APT 攻击与防护解决方案

APT 攻击介绍与危害：

高级持续性威胁(Advanced Persistent Threat，APT)，威胁着用户网络的数据安全。APT 是黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为，是一种蓄谋已久的“恶意间谍威胁”。这种行为往往经过长期的经营与策划，并具备高度的隐蔽性。APT 的攻击手法，在于隐匿自己，针对特定对象，长期、有计划性和组织性地窃取数据，这种发生在数字空间的偷窃资料、搜集情报的行为，就是一种“网络间谍”的行为。

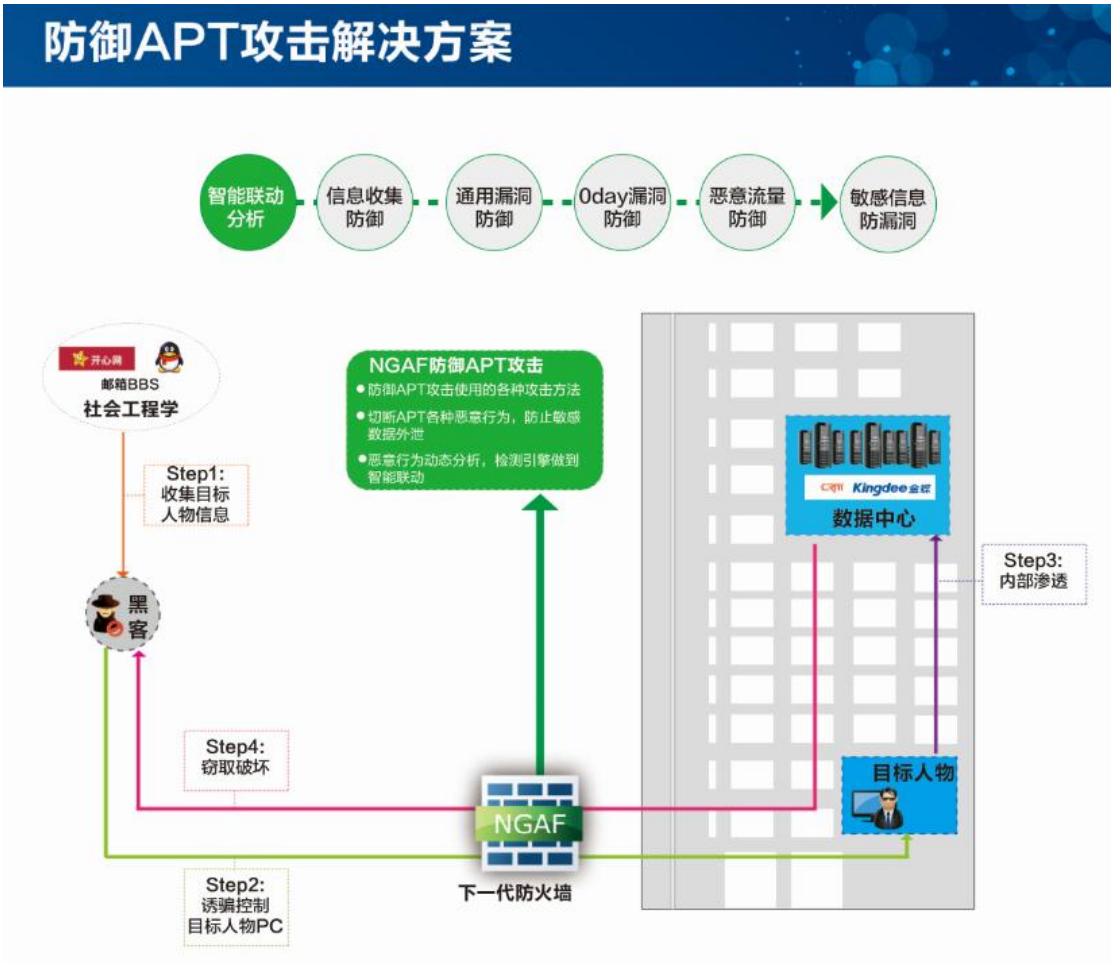
APT 攻击的过程：

- 第一步：攻击者通过各种途径收集用户相关信息，包括从外部扫描了解信息以及从内部利用社会工程学了解相关用户信息；
- 第二步：攻击者通过包括漏洞攻击、Web 攻击等各种攻击手段入侵目标系统，采用低烈度的攻击模式避免目标发现以及防御；
- 第三步：攻击者通过突破内部某一台服务器或终端电脑渗透进内部网络，进而对目标全网造成危害；
- 第四步：攻击者逐步了解全网结构及获取更高权限后锁定目标资产，进而开始对数据进行窃取或者造成其他重大侵害；

APT 攻击防御流程：

深信服下一代防火墙可以通过对 APT 攻击的每一步进行防御并阻断攻击者的 APT 攻击。

深信服下一代防火墙的 APT 攻击防御流程如下图所示：



APT 攻击防御方法：

深信服下一代防火墙主要通过以下几个方向对 APT 攻击进行抑制和防御。

- 信息收集防御：通过 WAF、IPS 等模块防御具有网络行为的信息收集、弱密码探测、端口扫描、扫描软件探测等；通过敏感信息防泄漏模块防御敏感信息收集，包括用户个人信息、账号信息、密码信息等资料；通过主动扫描和被动扫描模块提前进行系统风险评估，及时对可能被利用的漏洞信息进行修复，实现事前风险防护。
- 入侵防御：通过 WAF 模块解决 Web 架构下 SQL、XSS、Webshell 等安全问题；敏感文件泄漏、目录泄漏、源代码泄漏等信息泄漏问题；通过 IPS 模块解决缓冲区溢出攻击、0day 漏洞攻击、应用系统/操作系统漏洞等问题；
- 异常流量分析及防御：AV 防病毒模块通过特征匹配方式定位已知病毒；恶意流量识别模块通过流量行为分析，发现多种类型的恶意流量其中包括访问异常（IP 地址、访问频率、协议类型等）、基于恶意 URL、基于恶意 IP 地址、基于协议规范性等；
- 智能引擎联动：APT 攻击需要多种步骤，当发现恶意行为后，自动切断该 IP 的攻击，防止进一步攻击。对于内网 IP 发现行为异常后，隔离该主机，防止影响内网安全；

- 智能报表联动：深信服下一代防火墙多个安全防护模块统一生成一份安全报表，便于用户分析及了解内部安全状况，从而分析出可疑流量并协助用户解决安全问题；