

APT攻击与检测

高级持续性威胁

Advanced Persistent Threat

郑康锋
北京邮电大学

注：部分资料来源于互联网



主要内容

CONTENTS

1. APT简介
2. APT解析
3. APT检测



主要内容

CONTENTS

1. APT简介
2. APT解析
3. APT检测

APT:新兴安全威胁

The Washington Post

McAfee Calls Operation Aurora A "Watershed Moment In Cybersecurity" Offers Guidance

BBC

News

Sport

Weather

Capital

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health



REUTERS

EDITION: U.S.

ARTICLE



LEARN MORE >

DISCOVER
BRILLIANT
INVESTMENT
INSIGHTS
WITH

Virus found in Middle East finance transaction

Thu Aug 9, 2012 8:59am EDT

* Gauss found in Lebanon, Israel Territories

* Kaspersky Lab describes Gauss as cyber

* Says it may also be able to cause physical

* Says may be from same 'factories' as Stuxnet

By Jim Finkle

“火焰”病毒或引发网络战

人民日报
RENMING RIBAO

近一段时间以来，一种新型电脑病毒“火焰”入侵了伊朗、黎巴嫩、叙利亚等中东国家

人民网 people
www.people.com.cn

韩国电视台和金融机构网络遭遇瘫痪

人民网首尔3月20日电（记者马菲）韩国主要电视台和部分金融机构的网络从当地时间20日下午2点开始陆续遭遇瘫痪。

据韩国联合通讯社报道，韩国主要电视台KBS、MBC、YTN和新韩银行、农协银行等部分金融机构的网络当天遭遇瘫痪。韩国政府派遣联合应对小组进行调查后证实，网络瘫痪是由恶意代码所致。这些恶意代码破坏了计算机的主引导记录（MBR），导致网络瘫痪。

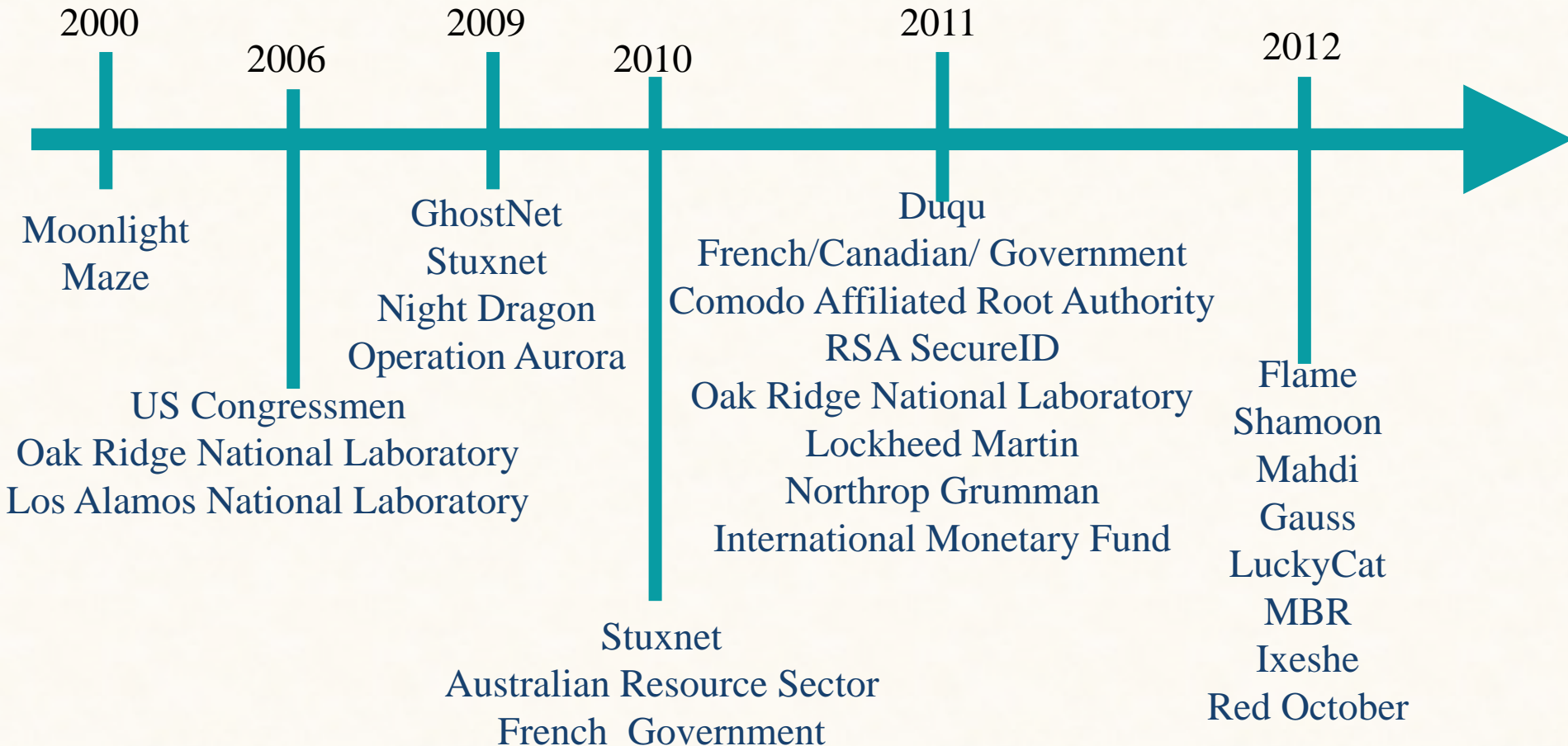
凤凰网 军事
mil.ifeng.com

凤凰网资讯 > 军事 > 环球军情 > 正文

“震网”：首个专门攻击物理基础设施的蠕虫病毒

一年前，美国和以色列曾警告说，伊朗只需一年就能拥有制造核武器的能力，但2011年2月伊朗突然宣布暂时卸载首座核电站的核燃料，从而西方国家认定伊朗的核计划因“技术问题”而被拖延。为什么会突然出现如此重大变化？原因是该核电站自2010年8月启用后，一种名为“震网”（Stuxnet）的蠕虫病毒，侵入了西门子公司为核电站设计的工业控制软件，导致1/5的离心机报废。

APT: 新兴安全威胁



急速升温

APT：新兴安全威胁

APT危害极大：

Operation Aurora

- Google、Adobe等20多家公司遭受攻击
- IT巨头的源代码、用户资料泄露

Stuxnet攻击

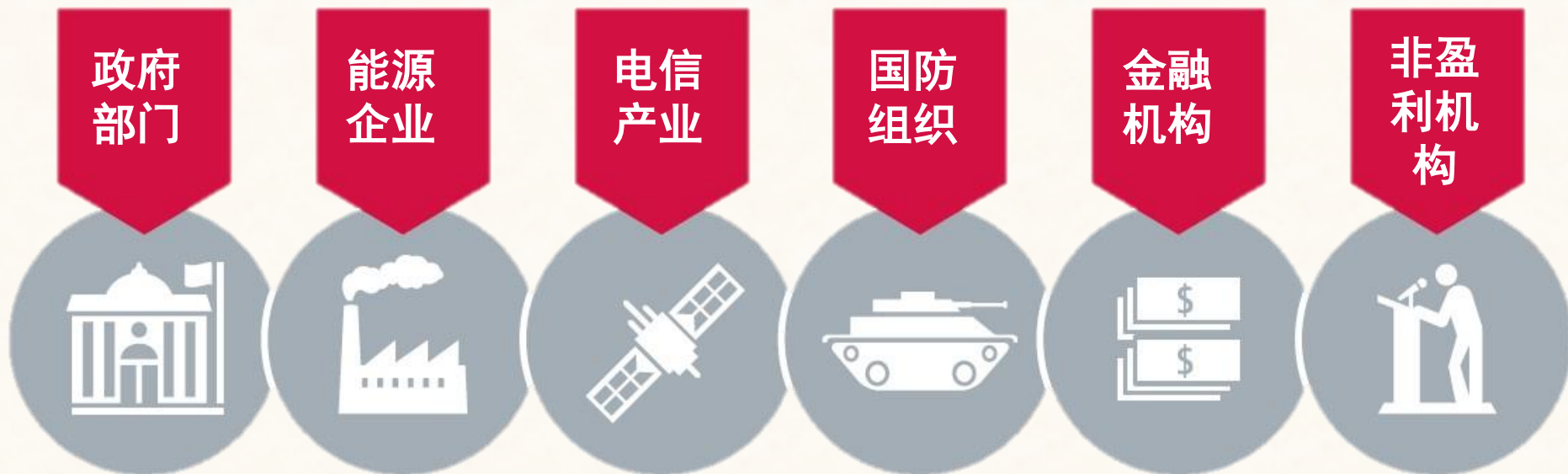
- 伊朗核设施瘫痪，核进程推迟近两年
- 震网病毒扩散传播后伊朗钢铁、电力、能源、化工等重要行业运行异常、商业资料失窃、停工停产

RSA SecureID泄露

- 相关技术及客户资料被窃，导致大量使用SecureID作为认证凭据建立VPN的公司受到攻击
- 美国企业、政府等关键组织接连遭黑客攻击

APT：新兴安全威胁

作用于核心机构：



- 威胁国家安全稳定
- 对企业经济、信誉造成严重损害
- 影响行业、企业正常运营

APT起源

“APT”一词最初起源于2005-2006年间在美国空军工作的网络安全工程师们对于一些安全事件的描述，他们创造了这个词以使公众不在此类安全事件小题大做……

---Peter Cap 在 Bruce Blog 上的留言



Peter Cap

Threat Analyst at Microsoft

Redmond, Washington | Computer & Network Security

Previous Symantec Corporation, US Navy

Education Beloit College

Send Peter InMail

Bruce Schneier

Schneier on Security

A blog covering security and security technology.

[« Unlocking any iPad2 using a Smart Cover »](#) | [Main](#) | [Commentary on Strong Passwords »](#)

November 9, 2011

Advanced Persistent Threat (APT)

It's taken me a few years, but I've come around to this buzzword. It highlights an important characteristic of a particular sort of Internet attacker.

A conventional hacker or criminal isn't interested in any particular target. He wants a thousand credit card numbers for fraud, or to break into an account and turn it into a zombie, or whatever. Security against this sort of attacker is relative; as long as you're more secure than almost everyone else, the attackers will go after other people, not you. An APT is different; it's an attacker who -- for whatever reason -- wants to attack you. Against this sort of attacker, the absolute level of your security is what's important. It doesn't matter how secure you are compared to your peers; all that matters is whether you're secure enough to keep him out.

APT attackers are more highly motivated. They're likely to be better skilled, better funded, and more patient. They're likely to try several different avenues of attack. And they're much more likely to succeed.

Peter Cap • November 9, 2011 3:33 PM

Well, Bruce, welcome to the debate, pull up a chair, make yourself comfortable.

Brief background--"APT" was originally coined in 2005 or 2006 by analysts working netsec issues for the Air Force. They created this term to discuss a *particular* threat with the press without invoking its classified covername. So, originally, it was actually meant to be a *name*--it could just as easily have been Biff or Steve or Maggie.

