msdtc后门的实现思路

嘶吼roartalk / 2017-08-22 08:20:46 / 浏览数 2513 安全技术 技术讨论 顶(0) 踩(0)

0x00 前言

Shadow
Force曾经在域环境中使用过的一个后门，利用MSDTC服务加载dll，实现自启动，并绕过Autoruns对启动项的检测。本文将要对其进行测试，介绍更多利用技巧，分析防御

0x01 简介

本文将要介绍以下内容：

· MSDTC简介

· 后门思路

· 后门验证

· 更多测试和利用方法

· 检测防御

0x02 MSDTC简介

MSDTC：

· 对应服务MSDTC，全称Distributed Transaction Coordinator，Windows系统默认启动该服务

· 对应进程msdtc.exe,位于%windir%\system32
· msdtc.exe是微软分布式传输协调程序，该进程调用系统Microsoft Personal Web Server和Microsoft SQL Server

0x03 后门思路

参考链接：
http://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company/

文中介绍的思路如下：

当计算机加入域中，MSDTC服务启动时，会搜索注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC\MTxOCI

如下图

分别加载3个dll：oci.dll,SQLLib80.dll,xa80.dll

然而特别的是， Windows系统默认不包含oci.dll

也就是说，将payload.dll重名为oci.dll并保存在%windir%\system32下

域中的计算机启动服务MSDTC时就会加载该dll，实现代码执行

0x04 后门验证

测试系统： Win7 x64

搭建域环境，如下图

使用Procmon监控msdtc的启动过程，筛选进程msdtc.exe，查看文件操作，如下图

msdtc.exe确实会尝试加载oci.dll，并且由于系统默认不存在oci.dll,导致加载失败

使用64位的测试dll,下载地址如下：

https://github.com/3gstudent/test/blob/master/calc_x64.dll

将其保存在%windir%\system32下

结束进程msdtc.exe，命令行参数如下：

```
taskkill /f /im msdtc.exe
```

等待msdtc.exe重新启动

等待一段时间，mstdc.exe重新启动,成功加载oci.dll，如下图

calc.exe以system权限启动

如下图

经实际测试，该方法偶尔会出现bug，通过taskkill结束进程后，msdtc.exe并不会重新启动

解决方法：

重新启动服务MSDTC就好，命令行参数如下：

```
net start msdtc
```

0x05 更多测试

1、测试32位系统

32位系统换用32位dll就好，下载地址如下：

https://github.com/3gstudent/test/blob/master/calc.dll

2、测试64位系统

64位系统，虽然SysWOW64文件夹下也包含32位的msdtc.exe，但是MSDTC服务只启动64位的msdtc.exe

因此，不支持32位oci.dll的加载

3、通用测试

经实际测试，MSDTC服务不是域环境特有，工作组环境下默认也会启动MSDTC服务

也就是说，该利用方法不仅适用于域环境，工作组环境也同样适用

4、以管理员权限加载oci.dll（降权启动）

上述方法会以system权限加载oci.dll，提供一个以管理员权限加载oci.dll（降权启动）的方法：

管理员权限cmd执行：

```
msdtc -install
```

启动的calc.exe为high权限，如下图

注：

关于为什么要降权及降权的更多实现方式可参照文章

《渗透技巧——程序的降权启动》

0x06 检测防御

检测：

检测%windir%\system32是否包含可疑oci.dll

防御：

对于普通用户主机，建议禁用服务MSDTC

0x07 小结

本文介绍了MSDTC的相关利用技巧，不仅能用作后门，同样可用于程序的降权启动。

本文为3gstudent原创稿件，授权嘶吼独家发布，如若转载，请注明来源于嘶吼： http://www.4hou.com/system/6890.html

上一篇：Burp Suite插件开发-HT... 下一篇：极验验证码破解—超详细教程（一）

1. 2 条回复


simeon 2017-08-23 03:01:09

牛逼的帖子，先收藏，再学习！

0 回复Ta


c0de 2017-08-23 03:27:04

不错。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板