开源软件供应链重大基础设施在开源生态“投毒”检测中获进展

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/18837.html

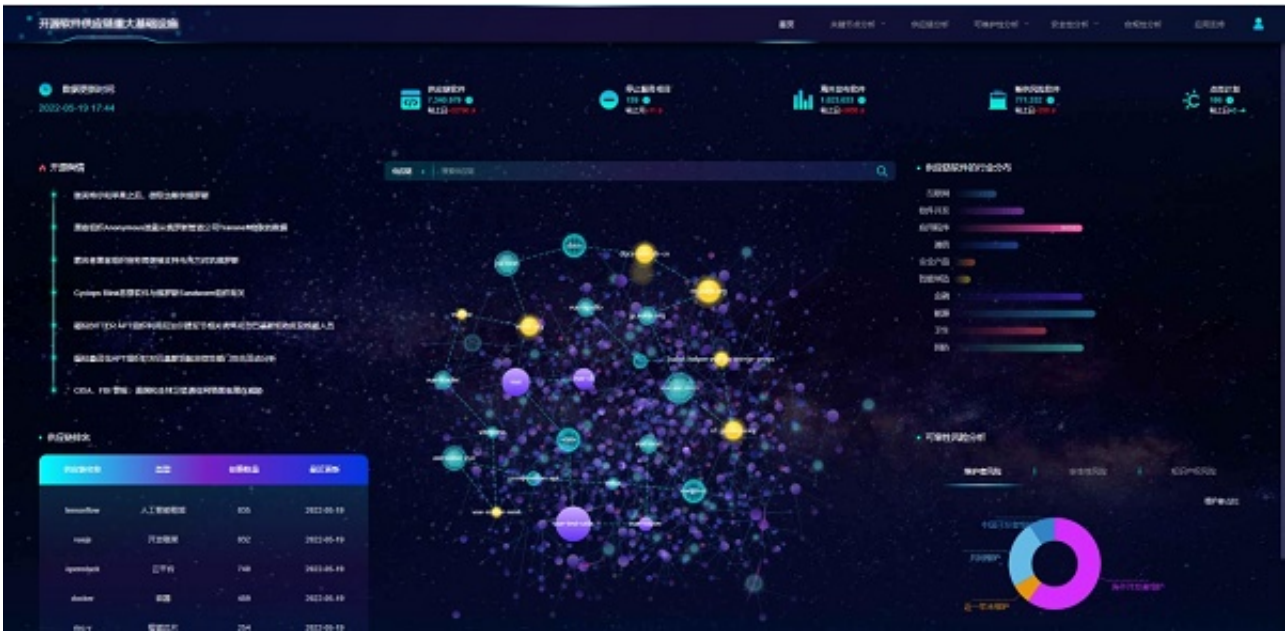
开源生态“投毒”攻击是指攻击者利用软件供应商与最终用户之间的信任关系，在合法软件的开发、传播和升级过程中进行劫持或篡改，从而达到非法目的的攻击类型。许多开源软件存储库在设计时强调方便快捷，忽略恶意代码检测机制，导致开源生态“投毒”攻击现象愈加严重。

近日，中国科学院软件研究所智能软件研究中心团队基于开源软件供应链重大基础设施，实现了面向全网针对开源生态“投毒”攻击现象的持续监测，在开源软件存储库进行恶意扩展包检测中，发现Python官方扩展包仓库被恶意上传了8个恶意包及707个被“投毒”成功的开源项目。

对于Python恶意包的检测，科研团队使用开源软件供应链重大基础设施的恶意包分析工具进行检测，现已检测出Python官方扩展包仓库上传了8个恶意包，其中包含恶意代码，存在巨大的安全隐患，包括窃取隐私信息、数字货币密钥、种植持久化后门、远程控制等一系列攻击活动。研究团队将在Python平台发现的8个恶意包上报给PyPI官方，并收到PyPI官方感谢信。

对于第三方插入的代码执行后门的扩展包的检测，研究通过开源软件供应链重大基础设施的供应链分析模块进行检测。检测发现707个被“投毒”成功的开源项目，其中85个发布在Python官方扩展包仓库，622个发布在公共代码托管平台（Github、GitLab）。同时，该团队正将707个被“投毒”成功的开源项目反馈给国家信息安全漏洞共享平台（CNVD）与国家信息安全漏洞库（CNNVD）等安全漏洞管理机构，其中17漏洞现已获得正式编号。