Later on, people who heard the term but did not necessarily do work in this area took it to stand for a *class* of threats. Then began the discussion on the nature of "advanced" when their typical M.O. involves spear-phishing and exploits from 2008 (ok, I'll allow that the methods of controlling their malware can get quite exotic) and how you define "persistent" (including one school that thought it meant "Patient and determined to get into your network" while another group insisted it meant "Once they establish a foothold, they will spread laterally and you will never get rid of them"--note that these are not mutually exclusive definitions).

Ultimately, as analysts, we use terms like "APT" as a shortcut--we take a whole body of data and slap a label on it--then we only work with that simple thought object rather than a giant data set. Only, if you do not already grok that data set, then the label really is devoid of value for you.

So, Maxim #1 for this post--if you are not actively engaged in analyzing and countering APT, then you have no business using the term, because it is a foreign word whose meaning you don't really understand. I mean this in the nicest possible way, not to shut anyone out, but just to make them aware that when you say "APT" it is a placeholder for a massive body of work that goes back over a decade and is truly globe-spanning. Not a space for dilettantes.

The corollary is that, as analysts, we use terms like this to *reduce ambiguity and complexity*. Therefore, if we fail at either then we are actually doing more harm than good.



Subscribe



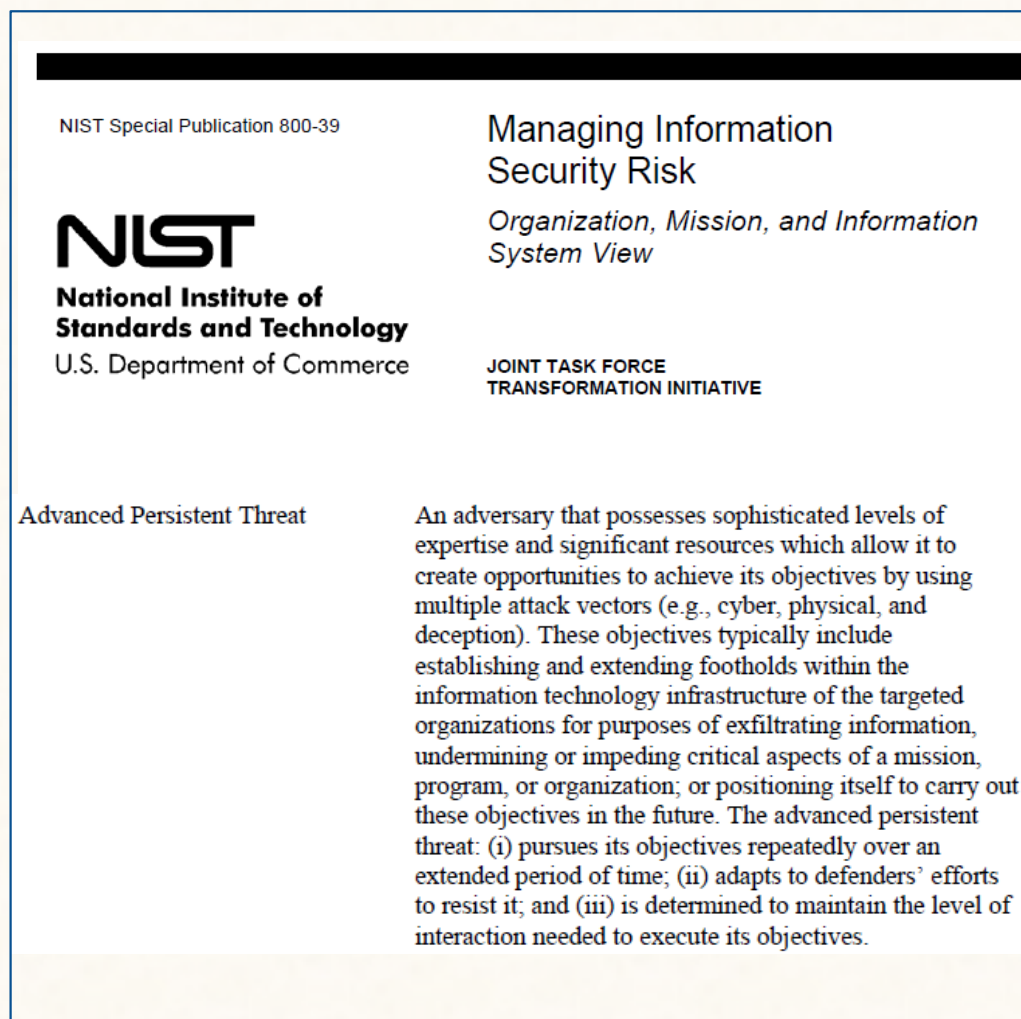
Subscribe via Kindle

APT定义

高级持续性威胁

——攻击者掌握**先进的专业知识**和**丰富有效的资源**，通过**多种攻击途径**(如网络、物理设施和欺诈手段等)，实现在特定组织的信息技术基础设施创建立足点，以窃取机密信息，破坏或阻碍任务、计划或组织的关键环节。此外，APT**会长时间重复地为实现其目标而努力**，能够**不断适应防御者**并产生抵抗能力，并为了达到目标**维持必需的交互和更新**。

美国国家标准与技术研究院
2011(NIST SP 800-39)





主要内容

CONTENTS

1. APT简介
2. APT解析
3. APT检测

APT实例(Aurora 极光)

概述


Motivation

攻击意图

- 窃取Google等公司的登录凭据、源代码及其他知识资产
- 窃取Gmail用户信息

Target

攻击目标



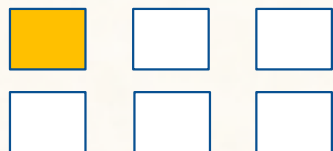
- Google为代表的高科技企业

极光是首个流行的对企业的APT攻击

APT实例(Aurora 极光)

1

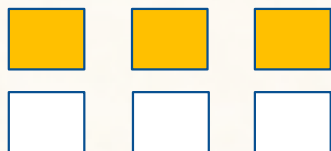
0day漏洞



CVE-2010-0249

3

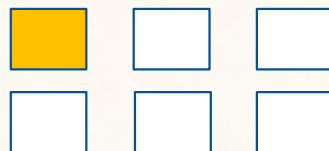
文件



%System%\[RANDOM].dll
%System%\acelpvc.dll
%System%\VedioDriver.dll

1

系统服务



RaS

[FOUR RANDOM CHARACTERS]

6

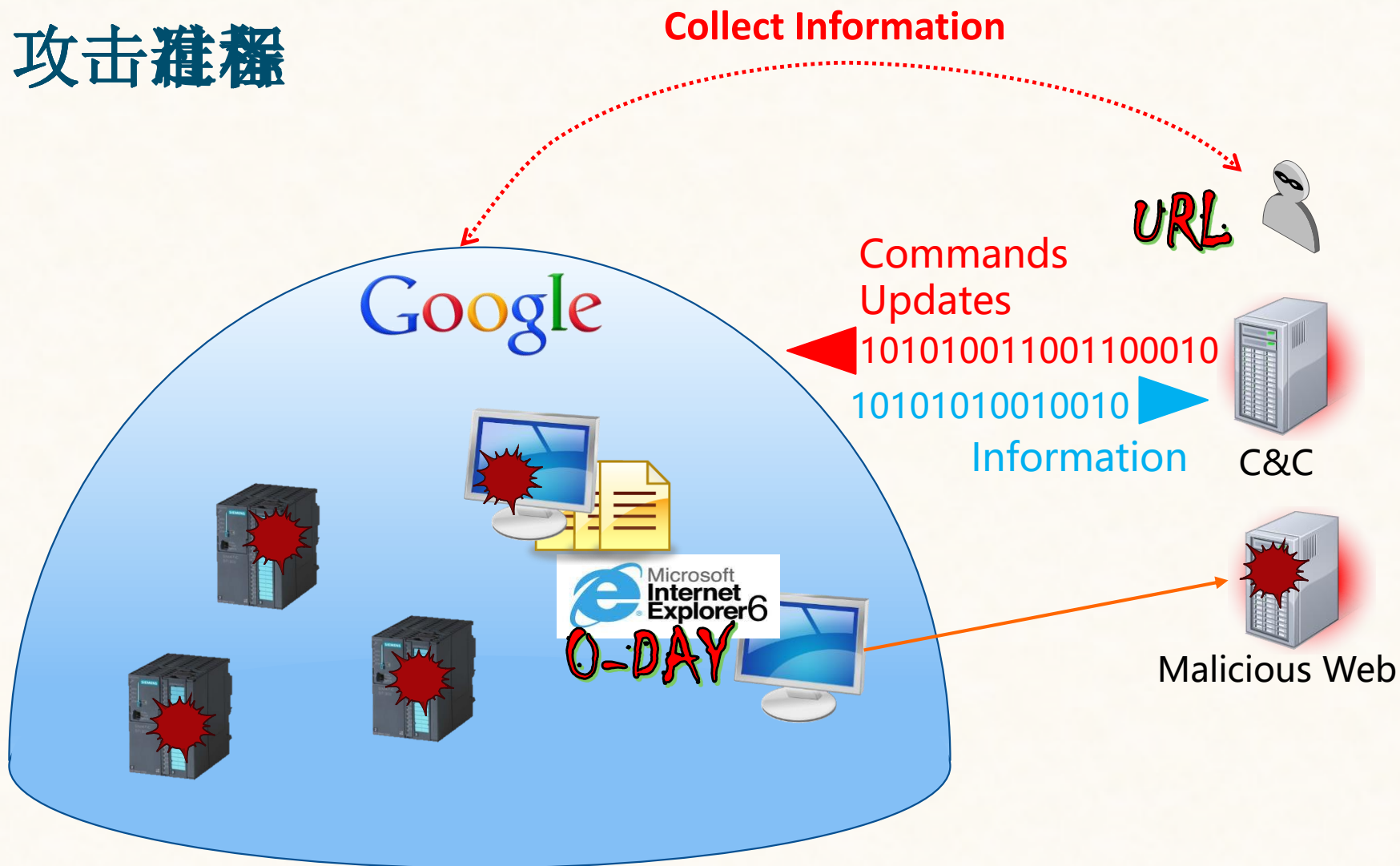
URL



yahooo.8866.org
sl1.homelinux.org
360.homeunix.com
li107-40.members.linode.com
ftp2.homeunix.com
update.ourhobby.com
blog1.servebeer.com

APT实例(Aurora 极光)

攻击流程



APT实例:(Stunex 震网)

概述

Motivation

攻击意图

- 改写工业控制系统代码，使工业系统按照攻击者的意图工作
- 向系统操作员隐藏其修改

Target

攻击目标



- 伊朗核电设施

Result

攻击后果

- 伊朗纳坦兹的核设施被破坏
- 伊朗布什尔核电站推迟启动

震网被称为第一个网络空间战武器

APT实例:(Stunex 震网)

