想開發一個安全軟件，怎麼搞?

黑客技術與網絡安全 今天

以下文章來源於小白學黑客，作者小白哥

小白學黑客

小白也能看懂的網絡安全教程

> **來自公眾號：小白學黑客**

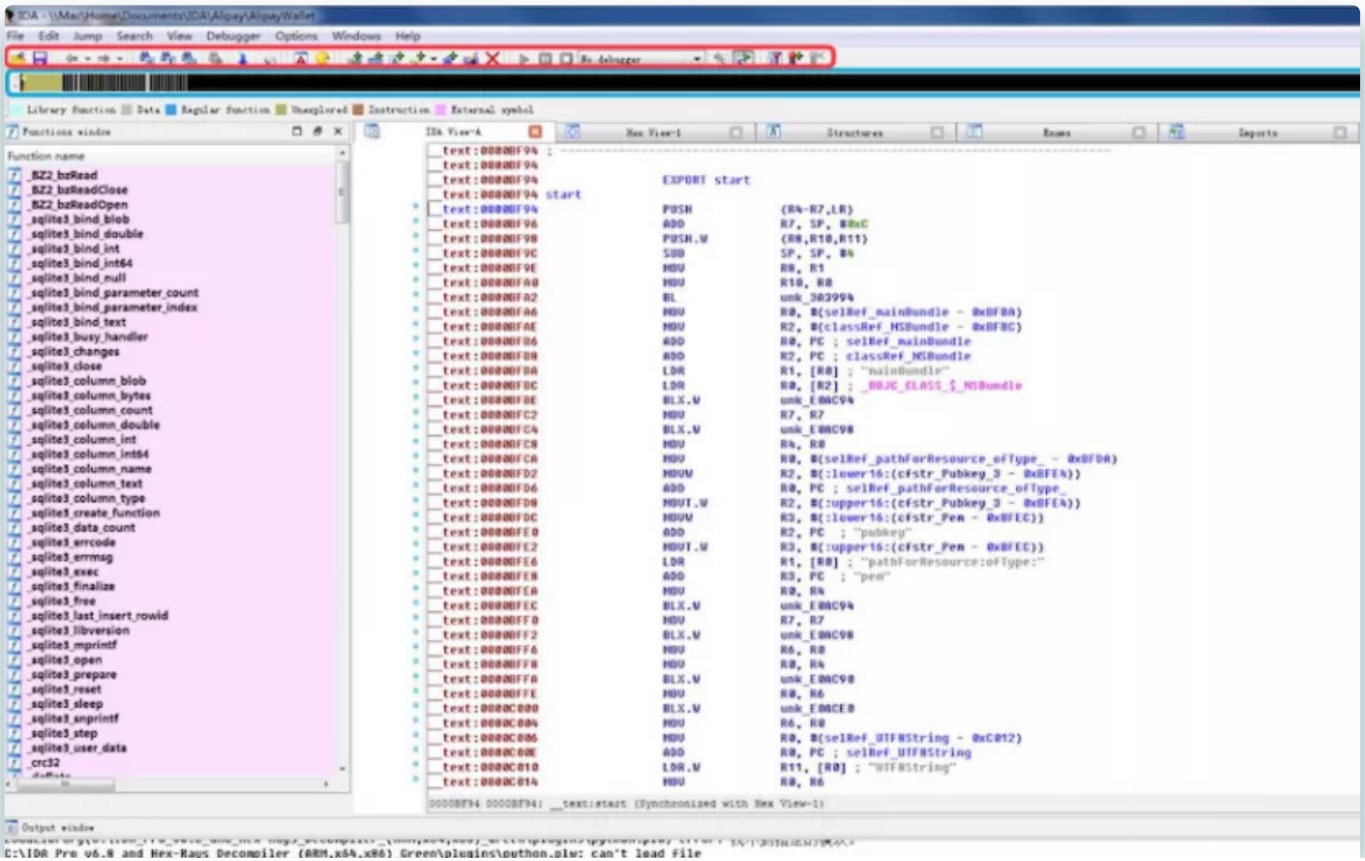
今天跟大家介紹一下，開發一個像360、QQ電腦管家這樣的安全軟件，有哪些核心技術，或者說哪些核心組件是必不可少的？

