安全小课堂第五十二期【详谈webshell检测】

京东安全应急响应中心 2017-04-07

webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。JSRC **安全小课堂第五十二期**，我们邀请到了**数据流**、**Blood_Zer0**师傅分享一下webshell检测原理及手段，以及 JSRC 白帽子们的精彩讨论。

讲师：数据流

讲师简介：

有多年的安全实战经验，擅长WEB安全与浏览器安全，喜欢研究一些冷门的猥琐流攻击领域。曾发现微软，Apple，opera，molliza，腾讯等大型厂商的WEB与客户端产品的高危漏洞。

讲师：Blood_Zer0

讲师简介：

饿了么安全研究员,安全白帽子,在应用安全领域有较深的研究。对webshell检测技术有着深入的研究。

简单介绍一下什么是webshell?

京安小妹

webshell实际上是一个在网站服务器可执行的脚本文件，例如ASP,PHP,JSP等,可通过此脚本 远程操控网站,通常攻击者入侵网站后都会上传webshell作为后门。
Webshell：是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。在我理解就是一个与web服务相同的权限。

讲师：数据流、Blood_Zer0

webshell有什么危害呢?

京安小妹

一般webshell拥有文件上传、编辑、删除、重命名，执行系统命令、服务器管理，提权等功能。当网站被上传webshell就意味着你的网站已被入侵，攻击者基本上可以 对你的网站为所欲为，包括篡改你的网页，窃取或删除数据库数据等高危操作；通过提升权限还可以完全控制整个服务器；另外还可以作为跳板进行下一步的渗透。
拿到Webshell，可以修改网站的文件；（相当于控制整个网站）
如果未做好权限控制还可以查看服务器上其他的网站（同服渗透）；
利用Webshell作为跳板继续渗透服务器（如提权，内网渗透）；

讲师：数据流、Blood_Zer0

检测webshell的重要性?

京安小妹

检测webshell是对企业自身的互联网资产的安全建设必不可少的一个环节，实时检测webshell可对攻击者的入侵进行阻断，并可排查出漏洞所在，成为攻击者的拦路石。检测webshell是对企业自身的互联网资产的安全建设必不可少的一个环节，实时检测webshell可对攻击者的入侵进行阻断，并可排查出漏洞所在，成为攻击者的拦路石

讲师：数据流、Blood_Zer0

白帽子观点:及时发现黑客

白帽子提问:如何快速发现网站目录下的webshell?

主流现在有3个方向，基于流量，基于agent，基于日志，但是还有一个国外在做的就是利用“统计学”。

讲师：数据流、Blood_Zer0

目前常见的webshell检测手段有哪些呢？原理是什么？

京安小妹

1 关键字匹配：即是对文件内容中的危险函数并可带入请求的关键字或是特定webshell的关键字进行匹配；例如的eval、assert、exec、call_user_func、call_user_func_array、array_map、preg_replace'Shell.Application'、'XXX专用大马'、'提权'等。通过搜集各种webshell样本组建正则进行匹配。还有危险的后缀 名，如asa、cer、php4|5等。

2 流量检测：通过收集发送请求的特征对网站的流量进行检测，例如著名webshell客户端“中国菜刀”最新版的HTTP请求中就包含：

array_map("ass"."ert",array("ev"."Al(\"\\\$xx%3D\\\"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\$xx('

在流量中检测出包含类似这一段关键字的请求就必然是中国菜刀webshell。

3 agent检测：在服务器安装监控探针；

例如通过监控系统文件，对新增的文件进行常规的webshell检测，可实时发现webshell；监控系统进程，当web服务的用户的权限起了个cmd或bash就有问题了。还有反 连的检测。通过agent可从多个角度去发现和拦截webshell攻击。

4 语法检测：语法检测可检测出构造奇妙的webshell；若文件经过加密编码单靠关键字匹配是无法检测出来的，用语法语义分析形式，根据php语言扫描编译的实现方式 ，进行剥离代码、注释，分析变量、函数、字符串、语言结构，来实现关键危险函数的捕捉方式。

5 统计学检测：通过检测文件的信息熵，最长单词、IC值等数学方式判断文件是否危险。这种方法混淆加密的webshll检测有不错的作用。例如信息熵是代表一个文件的 混乱程度，越是没有规则的文件内容熵就越高，加密过的webshell通常都是无序的；而检索出的最长单词是异常的话则表明文件代码被编码过，要是一大串单词连着肯 定有问题。

当然，检测webshell的方法还不止于此，检测webshell，可以从多个维度去发现，一个webshell的生命周期里接触的所有维度，攻击漏洞、webshell代码、文件生成、 行为、窃取资料、痕迹擦除等都可提取检测特征。不要从单纯检测webshell出发。

讲师：数据流、Blood_Zer0

有成熟的webshell检测工具推荐吗?

京安小妹

啊D：webshell查杀工具 支持所有脚本类型，可检测众多特殊函数和变量函数，效果非常不错。并有文件监控，进程监控等功能。

河马网站后门检测与查杀工具：支持linux，windows，并提供在线检测API。

Pecker Scanner：是一个PHP语言编写的基于php语法扫描、词法分析的webshell扫描工具。该项目太久没更新了，但也值得借鉴。

NeoPI：是一个基于统计学的webshell检测脚本，支持关键字特征、信息熵、重合指数、最长单词等检测方式，对一些加密编码过的webshell识别不错，但是没有混淆过的就基本检测不出来。

讲师：数据流、Blood_Zer0

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，回复“安全小课堂”或者点击阅读原文进行查看。

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

阅读原文