先进性

4

0day漏洞



CVE-2008-4250
CVE-2010-2568
CVE-2010-2729
CVE-2010-2743

2

SCADA漏洞



硬编码漏洞
DLL加载策略缺陷

3

RootKit



2 Windows Rootkit
1 PLC Rootkit

2

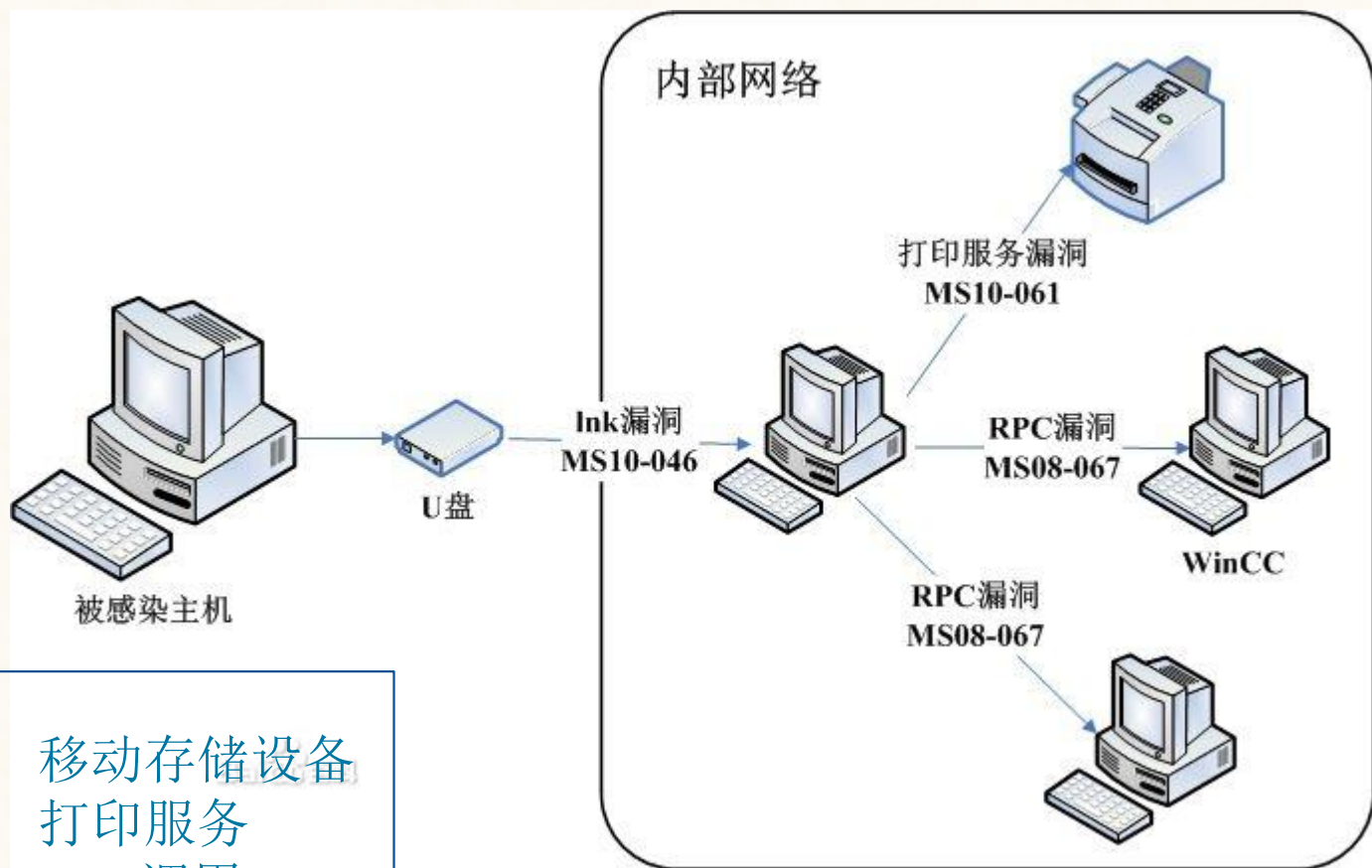
数字签名



Realtek Semiconductor
Corps
JMicon Technology Corps

APT实例:(Stunex 震网)

扩散



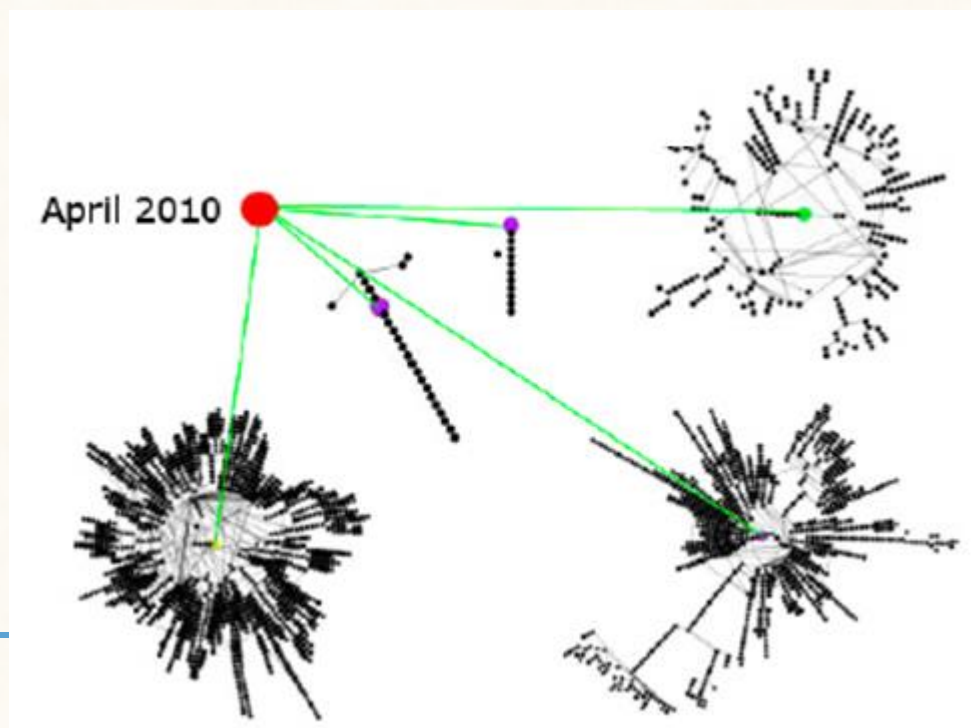
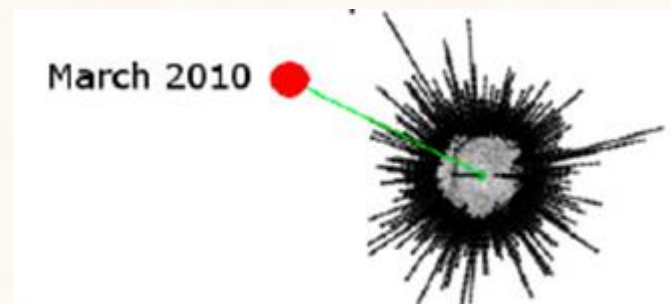
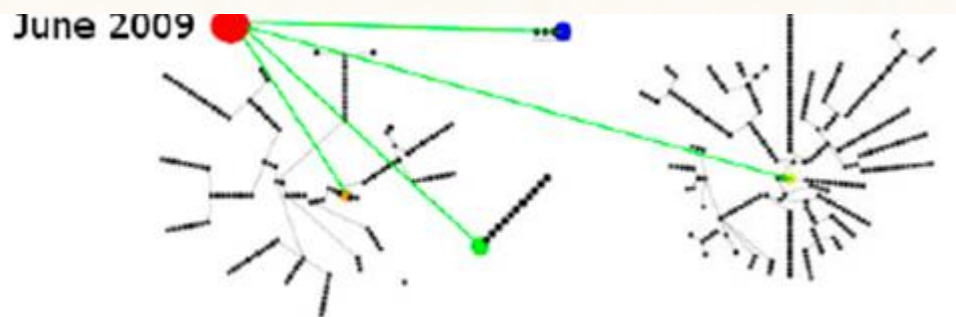
3



移动存储设备
打印服务
RPC调用

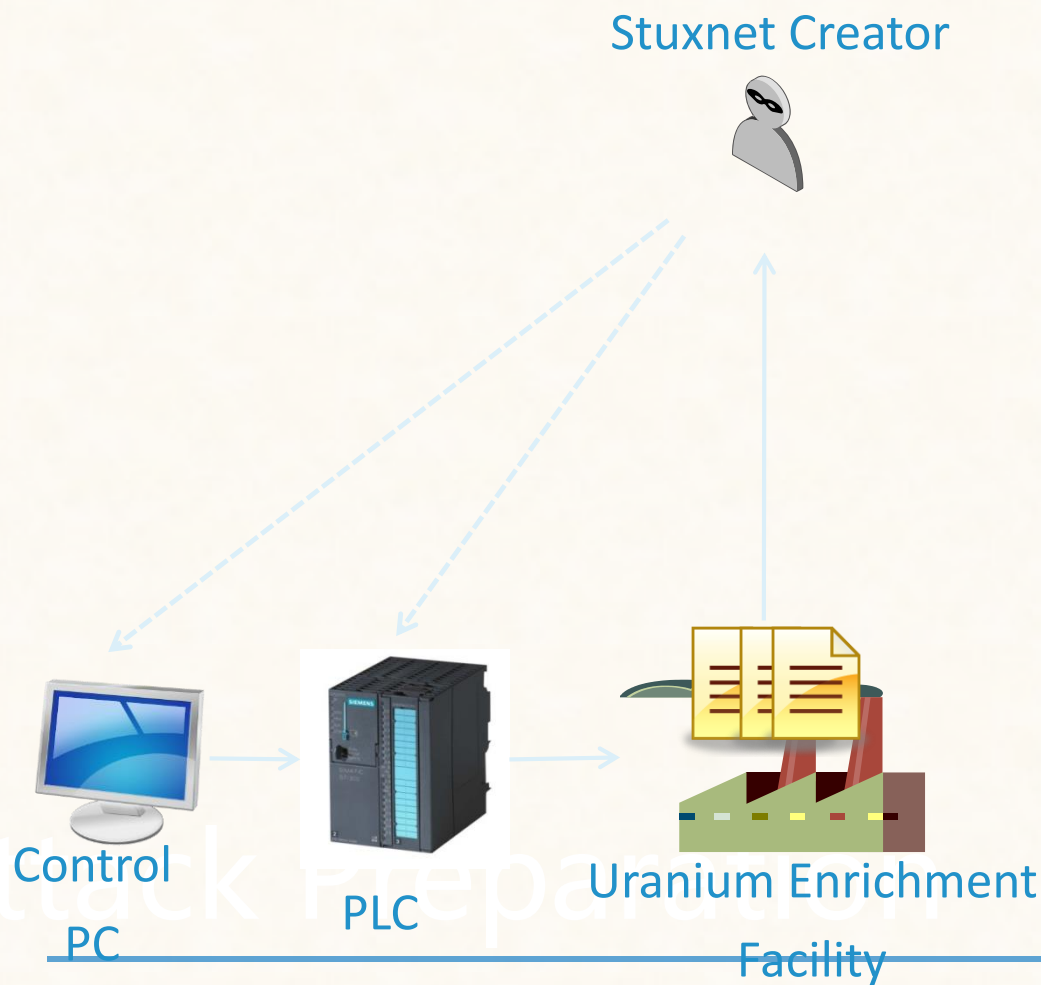
APT实例:(Stunex 震网)

