证券信息技术发展研究中心（上海）2018 年联合研究计划

课题报告

基于攻击链的网络威胁捕猎架构设计

课题主办单位：上海证券交易所

课题承接单位：长江证券股份有限公司

安信证券股份有限公司

北京长亭科技有限公司

课题组成员：　韦洪波、潘进、肖建国、陈传鹏、徐承文、

李家攀、徐鹏志、孙凡琦

目录

摘　要

面对国内外严峻的网络安全形势，习近平总书记提出要加快构建关键信息基础设施的安全保障体系，全天候全方位感知网络安全态势。“漏洞必然存在，威胁不可能绝对消除，安全与体验必然存在矛盾”，针对网络攻击威胁的捕猎，蜜罐技术已经成为网络安全领域的重要研究方向，然而，当前蜜罐技术的研究缺乏全面性和主动性。

本课题研究如何将蜜罐技术有效应用在金融行业，如何将蜜罐体系贯通于攻击链的各个环节，如何利用网络威胁捕猎技术快速响应网络威胁监测与失陷溯源。本课题以蜜罐技术为基础，设计了基于攻击链模型的网络威胁捕猎架构，通过伪装真实的目标主机和网络环境，诱骗攻击者进入蜜罐系统，收集其在蜜罐系统中的各种操作，分析总结其攻击手法和攻击意图，从而有利于加强关键网络对攻击入侵的防御能力，提升各机构的网络威胁预警能力、网络攻击监测能力，以及安全事件的快速应急响应能力。

本课题的主要创新点：

（1）基于轻量级代理的分布式蜜罐，提高概率，部署灵活；

（2）内嵌植入式的应用级业务分流，可基于业务场景定制增强、精确和业务逻辑相关的蜜罐检测机制，更加精准；

（3）攻击意图和未知手法的跟踪发现，区别传统蜜罐的阻断模式，对攻击链进行引流，探索威胁的真实意图和手法，可以防范未然。

关键词：攻击链；蜜罐；威胁捕猎；分布式

Abstract

Facing the severe cyber security situation at home and abroad, General Secretary Xi Jinping proposed to accelerate the construction of the security guarantee system of key information infrastructure，and perceive the cyber security situation all-weather and all-around. "Vulnerabilities must exist, threats cannot be eliminated absolutely, and there must be a contradiction between security and experience." Honeypot technology has become an important research area in network security to hunt cyber-attack threats. However, the research on honeypot technology is lack of comprehensiveness and initiative.

This paper researches how to apply honeypot technology effectively in financial industry, how to integrate honeypot system into each link of Intrusion Kill Chain, how to use cyber threat hunting technology to quickly respond to cyber threat monitoring and trace the fall to its source. Basing on current honeypot technology, this paper aims to design a network threat hunting architecture on Intrusion Kill Chain model. By disguising real target host and network environment, the attacker is lured into the honeypot system. All the operations will be collected in the honeypot system in order to analyze and summarize the attack techniques and intentions. The system will strengthen the defense capabilities of critical network. The system will improve the early warning capability of cyber threats and the ability to monitor cyber attacks. And also the system will improve the ability to quickly respond to safety incidents.

Main innovations of this project:

(1)The distributed honeypot based on lightweight proxy, in order to improve the probability of arrest. And the honeypot system can be deployed flexibly.

(2)The honeypot system is designed to be embedded application-level business triage. And the system can customize honeypot detection mechanism based on business logic. So it can be more accurate.

(3)The honeypot system can track the attack intent and unknown tactics. Distinguishing the blocking mode of traditional honeypot, the honeypot system diverting the attack chain and exploring the real intention and tactics of threats, so we can prevent it from happening.

Keywords: Intrusion Kill Chain; Honeypot; Threat hunting; distributed

第 1 章 绪论

1.1 课题背景

当前，黑客技术不断发展，数据泄露、勒索病毒等网络安全事件频繁发生，网络安全威胁已经成为了一个突出的社会性问题。在此形势下，证券行业随着互联网的发展和大数据、云计算等技术的应用发生了翻天覆地的变革，同时也面临着更高的安全风险。

由于网络安全攻守双方的视角不同，防守方往往处于被动局面，攻击方只需要找到一个突破点就能攻击成功，而防守方不仅要考虑全局，还要具备快速的检测能力和完善的应急机制才能尽可能地确保信息系统安全[1]。

蜜罐（honeypot）技术就是为了改变这种被动的防护状况而出现的一种主动防护技术[2]。通常将蜜罐定义为一种安全资源，它不需要提供实际的应用，存在价值就是诱导和记录攻击者的攻击行为，延缓其攻击进程，使得防御方可以了解攻击者的入侵方法和手段，并根据捕获的攻击行为数据，针对性地增强系统的安全防护能力[3]。

1.1.1 蜜罐的功能及分类

蜜罐通常具备数据捕获、数据分析和数据控制方面的功能。数据捕获主要收集主机数据或者网络数据，主机上可以捕获攻击者的 TCP 连接情况、执行的命令、各种日志信息等，网络数据包括防护系统日志、网络流量数据等。但蜜罐的价值通常需要对捕获的数据进行分析后才能体现，主要包括网络协议类型分析、攻击行为分析和攻击数据包内容分析等。数据控制主要是指通过对蜜罐的对外数据发送和网络进行限制，使得当蜜罐系统被攻击者攻破时，也不会造成更多的危害。

数据控制主要用来保障蜜罐本身的安全。

蜜罐通常可以分为低交互蜜罐和高交互式蜜罐两类。

低交互蜜罐通常只提供少量的交互功能，蜜罐在特定端口监听连接并记录数据包，可以用来实现端口扫描和暴力破解的检测。低交互蜜罐结构简单，易于安装部署，由于模拟程度低功能较少，收集信息有限但风险也较低。

高交互蜜罐通常基于真实的应用环境来构建，能提供真实的服务。高交互蜜罐可用来获取大量的信息，能够捕获攻击者多种操作行为，从而具备发现新的攻击方式和漏洞利用方法的能力。由于高交互蜜罐给攻击者提供了一个相对真实的应用环境，因此风险较大，通常会注重数据控制方面的功能。

1.1.2 蜜罐技术研究发展现状

蜜罐技术不是一个新概念，威胁情报概念的流行已有数年时间，“Threat”和“Intelligence”正成为大家关注的焦点。这几年随着威胁情报的成熟，蜜罐技术被关注的越来越多，也渐形成低交互、中交互、高交互等交互程度的各类蜜罐，从 Web 业务蜜罐、SSH 应用蜜罐、网络协议栈蜜罐到系统主机型蜜罐的各功能型蜜罐。小到一个 Word 文档的蜜标，到一个系统级的服务蜜罐，再到多功能蜜罐组成的蜜网，大到包含流控制重定向分布式蜜网组成的蜜场。

