ATT&CK在金融行业的落地实践

中国工商银行业务研发中心
安全攻防实验室
高级研究员 李亚敏

中国工商银行
业务研发中心

目录

CONTENTS

01. ATT&CK研究工作背景

02. 基于ATT&CK的安全研究

03. ATT&CK在金融行业的落地实践

04. ATT&CK在金融行业应用的前景展望

PART 01

ATT&CK研究工作背景

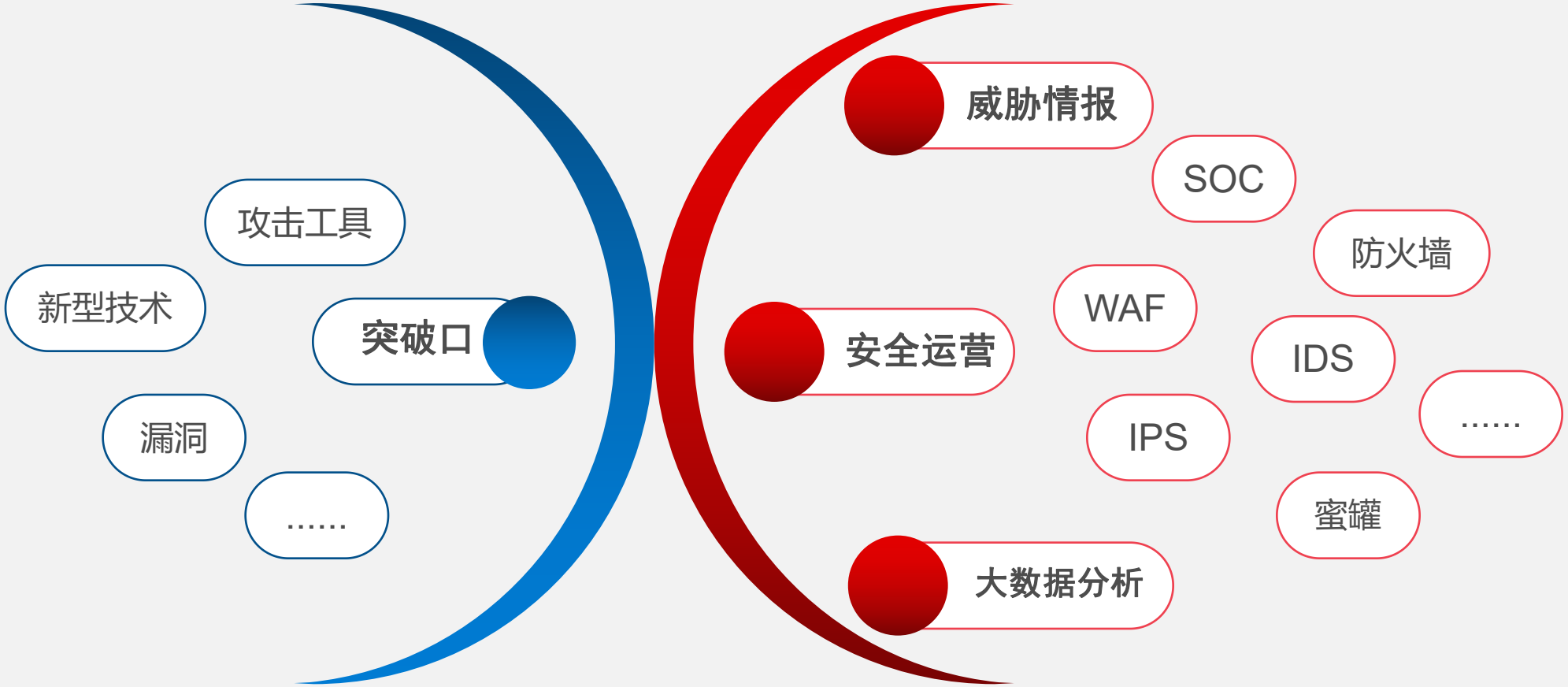
一、全球针对金融行业的网络入侵事件频发，网络安全威胁向体系化组织化演变

二、金融行业面临的潜在风险远超实际攻击

面临的实际攻击

面临的潜在风险

三、攻防角色的不对等属性



解决思路


攻击体系化
加强体系化攻击的应对能力
需要体系化的攻击知识库
防守局限性
加强潜在风险的预知能力
需要有效的威胁建模思路
攻防不对等
加强对攻击者行为的了解和防守有效性
需要全面了解TTP