扩散效果图



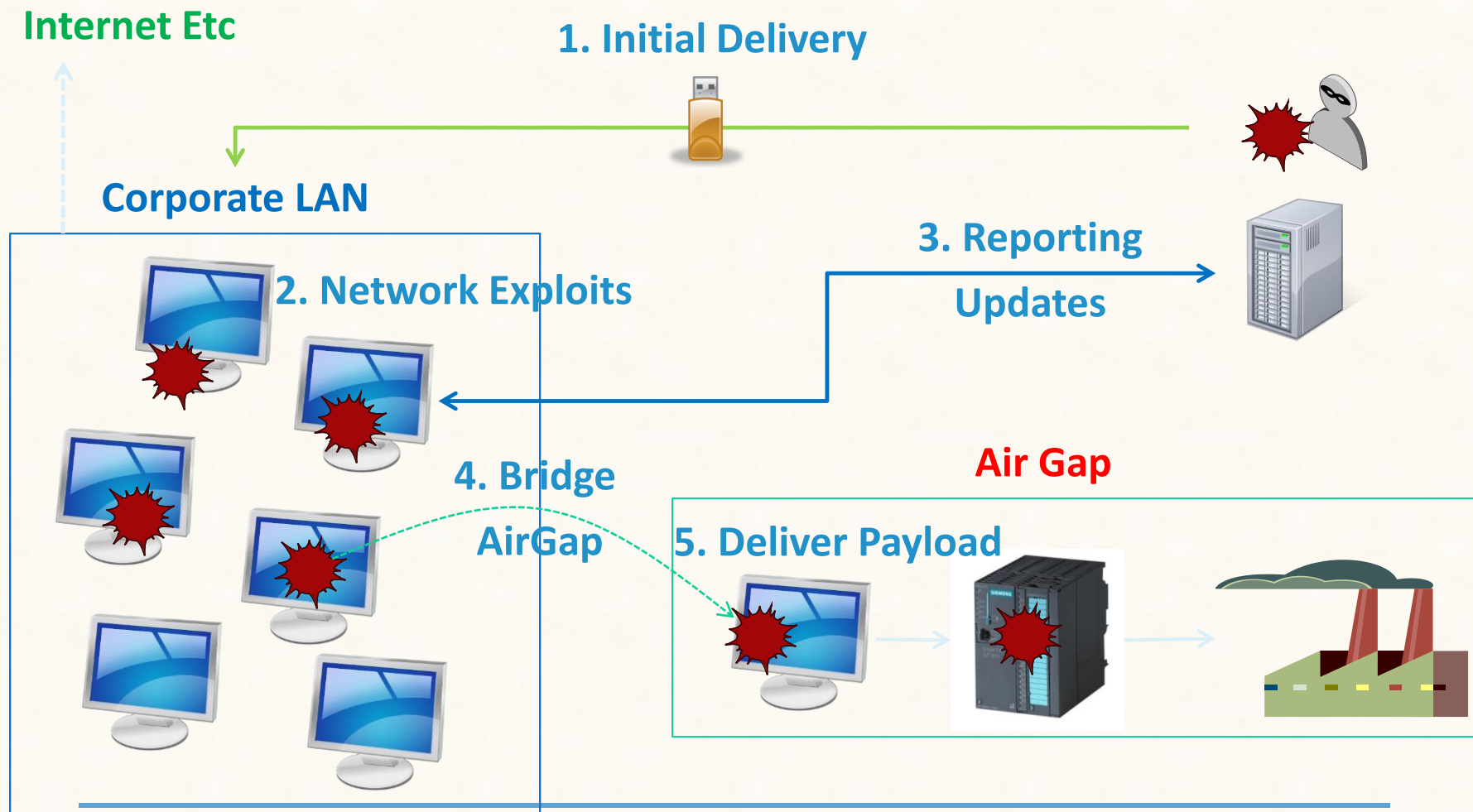
APT实例:(Stunex 震网)

攻击准备



APT实例:(Stunex 震网)

