浙江省科学技术奖公示信息表（单位提名）

提名奖项：技术发明奖

|  |  |
| --- | --- |
| 成果名称 | 高级持续性攻击（APT）检测与溯源关键技术及应用 |
| 提名等级 | 一等奖 |
| 提名书  相关内容 | 详见附件 |
| 主要完成人 | 陈铁明，排名1，教授，浙江工业大学  纪守领，排名2，教授，浙江大学  路晓明，排名3，高工，中移（杭州）信息技术有限公司  朱添田，排名4，副教授，浙江工业大学  吕明琪，排名5，副教授，浙江工业大学  鲁银冰，排名6，副高，中移（杭州）信息技术有限公司 |
| 主要完成单位 | 1.单位名称：浙江工业大学  2.单位名称：浙江大学  3.单位名称：中移（杭州）信息技术有限公司 |
| 提名单位 | 浙江省教育厅 |
| 提名意见 | 项目针对高级持续性攻击（APT）检测与溯源面临的攻击行为数据审计不全面、攻击过程知识刻画不完备、攻击路径溯源分析不精准等关键技术挑战，通过承担国家基金重点项目、工信部创新发展工程等，取得以下研究成果：1、提出APT全量攻击日志数据采集与管理方法，实现对云网边端多层域安全日志数据的高效采集、压缩、存储与建模，研制跨层域安全日志数据采集系统KELLECT。2、提出APT全貌攻击行为知识抽取与表征方法，实现对多源异构威胁情报的汇聚、抽取、表征与增强，建立支持攻击检测与路径推理的大型攻防知识库。3、提出APT全链攻击路径要素追踪与溯源方法，实现在小样本条件下的异常渗透点定位和攻击技战术识别，以及在高噪声环境下的攻击路径推理与溯源。成果覆盖APT智能检测与溯源的各个重要技术环节，通过最新国际标准数据集测试，性能领先，总体技术达到国际先进水平，其中APT技战术小样本检测和多时空关联的威胁全路径追溯方面达到国际领先。项目授权国家发明专利41项，发表安全领域国际顶会顶刊论文38篇，出版专著4部。研制多款APT攻击智能检测与分析产品，在电力能源、移动通信、银行金融等行业进行规模应用，服务78家大型工业企业，38个关键信息基础设施，以及2000多家中小企业，服务中国移动2.3亿家庭宽带用户。近三年累计产生经济效益超24亿元，产品首次检测国家级APT攻击10次，追踪覆盖超100个境外APT组织，为三峡大坝控制系统、中国移动网络平台、杭州G20峰会、世界互联网大会、北京冬奥会、杭州亚运会等提供最高等级安保服务，受到国家重要部委单位的肯定和表彰。  提名该成果为省技术发明奖一等奖。 |

附件： 主要知识产权和标准规范目录（不超过10件）

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 知识产权  （标准规范）类别 | 知识产权（标准规范）具体名称 | 国家  （地区） | 授权号  （标准规范编号） | 授权（标准发布）日期 | 证书编号（标准规范批准发布部门） | 权利人（标准规范起草单位） | 发明人（标准规范起草人） | 发明专利（标准规范）有效状态 |
| 授权发明专利 | 一种基于起源图的日志采集、压缩、存储方法 | 中国 | ZL202211517274.9 | [2023-04-07](https://www.uyanip.com/result?exp=GKN:(2023)) | 证书号第5842425号 | 浙江工业大学 | 陈铁明, 郑陈彬, 朱添田, 吕明琪, 路晓明 | 有效 |
| 授权发明专利 | 一种基于Windows内核的事件日志采集方法及系统 | 中国 | ZL202211061051.6 | 2022-11-25 | 证书号第5604830号 | 浙江工业大学 | 陈铁明, 仇学博, 宋琪杰, 朱添田, 吕明琪, 路晓明 | 有效 |
| 授权发明专利 | 一种面向物联网设备的用户数据深层取证分析方法及系统 | 中国 | ZL202210463280.4 | 2023-08-25 | 证书号第6271045号 | 浙江大学 | 纪守领; 刘沛宇; 付丽嫆; 夏思怡; 张旭鸿; 陈文智; 邓水光; 王文海; | 有效 |
| 授权发明专利 | 一种基于上下文行为分析的APT检测方法 | 中国 | ZL202110909243.7 | 2024-02-27 | 证书号第6742600号 | 浙江工业大学 | 朱添田, 余金开 | 有效 |
| 授权发明专利 | 一种基于图匹配的威胁狩猎方法 | 中国 | ZL202211536047.0 | 2023-03-31 | 证书号第5831121号 | 浙江工业大学 | 朱添田, 李爽, 陈铁明, 吕明琪 | 有效 |
| 授权发明专利 | 基于元路径学习与子图采样的APT网络攻击检测方法 | 中国 | ZL202011319217.0 | 2021-11-23 | 证书号第4812710号 | 浙江工业大学 | 王婷, 董程昱, 吕明琪, 朱添田, 陈铁明, 顾国民, 陈波, 江颉 | 有效 |
| 授权发明专利 | 一种基于因果分析的APT溯源研判方法 | 中国 | ZL202211068267.5 | 2022-11-25 | 证书号第5605688号 | 浙江工业大学 | 朱添田, 张加波, 陈铁明, 吕明琪 | 有效 |
| 授权发明专利 | 一种基于跨主机异常行为识别的复杂网络攻击检测方法 | 中国 | ZL202310423444.5 | 2023-07-25 | 证书号第6173707号 | 浙江工业大学 | 吕明琪, 刘海文, 谢海江, 朱添田, 陈铁明, 路晓明, 姚一杨 | 有效 |
| 授权发明专利 | 一种基于元行为的APT攻击样本增强及检测方法 | 中国 | ZL202210849732.2 | 2024-04-05 | 证书号第6873318号 | 浙江工业大学 | 朱添田, 应杰, 王佳宇, 陈铁明, 吕明琪 | 有效 |
| 授权发明专利 | DNS隐蔽信道检测方法、装置、设备及存储介质 | 中国 | ZL202110884131.0 | 2022-12-27 | 证书号第5665754号 | 中移（杭州）信息技术有限公司, 中国移动通信集团有限公司 | 袁勇，鲁银冰，王悦，陈东，钱湖海，王伟杰 | 有效 |