ATT&CK研究工作背景

攻击知识库、威胁建模、TTP与ATT&CK

攻击知识库

威胁建模

TTP

ATT&CK

痛苦金字塔模型

PART 02

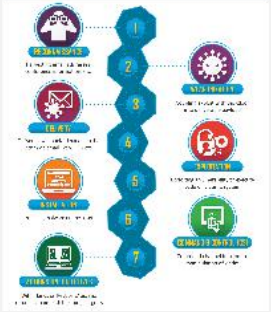
基于ATT&CK的安全研究

ATT&CK的相关模型研究

由洛克希德-马丁公司提出，描述的是针对性的分阶段攻击，每一环节都是对攻击做出侦测和反应的机会。

高级模型

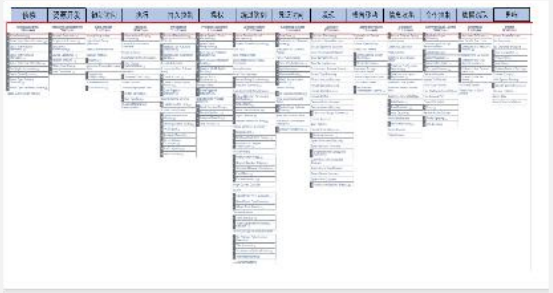
THE CYBER KILL CHAIN®



MITRE公司基于真实观察的网络攻击者战术、技术、过程等数据形成的攻击行为知识库，为不同组织机构提升自身安全能力提供强大的战术、技术和工具支撑。

中级模型

ATT&CK®

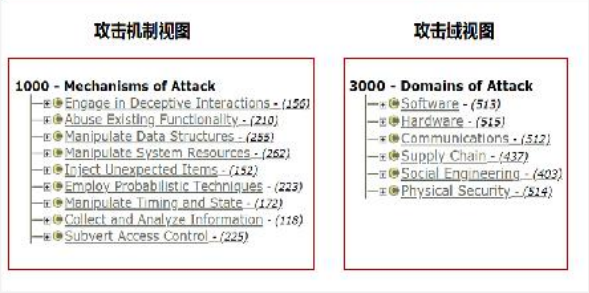


MITRE在2007年发布的一个包含攻击者为利用网络功能中的已知弱点所采用的已知攻击模式的全面的字典，是一种可用于识别、收集、完善和分享攻击模式的标准机制。

低级模型

CAPEC™

capec.mitre.org

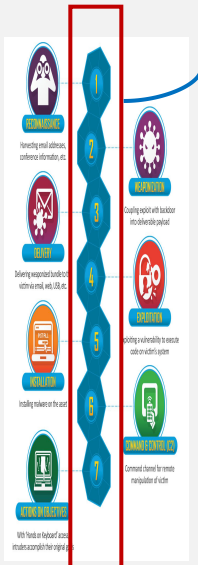


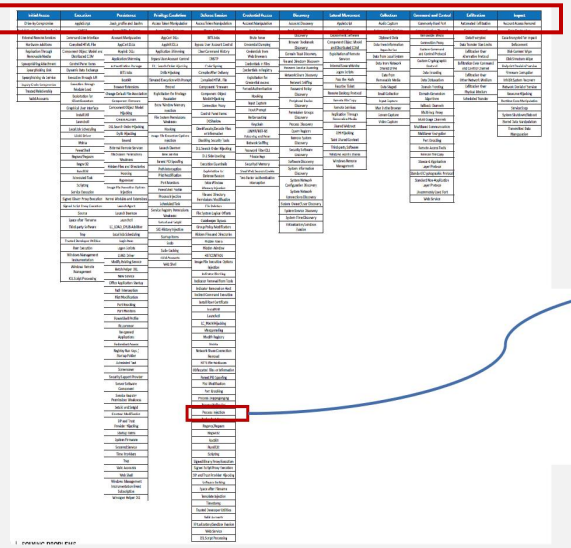
基于ATT&CK的安全研究

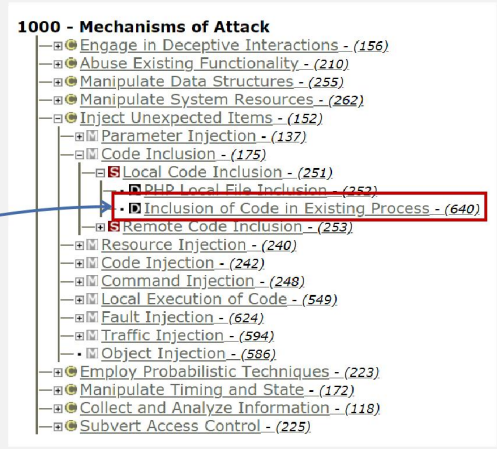
Kill chain-ATT&CK-CAPEC之间的关联关系

ATT&CK for Enterprise->Defense Evasion->Process Injection (T1055)

