Time-based DGA Generation

Explanation: This DGA generates domains based on the current time.

Usefulness: This type of DGA can be used by malware authors to create a set of constantly changing domains for C&C communication or data exfiltration.

Strengths: The generated domains change frequently, making it difficult to block them all.

Weaknesses: The time-based pattern may be detectable, and the generated domains may be predictable if the algorithm is known.

Deception: This DGA can be deciphered by analyzing the pattern of generated domains and identifying the relationship between the domains and the current time.

www.2024031819.info
www.2024031819.org
www.2024031.org
www.2024031819.info
www.2024031.net
www.2024031819.biz
www.2024031.biz
www.2024031819.biz
www.202403181.com
www.20240318.biz

Regex for Time-based Generated DGAs: [r|w|o|b|i|g|n|f|z]+|[9|4|0|8|2|3|1]+|[^mect.]{0,2}{1,3}

Yara rule:

```
 rule dga_domain_detection {
    meta:
        description = "Detects DGA-generated domain names"
    strings:
        $dga_regex = /[r|w|o|b|i|g|n|f|z]+|[9|4|0|8|2|3|1]+|[^mect.]{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