随着虚拟化技术的发展，各种虚拟蜜罐也得到发展，可以通过虚拟机来实现高交互蜜罐，以及通过 Docker 实现的业务型蜜罐，不再像是以前需要昂贵硬件设备的部署支撑，这也大大减少了蜜罐的部署成本，一台主机就可以实现整个集群数据控制，数据捕获和数据分析于一体多功能多蜜罐高交互蜜网的体系架构。也已经产生了一些不错的开源蜜罐产品或项目，比如 T-Pot、MHN、HoneypotProject 等。T-Pot 是一个基于 Docker 容器的集成了众多针对不同应用

蜜罐程序的系统，该蜜罐平台直接提供一个系统 ISO，里面使用 Docker 技术实现多个蜜罐，更加方便进行蜜罐研究与数据捕获。MHN 现代蜜网简化了蜜罐的部署，集成了多种蜜罐的安装脚本，可以快速部署、使用，也能够快速的从节点收集数据。

蜜罐高保真高质量的数据集把安全人员从以前海量日志分析的繁琐过程中解脱出来，对于蜜罐的连接访问都是攻击信息，并且不再像以前的特征分析具有一定的滞后性，可以用于捕获新型的攻击和方法。

1.1.3 研究目的与意义

网络攻击链描述了攻击者完成一次攻击需要执行的 7 个步骤，包括侦查探测、制作攻击工具、将工具投送到目标、释放代码、成功安装并控制、主动外联、远程控制及扩散。在攻击链的所有步骤中，防御者在各个阶段都有机会阻断攻击行为。借助攻击链检测和安全控制措施，企业将能够：

（1）更好地了解基于攻击链各个阶段的控制措施；

（2）更早地识别攻击，尽可能降低攻击影响，最大化防御效果；

（3）如果已经出现攻击者，在数据泄露之前能够检测到；

（4）获取攻击者真实的攻击意图和攻击手法。

1.2 课题研究目标

本课题主要实现以下 6 项研究目标：

（1）研究典型攻击链的威胁捕猎场景；

（2）研究分布式网络威胁捕猎技术设计与部署架构；

（3）研究高交互式蜜罐设计方案；

（4）研究基于业务逻辑的轻量级攻击捕猎探针设计；

（5）研究攻击意图和未知手法的跟踪发现；

（6）研究基于蜜标的攻击溯源设计。

1.3 研究方法

课题以蜜罐技术为基础，设计了基于攻击链模型的网络威胁捕猎架构，通过伪装真实的目标主机和网络环境，诱骗攻击者进入蜜罐系统，收集并分析其在蜜罐系统中的各种操作日志，了解其攻击手法，总结其攻击意图。

课题研究方法：

（1）课题深入研究经典攻击链模型的七个步骤，并将其划分为四个攻击阶段，对应每一个阶段，分别设计出网络欺骗模块、攻击捕获模块、信息控制模块与特征提取模块，并以此四个模块为基础来构建网络威胁捕猎技术框架。

（2）课题提出一种基于轻量级代理的蜜罐体系建设方案，分别从分布式代理模式设计、配置高交互式蜜罐两个方面来阐述此建设方案。

（3）课题研究应用级业务分流的陷阱捕获方案，设计基于业务逻辑的攻击捕猎探针，用以提高蜜罐捕猎的有效性。

（4）课题通过日志聚合与攻击画像研究攻击链模型的每个攻击阶段，从而探测攻击者的攻击意图和手法，为追溯与分析安全威胁提供基础数据支持。

第2章　网络威胁捕猎场景与设计

2.1 典型攻击链的威胁捕猎场景

信息安全是基于攻防双方力量不均衡和信息不对称的博弈[4]。虽然对手信息在变，但通过预测对手行为尽可能多地掌握对手信息会让战局处于相对优势，即所谓“未知攻，焉知防”。因此，从攻击者角度出发的攻击链（Intrusion Kill Chain）模型就有借鉴意义。该模型由美国洛克西德·马丁公司于 2011 年提出，将网络空间攻击行为分为七个步骤，包括侦查探测（Reconnaissance）、制作攻击工具（Weaponization）、将工具投送到目标（Delivery）、释放代码（Exploitation）、成功安装并控制（Installation）、主动外联（Command & Control）、远程控制及扩散（Actions on Objectives）[5]，如图 1 所示。

图 1　典型攻击链模型

攻击链模型的精髓在于明确提出网络攻防过程中攻防双方互有优势，攻击方必须专一持续，而防守方若能阻断或瓦解攻击方的任何进攻组织环节，即可成功地挫败对手的攻击企图。同时，攻击链模型提供了一种纵深防御的概念，即在攻击最终造成损失的七步中，任何一步的察觉或者阻挡均能有效阻止和阻断[6]。意即，即使发现了被攻破，在造成最后的损失前，还有机会进行补救。

2.2 网络威胁捕猎技术框架

攻击链的构建会直接影响网络威胁捕猎的效果。为适应新的攻击行为和攻击手法，本课题将典型攻击链模型的七个步骤分为了四个攻击阶段，即侦查阶段、渗透攻击阶段、攻陷阶段与恶意行为阶段[7]，如图 2 所示。对应每一个阶段，分别设计出网络欺骗模块、攻击捕获模块、信息控制模块与特征提取模块，并以此四个模块为基础来构建网络威胁捕猎技术框架。

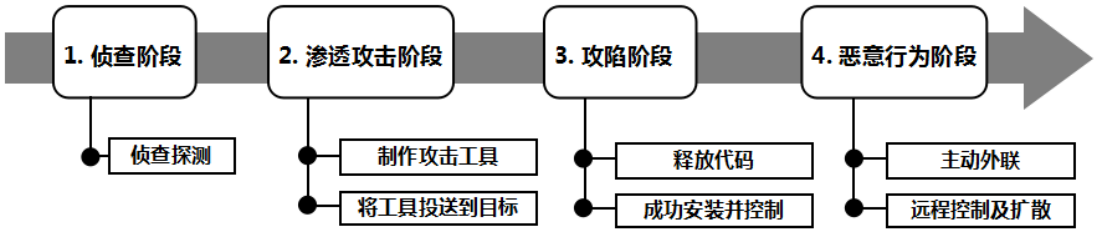

图 2 攻击链攻击阶段

2.2.1 网络欺骗模块

网络欺骗模块主要针对攻击链的侦查阶段，本课题主要通过蜜罐的伪装来达到攻击欺骗的目的。为了达到更好更真实的诱捕效果，蜜罐系统主要从网络、终端以及应用三个层次进行伪装，如图 3 所示，网络层面主要是将蜜罐节点与真实节点部署在相同的网段，终端层面主要是使用相似的终端并模拟交互命令，应用层面则是制定高交互蜜罐仿制系统应用。同时为了提高伪装的程度，还可以根据系统的特点在蜜罐中加上业务特点、虚假的敏感数据以及中间件服务。