(V)CAPEC攻击机制-(1000)
->(C)Inject Unexpected Items-(152)
->(M)Code Inclusion-(175)
->(S)Local Code Inclusion-(137)
->(D)Inclusion of Code in Existing Process-(640)







THE CYBER KILL CHAIN®

ATT&CK®

CAPEC™ capec.mitre.org

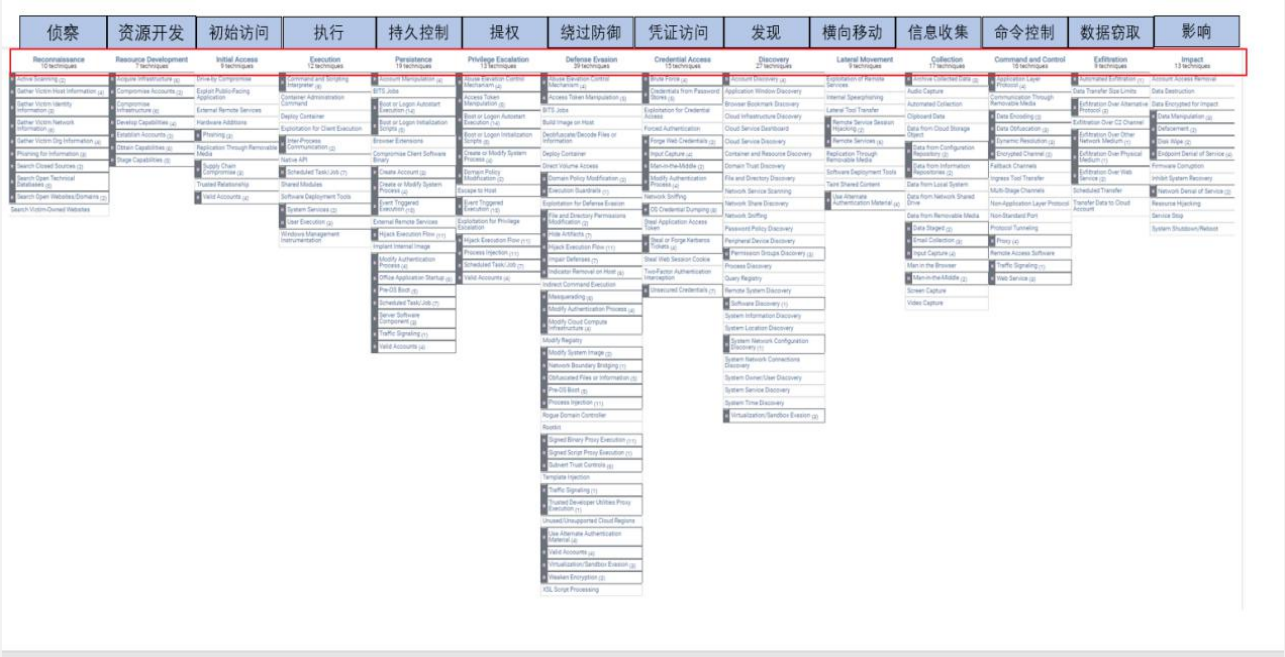
