HOLMES

1 Introduction

1.HOLMES的目标：将主机日志中发现的行为和产生的警报直接映射到kill-chain模型中；

2.HOLMES使用系统中的低级实体（file，process）之间的信息流作为警报关联的基础。通过检测与APT步骤相关的低级系统事件，并且利用信息流将它们进行关联，就可能构建该次APT攻击活动相应的攻击链（攻击步骤）；

3.HOLMES提出高级场景图（high-level scenario graph）的概念，HSG中的节点对应TTP（tactics、techniques、procedures），边则对应着TTP实体之间的信息流

- ancestral cover：评估HSG中节点之间的依赖程度；
- noise reduction：尽量忽略与已知良性事件相关的依赖；
- ranking and prioritization：剔除与APT活动无关的大部分节点和边；

> 如何删除与APT攻击行为完全无关的节点和边？

4.HSG提供了一个紧凑的、可视化的攻击事件的总结；

2 Example

3 Approach

攻击步骤可能是离散的，但是high-level的APT行为往往会符合kill-chain模型的相应阶段；

每个APT步骤的具体表现也许会不同，但是，APT步骤本身就是攻击者攻击意图的高级抽象，因此，即使所使用的具体战术不同，其攻击意图或目的仍然会有所体现；

此外，不同APT步骤之间的信息流或因果关系也是逻辑上必然存在的；

semantic gap between low-level audit data and the very high-level kill-chain view of attacker's goals, intentions, and capabilities.

HOLMES基于ATTCK设置了一个中间层，通过溯源图中的节点和边所描述的TTP，映射到ATTCK框架中的各种战术，然后再进一步地映射到kill-chain的不同阶段；

