基于主动欺骗的反勒索软件方法

陈凯[1,2]，马多贺[1,2]，唐志敏[1,2]，DAI Jun[3]
（1.中国科学院信息工程研究所，北京 100095；2.中国科学院大学网络空间安全学院，北京 100095；
3.伍斯特理工学院计算机科学系，伍斯特 01609）

摘 要：考虑到勒索软件对数据安全构成的严重威胁及其攻击手段的日益智能化和复杂化，针对传统防御方法的局限性，提出了一种基于主动欺骗的反勒索软件方法。结合静态启发式算法和动态启发式算法对欺骗文件进行动态部署，在此基础上建立了基于主动欺骗的动态文件安全模型。针对不同风险级别的勒索软件，采用不同的策略生成动态欺骗文件，通过模拟真实数据的特征来迷惑勒索软件，使其无法区分真实数据和欺骗数据，从而保护用户的真实数据不被加密或破坏。实验结果表明，所提方法有效增加了文件的动态性、多样性和欺骗性，大幅扩展了数据攻击面的转换空间，能够有效地抵御勒索软件攻击。

关键词：主动欺骗；反勒索软件；数据攻击面；数据欺骗
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024120

Anti-ransomware method based on active deception

CHEN Kai, MA Duohe, TANG Zhimin, DAI Jun
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100095, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100095, China
3. Department of Computer Science, Worcester Polytechnic Institute, Worcester 01609, USA

Abstract: Considering the serious threat that ransomware poses to data security and the increasing intelligence and complexity of its attack methods, an anti-ransomware method based on active deception was proposed to address the limitations of traditional defense methods. By combining static heuristic algorithms and dynamic heuristic algorithms to dynamically deploy deceptive files, a dynamic file security model based on active deception was established. Different strategies were employed to generate dynamic deceptive files for ransomware of different risk levels, confusing ransomware by simulating the characteristics of real data, making it unable to distinguish between real and deceptive data, thus protecting users' real data from encryption or destruction. Experimental results show that the proposed method effectively increases the dynamism, diversity, and deceptiveness of files, significantly expanding the shifting space of data attack surfaces and effectively defending against ransomware attacks.

Keywords: active deception, anti-ransomware, data attack surface, data deception

0 引言

随着互联网技术的迅猛发展、数据资产价值的不断提升以及数字货币市场的持续繁荣，勒索软件攻击呈现愈发严重和频繁的态势。如今，勒索软件已成为全球网络安全领域的主要威胁，各国的数据资产不同程度地受到勒索软件攻击的困扰[1]。令人

收稿日期：2023–12–12；修回日期：2024–05–31
通信作者：马多贺，maduohe@iie.ac.cn
基金项目：中国通信标准化协会“电信网和互联网勒索软件防范技术要求”标准基金资助项目（No.2023-0722T-YD）
Foundation Item：China Communications Standards Association's Standard Project Funding for "Technical Requirements for Ransomware Prevention in Telecom Networks and Internet" (No.2023-0722T-YD)

担忧的是，2022 年，全球范围内遭受勒索软件的攻击高达 3 583 万次，与去年相比增加了 1 300 多万次[2]。勒索软件的数量和攻击频率的急剧增加，给经济发展、国家安全和社会稳定带来了严重的威胁。各国纷纷颁布一系列法律法规，并在国际上加强合作，以加大对该类犯罪的打击力度。

勒索软件，也称勒索病毒，是一种通过加密文件、锁定系统或破坏基础设施来控制用户资源的恶意软件。它要求受害者支付赎金以恢复数据访问或系统功能，否则就引发数据丢失、服务中断和信息泄露等严重安全风险。目前，许多数据安全研究都围绕系统和网络方面进行威胁检测和攻击阻断，但很少触及数据本身[3]。以加密为中心的数据安全解决方案限制了数据的可用性，这一限制使得数据加密技术在大规模应用上存在一定困难[4]。现有数据安全解决方案的弊端可以归纳为以下 2 个方面。首先，未知的威胁（如零日漏洞、勒索软件）和持续的威胁（如分布式拒绝服务攻击、高级持续性威胁攻击）使防御者处于被动地位。其次，确定性的数据内容、静态的数据结构和单一的数据访问方式为网络攻击提供了更大的攻击面。鉴于勒索软件加密后的数据难以破解，传统的被动防御策略如恶意软件检测和数据恢复已不足以应对，亟须主动防御策略。

采取积极主动的弹性防御策略，能够在攻击行为对系统造成不利影响之前，通过部署精准预警、及时阻断和充分修复等措施，降低甚至消除网络安全威胁。主动防御的优势在于它能够在攻击发生之前采取预防措施和应对潜在的网络风险，从而减少安全事故的发生。图 1 展示了针对勒索软件的主动防御和被动防御技术的对比，利用全面的威胁情报分析方法、有效的安全管理和监控机制，确保目标系统的安全性和可靠性。

作为主动防御的排头兵，移动目标防御（MTD, moving target defense）通过动态转换攻击面的方式将被动防御变为主动防御[5]。数据 MTD 根据防御需求动态地改变数据的形式、编码和排列，将 MTD 应用于数据安全可以有效降低数据的相似性、确定性和静态性，提高数据系统的内生安全性；动态数据极大地增加了攻击者获取和使用数据的难度和成本。

数据欺骗防御是另一种主动的防御手段，通过误导和混淆信息提升数据安全，有效干扰攻击者行动。该方法涵盖蜜罐、诱饵等工具，以低成本、易部署的特点开辟了勒索软件防御的新路径，通过预先部署诱饵，实现勒索攻击的早期识别和预警。文献[6-8]使用诱饵数据来阻碍攻击者窃取身份信息。诱饵文件也经常被用来防止勒索软件攻击。Salem 等[9]研究了应用于检测伪装攻击的诱饵文件。Voris 等[10]专注于自动分发诱饵以增加检测组织内部人员犯罪的机会。Kapravelos 等[11]使用蜂蜜页面来诱导恶意行为。然而，现有技术的攻击面转换频率较低，导致数据暴露周期延长，数据缺乏充分的动态性，这给攻击者提供了充足的机会来访问和操纵数据。此外，攻击面转换也对系统的正常运行造成了一定程度的干扰，并对性能产生了负面影响。

本文主要的研究工作如下。

1) 引入主动欺骗的概念并建立动态文件安全模型，动态生成欺骗文件，最大限度地迷惑攻击者并增加其攻击成本和难度。

2) 对于不同风险级别的勒索软件，采用不同的策略生成动态文件，从文件属性和内容 2 个方面对文件进行变换，增加数据的动态性和不可预测性，防止文件受到勒索软件的损害。