FCC FINANCIAL COMPUTER OF CHINA

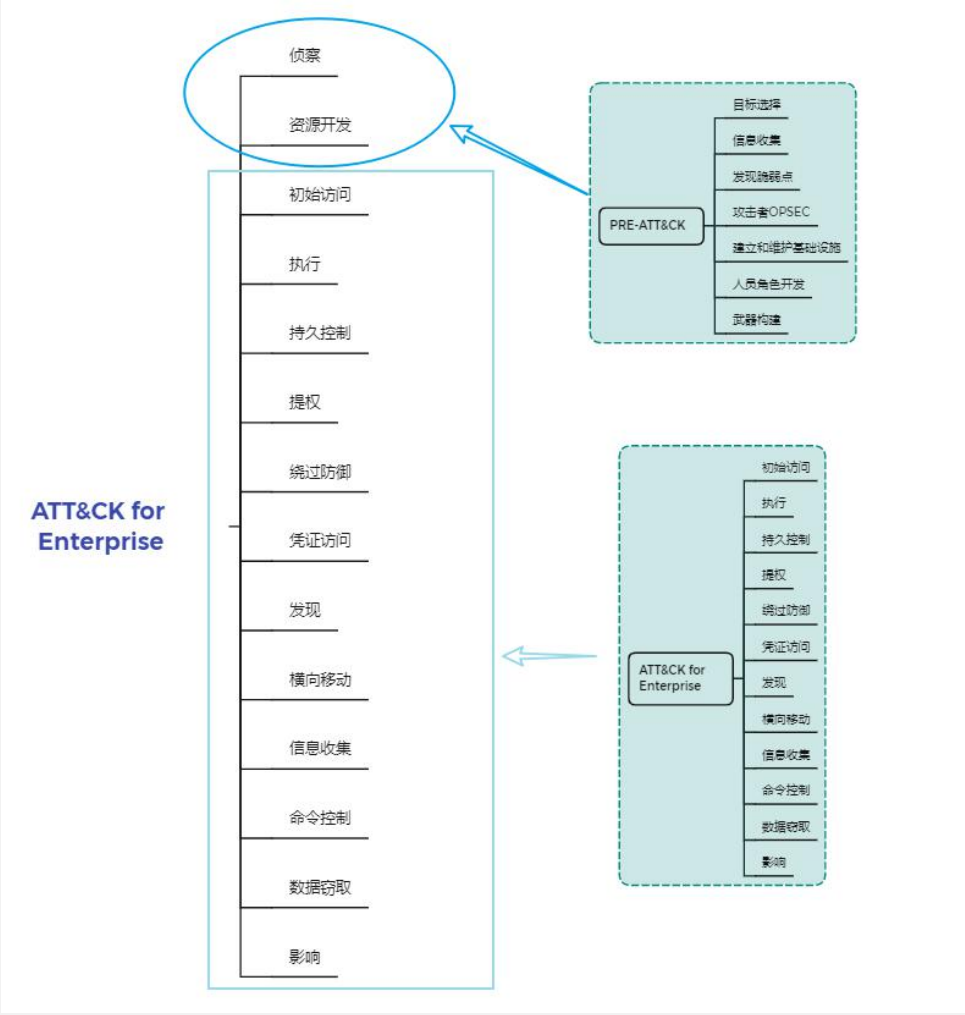
FCC30+

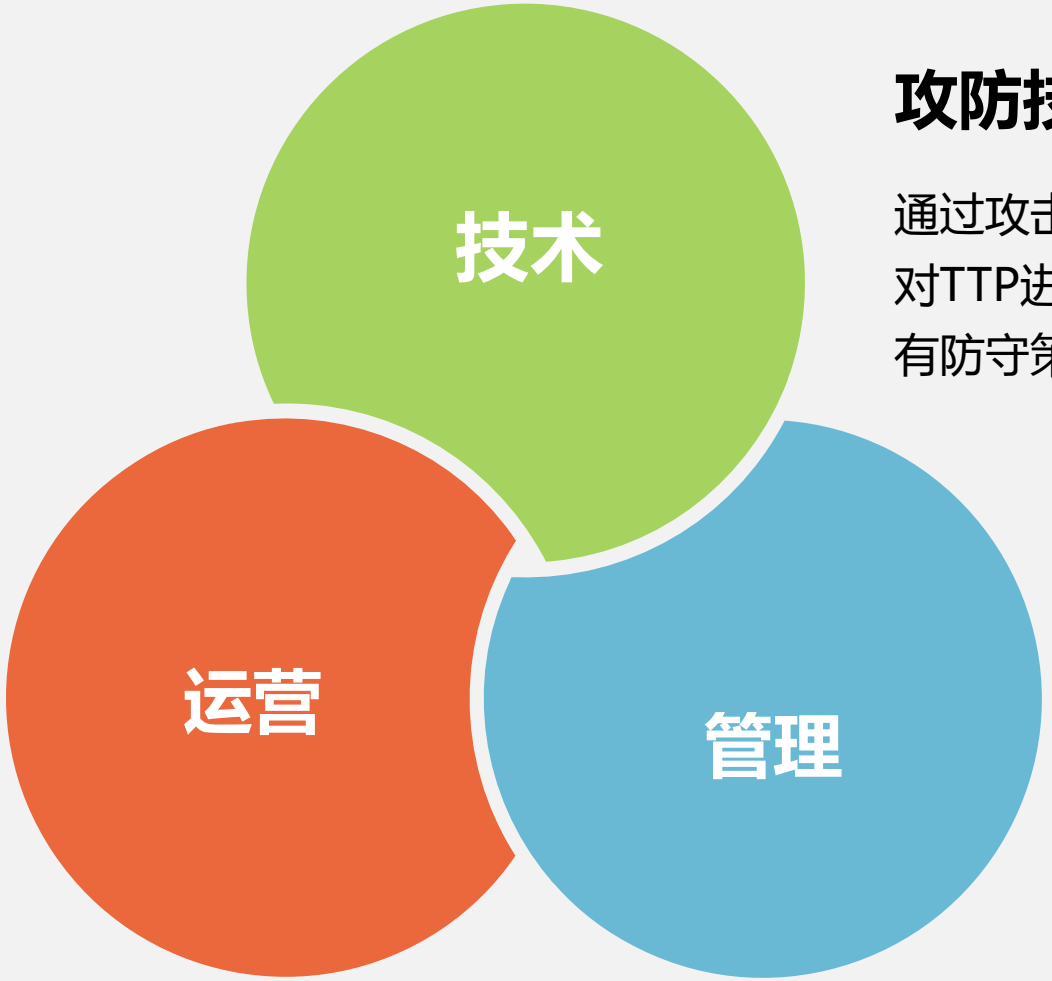
微信扫一扫
关注该公众号

ATT&CK简介

目前最新版ATT&CK Matrix for Enterprise包括 14项战术，185项技术，367项子技术，42种缓解措施。ATT&CK框架还囊括了122个黑客组织和其发起攻击时常用的585个工具梳理，同时还包括这些不同黑客组织攻击的行业和组织类型。