反病毒引擎

首先，第一個必不可少的就是反病毒引擎。安全軟件最早的核心也就是這個東西，它的目的就是檢測一個文件是不是惡意軟件。

反病毒引擎主要通過對文件進行**靜態分析**，識別惡意文件的特徵，與自己的病毒特徵庫進行匹配，來判斷目標是否是惡意的。

這裡面主要用到的技術有文件格式識別、加殼脫殼技術、加密解密技術、可執行文件的反彙編、指令級的特徵匹配、虛擬執行、樣本家族團伙基因判別、機器學習等等。

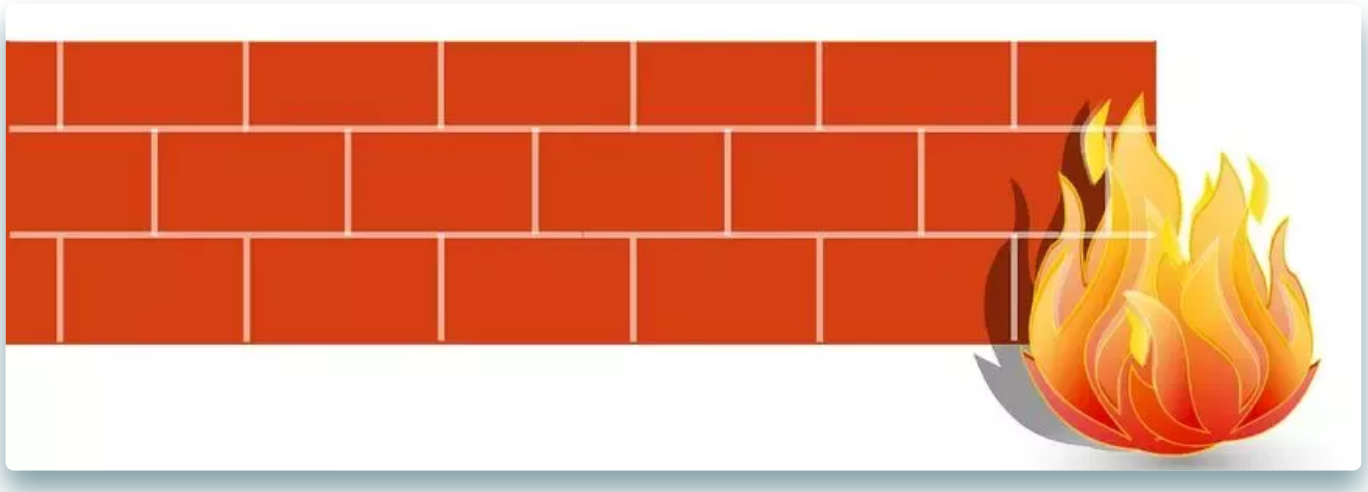


HOOK驅動

安全軟件的主要任務，就是要保護我們的電腦不受病毒、木馬這些惡意軟件的侵害，除了能通過靜態分析識別已知的威脅，還要守住計算機的安全防線，防止被惡意軟件攻破。

那如何防守呢？

安全軟件需要感知計算機上發生的一切事情，這包含，每一個進程線程的創建、每一個文件的創建和讀寫、每一次網絡連接的建立，甚至每一次系統服務的調用。



安全軟件是通過**HOOK技術**來做到這一切的。

安全軟件使用內核驅動程序，劫持應用程序通向操作系統內核的關鍵入口，從而監控所有進程的行為。

几乎每一个安全软件都有这么一个驱动程序，它内部有一套HOOK框架，提供编程接口给其他驱动程序调用，比如360中大名鼎鼎的**hookport.sys**。

主动防御驱动

光有一个HOOK框架驱动不行，还得配套有一个主动防御驱动，负责完成具体的安全防御。

应用层上一般会有一个主动防御进程，负责从安全软件云端服务器接收控制指令，下发最新的防御规则，最新的特征库，比如拦截哪些程序，拦截哪些操作等等。

主动防御进程拉取到这些信息后，下发给内核空间的主动防御驱动程序，由它来具体执行对应的拦截行为。

文件过滤驱动

通过HOOK驱动来进行监控，有时候并不能完全解决问题。有一些底层软件，可以绕过系统API调用，这样一来HOOK驱动就监控不到了。

因此，安全软件一般还会配套有一个文件过滤驱动，通过文件系统提供的接口实现更底层的文件监控功能。

这一类驱动一般使用的技术有minifilter、sfilter等。

网络监控驱动

和文件过滤驱动类似，对于网络同样需要一个更底层的驱动程序，来监控计算机中所有的网络连接，通过操作系统网络架构底层的接口，监控计算机进进出出所有的数据包，将网络通信情况完全了如指掌。

