墨菲安全
MURPHYSEC

以开发者为核心
企业级软件供应链安全云平台

2023.05

关于墨菲安全

墨菲安全 MURPHYSEC

专注

- ✓ 专注软件供应链安全领域
- ✓ 供应链安全闭环解决方案

专业

- ✓ 超过十年企业安全建设经验
- ✓ 百度、华为、乌云核心团队

可靠

- ✓ 数十家头部行业客户的信赖
- ✓ 数百个顶级开源项目的认可

典型客户及合作伙伴

中国人民银行 THE PEOPLE'S BANK OF CHINA

CAICT 中国信通院

蚂蚁集团 ANT GROUP

快手

中国平安 PING AN 保险·银行·投资

美团

apache/rocketmq
18365 10311
OSCS白帽子为项目修复了 1 个安全风险
平均处理时长 19.4 h

中国银行 BANK OF CHINA

中国电信 CHINA TELECOM 世界触手可及

天翼云

xiaomi

Transfar 传化物流

小红书

pingcap/tidb
32818 5325
OSCS白帽子为项目修复了 1 个安全风险
平均处理时长 14.3 h

核心团队

章华鹏，创始人&CEO

前百度安全架构师，乌云产品合伙人，超十年企业安全经验，漏洞攻防专家

欧阳强斌，联合创始人&实验室负责人

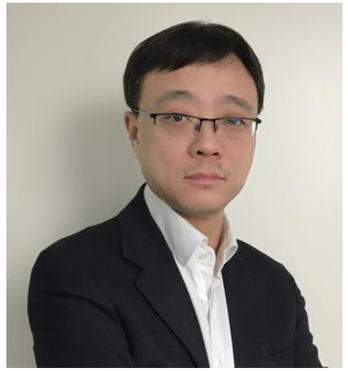
前百度安全蓝军团队负责人，贝壳找房基础安全负责人，丰富的安全攻防经验

宇佰超，联合创始人&研发负责人

超十年的安全产品研发经验，前华为多个产品研发负责人

崔泷跃，联合创始人&解决方案架构师

前平安DevSecOps负责人，百度资深安全工程师，拥有丰富的DevSecOps建设经验



周欣，合伙人&COO

前梆梆安全COO，营销中心负责人，多年信息安全行业市场营销经验

车志远，联合创始人&产品负责人

前百度高级安全工程师，贝壳找房资深安全产品经理，拥有丰富的安全产品经验

和墨菲安全的创始人交流

墨菲安全
MURPHYSEC

墨菲未来
zhanghuapeng@murphysec.com

章华鹏

- 墨菲安全创始人&CEO
- 曾用ID:booooooom、goderci
- 前百度安全架构师、乌云合伙人、贝壳集团平台安全负责人
- 长期活跃在安全社区，乌云核心白帽子为国内外的知名安全企业报告数百个严重安全漏洞

墨菲未来
ouyangqiangbin@murphysec.com

欧阳强斌

- 墨菲安全联合创始人&实验室负责人
- 前百度安全攻防专家、贝壳基础安全&攻防负责人
- 曾负责百度蓝军攻防团队，对web、IoT、智能汽车、二进制等都有丰富的安全攻防经验