攻防技术

通过攻击技术提升，在实践工作中对TTP进行深刻了解，并且审视已有防守策略

威胁建模

通过更加细粒度的威胁模型构建，提升潜在风险应对能力

演练模式

通过体系化的、专项攻防演练模式，增强对体系化攻击的应对能力

PART 03

ATT&CK在金融行业的落地实践

ATT&CK在金融行业的落地实践

管理层面——攻防演练模式

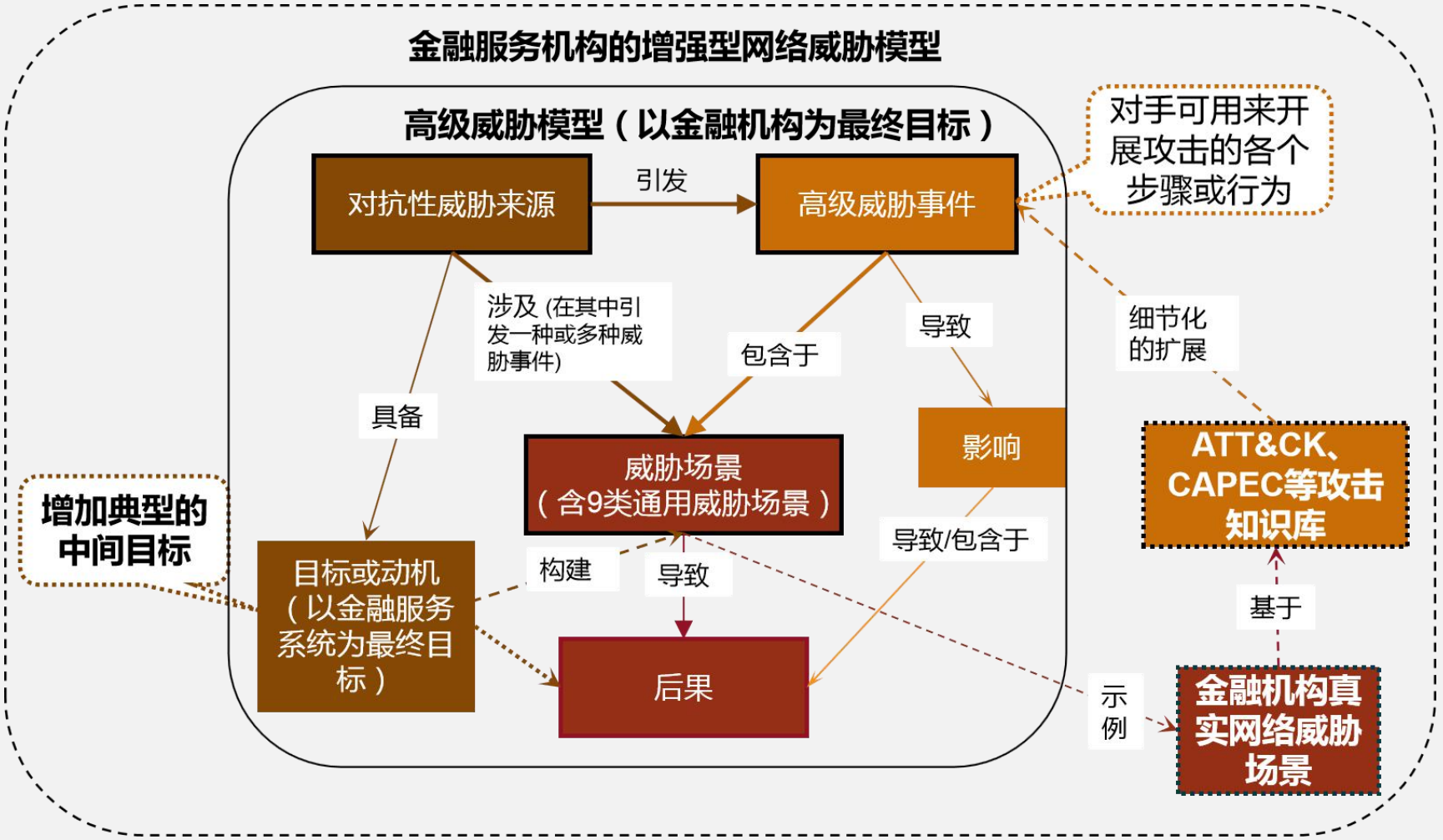
在内部攻防演练中基于**ATT&CK**框架和典型攻击阶段，选取适用度较高的攻击技术开展专项演练

