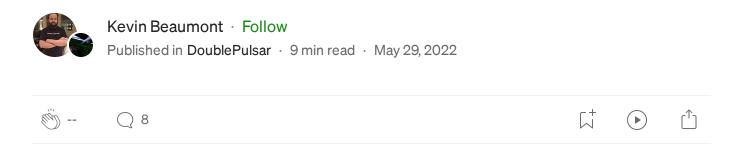




## Follina — a Microsoft Office code execution vulnerability



Two days ago, on May 27th 2022, Nao\_sec identified an odd looking Word document in the wild, uploaded from an IP address in Belarus. This turned out to be a zero day vulnerability in Office and/or Windows.

oublepulsar.co	m/follina-a-mid	crosoft-office-	-code-execut	lion-vuinerabiii	ty-1a47fce56	oublePulsar - 31 29e	
	ht my atte	ntion, as [	Defender	for Endpoi	nt missed	execution:	
This caug	incirry acco						
This caug	The first dece						
This caug	nemy acco						
This caug	nemy acco						
This caug	nemy acco						
This caug	The mily deco						
This caug	The miny deceo						
This caug							
This caug							
This caug							
This caug							

Follina — a Microsoft Office code execution vulnerability   by Kevin Beaumont   DoublePulsar - 31/10/2024 https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e	18:34
The document uses the Word remote template feature to retrieve a HTML file	
The document uses the Word remote template feature to retrieve a HTML file from a remote webserver, which in turn uses the ms-msdt MSProtocol URI scheme to load some code and execute some PowerShell.	
That should not be possible.	
That code does this, when decoded:	
There's a lot going on here, but the first problem is Microsoft Word is executing the code via msdt (a support tool) even if macros are disabled. Protected View does kick in, although if you change the document to RTF form, it runs without even opening the document (via the preview tab in Explorer) let alone Protected View.	











## Written by Kevin Beaumont

17.4K Followers · Editor for DoublePulsar

Everything here is my personal work and opinions.