challenges：

- 低级系统事件流如何有效与TTP进行匹配；
- 攻击步骤之间的关联性如何检测；
- 如何减少误报率；

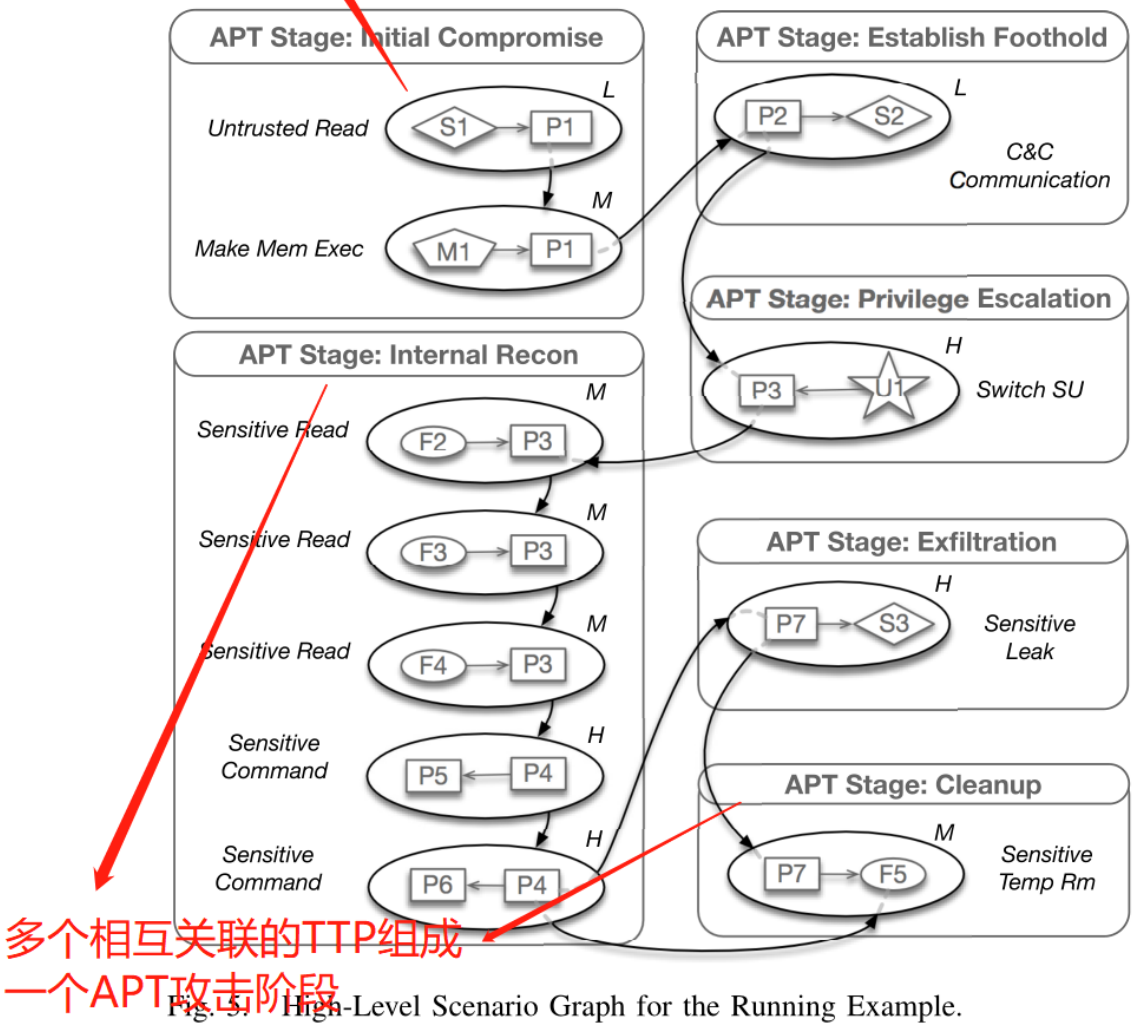
TTP规则

APT Stage	TTP	Event Family	Events	Severity	Prerequisites
$Initial\_Compromise(P)$	$Untrusted\_Read(S,P)$	READ	FileIoRead (Windows), read/pread/readv/preadv (Linux,BSD)	L	$S.ip \notin$ {Trusted_IP_Addresses}
	$Make\_Mem\_Exec(P,M)$	MPROTECT	VirtualAlloc (Windows), mprotect (Linux,BSD)	M	\$PROT_EXEC\$ $\in M.flags$ $\wedge \exists\, Untrusted\_Read(?,P') :$ $path\_factor(P',P) <= path\_thres$
$Establish\_Foothold(P)$	$Shell\_Exec(F,P)$	EXEC	ProcessStart (Windows), execve/fexecve (Linux,BSD)	M	$F.path \in$ {Command_Line_Utilities} $\wedge \exists\, Initial\_Compromise(P') :$ $path\_factor(P',P) <= path\_thres$

TABLE 4. Example TTPs. In the Severity column, L=Low, M=Moderate, H=High, C=Critical. Entity types are shown by the characters: P=Process, F=File, S=Socket, M=Memory, U=User.

溯源图→HSG→APT攻击阶段

HSG中的一个TTP节点



多个相互关联的TTP组成一个APT攻击阶段

Fig. 5. High-Level Scenario Graph for the Running Example.

of TTPs in the HSG at any time, making it possible to carry out sophisticated analyses without impacting real-time performance.

从溯源图中的系统事件 → TTP：规则引擎实现；

每个TTP根据其serverity赋予不同的分数，不同的APT阶段的TTP还可以 ，赋予不同权重，从而可以突出对于某一个特定的APT阶段的探索；

HOLEMS 系统架构

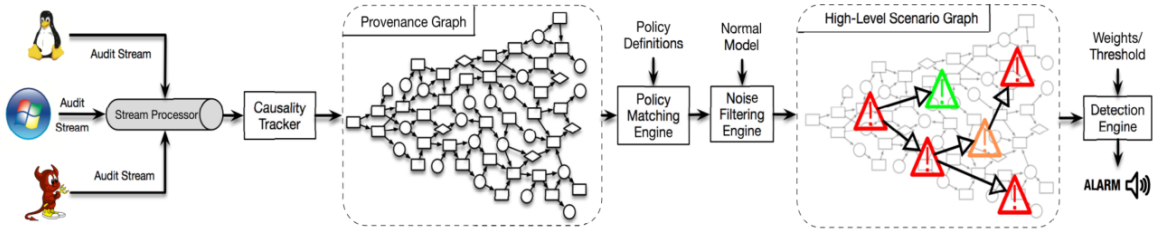


Fig. 6. HOLMES Architecture.