黑客派

盘点韩剧《幽灵》出现的黑客软件工具

作者：oncereply

原文链接：https://hacpai.com/article/1366337937314

来源网站：黑客派

 今年韩国出了一部不错的电视剧——《幽灵》，相信看过的朋友对此剧应该印象深刻，在这个息泛滥的年代，PC、平板、智能手机不断进入到我们的生活。在享受高科技给我们带来便捷服务的同，你有没有想过有一天这些产品会给我们带来杀身之祸？有没有想过自己的一举一动，一言一行都在别有用心的人掌控？

 附《幽灵》电视剧里黑客哈达斯电脑的1280*720高清壁纸一张：
 <im title="hadasi" src="https://static.hacpai.com/images/img-loading.svg" alt="韩剧 幽灵 哈达斯壁纸 - www.singlex.net" width="583" height="329" data-src="http://www.singlex.net/wp-content/uploads/2012/08/hadasi.jpg">
 科普一下，援引搜搜百科词条“韩剧幽灵”：
<blockquote>
 《幽灵》为2012年韩国SBS电视台水木电视剧，由金亨植导演执导拍摄。该剧由苏志燮、李妍、严基俊等人主演，以网络犯罪和网络刑警为题材。讲述了随着社交网络的发展而产生的新型犯罪和这些犯罪做斗争的网络刑警们的故事。
</blockquote>
 下面将对《幽灵》中出现的黑客软件工具一一盘点：
 一、入侵检测类：
 1、Wireshark
 抓包工具，前称Ethereal。是一个网络封包分析软件，用来撷取网络封包，并尽可能显示出最为细的网络封包资料。Wireshark是目前全世界最广泛的网络封包分析软件之一。
 系统支持：Windows、linux、Mac OS
 官网下载：http://www.wireshark.org/download.html
  2、Metasploit
 渗透测试工具。Metasploit是一款开源、免费的安全漏洞检测工具，安全工作人员常用Metasploit工具来检测系统的安全性。2004年8月，在拉斯维加斯召开的黑帽简报（Black Hat Briefings)交流上，这款叫Metasploit 的攻击和渗透工具备受众黑客关注，出尽了风头。
 系统支持：Windows、linux
 官网下载： http://www.metasploi.com/download/
 3、NMap
 Network Mapper的简称，一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。Nap能够确定哪些服务运行在哪些连接端，并推断哪个操作系统计算机运行。黑客会利用nmap来搜集标电脑的网络设定，从而计划攻击的方法。
 系统支持：Windows、linux、Mac OS
 官网下载：http://nmap.org/download.html
 4、HDSI
 国产的注入工具神器，作者教主。是一款支持asp和php的SQL注入工具，堪比明小子和啊D。款注入神器出现在金宇炫为了复制电话卡而入侵韩国电话系统的时候。
 系统支持：Windows

