
FIT 2017 | REEBUF

# 网络欺骗：防御者的“诡计”

ArkTeam

- 从战争说起
- 网络欺骗
- 公司和产品
- NIPRNet防卫

# 从战争说起



金蝉脱壳
擒贼擒王
笑里藏刀
树上开花
空城计
连环计

抛砖引玉
关门捉贼
调虎离山
暗渡陈仓
苦肉计
美人计

借刀杀人
打草惊蛇
顺手牵羊
假痴不癫
远交近攻
借尸还魂

以逸待劳
浑水摸鱼
李代桃僵
欲擒故纵
反客为主
隔岸观火

指桑骂槐
瞒天过海
无中生有
走为上
上屋抽梯
围魏救赵

趁火打劫
反间计
声东击西
釜底抽薪
偷梁换柱
假道伐虢

ArkTeam

# 从战争说起

- **蒋干中计**
  - ✓ 曹操：攻击者
  - ✓ 周瑜：防御者
  - ✓ 攻击：蒋干劝降
  - ✓ 防御：拒之门外，乱棍打出

**传统防御策略**

ArkTeam

# 从战争说起

- **蒋干中计**

✓ 曹操：攻击者

✓ 周瑜：防御者

✓ 攻击：蒋干劝降

✓ 防御：**佯装酒醉，诱其盗书**

**欺骗防御策略**

ArkTeam

# 从战争说起

- **蒋干中计**

✓ 发现攻击：劝降（行为）

✓ 释放蜜饵：书信

✓ 欺骗效果：杀蔡、张二将

**欺骗防御策略**

ArkTeam

# 从战争说起


# 从战争说起

- “智子”锁死人类科技
  - ✓ 干扰物理学实验结果
  - ✓ 物理学家自杀
  - ✓ 锁死基础科学


ArkTeam

# 从战争说起

- **面壁计划**

✓ 三体文明监视地球一切，三体舰队即将抵达地球

✓ 面壁者对外界表现出来的完全是假象，是精心策划的伪装、误导和欺骗，真正的计划只在大脑中

✓ **使敌人丧失正确的判断**

# 从战争说起

- “欺骗”在人类战争中被运用到了极致
- “欺骗”同样也被用于网络攻防

# 欺骗早已用于网络攻击


网络钓鱼

# 欺骗早已用于网络攻击


水坑攻击

鱼叉式钓鱼攻击

ArkTeam

# 欺骗早已用于网络攻击

## 社会工程学

## *Social Engineering*


ArkTeam

# 网络攻击不可避免

世界上只有两种人：

一种是知道自己被黑了的，另外一种是被黑了还不知道的。

ArkTeam

# 网络攻击不可避免

APT（高级持续威胁）

不怕贼偷，就怕贼惦记，防不胜防

ArkTeam

# 网络欺骗

- Garter定义

✓ 使用骗局或者假动作来阻挠或者推翻攻击者的认知过程，扰 乱攻击者的自动化工具，延迟或阻断攻击者的活动，通过使用虚假的响应、有意的混淆、以及假动作、误导等**伪造信息**达到“欺骗”的目的。

✓ *Deception technologies are defined by the use of deceit and/or feints designed to thwart or throw off an attacker's cognitive processes, disrupt an attacker's automation tools, delay an attacker's activities or disrupt breach progression. Deceptions are achieved through use of deceitful responses, purposeful obfuscations, feints, misdirections and other falsehoods.*

# 积极主动的防御策略

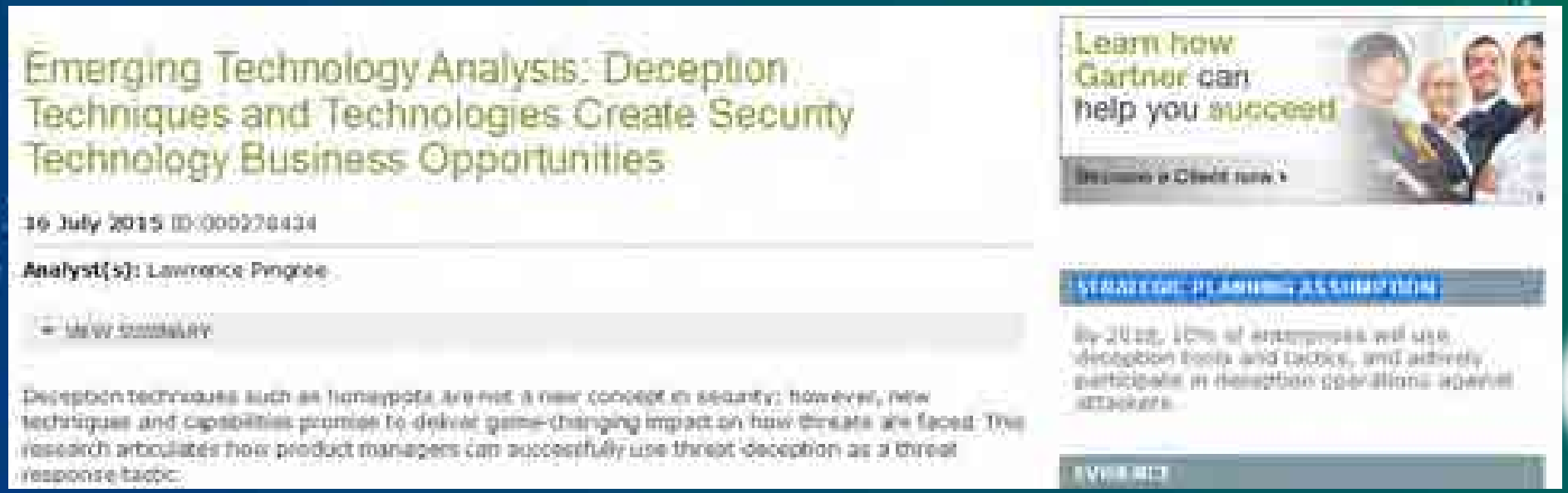
- 发现网络攻击：正在的攻击，潜在的攻击
- 粘住网络攻击：消耗攻击者的时间、精力
  暴露攻击意图，攻击手段
- 溯源取证，采取反制措施

# 美国军方

- 2014年美国空军发布研究报告（BAA-RIK-14-07），指出要研究网络欺骗技术，并在2015年签订了两份总值9800万美元的合同，其中的一份是关于网络欺骗技术

