

Microsoft Office Russian Dolls

 dshield.org/diary/Microsoft+Office+Russian+Dolls/32484

Process Tree

☐ Only show processes still running at end of current trace

☒ Timelines cover displayed events only

				Company	Own
	wmiprvse.exe (2532)	WMI Provider ...	C:\WINDOW...	Microsoft Cor...	NT...
	EQNEDT32.EXE (612)	Microsoft Equ...	C:\Program Fi...	Design Scien...	DES...
	CmD.exe (4116)	Windows Co...	C:\WINDOW...	Microsoft Cor...	DES...
	Conhost.exe (7028)	Console Wind...	C:\WINDOW...	Microsoft Cor...	DES...
	rundll32.exe (7072)	Windows host...	C:\WINDOW...	Microsoft Cor...	DES...
	rundll32.exe (6164)	Windows host...	C:\WINDOW...	Microsoft Cor...	DES...
	WerFault.exe (3892)	Windows Pro...	C:\WINDOW...	Microsoft Cor...	DES...
	svchost.exe (844)	Host Process ...	c:\windows\sy...	Microsoft Cor...	NT...
	svchost.exe (308)	Host Process ...	c:\windows\sy...	Microsoft Cor...	NT...
	svchost.exe (344)	Host Process ...	c:\windows\sy...	Microsoft Cor...	NT...
	svchost.exe (1064)	Host Process ...	c:\windows\sy...	Microsoft Cor...	NT...
	taskhostw.exe (736)	Host Process ...	c:\windows\sy...	Microsoft Cor...	DES...
	wermgr.exe (7636)	Windows Pro...	C:\WINDOW...	Microsoft Cor...	NT...
	svchost.exe (1072)	Host Process ...	C:\WINDOW...	Microsoft Cor...	NT...
	svchost.exe (1124)	Host Process ...	c:\windows\sy...	Microsoft Cor...	NT...
	svchost.exe (1176)	Host Process ...	c:\windows\sv...	Microsoft Cor...	NT...

Description: Windows Command Processor

Company: Microsoft Corporation

Path: C:\WINDOWS\SysWOW64\CmD.exe

Command: CmD.exe /C rundll32 %tmp%\license.ini,IEX A□▲C

User: DESKTOP-2C3IQHO\REM

PID: 4116

Started: 11/14/2025 2:20:19 PM

Exited: 11/14/2025 2:20:50 PM

Go To Event

Include Process

Include Subtree

Close

Handler on Duty: [Brad Duncan](#)

Threat Level: [green](#)

My next class:

[Reverse-Engineering Malware: Advanced Code Analysis](#)

Online | Japan Standard Time

Dec 8th - Dec 12th 2025

Published: 2025-11-14. **Last Updated:** 2025-11-14 13:42:55 UTC

by [Xavier Mertens](#) (Version: 1)

[0 comment\(s\)](#)

You probably know what are the Russian or Matryoshka dolls. It's a set of wooden dolls of decreasing size placed one inside another^[1]. I found an interesting Microsoft Office document that behaves like this. There was a big decrease in malicious Office documents due to the new Microsoft rules to prevent automatic VBA macros execution. But they remain used, especially RTF documents that exploits the good [CVE-2017-11882](#).

The document

(SHA256:8437cf40bdd8b005b239c163e774ec7178195f0b80c75e8d27a773831479f68f) that I found uses another technique to prevent the RTF document to be spread directly to the victim. The RTF document is placed into the OOXML document:

```
remnux@remnux:~/malwarezoo/20251113$ zipdump.py mexico_november_po.docx
```

```
Index Filename Encrypted Timestamp
1 _rels/ 0 2025-10-22 21:55:10
2 docProps/ 0 2025-10-22 21:55:10
3 word/ 0 2025-11-12 02:58:50
4 [Content_Types].xml 0 2025-10-22 21:55:22
5 docProps/app.xml 0 1980-01-01 00:00:00
6 docProps/core.xml 0 1980-01-01 00:00:00
7 word/_rels/ 0 2025-10-22 21:55:10
8 word/theme/ 0 2025-10-22 21:55:10
9 word/document.xml 0 2025-11-12 02:59:04
10 word/endnotes.xml 0 1980-01-01 00:00:00
11 word/Engaging.rtf 0 2025-11-12 02:58:34
12 word/fontTable.xml 0 1980-01-01 00:00:00
13 word/footer1.xml 0 1980-01-01 00:00:00
14 word/footnotes.xml 0 1980-01-01 00:00:00
15 word/numbering.xml 0 1980-01-01 00:00:00
16 word/settings.xml 0 1980-01-01 00:00:00
17 word/styles.xml 0 1980-01-01 00:00:00
18 word/webSettings.xml 0 1980-01-01 00:00:00
19 word/theme/theme1.xml 0 1980-01-01 00:00:00
20 word/_rels/document.xml.rels 0 2025-11-12 02:58:58
21 word/_rels/settings.xml.rels 0 1980-01-01 00:00:00
22 _rels/.rels 0 1980-01-01 00:00:00
```

