**MITRE ATT&CK威胁检测框架研究心得分享**

**青藤云CEO-张福先生**

**张：**大家好，我是青藤云安全的CEO张福，和大家一样，我也是个安全技术爱好者。感谢聂总的邀请，今天有幸能在这里给大家分享一下我们这段时间对MITRE ATT&CK的研究，希望能和大家多沟通交流，如果有什么没说到的，也欢迎大家多多提问哈。

**张：**讲MITRE ATT&CK之前，首先我们来谈一下站在攻防角度，作为一个防守方会遇到的困难。

**张：**由于敌暗我明，防守方始终处于一个被动地位，因此，防御总是比进攻要难。这个情况在网络安全中尤其普遍。在网络安全领域，攻击方始终拥有取之不竭、用之不尽的网络弹药，可以对组织机构随意发起攻击，而防守方则必须每次都要成功地防止攻击者攻击成功。

**张：**由于这种天生的劣势，防守方始终会为以下问题而困扰：

1. 我们的防御方案有效吗？
2. 我们能检测到APT攻击吗？
3. 我们收集的数据有用吗？
4. 我们的安全工具覆盖范围是否有重叠呢？

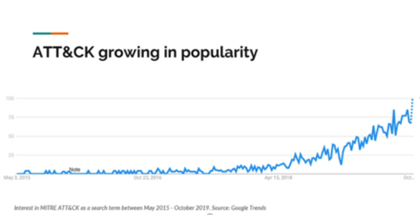
5这款新产品对于我们组织机构的防御有用吗？......等等

**张：**因为缺乏一个明确的，可衡量，可落地的标准，所以防守方对于入侵检测通常会陷入不可知和不确定的状态中，从而无法有效的弥补自己的短板。

**张：**因为缺乏一个明确的，可衡量，可落地的标准，所以防守方对于入侵检测通常会陷入不可知和不确定的状态中，从而无法有效的弥补自己的短板。

**张：**MITRE为了解决防御者面临的困境，基于现实中发生的真实APT攻击事件，创建了一个对抗战术和技术知识库，即MITRE ATT&CK框架。由于该框架内容丰富，实战性强，最近几年发展得炙手可热，得到了业内的广泛关注。

下图显示了Google trends 对ATT&CK框架的热度发展趋势：