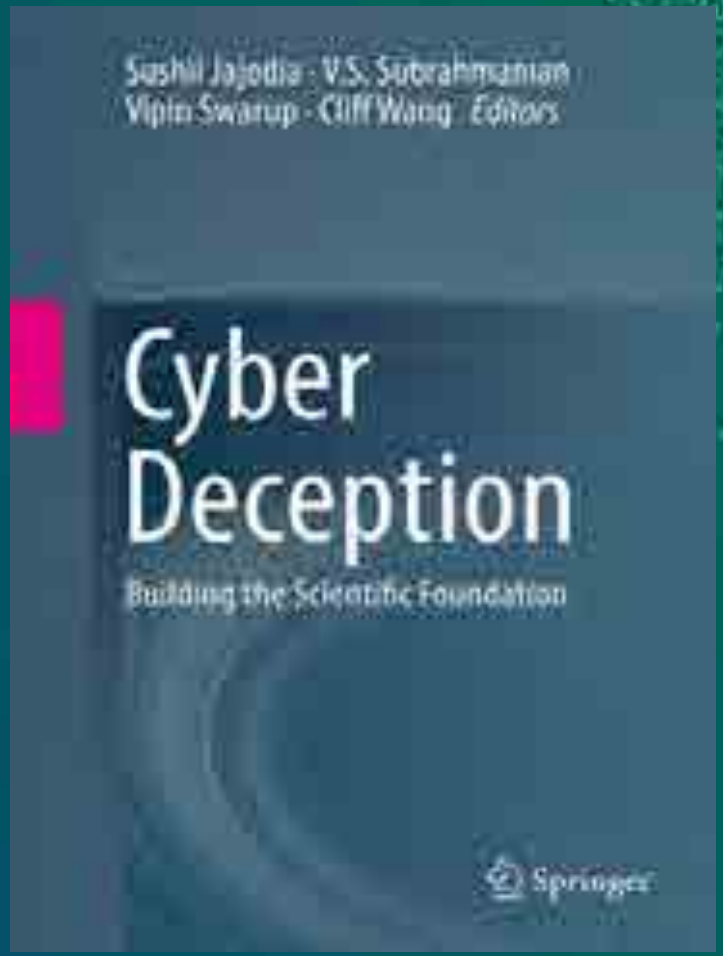

# 市场预测

- 2015年7月，Gartner的报告指出：基于欺骗的安全防御技术将会有很大的市场前景，并预测到2018年，将会有10%的单位使用欺骗工具或策略来对抗网络攻击



# 权威著作

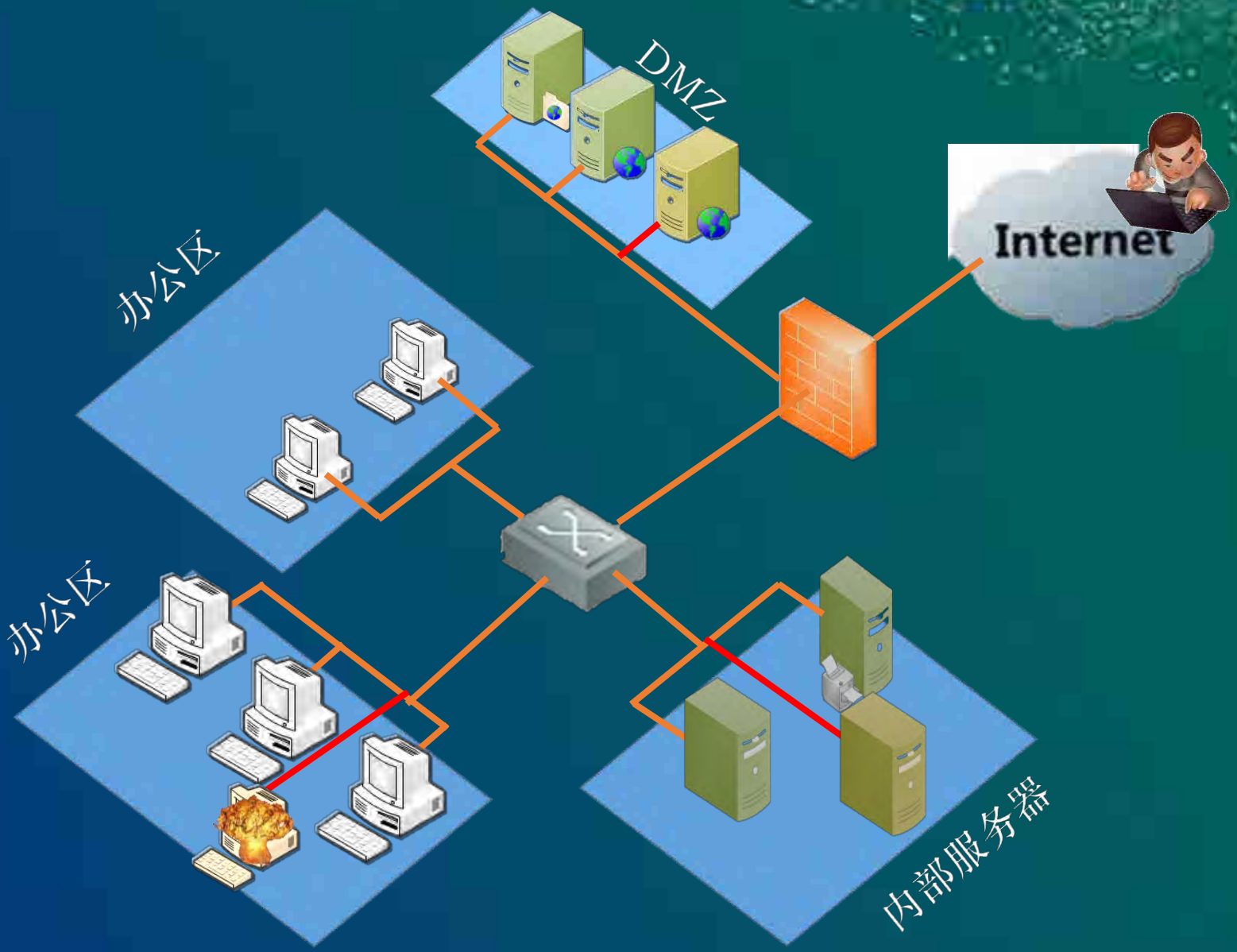
- 2016年7月，Springer出版《Cyber Deception：Building the Scientific Foundation》书中内容是由世界各地顶级网络欺骗研究人员最新研究整理而成，目的是为网络欺骗建立学科基础。



