安全小课堂第八十四期【APT攻击与防御】

京东安全应急响应中心 2月6日

近年来，一系列安全事件的发生将一个新名词“APT攻击”带入人们的视野，如暗鼠行动：一系列持续网络攻击，攻击目标包括至少72个组织，包括国防承包商，世界各地的企业。那么到底什么是APT攻击，又是如何防御APT攻击？

JSRC **安全小课堂第八十四期**，邀请到**gaoxyz**作为讲师就**APT攻击与防御**为大家进行分享。也感谢白帽子盆友的精彩提问与互动~

什么是APT攻击？

京安小妹

gaoxyz：

一般来说，APT攻击指的是某个团伙或者组织为了获取攻击目标的敏感数据或者资产，利用高级的攻击手法和攻击资源对目标发起的持续性的攻击。

APT攻击的定义其实目前在安全界有一些分歧，主要分两种大的范畴：一种认为非常高危且持续很长时间的攻击称为APT攻击，这种属于侠义上的APT攻击；另外一种，则会将某一次具有定向性质的攻击称为APT攻击，这种可以看作为广义上的APT攻击。具体定义见仁见智了。

讲师

APT攻击原理是什么呢？能不能简单介绍一下

京安小妹

gaoxyz：

APT攻击本身并没有利用其他额外的技术，而是将一些攻击技术做了聚合，然后用来持续的对攻击目标进行定向攻击。区别于普通攻击，APT攻击具有定向性、持续性、高危害性。其原理并没有什么高深的地方，更多的是描述一种攻击的状态（可持续性）、一种攻击的理念。

讲师

APT攻击特点有哪些？

京安小妹

gaoxyz:

APT是Advanced persistent threat的缩写。顾名思义，APT攻击包含了三个方面的特点，即高级（Advanced）、持续性（persistent）、威胁（threat)。

所谓高级，值得是背后攻击组织的攻击手法很隐蔽和高明，攻击用资源很丰富，比如雄厚的资金和强大的技术资源。

持续性，即攻击组织为了达到自己的攻击目的，会利用各种途径和攻击方法尝试对攻击目标的各个攻击界面进行不间断的攻击，直到成功突破防御边界，并达到最终的攻击目的。一般来说，整个攻击过程会持续较长一段时间。

威胁，是相对于目标的资产而言的。即攻击组织通过高级且可持续性的攻击，导致目标的敏感数据或者其他资产面临了很大的威胁。

分享一些经典的APT攻击案例?

京安小妹

gaoxyz：

1） 蠕虫病毒Stuxnet对伊朗核设施进行攻击，并且极大的干扰了伊朗的核计划。10年被首次发现，该蠕虫利用了4个windows系统的0day漏洞对ICS/SCADA进行攻击，属于第一个针对工控系统的恶意软件，并且成功的对伊朗的核设施造成了沉重的打击。

2） Lazarus对全球银行业的大洗劫。

至少自2015年开始对全球银行业的SWIFT系统发起攻击，攻击目的是获取资金。典型的案例就是2016年2月孟加拉央行被盗取8100万美元，其他受到攻击的国家和地区还有印度尼西亚、越南、墨西哥、波兰、台湾等等。

3） 白象对我国的持续多年的攻击行动。

白象是具有印度政府背景的APT组织，长期对我们国家的科研机构、政府、军队发起定向攻击，攻击目的是获取我们国家党政机关的机密数据，我们目前对该组织的攻击行动保持了实时的监测。17年我们发布了近10份关于白象攻击活动的分析报告，侧面说明白象对我们国家的攻击活动是非常猖獗的。

讲师

谈一谈APT攻击的未来的一些趋势呢?

