中关村实验室
ZGC LAB

“数字替身”防护软件
中关村实验室APT团队

“数字替身”数据资源防护软件

抵御未知APT攻击、达成危害消解

目标定位

APT（高级持续威胁）已成为境外黑客组织攻击我国重点单位和领域的主要技术手段。高水平APT攻击手法和武器不断演进，存在大量“检不出”、“看不见”的未知APT攻击，现有APT终端防御技术依赖已知情报及线索，难以抵御高水平未知APT攻击。

创新理念

“数字替身”理论模型的核心是变“本体受害”为“李代桃僵”，由“替身”无感代替“本体”承受攻击，通过建立链式诱导防御机制，变“未知”为“已知”，改变“敌暗我明”的信息不对称攻防格局，指导建立抵御未知APT攻击全新解决方案[1]。

优势技术

“数字替身”数据资源防护软件包括客户端和服务端两部分，客户端围绕关键数据资源建立最小防护面，通过关键API无感劫持与重定向等技术，发现可疑行为，提取未知样本，诱导攻击者；服务端全面存证客户端日志与样本，开展关联分析与智能威胁研判。

关键API无感劫持与重定向

对文件访问关键API进行劫持、验证，放行正常访问行为，重定向可疑行为。首次在日常办公系统中实现“本”“替”同体的诱导观测

运行态多因子 “零信任”身份验证

建立进程链验签、事件强关联、无感人脸识别、智慧钥匙等多层身份验证机制，并无感融入到运行态关键资源访问过程中，快速识别并发现可疑进程与异常访问行为

多级隐蔽存证与线索发现

部署事件、进程、API、网络等多级探针，全面存证未通过验证的访问行为日志及相关样本，及时发现未知木马和高价值IOC

多模态高拟真替身与认知对抗

通过AI大模型提取不同模态数据资源“密点”，并自动生成脱敏的高仿替身文件，诱导真实攻击者窃取替身文件，达到认知欺骗的对抗效果

部署应用

- 系统支持Windows、Linux等操作系统，提供精简的安装向导与灵活的用户配置。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、金融等重点单位、重点高校规模化部署，发现并实证多起重大窃密事件，获来函评价“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、方案详情： 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