# 关键技术

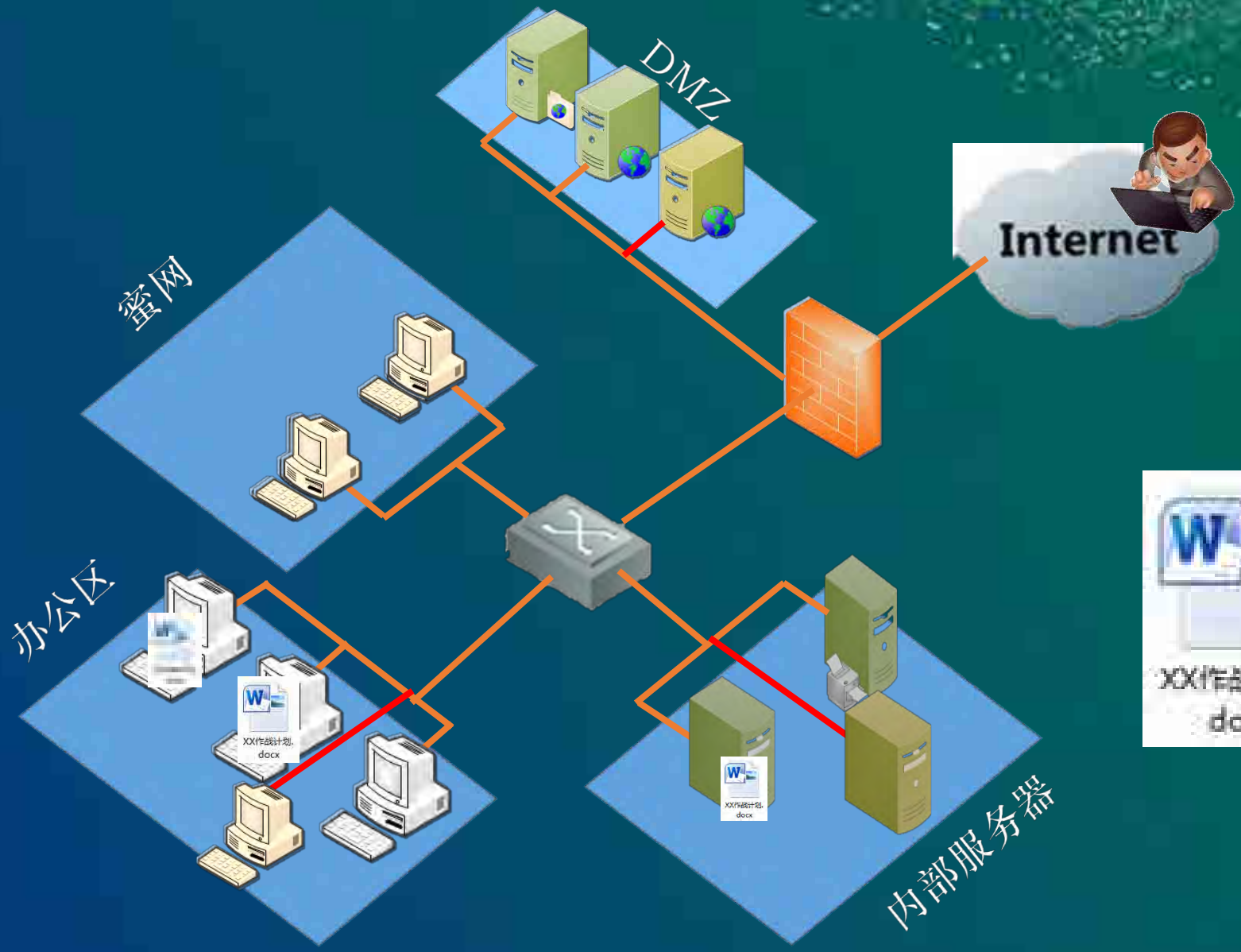

ArkTeam

# 蜜罐




ArkTeam

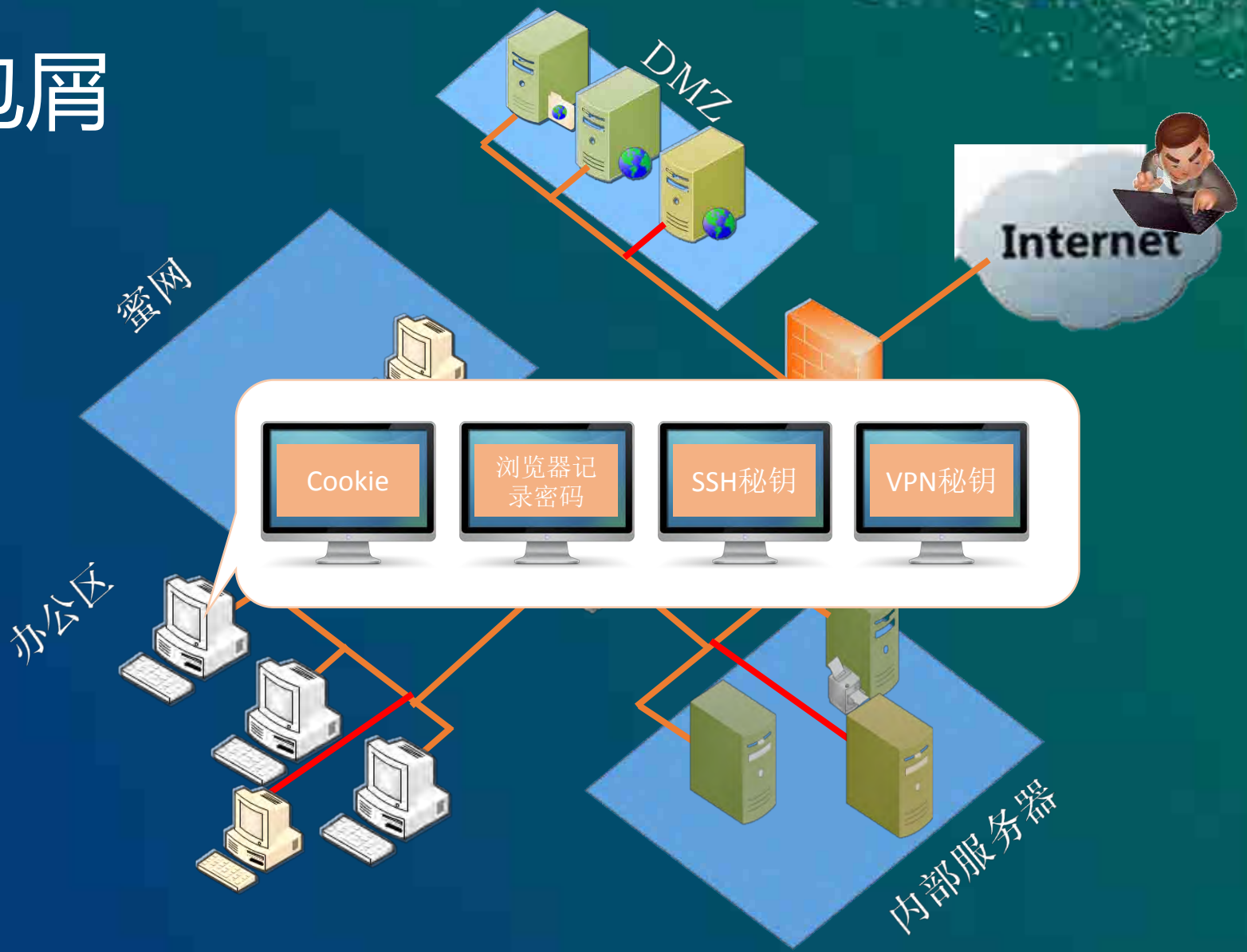
# 蜜饵





ArkTeam

# 面包屑




ArkTeam

# 发现网络攻击

- 蜜罐
- 蜜饵/面包屑
- 密标

**WEB蜜饵/面包屑**

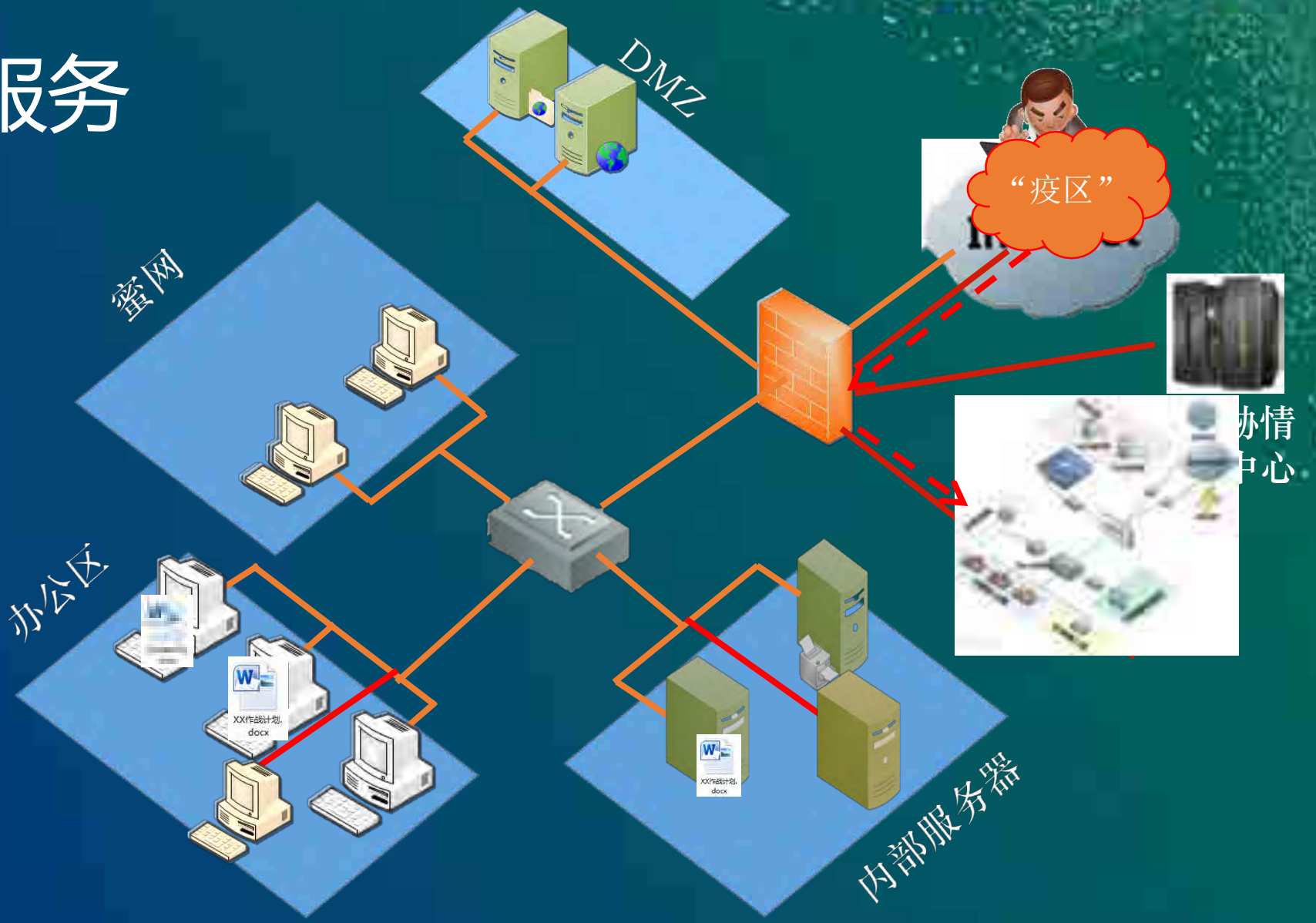
- ✓ 网站后台
- ✓ 管理员密码
- ✓ 代码注释
- ✓ Robots文件
- ✓ 数据库记录
- ✓ 数字证书
- ✓ DNS记录
- ✓ 数据库密码
- ✓ ……

