INFORME REGLAS YARA

Informe Reglas Yara

Análisis de Malware / Seguridad de la Información

Jordan Andres Diaz Sanchez
Profesor: Adrián Rodríguez

TABLA DE CONTENIDO

1. INFORME TECNICO

1.1. Estructura General del Script

Este script automatiza la recolección, compilación y ejecución de reglas YARA obtenidas desde múltiples repositorios públicos de GitHub. Su objetivo principal es detectar patrones maliciosos en muestras de malware, facilitando tareas de análisis y cacería de amenazas (Threat Hunting). **(yara_malware_scanner.py)**

1.2. Estructura General del Script

El script se organiza en cinco fases clave:

Fase	Descripción
1. Clonado/Actualización	Se descargan 25 repositorios de reglas YARA desde GitHub.
2. Recolección de Reglas	Se unifican todos los archivos .yar/.yara en una carpeta común.
3. Normalización	Se renombran los archivos .yara a .yar para uniformidad.
4. Compilación	Se compilan todas las reglas en un único archivo binario.

Cada función está modularizada para permitir fácil mantenimiento y expansión.

1.3. Repositorios Utilizados

Se integran 25 fuentes públicas de alta calidad que contienen reglas YARA especializadas:

- CAPEv2
- malice-plugins

- jeFF0Falltrades
- malpedia
- McAfee ATR
- Neo23x0 (signature-base)
- Yara-Rules/rules
- bartblaze
- h3x2b
- Intezer
- Elastic
- Security Without Borders
- SentinelOne
- RevSkills
- TrendMicro
- ChkSecurity
- Google Malware Detection
- Tenable
- MalwareHunterTeam
- Hasherezade
- AresS31
- REMnux
- Palo Alto Networks
- MikeSXRS
- ThreatFoundry

1.4. Requisitos Técnicos

Elemento	Requerimiento
Sistema	Linux (Ubuntu/Debian recomendado)
Python	Python 3.x
Librerías	yara-python, GitPython, shutil, glob, os
Acceso	Conexión a internet para clonar repos
Muestras	Carpeta con malware para analizar

Para instalar dependencias:

- pip install yara-python GitPython

1.5. Guía de Ejecución

A. Descargar y dar permisos
Coloca el archivo yara_malware_scanner.py en tu entorno de trabajo:

- chmod +x yara_malware_scanner.py

B. Asegúrate de tener las siguientes rutas creadas:

- /home/Desktop/yara_automatico/malware/

C. Ejecutar el script

- python yara_malware_scanner.py

Este script mostrará los repositorios que va clonando/actualizando, el proceso de compilación y las coincidencias encontradas al escanear las muestras.

1.6. Notas Finales

- El script puede demorar (por la descarga de repositorios).
- Las reglas se guardan compiladas para reutilizar sin recompilar cada vez.
- Es ideal para usar en entornos de laboratorio, CTFs o formación en análisis de malware.