墨菲安全

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

软件供应链风险已成为企业面临的严重安全威胁

墨菲安全 MURPHYSEC

漏洞攻击 | 产权合规 | 供应中断

供应链软件

开源组件

闭源商业

开源软件

软件分发渠道

亚马逊 aws | android

GitHub | Apache Maven

tuna 清华大学开源软件镜像站

私有源

JFrog | nexus repository

代码开发

IJ | VS Code

代码仓库

GitLab | SVN

编译构建

Jenkins | GitLab

制品及镜像

Harbor | JFrog

部署运行

Linux | Windows | macOS

商采系统

ERP | OA

办公环境

针对软件供应链的三大主要威胁

墨菲安全 MURPHYSEC

开源技术应用、国际紧张对抗、软件供应链的多样化，使得针对供应链各个环节的攻击急剧上升

产权合规

- 开源许可证合规
- 未授权知识产权

漏洞攻击

- 0day漏洞
- 软件投毒
- 软件劫持
- 数据泄露
- 配置缺陷

供应中断

- 停止维护
- 被攻击破坏

合规处罚
声誉损失
业务中断
数据泄露

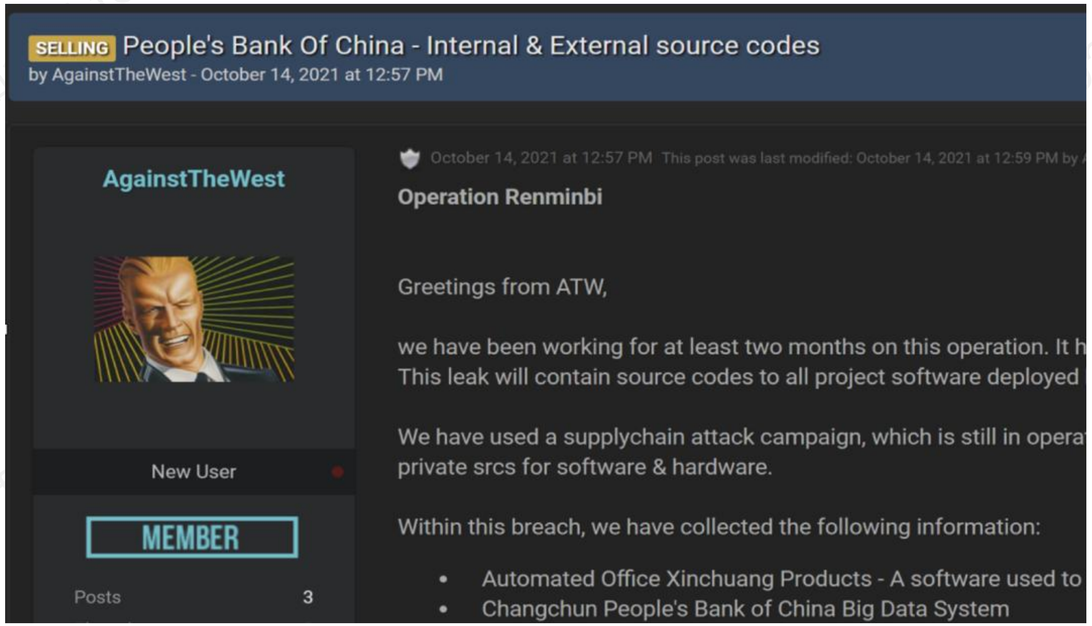
开源及商业外采软件供应链安全事件

墨菲安全 MURPHYSEC

2021年12月，Log4j2曝出严重漏洞，可直接获取服务器权限，影响范围极广，大量企业抱怨修复困难

17W *受到log4j漏洞影响组件数 **13.3%** *受log4j漏洞影响项目数

2021年10月，国外某黑客团队声称通过使用软件供应链攻击手段，窃取到了 中国**银行 内部多个系统的源代码和数据



软件供应链 知识产权风险事件

墨菲安全 MURPHYSEC

2021年6月，国内首例由于违反GPL版权纠纷案裁判文书公示，标志着我国法律对开源许可证的认可

2021年12月，TikTok被曝出违法开源许可证协议，引发社区大量讨论和质疑，TT内部P0级事故

国家高度重视软件供应链安全，行业监管趋严

墨菲安全 MURPHYSEC

随着供应链各个环节的攻击次数急剧上升，危害急剧加大，国家对软件供应链安全的治理力度也在不断增强。

- 2020年11月：国家发布十四五规划建议，8次提到供应链安全
- 2021年9月：《专家解读丨落实关键信息基础设施安全保护制度，加快推进关键信息基础设施供应链安全》《关键信息基础设施安全保护条例》《网络产品安全漏洞管理规定》
- 2021年10月：《关于规范金融业开源技术应用与发展的意见》
- 2022年9月：《信息安全技术 软件供应链安全要求》国标征求意见稿发布

中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅关于规范金融业开源技术应用与发展的意见

标题： 中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅关于规范金融业开源技术应用与发展的意见

索引号： HB/2021-4364505　**文号：** 银办发〔2021〕146号

发文机关： 中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅　**公文种类：**

发布日期： 2021年10月20日

生效日期：

主题词： 金融业开源技术

2021年银保监会发布关于软件供应链安全风险提示的函

中国银行保险监督管理委员会统信部

内部　银保监统信函〔2021〕371号

关于供应链安全风险提示的函

各银保监局，各政策性银行、大型银行、股份制银行、外资

2022年国家大型攻防演练中，软件供应链安全的攻击重点加分

供应链安全得分点

攻击队从防守方供应链（的系统）获取到参演单位的重要数据（个人信息、生产数据、重要文件、源代码、敏感系统管理信息等），**可获得 200-500 分不等的加分。**