**主机蜜饵/面包屑**

- ✓ 文档
- ✓ 分区
- ✓ Cookie
- ✓ 浏览器存储
- ✓ 密钥
- ✓ ……

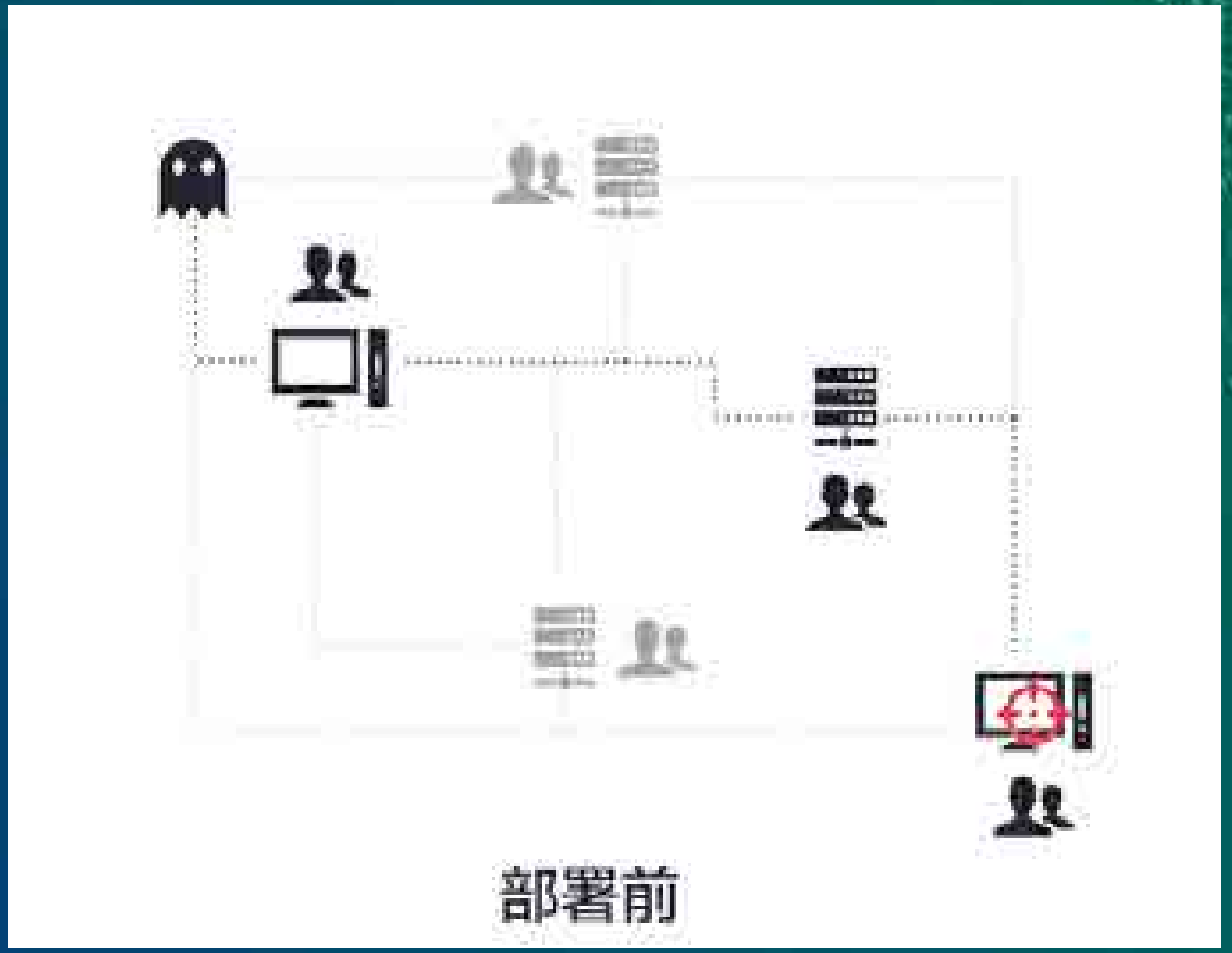
ArkTeam

# 影子服务



# 影子服务

# 虚拟资产






长亭科技谛听威胁感知：https://chaitin.cn/cn/dsensor.html

ArkTeam

# 粘住网络攻击

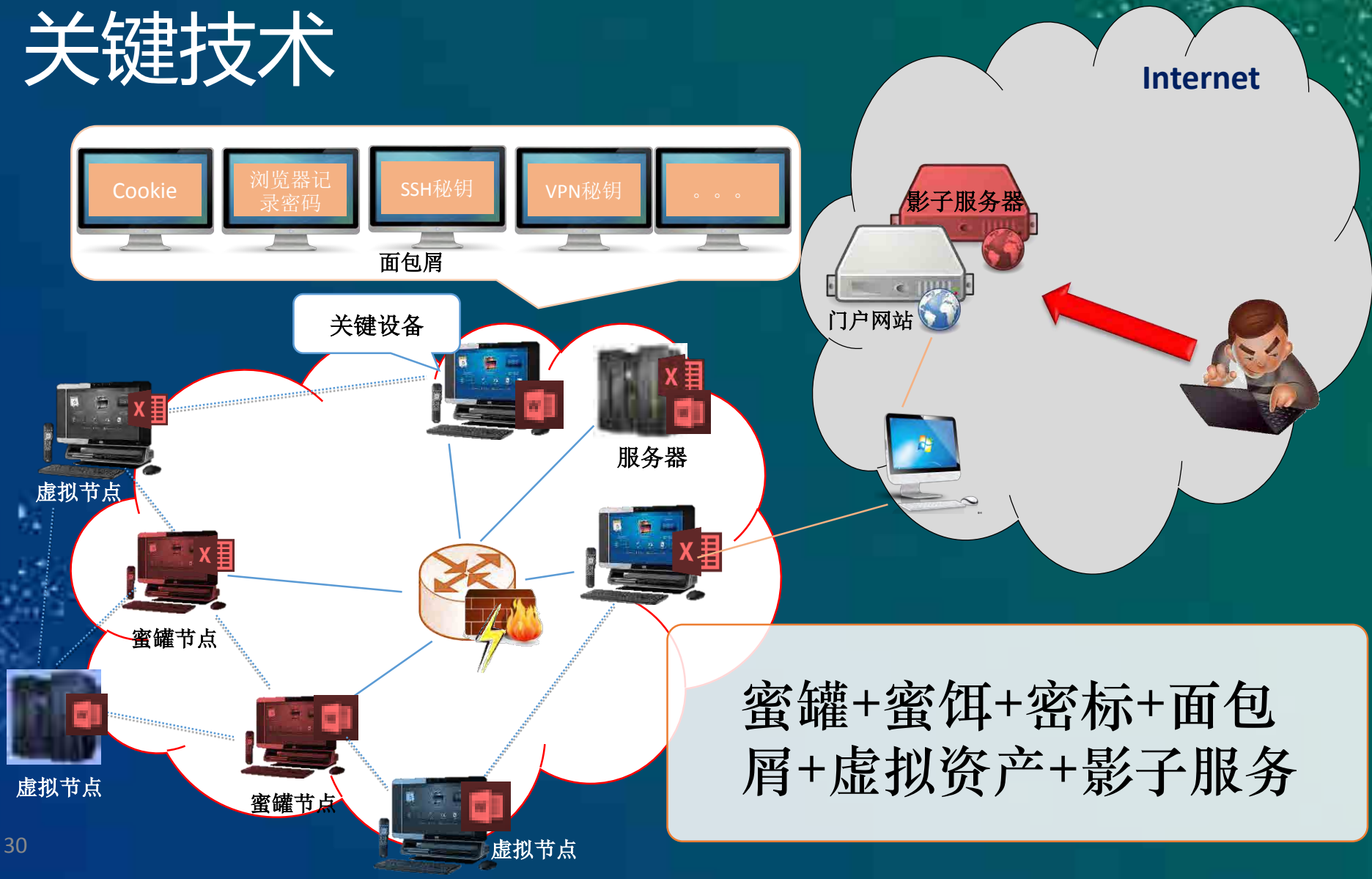
- 虚拟资产
- 影子服务

保护真正资产

消耗攻击者

ArkTeam

# 关键技术




蜜罐+蜜饵+密标+面包屑+虚拟资产+影子服务



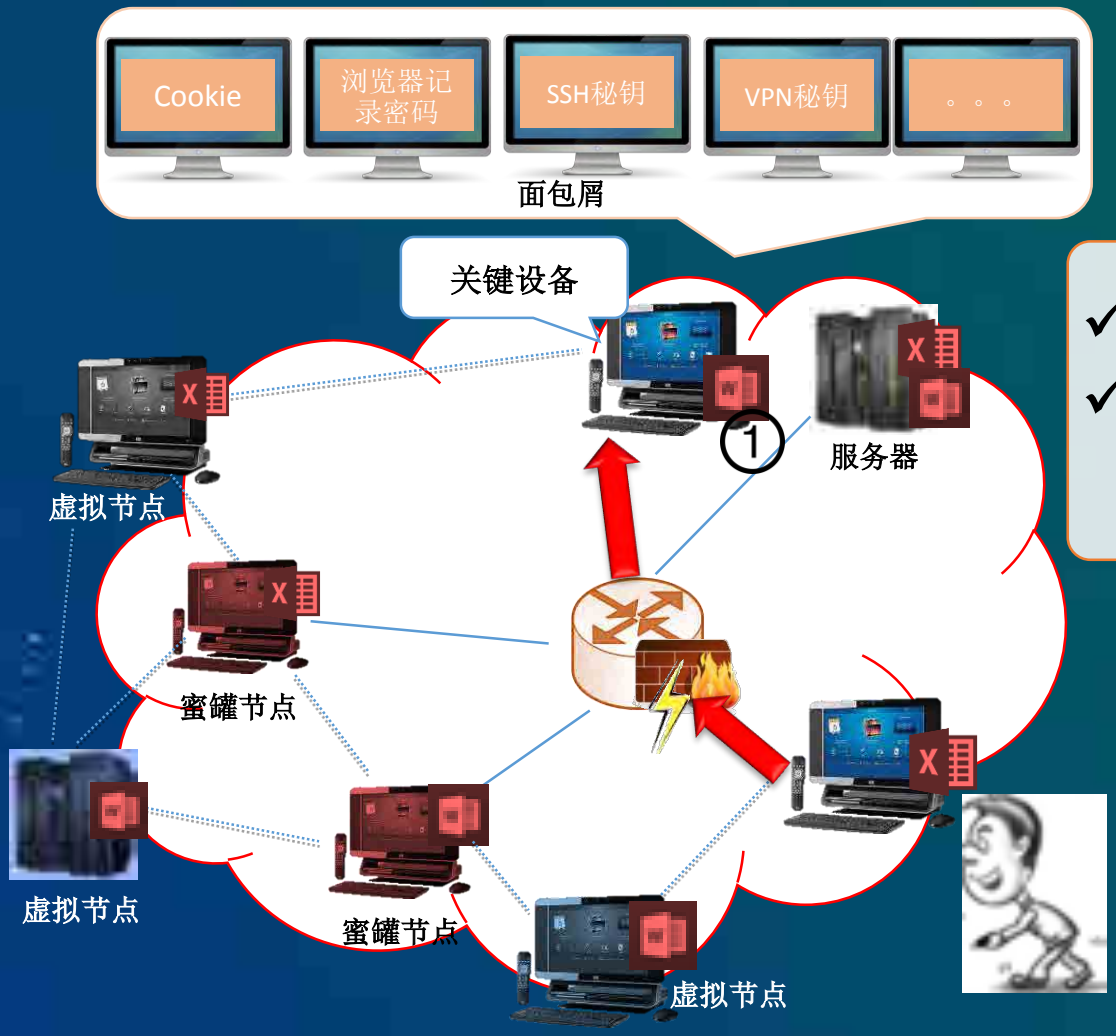
ArkTeam

# 应用场景

- 保护重要资产
- 防御门户向内网渗透
- 溯源与反制