3) 采用启发式算法在文件系统中部署欺骗文件，保证欺骗文件的覆盖度，基于勒索风险判定结果动态增添欺骗文件，进一步提升欺骗效益和诱捕效果。

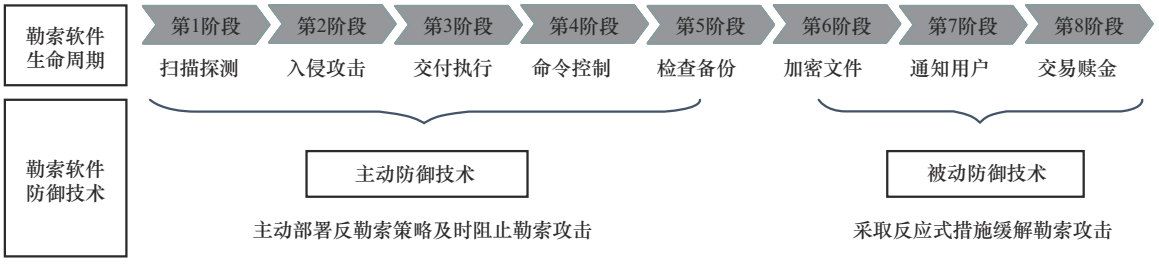


图 1　针对勒索软件的主动防御和被动防御技术的对比

4) 通过实验分析，对所提方法在数据多样性、攻击面转换空间和系统性能等方面的效果进行全面评估。

1 相关工作

应用于数据安全领域的反勒索软件方法主要分为基于数据的勒索阻断方法和基于数据欺骗的勒索防御方法。下面，分别介绍这2种方法的研究进展。

基于数据的勒索阻断方法主要通过访问控制的机制来管理权限，防止未授权访问和篡改，确保系统合法使用。通常用黑名单监控操作行为可以检测勒索软件，但这种方法对未知勒索软件的防护效果有限。文献[12-13]提出在用户应用程序级使用白名单来限制勒索软件对系统资源的访问权限，以抵御勒索软件攻击。基于白名单的访问控制不需要定期更新勒索软件信息，因此能够实时防止已知和未知的勒索软件。然而，如果攻击者使用动态链接库（DLL, dynamic link library）注入方法将恶意代码注入白名单进程的内存空间中，应用程序级白名单解决方案可能对这类勒索软件失效。为应对勒索软件，Lee等[14]引入了基于I/O活动的白名单技术，通过监控I/O活动来保护固态硬盘（SSD, solid state drive）文件。Ami等[15]开发了一种文件访问控制系统，利用生物特征和身份验证防止未授权的文件加密和删除。尽管如此，文件级访问控制可能会影响用户体验，并受限于攻击者通过合法程序的攻击，预防效果有限。

基于数据欺骗的勒索防御方法通过在勒索攻击开始之前部署欺骗诱饵，实现对勒索攻击的识别、分析和预警，进而有效应对此类威胁。Kohlbrenner等[16]提出了一种文件系统视图分离的方法，即把文件系统的视图分成堆叠的多个层级，一部分层级包含诱饵数据，另一部分层级包含实际数据。Mehnaz等[17]通过部署诱饵文件和监控运行进程及文件系统，实时识别勒索软件进程。Feng等[18]提出了一种基于欺骗和行为监控的检测方法，通过拦截和改变函数调用的方式使勒索软件首先访问并操作诱饵文件，以实时检测加密勒索软件。Gómez-Hernández等[19]开发了一个名为R-Locker的工具，该工具在目标环境周围部署一组先进先出格式的蜜文件以捕获勒索软件。Sheen等[20]提出了R-Sentry，使用文件访问模式来识别勒索软件攻击，通过分析不同的勒索软件变种来确定部署诱饵文件的最佳位置，然后在文件系统中分发欺骗文件，任何访问这些文件的进程都将被标记为异常。但是，诱饵方法难以准确识别更改是否由勒索软件执行，而且勒索软件可能在攻击诱饵之前对文件进行全部或部分加密，从而绕过诱饵方法的防御。Wang等[21]提出了KRProtector，这是一个针对物联网设备的检测和用户文件保护系统，该系统使用诱饵来对勒索软件应用欺骗策略，用于保护物联网设备上的用户文件，并且可以在没有Root权限的情况下基于诱饵检测Android加密勒索软件，但不能用于保护系统文件。Li等[22]提出了一种基于博弈论的方法，采取数据加密和数据欺骗的预防性组合来阻止勒索软件攻击，通过减轻勒索软件攻击产生的影响来提高数据的安全性，但这一工作缺少实证研究的支撑。

数据的动态性、多样性和欺骗性对勒索软件防护至关重要。动态性意味着数据结构和访问模式不断变化，使得勒索软件难以找到稳定的攻击目标；多样性意味着系统中存在多种不同类型的数据，使得勒索软件无法通过单一的模式识别真实数据；欺骗性是指通过部署诱饵数据来误导攻击者，使其在攻击过程中浪费资源和时间。这些特性对提高系统的整体安全性具有实际意义，能够有效地抵御勒索软件的攻击。上述研究工作在基于数据的勒索防御领域取得了一定的进展，但当前仍缺乏针对数据本身动态性、多样性和欺骗性的技术研究。基于此，本文提出了一种关于数据本身的创新型动态欺骗文件方法，该方法可以提高数据的动态性、多样性和安全性，同时保证数据的兼容性、完整性和可用性。

2 基于主动欺骗的动态文件模型

基于主动欺骗的动态文件模型针对勒索软件的不同风险等级动态变换文件的属性和内容，如图2所示。该模型的核心策略是基于实时的多维度访问信息动态地转换文件的属性和内容，主要目标是迷惑和抵御攻击者，使其在访问文件时难以获取真实有效的数据，勒索软件通常依赖于识别特定文件类型或结构来执行加密，动态变化使得这一过程变得复杂，从而增加了攻击的难度。该模型主要通过以下2个方面来实现这一目标。

