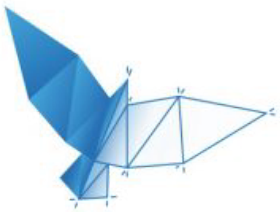


NVISO Labs

Cyber security research, straight from the lab!

Detecting DDE in MS Office documents

Didier Stevens | Maldoc, Remote Code Execution | October 11, 2017 | 1 Minute

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):

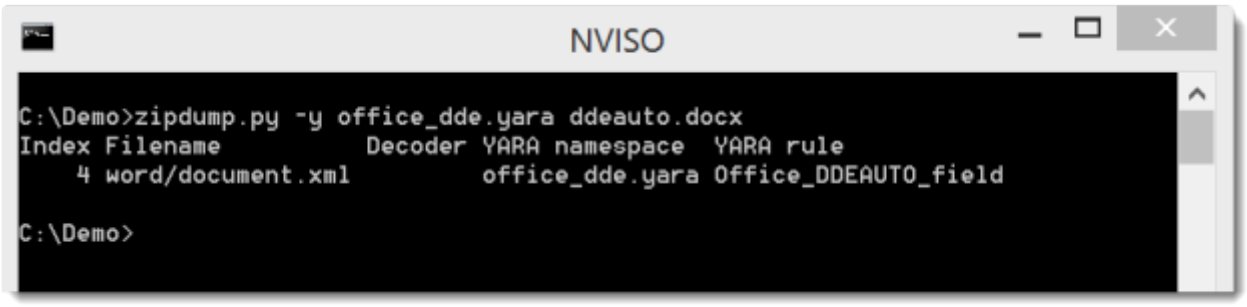
Update 1: our YARA rules detected several malicious documents in-the-wild.

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

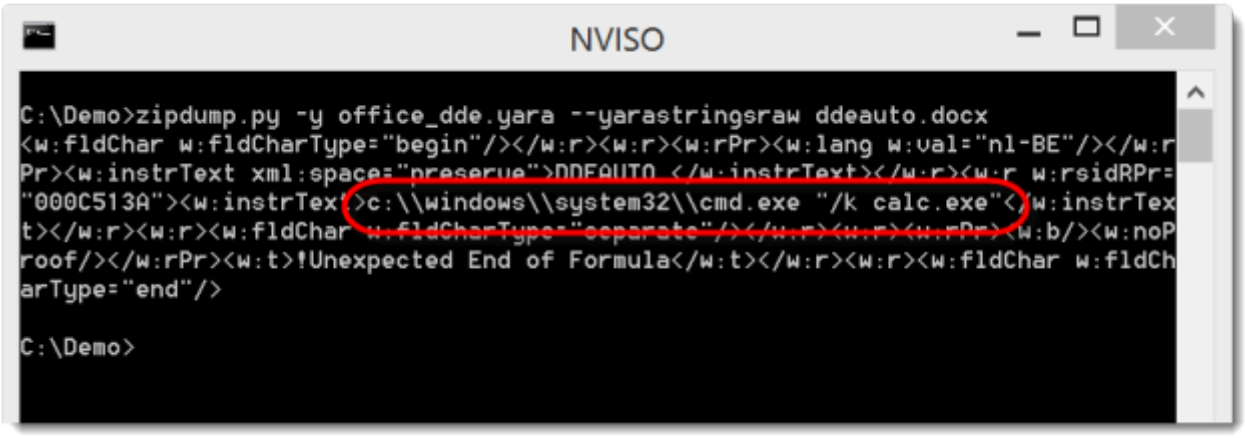
```
1 // YARA rules Office DDE
2 // NVISO 2017/10/10 - 2017/10/12
3 // https://sensepost.com/blog/2017/macro-less-code-exec-in-mswo
```

```
rule Office_DDEAUTO_field {
  strings:
    $a = /&lt;w:fldChar\s+?w:fldCharType=&quot;begin&quot;\/&gt
  condition:
    $a
}

rule Office_DDE_field {
  strings:
    $a = /&lt;w:fldChar\s+?w:fldCharType=&quot;begin&quot;\/&gt
  condition:
    $a
}

rule Office_OLE_DDEAUTO {
  strings:
    $a = /\x13\s*DDEAUTO\b[^\x14]+/ nocase
  condition:
    uint32be(0) == 0xD0CF11E0 and $a
}

rule Office_OLE_DDE {
  strings:
    $a = /\x13\s*DDE\b[^\x14]+/ nocase
  condition:
    uint32be(0) == 0xD0CF11E0 and $a
}
```