- ……

ArkTeam

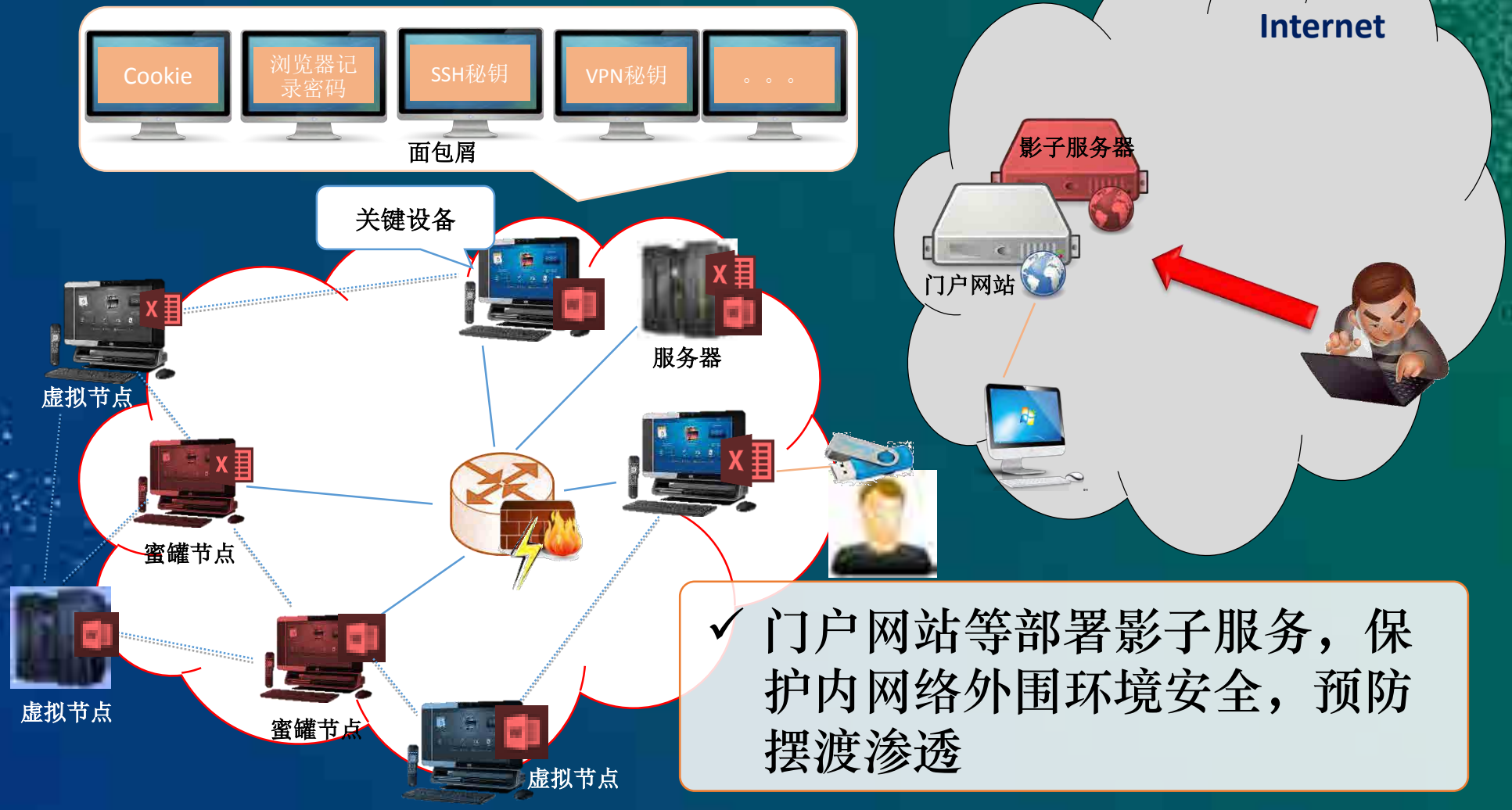
# 保护重要资产




- ✓ 触碰蜜饵文档，引发警报
- ✓ 蜜饵文档不慎丢失，打开文档后，主动联网警报

ArkTeam

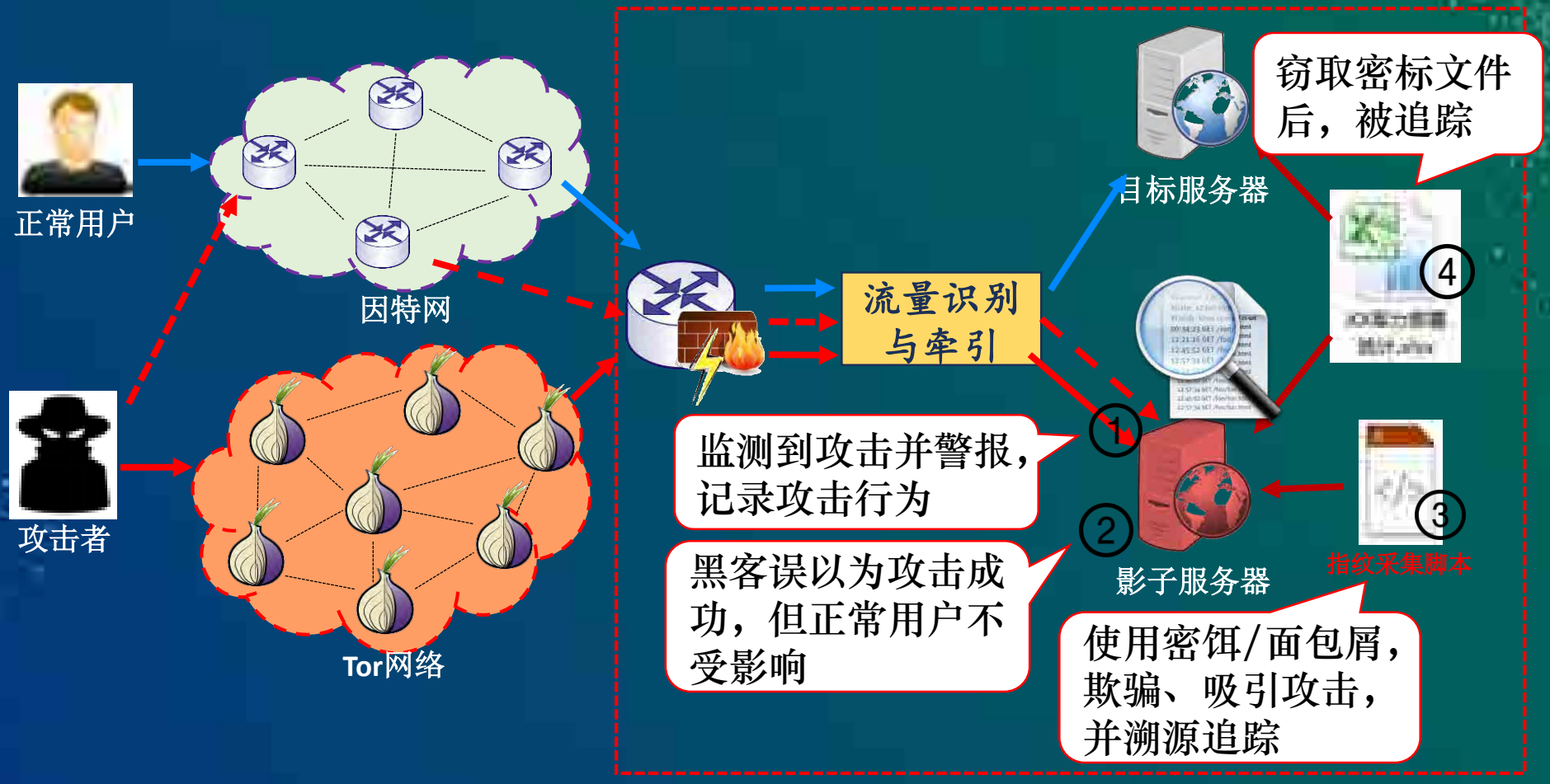
# 防御门户向内网渗透




✓ 门户网站等部署影子服务，保护内网络外围环境安全，预防摆渡渗透

ArkTeam

# 溯源与反制


正常用户
因特网
攻击者
Tor网络
流量识别
与牵引
监测到攻击并警报，
记录攻击行为
黑客误以为攻击成
功，但正常用户不
受影响
目标服务器
窃取密标文件
后，被追踪
4
1
2
3
影子服务器
指纹采集脚本
使用密饵/面包屑，
欺骗、吸引攻击，
并溯源追踪

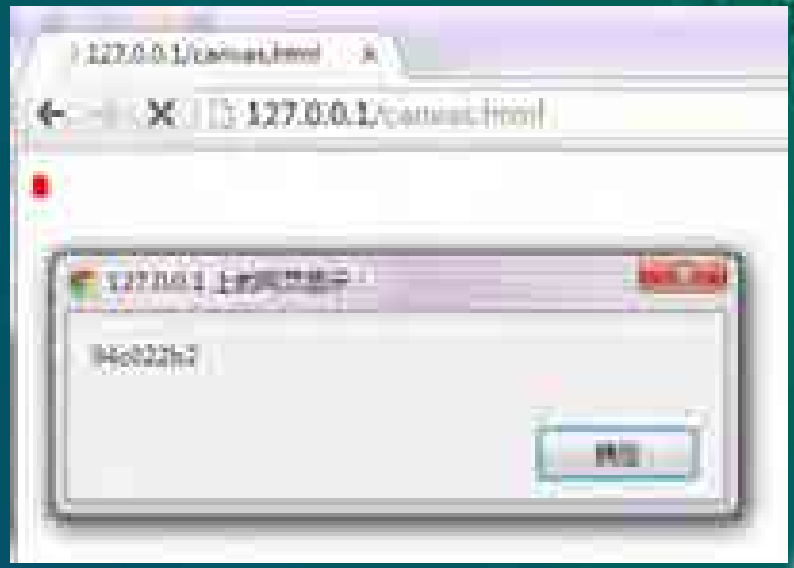
# 溯源与反制

```
One of your canarydrops was triggered.

Channel: HTTP
Time    : 2016-10-02 10:42:50.308579
Memo    : test
Source IP: 59.64.255.138
User-agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.307
InfoPath.3; .NET4.0C; .NET4.0E; ms-office; MSOffice 14)

Manage your settings for this Canarydrop:
http://canarytokens.org/manage?token=dzbk9hxcxyy1j6nldrn9h8hmg&auth=24c25bc8deafaa60e38758384f6dff43
```