**张：**以上是背景介绍,下面我们开始今天的主要内容，分为三个部分：

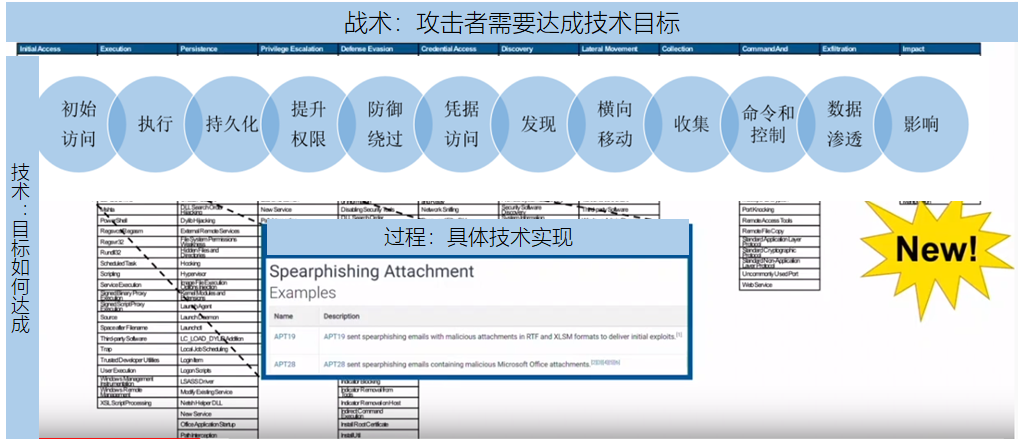
**一、MITRE与ATT&CK概念介绍；**

**二、ATT&CK背后的核心设计思想；**

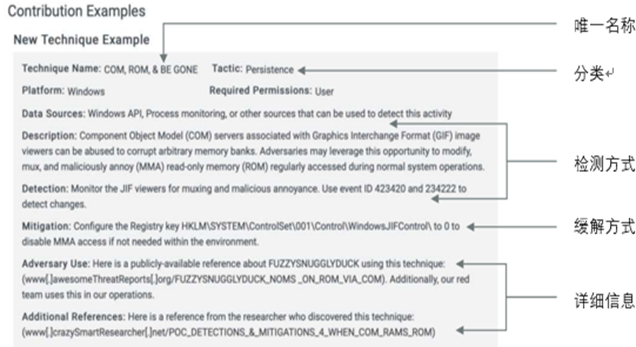
**三、ATT&CK的四大使用场景；**

**下面是第一部分：MITRE与ATT&CK概念介绍：**

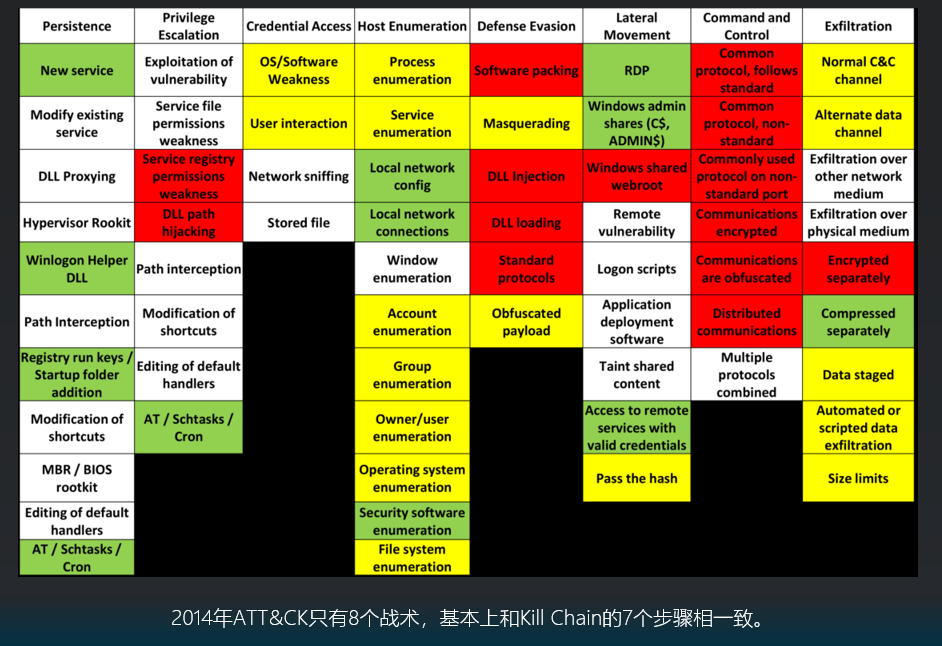
* 首先提一下MITRE是谁：MITRE是美国NIST标准化组织选择的专注于网络安全的组织，由美国联邦政府资助。很多安全标准都MITRE制定的，比如有名的漏洞CVE编号规则以及威胁情报格式STIX。所以ATT&CK非常有影响力，而且未来能成为一个公认的标准，今年RSA大会上MITRE也在大力推广这个框架。
* ATT&CK是对抗战术、技术和常识的缩写。战术（Tactics）代表了实施ATT&CK技术的“原因”。战术是攻击者执行某项行动的战术目标。战术提供了各项技术的环境类别，并涵盖了攻击者在攻击时执行活动的标准、高级标记，例如持久化、信息发现、横向移动、文件执行和数据泄露。
* 技术（Techniques）代表攻击者通过执行动作来实现战术目标的“方式”。例如，攻击者可能会转储凭据，以便访问网络中的有用凭据，之后可能会使用这些凭据进行横向移动。技术也可以表示攻击者通过执行一个动作要获取“内容”。这与“发现”战术有明显的区别，因为技术侧重的是攻击者采取特定动作是为了获取什么类型的信息。



