2016 年 4 月 15 日，星期五

广泛存在的 JBOSS 后门带来重大威胁隐患

最近，在勒索软件传播方面，一个传播 Samsam 的大规模勒索软件活动改变了威胁形势。该活动专门利用服务器中的漏洞传播勒索软件，导致这种本已十分猖獗的威胁上升到新的维度。基于思科 IR 服务团队从最近的一项客户活动中获得的信息，我们开始更深入地研究被用作攻击起始点的 JBoss 传播媒介。首先，我们的第一步工作是扫描互联网，寻找易受攻击的计算机。结果，我们发现有约 320 万台计算机存在风险。

作为本调查的一部分，我们对已被入侵并且可能在等待勒索软件负载的计算机进行了扫描。我们从中发现了近 1600 个 IP 地址上安装的 2100 多个后门。最近几天，Talos 陆续向受感染的各方做出通知，其中包括学校、政府、航空公司等各种组织。

这些已被入侵的系统中，有许多都安装了 Follett 的 Destiny 软件。Destiny 是一个专用于跟踪学校图书馆资产的图书馆管理系统，主要用于全球各地的中小学。我们联系了 Follett，对方向我们介绍了一个令人印象深刻的修补系统，不仅可以修补 9.0-13.5 版本的所有系统，而且可以捕捉系统中存在的非 Destiny 文件，以帮助消除系统中的任何现有后门。Follett 技术支持部门将联系系统中发现可疑文件的客户。考虑到这种威胁的普遍性，我们呼吁所有 Destiny 用户务必安装该补丁。

Follett 还请我们分享以下内容：

Follett 根据内部系统安全监控和协议查明了问题，并立即采取行动代表我们的客户解决和封杀该漏洞。

Follett 非常重视数据安全。因此，我们会持续监控我们的系统和软件是否受到威胁，并改善我们的技术环境，以便帮助我们所服务的机构最大限度降低风险。

作为本调查的一部分，Talos 和 Follett 会继续合作，分析被入侵服务器中发现的 webshell，并确保告知我们的客户如何最有效地保护其网络。

通过分析，我们了解到被入侵的 JBoss 服务器上通常有不止一个 webshell，这对于查看作业状态页面的内容非常重要。我们看到了多种不同的后门，包括“mela”、“shellinvoker”、“jbossinvoker”、“zecmd”、“cmd”、“genesis”和“sh3ll”，而“Inovkermngrt”和“jbot”可能也是后门程序。这意味着这些系统中有很多已经被不同的攻击者入侵过多次。

美国计算机应急响应小组 (US-CERT) 曾发布下列关于 webshell 的公告：
https://www.us-cert.gov/ncas/alerts/TA15-314A

webshell 是一个重要的安全问题，因为它表明攻击者已经入侵到服务器中，并且可以远程控制该服务器。因此，已被入侵的 Web 服务器可被用于在内部网络中进行透视和逐步渗透。

考虑到这个问题的严重性，我们建议立即中断被入侵的主机，因为这个主机可能会以各种方式被滥用。这些服务器托管着 JBoss，而最近的一个备受瞩目的勒索软件活动中便有 JBoss 的身影。

该外壳程序的软件可以在此处找到。

建议补救措施

如果您发现某个服务器上被安装了 webshell，您需要采取一系列措施。我们的第一个建议是，如果有可能，请取消该服务器的外部访问权限。这可以防止攻击者远程访问该服务器。在理想的情况下，您还可以对系统进行重镜像，并安装更新版本的软件。这是确保攻击者无法访问服务器的最佳方法。如果出于某种原因您无法彻底重建服务器，那么次一级的最佳方案是使用受入侵之前的备份恢复系统，再将系统升级到不容易受攻击的版本，然后再恢复运行。

对于 Follett Destiny 用户，请遵循自动更新通知，并确保正确安装补丁。据 Follett 称，此过程应该可以删除有害的后门外壳。

虽然是老生常谈，但是我们建议使用声誉良好的防病毒软件。

总结

有大约 2100 台服务器受到影响，遭到入侵的原因可能多种多样。但是，所有情况都可以归结为一个问题，那就是需要更新补丁。更新补丁是软件维护的关键内容之一，但却经常被软件用户和制作者忽略。此链条上任何环节出现问题都会使得此类攻击总能成功。如果攻击中伴随着勒索软件，那么无论是对小型企业还是对大型企业，都会构成灾难性的潜在危害。

危害表现

此列表目前可能并不完整，但是可以为发现由各种 webshell 和相关攻击工具带来或留下的更多威胁表现提供基础。

jbossass.jsp	jbossass_jsp.class
shellinvoker.jsp	shellinvoker_jsp.class
mela.jsp	mela_jsp.class
zecmd.jsp	zecmd_jsp.class
cmd.jsp	cmd_jsp.class
wstats.jsp	wstats_jsp.class
idssvc.jsp	idssvc_jsp.class
iesvc.jsp	iesvc_jsp.class

覆盖范围

以下 Snort 规则可以解决此威胁。请注意，Talos 未来可能会发布更多规则，当前规则会根据未来得到的更多漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心或 Snort.org。

SNORT 规则

- **JBoss 服务器漏洞**：18794、21516-21517、24342-24343、24642、29909
- **Web Shell**：1090、21117-21140、23829、23830、27729-27732、27966-27968、28323、37245
- **Samas**：38279、38280、38304、38360、38361

产品	保护
AMP	✔
CWS	不适用
ESA	不适用
网络安全	✔
WSA	不适用

此外，高级恶意软件防护 (AMP) 可帮助侦测和阻止此恶意软件在目标系统上运行。

网络安全包括 IPS 和 NGFW。这两者均具有最新的签名，可侦测此攻击活动表现出来的恶意网络活动。

发布者：ALEXANDER CHIU；发布时间：上午 11:29
标签：公告、后门、JBOSS、补丁、勒索软件、SAMSAM、服务器、漏洞、WEBSHELL