ArkTeam

# 浏览器指纹

- 一个字符串，用于唯一标识浏览器

# 浏览器指纹

百万级

**软硬件指纹**

- ✓ UA
- ✓ 语言
- ✓ 颜色深度
- ✓ 屏幕分辨率
- ✓ 时区
- ✓ 缓存状态
- ✓ 数据库状态
- ✓ 内外网IP
- ✓ VPN IP

**软硬件指纹**

- ✓ CPU等级
- ✓ 系统平台
- ✓ 追踪设置
- ✓ 是否支持触摸
- ✓ 插件信息
- ✓ 系统字体信息
- ✓ Canvas
- ✓ AudioContext

**软硬件指纹**

- ✓ GPU频率
- ✓ 摄像头
- ✓ 气场器
- ✓ 麦克风
- ✓ 传感器
- ✓ GPS
- ✓ 电池

ArkTeam

# 信息泄露

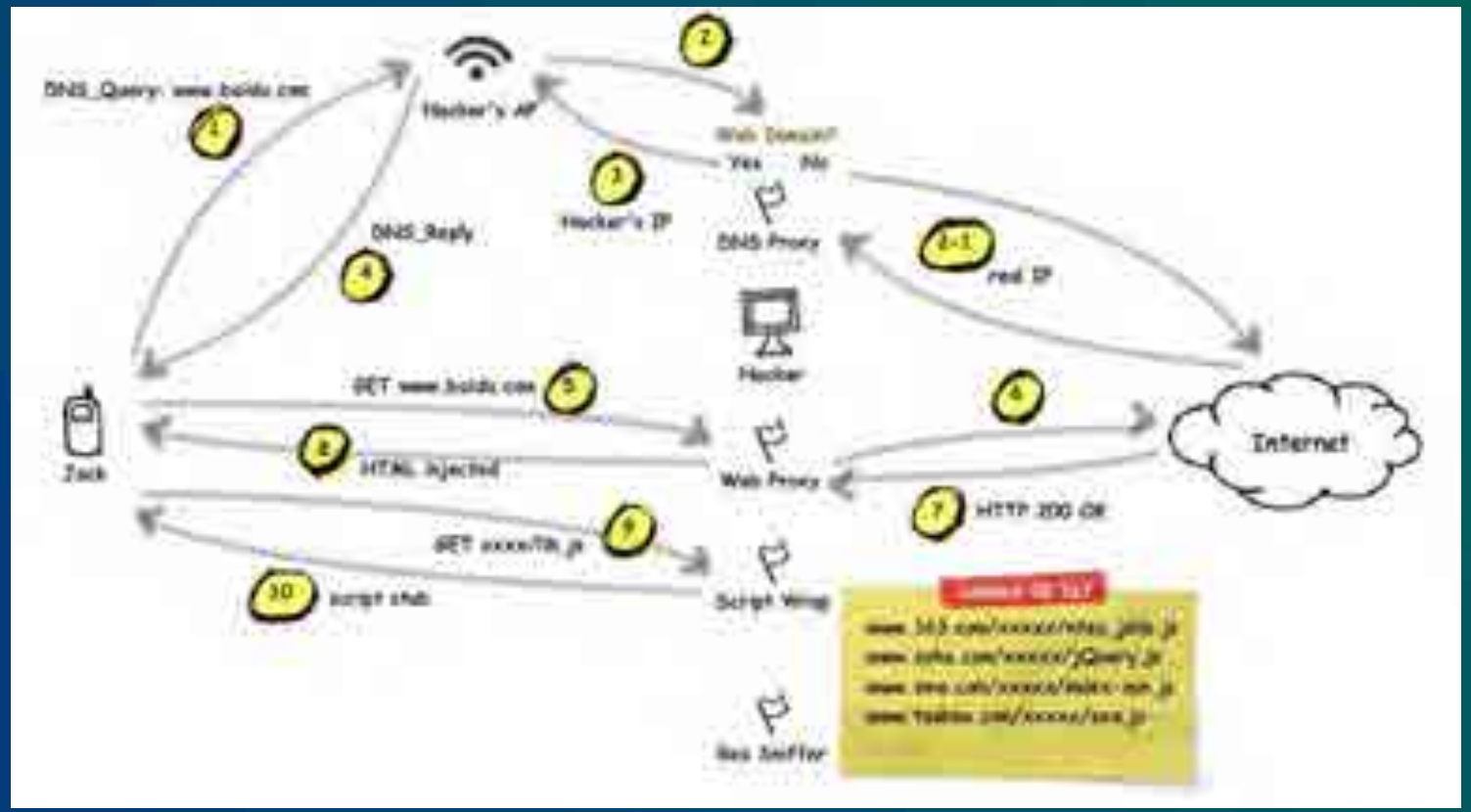
- 已登陆账户
- http://weibo.com/ajaxlogin.php?fmelogin=1&callback=weibo



ArkTeam

# 信息泄露

- JS缓存投毒
- 参考：www.cnblogs.com/index-html/p/wifi_hijack_3.html



# 公司和产品

| 公司 | 成立时间 | 国家 | 融资总额 | 统计 | | |
|---|---|---|---|---|---|---|
| | | | | 时间 | 金额 | 轮次 |
| illusive network | 2014年 | 以色列 | 3000万美金 | 2015.6 | $ 5M | A轮 |
| | | | | 2015.10 | $ 22M | B轮 |
| | | | | 2016.5 | $ 3M | B轮 |
| Cymmetria | 2014年 | 以色列 | 1060万美金 | 2014.1 | $ 100K | 天使轮 |
| | | | | 2015.7 | $ 1.5M | 天使轮 |
| | | | | 2015.11 | $ 9M | A轮 |
| TrapX security | 2010年 | 美国 | 1900万美金 | 2014.12 | $ 5M | A轮 |
| | | | | 2015.7 | $ 9M | B轮 |
| | | | | 2016.4 | $ 5M | B轮 |
| AttivoNetworks | 2011年 | 美国 | 800万美金 | 2015.4 | $ 8M | A轮 |