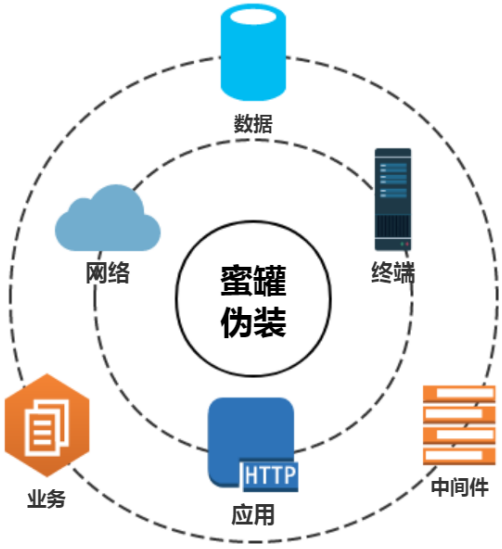

图 3 网络欺骗模块

2.2.2 攻击捕获模块

攻击捕获模块主要针对攻击链的渗透攻击阶段，用以监视与记录进入蜜罐系统的所有行为。一旦监控到有攻击者对蜜罐系统的非法操作，马上生成相关记录信息，如图 4 所示，记录的内容至少包括时间戳、探针 ID、源 IP、源端口、源 MAC 地址、目的 IP、目的端口、威胁等级、额外信息（具体的事件详情）、时间 ID、事件类型、来源蜜罐等，以 json 格式进行记录，并通过表格、图形等方式进行可视化展示。

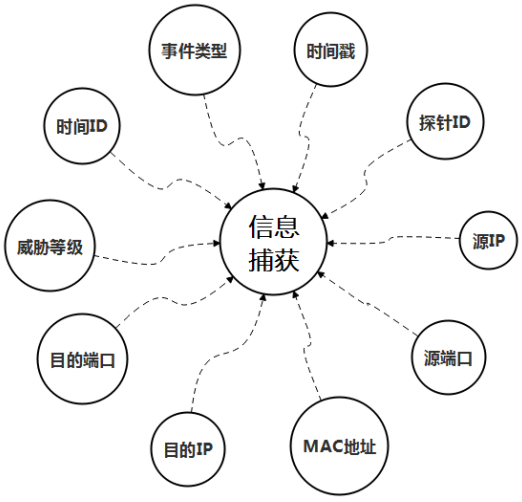

图 4 攻击捕获模块

2.2.3 信息控制模块

信息控制模块主要针对攻击链的攻陷阶段，通过对进入蜜罐系统的攻击行为进行限制，保证攻击者不会以被攻陷的蜜罐主机为跳板，渗透攻击其他系统并造成危害。

伪装越真实的蜜罐，越要控制突破风险。如图 5 所示，本课题通过流量监控、网段封锁和虚拟化三个层面来达到信息控制的目的。一般地，流量监控主要是监控攻击者的所有入侵流量，若存在内网端口嗅探、反向代理等内网攻击行为，则立刻发出报警并阻断攻击；网段封锁通常是通过防火墙与路由器设置各网段的访问规则，禁止蜜罐中的流量访问真实资产；虚拟化则是采用虚拟化技术配置蜜罐，确保攻击者入侵后不会影响其他服务，把攻陷阶段的风险控制在最小范围。

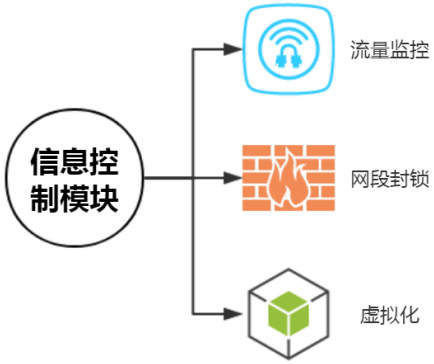

图 5 信息控制模块

2.2.4 特征提取模块

特征提取模块主要针对攻击链的恶意行为阶段，通过提取攻击者在目标主机安装的恶意软件特征，监控恶意软件的行为，探测攻击者的入侵意图，获取攻击者的关键情报，从而可以针对性地对攻击行为进行防御。

特征提取模块主要是从攻击行为和关键情报进行特征提取，如图 6 所示。攻击行为主要是针对恶意行为阶段的攻击特征提取；而关键情报可以分为武器类情

报和资产类情报，武器类情报包括攻击者使用的攻击工具、恶意软件以及病毒木马等，资产类情报包括攻击者所掌控的信息资源、爆破字典、病毒分发服务器以及远控 IP 信息等。

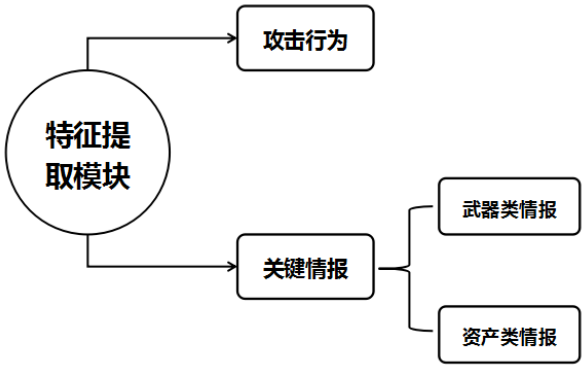

图 6 特征提取模块

第3章　基于轻量级代理的蜜罐体系建设方案

在攻击侦查阶段，传统蜜罐往往存在流量控制困难、物理机部署不方便、动态性与扩展性不足的问题[8]。本课题提出一种基于轻量级代理的蜜罐体系建设方案，本节分别从分布式代理模式设计、配置高交互式蜜罐两个方面来阐述此建设方案。

3.1 分布式代理模式设计

为了适应流量包的高速需求，避免交换瓶颈，提高运营效率，蜜罐系统采用便于轻量化部署的分布式代理模式设计。本课题中将蜜罐系统共分为两个部分，即蜜罐服务部分与探针部分，可分别视作管理节点和探针节点。

其中，管理节点位于一台性能较高的 Linux 上，通过 Docker 虚拟化部署蜜罐服务。Docker 容器是一种轻量级的虚拟化技术，与传统的虚拟化技术相比，它能让更多数量的应用程序在同一硬件上运行，简化了管理和部署应用程序的任务，能够实现高速、轻量的目标[9]。

管理节点是整个系统的中枢部分，负责策略管理、日志收集、请求处理，通过 OpenAPI、SysLog、邮件告警与网络中其他运维设备进行交互，通过前端 Web 界面实现对系统的可视化管理。管理节点的主要作用包括对探针的运行状态进行监控、对探针转发的数据进行处理和响应。

