信诺克安全
SINOSEC

APT与电商安全

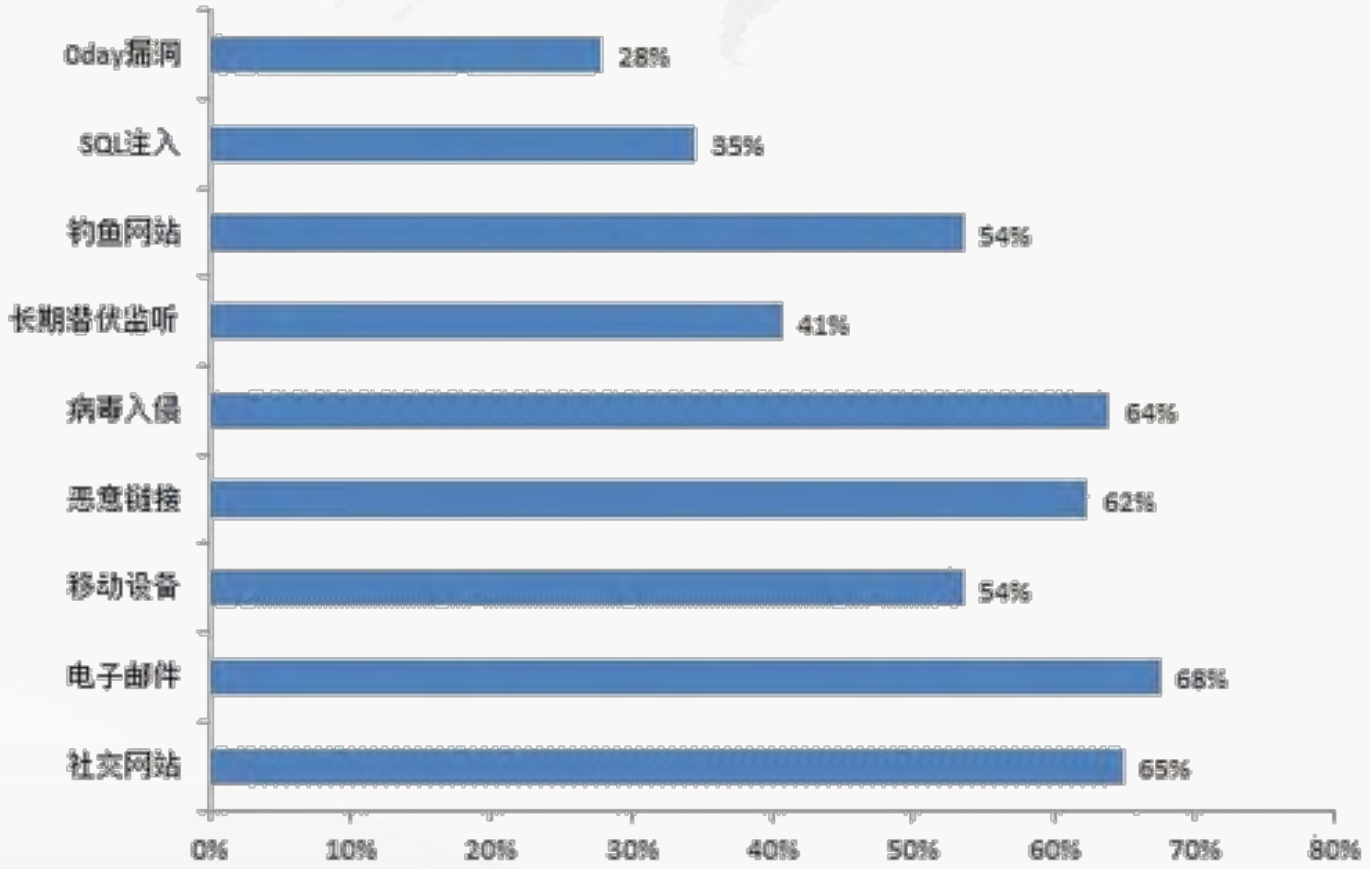
公司介绍

信诺克安全、成立于2008年。早期以内部论坛的形式，进行技术的研究与交流，早期漫游多家安全网站，

