**Hashes:**

PO-SCSP24090838.docx:
897ee7659b61315c82b5d89f9a7d4297f2840b54da61efb9ae543f35e2517f63

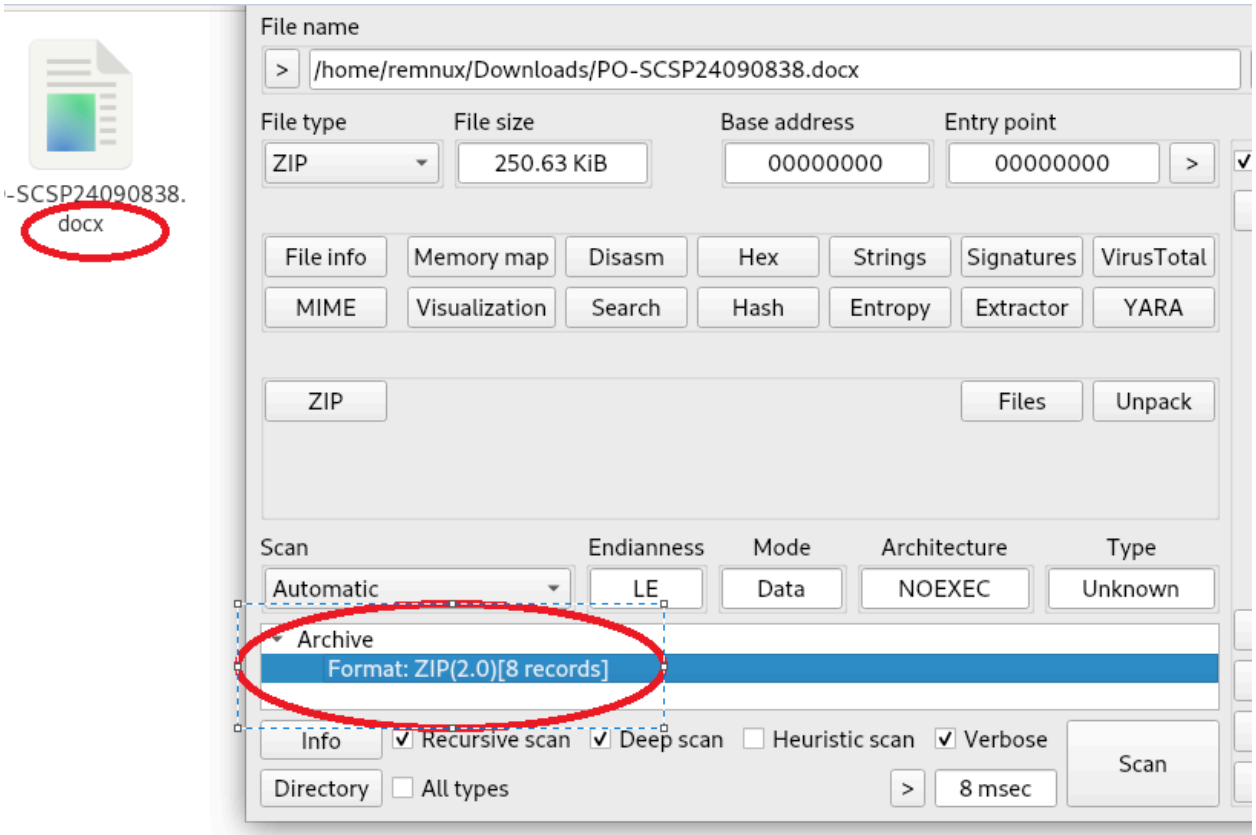
Austria.rtf: a2987f63f96d725c2e95d3133a150716208382f06abedd07b93c4249374d82cf