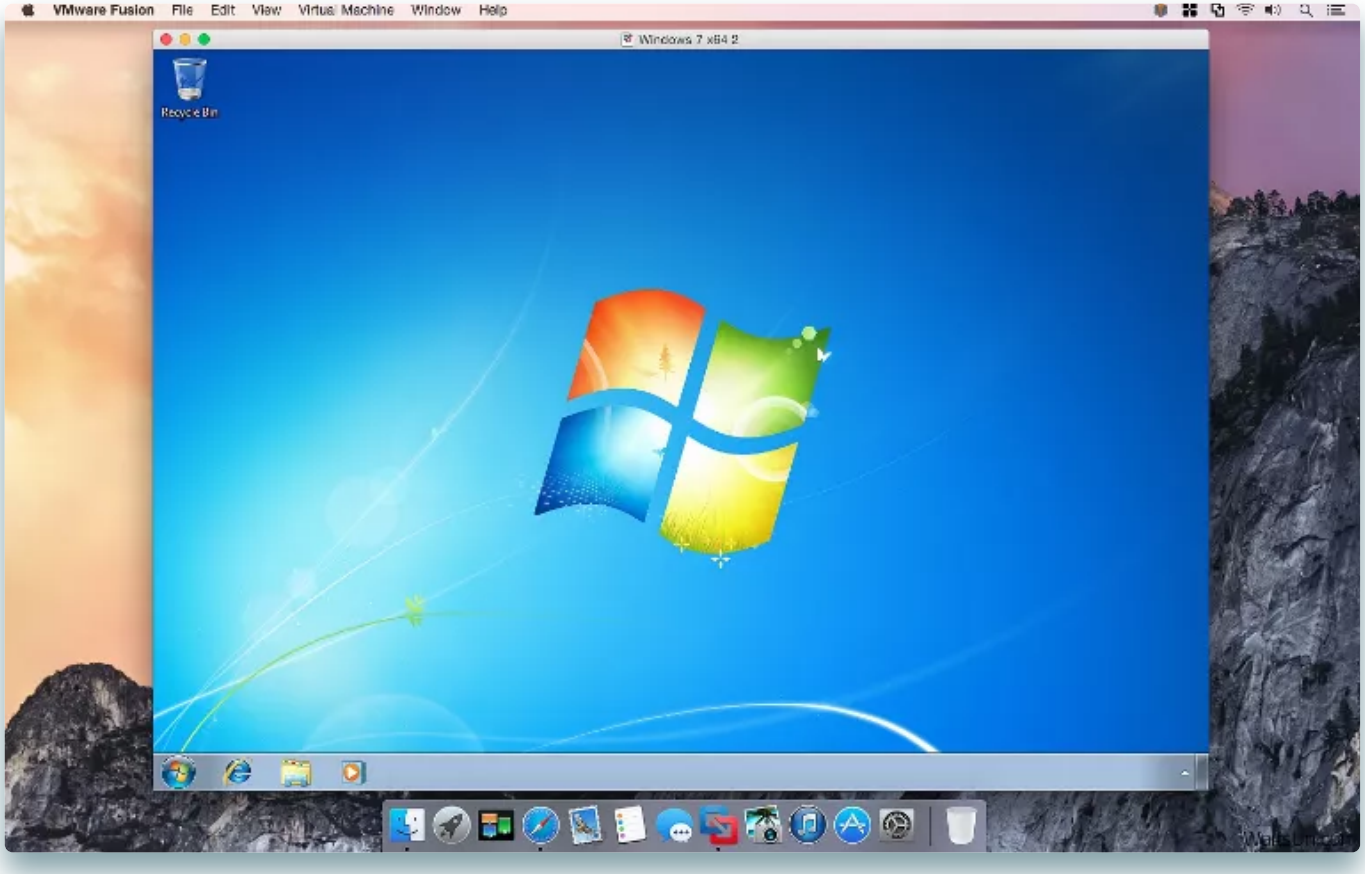
这一类驱动使用的技术有TDI、NDIS、WFP等。

沙箱驱动

除了守护我们的计算机，安全软件的另外主要工作还是分析恶意程序。

前面提到的反病毒引擎主要是**静态分析**，但静态分析有一定的局限性，很多时候程序的恶意需要运行以后才会暴露出来。因此，**动态分析**技术少不了。

虽然网络安全技术发展了很多年，但动态分析用到的主要技术还是“**沙箱分析**”。



所谓沙箱分析，就是提供一个仿真的环境，把目标丢进去，让它跑起来，等到它原形毕露，是不是恶意就能一目了然。

因此，許多安全軟件也會提供一個沙箱驅動，通過內核隔離，模擬出一個“安全”的執行環境，讓目標在其中運行。

攻防驅動

安全軟件目標這麼大，自然會招來很多惡意軟件的攻擊。除了惡意軟件，有些安全軟件互相為了搶奪用戶，也會互相攻擊。

