Emoji DGA Generation

Explanation: This DGA generates domains using emojis.

Usefulness: This type of DGA can be useful for malware authors to create domains that appear obfuscated and less suspicious.

Strengths: The generated domains are less likely to be recognized as DGA domains and may bypass filters.

Weaknesses: The emoji pattern may be detectable, and the emoji set used may be known or reverse-engineered.

Deception: This DGA can be deciphered by analyzing the pattern of generated domains and identifying the emoji set used.

```
www.💡💡🙌😀😀🚀🤔😀🙌.net
www.🚀🌍🤔😂😍😍🤔.gov
www.😍🎉😍🎉🎉🙌👍🙌.net
www.👍😀🙌👍🙌😍🚀😀.info
www.😂🚀🎉🤔😍🙌🤔👍😀🤔.gov
www.🎉💡😂🌍🚀👍💡😀.org
www.😍😍💡🙌🤔🤔🚀🤔.com
www.😀😂🤔🚀😍😂😍🎉🤔🌍.com
www.🚀🙌🙌🚀🌍😂🌍🌍.info
www.😂😀🤔🎉🤔🌍😂🙌.org
```

Regex for Emoji Generated DGAs: `[r|w|m|e|o|c|v|i|g|n|f|t]+|[^🙌🎉😀😂💡😍🤔🚀👍.🌍]{0,2}{1,3}`

Yara rule:

```
 rule dga_domain_detection {
    meta:
        description = "Detects DGA-generated domain names"
    strings:
        $dga_regex = /[r|w|m|e|o|c|v|i|g|n|f|t]+|[^🙌🎉😀😂💡😍🤔🚀👍.🌍]{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