Zodiac-based DGA Generation
Explanation: This DGA generates domains based on zodiac signs and random strings.
Usefulness: This type of DGA can be useful for malware authors to create a unique set of domains for command and control (C&C) communication or data exfiltration.
Strengths: The use of zodiac signs and random strings makes the generated domains unpredictable and difficult to block.
Weaknesses: The zodiac sign pattern may be detectable, and the random string generation algorithm may be reverse-engineered.
Deception: This DGA can be deciphered by analyzing the pattern of generated domains and identifying the relationship between the zodiac signs and dates.
Random seed: $-i]b"}B,R*KG!?,
www.2de154bbd.net
www.b66c09d9.biz
www.18d851v.com
www.b109635x8.net
www.f4w8t15.biz
www.f644d25ac8.org
www.04996c0d9b.biz
www.935052844.net
www.8049b2gd.org
www.f6c122b.org

Regex for Zodiac Sign Generated DGAs: [r|w|e|o|b|c|d|i|g|n|f|t|z]+|[9|4|0|8|2|3|5|6|1]+|[^mxav.]{0,2}{1,3}

Yara rule:

```
 rule dga_domain_detection {
    meta:
        description = "Detects DGA-generated domain names"
    strings:
        $dga_regex = /[r|w|e|o|b|c|d|i|g|n|f|t|z]+|[9|4|0|8|2|3|5|6|1]+|[^mxav.]{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