****

**Any.run 交互式在线恶意软件分析沙盒**

Any.Run是一个相对较新的在线沙箱分析系统，用于运行分析可疑的可执行文件或访问可疑的站点，并记录系统和网络级别的活动。有一个订阅服务可以解锁更多的功能，但是对于个人使用，免费版本已经足够了。

**沙盒sandbox：**沙盒的特点在于很好的系统隔离性。在某种程度上，沙盒sandbox可以视为一个容器container，application运行在沙盒中，沙盒运行在windows操作系统上。运行在沙盒中的application和沙盒外的application一样可以访问硬盘中的文件等资源。

运行在**沙盒内外的application的主要区别**在于：

1. 对于沙盒外的application而言，沙盒内的application是透明的（即不可见的）；

2. 当沙盒内的application退出后，所做的更改将不会被保存。

一个很好的例子是：当沙盒内的application退出后，沙盒内的application已下载或“安装”的恶意软件都将被丢弃。

**虚拟机virtual machine**：虚拟机简称VM，其本质上是一个运行在操作系统之上的application，其特殊之处在于，虚拟机通过软件的方法模拟出一个完整独立的计算机的环境（但是并不是真是的计算机环境），这也是虚拟机名字的由来。因此，虚拟机就像是真实计算机的一个copy副本，虚拟机可以视为“机器内部的机器”。比如我们经常在windows操作系统上安装一个linux虚拟机，在这种情况下windows被称为host，linux被称为guest，一个host上可以安装多个guest虚拟机，就像是一个windows上可以安装多个application。

**虚拟机和沙盒的主要区别**在于：1. 当沙盒中的应用程序退出后，其所做的更改会被丢弃；而当虚拟机退出后，其所做的更改会被保存下来；2. 沙盒中的application和其他application共享机器的硬件资源；而虚拟机在安装时需要为其指定内存memory和cpu核且虚拟机不和其他application共享硬件资源。因此虚拟机实际上是很耗系统资源的。

**反汇编(Disassembly)**：把目标代码转为汇编代码的过程，也可以说是把机器语言转换为汇编语言代码、低级转高级的意思，常用于软件破解（例如找到它是如何注册的，从而解出它的注册码或者编写注册机）、外挂技术、病毒分析、逆向工程、软件汉化等领域。学习和理解反汇编语言对软件调试、漏洞分析、OS的内核原理及理解高级语言代码都有相当大的帮助，在此过程中我们可以领悟到软件作者的编程思想。总之一句话：软件一切神秘的运行机制全在反汇编代码里面。

**APT 高级长期威胁**，Advanced Persistent Threat又称高级持续性威胁、先进持续性威胁等，是指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，针对特定的目标。其通常是出于商业或政治动机，针对特定组织或国家，并要求在长时间内保持高隐蔽性。高级长期威胁包含三个要素：高级、长期、威胁。高级强调的是使用复杂精密的恶意软件及技术以利用系统中的漏洞。长期暗指某个外部力量会持续监控特定目标，并从其获取数据。威胁则指人为参与策划的攻击。

**C2服务器**（也称C&C，是Command and Control的缩写）服务器