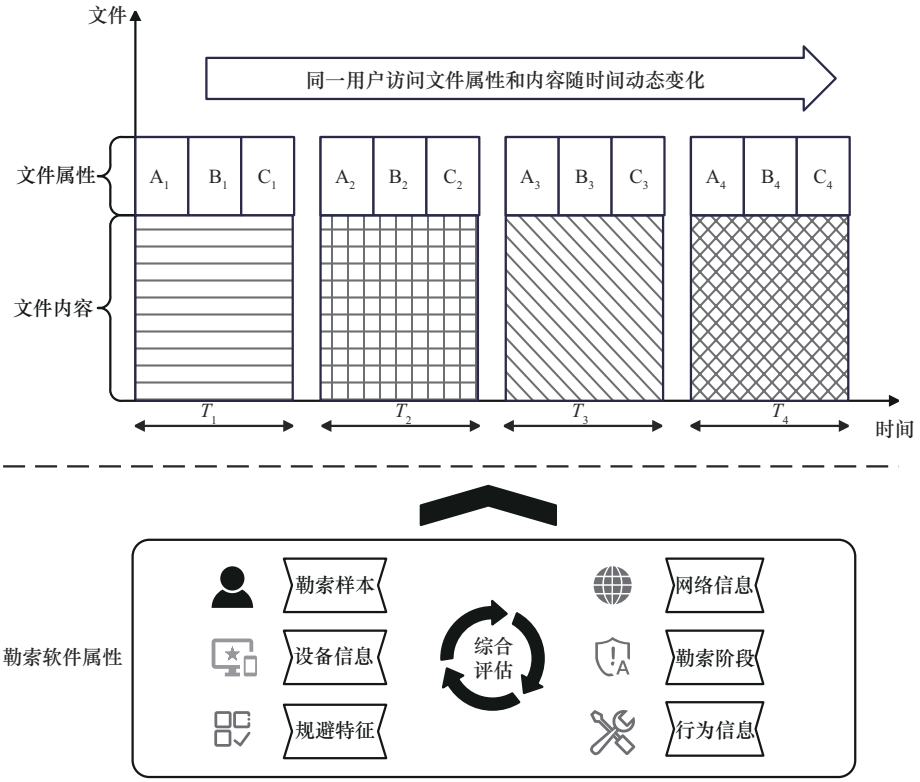


图2　基于主动欺骗的动态文件模型

首先，该模型通过结合变换文件属性和文件内容，显著扩展了攻击面的转换空间。文件属性包含文件各个方面的信息，在定位、挖掘和窃取数据方面至关重要。文件内容则涵盖了攻击者渴望获取的敏感、重要和隐私数据等内容。通过对文件属性和文件内容进行组合变换，扰乱了攻击者的实际视图，从而提高了文件的安全性。在转换过程中，文件属性会被转换成欺骗性信息，例如大小、所有者、权限、修改时间和文件类型等属性可能被更改为欺骗数值。同时，文件本身可能会插入欺骗数据内容或隐藏真实数据内容。即使攻击者察觉到数据可能是假的，也很难从包含随机分布的欺骗数据的视图中辨别出真实数据。

其次，该模型通过在勒索软件访问系统时实时变换文件来增加攻击面的转换频率。将勒索软件的访问信息划分为多个维度进行综合评估，其结果是不断变化的，因此文件也呈现出持续性动态变化的状态。当同一个可疑勒索软件的2次访问请求之间的时间间隔超过一定阈值时，文件也会相应地发生变化。因此，可疑勒索软件无法使用相同的检测、分析或处理方法来处理动态文件。频繁的文件转换使得攻击者的感知和行为路径持续受到干扰，从而使得探测和攻击新的攻击面变得更加困难且成本更高。

3　反勒索软件系统实现

反勒索软件系统通过实现动态数据访问使勒索软件在不同的状态或执行不同的操作时得到不同的数据文件。实现动态数据访问的方法主要有2种：一是根据勒索软件的属性，如攻击特征、访问时间和权限等进行数据访问控制；二是根据勒索软件的行为操作，如预览文件和获取文件等进行数据访问控制。

动态数据可以根据勒索软件的风险等级动态地变换文件的形式、编码和排列，使得每个勒索软件看到的文件内容都不同。对于低风险的勒索软件，文件内容可能与原始文件相似；对于风险等级较高的勒索软件，文件内容会被大幅度扭曲，欺骗信息也会被注入其中，这样会增加攻击者获取和使用数据的难度和成本。此外，针对不同勒索软件生成的虚拟文件大小相差也很大，这样会增加攻击者分析和窃取数据的成本。但是需要注意的是，系统本身会尽量减少对合法的访问产生影响，避免他们看到的文件内容有所失真。因此，在采用动态数据策略

时需要平衡系统整体的安全性和易用性。

反勒索软件系统通过勒索风险识别机制确定是否以及如何动态转换勒索软件访问的文件属性和内容视图。该系统由4个核心组件组成：勒索风险识别、动态文件安全控制器、动态文件生成和动态文件管理，系统架构如图3所示。

3.1 勒索风险识别

勒索风险识别通过计算综合风险度来评估勒索软件访问的风险等级，为制定动态文件的生成策略提供依据。将勒索软件的访问划分为6个属性，包括勒索样本、规避特征、设备信息、网络信息、勒索阶段和行为信息，然后从多个数据源（包括相关日志、网络监控工具、威胁检测系统等）收集风险证据。风险等级评估参数如表1所示。

该模块通过结合静态启发式检测和动态启发式检测的方法来识别勒索软件的风险，可连接到勒索软件的Web服务，定期学习和更新有关勒索软件策略的最新情报。静态部分通过分析正常样本与病毒样本的启发式特征差异，识别勒索软件风险。关键特征包括哈希值、文件头、系统调用、字符串和操作码。同时，考虑勒索软件使用的加密、多态和变形技术，以及历史高风险和未知设备信息，以提高风险识别的准确性。来自已知恶意IP地址的访问可能表明勒索软件正在尝试建立连接，而特定硬件ID或软件版本的出现可能表明勒索软件正在利用已知的漏洞。勒索软件样本的静态检测维度包含勒索样本、规避特征和设备信息。动态部分则主要针对勒索软件的行为特征对勒索软件进行综合分析，达到检测未知勒索软件的目的。勒索软件样本的动态检测维度包含网络信息、勒索阶段和行为信息。

使用因素权重和因素得分评估勒索风险等级，其中，因素包括勒索样本因素、规避特征因素、设备信息因素、网络信息因素、勒索阶段因素和行为信息因素，因素权重表示每个因素对勒索风险等级的影响程度，因素得分表示每个因素的具体评估结果，根据专家的知识和经验来分配因素权重和得分。

具体而言，可以将每个因素的权重和得分表示为向量的形式，则因素权重向量$\boldsymbol{W}_f$和因素得分向量$\boldsymbol{S}_f$分别为

$$\boldsymbol{W}_f=[\boldsymbol{w}_1,\boldsymbol{w}_2,\boldsymbol{w}_3,\cdots,\boldsymbol{w}_6] \tag{1}$$