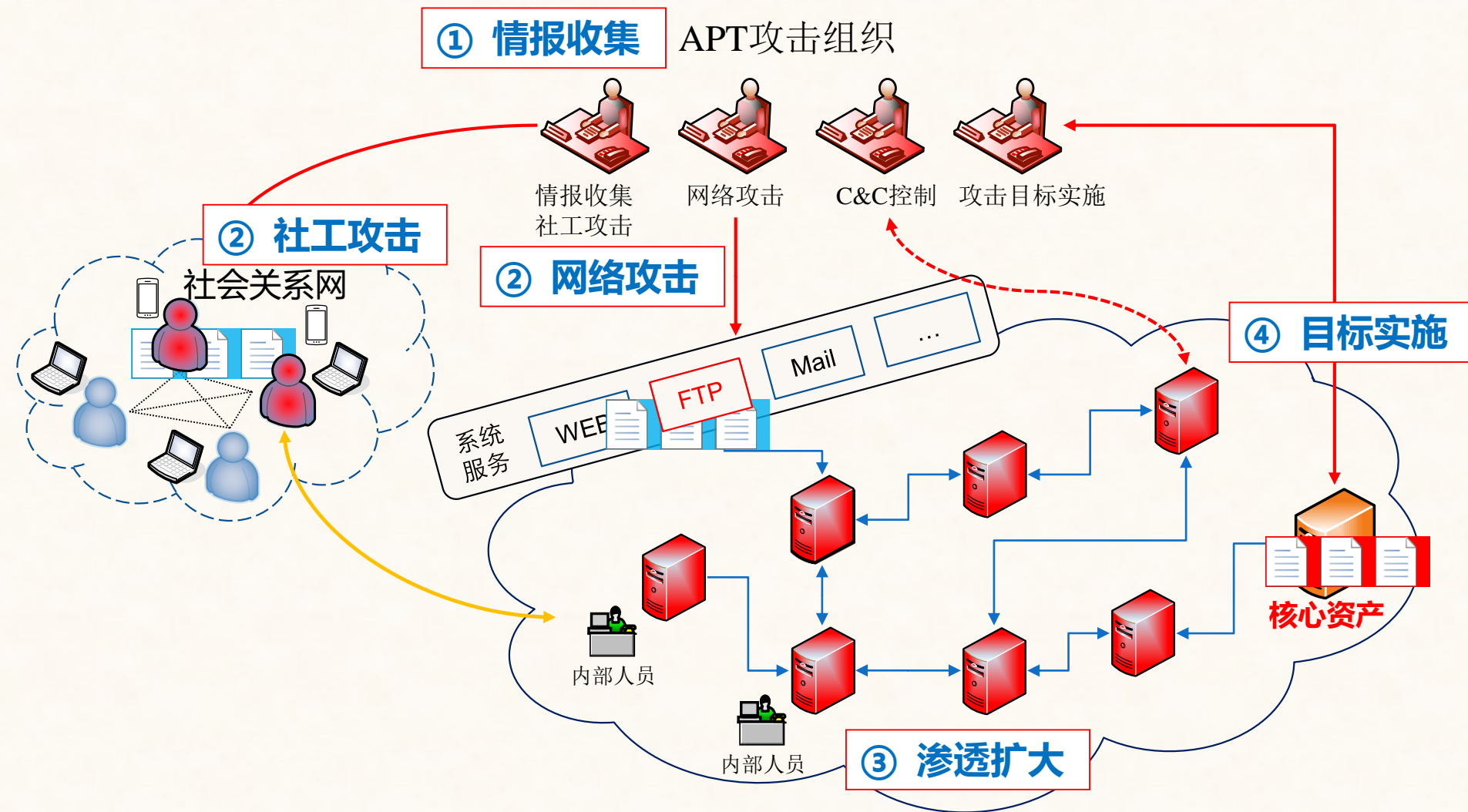
攻击过程



APT生命周期



APT攻击解析

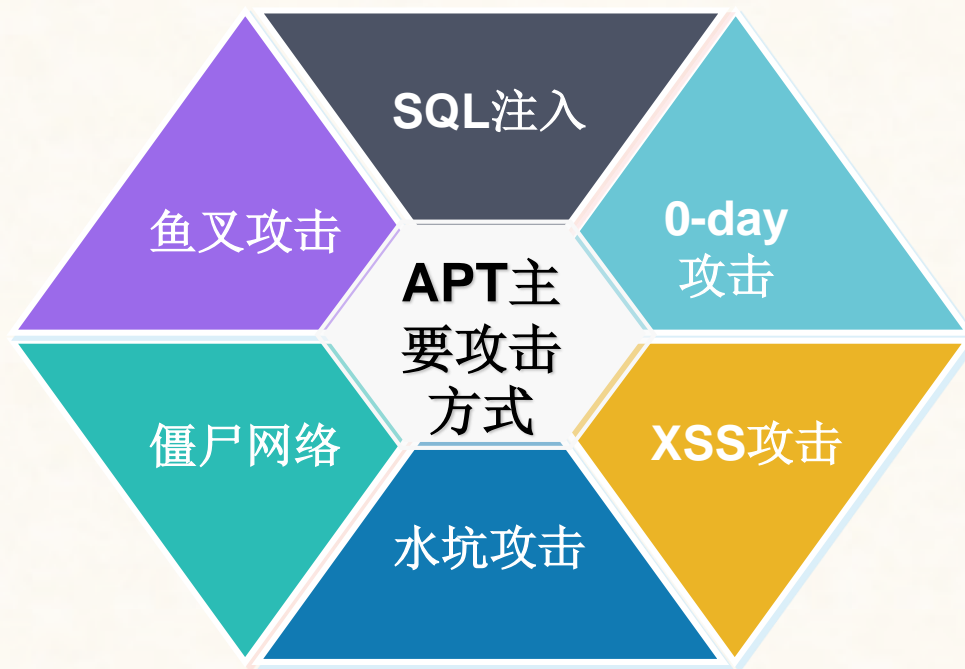


APT攻击的特点

APT 攻 击



APT攻击方式



APT攻击是多种攻击形式的混合利用。

水坑攻击

黑客通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待被攻击者来访时实施攻击。

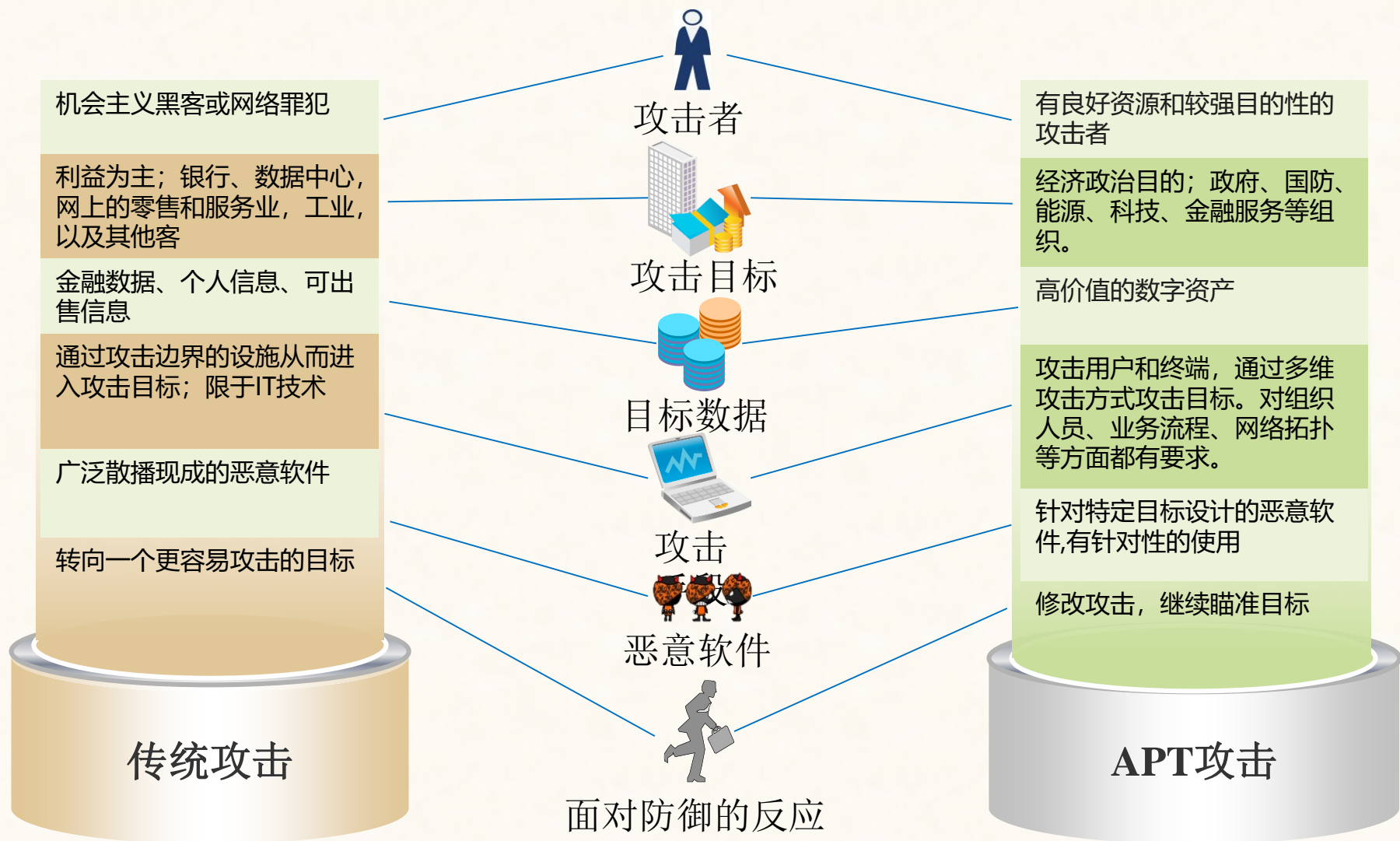


鱼叉式网络钓鱼

- 鱼叉式网络钓鱼（Spear phishing）指一种源于亚洲与东欧[1]，只针对特定目标进行攻击的网络钓鱼攻击。
- 锁定之对象并非一般个人，而是特定公司、组织之成员，故受窃之资讯已非一般网络钓鱼所窃取之个人资料，而是其他高度敏感性资料，如智慧财产权及商业机密



APT vs. 传统攻击



APT vs. 传统攻击

攻击形式	攻击定向性	传播性	可控性	窃密性	危害
APT攻击	高度定向	定向传播	完全可控	主要目的	基础设施、敏感信息等全面威胁
僵尸网络	定向	具备	可控	有	被控攻击
蠕虫	不定向	主动传播	不可控	无	影响网络、系统
木马	定向	较弱	可控	有	信息窃取为主
病毒	不定向	用户干预	不可控	无	破坏系统

安全措施亟待提升

APT攻击通常定制攻击，能够避开传统安全工具的检测

A

传统安全工具无法将攻击事件关联起来，无法在长时间维度上检测攻击

P

APT攻击包括物理攻击、社工攻击等非网络攻击手段。能够对目标造成全面威胁

T

APT攻击是目标明确、定制化、智能的攻击。传统安全工具无法检测出攻击的总目标

T

Advanced
Persistent
Threat
Target



主要内容

CONTENTS

1. APT简介
2. APT解析
3. APT检测

APT攻击检测难点

- 攻击方式复杂
- 攻击手段多样
- 攻击来源不明

A特征

- 攻击持续时间长
- 攻击过程片段化

P特征

- 攻击数据量大
- 攻击产生告警多
- 关联分析难度大

大数据

APT攻击检测亟待解决的问题

微观角度

- 0day攻击
- 未知攻击

难以发现

宏观角度

- 攻击过程
- 攻击目的

片段化
难以还原

网外因素

- 社工方法
- 非电子化因素

难以发现
多被忽略

APT攻击检测——要点

- 攻击过程不可能完全隐身
 - 攻击过程还原
 - 攻击片段组合
 - 攻击数据挖掘
- 未知攻击可实现部分检测
 - 0day漏洞
 - 终端安全
 - 通信分析
- 特定目标重点防护
 - 安全技术
 - 安全管理

APT攻击检测——关联分析

- 通过数据之间的关系进行关联，将具有共同特征的数据统一处理
 - 地址
 - 邮件账号
 - 用户名
 - 即时通信、社交网络等身份
 - 关系
- 优点：直观、容易处理
- 缺点：很多数据不具有共同特征

APT检测方案

□基于0day漏洞和恶意软件检测的APT检测方案

■主要技术：沙箱隔离，终端执行控制



□基于大数据分析的全流量APT检测方案

■主要技术：大数据存储，应用和文件还原，数据关联性分析



AT&T SECURITY RESEARCH CENTER

APT检测方案

❑ 基于0day漏洞和恶意软件检测

● 检测原理

● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案

漏洞利用的软肋

操纵内存
部署代码

利用漏洞
跳转执行流

Shell Code
代码执行

没有能力影响执行逻辑

需要利用系统当中的特定指令、特定内存布局、需要内存属性变更

需要系统调用

APT检测方案

❑ 基于0day漏洞和恶意软件检测

● 检测原理

● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案

0day漏洞检测手段

操纵内存
部署代码

利用漏洞
跳转执行流

Shell Code
代码执行

内存布局侦测
内存块源头追踪
关键指令代码监控
预先内存占坑

系统调用入口埋点
系统调用环境检测
调用来源内存属性检测
调用链条回溯

APT检测方案

❑ 基于0day漏洞和恶意软件检测

● 检测原理

● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案

未知恶意代码软肋

必然落在一个**终端**上

必然要在此终端上**运行**

必然需要接触**敏感数据**

必然有**网络行为**

未知恶意代码检测

主动防御+隔离沙箱

---监控和审计程序的敏感行为，包括网络行为

---模拟执行环境，实行隔离

终端执行代码控制

---只运行经过检测的可信程序（白名单）

---将攻击者逼回到漏洞利用

APT检测方案

❑ 基于0day漏洞和恶意软件检测

● 检测原理

● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案



启发式追踪

- 利用启发式方法检测追踪恶意软件的外壳代码片段
- 片段拼接，识别攻击的真正意图



多维沙箱

- 领先的沙箱技术
- 多维虚拟执行



私有云安全系统

- 应用、文件可信管控
- 基于主机文件保护的私有云安全防护体系

APT检测方案

❑ 基于0day漏洞和恶意软件检测

● 检测原理

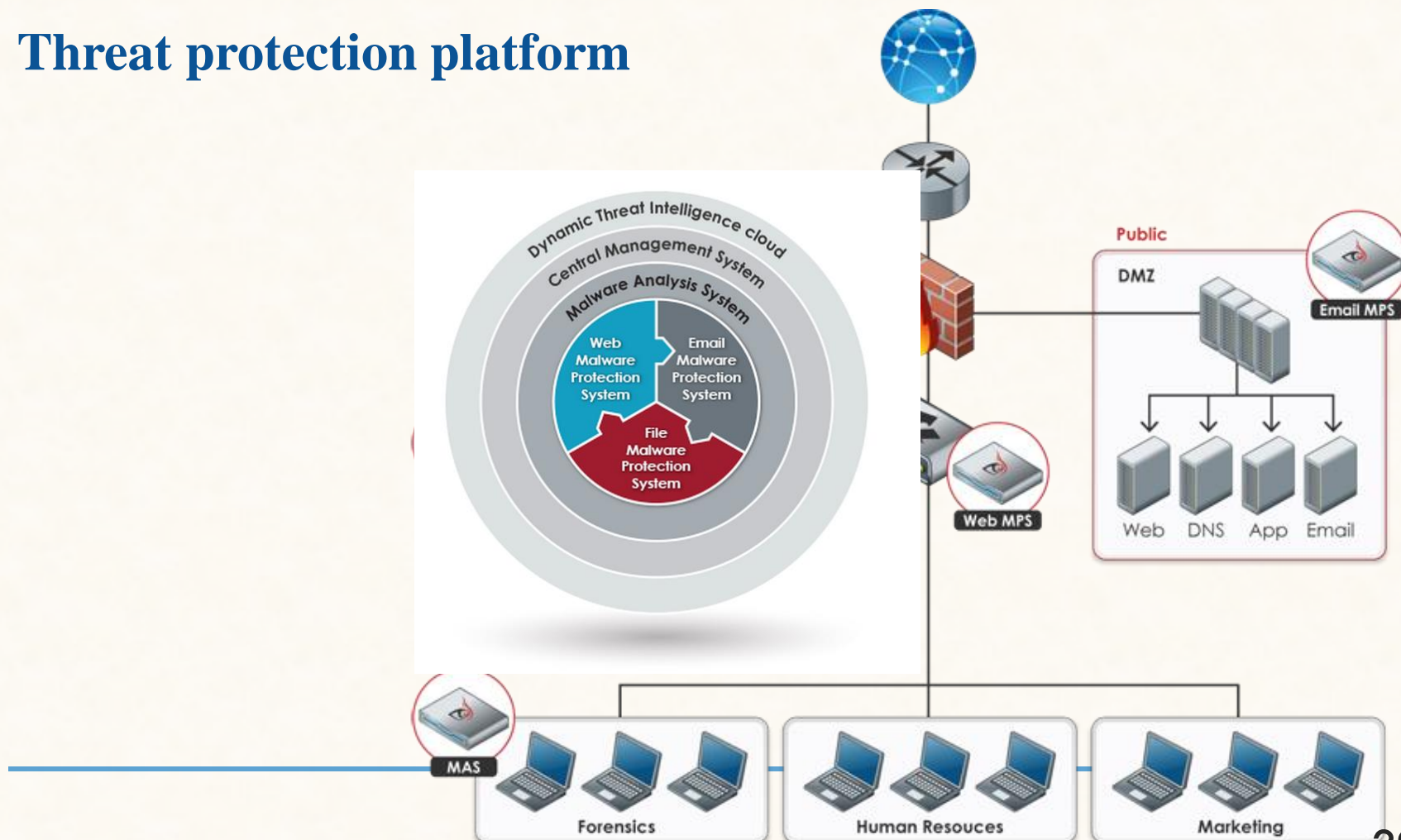
● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案

