“数字替身”数据资源防护软件

抵御未知网络攻击、达成危害消解

目标定位

智能化网络渗透攻击已经成为网络攻击的新态势，加剧攻防信息失衡，导致我国重点单位存在大量“检不出”“看不见”的未知网络攻击。现有防御技术过度依赖威胁情报及入侵指标（IOC），难以抵御高水平未知网络攻击，防护关键资源，实现危害消解。

创新理念

“数字替身”的核心是变“本体受害”为“李代桃僵”，由“替身”无感代替“本体”承受攻击，在业务系统中建立链式诱导防御机制，改变“敌暗我明”的信息不对称攻防格局，为重点单位抵御未知APT攻击、勒索攻击提供全新的解决方案[1]。

优势技术

“数字替身”数据资源防护系统包括客户端和服务端两部分，客户端在真实业务系统中对关键数据资源建立最小防护面，突破API无感劫持与重定向等关键技术，发现可疑行为，提取未知样本；服务端全面存证客户端替身日志与样本，开展智能化威胁研判。

API无感劫持与重定向

对访问文件的API进行劫持、验证，放行正常访问行为，重定向可疑行为，首次在日常办公环境中实现“本”“替”同体的诱导防御机制

运行态多因子 “零信任”身份验证

建立进程链签名验证、用户行为感知等多层验证机制，快速识别并发现可疑进程的异常访问行为，实现“人在回路”可信身份验证

多级隐蔽存证与线索发现

部署多级隐蔽探针，全面存证可疑进程访问日志及样本，开展基于智能体的威胁研判，发现未知木马和高价值IOC

多模态高拟真替身与认知对抗

研制“替身智能体”自动提取多模态数据资源“密点”，生成高仿不真替身文件，诱导攻击者窃取并观测其行为，达到认知欺骗对抗效果

部署应用

- 系统支持Windows、Linux等操作系统，提供灵活的安装向导与用户配置。系统已经通过1200余项企业级集成测试，完成在头部安全企业产品线的集成和应用验证。
- 系统具备独立部署能力，已在电力、金融、重点高校等单位规模化部署，发现并实证多起重大事件，来函评价“率先形成我国体系化、可落地、具备实战操作性的未知网络攻击危害消解方案”“为核心产品提供技术代差优势”。
- 申请试用详情可访问： https://digitalscapegoat.cn。

1. Digital Scapegoat: An Incentive Deception Model for Resisting Unknown APT Stealing Attacks on Critical Data Resource," in IEEE Transactions on Information Forensics and Security, vol. 20, pp. 10699-10714, 2025