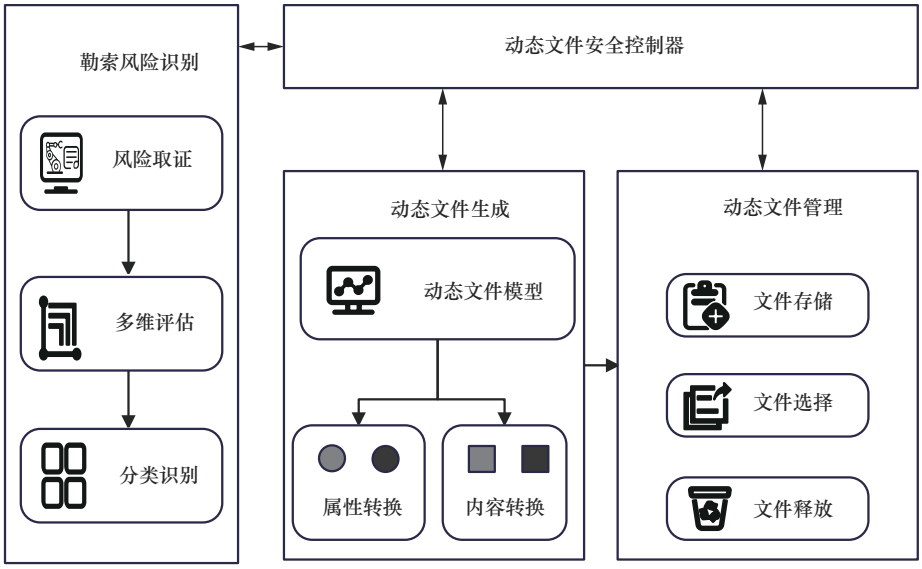


图3 系统架构

表1 风险等级评估参数

勒索样本	规避特征	设备信息	网络信息	勒索阶段	行为信息
样本哈希	加密算法	IP信息	上传带宽	扫描探测	访问时间
样本头信息	多态规则	硬件ID	下载速率	入侵攻击	访问频率
函数/系统调用	变形方法	软件版本	丢包率	命令控制	资源使用率
样本字符串	指令地址	操作系统	响应时间	检查备份	操作习惯
样本操作码	指令类型	平台架构	通信成本	加密文件	位置变化频率

$$\boldsymbol{S}_f = [\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3, \cdots, \boldsymbol{s}_6] \tag{2}$$

其中，$\boldsymbol{w}_i = [w_{i1}, w_{i2}, w_{i3}, w_{i4}, w_{i5}]$，$\sum_{j=1}^{5} w_{ij} = 1$；$\boldsymbol{s}_i = [s_{i1}, s_{i2}, s_{i3}, s_{i4}, s_{i5}]$，$s_{ij} \subset [0,1]$。则评估勒索风险等级的计算式可以表示为

$$R = \sum_{i=1}^{6} \boldsymbol{w}_i \boldsymbol{s}_i^{\mathrm{T}} \tag{3}$$

最后，将风险等级划分为7个不同级别，级别0代表无风险，级别6代表最高级别风险。如果合法的用户访问意外地触发了风险警报，如大量使用文件，用户可以向管理员申请文件访问权限，并使用特定的恢复方法来获得真实数据。而攻击者没有特权，不知道欺骗文件的位置和权限恢复过程。风险等级评估还会根据相关的误报信息不断优化每个指标和权重，以减少误报率。

3.2　动态文件安全控制器

动态文件安全控制器组件负责管理动态文件的生成和转换过程。如算法1所示，当勒索软件访问数据时，控制器组件根据勒索软件的风险级别和访问属性为其分配相应的动态文件，并将结果返回给攻击者。为了保证数据MTD系统的性能和存储空间，控制器组件需要及时释放不再需要的动态文件。当动态文件的访问时间间隔超过一定阈值时，控制器组件将其释放并删除。此外，它还负责管理动态文件的属性和内容，包括伪装策略、伪装程度、伪装内容等。只有经过勒索风险识别且组件评估为合法的访问请求才能够访问原始文件，而可疑访问者只能够访问采取伪装策略进行变换的动态文件。

算法1　动态文件安全控制器控制算法

输入 勒索软件访问的文件F_{ori}的路径

输出 生成的动态文件F_{dyn}

1) 按照式(3)计算勒索软件的风险等级R = getRiskLevel()。

2) 如果$R = 0$：

3) 返回原始文件F_{ori}的数据块索引$\mathrm{Idx}_{\mathrm{ori}}$；

4) 否则查询根据R生成的动态文件F_{dyn}是否存在：

5) 如果动态文件F_{dyn}存在，则返回应的动态文件F_{dyn}；

6) 否则根据R和访问属性P生成相应的动态文件数据块索引$\mathrm{Idx}_{\mathrm{dyn}}$；

7) 根据数据块索引$\mathrm{Idx}_{\mathrm{ori}}$和$\mathrm{Idx}_{\mathrm{dyn}}$生成新的动态文件$F_{\mathrm{dyn}}$，并返回给勒索软件。

8) 记录勒索软件访问动态文件F_{dyn}的时间并定期检查；

9) 如果访问时间间隔超过一定阈值，则释放相对应的动态文件F_{dyn}。

3.3　动态文件生成

稀疏文件技术可以被应用于创建一种动态文件生成策略。这种技术允许创建的稀疏文件在逻辑上与原始文件大小相同，但实际上只有非零数据块会被存储在磁盘上，而空白数据块则不占用物理存储空间。这种方法可以更加高效地使用文件系统中的空间。当系统需要访问原始文件时，它会被替换为一个稀疏文件。这个稀疏文件可能包含以下几种内容：全部真实数据、部分真实数据、部分真实数据和部分欺骗数据、全部欺骗数据。面对勒索软件的访问请求，系统能够根据识别到的勒索风险级别，生成相应形态的文件以响应勒索软件。在修改文件内容以提高可访问性时，系统还会相应地更新文件系统中显示的文件大小和其他相关属性。动态文件生成策略中的欺骗级别是根据勒索风险识别组件评估的风险等级来确定的，不同级别的欺骗对应不同的文件生成策略。

图4展示了基于稀疏文件产生的动态数据文件。相比于创建多种不同的数据格式，使用统一的标准数据格式生成欺骗数据更为简便。这些欺骗数据必须与环境或上下文保持一致，易于吸引攻击者，并且可以透明地更新。系统中存储了文件的真实数据块和欺骗数据块，假设某个文件包含m个真实数据块$S_1, S_2, S_3, \cdots, S_m$和$k$个欺骗数据块$D_1, D_2, D_3, \cdots, D_k$，则生成的动态数据文件包含以下4种情况。