管理节点与探针节点采用一对多设计。在网络可达的前提下，一个管理节点即可统一管理网络中多个探针节点。探针节点会自动注册到管理节点，并定时发送自身的运行状态信息。

探针节点分布于网络中各个独立的主机系统上，其的主要作用是监听端口、

伪装真实服务、采集攻击流量、代理攻击流量到蜜罐服务。在监听的端口接收到流量时，探针节点并不直接对请求作出回应，而是先通过网络欺骗模块将流量转发到蜜罐服务运行的环境，由后者对数据包进行处理，并将响应请求发送至探针，再由探针对发起请求的客户端进行响应。

在该结构中，管理节点与探针节点之间的数据传输信道经过加密处理，管理节点不对外直接监听服务，经探针代理转发到管理节点的流量仅在 Docker 的虚拟环境中运行，且每个蜜罐服务使用不同的 Container 独立运行，以此来保证蜜罐系统的安全性。

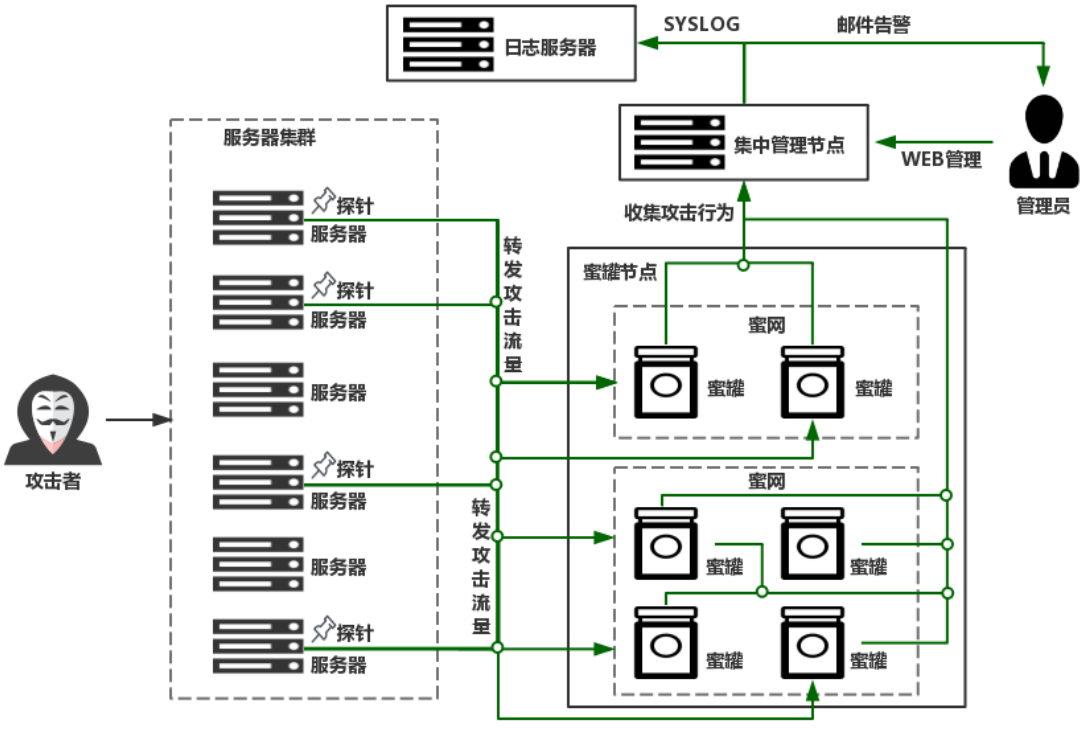

图 7 分布式代理设计

如图 7 所示，在服务器集群中，将部署有探针的节点与其他服务器的节点混合。一旦入侵者试图访问真实的服务，如建立完整 TCP 连接、SYN 探测、业务数据访问等，探针节点即将流量代理转发至位于管理节点的蜜罐中。蜜罐处理后，将响应数据包交由探针节点，再由探针节点对入侵者进行应答。信息控制模块将

整个交互过程控制在一个闭塞的虚拟化平台中，保证蜜罐服务所在的环境不会被攻陷并作为一台跳板机向内网其他机器发起攻击。

3.2 高交互式蜜罐设计

在渗透攻击阶段攻击者往往只会在确定了攻击目标才会“将工具投送到目标”。从攻击链的角度来看，想要捕获整条攻击链上的数据信息，必须要采用高交互式的蜜罐设计。

高交互蜜罐通常基于真实的应用环境来构建，能提供真实的服务。高交互蜜罐能够捕获攻击者多种操作行为，具备发现新的攻击方式和漏洞利用方法的能力。由于高交互蜜罐给攻击者提供了一个相对真实的应用环境，因此风险较大[10]，信息控制模块通常会注重数据控制方面的功能。

本课题在真实运行环境中，根据网络拓扑信息、服务器列表、网络安全域划分以及 IP 分布情况，计算出各个网段需要部署的蜜罐数量，并在实际运行过程中动态调整。

蜜罐的网络欺骗模块包括常见的主流服务类型，例如 Web 类、数据库类、系统服务类、漏洞缺陷类等，所使用的协议均为标准协议，敏感信息经过混淆后加入蜜罐中，提高伪装程度，更真实地模拟业务系统。入侵者在访问探针节点时，能够得到真实的响应和数据。通过在合适的区域场景选择合适的蜜罐类型，能够达到高度的迷惑性。

蜜罐服务打包成 Docker 镜像，直接使用 Docker 运行加载。信息控制模块通过给每个蜜罐配置单独的 Docker 容器，确保攻击者入侵后不会影响其他服务，把入侵风险控制在最小范围。

第4章　陷阱捕获设计方案

正如陷阱一样，蜜罐必须经过恰当的配置才能吸引正确的目标，并在不被察觉的情况下捕捉攻击者并对其行为进行监测。蜜罐的管理者要思考以下几个问题：对哪些行为进行监测，对谁的行为进行监测，什么时候进行行为监测等[11]。如果配置不当，蜜罐不仅不能吸引到猎物，而且很容易被攻击者劫持。另外，盲目捕捉大量的网络行为将导致数据处理上的困难。因此，需要针对某个特定的目标，对蜜罐进行定制化的配置。本节中讨论基于业务逻辑的攻击捕猎探针的设计，以及内嵌植入式的应用级业务分流方案，用以提高蜜罐捕猎的有效性。

4.1 基于业务逻辑的攻击捕猎探针设计

作为主动引流蜜罐，探针的设计需要符合业务逻辑，否则很难具有真正意义上的伪装和诱导作用。

针对渗透攻击阶段的特点，攻击捕获模块基于业务场景定制业务逻辑相关的蜜罐检测机制。证券行业的业务模式与一般互联网 Web 业务不尽相同。对于互联网 Web 系统，攻击者关注的一般都是传统的漏洞，蜜罐探针只需要基于传统的攻击引流即可。而证券行业涉及到各种各样的业务模型，每个业务模型又会有多种业务功能，攻击者在进行攻击嗅探和信息收集时，会根据业务形态加以判断，是否有部署蜜罐的可能性[12]，存在刻意避开特定服务（探针服务）的可能性。因此，探针的设计需要更加契合业务形态或逻辑，针对每一项业务安全场景，设计相应的探针进行攻击引流。