The file is referenced in the Word document:

```

remnux@remnux:~/malwarezoo/20251113$ zipdump.py mexico_november_po.docx -s 20 -d | grep
Engaging.rtf
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
...
<Relationship
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/aFChunk"
Target="/word/Engaging.rtf" Id="YAjq8U"/>
</Relationships>

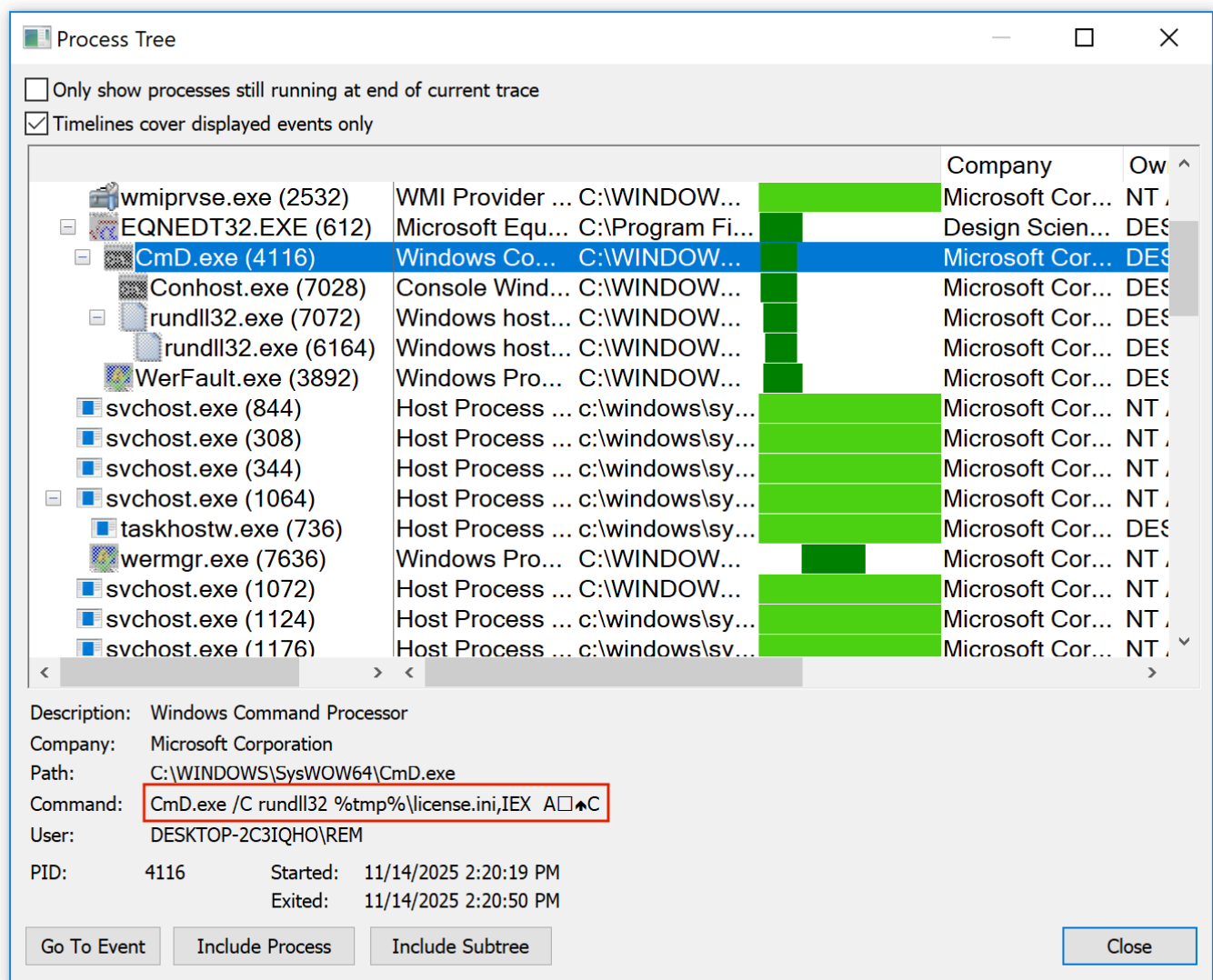
remnux@remnux:~/malwarezoo/20251113$ zipdump.py mexico_november_po.docx -s 9 -d | grep
YAjq8U
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas"
...
<w:body><w:altChunk r:id="YAjq8U"/>
...
</w:document>

```

The RTF document contains a shellcode that triggers the Equation Editor exploit. The next payload is C:\Users\user01\AppData\Local\Temp\license.ini. It's a DLL (SHA256:d8ed658cc3d0314088cf8135399dbba9511e7f117d5ec93e6acc757b43e58dbc) that is invoked with the following function: IEX

```
CmD.exe /C rundll32 %tmp%\license.ini,IEX A\x12\x0cC
```

You can see the special characters used as parameters to the function here:



This DLL is pretty well obfuscated, I'm still having a look at it but the malware family is not sure... Maybe another Formbook.

[1] https://en.wikipedia.org/wiki/Matryoshka_doll

Xavier Mertens (@xme)

Xameco

Senior ISC Handler - Freelance Cyber Security Consultant

[PGP Key](#)

Keywords: [Malware](#) [RTF](#) [Office](#) [Microsoft](#)

[0 comment\(s\)](#)

My next class:

[Reverse-Engineering Malware: Advanced Code Analysis](#)

Online | Japan Standard Time

Dec 8th - Dec 12th 2025

Comments

[Login here to join the discussion.](#)

[Diary Archives](#)

- [Homepage](#)
- [Diaries](#)
- [Podcasts](#)
- [Jobs](#)
- [Data](#)
- [Tools](#)
- [Contact Us](#)
- [About Us](#)