* What language should be used to write malware?

Can be written in many languages like C#, python, go, c/++ which impacts speed and ease of detection. For now C# sounds like a good compromise between ease of coding and detectability. Although it could be nice to start learning c/++

* What should be its capabilities? Possible features:
  + Sandbox detection
  + Reboot survival
  + Payload hidden in macro enabled documents
  + Additional reproduction (resharing via email, scanning local hosts)
  + CnC connection (maybe via MQTT)
  + Kibana management
  + Update features
  + Self backup
  + Malicious actions:
    - Reverse shell
    - Host scanning
    - Key logging
    - Clipboard monitoring ( eg. Recognizing account numbers) – it could recognise bitcoin wallets and substitute them with a predefined one. Gives a possibility of transferring btc to attackers wallet.
* Reading points:
  + Emotet
  + C2/CnC server
  + Cucko
  + Files
* Links:
  + <https://niiconsulting.com/checkmate/2018/02/malware-development-welcome-dark-side-part-1/>
  + <https://niiconsulting.com/checkmate/2018/02/malware-development-welcome-dark-side-part-2-1/>
  + <https://niiconsulting.com/checkmate/2018/03/malware-development-welcome-dark-side-part-2-2/>
  + <https://niiconsulting.com/checkmate/2018/03/malware-development-welcome-dark-side-part-3/>
  + <https://niiconsulting.com/checkmate/2018/03/malware-development-welcome-to-the-dark-side-part-4/>
  + <https://www.varonis.com/blog/malware-coding-lessons-people-part-learning-write-custom-fud-fully-undetected-malware/>
  + <https://docs.microsoft.com/en-us/office/vba/library-reference/concepts/getting-started-with-vba-in-office>
  + <https://eforensicsmag.com/analysis-of-malicious-excel-spreadsheet-by-monnappa-k-a/>
  + <https://www.mimecast.com/blog/2020/03/velvetsweatshop-microsoft-excel-spreadsheet-encryption-rises-again-to-deliver-limerat-malware/>
  + <https://securitynews.sonicwall.com/xmlpost/excel-4-0-macro-being-used-to-deliver-malware/>
  + <https://niiconsulting.com/checkmate/?s=malware>
* Pytania:
* Plan:
  + Poczytać o persystancji malware’u
  + Obfuskacja malwareu’u
  + Do 13 przygotować plan