公布多个漏洞利用程序如PHPBB盲注漏洞、word、excel、PDF、多款任意代码执行的漏洞与利用程序开发。

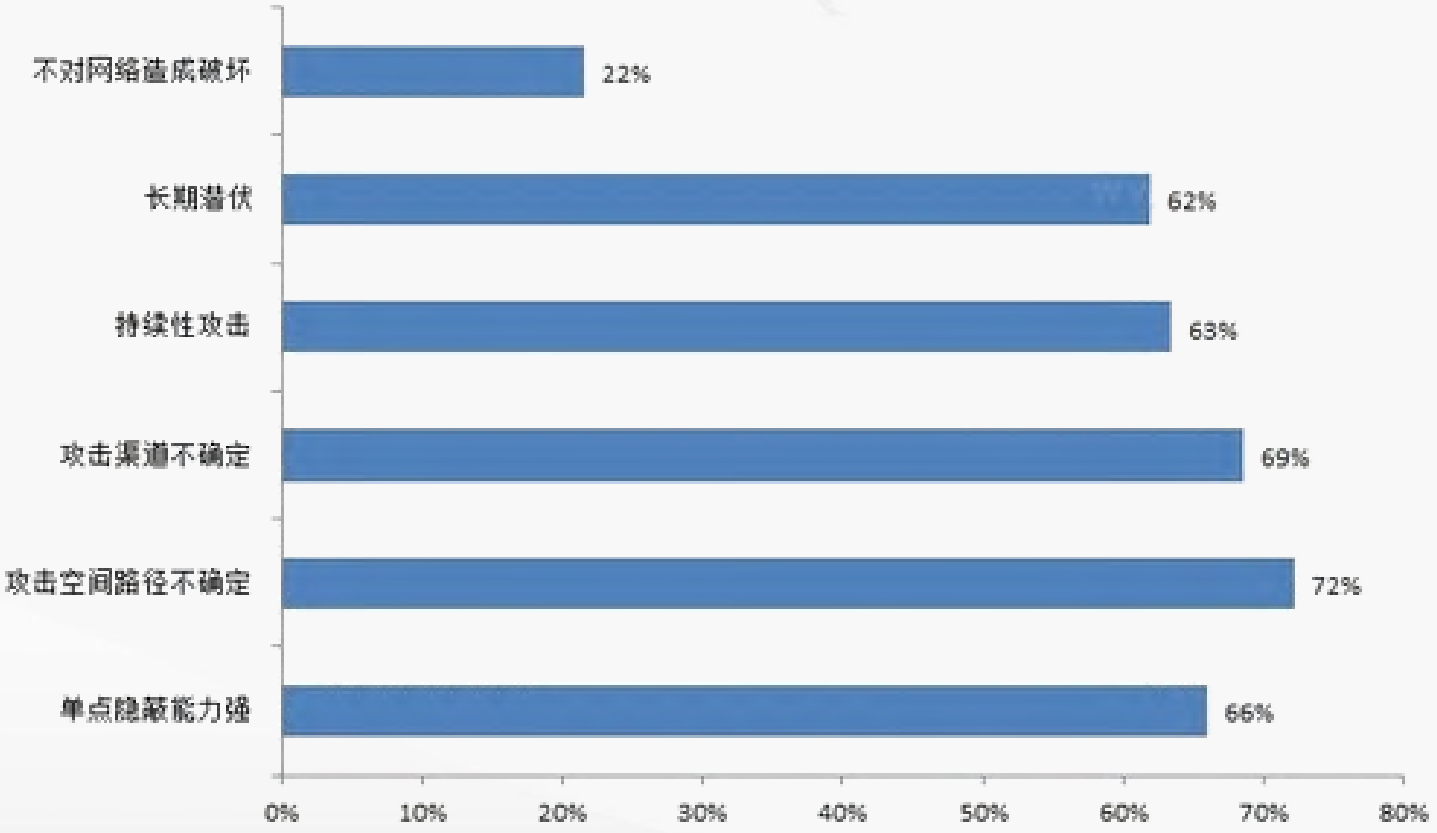
2015年7月正式注册成立郑州信诺克安全公司，致力于电商安全定制化安全服务、为广大电商提供具有针对性的安全服务，与安全产品！