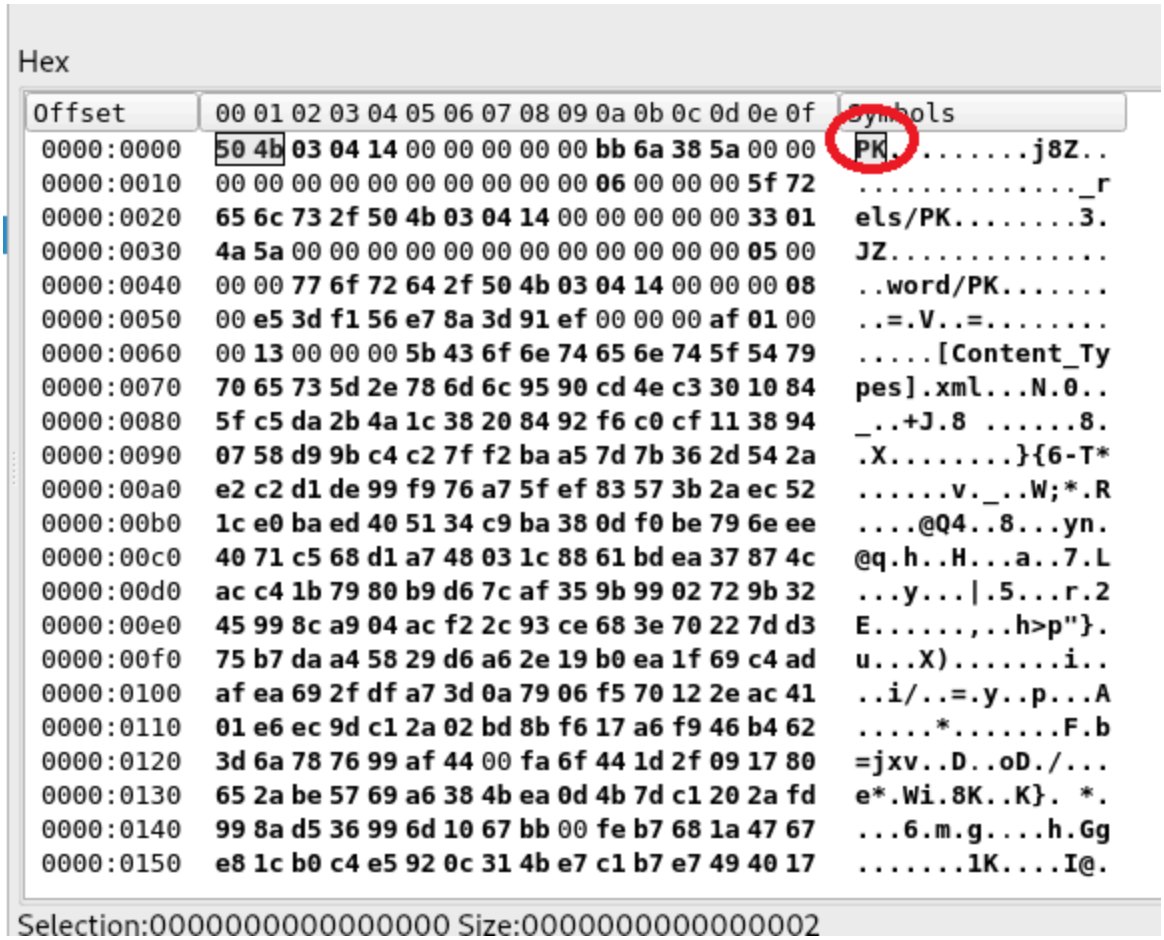
AdobeID.pdf: 447fdc076abf331b88f87809ee194cd1c3634d0556339c9711d61adcdc2c01cf

Austria.rtf.bin: 2a2dc8f2ce00edf7cfecbeb4affd36833e300c42df27a9495c5daf70a4c6537c