墨菲安全

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

企业面临的四大安全威胁场景

墨菲安全
MURPHYSEC

01

开源组件安全漏洞

随着开源技术的发展，开源漏洞的危害和影响力在持续上升，2021年81%的代码存在开源安全漏洞

02

商业外采软件风险

在软件协作和交付的体系下，安全是一个整体，安全不仅取决于自身安全，也依赖上游企业的安全性。

03

开源组件许可证合规

全球范围内的开源许可协议已达上百种。2020年，63%的代码库存在许可证冲突

04

供应链投毒攻击

软件供应链在分发的过程中非常容易出现被篡改投毒的情况，因为上游的投毒导致下游的企业&单位受到严重影响

企业软件供应链安全治理过程中三大难点

墨菲安全 MURPHYSEC

行业缺乏成熟治理体系

- 软件供应链安全问题强依赖开发者参与，传统产品面向开发者不友好
- 行业缺乏成熟治理体系
- 国家监管趋严

供应链资产依赖庞杂

- 开源组件依赖血缘复杂，成分分析的准召率差
- 商业软件SBOM不可见
- 软件供应链资产缺乏统一管理

治理落地难

- 外部软件供应链组件准入准出管理及选型难
- 开发者处置漏洞难，兼容性评估及修复成本高
- 突发0day漏洞及投毒事件响应难

墨菲安全

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

企业软件供应链安全治理场景全景图

墨菲安全 MURPHYSEC

供应链软件

开源组件 LOG4J Spring MVC

闭源商业 ORACLE cisco

开源软件 hadoop NGINX

专业漏洞知识库

专业组件知识库

软件分发渠道

亚马逊 aws android

GitHub Apache Maven

tuna 清华大学开源软件镜像站

0day漏洞及投毒应急预警

私有源安全网关

开源组件选型准入

部署运行

二进制软件成分分析

制品及镜像 Harbor JFrog

软件成分分析

编译构建

自研系统开发流程

私有源 JFrog nexus repository

代码开发 IJ

代码仓库 SVN

供应链资产管理

许可证代码合规管理

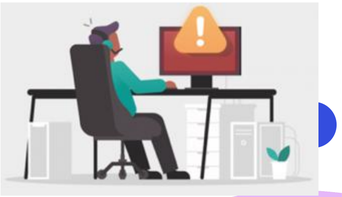
软件成分分析

自主可控代码合规

商采系统 ERP OA

二进制软件成分分析

办公环境



二进制软件成分分析

0day漏洞及投毒应急预警

企业软件供应链安全治理框架

墨菲安全 MURPHYSEC

管理体系

- 制度
- 流程
- 规范

控制体系

软件供应链主要管控对象
- 开源组件
- 开源软件
- 闭源软件

三大风险
- 漏洞攻击
- 中断供应
- 产权合规

事前 准入预防
- 开源选型
- 资产台账
- 安全基线
- 准入准出
- 私有源拦截
- 商采准入

事中 持续管理
- 成分分析
- 二进制检测
- 漏洞检测
- 镜像扫描
- 许可证识别
- 漏洞修复
- 代码溯源
- 自查整改

事后 应急处置
- 漏洞情报
- 投毒情报
- 应急止损
- 威胁溯源

产品能力

源安全网关
- 准入评估
- 私有源管理

软件成分分析
- SBOM清单
- 漏洞检测
- 快速修复

静态代码扫描
- 漏洞检测
- 规则自定义

代码合规管理
- 开源许可证管理
- 代码溯源分析

容器镜像检测
- 容器环境安全检测
- 容器内应用安全检测

漏洞&投毒情报
- 0day漏洞情报
- 投毒漏洞情报

软件供应链安全管理平台

核心技术

- 专业漏洞知识库
- 专业组件知识库
- 检测引擎

墨菲安全

面向开发者打造 企业级软件供应链安全云平台

墨菲安全 MURPHYSEC

用户

- 研发工程师
- 安全工程师
- DevOps工程师
- 运维工程师
- 法务
- 工程管理人员

软件供应链安全云平台

用户功能

- 商采软件审查
- 开源漏洞检测
- 漏洞快速修复
- 二进制成分分析
- 供应链资产台账
- 应急指南
- 0day/投毒预警
- 风险组件拦截
- 开源组件选型推荐
- 组件安全基线
- 自主可控率评估
- 许可证合规管理
- 二进制成分分析
- 云平台门户
- 漏洞真实影响分析
- 代码安全漏洞

