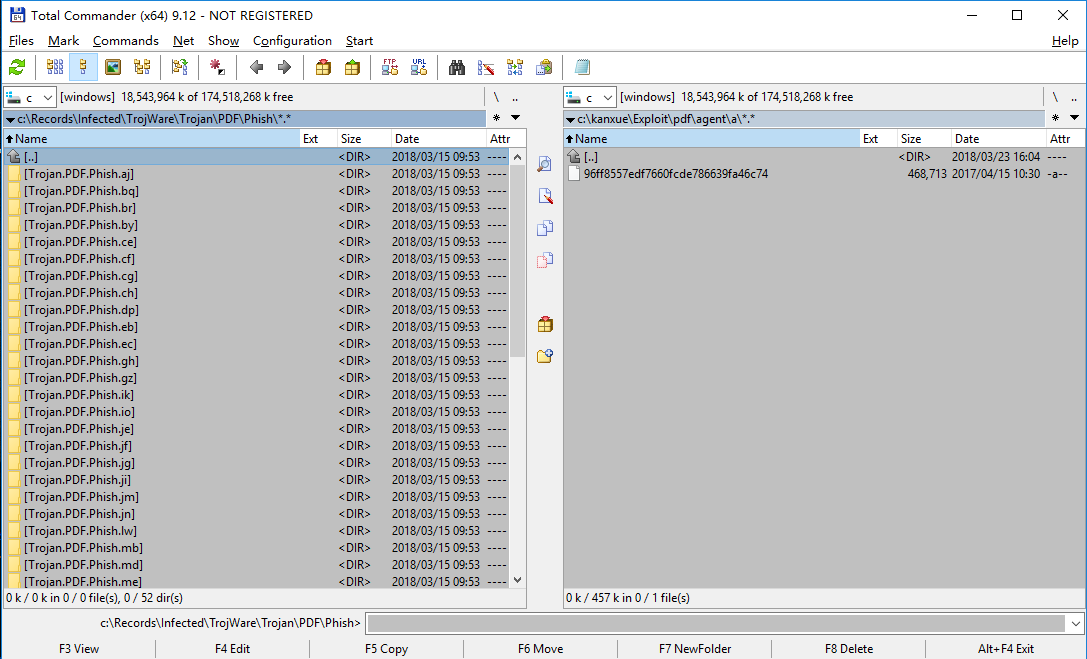
**前言**

本次课程为大家介绍的是我们病毒分析师在日常工作中经常使用的一些工具以及快速分析的技巧。一般来说，在不写分析报告以及不做高级查杀研究的情况下，病毒分析师并不需要对样本进行深入分析，只要判断样本黑白、进行归类并提取特征即可。这里我会将这一系列完整的流程展现给大家。

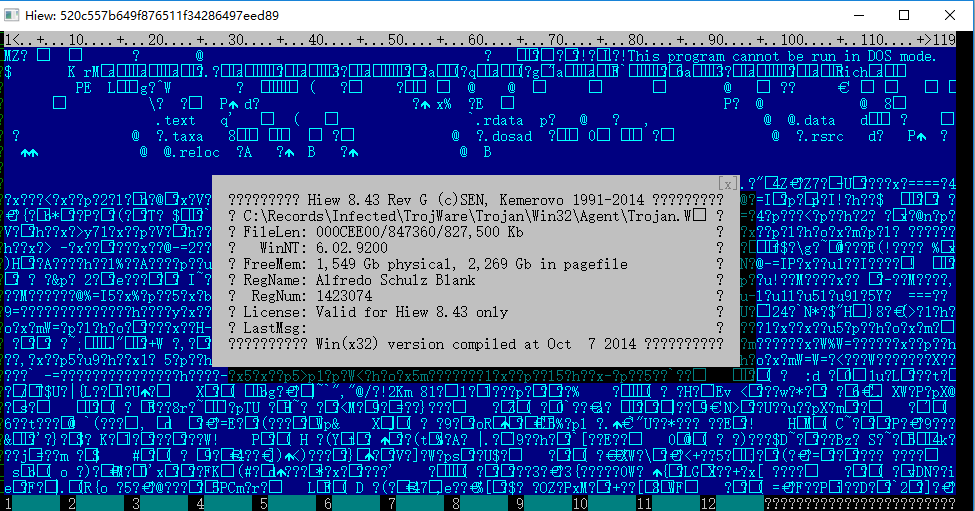
**工具介绍**

由于我们在日常的分析中要面对大量的样本文件，并且还需要对这些文件进行复制、删除以及目录的创建等操作，因此需要一款文件管理工具来辅助我们的工作，这里我所使用的是Total Commander：



主界面中有两个窗格，便于文件的复制等操作，使用Tab键可实现两个窗格之间的切换。界面下方还有一些快捷键的说明。比如F3是查看文件，F5是复制文件，F7是创建目录等。

