。

平常说的杀毒软件部署于本机，针对操作系统的杀毒。

0x01 实验环境

这里的任意一个都可以，推荐几个企业版集中管控杀毒软件(c/s)

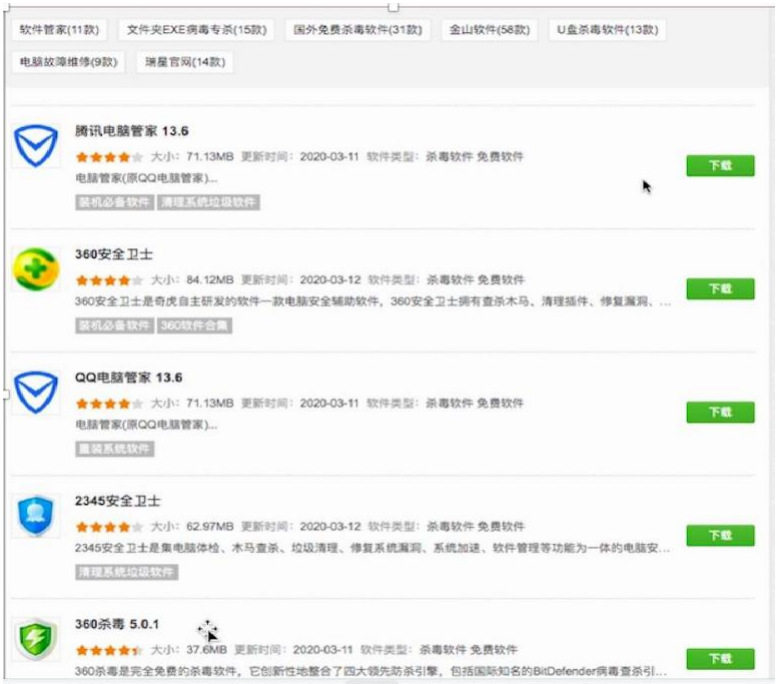
奇安信：天擎【带终端管理功能】政务单位、国企、央企

360:安全卫士

瑞星：

卡巴斯基

赛门铁克



0x02 原理介绍

第一种：基于特征，特征码。优点：判断准，误报比较低。缺点：不能发现未知恶意代码，效率下降

第二种：异常行为， 【基线判断】,>10 次/次。能发现未知恶意代码，误报率高

0x30 实践操作

自己安装一个安全卫士。C/S,能反应整个的情况，统一防病毒软件。

不能迷信杀毒软件，Oday,过杀软。