**前言**

本系列课程名为《恶意程序分析与高级对抗技术》，重点给大家介绍各种类型恶意程序的基本分析方法以及针对于某一批类似样本的高级对抗技术，利用高级查杀技术，从而实现对恶意程序的通杀。

**课程概述**

为了使大家能够循序渐进地理解相应的技术，本系列课程主要分为四个部分进行讲解。其中的概论篇主要是对课程的一个总体介绍，以及课程中所使用的一些分析工具的简单讲解。基础篇主要教给大家的是快速对恶意程序进行判断的技巧，力求以最少最简单的工具实现对目标样本恶意与否的判断。以求让大家了解各种恶意程序的特点，打消大家对恶意程序的恐惧。在进阶篇里面主要讨论的是如何对恶意程序进行完整详细的分析，需要结合对应的静态与动态分析工具，从而全面的了解一个恶意程序的行为，进而为写出专杀工具打下基础。高级篇里面主要讲解的是如何对一批类似样本实现通杀，有别于传统的病毒特征，高级特征的编写需要在对大量样本进行深入分析的基础上，运用创新的思维以程序的形式来对抗大批量的恶意程序。重点会介绍启发式查杀以及基本的机器学习方式来对抗不同类型的恶意程序的技术。相信通过本系列课程的学习，不单单能够让大家掌握恶意程序分析的基本技巧，更加能够拓宽大家的思维，让大家知道，反病毒领域的工作，不单单是病毒分析，不单单是特征的提取，其实还有更加广阔的世界是值得我们去探索的，从而在这场没有硝烟的战场中，贡献自己的智慧。

**常用工具简介**

正所谓“工欲善其事，必先利其器”，这一观点在我们病毒分析领域尤为重要。优秀的工具对我们的工作往往能够起到事半功倍的效果，因此从某种程度上来讲，病毒分析其实就是建立在对相关编程语言深入理解的基础上，对各种分析工具综合运用的一种技术。以下所列出的是我在本系列课程中重点使用的一些工具：

1、静态分析工具：Hiew、IDA等

在我们病毒分析的日常工作中，大部分时间是利用Hiew这款工具对目标程序进行分析的，只有在目标程序比较复杂，或者需要写分析报告的时候，才会使用IDA进行分析。那么在本系列的课程中也是如此，在基础篇中，我主要会使用Hiew来为大家演示样本的快速判断技术，而在进阶篇里面，则主要依靠IDA来对目标样本进行详细分析。

2、动态分析工具：OllyDbg、WinDbg以及火绒剑等

一般来说，用户层（Ring3层）的动态调试，OD是我们的不二选择，而在内核层（Ring0层）或者在软件排错领域，我们更多地会选择WinDbg。而火绒剑则主要用于目标样本的动态监控，可以获取到目标样本的详细行为。

3、虚拟机工具及操作系统：VMWare、Windows XP、Windows 7 64位版本

由于我们分析的样本可能具有极强的破坏性，因此如果需要将目标样本运行起来进行分析的话，那么一定要在虚拟中进行。我所使用的是VMWare，并且在虚拟机里面安装了Windows XP操作系统用于分析32位程序，如果需要动态分析64位程序，我在虚拟机里面使用的是Windows 7的64位版本。

以上是对本系列课程中主要使用的工具的简单介绍，事实上在应对不同的样本的时候，我们还会使用其它的一些辅助分析工具，那么这些工具会在具体的课程中再进行介绍。

**小结**

以上就是本系列课程的简单介绍与常用工具的讲解。我会在未来的课程中给大家循序渐进地剖析恶意程序的分析方法以及对抗技术。希望能够让大家早日成为计算机网络安全领域的杰出工程师。