Threat protection platform

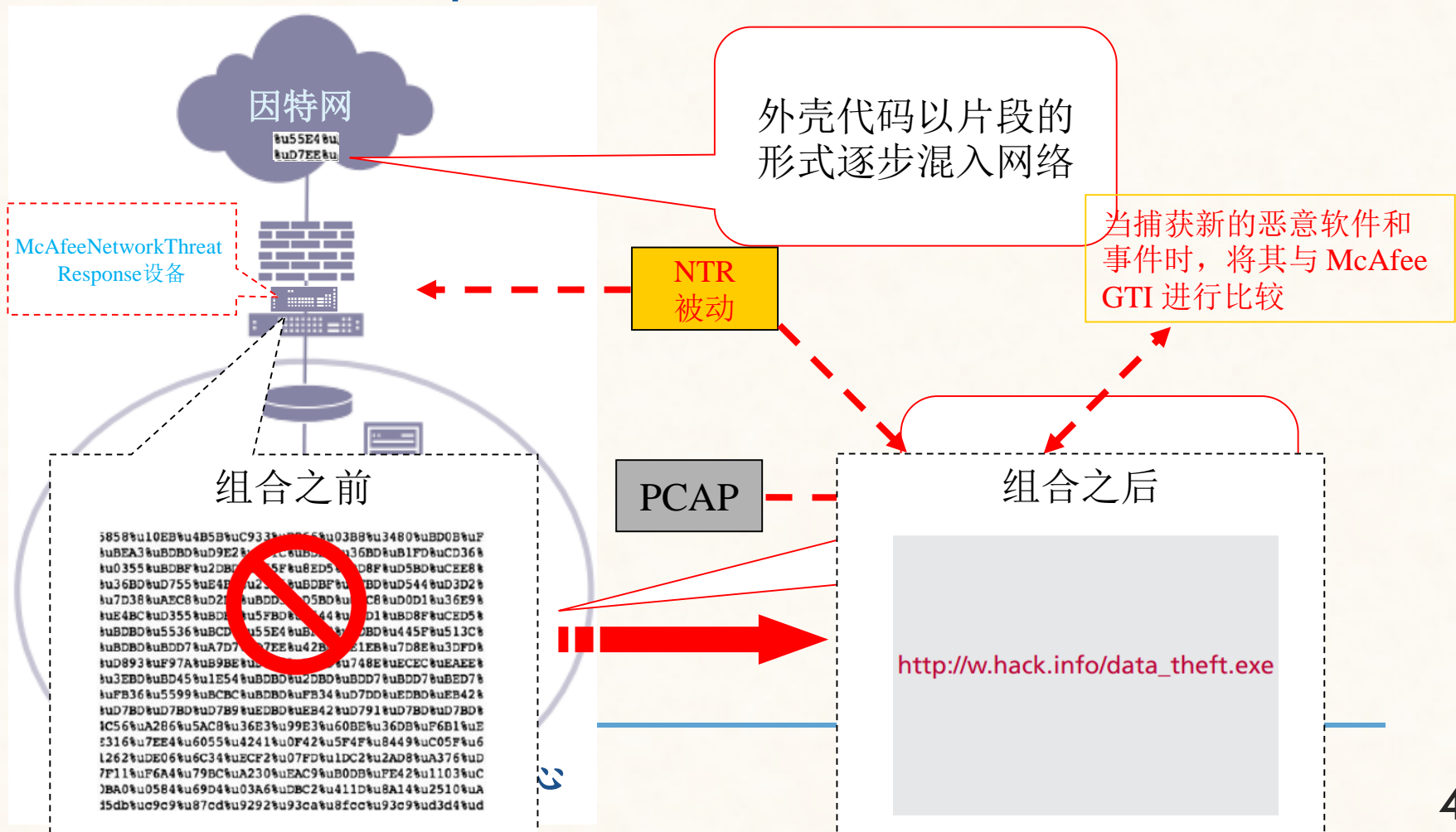


APT检测方案

❑ 基于0day漏洞和恶意软件检测
● 检测原理 ● 解决方案

❑ 基于大数据分析
● 检测原理 ● 解决方案

Network Threat Response



APT检测方案



❑ 基于0day漏洞和恶意软件检测

● 检测原理

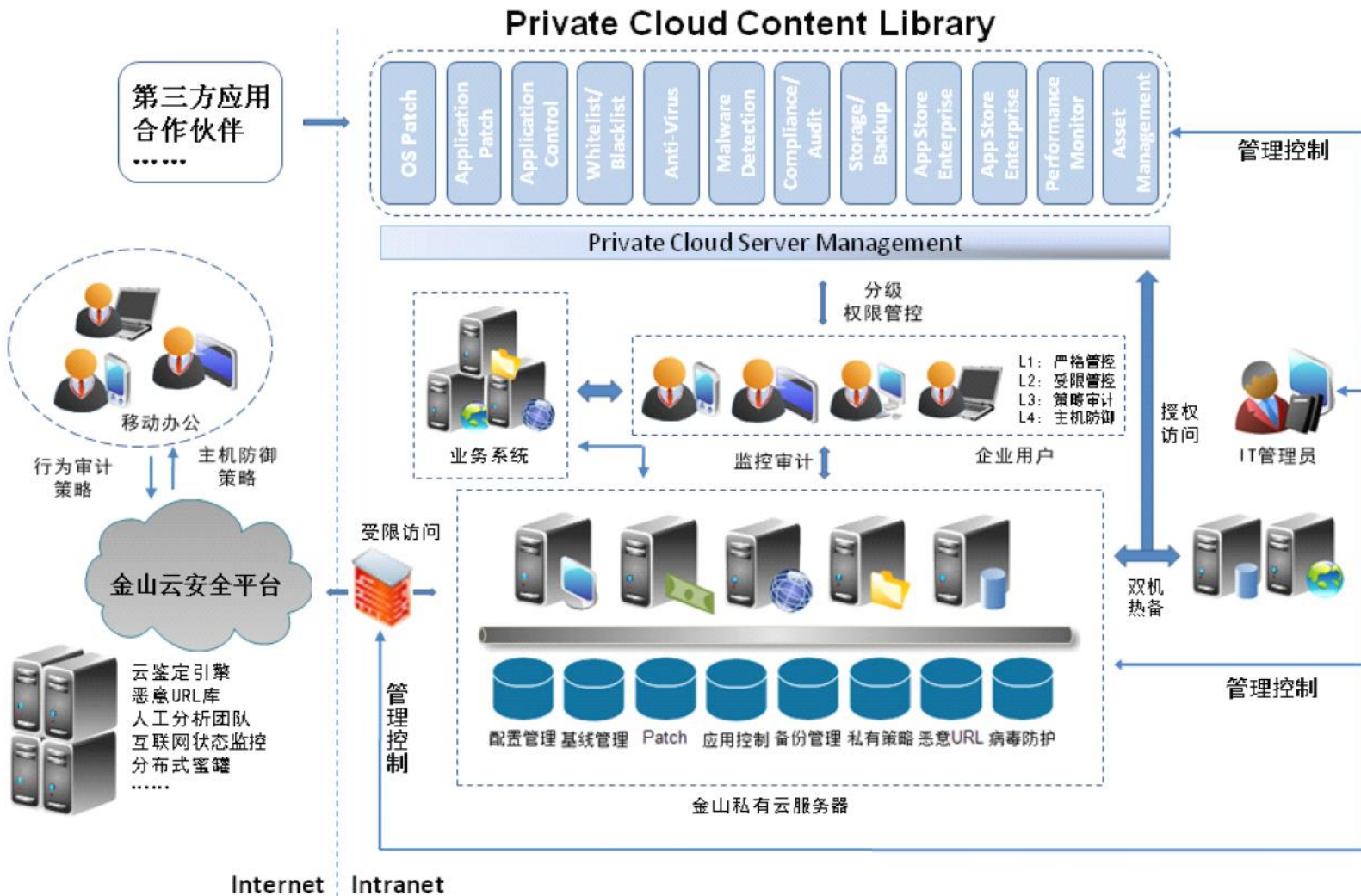
● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案