1) 当限制勒索软件对某些文件的访问权限时，仅允许其访问文件的部分内容，如图4中的动态文件1和动态文件2所示，勒索软件分别只能访问真实数据块S_1、真实数据块S_2和S_3所包含的文件内容。

2) 勒索软件获取到包含真实和欺骗数据块的文件，如图4中的动态文件3，其包含真实数据块S_m、欺骗数据块D_1和D_2。

3) 勒索软件获取到一个完全欺骗性的文件，如图4中的动态文件4，为了引诱和分析不受信任

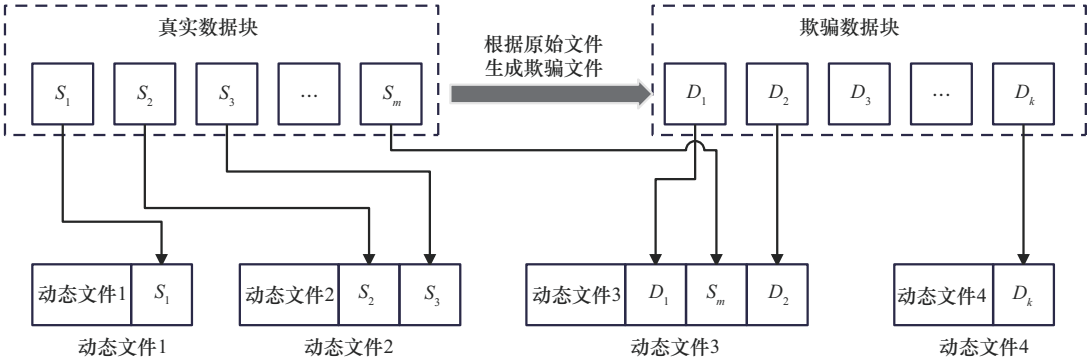


图4 基于稀疏文件产生的动态数据文件

的攻击者，其被设置成完全欺骗性的文件。

4) 勒索软件获取到完整且真实的数据文件。

为了生成动态数据文件，动态文件引擎将读取动态文件数据块索引并确定链接的数据块的位置，然后将动态文件数据块索引发送至动态文件生成组件，动态文件生成组件实时生成动态文件供勒索软件访问。

3.4 动态文件管理

动态文件管理主要用于管理动态文件生成组件生成的各种文件，并接受控制器的调度。动态文件管理模块会对生成的文件进行分类管理，包括原始文件和不同风险等级对应的文件等。它还会对不同类型的文件进行分类和存储，并对其进行适当的索引和标记，以便后续的访问和管理。对于长时间未访问的文件，它会及时将其删除，以释放存储空间。当下次有访问这些文件的请求时，该组件会重新触发动态文件生成组件，生成新的文件以满足访问者的需求。

启发式算法在欺骗文件部署中的应用是指利用基于经验法则和规则的算法，模仿人类专家的判断力和经验，来设计和安排欺骗文件。这种算法旨在优化部署文件的布局和数量，以实现高仿真度、增强欺骗效果、提升诱捕能力，并在成本上实现最优化。通过这种方式，可以有效地迷惑攻击者，保护真实数据不受侵害。

贪心算法是一种常见的优化算法，其基本思想是在每一步选择当前状态下的最优解，以期通过一系列局部最优选择得到全局最优解。基于贪心算法部署的欺骗文件如图5所示。使用攻击图对文件环境进行建模，攻击图中的节点i代表系统中的一个文件目录，其权重值为欺骗能力大小；攻击图中的边v代表文件目录之间的连接关系；节点i的度中心性指节点i被攻击者作为攻击的起始节点时，攻击者的攻击能力可以覆盖到的节点数量，覆盖节点数量对欺骗文件的欺骗属性以及产生的欺骗影响力进行量化。

本文采用贪心算法高效率、低成本地确认欺骗文件部署的位置，然后利用目标函数确定欺骗文件的数量，以获取欺骗效果、防御能力、系统性能和开销成本的最优解。成本的总和定义为

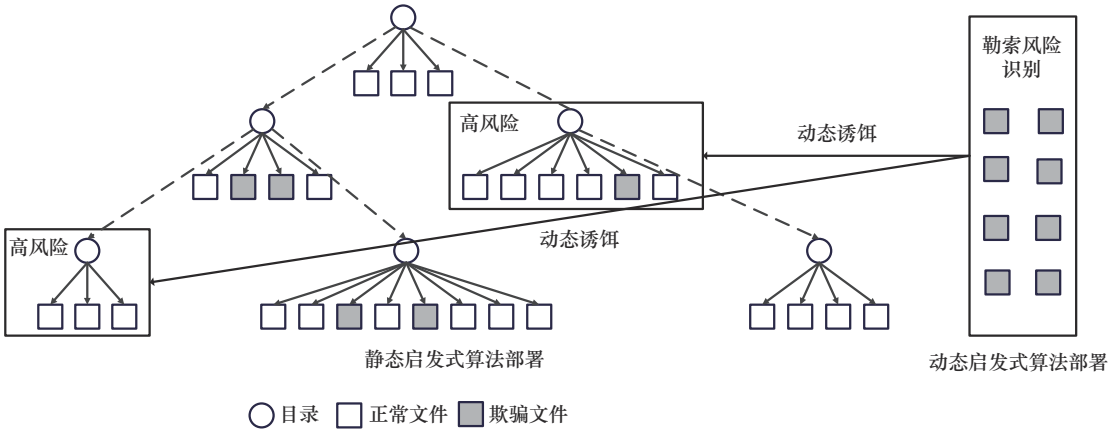


图5 基于贪心算法部署的欺骗文件

cost，$C\left(N_i\right)$表示在N_i位置部署一个欺骗文件时系统的安全收益。攻击成功概率定义为$P=\frac{1}{\mathrm{AD}}$，其中AD代表节点的攻击难度。同时，在攻击者遍历文件时，无法区分文件是否具有诱捕性。当有k个欺骗文件来保护一个实际节点N_i时，N_i被成功破解的概率为$\frac{P}{k+1}$。因此，这里定义收益函数为成功保护工作节点未受攻击时的收益减去部署欺骗文件所带来的性能消耗，然后乘以成功保护工作节点未受攻击的概率，如式(4)所示。当收益函数最大时，k的值为要在该位置部署的欺骗文件的数量。