攻击目标： 对组织进行欺诈或盗窃
角色类型： 犯罪分子（个人或有组织的团体）
网络影响： 数据污染、修改或添加
组织后果： 财务损失、声誉受损
威胁场景简介： 使用鱼叉式网络钓鱼感染银行中的系统，收集有关用户和系统的信息，使用用户角色以多种方式窃取资金，包括通过资金转账或在线银行将资金从其他帐户转移到自己的帐户，修改帐户数据库 ，并通过ATM提款。

威胁事件/行为	事件简要描述
提供针对性的恶意软件以控制内部系统或泄露数据 [ATT&CK：入口点-带有恶意附件的鱼叉式钓鱼T1092、带有恶意链接的鱼叉式钓鱼T1093]	攻击者感染了银行员工的计算机，并传播了Carbanak恶意软件，该恶意软件为攻击者提供了远程访问和控制功能。然后，他们能够监视受感染的系统，并找到将控制扩展到目标组织内其他平台的方法
获取与用户帐户、进程、服务或域相关的特权 [ATT&CK：指挥与控制-远程访问工具T1219]	进入系统后，该恶意软件对员工计算机的桌面显示进行了视频捕获。攻击者使用此视频来了解目标组织的业务流程
通过污染或破坏关键数据而导致完整性损失 [ATT&CK：入口点-有效账户T1078]	通过破坏不同用户的系统，攻击者可根据每个员工的角色来利用业务的不同方面，如操纵银行的业务数据库向帐户中添加资金以便以后转账，以及将折衷方案扩展到ATM网络以强制现金分发
通过多种方式来逃避检测 [ATT&CK：执行-Rundll32 T1085、防御回避-Web服务T1102]	使用与银行管理员所依赖的相同的工具，以使攻击者逃避检测。 例如，威胁参与者利用了诸如虚拟网络控制台（VNC）、PuTTY和安全外壳协议（SSH）之类的工具
通过代码签名来降低被检测到的风险 [ATT&CK：防御回避-代码签名 T1116]	Carbanak威胁参与者使用数字签名来进一步降低被检测到的风险
通过权限维持和持久的身份隐藏来获取更多利益 [ATT&CK：防御回避- HISTCONTROL T1148]	通过避免长时间的侦查，攻击者能够在从受害者机构窃取钱财方面取得相当大的成功
通过攻击过程了解受害机构内部的网络结构 [ATT&CK：发现-网络服务扫描T1046]	在活动期间，攻击者了解了受感染机构中网络的详细信息
通过了解到的内部网络结构来进一步横向探索 [ATT&CK：横向渗透]	在活动期间，Carbanak威胁参与者通过观察用户和窃取凭据来进行横向移动
获取机构内部敏感数据或用户数据 [ATT&CK：收集]	在整个行动过程中，攻击者收集并窃取了宝贵的数据
通过恶意软件远程控制受害用户或系统 [ATT&CK：命令和控制]	攻击者使用Carbanak软件的远程控制功能在受攻击的系统上执行和协调活动