APT攻击形式



在APT攻击的主要途径调查中，我们列出了APT攻击可能利用的大部分工具、系统漏洞、病毒等。其中，电子邮件和社交网站成为黑客发动APT攻击最主要的途径，电子邮件被利用高达68%，社交网站被利用高达65%。从下图我们看到，电子邮件和社交网站甚至超越了病毒、恶意链接、钓鱼网站等传统的黑客攻击途径。

APT攻击特点与防御难点



APT攻击之所以让企业难以防护，其主要原因是它独特的攻击方式和手段难以检测到。在我们以下的调查中，最让企业困扰的APT攻击特点攻击空间路径不确定、攻击渠道不确定、单点隐蔽能力强、持续性攻击、长期潜伏均有超过60%的用户认为这些是最让企业困扰的APT攻击特点

经典案例

信诺克安全
SINOSEC

- Google Aurora(极光)攻击是一个十分著名的APT攻击。

  Google的一名雇员点击即时消息中的一条恶意链接，引发了一系列事件导致这个搜索引擎巨人的网络被渗入数月，并且造成各种系统的数据被窃取。这次攻击以Google和其它大约20家公司为目标，它是由一个有组织的网络犯罪团体精心策划的，目的是长时间地渗入这些企业的网络并窃取数据。

经典案例

-) 对Google的APT行动开始于刺探工作，特定的Google员工成为攻击者的目标。攻击者尽可能地收集信息，搜集该员工在Facebook、Twitter、LinkedIn和其它社交网站上发布的信息。
- 2) 接着攻击者利用一个动态DNS供应商来建立一个托管伪造照片网站的Web服务器。该Google员工收到来自信任的人发来的网络链接并且点击它，就进入了恶意网站。该恶意网站页面载入含有shellcode的JavaScript程序码造成IE浏览器溢出，进而执行FTP下载程序，并从远端进一步抓了更多新的程序来执行(由于其中部分程序的编译环境路径名称带有Aurora字样，该攻击故此得名)。

经典案例

3) 接下来，攻击者通过**SSL**安全隧道与受害人机器建立了连接，持续监听并最终获得了该雇员访问**Google**服务器的帐号密码等信息。

4) 最后，攻击者就使用该雇员的凭证成功渗透进入**Google**的邮件服务器，进而不断的获取特定**Gmail**账户的邮件内容信息

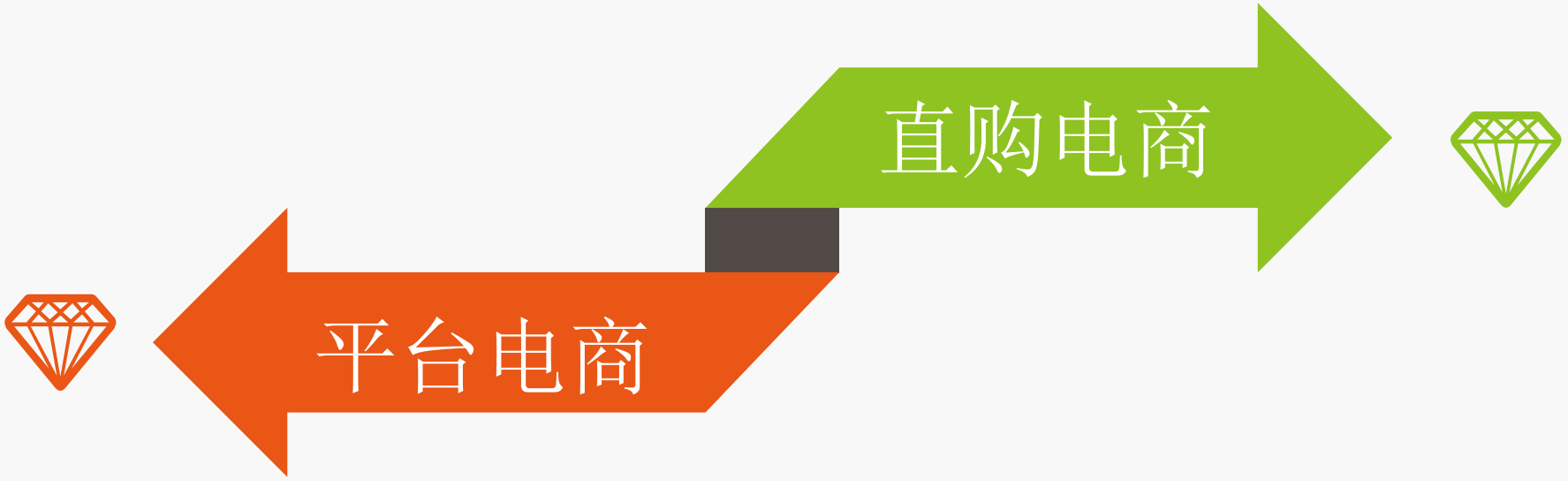
2012年**3**月份，**TrendMicro**发布的报告中披露了一个针对印度和日本的航空航天、军队、能源等单位进行长时间的渗透和刺探的攻击行动，并命名为**Luckycat**。

