Arithmetic-based DGA Generation
Explanation: This DGA generates domains by performing arithmetic operations on a base value and a random number.
Usefulness: This type of DGA can be useful for malware authors to create a unique set of domains for C&C communication or data exfiltration, based on a shared base value.
Strengths: The generated domains are unpredictable without knowledge of the base value and the arithmetic operation used.
Weaknesses: If the base value or the arithmetic operation is compromised, the generated domains can be predicted.
Deception: This DGA can be deciphered by analyzing the pattern of generated domains and attempting to reverse-engineer the base value and the arithmetic operation.
www.0012595.info
www.0012634.org
www.0000012962.com
www.0000013254.info
www.00012631.net
www.000012472.org
www.0000012625.net
www.00012627.info
www.0000012970.org
www.0012568.info

Regex for Arithmetic-based Generated DGAs: [r|w|o|e|i|g|n|f|t]+|[9|4|0|2|3|5|7|6|1]+|[^8c.m]{0,2}{1,3}

Yara rule:

```
 rule dga_domain_detection {
    meta:
        description = "Detects DGA-generated domain names"
    strings:
        $dga_regex = /[r|w|o|e|i|g|n|f|t]+|[9|4|0|2|3|5|7|6|1]+|[^8c.m]{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