APT

APT攻击的中文名字叫高级持续性威胁，是黑客对企业，策划和蓄意已久的有计划的“间谍”行为。我之前在安天分析过一次完整的APT攻击。攻击者通过office中的word的宏定义漏洞释放攻击程序，并自动启动，修改注册表等常规病毒的攻击方式。通过对病毒程序的逆向分析，我找到了病毒的特征序列号，通过与导师的沟通，导师通过特征码找到了以前的一些相似病毒，对请进行对比分析，发现特征序列号，盗取信息后对其的加密算法（这种算法是作者自己写的，并非市面上常见的算法，如DES等，我已经对这个算法进行了完整的还原，并写出了解密算法）与代码结构惊人的相似，说明这是同一个组织批量制造出的病毒，而这次的病毒是一个变种体。通过其他的社工信息，发现这可能是一个有一定规模的组织（名字不方便透露），病毒源在亚洲（作者使用了伪造IP， 开始时误以为是在德国）。

当时的传播word文档内容是关于南海问题，内容也是攻击者为了博大陆人民眼球而精心设计的，通过以上描述，我们可以看出，这是有计划和组织的目的性极强的攻击。

XSS

XSS攻击是跨站脚本攻击，顾名思义，是攻击者通过在靶机网站输入一些恶意的脚本，并期待有xss漏洞的网站去响应执行这些恶意脚本，通常的攻击地点都是留言板等提交表单的地方。Xss分为反射型和存储型，反射型利用价值相对较低，构造后需要被攻击用户主动点击，并且一般攻击代码都在发送的url中，虽然可经过精心编码，但是过长的奇怪url不免会引起怀疑。而存储型直接成为了网站的代码，任何访问者都会执行恶意代码，管理员也不例外，所以经常被用来盗取管理员cookie。这种攻击一般都是用隐藏的iframe（宽度设置为0），利用src，onerror等危险的javascript代码进行cookie的盗取并传送给攻击者服务器。攻击者一旦拿到cookie，就可以不使用密码直接以被攻击者的身份登陆网站，从而做一些坏事。我之前给一位大神分享了一个网站，大神第二天说这个网站有xss，他还拿到了管理员cookie。虽然很多网站已经有了安全防护，但是xss攻击还是主流安全事件攻击中比较重的一员。