京安小妹

gaoxyz：

APT攻击这个概念虽然已经由来已久，但真正进入大众的视野也是近几年的事情。同时，APT攻击也从以前的零星案例发展到了目前较为活跃的状态，近年来的APT攻击案例层出不穷，尤其是具有国家背景的APT攻击团伙越来越多，发起的各类攻击行动也呈现快速上升的趋势。我所负责微步在线的安全分析团队的一大职责就是分析和监控各大APT攻击组织的攻击行动，根据我们分析了数十起攻击案例，我们总结了如下的趋势：

1） APT攻击手法会越来越高明和难以防御。

APT攻击中用的攻击手法，从传统的反沙箱技术、入侵，到目前的通过无文件攻击、基于供应链的攻击的逐渐流行，未来不排除通过更加多发BGP劫持等骨干网层面的攻击，攻击的手法会越来月高明。

2） 国家间的APT攻击会愈发常见。

目前我们微步对全球上百个的APT攻击组织进行了持续的监控和分析，这其中相当比例的都是来自于欧美、印度、俄罗斯、越南、朝鲜、日本、韩国、中东等国家和地区的APT攻击组织，且均具有对应国家的政府背景。 可以说目前网络事件已经成了一个无硝烟的战场。

3） APT攻击作为网络世界的“核武器”对基础设施产生了越来越大的危害。

从早期通过Stuxnet对伊朗的核设施进行感染，到16年Sandworm组织使用BlackEnergy木马造成乌克兰电网大范围的断电看出，APT攻击对关键基础设施的攻击产生的危害越来越大，很可能危害到国计民生。

4） APT攻击的检测和防御也会越来越创新。

从洛克希德马丁攻击提出kill-chain的入侵模型，到今年mitre提出的ATT&CK模型，一定程度上对于描述APT攻击的特点，采取更加针对性的检测措施起到了很大的帮助。

：

讲师

企业中如何应对APT攻击有哪些防御措施呢？

京安小妹

gaoxyz：

基于上述所讲的APT攻击的特点，可以看到，APT攻击背后的攻击者会尝试收集攻击目标的缺陷和弱点，然后利用各种攻击手法对目标发起持续性的攻击，因此传统的安全防护思路和安全防护设备，比如IPS、防火墙、WAF等在APT性质的定向攻击面前根本没有招架之力，基于此的各种防御边界最终都会被突破。也就是说，攻击者最终都会攻入内网，并且会尝试在内网发现真正的攻击目标，获取敏感数据和其他资产，达到攻击目的。 而从突破防御边界到达到攻击目的，攻击者还需要再内网潜伏较长时间，并且利用各种方法，再内网进行横向移动。因此，对于企业来说，我们仍然可以利用多种手段再这段时间内进行检测，发现入侵威胁，并快速响应和清理。

具体建议，包括几点：

1）改变传统的被动、盲目的防御思路，转向检测与响应的建设思路。

多年来的APT攻击案例表明，传统的安全设备对于APT攻击毫无招架之力。企业应该讲更多的安全预算投入到检测与响应方向，这也是Gartner所提倡的思路和方向。

2）企业应该首先“知己知彼”。

传统的安全建设思路再攻击面前收效甚微的原因就在于企业往往并不清楚自己的安全弱点再哪里，哪里最有可能被突破；同时企业也没有花时间来研究自己的对手是谁，可能面临那些威胁。这就好比参加拳击比赛，既不了解自己弱点再哪里，也不了解对手是谁，有什么优势和弱势，因此，结果往往就是以失败告终。所以，企业应该花费时间和预算了解自己的弱点再哪里，那些服务器存在风险，并针对性的进行修复。同时，也应该研究自己的对手是谁，有什么优缺点，并针对性进行防护。威胁情报正是“知彼”的知识，可以让企业充分了解目标APT的高级威胁有那些，各自有那些特点，常用的攻击手法和攻击资产是什么。

3）建立多层次、立体的安全检测和防御体系。

从kill-chain的角度来看，攻击者的攻击活动是分阶段的，同时也是分不同的活动区域的。因此，对于企业来说，通过多个区域和维度的层层布控，可以增加发现APT类威胁的可能性。

4）建立内部资产安全分级制度，加强对重点资产的保护力度。

由于APT类攻击的目标往往很明确，一般包括获取敏感数据或者窃取资金，如果我们对此类资产进行了重点防护，比如做了较好的隔离或者加密处理，也就增加了APT攻击成功的难度。

4）加强内部员工安全意识培训。

很多APT攻击往往也会利用社会工程的手法，对内部进行渗透。因此，加强内部员工的安全意识培训，对各种异常的邮件、系统保持较高的警惕，可以进一步降低被攻击成功的可能性。

讲师

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心