 作者网站：http://www.HDSI2005.com，目前已无访问，可以搜索下载。
 二、电子取证类：
 1、Encase
 EnCase被誉为真正的电子取证工具。全球多数法庭将EnCase作为电脑犯罪侦查之认证工具，已超过百万件之公开使用案例。该软体被设计为以鉴识角度来取得电磁资料，并有强大的比对与分析工可供使用，不仅可复原被抹除的资料档案，还能进行各种资料的分析作业，帮助检调人员取得犯罪证。Encase 司法取证工具由犯罪司法专家参与开发，因此在法庭上得到认可。 支持多种文件系。目前貌似已有破解版流出。
 官方网站：http://www.gudancesoftware.com/encase-enterprise.htm
 电驴下载：http://www.verycd.com/opics/2897450/
 2、RoadMASSter
 RoadMASSter是一套用于司法部门的取证和数据分析专业系统，特别适于移动取证和高速数据获的需要。支持各种数据存储介质，包括Ultra DMAIDE硬盘/Ultra.SCSI硬盘/SATA硬盘/软盘/CDR/VD/CF-1/CF 2/MD/SD/MMC/SM/MS闪存卡和其他移动存储设备。该系统具有各种常用接口，包千兆网络接口/Firewire/1394A/B/和USB 接口。当连接了疑犯硬盘和证据硬盘后，可直接在Window环境下利用第三方数据分析软件进行分析。
<script async src="https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script>
<!-- 黑客派PC帖子内嵌-展示 -->
<ins class="adsbygoogle" style="display:block" data-ad-client="ca-pub-5357405790190342" data-ad-slot="8316640078" data-ad-format="auto" data-full-width-responsive="true"></in>
<script>
    (adsbygoogle = window.adsbygoogle || []).push({});
</script>
 官方网站：http://www.ics-iq.com/The-RoadMASSter-Forensics-Data-Acquisitionp/f.gr-7700-901d.htm
 三、加密解密类：
 1、OpenStego
 OpenStego可以把任何文件隐藏在图像中，采用GZIP压缩技术，采用PBE With MD5 And DE加密，使用时选取要隐藏的文件和用作表面掩饰的图像，即可生成PNG格式的图像文件。注：此软件JAVA环境支持。
 官网下载：http://sourcforge.net/projects/openstego/files/
 2、cain
 全称Cain & Abel。是由Oxid.it开发的一个针对Microsoft操作系统的免费口令恢复工具。称穷人使用的L0phtcrack。它的功能十分强大，可以网络嗅探，网络欺骗，破解加密口令、解码被打的口令、显示口令框、显示缓存口令和分析路由协议，甚至还可以监听内网中他人使用VOIP拨打电。
 四、动态调试类：
 1、OllyDbg
 简称OD，一个可视化界面的32位汇编分析调试器，是一个新的动态追踪工具，将IDA与SoftICE合起来的思想，Ring3级调试器,非常容易上手,已经代替SoftICE成为当今最为流行的调试解密工具，时还支持插件扩展功能,是目前最强大的调试工具。基本上，调试自己的程序因为有源码，一般用vc，解别人的程序用OllyDebug。目前已经有好多中文版本和入门教程了。

 官方网站：http://www.ollydbg.de/
 五、进程查看类
 1、Process Explorer
 也叫procexp，由Sysinternals开发的Windows系统和应用程序监视工具，目前已并入微软旗。Process Explorer不仅结合了文件监视器和注册表监视器两个工具的功能，还增加了包括稳定性和能改进、强大的过滤选项等多项重要的增强功能。Process Explorer最大的特色就是可以中终任何进，甚至包括系统的关键进程！
 官网：http:/technet.microsoft.com/en-us/sysinternals/bb896653.aspx
 六、卸载清除类
 1、BCWipe
 对于一些存有重要敏感文件的电脑，BCWipe是一个强力的文件清除工具。它提供 Delete with wping、Wipe free disk space 两种方式来清除你的磁盘文件。另外还有Swap file wiping、wipe Files slacks及wipe empty directory entries 3 个选项，BCWipe能够彻底销毁电脑硬盘里的敏感资料，你删除后的档案、文件真正永不见天
 系统支持：Windows
 官网下载：http://www.jetico.com/download
 七、后门木马类
 1、keylogger
 键盘记录器。可以将键盘的输入详细记录下来，包括时间，使用者，窗口，输入内容等等，有版本除键盘记录功能外，还有屏幕截图、远程控制等更加强大的功能
 官网下载：http://www.keylogger.ws/keylogger/download.html

 八、其它工具
 1、backtrack 5
 简称BT5。backtrack5是一款基于ubuntu的linux系统，其中集成了大量安全测试 渗透测试工。如今它是被最广泛采用的渗透测试框架并被世界各地的安全社区所使用。其一个强大的功能是破解线网络密码。
 官网下载：http://www.backtrack-liux.org/downloads/
 2、Browser History Spy
 一款浏览器缓存查看及恢复工具
 国外下载：http://securityxploed.com/browser-history-spy.php

 原文地址: http://www.singlex.net/1658.hl