基于主机的白名单策略



APT检测方案

□ 基于0day漏洞和恶意软件检测
检测原理 解决方案

□ 基于大数据分析
检测原理 解决方案

APT特征

攻击特征难以提取

单点隐蔽性强

攻击渠道多样化

持续和隐蔽时间长

大数据分析

数据覆盖

-----时间：APT攻击整个过程；

-----空间：终端、网络、人员等的全记录；

全流量分析

-----数据降维，知识，关联性分析

APT检测方案

❑ 基于0day漏洞和恶意软件检测

- 检测原理
- 解决方案

❑ 基于大数据分析

- 检测原理
- 解决方案



SECURITY

大数据检测策略

- 搜集终端、服务器上的日志信息
- 搜集网络设备上的原始流量
- 数据处理、挖掘



AT&T SECURITY RESEARCH CENTER

基于上下文的大数据检测

- 时间维度上涵盖APT每一步骤的所有事件
- 空间维度上涵盖物理层、用户层和网络层三层所有安全事件
- 通过IP和用户组成安全事件的上下文

APT检测方案

RSA

❑ 基于0day漏洞和恶意软件检测

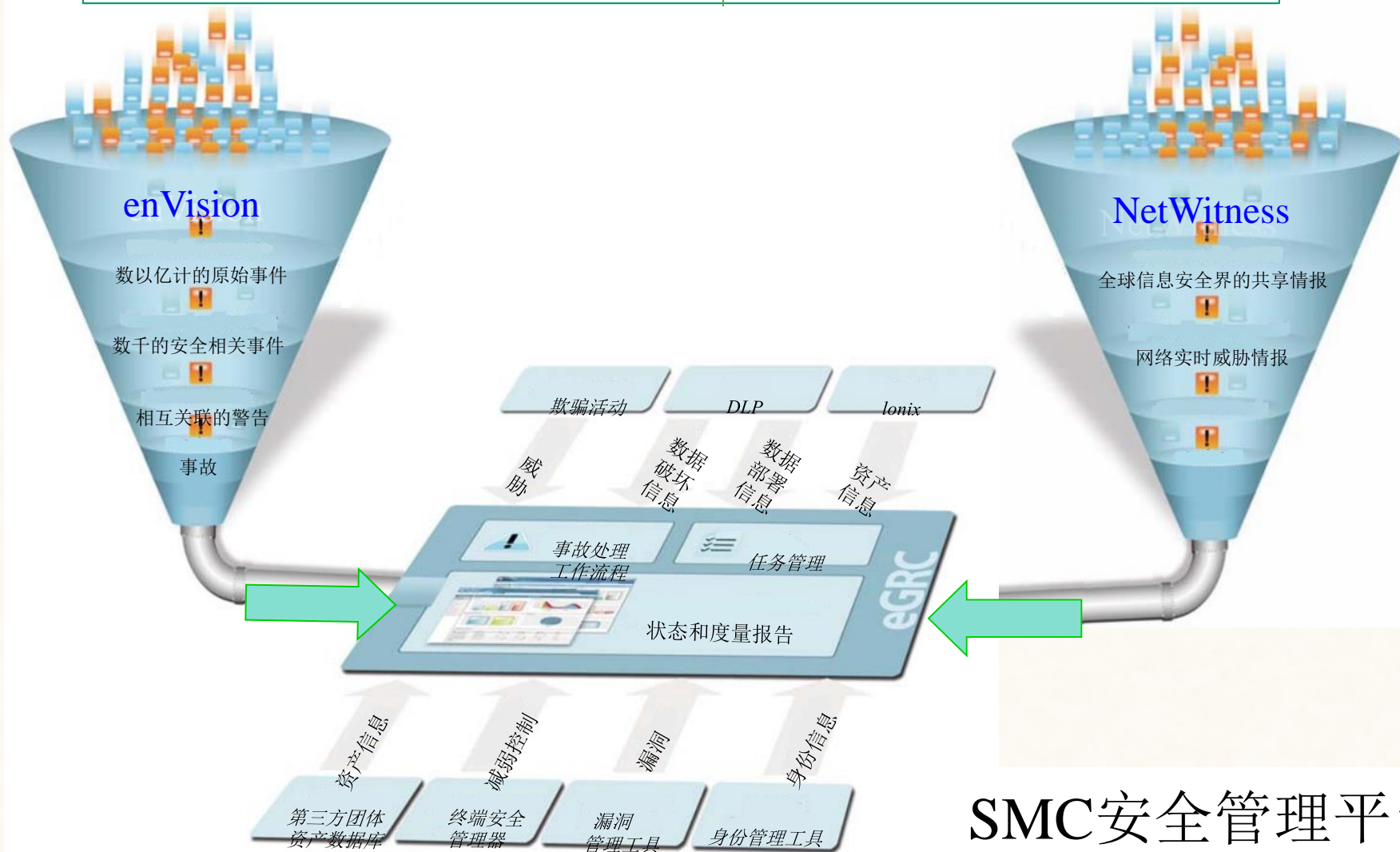
● 检测原理

● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案



APT检测方案

RSA

❑ 基于0day漏洞和恶意软件检测

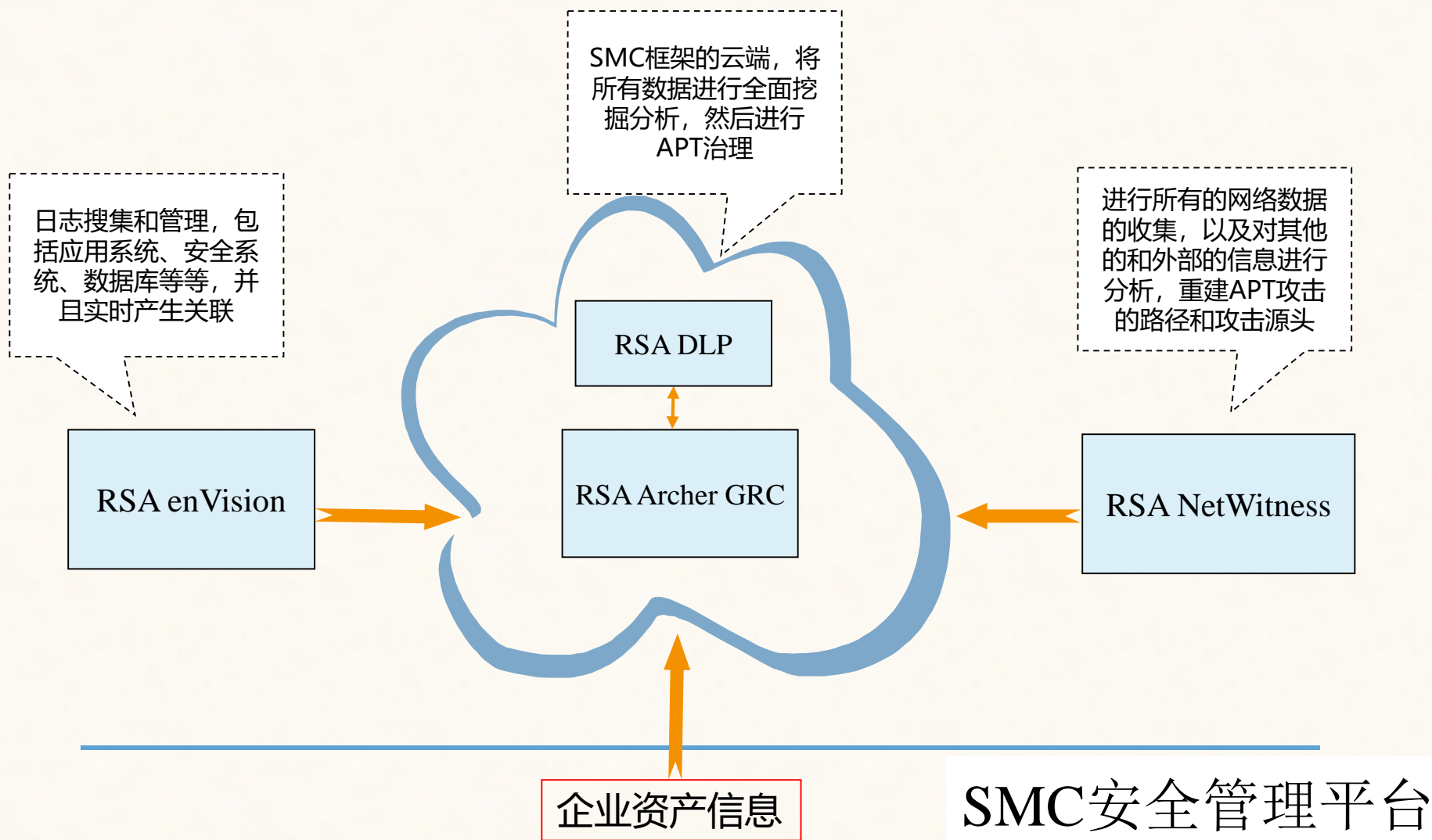
● 检测原理

● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案



❑ 基于0day漏洞和恶意软件检测

● 检测原理

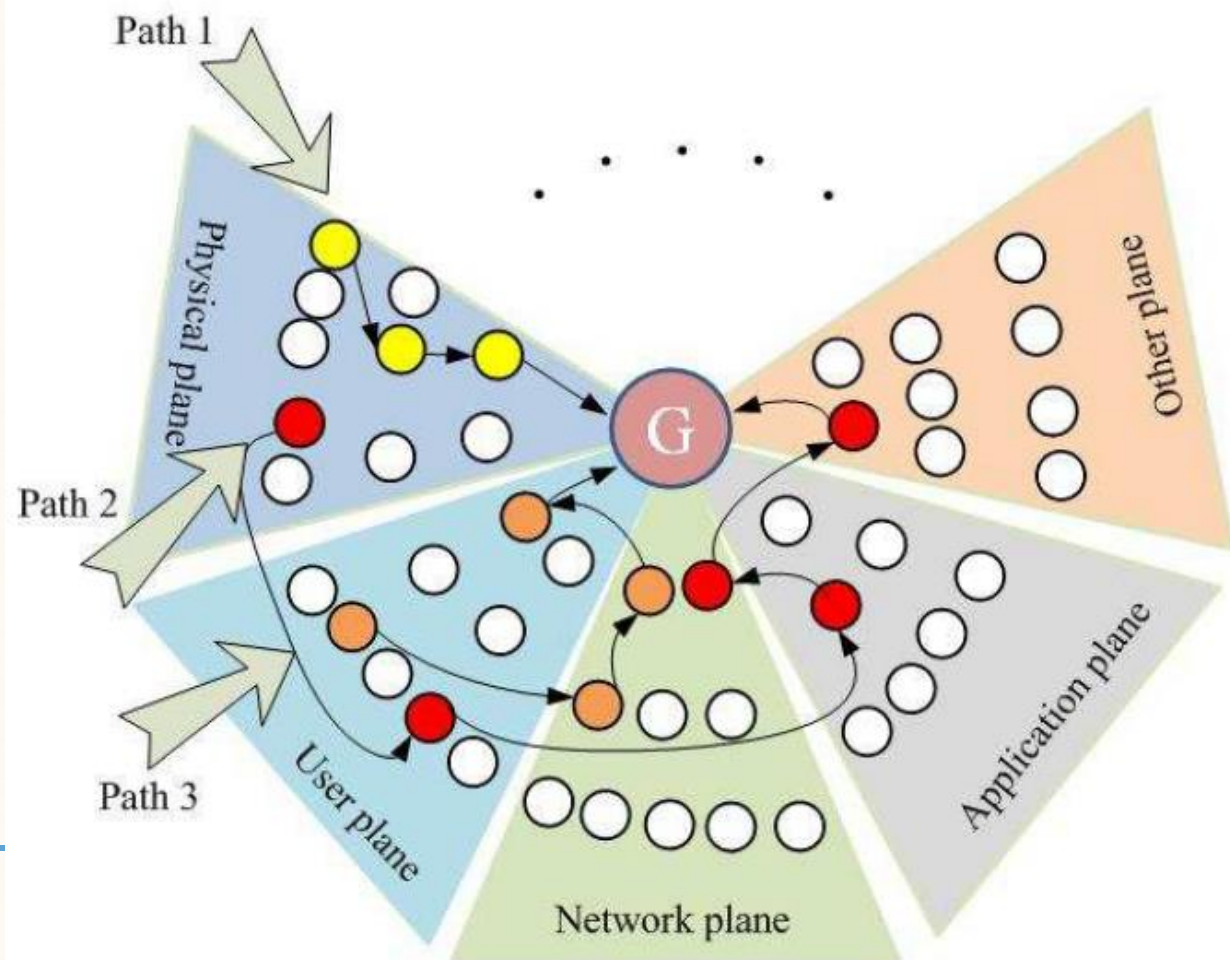
● 解决方案

❑ 基于大数据分析

● 检测原理

● 解决方案

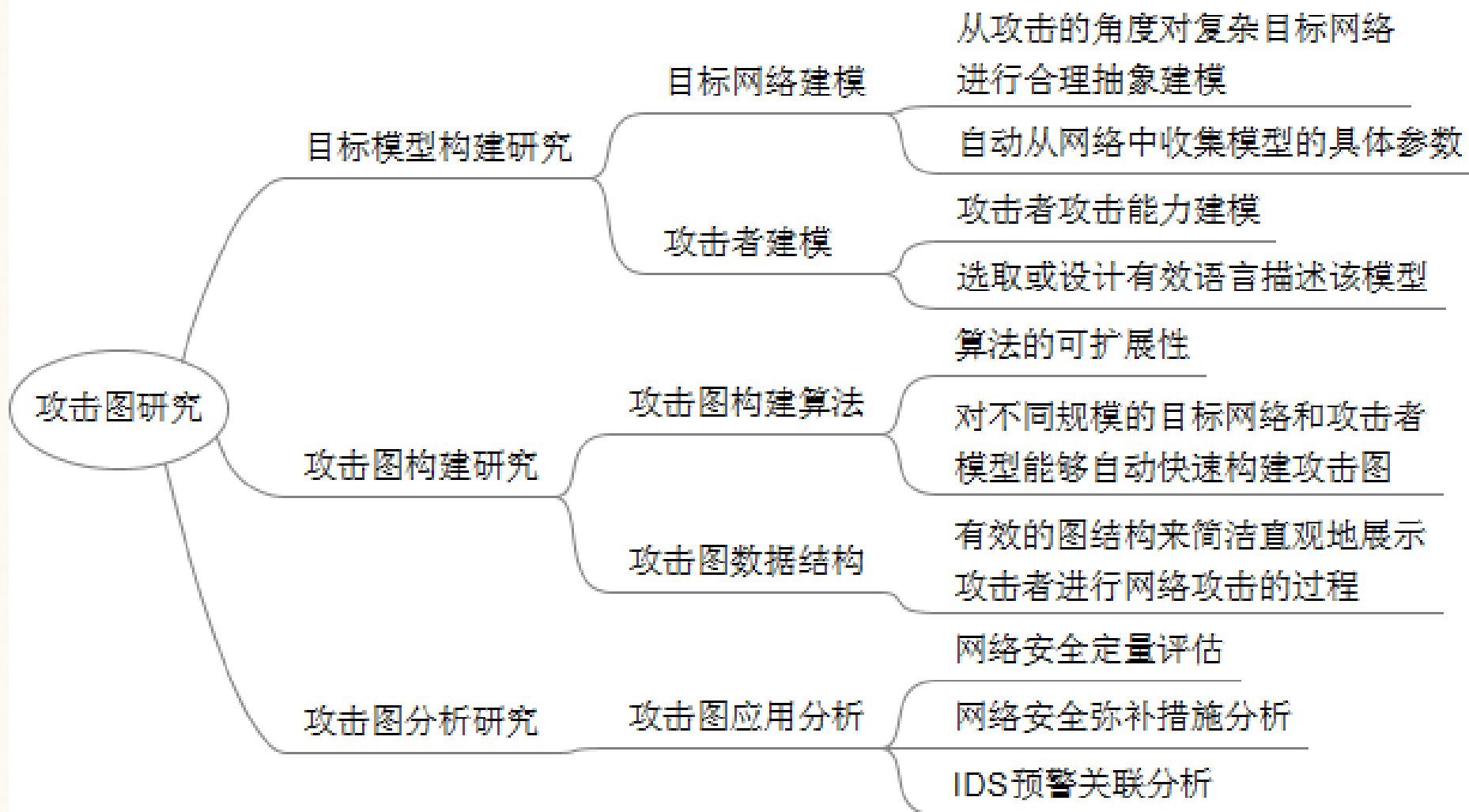
Content-Based APT Detection