$$F_k=\left(C\left(N_i\right)-k\mathrm{cost}\right)(1-kP+1) \tag{4}$$

基于贪心算法的欺骗文件部署算法如算法2所示。

算法2　基于贪心算法的欺骗文件部署算法

输入 文件系统攻击图

输出 生成的欺骗文件F_{dec}

1) 根据文件系统的构造对攻击图AG进行建模，并实时记录各节点的风险识别参数；

2) 计算得到攻击图中度中心性最大的节点部署欺骗文件，并将其可以覆盖和保护的相应子图从攻击图中删除；

3) 在新的攻击图中重新计算度中心性最大的节点，并重复欺骗文件部署和子图删除操作，直到欺骗文件能够覆盖整个AG；

4) 若某一节点的风险识别参数超过一定阈值，则优先在这一节点动态地部署欺骗文件；

5) 持续监控系统的更新事件，同时更新AG；

6) 根据新的AG重新计算当前的欺骗文件是否能够覆盖和保护这些新节点。如果能，转至步骤7)；如果不能，为它们选择新的位置部署欺骗文件，以对其进行保护。

7) 根据式(4)计算在收益函数取得最大值时k的值，并确定最终部署欺骗文件数量。

4　实验与评估

4.1　欺骗度评估

本文使用示假度和隐真度两大指标来评估上述系统抵御攻击的效果，并为改进和优化动态安全策略提供指导；应用多属性加权理论计算所有属性的欺骗距离。假设模型的属性集是$\boldsymbol{X}=\left\{X^i\right\}_{i\in N}$，其中，$X^i$是第$i$个属性，$N$是属性的数量。相应地，模型的欺骗性属性集合为$\boldsymbol{Y}=\left\{Y^i\right\}_{i\in N}$，其中，$Y^i$是第$i$个欺骗性属性，$N$是欺骗性属性的数量。属性的权重表示为$\boldsymbol{\omega}=\left\{\omega^i\right\}_{i\in N}$，所有属性的权重之和为1。整个模型的示假度为

$$E_{\mathrm{M}}=\sum_{i=1}^{N}\omega_i\sqrt{(X^i-Y^i)^2} \tag{5}$$

模型的欺骗性属性可以用向量$\boldsymbol{v}=\left\{v^i\right\}_{i\in N}$来描述，其中，$v^i\in\{0,1\},1\leqslant i\leqslant N$表示相应属性是否被改变。基于信息熵理论，欺骗性属性的不确定性可以根据其概率来衡量。如果概率大，不确定性就小；反之，不确定性就大。用p代表该欺骗性属性发生的概率，那么模型M的隐真度为

$$H_{\mathrm{M}}=-\sum_{i=1}^{N}\omega_i p\left(v_iX_i\right)\log p\left(v_iX_i\right) \tag{6}$$

属性示假度E_{p}用于衡量系统中真实属性和欺骗属性之间的相似程度，采用特征提取的方式将欺骗属性和真实属性映射到特征空间，并使用欧氏距离来衡量单个属性的示假度。同理，内容示假度E_{c}用于衡量系统中真实内容和欺骗内容之间的相似程度。内容隐真度H_{c}用于衡量系统中真实内容的隐蔽程度。高隐真度表示真实内容在欺骗内容中隐藏得很深，攻击者难以区分；低隐真度则意味着真实内容与欺骗内容易于辨认。

本文采用内容欺骗度D_{c}综合评价内容示假度E_{c}和内容隐真度H_{c}。内容欺骗度D_{c}的计算式为

$$D_{\mathrm{c}}=\frac{2E_{\mathrm{c}}H_{\mathrm{c}}}{E_{\mathrm{c}}+H_{\mathrm{c}}} \tag{7}$$

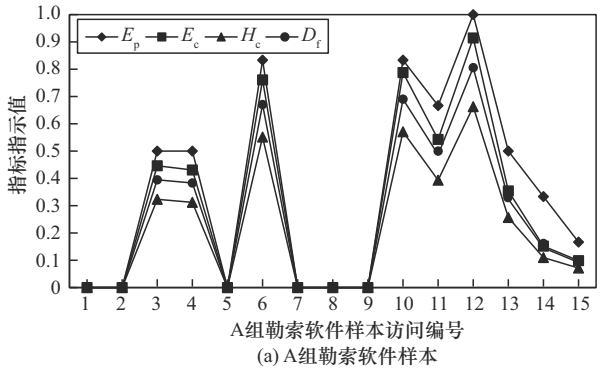
本文进一步结合属性示假度E_{p}，计算出文件欺骗度D_{f}为

$$D_{\mathrm{f}}=\left(1+\beta^2\right)\frac{E_{\mathrm{p}}D_{\mathrm{c}}}{\beta^2E_{\mathrm{p}}+D_{\mathrm{c}}} \tag{8}$$

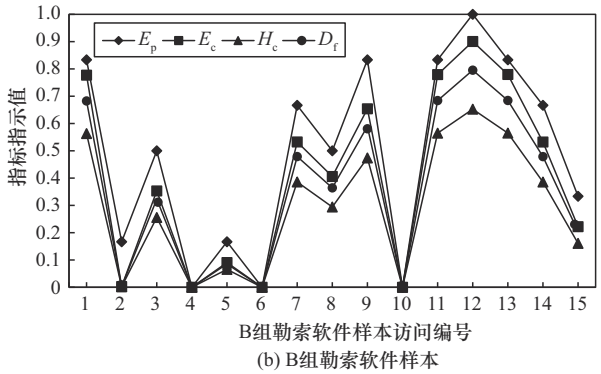
本文使用A、B、C这3组勒索软件样本模拟勒索攻击，勒索软件样本按照表2所示的顺序访问同一个文件，表中数字记录的是每个访问样本的风险级别。通过实验观察式(8)中不同β值对文件欺骗度的影响，这里取$\beta=2$，重复进行10次实验，并对结果取平均值以减少随机性，3组勒索软件样本的实验结果如图6所示。

表 2　　3 组不同勒索软件样本的访问顺序

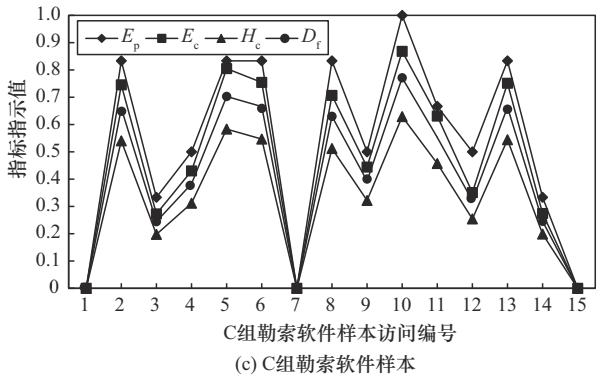
组序	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	0	0	3	3	0	5	0	0	0	5	4	6	3	2	1
B	5	1	3	0	1	0	4	3	5	0	5	6	5	4	2
C	0	5	2	3	5	5	0	5	3	6	4	3	5	2	0