为应对开源生态存在的风险，软件所于2021年联合中科南京软件技术研究院启动开源软件供应链重大基础设施，建设国内首个集开源软件采集存储、开发测试、集成发布、运维升级等一体化设施，旨在打造全球最大的开源代码知识图谱和开源软件供应链体系，以保障我国开源软件供给安全和产业创新发展，其功能主要包括开源软件供应链关键节点分析、开源软件供应链可靠构建、开源软件可维护性分析、开源软件及其供应链安全分析及开源软件合规性分析等。开源软件供应链重大基础设施将推进开源软件及其供应链的自主可控与安全可靠，逐步形成维护与指导开源生态健康发展的能力，有效支撑国内各行业与开源应用场景。

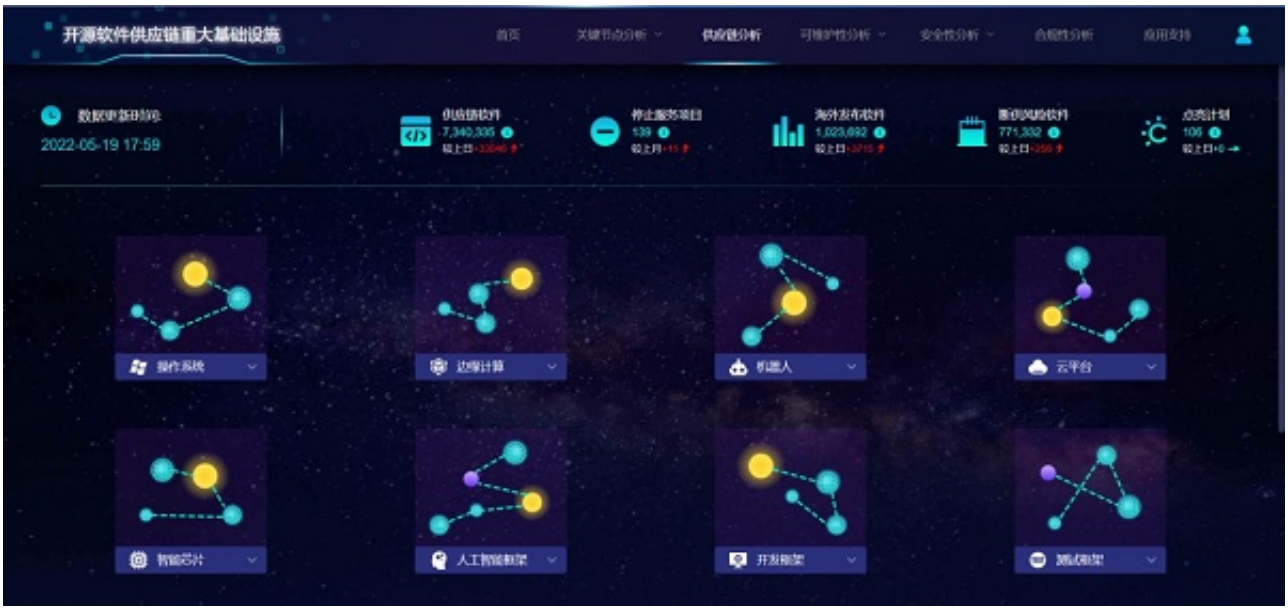


开源软件供应链重大基础设施界面图

恶意包分析工具

名称	版本	管理者	位置	描述
csitools	999.9.0	serb-akamai	setup.py	窃取用户信息
dbattery-python-api	999.9.0	serb-akamai	setup.py	窃取用户信息
eaa-commons	999.9.0	serb-akamai	setup.py	窃取用户信息
yow_utils	999.9.0	serb-akamai	setup.py	窃取用户信息
portal-api	999.9.0	serb-akamai	setup.py	窃取用户信息
Backdoorxrat	0.0.1、0.0.2	KanekiX	BackdoorXRat/BackdoorXRat.py	安装后门
gethttpanand	0.0.1	ananddanana	pythonlibtest/__init__.py	窃取用户信息
pythonlibtest	0.0.3	ananddanana	pythonlibtest/__init__.py	窃取用户信息

已检测到的PyPI中8个恶意包



供应链分析平台

研究团队单位：软件研究所

更多 科学进展 请访问 https://www.iikx.com/news/progress/