Regles Yara

Les **regles YARA** són un conjunt de patrons utilitzats per identificar i classificar arxius maliciosos, codi maliciós o comportaments sospitosos en sistemes informàtics. Van ser desenvolupades per **Víctor Álvarez**, un investigador de seguretat, amb l'objectiu de facilitar la identificació de codi maliciós en investigacions de seguretat i anàlisi forense.

YARA (Yet Another Ridiculous Acronym) permet definir regles que descriuen les característiques de fitxers o processos sospitosos mitjançant patrons de text o seqüències de bytes. Aquestes regles són especialment útils en la recerca de codi maliciós, ja que ajuden a detectar famílies de codi maliciós basades en similituds, fins i tot si el codi maliciós ha estat modificat lleugerament per evitar ser detectat per mètodes tradicionals.

És un estàndard de factor àmpliament utilitzat a la comunitat de la ciberseguretat i de gran implementació i integració amb altres eines.

Estructura bàsica d'una regla YARA

Cada regla YARA té tres seccions principals:

1. **Identificador (nom de la regla)**: El nom de la regla que s'utilitzarà per referir-s'hi.
2. **Metadades (opcional)**: Informació addicional com a descripcions, autor, data, etc.
3. **Condicions**: Defineixen quines característiques o patrons ha de complir un fitxer per ser considerat com una coincidència.

Exemple d'una regla YARA:

```
rule DetectaMalwareExemmple
{
    meta:
        author = "Investigador"
        description = "Regla per a detectar malware"
        date = "2024-10-24"

    strings:
        $cadena1 = "malware"
        $cadena2 = {6A 40 68 00 30 00 00 6A 14 8D 91}

    condition:
        $cadena1 or $cadena2
}
```

Explicació de l'exemple:

- **meta**: Conté informació addicional sobre la regla, com l'autor i una descripció.
- **strings**: Conté els patrons que es buscaran, com ara cadenes de text o seqüències hexadecimals.
- **condition**: És la part que especifica quan s'activarà la regla. En aquest cas, la regla s'activarà si es troba "**malware**" o la seqüència de bytes hexadecimal.

Característiques principals:

- **Simplicitat**: El llenguatge YARA és senzill d'aprendre i entendre, però és extremadament potent per detectar patrons complexos.
- **Eficiència**: YARA pot analitzar grans volums de dades de manera eficient, cosa que és essencial en anàlisi forense o detecció d'amenaces en temps real.
- **Extensibilitat**: Permet afegir múltiples patrons (cadenes de text, expressions regulars, seqüències de bytes) i condicions lògiques.

Casos d'ús:

- **Detecció de codi maliciós**: Identificació de variants de codi maliciós basades en patrons coneguts.
- **Anàlisi forense**: Durant una investigació de ciberseguretat, es poden fer servir les regles YARA per escanejar sistemes i arxius a la recerca d'indicadors de compromís (IoC).
- **Protecció proactiva**: Algunes solucions de seguretat integren regles YARA per detectar amenaces emergents de manera proactiva.

En resum, les regles YARA són una eina fonamental en la ciberseguretat per a la identificació i l'anàlisi d'amenaces, gràcies a la seva flexibilitat i potència per detectar patrons en fitxers o

en la memòria del sistema.

Tasca

En el nostre cas tindrem una presa de contacte amb les regles Yara d'una manera força senzilla. Ens crearem una regla que pugui detectar un malware real, en aquest cas el conegut com a ***Vidar***.

Puja primer la mostra a Virustotal i comprova com efectivament multitud de motors d'antivirus la detecten com a codi maliciós (malware).

Per continuar, l'estructura de la regla serà la que es mostra més amunt, feu una cerca a Internet si així ho necessiteu per al vostre cas concret. Es pretén que la regla Yara elaborada inclogui:

- Metadades
- Com a autor el vostre nom i cognom
- Com a descripció el vostre curs i l'any acadèmic (ex. 4C - 98/99)
- Data
- Que es detectin dues cadenes
- Sobre la mostra de malware proporcionada i fent ús de l'ordre `strings`, intenteu localitzar dues cadenes que semblin úniques i relatives a aquest malware (IPs, comunicacions mitjançant canals de Telegram, dominis, ubicacions de disc...)
- Utilitzeu dues d'aquestes informacions com les cadenes a detectar
- La condició és que s'hagin de complir ambdues cadenes obligatòriament

Instal·lació de Yara

Per instal·lar Yara a Rocky no teniu més que:

```
sudo dnf install yara
```

i arreglat. Per provar la regla contra la mostra de codi maliciós la sintaxi serà:

```
yara ruta/a/la/regla_yara.yara ruta/a/la/mostra_malware
```

Si la detecció és exitosa, veureu que se us repeteix el nom de la regla per pantalla, en cas contrari no obtindrem cap sortida.