**CVE attempted to Exploit:**
CVE-2023-36884
CVE 2018-0802
CVE 2017-1882

**Information on Binaries**
Fake docx extension. Identified as zip based on the magic bytes






OleID

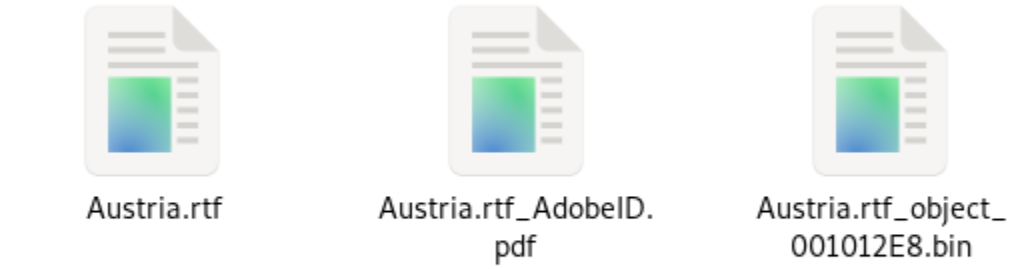
```
Filename: PO-SCSP24090838.docx
--------------------+--------------------+----------+--------------------------
Indicator           |Value               |Risk      |Description
--------------------+--------------------+----------+--------------------------
File format         |Generic OpenXML file|info      |
--------------------+--------------------+----------+--------------------------
Container format    |OpenXML             |info      |Container type
--------------------+--------------------+----------+--------------------------
Encrypted           |False               |none      |The file is not encrypted
--------------------+--------------------+----------+--------------------------
VBA Macros          |No                  |none      |This file does not contain
                    |                    |          |VBA macros.
--------------------+--------------------+----------+--------------------------
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
--------------------+--------------------+----------+--------------------------
External            |0                   |none      |External relationships
Relationships       |                    |          |such as remote templates,
                    |                    |          |remote OLE objects, etc
--------------------+--------------------+----------+--------------------------
remnux@remnux:~/Downloads$
```