在本课题中，蜜罐中设计的业务场景如下表。其中，“数据校验探针”可以将那些正在尝试“0 元购”的攻击者引流到蜜罐中，“接口流量探针”可以对重要业务接口进行异常流量监测并引流。

表 1 业务安全与探针设计

业务安全类型	探针名称	探针作用
验证码突破	验证码探针	验证码爆破攻击引流
业务授权安全	权限探针	未授权访问流量引流
业务流程乱序	流程顺序探针	流程乱序攻击引流
业务接口调用	接口流量探针	接口异常流量引流
身份认证安全	认证失败探针	身份认证攻击引流
业务一致性安全	一致性校验探针	非一致性流量引流
业务数据篡改	数据校验探针	数据篡改流量引流
时效绕过	时效监控探针	可疑时效流量引流

4.2 内嵌植入式的应用级业务分流

攻击者在前期进行信息收集时，会逐个 VLAN 或者子网进行扫描，然后对发现的资产进行筛选，最后尝试攻击感兴趣的服务。因此，攻击行为具有不确定性，不确定因素在于攻击的范围和应用的类型。

如图 8 所示，通过分布式架构设计，以子网为最小部署单位，将探针分散部署到不同的子网中。根据真实资产的分布特点，部署合适数量及类型的探针节点，与真实资产节点混合，能够有效实现业务分流。

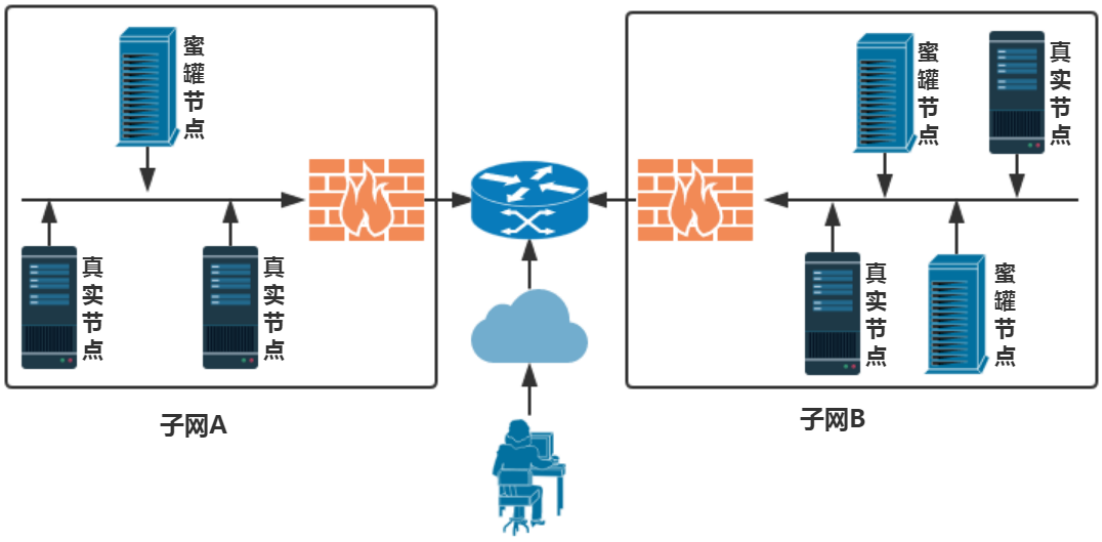

图 8 探针内嵌植入式设计

这种分布式的特性，有效地增强了不同网段对于入侵流量的承载面，加大了与入侵者的碰撞率，使得入侵流量能够更大几率地被引流到蜜罐，同时减小了真实资产节点的攻击面。另外，通过增加各网段的服务数量，增长了入侵者的筛选时间，延缓了攻击过程。

第5章　攻击意图和攻击溯源探测研究

传统的网络安全防御会阻断攻击行为，因而无法对攻击者的攻击行为进行持续追踪。本课题通过攻击捕获模块和特征提取模块对攻击意图和未知手法进行不间断的跟踪发现，深度追踪攻击者行为，探索其真实意图和手法，针对性地采取更高效的防御措施。本节介绍捕获威胁数据之后的日志聚合与攻击画像，探测攻击者的攻击意图和手法，为追溯与分析安全威胁提供基础数据支持。

5.1 日志聚合与攻击画像

要记录攻击链上每个环节的数据信息，必须对日志进行聚合。所有入侵的事件均由正在提供服务的蜜罐报告，并且通过管理节点上的其他关键组件进行日志聚合。目前来看，最为合理的方式是以蜜罐为记录对象，以时间线的方式进行聚合。从攻击链的侦查阶段开始，到恶意行为阶段结束，由上往下呈现，中间按照时间穿插攻击事件，每个攻击事件有不同类型，类型对应着固定的危险等级。日志的内容至少包括时间戳、探针 ID、源 IP、源端口、源 MAC 地址、目的 IP、目的端口、威胁等级、额外信息（具体的事件详情）、时间 ID、事件类型、来源蜜罐等，以 json、XML 等跨平台数据格式进行传递。

日志聚合的细分维度如图 9 显示，其中入侵时间线包括时间、事件类型、时间详情、操作回放，此四个维度能够对一次入侵事件进行还原。

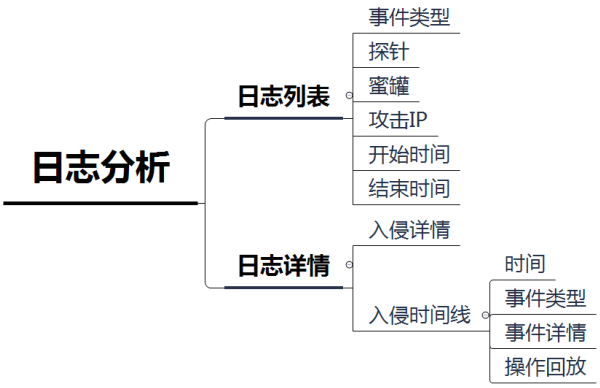

图 9 日志聚合细分维度

攻击链模型的每个阶段的数据都在日志中记录，因此可基于日志数据进行攻击画像。一次完整的攻击画像应该包括：动机、作息、深度和广度、复杂度、隐蔽性、攻击源、脆弱性、工具以及目标，如图 10 所示。