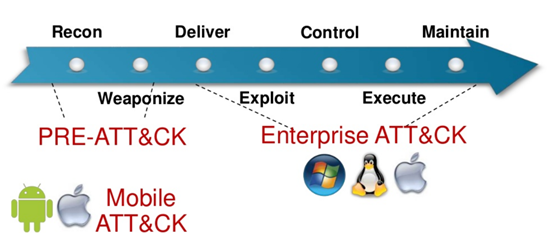
* 由于战术代表了攻击者的战术目标，因此随着时间的推移，这些战术将会保持相对不变，因为攻击者的目标不太可能改变。战术将攻击者试图完成的任务的各方面内容与他们运行的平台和领域结合了起来。通常，不管是在哪个平台上，这些目标都是相似的，这就是为什么Enterprise ATT&CK战术在Windows、MacOS和Linux系统中基本保持一致。
* 下面这张图是ATT&CK里面“技术”的说明图：



* 技术是ATT&CK的基础，代表攻击者进行某个动作或攻击者通过执行某项动作而了解到的信息。每一个技术都包括唯一的名称、分类、检测方式、缓解方式、详细信息等。
* 那么ATT&CK和KillChain是什么关系呢？在早期，ATT&CK模型是在洛克希德-马丁公司提出的Kill Chain模型的基础上，构建了一套更细粒度、更易共享的知识模型和框架。
* 如下图所示，2014年ATT&CK只有8个战术，基本上和Kill Chain的7个步骤相一致。



* 现在经过几年的发展，整个矩阵内容变得丰富， 被拆分为PRE-ATT&CK和ATT&CK for Enterprise，其中PRE-ATT&CK覆盖了Kill Chain模型的前两个阶段，包含了与攻击者尝试利用特定目标网络或系统漏洞进行相关操作有关的战术和技术。ATT&CK for Enterprise覆盖了Kill Chain的后五个阶段。



* 但是，ATT&CK的战术跟洛克希德-马丁的网络杀伤链不一样，并没有遵循任何线性顺序。相反，攻击者可以随意切换战术来实现最终目标。没有一种战术比其它战术更重要。组织机构必须对当前覆盖范围进行分析，评估组织面临的风险，并采用适当措施来减小差距。
* 另外，除了在Kill Chain战术的基础上更加细化之外，ATT&CK还描述了可以在每个阶段使用的技术，而Kill Chain则没有这些内容。
* 另外，除了在Kill Chain战术的基础上更加细化之外，ATT&CK还描述了可以在每个阶段使用的技术，而Kill Chain则没有这些内容。
* ***以上是第一部分：***

**张: 下面是第二部分：ATT&CK背后的核心设计思想**

* ATT&CK背后的设计思想是十分明确的，主要有三个核心思想：

**1、始终从攻击角度看待问题，保持攻击者的视角。**

**2、不断进行实践证明，通过跟踪APT活动来更新技术。**

**3、进行抽象提炼，通过抽象提炼，将进攻行动与防御对策联系起来。**

我们先说说第1个设计思想：用攻击的视角看问题：

* ATT&CK在其术语以及模型中介绍的战术和技术是从攻击者的视角出发的。相比之下，许多安全模型从防御者的视角自上而下地介绍安全目标（例如CIA模型），有的则侧重于漏洞评级（例如CVSS），有的则主要考虑风险计算（例如DREAD）。
* ATT&CK使用攻击者的视角，比从纯粹的防御角度更容易理解攻击者的行动和潜在对策。对于检测，其它防御模型会向防御者显示警报，而不提供引起警报的事件的任何上下文，因此无法很好的理解攻击者的意图

第2个设计思想：不断地通过追踪真实的APT攻击，来获得最新的技术：

* 由于对真实的APT攻击进行了追踪和分析，提炼出了技术点，因此，能够准确地描述正在发生或可能发生的在野攻击。
* 通过继续不断地积累ATT&CK知识库，使得该模型是基于可能遇到的实际威胁来完善进化的，有很大的实用价值而不是理论价值。