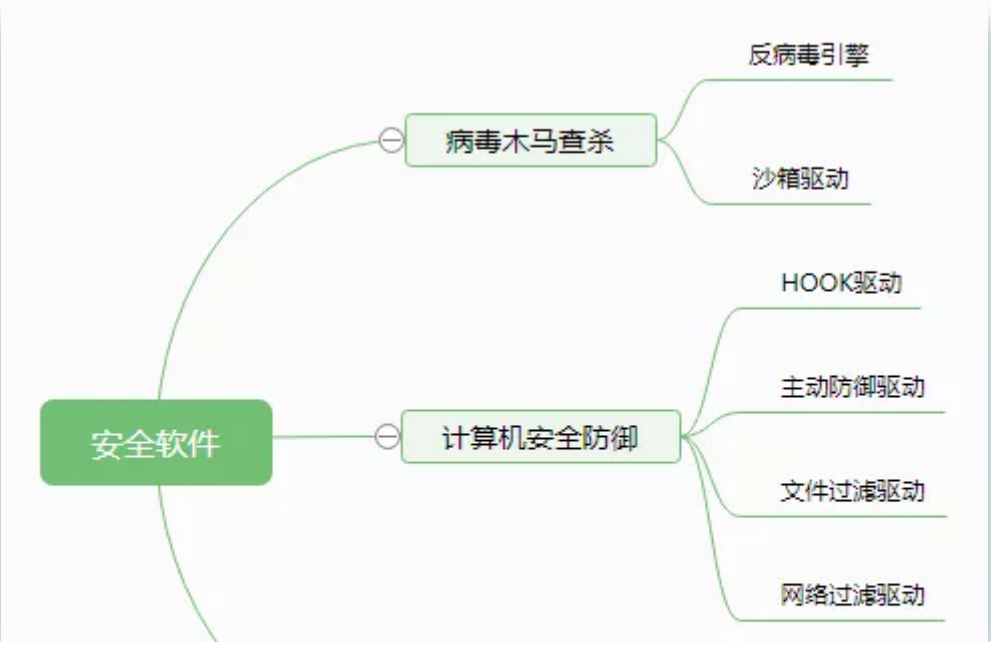
所以，安全軟件必須加強自身的防禦。

前面提到的主動防禦，屬於正規軍作戰，也包含有保護自己的能力，但面對同樣是內核級的攻擊對手，這一招基本就收效甚微了。

因此，安全軟件一般還會有一個攻防驅動，通過各種手段和對手作戰，保護自己，這裡面用到的技術就五花八門了。

總結

總結一下，開發一款安全軟件，主要有三方面的事情要做：



看完這篇文章，你有什麼收穫嗎，寫作不易，歡迎動動手指轉發分享。

--- EOF ---

推薦↓↓↓

Linux學習

專注分享Linux/Unix相關內容，包括Linux命令、Linux内核、Linux系統開發、Linux運維、網絡編程、開發工具等Linux相關知識和技術

公眾號

喜歡此內容的人還喜歡

滲透安全及滲透測試流程

天億網絡安全

逆向實戰｜jni與魔改base64解密

WhITECat安全團隊