Unzip docx

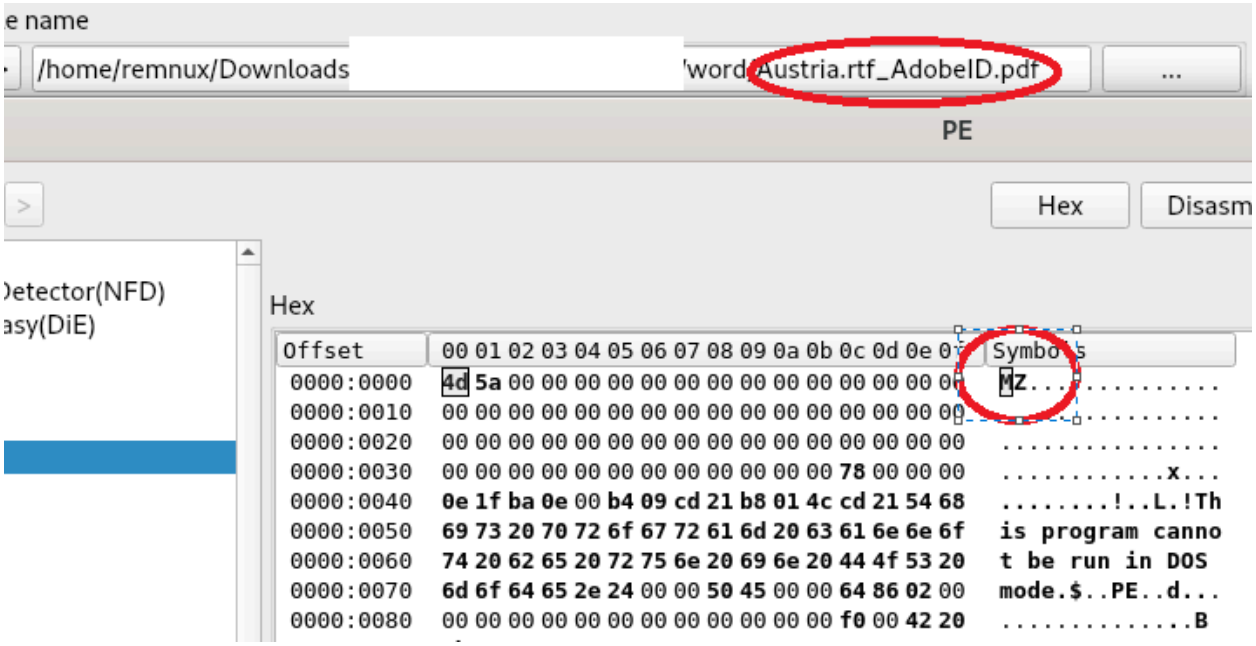

Rtfobj Austria.rtf

```
================================================================================
File: 'Austria.rtf' - size: 2945181 bytes
---+----------+-----------------------------------------------------------------
id |index     |OLE Object
---+----------+-----------------------------------------------------------------
0  |00003A12h |format_id: 2 (Embedded)
   |          |class name: b'Package'
   |          |data size: 482968
   |          |OLE Package object:
   |          |Filename: 'AdobeID.pdf'
   |          |Source path: 'C:\\Path\\AdobeID.pdf'
   |          |Temp path = 'C:\\Path\\AdobeID.pdf'
   |          |MD5 = 'b3dd9f55fbd3ecbb5b8831102cf9d4c2'
   |          |File Type: Windows PE Executable or DLL
---+----------+-----------------------------------------------------------------
1  |001012E8h |format_id: 2 (Embedded)
   |          |class name: b'Equation.3'
   |          |data size: 3072
   |          |MD5 = '403344b66690885723c6bf13bdc24fe9'
   |          |CLSID: 20E02C00-0000-0000-0C00-000000000004
   |          |unknown CLSID (please report at
   |          |https://github.com/decalage2/oletools/issues)
   |          |Possibly an exploit for the Equation Editor vulnerability
   |          |(VU#421280, CVE-2017-11882)
---+----------+-----------------------------------------------------------------
remnux@remnux:~/Downloads/PO-SCSP24090838.docx.2/word$
```

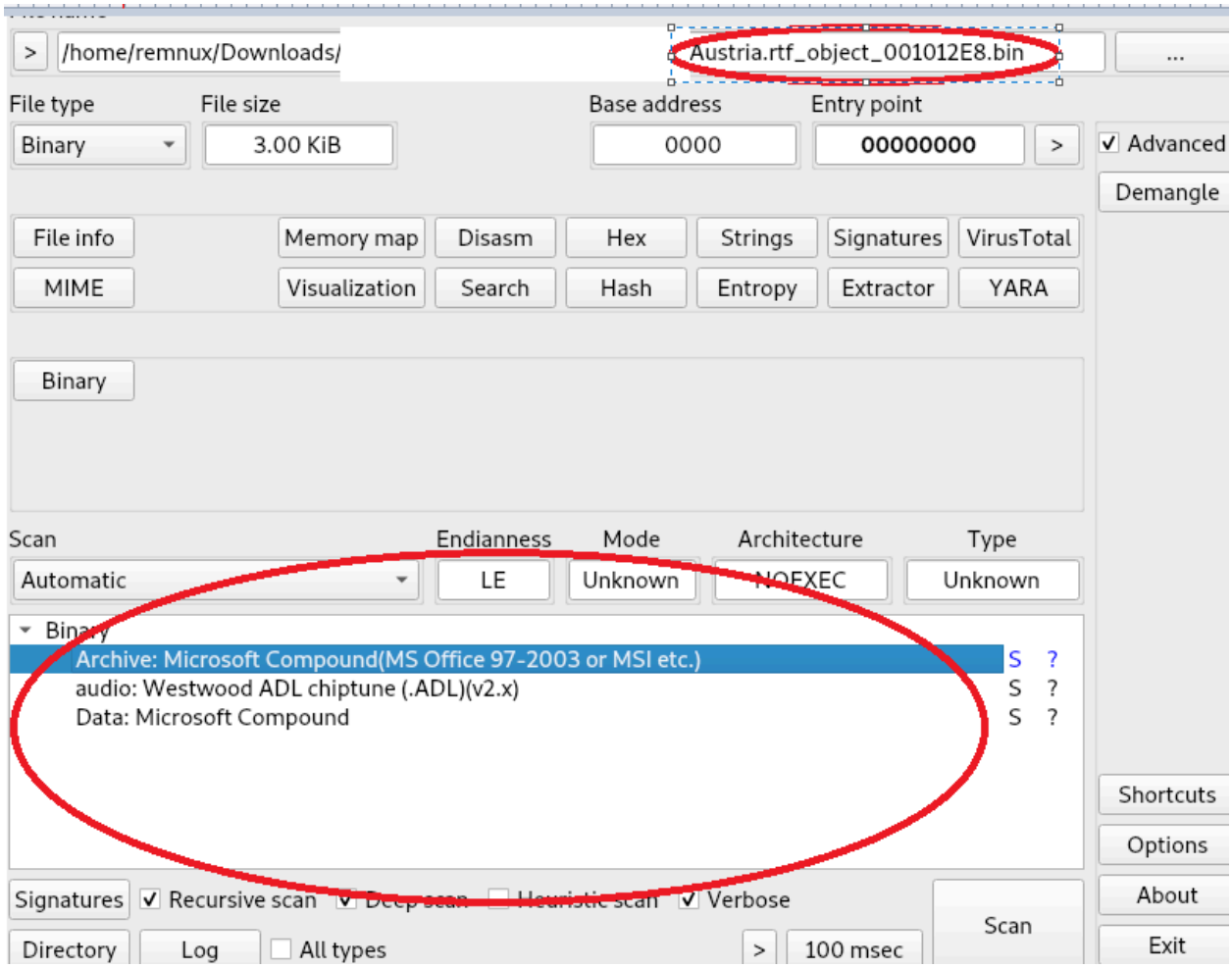
Rtfobj -s 0 Austria.rtf and rtfobj -s 1 Austria.rtf



