

Microsoft Word 中的 DDE 攻击



浏览，发现 1 个不明物体

系统安全



Microsoft Word 是一款广泛

的办公软件。然而就是因为这样，也使它成为了黑客的主要攻击目标之一，例如来窃取域哈希，甚至执行任意代码。

从

Microsoft Office 中执行任意代码往往是通过宏来实现的。那么，有没有其它方法可以实现任意代码执行呢？答案是肯定的。[SensePost](#) 就发现了一种利用 DDE（动态数据交换）协议，来执行任意代码的方法。办公产品内有许多可通过 DDE 接收代码并执行的地方，本文我将为大家演示一些这类攻击的常用手法。此外，关于 payload 可以结合 [DDE Payloads](#) 作为参考。

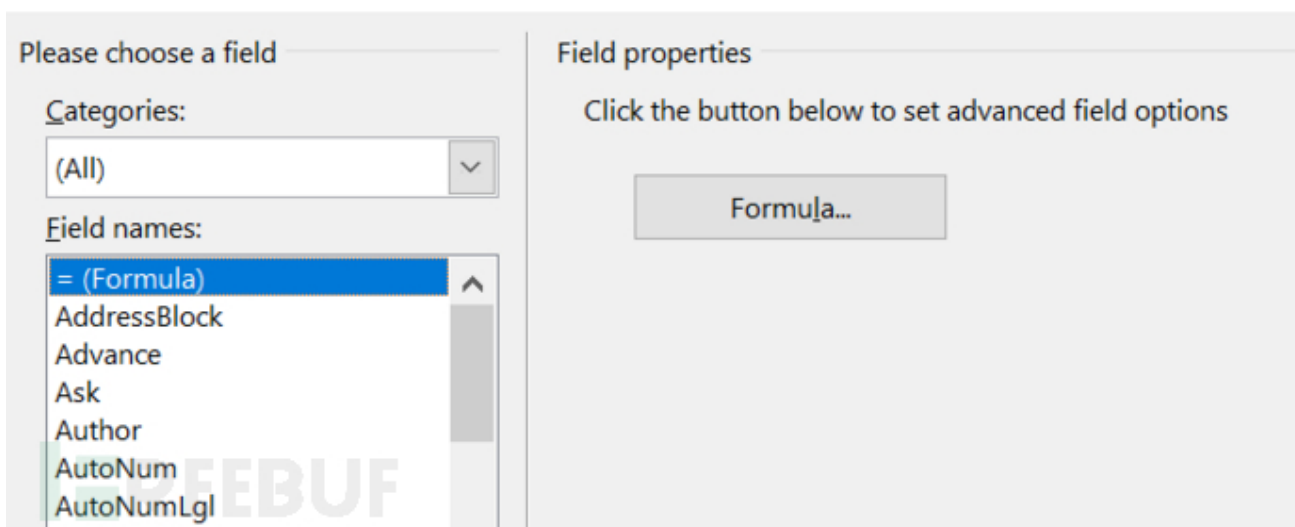
关注我们 分享每日精选文章

Word

在 Microsoft Word 中，最简单的方法是插入一个字段代码，如 [SensePost 文](#) 中所述，并在 formula 中嵌入 payload。

Insert -> Quick Parts -> Field

Field



在括号内添加以下 payload 内容，将会在下次打开文件时弹出一个对话框。如果用户选择“Yes”选项，则 payload 将被执行。



关注我们 分享每日精选文章

或者，我们也可以像[Paul Ritchie](#)在其[博客](#)中描述的那样，使用宏将payload插入字段代码。

```
''' Programmatically inserts a new field code into a word document at the current
''' This is of type "wdFieldDDEAuto" which is a field code which executes Dynamic
''' When the document is opened. This includes an example PoC which launches calc.
Public Sub FieldCodeFun()
' Payload String
Dim payload As String
payload = ""c:\\windows\\system32\\calc.exe"" ""/c calc.exe""
' Insert our payload as a field code
Selection.Collapse Direction:=wdCollapseEnd
```

```
Type:=wdFieldDDEAuto, Text:=payload
```

```
End Sub
```