第3个设计思想：通过“适当”的抽象，可以将进攻和防御联系起来：

* ATT&CK框架对相关的对抗战术和技术进行抽象提炼是ATT&CK与其它类型威胁模型之间的重要区别所在。各种针对攻击者生命周期的高级抽象模型，例如Cyber Kill Chain、Microsoft STRIDE等，对于理解高级过程和攻击者目标很有用。但是，这些模型不能有效地传达攻击者要采取哪些动作、一个动作与另一个动作之间的关系、动作序列与攻击者战术目标的关系、以及这些动作与数据源、防御措施、配置和其它用于平台与域安全的应对措施之间的关系。
* ATT&CK技术的抽象提炼的价值在于：

1、通过抽象提炼，形成一个通用分类法，让攻击者和防御者都可以理解单项对抗行为及其目标。

2、通过抽象提炼，完成了适当的分类，将攻击者的行为和具体的防御方式联系起来。

* 本质上是通过“适当”的抽象，既不很模糊，也不是太具体，而是很适度的抽象，给攻击和防御之间建立起了一个标准化的“语言”，能够让攻防双方站在同一语境下对话。
* ***以上是第二部分：***

**张：最后说一下ATT&CK的实际使用场景，主要有以下四个用途；**

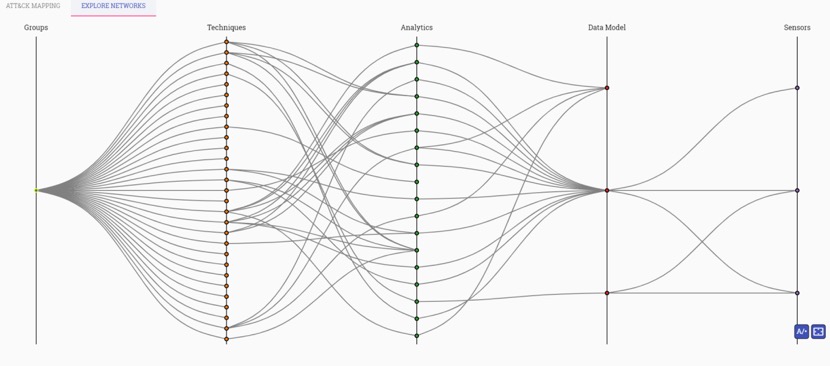
1、威胁情报：使用ATT&CK框架来识别攻击组织；

2、模拟攻击：基于ATT&CK进行红蓝攻防演练；

3、检测分析：基于具体的”技术“，有效增强检测能力；

4、评估改进：将解决方案映射到ATT&CK威胁模型，发现并弥补差距。

* 网络**威胁情报**（CTI）的价值在于了解攻击者的行为，并用这些信息来改善决策。对于希望开始使用ATT&CK框架来收集威胁情报的小型组织机构，可以先从一个威胁组织着手，并按照框架中的结构检查其行为。
* 这样能通过攻击组织使用的技术和行为，来定位攻击组织。另外也可以随着时间的推移，来分析同一个攻击组织的技术变化。
* **模拟攻击：**使用ATT&CK来组织红队计划开展一系列基于威胁的安全测试，模拟真实攻击者的技术，关注技术行为，即便没有红队，防御者可以先使用红队工具来尝试，并使用ATT&CK打造一支成熟的红队。
* 让企业的团队选择不同的ATT&CK技术，讨论如何使用不同步骤来执行攻击行为，邀请威胁情报分析人员谈谈攻击者是如何使用的，将ATT&CK作为通用语言与蓝队沟通，让红队主动模拟ATT&CK技术，制定自己的攻击者模拟计划。
* 这和一般的渗透测试有什么不同呢？主要在于可以模拟多个组织的攻击，而非单一组织的。
* **检测分析：**检测分析可以用CAR（Cyber Analytics Repository）安全分析库项目举例。主要是针对ATT&CK的威胁检测和追踪。这个项目主要基于四点考虑：根据ATT&CK模型确认攻击优先级；确认实际分析方法；根据攻击者行为确认要收集的数据；确认数据收集主体sensor的数据收集能力。后面三个方面与的Analytics、Data Model、Sensor相对应。这个分析库是由对每一项攻击技术的具体分析构成的。
* 大家可以看看这张图，显示了哪些数据源可以用来检测哪些攻击技术:



*这个图回头我会发下链接，这里只是个示意*

* **评估改进：**首先进行差距分析，弄清楚“我们现在在哪儿”，ATT&CK有助于企业确定自身在人员、流程和技术方面的差距，根据可见性来决定你要收集（和购买）哪些内容：你的差距在哪里？你还可以选择其它哪些工具？这些工具会帮助你建立更有效的防御措施吗？帮助企业拓宽安全视野，不仅仅是局限于检测；加强认识，了解可能需要承受哪些方面的风险；哪些内容是你无法检测或缓解，检查你的安全预算与计划，实现资源的优化利用。
* 之前企业做差距分析，是做自身安全状况的差距分析，分析后的内容主要用于指导安全体系的建设。但是并无法很明确的了解自身防御和检测能力的差距，ATT&CK可以在检测覆盖度上（明确分析出哪些攻击技术在目前的安全体系里无法覆盖），以及检测深度上（比如留后门一共有哪些姿势）提供一个清晰的差距分析，指导企业加强入侵检测能力.
* ***以上是第三部分：***
* 今天的分享就到这里，因为ATT&CK是一个非常庞大的框架，所以无法在这么短时间内说的足够透彻，时间也没控制好，在这里向大家致歉。
* Q&A环节：A-->张总

Q:「 张福-青藤云安全: 1.威胁情报：使用ATT&CK框架来识别攻击组织

2.模拟攻击：基于ATT&CK进行红蓝攻防演练

3.检测分析：基于具体的”技术“，有效增强检测能力

4.评估改进：将解决方案映射到ATT&CK威胁模型，发现并弥补差距 」

- - - - - - - - - - - - - - -

请问一下，业内有哪些甲方在用这个落地的么？有没有一些具体的实践可以参考

A：张：我们之后会出一个ATT&CK的使用手册，有需要的同学可以找我们要一本，另外关于ATT&CK的更多实战指南，可以参考：<https://mp.weixin.qq.com/s/-K5B_ZdxLxN7oSCVfWMWpg>

* ATT&CK是非常具体可以落地的，比如里面一个留后门的方式，大家可以试试；
* 把cmd.exe拷贝为C:\Program.exe
* 你们以后会有各种惊喜

Q:1、攻击者计划性的执行转储凭据的动作，对防守方如何能有效或及时发现？凭据如何保护才能真正有效？

A：@刘强-联易融金融 可以的，每种组织使用的技巧都不一样，连起来就是个类似DNA的东西；

1. 针对DLL劫持利⽤搜索顺序来加载恶意DLL以代替合法DLL，如何避免被恶意加载而导致被持久化攻击？

A：这个ATT&CK里有检测方法的，判断同一进程是否有同名的dll，很有效。

Q：如果说是指导理论与原来的渗透测试指导区别在哪里呢？

A：我们现在正在对每种ATT&CK的攻击技术进行还原实现，写出测试工具和检测工具，回头也可以提供给大家试试。

Q：印象中ATT&CK也有一些详细程度不高的TTPs，比如 面向公网的服务被利用 。。针对这种比较粗的TTPs，有什么解读或者应对么？

A：@美团赵弼政 有的，需要梳理具体的use case，就是挨个整理，工作量巨大。

Q：青藤云现在完成度如何？

A：我们现在正在逐步复现技术和写检测规则，目前每周都会进展一部分。

A：这就是我说的深度问题，比如webshell在ATT&CK里就是一个技术，但是其实有很多use case，每种代表了一种webshell姿势。

Q：甲方如何应用呢?

Q：手册里面会有这种整理的案例嘛？

A:手册里会有案例

Q：比如检测webshell，能检测1个，也能号称覆盖了这一个技术，但是其实我们期望是能检测出大多数webshell，才算是覆盖了。这样对ATT&CK的覆盖率，如何评价啊

A：这个我们会给use case，比如给出50种不同技巧的，可以测试覆盖率，我们对use case的梳理也只是一部分，最好能大家一起来。

Q：但是这只是针对1个点，如果ATT&CK的200多个点，都要这种逻辑去梳理，汇总总的覆盖率，有什么好的实践思路不？

A：这个我想可以建立一个开源项目，大家一起来补充case。

Q:而且200多个点应该也有分轻重缓急的吧。。。这个你们先聚焦哪些点，有什么逻辑思考么?理由是什么啊，背后是怎么思考的。

A：聚焦第2~4个阶段。

A：把威胁发现在早期...