文件的查看与分析工具使用的是Hiew，可以在Total Commander的Configuration下的Options里面找到Edit/View，将External Viewer设置为我们的Hiew的路径即可，这样我们以后只要使用F3这个快捷键，就可以用Hiew实现对样本的查看了：

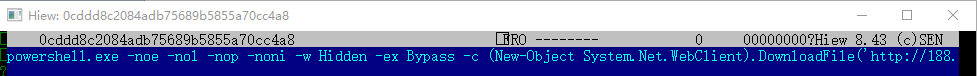


起初Hiew默认的是以文本的形式打开的，我们也可以通过回车键进行切换，比如切换到十六进制模式或者反汇编模式等，用于不同情况的分析工作。Hiew的下方也有一些快捷键的说明，来便于我们的分析工作。我们之所以要使用Hiew这款工具，是因为它小巧快速，特别是当目标文件比较大的时候，我们用Hiew可以实现瞬间将文件打开。这款软件的优势，也会在接下来的分析中，有所体现。

**样本分析**

本次课程为大家准备了八个样本，是我们分析师几乎每天都会遇到的样本类型。这些样本看似很简单，但是往往能够有效躲避杀软的查杀，因此是值得我们进行深入研究的。

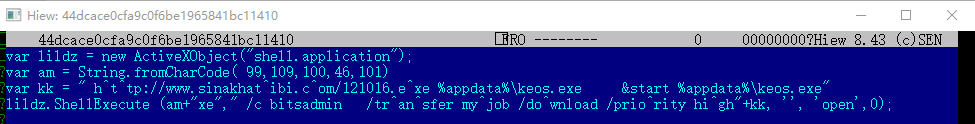
**1、0cddd8c2084adb75689b5855a70cc4a8**



利用Hiew打开后，首先从前几个字符可以知道这是一个Powershell程序，由后面的Hidden可知它会以隐藏的形式运行，接着分析可以发现，它又在某网站执行了下载操作，并且将下载下来的exe文件保存在了临时文件夹，并将其后缀修改成了pif类型，之后再执行这个文件。“隐藏执行”、“下载并修改文件后缀”等，都属于非常可疑的操作，正常程序是不会这么做的，因此基本可以确定说它就是一个恶意程序了。当然了，为了谨慎起见，还应该分析这里出现的网站所对应的下载下来的程序，如果确定下载的程序是恶意的，那么不单单要拉黑这个原始的执行下载的文件，还应该将该网站以及下载下来的文件拉黑才可以，这才是完整的分析流程。

接下来我们可以给这个文件归类，我所采用的是四段命名法。第一段是这个恶意程序的类型，我们发现它是一个下载者程序，所以可以起名为Trojan-Downloader。第二段是这个程序的类型，它属于Powershell。第三段是这个程序的家族名称，这里起名为Agent即可。第四段是这个程序的编号，我习惯以字母进行排序表示，由于这是第一个样本，因此编号为a。于是，完整的名称是：Trojan-Downloader. Powershell. Agent.a。于是这个样本就分析并归类完成了。

**2、9b2293323610ccb2af33f977cb21f45c**

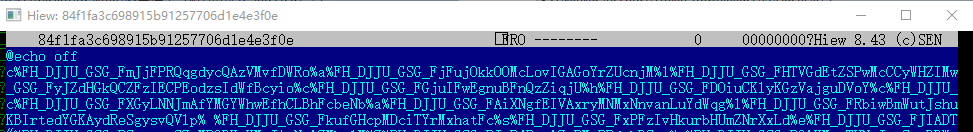


首先由变量声明符号var就可以知道它是一个JavaScript脚本，接下来在第三行可以发现，这里出现了一个网址，但是奇怪的是，这个网址里面的http、com以及exe等几个字符都被尖角号给隔开了，包括第四行也有类似的情况，而这种写法在正常的程序里面是不可能出现的，所以就可以直接将这个程序判定为有问题的程序了。

同样的，为了谨慎起见，还应该将这个网址对应的程序下载下来分析，如果也是恶意程序，那么网址和该程序都是要拉黑的。但是到目前这一步，我们就可以直接给这个程序归类了。依据之前讲过的归类原则，这里将其命名为Trojan-Downloader. JS. Agent.a。

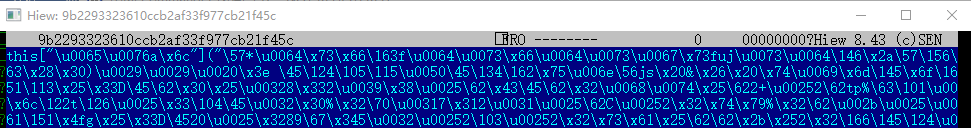
如果想要提取传统的特征，那么可以在http、com或者exe的位置进行提取，因为正常的程序不可能将这些字符分开来写。