基于**ATT&CK**框架中对APT组织的TTP描述，选取典型的、特别是攻击过金融行业的APT组织攻击路径，模拟攻击自身信息系统

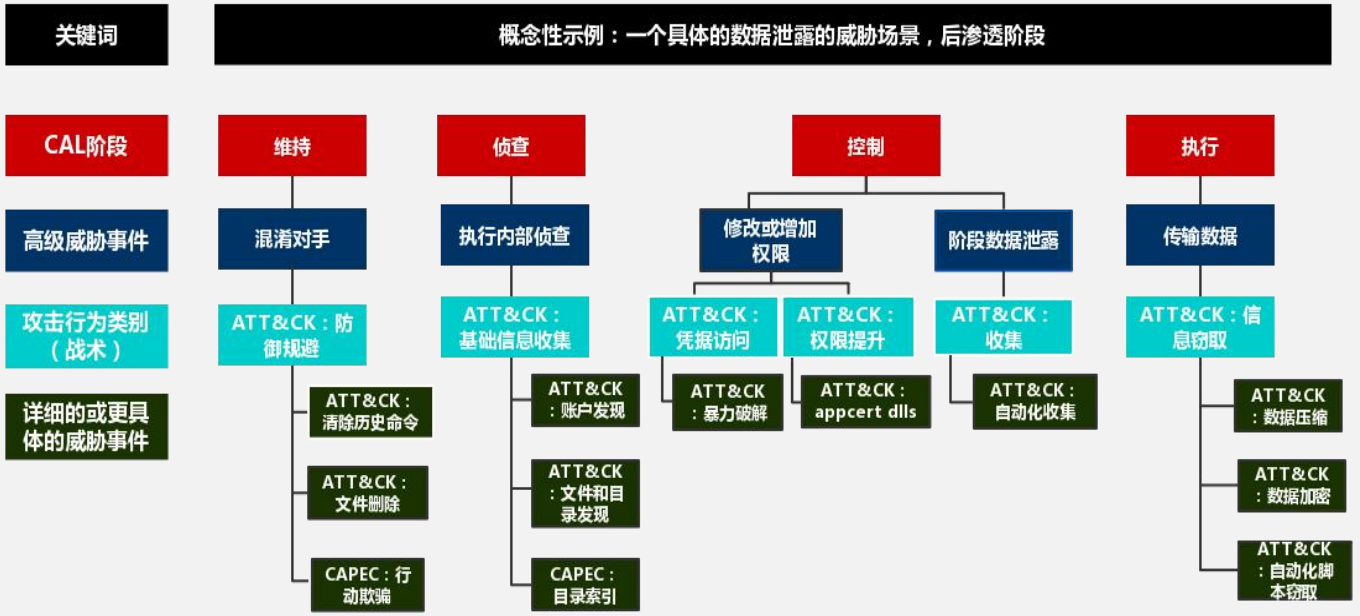
运营层面——威胁模型构建


金融服务机构的增强型网络威胁模型
高级威胁模型（以金融机构为最终目标）
对抗性威胁来源
引发
高级威胁事件
对手可用来开展攻击的各个步骤或行为
涉及（在其中引发一种或多种威胁事件）
包含于
导致
细节化的扩展
具备
影响
ATT&CK、CAPEC等攻击知识库
威胁场景（含9类通用威胁场景）
增加典型的中间目标
目标或动机（以金融服务系统为最终目标）
构建
导致
导致/包含于
基于
后果
示例
金融机构真实网络威胁场景