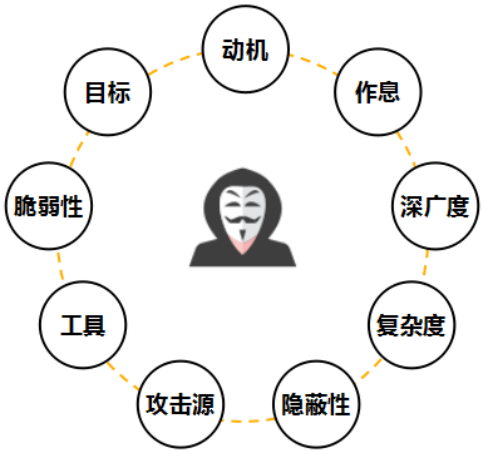

图 10 攻击画像

动机主要描述攻击的原因，通常只能猜测，但是对高交互蜜罐的动作可能会揭示一些见解；广度和深度可以从攻击频率、攻击传播和高交互蜜罐通过感染的程度推断出；攻击复杂度是用来描述攻击执行的难度；攻击源通常可以通过事务元信息来确定；脆弱性通常通过利用检测技术来识别；工具则是记录具有一定交互度的攻击工具[13]。

5.2 攻击意图探测与情报获取

基于攻击链的入侵意图分析，是最直接有效的入侵证据链。本课题区别于传统蜜罐的阻断模式，代之对攻击链进行引流，以分析威胁的真实意图和手法。

课题通过攻击捕获模块记录攻击者的所有攻击行为，并进行日志聚合与攻击画像，在此基础上可以还原攻击链的完整过程，针对攻击链的恶意行为阶段，特征提取模块通过提取攻击者在目标主机安装的恶意软件特征，监控恶意软件的行为，从而探测攻击者的入侵意图，获取攻击者的关键情报。

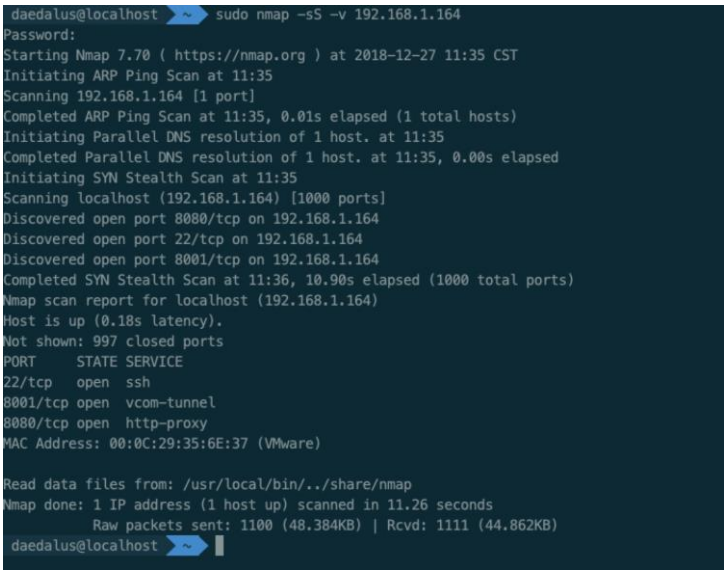

图 11 端口扫描攻击模拟

攻击意图的预测依赖于内置的攻击路径模型，如图 11 所示，攻击者使用 nmap 对蜜罐系统进行全端口扫描，在扫描出 22 端口后对系统进行 SSH 爆破，并成功拿到系统权限，攻击捕获模块监视并记录着此次攻击行为。蜜罐管理节点会立即向系统管理员发出邮件告警，如图 12 所示，邮件里面会详细记录攻击者的入侵时间段、入侵信息以及攻击事件统计。


威胁感知告警汇总

通知详情

谛听于北京时间 2018-12-25 16:08:41 至 2018-12-25 17:01:40 捕获到一次入侵，入侵统计如下

入侵信息

探针名称	linux
探针IP	192.168.1.164
蜜罐名称	ssh
蜜罐类型	SSH
发生时间	2018-12-25 16:08:41 - 2018-12-25 17:01:40
攻击者IP	10.2.7.147

事件统计

事件类型	Shell 命令执行
危险等级	高危
发生次数	2
事件类型	密码登录事件
危险等级	高危
发生次数	1

图 12 邮件告警

在这次攻击中，攻击者的所有动作都被蜜罐捕获，如图 13 所示，蜜罐详细的记录此次攻击时间线，我们可以很直观的观测到攻击者是何时开始建立连接，用哪个密码爆破成功，登录进来后的高危命令执行事件，以及在蜜罐主机中遗留的恶意文件。

图 13 告警详情

为了更详细的分析入侵者的所有攻击过程，我们还可以对蜜罐日志进行分析，蜜罐管理系统提供了日志下载功能，经过日志分析可以完整地还原此次攻击过程，如图 14 所示：首先，入侵者对目标系统进行全端口扫描，然后进行 SSH 爆破；爆破成功拿到权限后，会检查系统或服务自身的安全措施；接着对安全措施进行破坏，例如修改 Iptables、Selinux 等；然后使用目标系统下载攻击程序或脚本；最后使用下载的程序或脚本执行攻击命令，对外发起 DDOS 攻击。

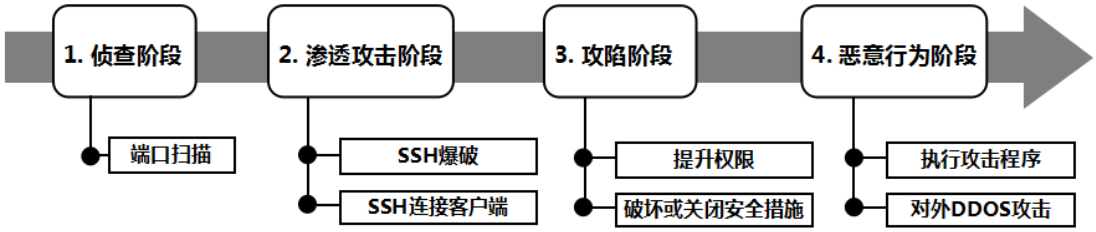

图 14 攻击过程

在此次攻击链的恶意行为阶段，特征提取模块监控着恶意软件对外执行攻击命令的行为，成功地探测到攻击者的攻击意图。除此之外，特征提取模块还能在这次攻击链还原中获取到关键情报，如图 15 所示。获取的情报分为两类：一是“资产类情报”，包括 SSH 爆破字典、SSH 连接客户端、病毒分发服务器 IP/域名、远程控制域名/IP 等；二是 “武器类情报”，包括病毒样本、攻击时执行的命令、攻击时对系统产生的影响等。蜜罐系统依赖这两类情报，对入侵流量进行标记，与攻击路径模型进行匹配，以此预测攻击意图；对于未知手法，则依据对系统造成的最终影响进行判断，以此完善和丰富攻击路径模型。