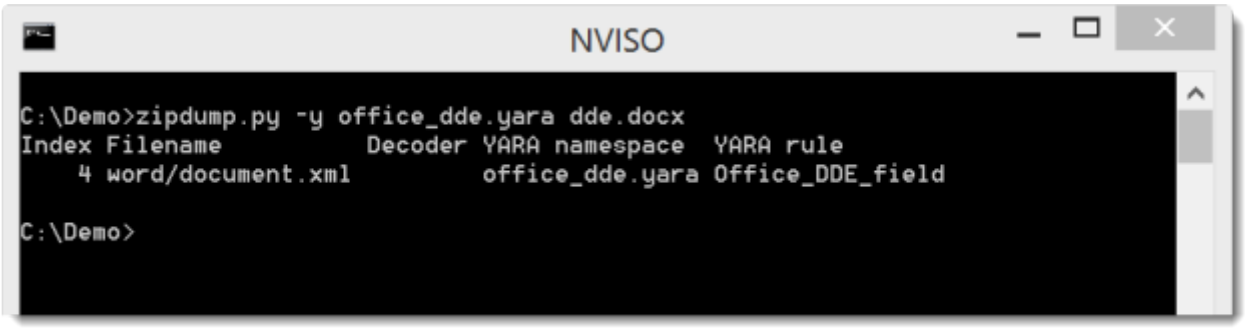
These rules can be used in combination with a tool like zipdump.py to scan XML files inside the ZIP container with the YARA engine:



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 by Didier Stevens

View all posts by Didier Stevens

‹ YARA rules for CCleaner 5.33

YARA DDE rules: DDE Command Execution observed in-the-wild ›

52 thoughts on “Detecting DDE in MS Office documents”

> Pingback: #microsoft is a gift that keeps giving.. To the #nsa et al. https:/... | Dr. Roy Schestowitz (罗伊)

> Pingback: YARA DDE rules: DDE Command Execution observed in-the-wild | NVISO LABS – blog

> Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled – Professional Hackers

> Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled – AnonymousMedia

> Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled

> Pingback: Microsoft Office Attack Runs Malware Without Needing Macros - Groovy Cloud

> Pingback: La función incorporada de MS Office permite la ejecución de malware sin macros activada

> Pingback: SANS ISC Stormcast: Every day Community Safety Information Abstract; Cyber Safety Podcast | NETWORKFIGHTS.COM

> Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled | TechNewsMix.com

Pingback: Microsoft Office Attack Runs Malware Without Needing Macros | 95CN Security

Pingback: Kritische Lücke in Microsoft Office ermöglicht Remote Code Execution - edv-tutorial

Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled – GeekFreak

Pingback: Fitur Microsoft Office Ini Memungkinkan Eksekusi Malware Tanpa Mengaktifan Makro - Error 404 Cyber News

Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled - Amicki's Tech Store

Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled – Antivirus Studio

Pingback: Macroless DOC malware that avoids detection with Yara rule – Furoner.CAT

Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled | DNN NEWS

Pingback: Old MS Office feature weaponized in malspam attacks – Computer Security Articles

Pingback: Old MS Office feature weaponized in malspam attacks | Computer Repair Newport RI 401-366-2249

Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled | ProDefence Security News | Website Protection | Antivirus - Firewall | Child Protection | Pc Protection

Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled – Cyber Security Research

Pingback: Office DDEAUTO attacks – Secure Your Way | Professional IT Services & Consultation Firm

Pingback: Malware abusing Microsoft Office DDE features - Koen Van Impe - vanimpe.eu

Jon Ketchum

October 25, 2017 at 4:38 pm

Awesome work! It appears that older versions of MSWord (2007/2010 saving in XML-format) insert DDE using a SimpleField tag that won't be caught by the regex above.
Sample XML from a 2007 Word Doc:
!Unexpected End of Formula

a quick stab at a yara rule to catch it would be something like:
$a = /w:instr="\s*\b(DDE|DDEAUTO)\b.+;\s*">/ nocase

Loading...

↩ Reply

Jon Ketchum

October 25, 2017 at 4:47 pm

The comment actually rendered the document XML sample in my original post. Here it is again using "code" meta-tag to (hopefully) avoid XML rendering:

```
!Unexpected End of Formula
```

Loading...