(a) A组勒索软件样本



(b) B组勒索软件样本



(c) C组勒索软件样本

图6　3组勒索软件样本的实验结果

从图6可以看出不同风险等级的勒索软件访问文件时文件示假度和隐真度的变化情况。对于非法勒索软件来说，文件属性和内容欺骗度随着勒索风险等级的提高而增加，而合法的正常访问则不受影响。

本文采用欺骗文件诱捕时间来评估启发式动态欺骗策略的有效性。实验计算3组勒索软件样本检测时间的平均值，并将其作为衡量欺骗文件诱捕时间的标准。3组勒索软件样本的平均诱捕时间如图7所示。从图7可以看出，每组欺骗文件平均诱捕时间均在1 ms以内，这说明启发式动态欺骗策略能够有效地识别和应对勒索软件攻击。

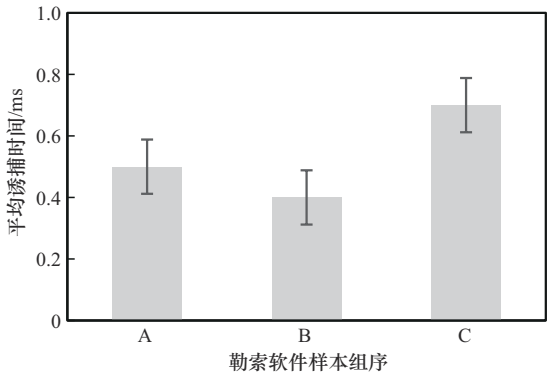


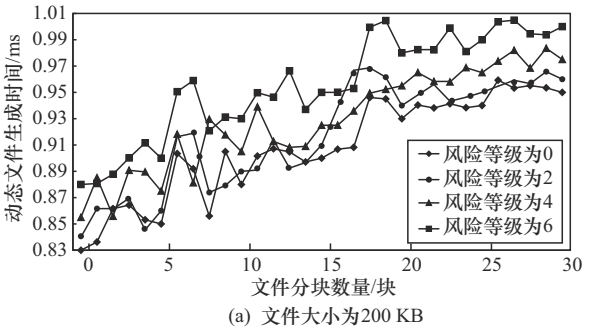
图7　3组勒索软件样本的平均诱捕时间

4.2　勒索时间分析

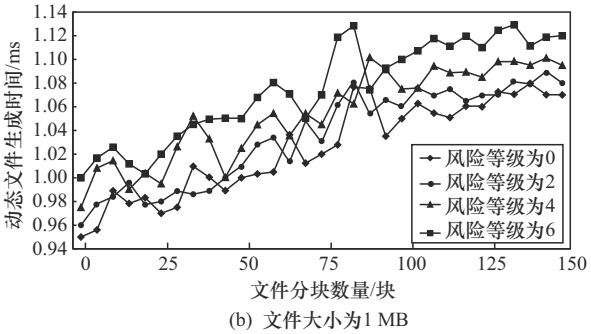
为了评估反勒索系统对勒索软件的影响，本文采用响应时间指标来衡量系统的性能开销，且响应时间通过测量动态文件生成时间和文件加载时间来评估。其中，动态文件生成时间用于度量文件生成速度，文件加载时间则用于度量勒索软件感知度。本文在Ubuntu系统上测试了系统原型，该机器配备了2.40GHz Intel Core i7处理器和12 GB内存。本文评估了原始大小分别为200 KB、1 MB和5 MB的3种文件的响应时间。

1) 动态文件生成时间

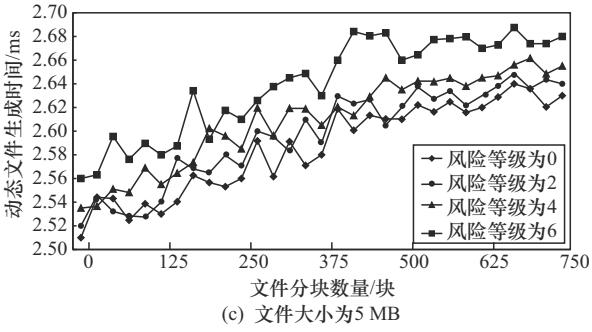
为了研究文件大小对勒索软件访问文件的影响，本文分析了不同文件大小下的动态文件生成时间。为了减少真实数据的随机性，本文采用了取平均值的方法来确定文件生成时间。对于具有不同勒索风险级别的文件，系统会尝试生成包含动态文件索引的稀疏文件，重复进行100次实验，并将这些结果的平均值作为动态文件生成时间，如图8所示。从图8可以看出，动态文件生成时间随文件大小增大而线性增加，并且随着勒索风险级别的提升，文件生成时间会缓慢增加，但仍在可控的范围内。



(a) 文件大小为200 KB



(b) 文件大小为1 MB



(c) 文件大小为5 MB

图8　动态文件生成时间

2) 文件加载时间

文件加载时间是指勒索软件读取文件所需要的时间。动态文件的操作会增加读取文件内容所需的时间。这种增加可能会引起攻击者警觉，因为需要等待更长的时间才能查看文件内容。因此，在设计动态文件系统时，需要平衡动态文件和使用体验之间的关系，以确保系统的性能和可用性。文件加载时间如图9所示。从图9可以看出，文件加载时间在相同文件大小下会随着勒索风险等级的提升而变长，但是与正常的文件加载时间相比没有明显的延迟。

4.3　勒索软件样本防护

从2019年开始，采用数据加密和数据泄露结合的混合勒索软件逐渐增多。表3总结分析了近年来的主流勒索软件样本使用本文方法的防护效果，重复进行10次实验，并对结果取平均值。从表3可以看到，所有测试样本均被识别为最高风险，欺骗度都在75%以上，防护效果显著。

