文本

描述已自动生成

定义

攻击者行为特征：

1、在特定时段频繁访问其目标对象

2、避免被检测系统发现

3、is determined to maintain the level of interaction needed to execute

its objectives

普通攻击与APT的区别

1. 攻击可从多个角度避免
2. 攻击者不需要花费巨大的努力突破目标系统
3. 攻击过程并不具备新颖性

表格

中度可信度描述已自动生成

APT的五个阶段

1. 信息收集：包括但不限于公司的员工信息、网络设备（路由、防火墙、服务器等）、社工、公开的互联网资源（网站、ip、签名等）、硬件信息
2. 进入目标系统（网络或电脑）：手段包括利用已知应用漏洞、零日漏洞、恶意软件（钓鱼、水坑、网页下载）
3. 渗透转移：在目标系统的主机中转移（盗取账密）直到找到目标数据或应用表格

   描述已自动生成
4. 盗取数据/破环组件：泄露数据时通常将说数据分割间歇性发给服务器（服务器不同的ip地址）
5. 盗取/破坏后行为：消除入侵痕迹后离开目标系统或者继续隐藏

前两个阶段是必须的，后三个阶段依据目标不同而改变。

APT攻击的防御方法

图示

描述已自动生成

监测方法：

磁盘和内存的异常读写

流量监测关注于CTC连接的建立：使用的协议、端口、时间、大小

代码监测：对恶意软件的静态分析与动态分析

日志监测：内存、CPU、程序运行、系统日志，数据规范化、特征提取、聚类

异常检测：使用机器学习，无监督、监督、半监督学习

针对系统行为的基于序列的检测

若干机器学习方法：SVM 、Fuzzy Logic 、Genetic Algorithm、K-means

机器学习犯的第二类错误比较多

表格

描述已自动生成