↳ Reply

Jon Ketchum

October 25, 2017 at 4:51 pm

Trying again…replacing angle-brackets with square-brackets to avoid XML rendering:
[w:fldSimple w:instr=” DDEAUTO c:\\Windows\\System32\\cmd.exe "/k calc.exe" “][w:r][w:rPr][w:b/][w:noProof/][/w:rPr][w:t]!Unexpected End of Formula[/w:t][/w:r][/w:fldSimple]

Loading...

↳ Reply

Pingback: MS Office Built-in Feature Allows Malware Execution Without Macros Enabled | Nastech

Pingback: Overview of Content Published In October | Didier Stevens

Pingback: Russian 'Fancy Bear' Hackers Using (Unpatched) Microsoft Office DDE Exploit - Sortiwa, Worlds largest web portal

Pingback: Russian ‘Fancy Bear’ Hackers Using (Unpatched) Microsoft Office DDE Exploit – NuclearCoffee

Pingback: Russian ‘Fancy Bear’ Hackers Using (Unpatched) Microsoft Office DDE Exploit – Security Newsfeeds

Pingback: Russian ‘Fancy Bear’ Hackers Using (Unpatched) Microsoft Office DDE Exploit | Nastech

Pingback: Russian ‘Fancy Bear’ Hackers Using (Unpatched) Microsoft Office DDE Exploit – AnonymousMedia

Pingback: Fancy Bear Adopts New DDE Attack Against Microsoft Office - Security Boulevard

Pingback: Russian 'Fancy Bear' Hackers Using (Unpatched) Microsoft Office DDE Exploit | TechNewsMix.com

Pingback: Russian ‘Fancy Bear’ Hackers Using (Unpatched) Microsoft Office DDE Exploit | Totally Secure

Pingback: Russian 'Fancy Bear' Hackers Using (Unpatched) Microsoft Office DDE Exploit - Amicki's Tech Store

Pingback: Russian ‘Fancy Bear’ Hackers Using (Unpatched) Microsoft Office DDE Exploit – carding news

Pingback: Microsoft Office Built-in Features Allow Malware Execution Without Enabling Macros - Cybcurity

Pingback: Cybercriminals Are Taking Advantage Of Microsoft Office Vulnerability That Microsoft Doesn't Consider As Threatening - Cybcurity

Pingback: Sicurezza informatica: Fancy Bear è tornato e stavolta sfrutta Office

Pingback: Fonctionnalité intégrée de MS Office permettant l'exécution de programmes malveillants sans macros activées ~ Red Monarch News

Pingback: Russian ‘Fancy Bear’ Hackers Using (Unpatched) Microsoft Office DDE Exploit | Rajveer Shinghania

Pingback: Update: Kritische Lücke in Microsoft Office ermöglicht Remote Code Execution | ISecM #Austria

Pingback: The Winter Games in Korea and Support from Sports-ISAO | Sports - ISAO

企业宣传片制作d2film.com影视视频制作公司QQ30998

April 15, 2018 at 3:11 pm

公司宣传片拍摄哪家好_公司宣传片制作哪家强_公司宣传片拍摄哪家强_宣传片拍摄报价企业宣传片制作d2film.com影视视频制作公司QQ30998
企业宣传片制作d2film.com影视视频制作公司QQ30998 http://www.d2film.com/

Loading...

↳ Reply

婚礼摄影MV-5aivideo.com婚礼摄像微电影QQ73595

April 29, 2018 at 5:16 am

结婚mv创意视频短片_婚礼创意mv婚礼上播放_婚礼摄像师_婚礼摄像价格_婚礼高清摄像婚礼跟拍视频5aivideo.com婚礼摄像微电影QQ73595
婚礼摄影MV-5aivideo.com婚礼摄像微电影QQ73595 http://www.5aivideo.com/

Loading...

↳ Reply

Pingback: HIDDEN RISKS IN THE MICROSOFT OFFICE SUITE - Votiro

Pingback: dde – secblog

Pingback: Built-in Feature of MS Office Lets Malware Execute Itself Without Macros Enabled – Tech N Gadgets

Pingback: Update: Kritische Lücke in Microsoft Office ermöglicht Remote Code Execution - edv-tutorial

Pingback: DDE and oledump, (Sun, Feb 21st) « CyberSafe NV

Leave a Reply

Enter your comment here...