Wordlist-based DGA Generation
Explanation: This DGA generates domains by combining random words from a
predefined wordlist.
Usefulness: This type of DGA can be useful for malware authors to create domains
that appear more human-readable and less suspicious.
Strengths: The generated domains are more likely to bypass filters and appear
legitimate.
Weaknesses: The wordlist used may be known or detectable, and the pattern of
combining words may be recognizable.
Deception: This DGA can be deciphered by analyzing the pattern of generated
domains and identifying the wordlist used and the word combination algorithm.
www.figdate.net
www.cherrykiwi.org
www.grapemango.org
www.appleapple.gov
www.grapeapple.net
www.cherryfig.org
www.mangolemon.com
www.figkiwi.gov
www.figmango.net
www.elderberry.info

Regex for Wordlist-based Generated DGAs: [v|d|y|l|w|e|o|a|i|g|n|m|k|c|p|f|t|r|h]+|[^b.]{0,2}{1,3}

Yara rule:
 rule dga_domain_detection {
    meta:
        description = "Detects DGA-generated domain names"
    strings:
        $dga_regex = /[v|d|y|l|w|e|o|a|i|g|n|m|k|c|p|f|t|r|h]+|[^b.]{0,2}{1,3}/ nocase
    condition:
        $dga_regex
}

Note: Can use https://riskmitigation.ch/yara-scan/ or MalwareBazaar https://bazaar.abuse.ch/ but will need API Key