Blue Team Lab

# Reverse Engineering – Forked Tongue

*A French speaking client got a strange email from the local authorities about updates to GDPR guidelines and urgent action was required to avoid being fined.*

*Reverse Engineering*

*Medium*

Today, faced with the need to analyze vbs macros with insufficient tools, I learned that Libra Office is a tool I can use in inspect macros in documents. This only came to me when I read the postscript of a writeup from the blog “Click All the Things!”, where the author mentioned that URLs that are reached out to can be viewed in the Edit Links to Files button in word. Honestly, it was a bit of a leap in logic but thanks to that I no longer must work with obfuscated code. Recently learning more about the dark web it’s interesting to see that one of the referenced URLs is an onion one.