Q：投入多少人力在做这个事情。。。做了多久？

Q：这个问题估计敏感了，换一个

1、市场上很多EDR产品其实都声称有 xx%的覆盖度。但是似乎都没谈深度，而且聚焦的是客户端的层面。

2、还有HIDS似乎比较少拿这个ATT&CK来做覆盖率的描述的（我理解很多TTPs其实是聚焦在PC端为主）

-----张总对这个现象有什么解读么？

A：不是，有点回答不过来了，抱歉有点慢，现在的EDR对ATT&CK的覆盖能力都很弱，所以不会主动提...甲方可以拿这个来选产品...

Q：市场上似乎有一些产品已经声称60%甚至80%的覆盖率了。。。（不谈深度我也不敢信）

A：ATT&CK的广度问题目前已经基本解决了，往后发展就是不断增加深度，不是一个测试用例就算覆盖一个指标了，而是一组测试用例可以验证一个指标的深度。

Q：1、ATT&CK 是不是很依赖威胁情报，感觉这种情报和传统的还不太一样，更需要对很多攻击手法apt研究，单一组织很难覆盖

2、如果要做到高准确率，那势必要匹配攻击者的战术目标，需要触发一些特殊行为如持久化 提权，到这个阶段也不算“尽早发现威胁”，那怎么对比优劣于现有的防御模型呢

A：@黄猛@VIPKID ATT&CK带来的最大好处就是标准化、透明化了。让你比较清晰的知道自己哪里做的还行，哪里缺口很大。

Q：ATT&CK都覆盖了并不能说明反入侵做的就一定好，还是要看场景的深度，能不能发现关键动作的攻击行为。因为ATT&CK里有很多动作是在APT里使用的（以前被使用）不一定适合企业场景

A：之前的入侵检测，没有标准，只能凭感觉，之前的入侵检测，没有标准，只能凭感觉

Q：以绝大多数公司的现状，我觉得不太可能“都覆盖”。

Q：还是那个问题，知道有哪些甲方在实践，而且实践得比较好的么。。？

A：这是个非常先进的框架，目前国内估计还没有企业落地，但是我估计明年头部企业有一部分会应用这个框架……大家有兴趣可以一起来实践实践，我们可以提供我们的研究成果。

Q：职业欠钱:我们在努力，不过目前感觉还不是很成功。没有给出太实际的帮助（不是说这个框架不行，而是说我们建设阶段还没到）

A：我们弄到一个阶段了之后你们可以试试，我觉得可以落地。

**讨论环节：**

**avfisher|华为云：**我尝试回答一下欠钱总之前问的关于怎么确定优先级的问题 我在前司曾经将已检测或者已处理的真实安全事件或者威胁与att&ck做映射和对照最后形成一个自己企业威胁最大的ttp集合 根据这个来优先设计和优化检测系统来针对此类ttps

**职业欠钱：**相当于优先解决历史已暴露问题涉及的TTPs，潜台词是，历史已暴露问题的TTPs的建设其实挺花时间的，很多人历史已知问题可能还没能完全闭环。。。

**avfisher|华为云：**@美团赵弼政 是的 已暴露的问题的发现有的时候是很偶然的 发现一次也不代表你能一直发现 怎么优化检测率和准确度就是深度问题了

**钱文斌-支付：**那就回到了那个问题，大多数人其实是并不知道自己被黑的

「 钱文斌-支付: 那就回到了那个问题，大多数人其实是并不知道自己被黑的 」

- - - - - - - - - - - - - - -

问题不是很大，先把已经看见的被黑的解决了也不容易的。

---听上去是一场攻击者和防御者似乎在玩一个躲猫猫的对坑游戏，框架更像一场红蓝对抗教练模型，再次感谢CEO分享。