安全小课堂第八十五期【web攻击溯源】

京东安全应急响应中心 2月12日

web攻击愈发猖獗，该怎么应对呢?如何发现攻击行为的攻击者是谁，用了哪些招式和武器……
攻击无穷尽，防守不停歇……
知己知彼，百战不殆，今天咱们讲一讲如何打好这场安全攻防仗。
JSRC **安全小课堂第八十五期**，邀请到**MerJerson**作为讲师就**web攻击溯源**为大家进行分享。
也感谢白帽子盆友的精彩提问与互动~

溯源发现的手段？（比如日志、流量）

京安小妹

MerJerson:
溯源发现的手段主要是针对日志，流量，样本的分析。首先要明白攻击的几个阶段。每个阶段都有不同的方法。
阶段一：信息收集
阶段二：针对性入侵
阶段三：后渗透准备
阶段四：横向渗透
这四个阶段已经涵盖了攻击链的绝大部分，攻击目的不同，还会有不同的阶段。
阶段一二中，常用的是防火墙、IDS、WAF日志。其中针对性入侵不同的方式又延伸出不同的溯源发现方法，比如钓鱼邮件的一些威胁数据。此时的数据我们可以知道攻击者是如何进行入侵的。
第三四阶段，需要一些系统运行，网络设备，VPN，IDS日志。此时攻击者已成功进入到系统，文件落写，以及内、外部的恶意流量更有价值。这些数据可以让我们简单的推测出，攻击者的目的。

讲师

要有什么军备？（人、存储、研发、分析....等）

京安小妹

MerJerson：

对于军备来说，有四个方面。

第一：设备。主要是安全建设中部署的一些设备，以及一些例如如计算，网络，存储等基础设施。

第二：人。指的一些专业人才，数据分析师，安全运维人员，逆向工程师，安全分析师以及其中的一些协调人员等。

第三：平台。这算一个锦上添花的东西，有了人和设备，当然需要一个平台将攻击溯源的各个方面整合起来。利用溯源平台进行整体的调度，提高效率，快速处置。

第四：威胁情报。这个算是外部资源，现在主流的溯源方法还是以数据为驱动，只能局限在自身受到的攻击。有了外部威胁情报，可以让攻击溯源多了一个分析维度。

讲师

怎么划分？（比如事前探测型，事中正在利用的发现，事后响应）

京安小妹

MerJerson：

可以分为四个阶段，分别是攻击载荷投递，实际控制，应急响应，追踪溯源

攻击载荷投递

这个阶段细分可分为两部分，探查和入侵。攻击者端口、应用指纹扫描，或者社工情报搜集过后，采用爆破，漏洞，钓鱼等方法进行攻击。

- 实际控制

这个阶段攻击者已经成功进入到系统，此时会有一些恶意操作来达到自己的目的。同时，往往会伴随有。

横向渗透。

- 应急响应

安全运维人员会首先察觉异常，发现威胁事件。此时会进入应急响应阶段，攻击载荷投递和实际控制阶段，都可以触发应急响应。

- 追踪溯源

追踪溯源优先级低于应急响应，属于善后阶段。事后需要搞清楚攻击者入侵的细节，造成的影响，以及攻击者是谁。

在溯源过程中都会遇到哪些坑？怎么识别攻击者是谁？

京安小妹

MerJerson：

坑有很多，在此举一个例子：假身份信息。在溯源攻击过程中，会遇到一些攻击者的假身份信息，比如诱饵网址，虚假设备，虚假域名注册信息等。这些都会带偏分析方向。如何分别真假，只能依靠大量的分析以及关联信息，来提高置信度。

关于如何识别攻击者，这就涉及到对攻击者进行溯源画像了。其实溯源分为三个步骤，“怎么打进来的”，“进来做了什么”，最后才是“攻击者是谁”。溯源画像也是主要依靠前面两个阶段的分析。

攻击者如何进行攻击的，攻击源在哪，使用了哪些攻击手法，活动时间如何。实际控制后落写的恶意文件，被控制请求的恶意域名，域名解析的恶意IP，失陷主机与攻击者远控主机的通信等等。分析过程中还要注意和其他攻击事件的关联，比如恶意IP有没有在其他攻击中出现过，恶意样本的代码风格和其他攻击中的样本很接近，又或者本次攻击的手法，在其他攻击中是否也出现过。线索越多，溯源画像就越清晰。

关于溯源分析，业内有一个钻石分析模型，大家可以了解下，有助于勾画攻击者的溯源画像。

讲师

对内部的攻击溯源思路也是一样吗？

京安小妹

MerJerson：

对于内部， 溯源之前应当保证当前攻击已经不会继续造成进一步的损失，切断止损后进行，避免攻击造成的后续损失也避免多余的噪音信息干扰。对内部追溯拥有更多的数据和日志支撑，能够从更全面的角度支撑追溯，包括且不限于流量数据，服务日志数据，系统syslog等等，因为自身掌握机器权限所以能最大限度的从现有的数据中找到蛛丝马迹， 这也要求平时做好日志数据的保护工作，对敏感重要日志进行防篡改处理或离线备份。

此外，对攻击越熟悉，溯源时思路也会越清晰，从攻击造成的结果推断多个成因，从数据和日志上找到能够支撑推测的证据，逐步逆向分析，最后将多个行为进行关联，还原出一条完整的攻击链。

：

讲师

怎么能在攻击中发现有更有价值的东东，比如0day、Nday等等。

京安小妹

MerJerson：

Nday其实还是比较多的，对漏洞添加过滤规则后，遇到Nday攻击只需要分析捕获的文件，流量就可以了。

相对来说，发现0day攻击是比较难的。对于个人端，需要海量的布点和EK，样本着床，通过沙箱模拟执行等技术，从中捞出有价值的样本数据进行自动化或半自动化的确认分析，这需要安全分析人员对整个攻击流程有全面细致的描绘，并且具有敏锐的察觉力。对于服务端，漏洞无论从应用还是服务打进来，上层的流量记录都会给我们提供最原始的支撑纪录，将大量的批量式攻击记录排除后，留下的更多是涉及到漏洞本身的记录，通过前后文的比对，对攻击记录的分析即可从中判断出漏洞的攻击细节。

此外，部署蜜罐也是抓捕恶意样本，Nday，0day常用的方法。

讲师

白帽子提问1：

如果溯源期间发现日志信息被恶意抹掉了，或者修改过，如何进行下一步追查呢？

MerJerson：

其实我们做溯源分析，首先要知道的是，攻击者怎么进来的，以及攻击者做了什么。调查过程中，日志仅仅是一个参考。其他一些行为痕迹，比如流量，驻留的恶意样本都可以进行关联。如果安全建设的全的话，日志应该是会统一收集和管理的，所以本地怎么清一般没用，但是清了，日志这个参考没有那么重要了，还去查看系统哪些东西被改过了。

白帽子提问2：

师傅是如何针对一些恶意的肉鸡ip进行溯源的呢？

MerJerson：

组内的办法是查大网流量，反向套接字数据。

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。

祝大家新春吉祥，阖家欢乐

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