恶意代码分析工具

# 恶意代码分析相关工具

1.Windows系统和应用程序监视工具[ProcessExplorer .](http://technet.microsoft.com/en-us/sysinternals/bb896653)  
2.Windows 系统监视工具 [ProcessMonitor](http://technet.microsoft.com/en-us/sysinternals/bb896645)  
3.内存使用情况的统计工具 [Vmmap](http://technet.microsoft.com/en-us/sysinternals/dd535533)  
4.启动项目管理器[Autoruns](http://technet.microsoft.com/en-us/sysinternals/bb963902)  
5.注册表数据监视软件[RegMon](http://technet.microsoft.com/en-us/sysinternals/bb896652.aspx)  
6.网络抓包工具[WireShark](http://www.wireshark.org/download.html),[SmartSniff](http://www.nirsoft.net/utils/smsniff.html)  
7.安全监控分析应用软件[Gmer](http://www.gmer.net/)  
8.系统辅助工具 [SysinternalsSuite](http://technet.microsoft.com/en-us/sysinternals/bb842062)  
9.用户访问权限查看工具 [AccessChk](http://technet.microsoft.com/en-us/sysinternals/bb664922)  
10.调试工具[OllyDbg](http://www.ollydbg.de/),  [ImmunityDebugger](https://www.immunityinc.com/products-immdbg.shtml)  
11.十六进制编码处理工具[Hxd](http://mh-nexus.de/en/hxd/),[Winhex](http://winhex.com/winhex/)  
12.文件夹和文件对比工具[BeyondCompare](http://www.scootersoftware.com/download.php)  
13.十六进制（二进制）文件对比工具[HexCmp](http://www.fairdell.com/hexcmp/)  
14.提取字符串的工具[Bintext](http://www.mcafee.com/kr/downloads/free-tools/bintext.aspx)  
15.静态调试工具[IDA](https://www.hex-rays.com/products/ida/support/download.shtml)  
16.哈希值检测小工具[HashTab](http://www.implbits.com/HashTab/HashTabWindows.aspx)

# 扫描恶意代码及分析工具

[www.virustotal.com](https://blog.csdn.net/chichoo/article/details/www.virustotal.com)  
<http://virscan.org/>  
<https://malwr.com/>  
<http://www.threattracksecurity.com/>  
<http://www.threatexpert.com/submit.aspx>  
<http://virusscan.jotti.org/en>  
<http://anubis.iseclab.org/>  
<http://wepawet.iseclab.org/>  
<http://eureka.cyber-ta.org/>  
<https://analysis.f-secure.com/portal/login.html>  
<http://www.xandora.net/upload/>

# Office文件相关恶意样本分析资料

<http://blog.zeltser.com/post/23229415724/malicious-code-inside-office-documents>  
<http://zeltser.com/reverse-malware/analyzing-malicious-documents.html>  
<http://msdn.microsoft.com/en-us/library/cc313118.aspx>  
<http://digital-forensics.sans.org/blog/2012/05/29/extract-flash-from-malicious-office-documents>

# PDF文件分析网站

<http://www.malwaretracker.com/pdf.php>  
<http://sandsprite.com/blogs/index.php?uid=7&pid=57>  
<http://blog.didierstevens.com/programs/pdf-tools/>  
<http://blog.zeltser.com/post/5360563894/tools-for-malicious-pdf-analysis>

# AdobeFlash/SWF 文件分析

<http://labs.adobe.com/technologies/swfinvestigator/>  
<http://h30499.www3.hp.com/t5/Following-the-Wh1t3-Rabbit/SWFScan-FREE-Flash-decompiler/ba-p/5440167#.U0ZLNnCVNyY>  
<http://h30499.www3.hp.com/t5/Following-the-Wh1t3-Rabbit/SWFScan-FREE-Flash-decompiler/ba-p/5440167>  
<http://betanews.com/2012/01/18/decompile-flash-files-with-hp-swfscan/>

# Android逆向相关

<http://code.google.com/p/droidbox/>  
<https://github.com/wuntee/androidAuditTools>  
<http://developer.android.com/sdk/index.html>  
<http://www.webopedia.com/TERM/A/Android_SDK.html>  
<http://code.google.com/p/smali/>  
<http://varaneckas.com/jad/>  
<https://www.hex-rays.com/products/ida/6.1/>  
<http://mobilesandbox.org/>  
<http://code.google.com/p/androguard/>

[apktool](https://code.google.com/p/android-apktool)

[dex2jar](http://code.google.com/)

[APKtoJava](https://github.com/faber03/AndroidMalwareEvaluatingTools)

[androidMalwareEvaluating](https://github.com/faber03/AndroidMalwareEvaluatingTools)

[DroidBox](http://code.google.com/p/droidbox/)**动态分析应用的方案**

[fiddler](http://www.telerik.com/fiddler)**手机抓包工具**

[Drozer](https://github.com/mwrlabs/drozer)**安全测试框架**

[Tamer](https://androidtamer.com/)**实时监控的虚拟环境**

[**jd-**gui](http://jd.benow.ca/)**分析jar文件工具**

[simplify](http://github.com/CalebFenton/simplify)**安卓代码混淆和还原dex文件工具**

[APKfuscator](https://github.com/strazzere/APKfuscator)**dex文件混淆工具**