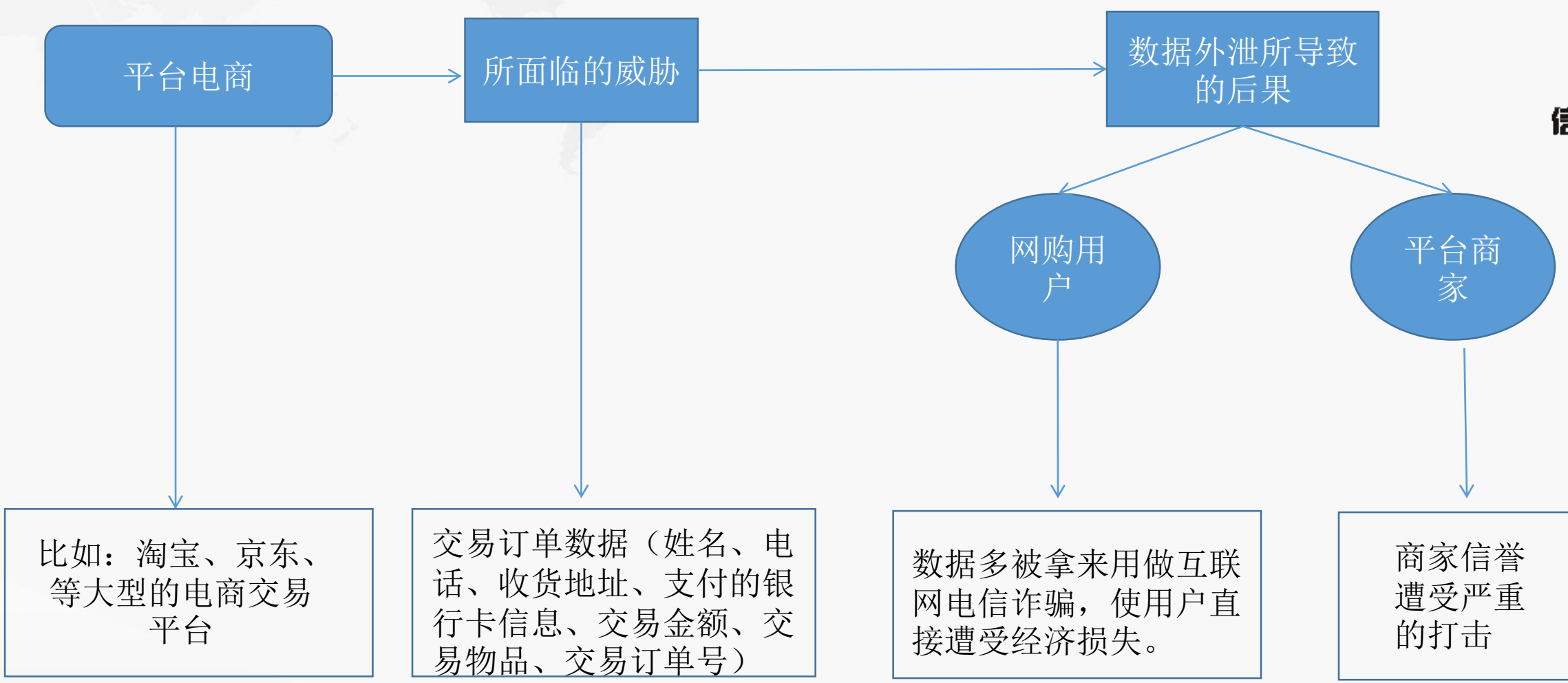
2011年**10**月底，**Symantec**发布的一份报告公开了主要针对全球化工企业的进行信息窃取的**Nitro**攻击。