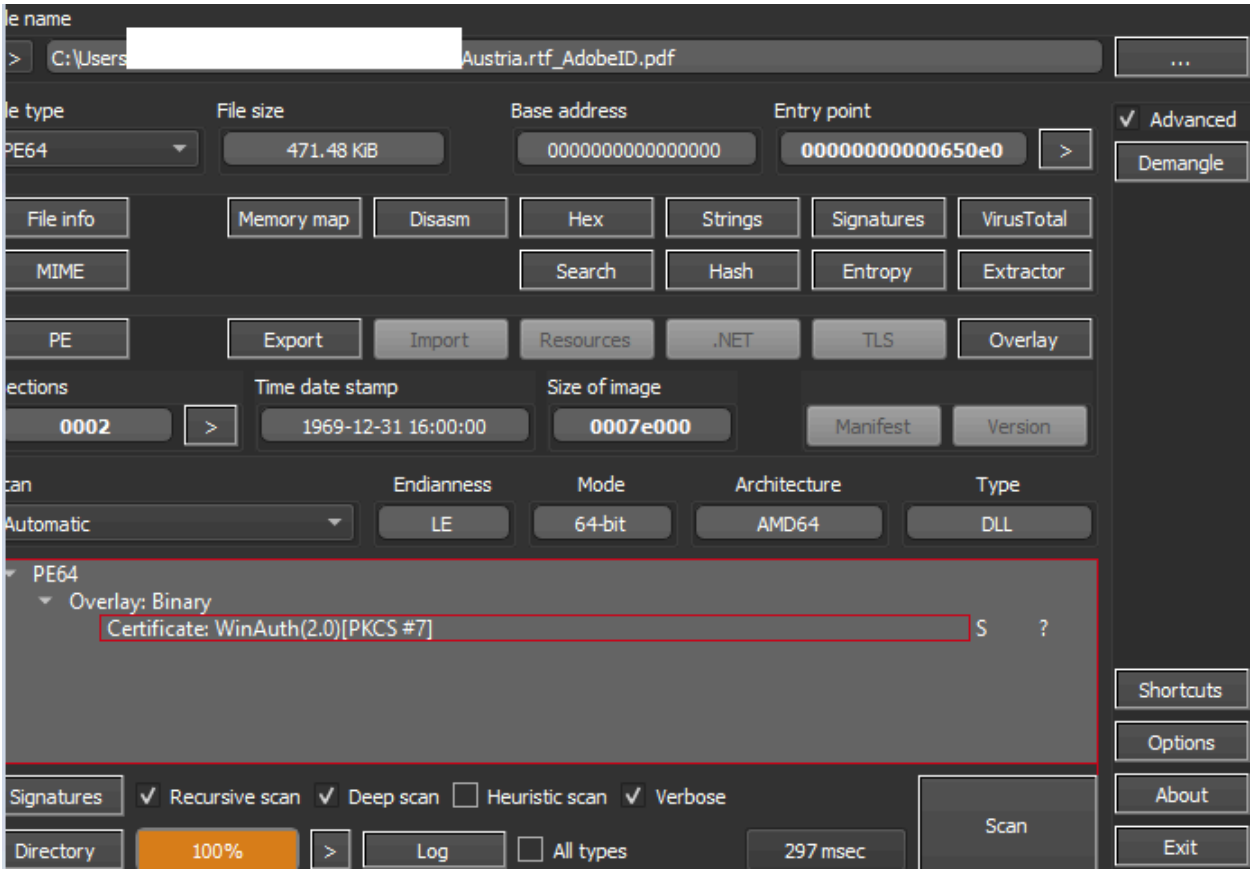

.Pdf payload is executable



Other binary object is a .ADL file?



DLL Info




***WIP**

Follow VirtualAlloc.Unpacks something