Member-only story

Follina — a Microsoft Office code execution vulnerability

Kevin Beaumont · Follow

Published in DoublePulsar · 9 min read · May 29, 2022

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.

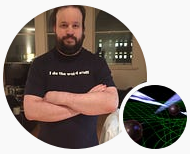
This caught my attention, as Defender for Endpoint missed execution:

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.