2016 年 5 月 17 日，星期二

通过积极主动的通知结交朋友

作者：Tazz。

Talos 一直在关注当前利用 JBoss 漏洞发起的攻击。通过不断研究，我们又发现了大约 600 个因为网络攻击者入侵未打补丁的 JBoss 环境，而受到侵害的主机，这些主机都被注入了 webshell。对此，Talos 努力通知这些受侵害主机的拥有者，以便他们能够采取适当的补救措施。本篇博文旨在概括介绍相关的通知流程，并补充提供一些危害表现信息（例如我们观察到的目前最常见的 500 种 webshell 的列表），以帮助您审视自己的 JBoss 环境。

我为什么会收到通知？

在发现带有一个或多个 webshell 的主机后，我们会确认该主机的 IP 地址，然后从拥有该 IP 地址的组织的 WHOIS 记录中提取出相关联系人的邮箱地址。通知邮件中会包含一个链接，可用于查看这一信息。我们会通过电子邮件将通知发送到所有相关的邮箱地址。这样做的原因是，我们发现许多组织的指定滥用举报联系邮箱已经无效。所以我们会向所有可以找到的联系人发送通知邮件，以便最大限度确保通知成功。

如果您的组织最近没有与您的互联网注册管理机构确认此联系人信息，可以趁现在进行确认。如果您不确定您的互联网注册管理机构是哪一家，请访问 https://www.iana.org/numbers 进行查找。

- 非洲网络信息中心 (AFRINIC) - 非洲地区
- 亚太网络信息中心 (APNIC) - 亚太地区
- 美洲互联网号码注册管理机构 (ARIN) - 加拿大、美国和加勒比海的一些岛国
- 拉丁美洲及加勒比地区互联网地址注册管理机构 (LACNIC) - 拉丁美洲和加勒比海的一些岛国
- 欧洲 IP 网络资源协调中心 (RIPE NCC) - 欧洲、中东和中亚

还有什么要补充的？

我们发现，有个别主机带有 100 多种不同的 webshell。为了方便查看，我们的通知中将仅列出 10 种最主要的 webshell。后面的 IOC 部分会提供我们观察到的 500 多种最常见的

webshell。由于大多数组织都会按主机跟踪漏洞或危害表现，所以我们会针对每个 IP 地址发送一封邮件。因此，您可能会收到多个具有相同主题的电子邮件。但是请特别注意这些邮件的正文。从我们在主机上发现 webshell 到我们成功通知您的这段时间里，相关主机或受侵害资产可以访问的其他主机上可能会被注入更多 webshell。我们强烈建议您进行全面的调查，以确定恶意攻击者对您的网络和其他资源可能拥有的权限范围。

TALOS 为什么要开展这项工作？

我们致力于使我们所生活的全数字化世界更加安全，以便我们在全球各地的客户、家人、亲友和邻居都能从中受益。我们免费发送这些通知，但是不承担任何义务。为了帮助我们继续开展这项行动，我们的通知中会列出一些详细的请求。如果您能够且愿意与我们分享任何信息，您可以在这里获得我们的 PGP 密钥。您可以使用该密钥来加密任何相关文件并进行安全的电子邮件传输。

我们知道，组织有时不能分享信息。在这种情况下，如果可能，我们衷心希望您能与我们联系，配合我们结束这项调查，并在修复主机后通知我们（发送电子邮件至 talos-abuse-notifications@cisco.com ，并提供您的 IP 地址。

如果您希望详细了解如何处理受侵害的主机，请参阅我们前一篇关于 JBoss 后门的博文中提供的建议补救措施：
http://blog.talosintel.com/2016/04/jboss-backdoor.html。

IOC

这里提供了我们检测发现的 500 多种 webshell 的列表。如果您想在您的主机上查找其中的某一种，请使用如下格式：http://<ip_address>/<webshell>。

发布者：ALEXANDER CHIU；发布时间：下午 12:39
标签：#SAVETHEINTERWEBZ、JBOSS、通知、漏洞、WEBSHELL