供应链攻击前期学习

定义：供应链攻击是一种传播间谍软件的方式，一般通过产品软件官网或软件包存储库进行传播。通常来说，黑客会瞄准部署知名软件官网的服务器，篡改服务器上供普通用户下载的软件源代码，将间谍软件传播给前往官网下载软件的用户。此外，黑客还会向一些软件开发者常用的软件包存储库如npm、PyPI和RubyGems等注入带有恶意代码的软件包。这些软件包在用户下载后安装时会触发恶意行为。

为什么防止供应链攻击：<http://blog.itpub.net/70000012/viewspace-2846177>

一些现有的工具（Some Software Composition Analysis tools）：

通过在Bing上进行检索，然后在github上检索得到的部分结果，发现现阶段工具已经挺丰富的了，也有一些软件是开源的，下面是一些软件：

1. 鸿渐SCA-代码成分分析及同源漏洞检测工具 V1.0.0
   1. 介绍文章：<https://zhuanlan.zhihu.com/p/383010781>
   2. 主要功能：软件成分分析、自主研发率分析、同源漏洞分析
2. openSCA:
   1. 仓库所在地：<https://github.com/XmirrorSecurity/OpenSCA-cli>
   2. 官网：<https://opensca.xmirror.cn/docs/v1/#>
   3. 软件实现的语言：Go语言
3. Dependency-Check：
   1. 仓库所在地：<https://github.com/jeremylong/DependencyCheck>
   2. 官网：<https://jeremylong.github.io/DependencyCheck/general/internals.html>
   3. 主要实现的方式：检测项目依赖项中包含的公开披露的漏洞。它通过确定给定依赖项是否存在通用平台枚举 (CPE) 标识符来做到这一点。如果找到，它将生成链接到相关CVE条目的报告。工作原理的链接：

<https://jeremylong.github.io/DependencyCheck/general/internals.html>

* 1. 最近还一直有人在提交commit

Deepcode的使用