当前电商安全形势

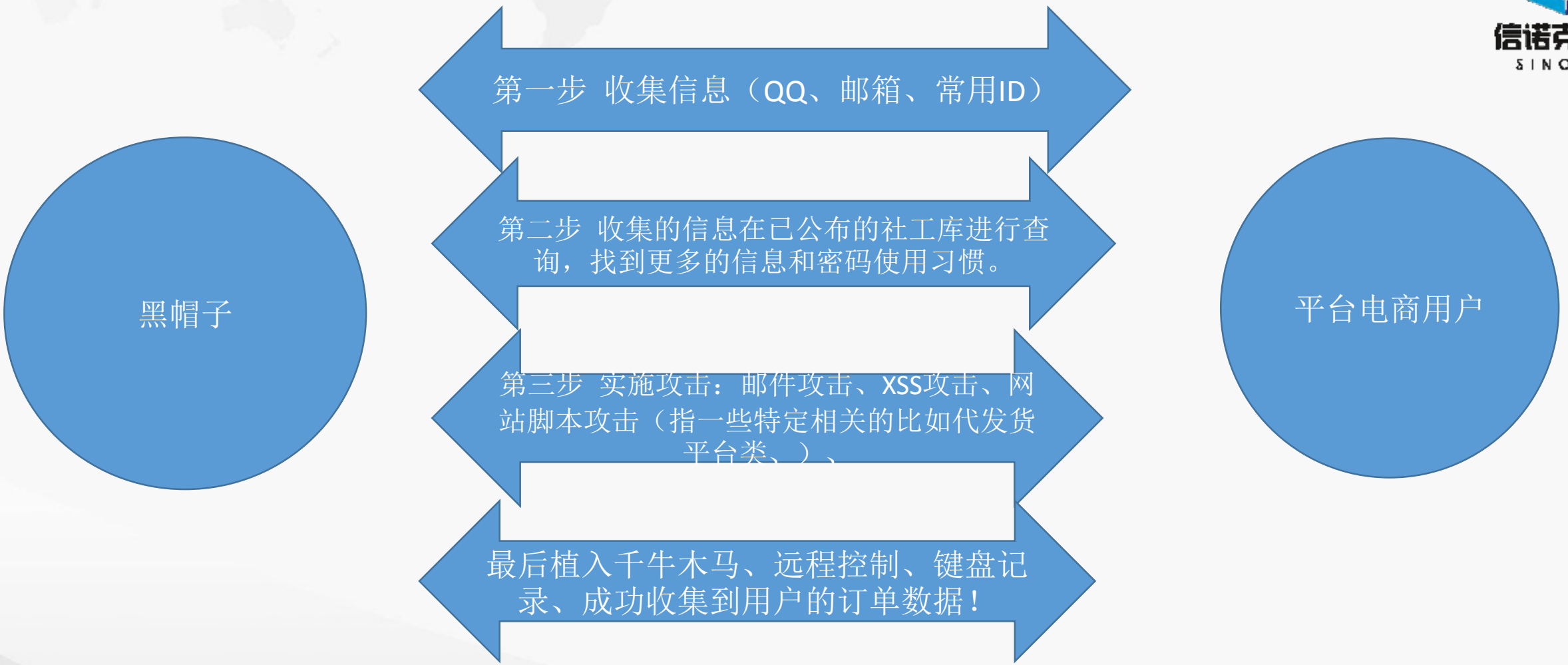
互联网电商成被攻击“新贵”仅次于互联网金融

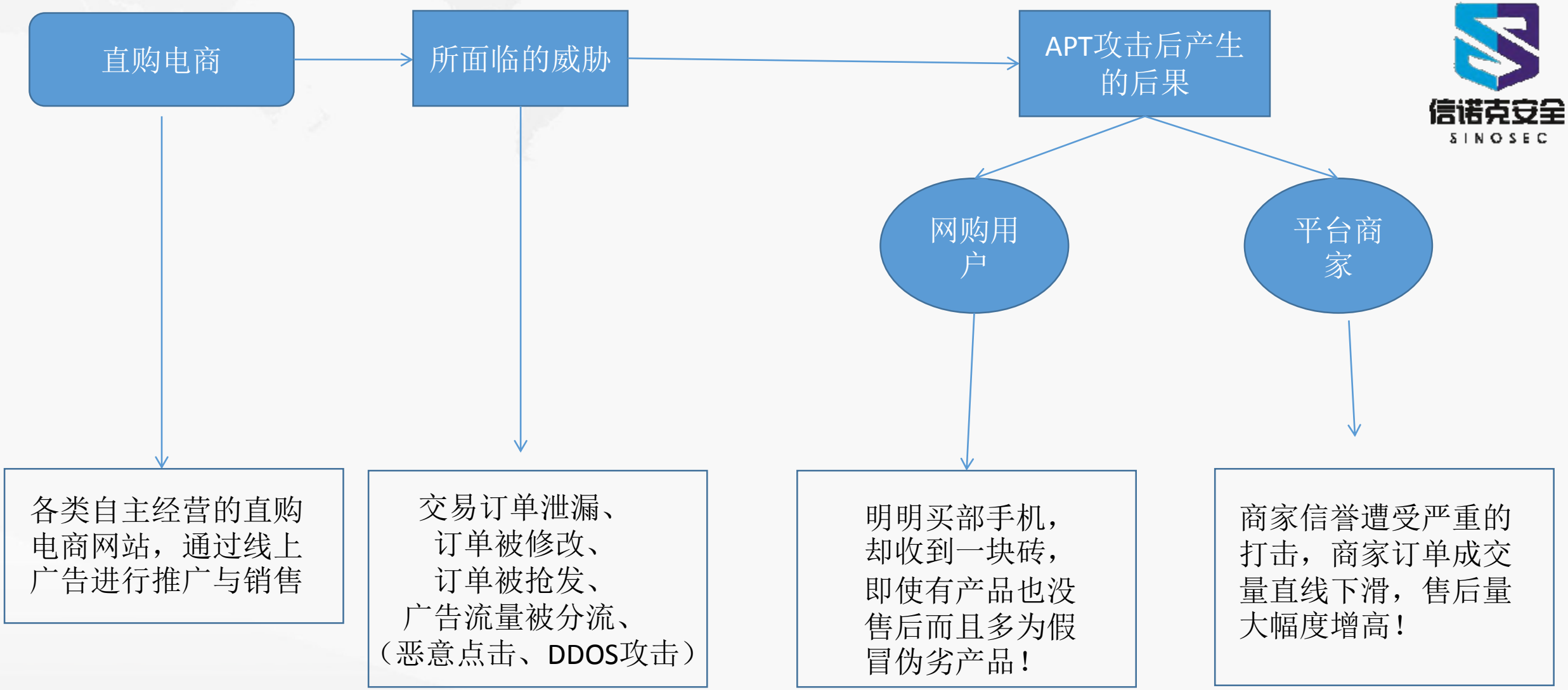
电商平台分类



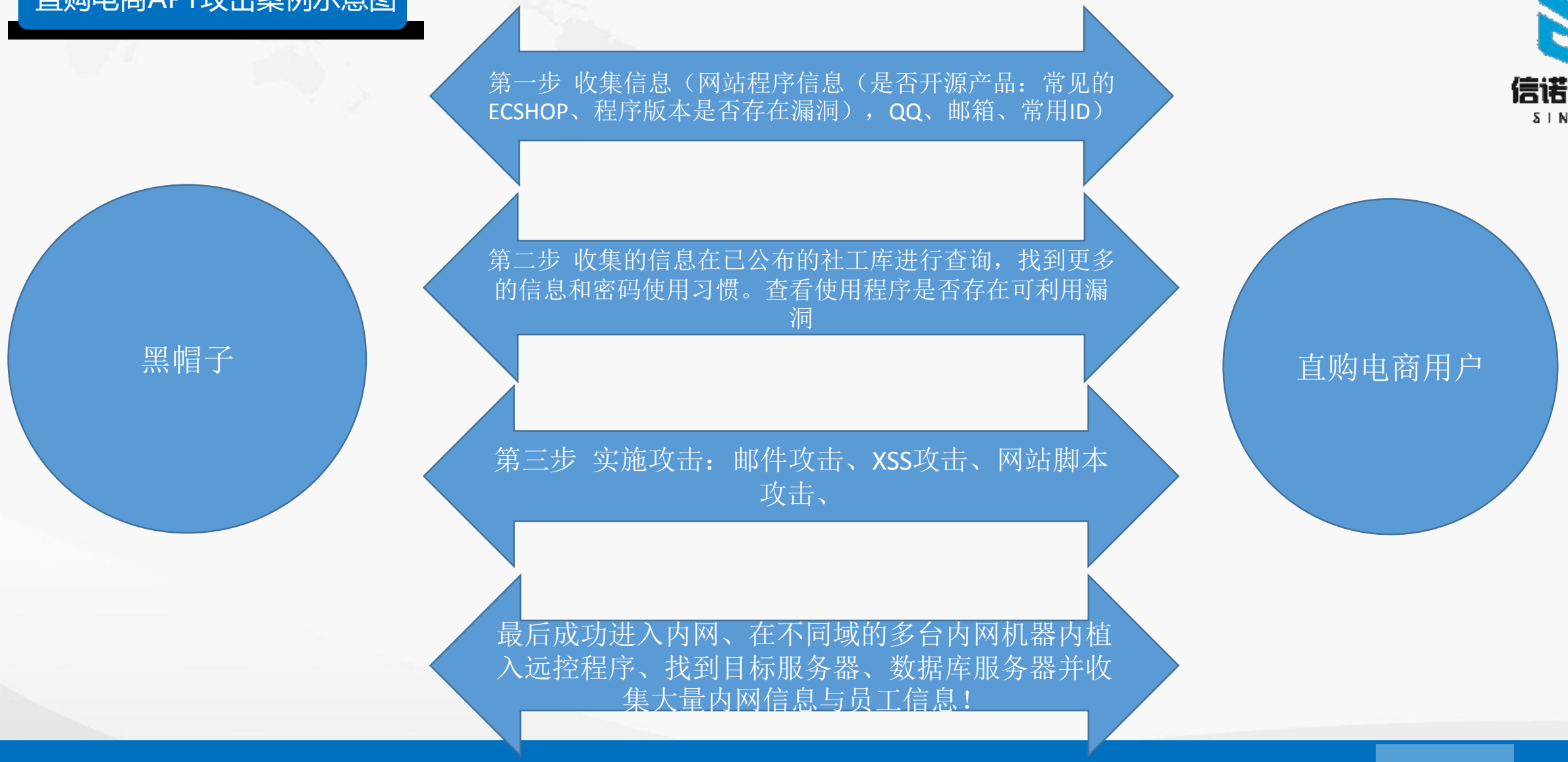

平台电商
所面临的威胁
数据外泄所导致的后果
网购用户
平台商家
比如：淘宝、京东、等大型的电商交易平台
交易订单数据（姓名、电话、收货地址、支付的银行卡信息、交易金额、交易物品、交易订单号）
数据多被拿来用做互联网电信诈骗，使用户直接遭受经济损失。