产品能力

- 软件成分分析
- 资产及应急预警
- 源安全网关
- 代码合规管理
- 静态代码扫描

- 专业漏洞知识库
- 专业组件知识库
- 分析引擎

关联能力

- 账号体系
- CMDB
- HIDS
- DevSecOps
- DevOps

自研软件开发流程

私有源 → 代码开发 → 编译构建 → 制品仓库 → 上线部署

商采软件

测试 → 采购 → 部署

办公软件

下载 → 安装

云平台产品架构：实施及运营成本低，易扩展

墨菲安全 MURPHYSEC

资产台账、风险管理、应急预警中心

① 风险量化管理
② 供应链资产图谱

① 低成本集成
② 无缝衔接全开发流程

源代码二进制固件

文件类型

检测及修复工具

检测&修复

组件引入 → 代码开发 → 代码库 → 构建/部署

客户端

检测结果

调用

检测结果

调用

动态成分分析

① 动态沙箱分析
② 投毒分析

软件样本库

特征库

漏洞知识库

① 漏洞覆盖全、准、快
② 明确漏洞真实影响
③ 各版本升级兼容性评估
④ 明确是否线上真实调用
⑤ 代码缺陷点及利用条件
⑥ 许可证合规风险信息

专有漏洞知识

漏洞投毒情报

组件可信库

服务端

交付能力

后端能力

客户开发流程

墨菲安全六大产品特性

墨菲安全
MURPHYSEC

10分钟远程快速部署

专业领先的漏洞知识库
(全准快精)

源码/二进制/制品/app检测

支持开发阶段一键修复

升级修复兼容性评估

线上漏洞触发分析

产品一：软件成分分析

墨菲安全 MURPHYSEC

SBOM分析

- 支持源代码及二进制
- 支持代码片段级分析
- 线上真实依赖识别，高准
- 一键接入IDE等十数种开发流程工具

风险检测

- 支持漏洞及投毒检测
- 支持许可证识别
- 漏洞线上是否会被攻击
- 独家专业漏洞知识库

快速修复

- 组件升级兼容性评估
- 编码阶段漏洞一键修复
- 支持多种处置方案
- 组件负责人自动关联

产品二：资产管理及0day漏洞预警

墨菲安全 MURPHYSEC

资产台账

- SBOM导入
- 系统及三方资产导入
- 负责人标签
- 资产风险等级标签
- 资产指纹识别

情报预警

- 公开0day分析及预警
- 独家0day漏洞分析预警
- 组件投毒情报分析及预警

应急处置

- 自动关联受影响资产
- 自动化预警配置
- 临时缓解处置方案
- 专业的漏洞应急指南

产品三：源安全网关

墨菲安全 MURPHYSEC

网关插件

- 插件式一键安装
- 支持jfrog及nexus

JFrog

nexus repository

策略配置

- 组件安全基线配置
- 黑白名单配置
- 支持观察模式及阻断模式
- 支持动态检测配置阻断

风险阻断

- 高危组件拦截下载
- 高风险许可证拦截使用
- 高危0day漏洞拦截止损
- 投毒组件屏蔽隔离

产品四：代码合规管理

墨菲安全
MURPHYSEC

成分分析

- 源代码组件成分分析
- 二进制成分分析
- 代码片段成分分析

合规策略

- 开源许可证合规策略
- 代码自主可控率策略
- 自主知识产权策略

报告&整改

- 合规检测报告
- 风险整改建议
- 实时风险提醒

平台及产品部署方式

墨菲安全
MURPHYSEC

软件部署

docker

可十分钟远程快速部署，极简！

硬件部署

即插即用，方便快捷

墨菲安全

目录

墨菲安全
MURPHYSEC

专业、专注、可靠

获取详细技术白皮书和资料

墨菲安全
MURPHYSEC

包含内容：

- ✓ 金融、互联网、运营商及国央企等行业最佳实践案例
- ✓ 墨菲安全软件供应链产品技术详细介绍
- ✓ 软件供应链安全国内外技术标准及技术文章
- ✓ 软件供应链安全国内外法律法规及标准
- ✓ 软件供应链安全事件合集

获取方式：

扫码在线申请

联系运营同学获取

电话获取：400 180 9568

公司联系方式

墨菲安全
MURPHYSEC

公司地址：

北京市海淀区上地十街1号院6号楼3层318B

联系人：

齐女士

联系电话：

400 180 9568