ATT&CK在金融行业的落地实践

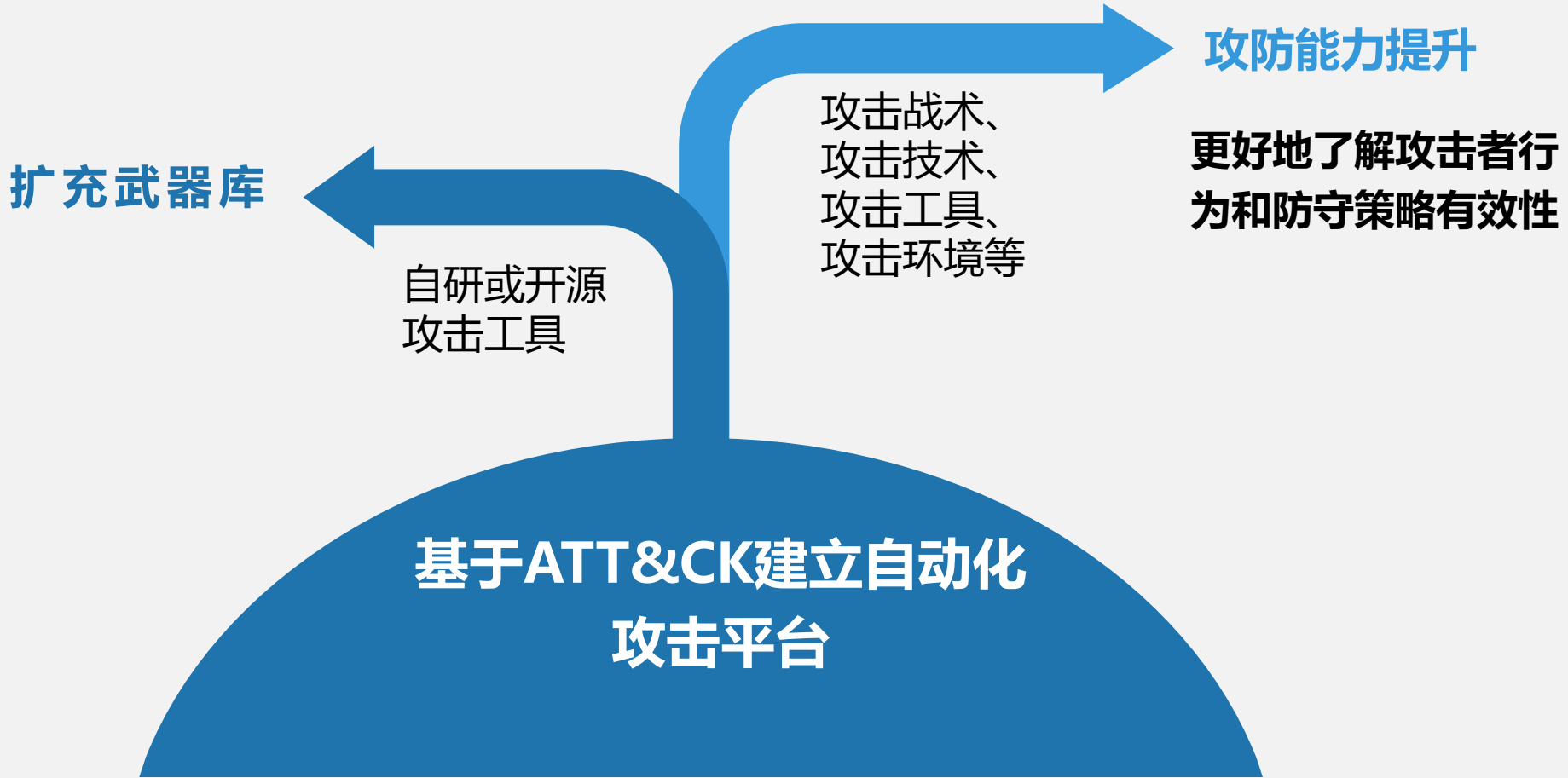
运营层面——威胁模型构建

通用威胁场景	典型的威胁参与者	典型的最终目标	典型的中间目标
突破口/泄露	不法分子（个人或组织）、被策反/被贿赂的内部员工、寻找有竞争力的信息以出售给竞争对手或内部交易客户的不法分子	客户信息资料库、战略规划信息、预测应用程序和数据库	身份和访问管理（IdAM）服务和数据（以获得对最终目标的访问）、目录服务（确定最终目标）、 防火墙和外部连接（泄露敏感信息）、审计服务和数据（隐藏行动证据）



通用威胁场景	典型的威胁参与者	CAL阶段（示例）	高级威胁事件（示例）	攻击行为类别（示例）	更详细的威胁事件（示例）	典型的最终目标
突破口/泄露	不法分子（个人或团体）、不满的内部员工、为获取有竞争力的信息，或将信息出售给竞争对手或内部交易客户的不法分子	维持	混淆对手	ATT&CK：防御规避	ATT&CK：清除历史命令、文件删除CAPEC：行动欺骗	客户信息资料库;战略规划信息；预测应用程序和数据库
		侦查	执行内部侦查	ATT&CK：基础信息收集	ATT&CK：账户发现、文件和目录发现CAPEC：目录索引	
		控制	修改或增加权限	ATT&CK：凭据访问	ATT&CK：暴力破解	
				ATT&CK：权限提升	ATT&CK：Appcert DLLs	
			数据泄露	ATT&CK：收集	ATT&CK：自动化收集	
		执行	传输数据	ATT&CK：信息窃取	ATT&CK：数据压缩、数据加密、自动化脚本窃取	

技术层面-攻防能力提升


攻防能力提升
更好地了解攻击者行为和防守策略有效性
攻击战术、
攻击技术、
攻击工具、
攻击环境等
扩充武器库
自研或开源
攻击工具
基于ATT&CK建立自动化
攻击平台

技术层面-攻防能力提升


防护系统平台
资产管理平台
漏洞管理平台
……
自动化信息收集
探测扫描信息
内部信息获取
自动化漏洞扫描
被动扫描任务
漏洞扫描任务
自动化边界突破
攻击工具集成
利用代码集成
其它纵深攻击
攻击工具集成
内部信息探测
分布式资源池
协同作战管理

PART 04

ATT&CK在金融行业应用的前景展望

ATT&CK在金融行业应用的前景展望

统一行业安全语言

- 行业级安全能力评估体系

协同联动，信息共享

- 行业级的威胁情报共享
- 与金融同业加强合作
- 建立跨行业的安全协防应急机制

ICBC

中国工商银行

业务研发中心

Thanks!

FCC30+

微信扫一扫
关注该公众号

扫一扫上面的二维码图案，加我微信