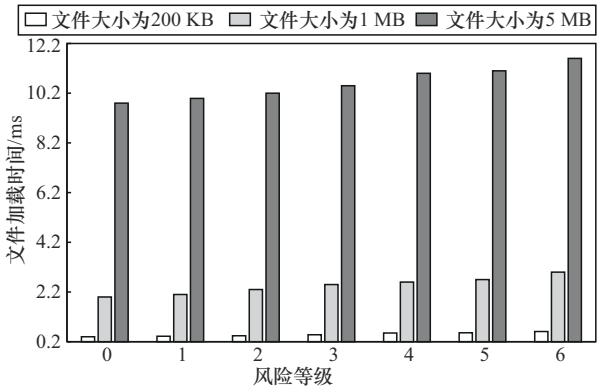


图9　文件加载时间

表3　主流勒索软件样本使用本文方法的防护效果

勒索样本名称	类别	欺骗度（风险等级）
Maze	混合勒索软件	77%（6）
Ryuk	混合勒索软件	82%（6）
Ekans	加密勒索软件	76%（6）
Clop	混合勒索软件	78%（6）
PureLocker	加密勒索软件	85%（6）
CovidLock	混合勒索软件	83%（6）
Corona	混合勒索软件	82%（6）
DarkSide	混合勒索软件	79%（6）
Babuk	混合勒索软件	78%（6）

5　结束语

本文探讨了勒索软件对数据安全构成的严重威胁，并提出了一种创新的主动欺骗方法来对抗这类攻击。该方法解决了传统数据安全防护中数据静态存储和单一访问路径的问题，通过实施动态文件生成策略，增强了数据的动态性和不可预测性，防止了勒索软件对文件的加密和锁定。此外，还提出了一种新型的启发式算法，用于高效部署欺骗文件，确保了欺骗的有效性和部署的效率，并成功地将对合法用户的影响和系统运行的开销降到了最低。展望未来，笔者计划引入人工智能技术，以构建一个更加智能化的反勒索软件系统。

参考文献：

[1] ALQAHTANI A, SHELDON F T. A survey of crypto ransomware attack detection methodologies: an evolving outlook[J]. Sensors, 2022, 22(5): 1837.

[2] MANSFIELD-DEVINE S. IBM: cost of a data breach[R]. 2022

[3] TAN L, YU K P, MING F P, et al. Secure and resilient artificial intelligence of things: a HoneyNet approach for threat detection and situational awareness[J]. IEEE Consumer Electronics Magazine, 2022,

11(3): 69-78.

[4] KAUR M, KUMAR V. A comprehensive review on image encryption techniques[J]. Archives of Computational Methods in Engineering, 2020, 27(1): 15-43.

[5] MA D H, TANG Z M, SUN X Y, et al. Game theory approaches for evaluating the deception-based moving target defense[C]//Proceedings of the 9th ACM Workshop on Moving Target Defense. New York: ACM Press, 2022: 67-77.

[6] JUELS A, RIVEST R L. Honeywords: making password-cracking detectable[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York: ACM Press, 2013: 145-160.

[7] MCRAE C M, VAUGHN R B. Phighting the phisher: using web bugs and honeytokens to investigate the source of phishing attacks[C]//Proceedings of the 40th Annual Hawaii International Conference on System Sciences. Piscataway: IEEE Press, 2007: 270.

[8] JUELS A, RISTENPART T. Honey encryption: security beyond the brute-force bound[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2014: 293-310.

[9] SALEM M B, STOLFO S J. Decoy document deployment for effective masquerade attack detection[C]//International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer, 2011: 35-54.

[10] VORIS J, JERMYN J, BOGGS N, et al. Fox in the trap: thwarting masqueraders via automated decoy document deployment[C]//Proceedings of the Eighth European Workshop on System Security. New York: ACM Press, 2015: 1-7.

[11] KAPRAVELOS A, GRIER C, CHACHRA N, et al. Hulk: eliciting malicious behavior in browser extensions[C]//Proceedings of the 23rd USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2014: 641-654.

[12] KIM D, LEE J. Blacklist vs. whitelist-based ransomware solutions[J]. IEEE Consumer Electronics Magazine, 2020, 9(3): 22-28.

[13] TURAEV H, ZAVARSKY P, SWAR B. Prevention of ransomware execution in enterprise environment on windows OS: assessment of application whitelisting solutions[C]//Proceedings of the 2018 1st International Conference on Data Intelligence and Security (ICDIS). Piscataway: IEEE Press, 2018: 110-118.

[14] LEE S G, KIM Y, LEE D, et al. Alohomora: protecting files from ransomware attacks using fine-grained I/O whitelisting[C]//Proceedings of the 14th ACM Workshop on Hot Topics in Storage and File Systems. New York: ACM Press, 2022: 113-118.

[15] AMI O, ELOVICI Y, HENDLER D. Ransomware prevention using application authentication-based file access control[C]//Proceedings of the 33rd Annual ACM Symposium on Applied Computing. New York: ACM Press, 2018: 1610-1619.

[16] KOHLBRENNER A, ARAUJO F, TAYLOR T, et al. POSTER: hidden in plain sight: a filesystem for data integrity and confidentiality[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 2523-2525.

[17] MEHNAZ S, MUDGERIKAR A, BERTINO E. RWGuard: A real-time detection system against cryptographic ransomware[C]//International Symposium on Research in Attacks, Intrusions, and Defenses. Berlin: Springer, 2018: 114-136.

[18] FENG Y, LIU C G, LIU B X. Poster: a new approach to detecting ransomware with deception[C]//Proceedings of the 38th IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2017: 1-2.

[19] GÓMEZ-HERNÁNDEZ J A, ÁLVAREZ-GONZÁLEZ L, GARCÍA-TEODORO P. R-Locker: thwarting ransomware action through a honeyfile-based approach[J]. Computers & Security, 2018, 73: 389-398.

[20] SHEEN S, ASMITHA K A, VENKATESAN S. R-Sentry: deception based ransomware detection using file access patterns[J]. Computers and Electrical Engineering, 2022, 103: 108346.

[21] WANG S M, ZHANG H, QIN S J, et al. KRProtector: detection and files protection for IoT devices on android without ROOT against ransomware based on decoys[J]. IEEE Internet of Things Journal, 2022, 9(19): 18251-18266.

[22] LI Z, LIAO Q. Preventive portfolio against data-selling ransomware—a game theory of encryption and deception[J]. Computers & Security, 2022, 116: 102644.

[作者简介]

陈凯（1987– ），男，山东东营人，博士，中国科学院信息工程研究所助理研究员，主要研究方向为移动目标防御、数据安全及隐私保护等。

马多贺（1982– ），男，安徽六安人，博士，中国科学院信息工程研究所副研究员、硕士生导师，主要研究方向为移动目标防御、网络主动防御、数据安全、隐私保护及反勒索等。

唐志敏（1999– ），女，湖南永州人，中国科学院信息工程研究所硕士生，主要研究方向为移动目标防御、反勒索、数据安全等。

Dai Jun（1985– ），男，博士，美国伍斯特理工学院副教授、博士生导师，主要研究方向为分布式系统安全、入侵检测、漏洞分析等。