商家信誉遭受严重的打击

平台电商APT攻击案例示意图




直购电商
所面临的威胁
APT攻击后产生的后果
网购用户
平台商家
各类自主经营的直购电商网站，通过线上广告进行推广与销售
交易订单泄漏、
订单被修改、
订单被抢发、
广告流量被分流、
（恶意点击、DDOS攻击）
明明买部手机，却收到一块砖，即使有产品也没售后而且多为假冒伪劣产品！
商家信誉遭受严重的打击，商家订单成交量直线下滑，售后量大幅度增高！

直购电商APT攻击案例示意图



解决方案

恶意代码检测：在互联网入口点对Web、邮件、文件共享等可能携带的恶意代码进行检测。

数据防泄密：在主机上部署DLP产品，APT攻击目标是有价值的数据信息，防止敏感信息的外传也是防御APT攻击的方法之一。

网络入侵检测：在网络层对APT攻击的行为进行检测、分析，例如网络入侵检测类产品。

大数据分析：全面采集网络中的各种数据(原始的网络数据包、业务和安全日志)，形成大数据，采用大数据分析技术和智能分析算法来检测APT，可以覆盖APT攻击的各个阶段。

针对性定制化安全服务，为客户构建安全高效的业务环境，针对性培训提高客户安全意识！

并为客户提供安全紧急响应在客户出现问题，能够及时迅速的找到问题与解决问题！

谢谢观看！

天一（SinoSec）

意大利 米兰

扫一扫上面的二维码图案，加我微信