APT检测方法——攻击图

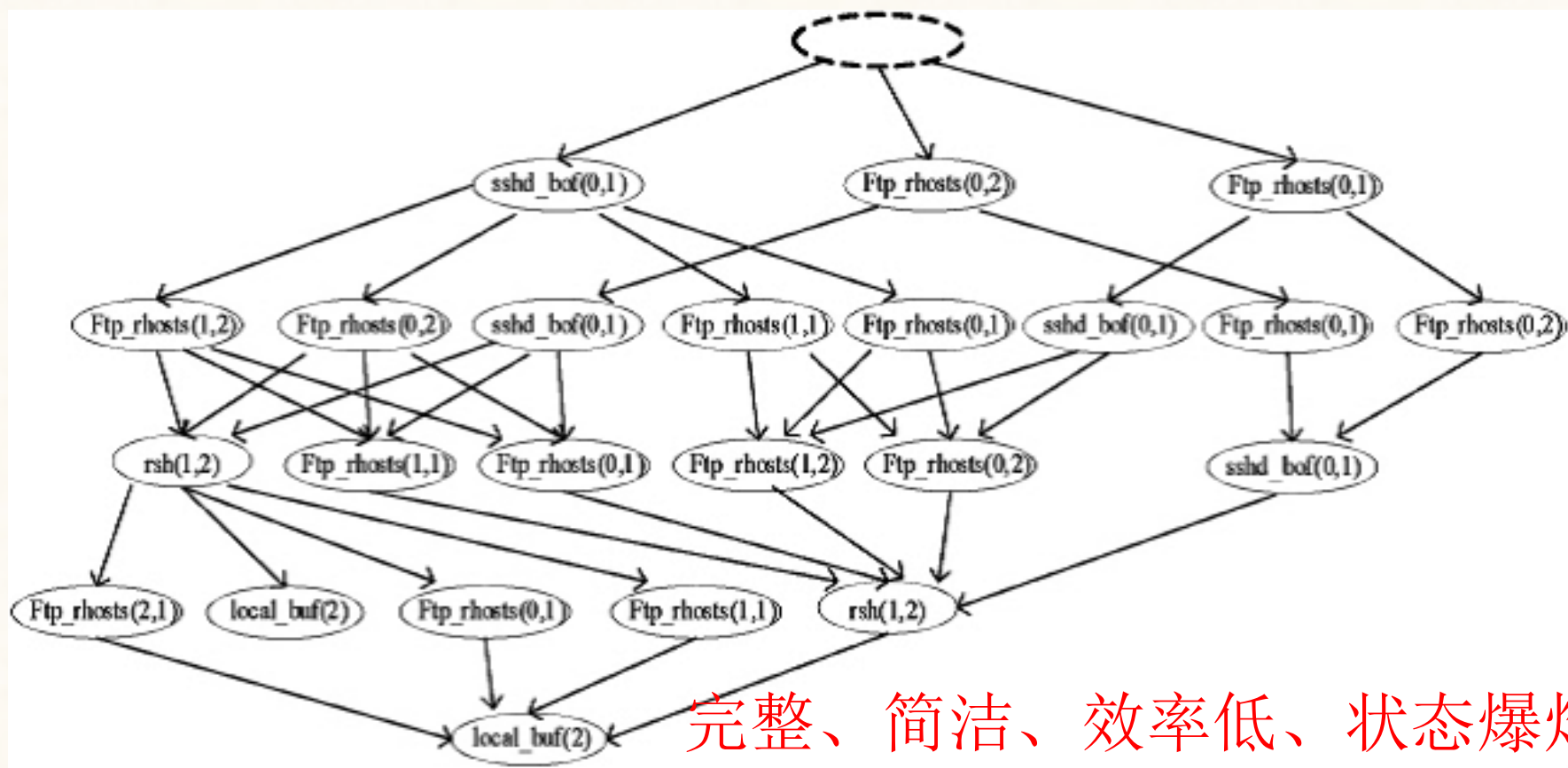
- 攻击图是**网络攻击建模技术**，它采用点和边的图形结构描述攻击场景。
- 在**目标网络建模**和**攻击者建模**的基础上，自动发现**系统脆弱性**间的关系，并根据攻击者和目标环境二者之间的相互作用关系计算产生攻击图。
- 展示**攻击路径**，并提供网络安全防护多方面的决策。
- 典型攻击图：**状态攻击图、属性攻击图、渗透依赖攻击图...**

APT检测方法——攻击图



状态攻击图

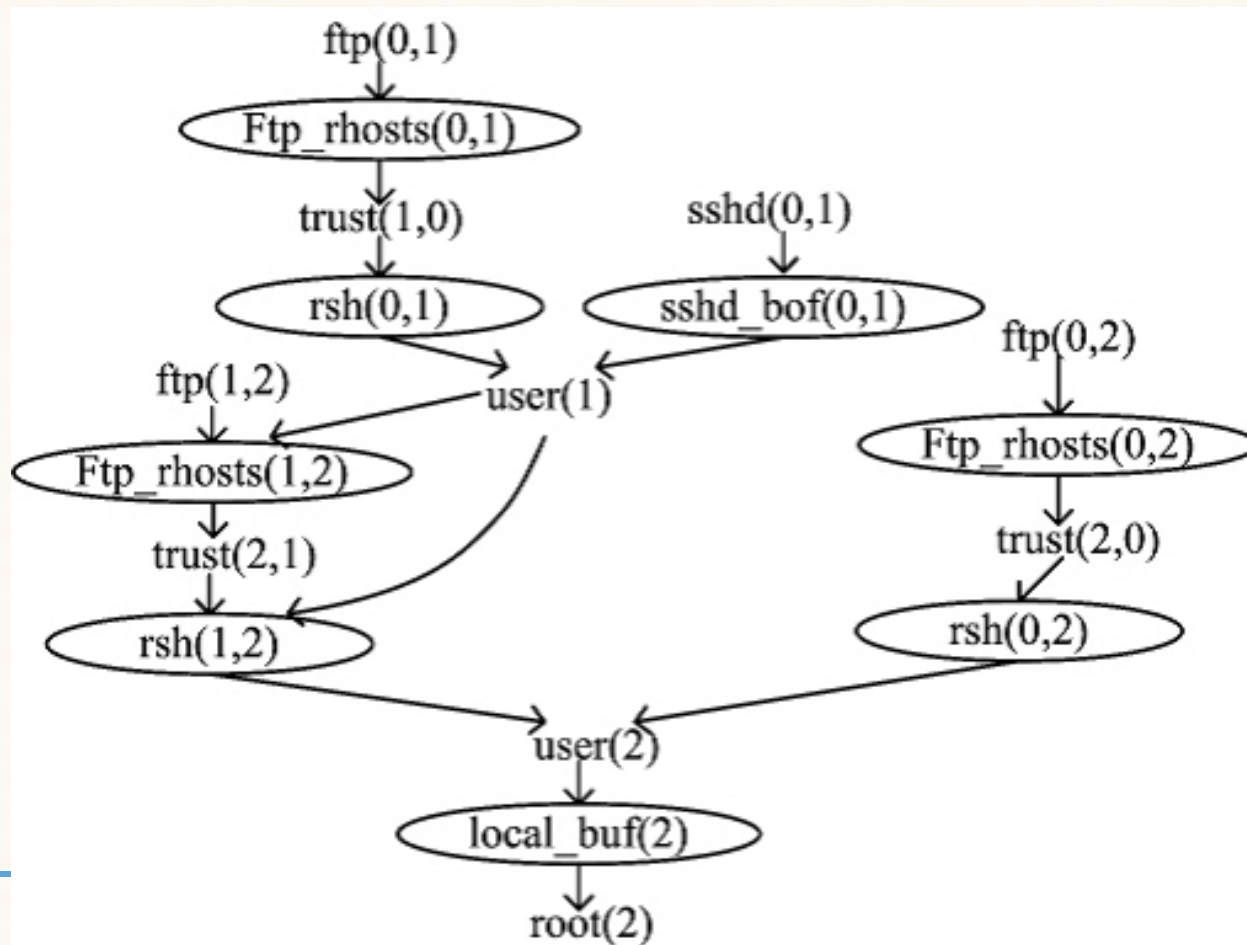
- 节点代表目标网络和攻击者的全局状态，节点内容通常包括主机名、用户权限、攻击的影响等。
- 每条弧代表原子攻击，它被执行后将会引起全局状态的变迁。



属性攻击图

椭圆：原子攻击节点；

文本：属性节点； 它表示这些原子攻击的每个前提或后果



攻击溯源

- APT攻击溯源的难点

- 攻击持续时间长，攻击起点、过程、终点难以确定；
- 攻击片段化，攻击间关联弱化，难以有效还原整个攻击过程；
- 攻击数据分散，分治式的安全防护难以获取完整攻击数据来源，导致攻击离散化
- 数据量大，处理难度大

路由安全

- **路由安全的重要性**
 - 物理位置上：网络核心节点
 - 逻辑位置上：数据汇聚点，决定性节点
- **路由安全威胁**
 - 系统漏洞、管理漏洞
 - 拒绝服务
 - 路由欺骗、干扰
- **路由安全防护**
 - 路由协议攻击检测
 - 路由器系统及管理攻击检测

思考

- **APT到底能不能够阻止？**
 - 做一个类比：个人安保
 - 个人：基本上没有安保措施
 - 明星：雇佣保镖
 - 总统：全方位的安全保护
- **APT攻击检测走向何方？**
 - 做一个类比：刑事案件
 - 发生：实际上是罪犯经过长时间多手段的准备及实施，治安措施（如摄像头）有部分记录可查
 - 破案：总能够找到蛛丝马迹，顺藤摸瓜
 - 结论：缺少明确保护目标导致检测失败

THANKS

欢迎提问