**3、44dcace0cfa9c0f6be1965841bc11410**



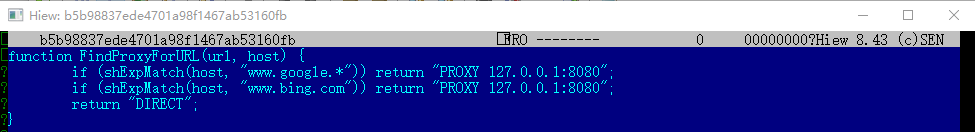
首先由echo off就可以知道它是一个BAT即批处理程序。接下来可以发现，程序写得很乱，根本看不出它要干什么，这也是恶意程序常用的混淆手段，因此就可以直接把它判定为是恶意的了。如果要提特征的话，那么提在这些乱码的位置也就可以了，正常的程序里面是不会出现这些的。于是可以将这个样本归类并命名为：Trojan.BAT.Agent.a。

**4、84f1fa3c698915b91257706d1e4e3f0e**



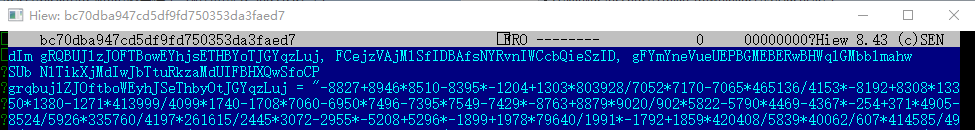
类似于上一个样本，这个样本的代码同样没有以明文的形式呈现，因此可以直接将其判定为是恶意的，将其归类并命名为：Trojan.JS.Agent.a。

**5、b5b98837ede4701a98f1467ab53160fb**



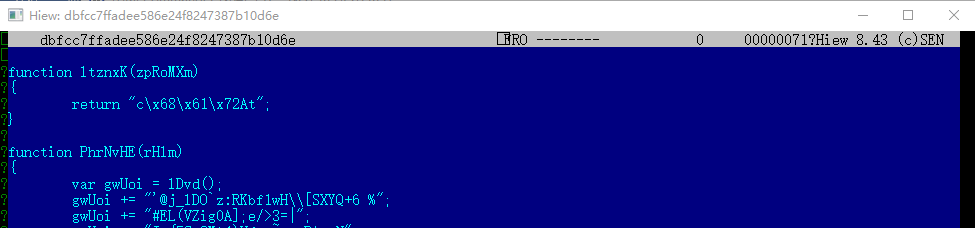
这个样本的代码就非常清晰了，由其语句可以知道，当这个程序执行后，如果用户想要访问google或者bing，那么就会直接重定向到127.0.0.1这个地址了，也就是会阻止用户的正常访问，因此就可以直接把它判定为是恶意的了。将其归类并命名为：Trojan.JS.Redirector.a。

**6、bc70dba947cd5df9fd750353da3faed7**



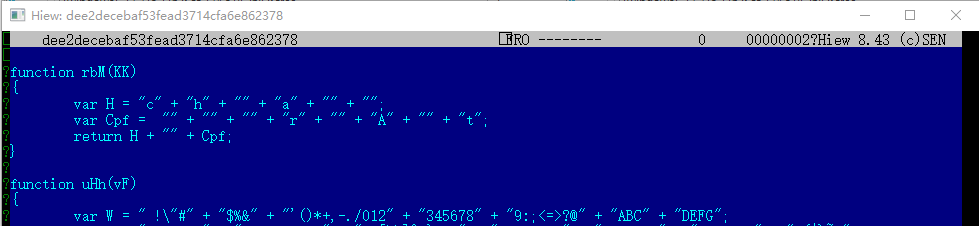
首先由最初的dim就可以知道它是一个VBScript脚本文件，由于它的代码写得很乱，同样地，也可以直接把它拉黑了，将其归类并命名为：Trojan.VBS.Agent.a。

**7、dbfcc7ffadee586e24f8247387b10d6e**



首先由var可知它是一个JavaScript文件，接下来由return后面的编码形式（ASCII码）以及后面的一些乱码可知，它也是一个有问题的程序，因此可以将其归类并命名为：Trojan.JS.Agent.b。特征提取在乱码的位置即可。

**8、dee2decebaf53fead3714cfa6e862378**



类似于上一个样本，这个样本的代码同样写得很不规整，所以可以直接将其拉黑。可以将其归类并命名为：Trojan.JS.Agent.c。

**小结**

通过本次课程的学习，相信大家已经掌握了常见的脚本类恶意程序的快速判断技巧以及特征的提取方式。从某种意义上来说，只要我们看到目标样本的代码写得非常晦涩难懂，那么它十有八九是恶意程序了。因为这是恶意程序经常使用的躲避杀软查杀的混淆方式。事实上，利用传统的特征码查杀的方式来对抗这类脚本木马的效果并不好，因此必须要使用诸如启发或者机器学习的方式来对抗这一批样本。这些高级技巧我会在未来的高级篇里面为大家讲解。