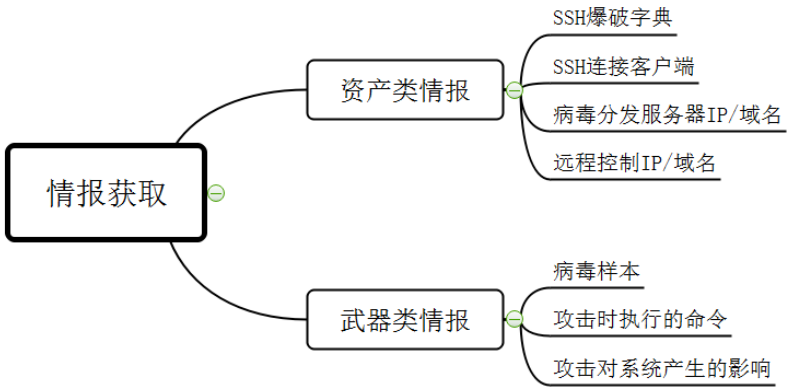

图 15 情报获取样例

5.3 基于蜜标的攻击溯源设计

无论是传统的网络防御设备还是传统的蜜罐系统，攻击溯源的追踪一直都是一个难以解决的问题，我们通常能获得到的仅仅只是攻击画像中的攻击源 IP 信息，然而，在服务器蜜罐的情况下，必须考虑他们可能已经接收到虚假的 IP 地址。本课题在基于传统的蜜罐攻击溯源的基础上，针对证券公司系统专有的业务特点，通过网络欺骗模块进行数据伪装，设计信息记录模块，以此来进行特有的溯源分析。

众所周知，攻击者针对证券公司系统的入侵，绝大多数都是以获取证券公司客户信息为目的，为此，我们在蜜罐伪装层面加入一些带“特定信息”的虚假客户数据，这些“特定信息”我们可以称之为蜜标。

通俗来讲，蜜标即嵌入数据中的特定标识，一旦攻击者入侵了蜜罐主机，窃取了带有蜜标的数据或文件，并执行相关操作，就会触发蜜标的内嵌脚本，记录并回传攻击主机的相关信息；同时远程服务器检测到相关异常，接收回传的攻击主机信息并向安全管理员发出告警，使其能够利用获取到的攻击数据进行追踪定位，以及对攻击者的相关行为分析。

课题通过网络欺骗模块进行数据伪装，设计带有蜜标的虚拟用户数据，数据的存储格式可以是 Word、Excel 以及 PDF 等文本格式，也可以是 MySQL、MSSQL 等数据库文件，在设计时要求这些文件中的蜜标容易检测，且对攻击者来说不可见，同时该文件在传输过程中仍能进行检测和提取；其次，蜜标文件的命名与分发部署要精心设计，一方面要能让攻击者容易发现并引起浓厚兴趣，另一方面又不能让攻击者引起怀疑而识别出蜜罐的陷阱环境。

蜜罐系统在攻击者感兴趣的资源中加入信息记录模块，当攻击者访问了带有信息记录模块的资源时，信息记录模块将会在攻击者使用的终端上运行，并收集攻击者终端的信息。收集到的信息用于对攻击者身份信息进行分析，根据身份信息实现攻击者的追踪。

本节提出的信息记录模块由两部分组成：蜜标文件和溯源服务器。蜜标文件负责对攻击者客户端信息的收集并将收集到的信息发送到溯源服务器，溯源服务器接受蜜标文件发回的信息，并对攻击者活动进行关联。

信息记录模块运转流程步骤如图 16 所示：

（1）防御者预先在攻击者可能访问的蜜罐中放置蜜标文件；

（2）攻击者访问部署有蜜标文件的资源；

（3）蜜标文件在攻击者终端上收集信息；

（4）蜜标文件收集的信息回传到溯源服务器；

（5）溯源服务器根据收集到的信息生成身份标识，依据身份标识对攻击者进行跟踪，将属于同一个攻击者的活动进行关联。

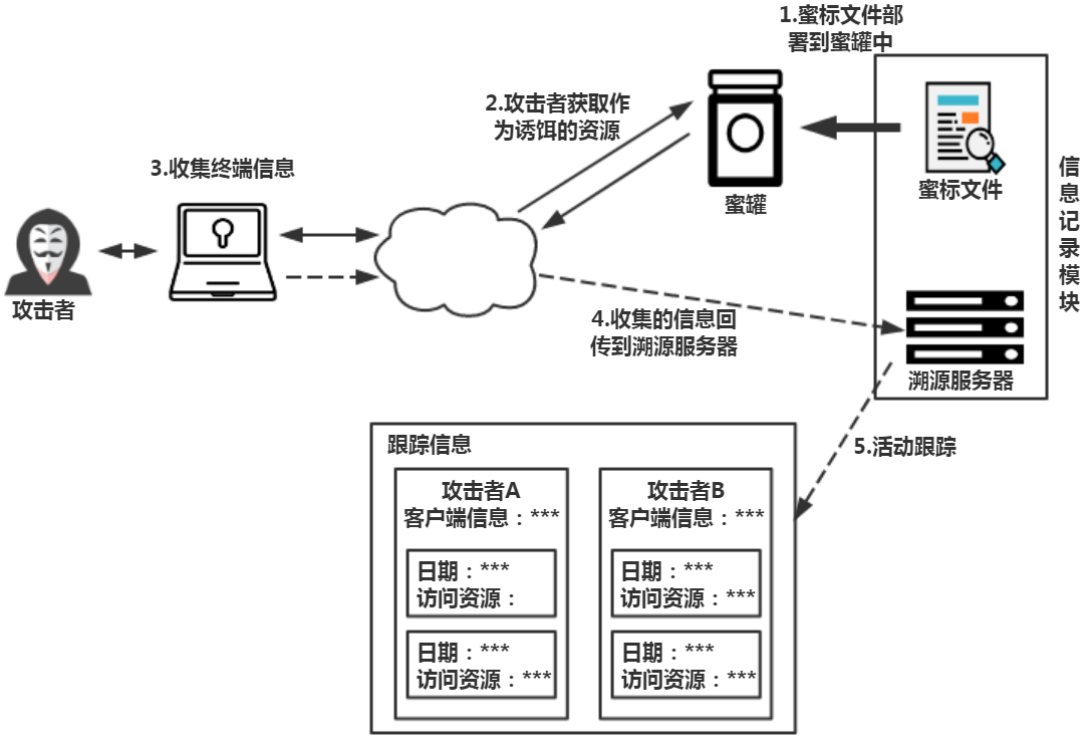

图 16 攻击溯源过程

当攻击者将我们蜜罐环境中的蜜标文件窃取并执行时，我们能够以蜜标为依据，分析获取攻击主机的 IP 地址、Windows 版本、浏览器指纹等相关信息，从而实现对多跳攻击窃密行为的追踪定位。当蜜标文件为我们设定的证券公司虚拟客户数据时，我们可以进一步监控该数据的流向以及倒卖路线，最终可为公安部门提供有效的情报数据分析。

