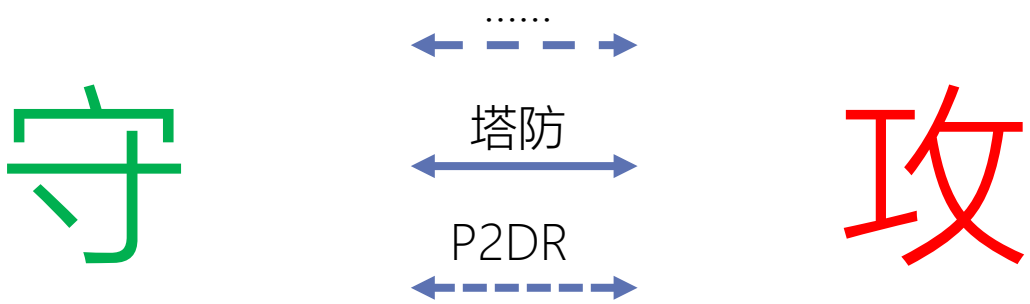
华云庵321春分雅集

从四方博弈窥网安动向

2015. 03. 21

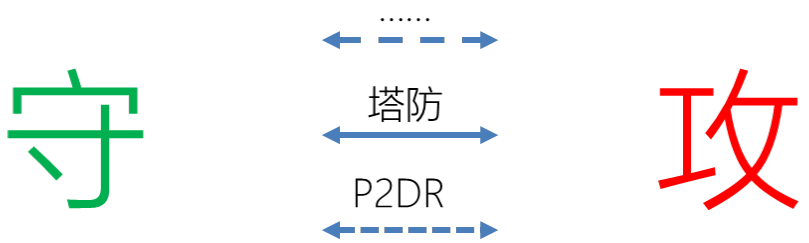
赵 粮

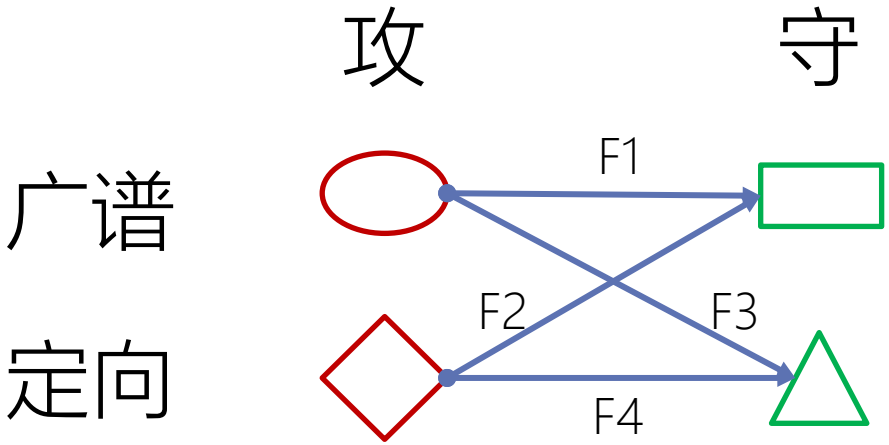
攻防博弈...



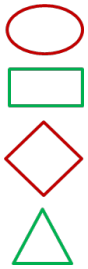
- 多方位技术和资源的对抗和博弈过程
- 定向和非定向（广谱）攻击长期持续并存
- 没有100%的安全，守方注定会遭遇"失败"
- 城防模型逐步演化为塔防模型
  - 守方可以接受局部"失败"，但须确保全局控制
  - 局部的战术性"胜利"对攻方意义不大
- 塔防战场胜负关键
  - 守方须有"实时曝光"攻方的能力（否则，守在明处，攻在暗处）
  - 守方须有全局视野和态势判断能力
  - 守方须有实时调度和部署能力
  - .....

细分战场F1-F4





细分战场上的战局预期



广谱攻:: 不区分行业和目标属性
广谱守:: 采用商业可得的大众化防护技术
定向攻:: 针对目标防护属性进行“免杀”、校准
定向守:: 在商业可得大众化防护技术上，采用独特的防护手段

F1:: 广谱攻对广谱守， 传统格局

F2:: 定向攻对广谱守，从定义和原理上看，广谱守无效，定向攻顺利

- 守方须有强大的威胁情报能力
- 守方所使用的技术手段具备“反情报”和反“免杀测试”能力

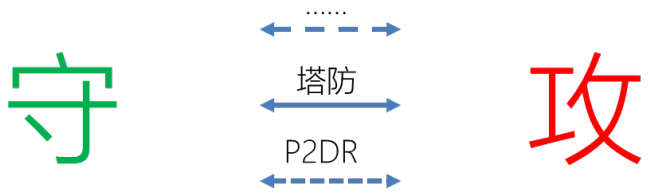
F3:: 广谱攻对定向守，取决于后者防护的范围，成本较高

- 完全DIY
- 专业提供商提供特别定制

F4:: 定向攻对定向守，战场斗法，胜负参半

- 轻武器组合+快速响应...

战场之外的思考



思考一： 既然没有100%的安全， 那守方注定会遭遇“失败”，那去哪里寻找“成功”、如何定义“成功”呢？

思考二：既然数据总是要丢失，那哪些可以丢？丢多少？怎么丢？丢给谁？ 怎么检测和判定呢？

思考三：如何在“局部失败”的情况下，实现全局可控呢？控什么？

世界上没有无缘无故的爱，也没有无缘无故的恨。

三体 - 猜疑链

两大基本原理：

- 生存第一
- 资源总和不变

两大技术基础：

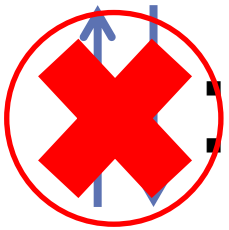
- 技术爆炸
- 猜疑链

攻防博弈中的新玩家

管理层
（赞助人）

买家
（赞助人）

- 确认效果
- 取得资源



- 证明价值
- 取得回报

守

……

塔防

P2DR

攻

四方博弈图像下的新视角

广谱攻:: 不区分行业和目标属性

>> 单次收益低，强调海量重复和自动化

广谱守:: 采用商业可得的大众化防护技术

>> 看概率、统计，减弱攻方的自动化和重复

定向攻:: 针对目标防护属性进行"免杀"、校准

>> "独特性"意味着成本，在独特性和收益之间取舍

>> "快速组装"...

定向守:: 在商业可得大众化防护技术上，采用独特的防护手段

>> Token、Honey、沙子、化整为零... 提高攻方"猜疑"度， 提高自身防护体系的"独特性"

>> 软件定义架构...

春天来了