# 公司和产品

- **illusive network**

✓ Deception Everywhere

ArkTeam

# 公司和产品

- **illusive network**

✓ Attacker View

ArkTeam

# 公司和产品

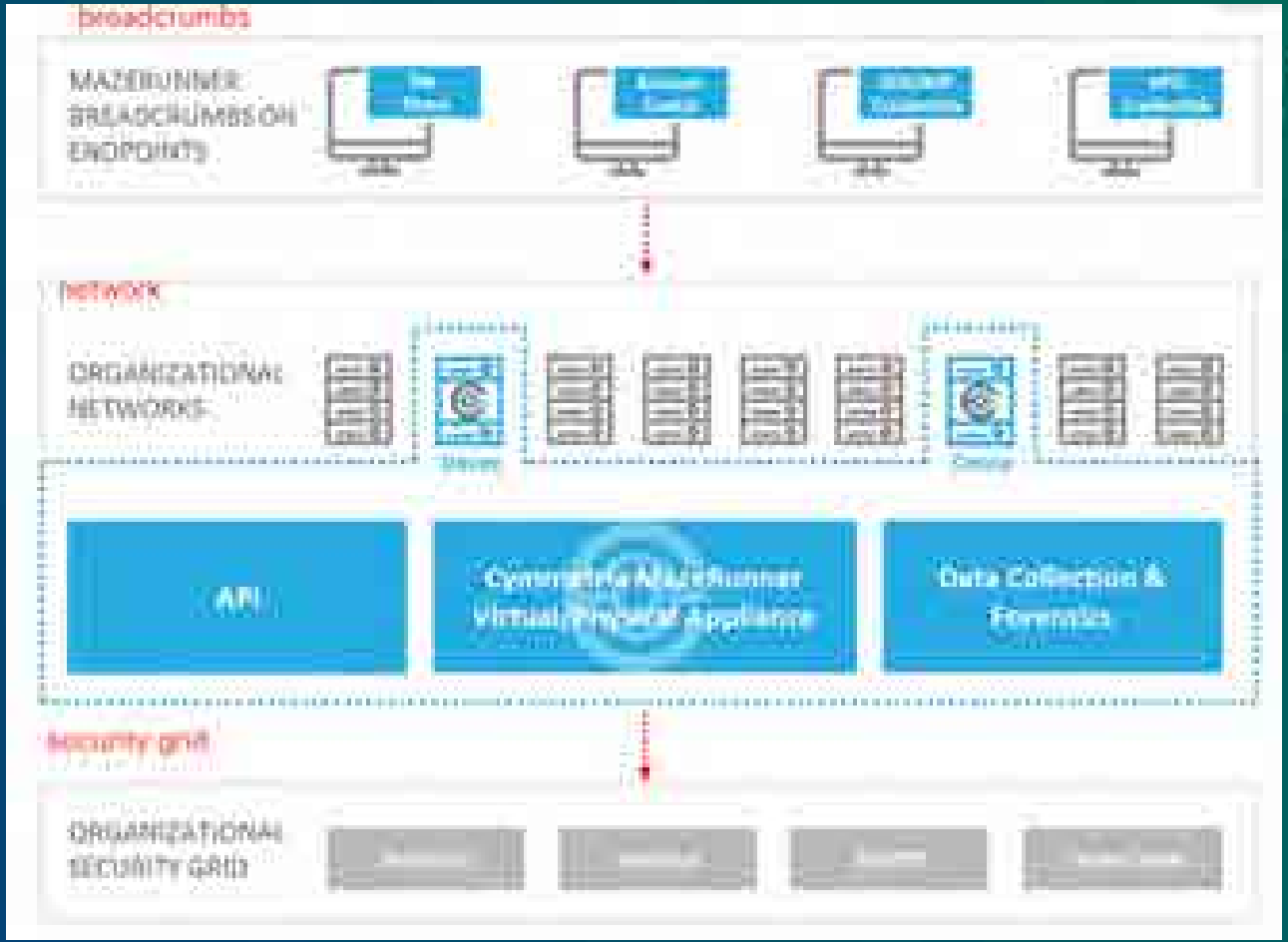
- **illusive network**

✓ Advanced Ransomware Guard

ArkTeam

# 公司和产品

- **Cymmetria**
  - ✓ MazeRunner






ArkTeam

# NIPRNet

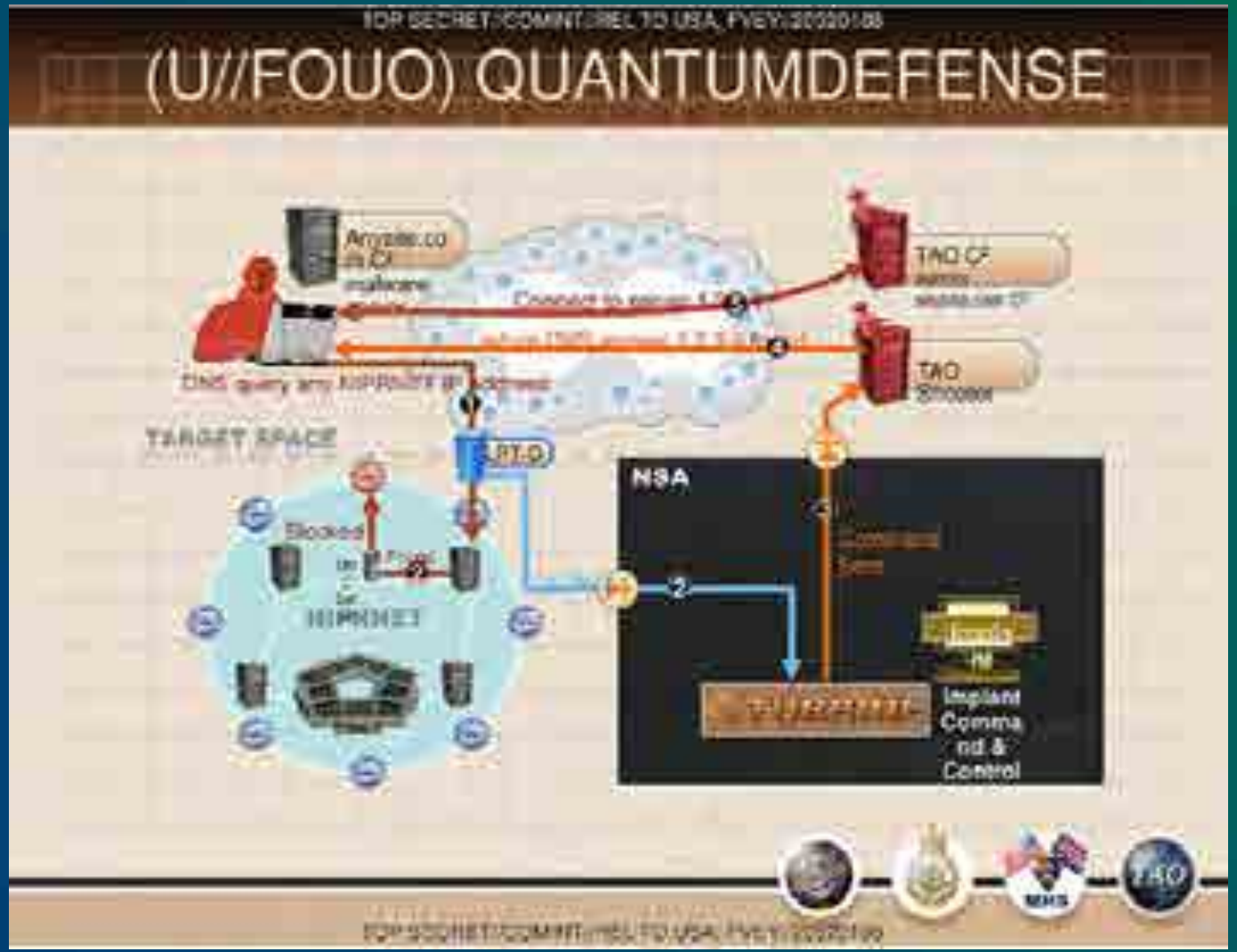
- 美国国防部国防信息系统局(DISA)根据可访问的数据密级不同提供不同的基于IP的服务：
- SENSITIVE BUT UNCLASSIFIED IP DATA（ NIPRNet ）
- SECRET IP DATA （ SIPRNet ）
- Top Secret/Sensitive Compartmented Information Data（JWICS)

ArkTeam

# NIPRNet

- **非安全互联网协议路由网络：**
- Non-Secure Internet Protocol Router Network（预算文件，DISA网站）
- Unclassified but Sensitive Internet Protocol Router Network（wiki等）
- **DISA创建的内部网络：**
- 在内部用户间（internal）交换非保密但是敏感的信息
- 与互联网相连，用户可以接入互联网

# NIPRNet防卫



# 谢谢大家！

ArkTeam官方微信(ArkTeam)

ArkTeam官方微博(@ArkTeam)

欢迎关注ArkTeam：www.arkteam.net

ArkTeam