第6章　总结与展望

信息安全不再局限于预防，更在于检测、响应和深度防御。构建全面、高效的网络威胁捕猎解决方案不仅有助于提高安全防御的有效性，还可以支持企业的整个安全生命周期。课题基于攻击链模型构建了网络威胁捕猎技术框架，以高交互式蜜罐伪装真实的目标主机网络环境，通过探针代理的方式监听相关服务，内嵌植入式的应用级业务分流对网络攻击进行诱骗，收集攻击者在蜜罐系统中的各种操作，进而分析总结其攻击手法和攻击意图等。

课题提出的网络威胁捕猎技术应用于证券交易所的展望：

（1）基于证券交易所安全防护自身特点，往往无法预先定义攻击者轮廓特征，正向情报收集面临效益少、命中率低的问题，且缺乏足够的恶意样本比对分析。通过部署蜜罐可以有效解决上述问题。本课题设计的分布式蜜罐系统在开放网络下部署启用多台蜜罐，每台蜜罐当中部署数种服务，如 HTTP、FTP、DNS、SSH 等，该类服务通常内嵌有明显漏洞，如匿名登录或知名的 0day 漏洞等，诱导攻击者利用，并通过脚本与攻击者进行一定程度的交互。在安全内网中搭建蜜罐统一管理和分析，实时或异步的方式分析蜜罐日志，提取威胁情报并与已有安全体系对接，更新有关策略与知识库，形成一个关于安全策略持续更新学习的闭环。

（2）区别于传统互联网的开源系统或者商务系统，证券交易所的相关系统一般只属于交易所独立特有的，虽然系统上线之前会经过各种安全测评，但谁也无法保证系统一定是没有任何漏洞的。又由于交易所系统独立特有的性质，互联网上很少会有针对交易所系统的研究文章，存在的安全风险虽然较小，但这也导致传统的安全防御设备难以部署有针对性的防御措施，倘若攻击者掌握某种系统

的 0day 漏洞，攻击行为可能让传统的安全设备毫无察觉。本课题提出的陷阱捕获方案，打造高交互性的蜜罐系统，可以搭建交易所仿真业务系统，并进行业务逻辑的攻击引流，若将攻击者成功引入到蜜罐系统中，我们不仅能获取到攻击者的所有攻击行为以及攻击工具，还能发现该业务系统的漏洞，并作用于真实业务系统，及时修复漏洞。

（3）区别于传统的网络攻击行为，针对证券交易所的攻击往往更具隐蔽性，被动的网络攻击防御措施往往难以察觉，或者在探测到攻击的初始阶段就阻断了攻击。但是伴随着新型的 APT 攻击的出现，很多传统安全技术手段已经无法满足对内部威胁的及时发现。攻击者可能通过社会工程学的手段得到用户的信息，使用网络钓鱼或者水坑攻击的方式进入企业内网个人电脑，但是要拿到有价值的内部敏感信息，攻击者需要进一步部署攻击链，包括获取凭证、内网资产扫描等探测工作。而由于证券交易所这种特殊的金融机构，往往难以在业务服务器上安装安全解决方案，甚至配置日志系统都不可以，那么，目前部署蜜罐是最好的解决方案。本课题提出的基于攻击链的蜜罐系统，可以有效的防御 APT 攻击中的内网探测风险。经典的攻击链模型则提供了一种纵深防御的概念，即在攻击最终造成损失的七步中，任何一步的察觉或者阻挡均能有效阻止和阻断。虽然攻击者可能通过某种途径拿到了企业内网个人电脑的权限，但在造成最后的损失之前，我们都有机会进行补救。这也是本课题的研究的目的之一：如果已经出现攻击者，在数据泄露之前能够检测到。

课题技术发展展望：

当前主动诱捕的追踪溯源技术还不完善，需要在攻击主机信息的隐蔽回传、对攻击者和攻击组织的溯源等方面继续深入研究。此外，全面地研究基于攻击链

的威胁捕猎技术，可以在深入理解攻击手法和攻击模式的基础上，帮助防御者实现攻击反制，有利于更好地保障关键信息系统和网络的安全运行，加强关键网络对攻击入侵的防御能力，提升各机构的网络威胁预警能力、网络攻击监测能力、以及安全事件的快速应急响应能力。

参考文献

[1]王 瑶，艾中良，张先国. 基于蜜标和蜜罐的追踪溯源技术研究与实现[J]. 信息技术.2018, 3:108-112

[2]诸葛建伟，唐勇，韩心慧，等.蜜罐技术研究与应用进展[J].软件学报.2013,24(4): 825-842

[3]杨德全，刘卫民，俞宙. 基于蜜罐的主动防御应用研究[J]. 网络与信息安全学报. 2018 ,4(1):57:63

[4]吕毅.基于攻击视角完善信息安全弹性防御体系的思考[n].金融电子化:2018-6-28(6)

[5]绿盟科技.基于攻击链的威胁感知系统[EB/OL].https://www.freebuf.com/news/83102.html,2015-10-27.

[6]bt0sea.态势感知攻击链分析-Redis 未授权访问检测[EB/OL].http://www.4hou.com/technology/13479.html,2018-9-8.

[7]段凯元，何申，程叶霞. 基基于 Kippo 蜜罐的 SSH 暴力破解行为分析[J]. 信息安全与通信保密，2014(3):104-109.

[8]elknot .企业安全建设—模块化蜜罐平台的设计思路与想法[EB/OL].https://xz.aliyun.com/t/1885/,2018-01-03.

[9] 信安之路.基于 docker 的蜜罐学习[EB/OL].https://mp.weixin.qq.com/s/C7RqU6NfOKgYyN_HsFxXNw,2017-07-29.

[10]安全值团队.2017 年证券行业网络安全报告[EB/OL].http://www.sohu.com/a/218372271_490113,2018-01-23.

[11]百度安全应急响应中心.被动防御之蜜网实践（一）[EB/OL].https://www.secrss.com/articles/3825,2018-07-10.

[12]李秋锐. 基于蜜罐网络的邮件捕获系统分析与部署[J]. 信息网络安全，2012(1): 64-67.

[13]陈周国，蒲石，郝尧，等. 网络攻击追踪溯源层次分析[J]. 计算机系统应用，2014，23(1): 1-7

[14]崔嘉. 蜜罐技术用于网络安全的分析与研究[J]. 信息安全与技术，2016，7(6):11-13.

[15]Naruoka H，Matsuta M，Machii W，et al. ICS Honeypot System Based on Attacker′s Human Factors [J] . Procedia Manufacturing，2015，30(3):65-69.

[16]Pham V H，Dacier M. Honeypot Traces Forensics: The Observation Viewpoint Matters [J] . Future Generation Computer Systems，2011，27(5):539-546.

[17]NASIR Q, AL-MOUSA Z A. Honeypots aiding network forensics: challenges and notions[J].Journal of Communications,2013,8(11):53-84.