关注我们 分享每日精选文章

以上示例中的payload只是打开了计算器，但我们也可以将其修改为其它任意代码（甚至恶意的）。

[Mike Czumaky](#)在他的博客中也为我们提供了一种很好的思路，从外部托管的另一个Word文档加载恶意的DDE。INCLUDE字段代码可被用来与该攻击向量结合外部URL使用。





关注我们 分享每日精选文章

Excel

在Microsoft Excel DDE有效载荷可以通过formula的使用来利用。以下两个formula将执行代码（本例中为计算器），二个formula将使警告消息框看上去更合理，以更好的欺骗用户。

```
=cmd|'/c calc.exe'!A1  
=MSEXCEL|'\\..\\..\\..\\Windows\\System32\\cmd.exe /c calc.exe'!''
```





关注我们 分享每日精选文章

当用户打开恶意Excel电子表格时，将出现以下对话框。



关注我们 分享每日精选文章

第二个formula仍将执行代码，但对话框中的消息内容将被修改，此时我们可以看到不再要求用户启动CMD.EXE而是要求启动MSEXCEL.exe。





关注我们 分享每日精选文章

Outlook

在Outlook中也有许多可执行DDE payload的地方。例如，你已经获取到了域凭据，则可以更好的伪装电子邮件发送其他用户，以获取更多内部的shell。

Message

发送包含DDE的Outlook消息也可以自动执行代码。这同样适用于以附件形式发送的电子邮件。





关注我们 分享每日精选文章

但需要注意的是，因为某些电子邮件服务器会将所有电子邮件转换为HTML，为了避免我们的DDE payload失效，手
需要将电子邮件以RTF格式发送。





关注我们 分享每日精选文章

当用户打开我们发送的邮件后，DDE payload将会被执行。



关注我们 分享每日精选文章

Contact

创建新的联系人或修改现有的联系人，并将DDE payload放入Notes区域可导致执行代码。





关注我们 分享每日精选文章

联系人需要发送给目标用户。





关注我们 分享每日精选文章

当用户打开联系人时，将执行嵌入的DDE payload。



关注我们 分享每日精选文章

Calendar Invite

同样，该方法也适用与calendar invitation功能。例如，发送一个添加了DDE payload的会议邀请，一旦目标用户与其行了交互（打开或取消），则DDE payload就将被执行。





关注我们 分享每日精选文章

参考

<https://medium.com/red-team/dde-payloads-16629f4a2fcd>

<http://staaldraad.github.io/2017/10/23/msword-field-codes/>

<http://willgenovese.com/office-ddeauto-attacks/>

<https://www.secarma.co.uk/labs/is-dynamic-data-exchange-dde-injection-a-thing/>

*参考来源: [pentestlab](#), FB小编 secist 编译, 转载请注明来自FreeBuf.COM

S



下一篇：[本篇已是最新文章](#)

已有 1 条评论

路人

炒冷

选择

昵

请输入昵称

邮箱

请输入邮箱地址

表情

插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



[secist](#)

每个人的心中都有一个梦。。

110

文章数

43

评论数

1楼

回了

亮了

关注我们 分享每日精选文章

必须 您当前尚未登录。[登陆?](#) [注册](#)

必须 (保密)


最近文章

- [Microsoft Office之DDE攻击](#)

2018.01.22

- MITM6：用IPv6攻陷IPv4网络的工具
- 2018.01.18

相



W

浏览更多

打开...

- 关注我们 分享每日精选文章

惧怕勒索软件攻击？

nginx 1.3.9-1.4.0 DoS PoC

黑客是如何通过RDP远程桌面服务进...

浅谈被加壳ELF的调试

特别推荐



- OpenVAS开源风险评估系统部署方
- 双刃剑与灰色地带：“泄露数据收藏

魅影儿

2017-04-30

孙毛毛

2016-09-27

[2015最酷的Hack方式有哪些？](#)

[【限时优惠】FreeBuf精品公开课 | 36W漏洞奖金先生CplusHua：](#)

简单

2016-01-05

FB客服


2017-09-16



关注我们 分享每日精选文章



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务