Detecting DDE in MS Office documents

By Didier Stevens

Published: 2017-10-11 · Archived: 2026-04-05 14:25:40 UTC

Dynamic Data Exchange is an old Microsoft technology that can be (ab)used to execute code from within MS Office documents. Etienne Stalmans and Saif El-Sherei from Sensepost published a blog post in which they describe how to weaponize MS Office documents.

We wrote 2 YARA rules to detect this in Office Open XML files (like .docx):

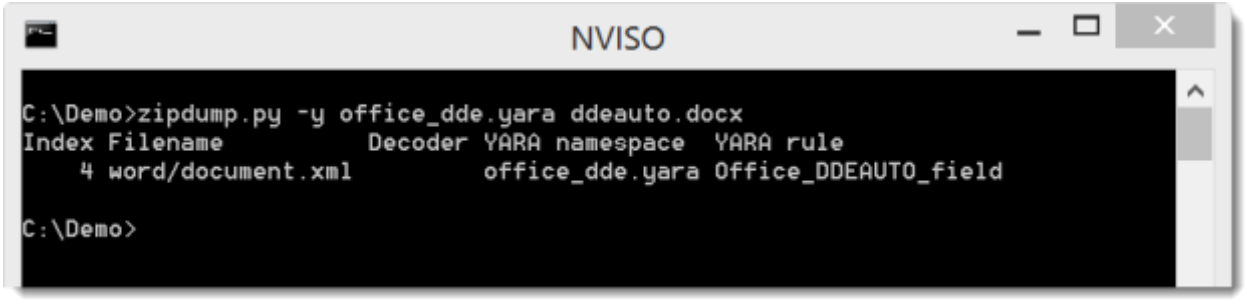
Update 1: our YARA rules detected several malicious documents in-the-wild.

Update 2: we added rules for OLE files (like .doc) and updated our OOXML rules based on your feedback.

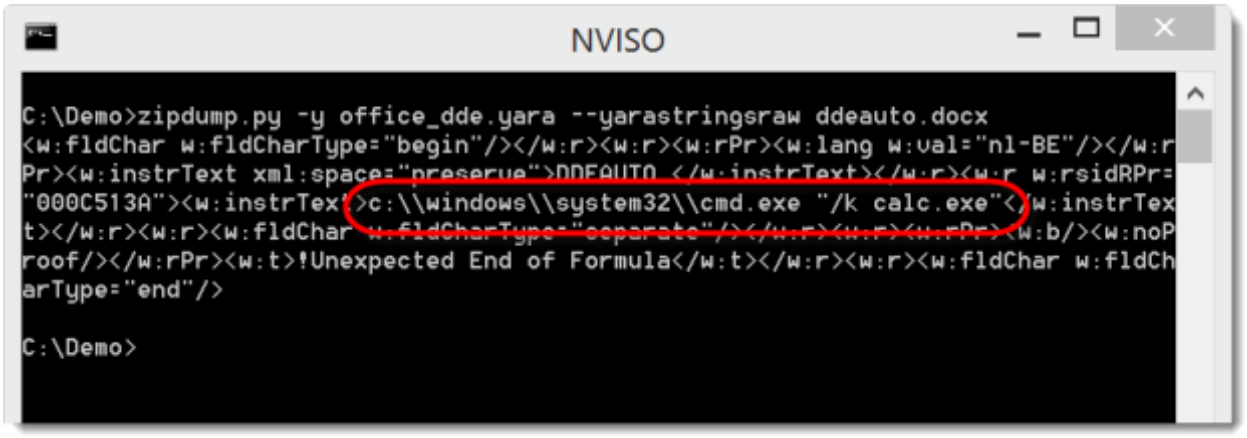
```
1  // YARA rules Office DDE
2  // NVISO 2017/10/10 - 2017/10/12
3  rule Office_DDEAUTO_field {
4      strings:
5          $a = /&lt;w:fldChar\s+?w:fldCharType=&quot;begin&quot;\/&gt;.+?\b[Dd][Dd][Ee][Aa][Uu]
   [Tt][Oo]\b.+?&lt;w:fldChar\s+?w:fldCharType=&quot;end&quot;\/&gt;/
6      condition:
7          $a
8  }
9  rule Office_DDE_field {
10     strings:
11         $a = /&lt;w:fldChar\s+?w:fldCharType=&quot;begin&quot;\/&gt;.+?\b[Dd][Dd][Ee]\b.+?
   &lt;w:fldChar\s+?w:fldCharType=&quot;end&quot;\/&gt;/
12     condition:
13         $a
14 }
15 rule Office_OLE_DDEAUTO {
16
```

```
17      strings:
18          $a = /\x13\s*DDEAUTO\b[^\x14]+/ nocase
19      condition:
20          uint32be(0) == 0xD0CF11E0 and $a
21  }
22  rule Office_OLE_DDE {
23      strings:
24          $a = /\x13\s*DDE\b[^\x14]+/ nocase
25      condition:
26          uint32be(0) == 0xD0CF11E0 and $a
27  }
28
29
30
31
```

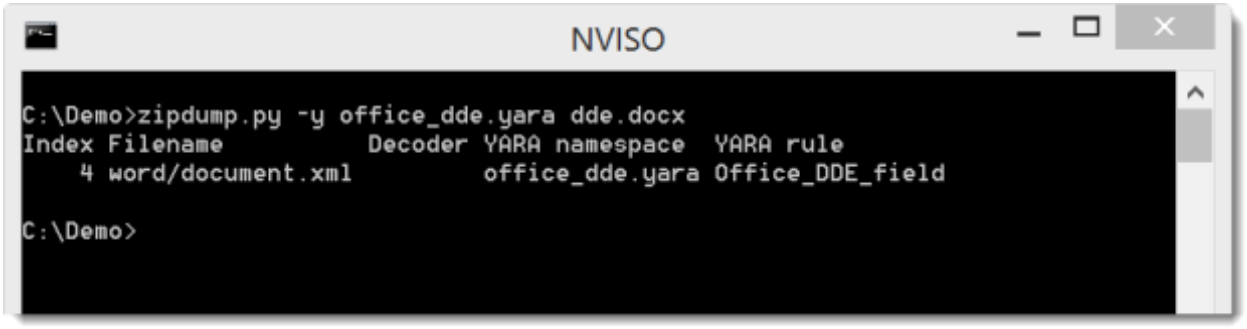
These rules can be used in combination with a tool like [zipdump.py] to scan XML files inside the ZIP container with the YARA engine:



The detection is based on regular expressions designed to detect fields containing the word DDEAUTO or DDE. By dumping the detected YARA strings with option –yarastringsraw, one can view the actual command:



Here is an example of the DDE rule firing:



You can also look for MS Office files containing DDE using this YARA rule in combination with ClamAV as described in this blog post.

Published October 11, 2017October 13, 2017

Post navigation

Source: https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/