**Why YARA?** Matthew Jang

2주+ 동안 YARA를 공부하고 실험해보고 제 생각 이랑 궁굼한 것 들을 써봤습니다.

YARA Pros (장점) +

1. 정말 간단하다

2. 사용하기가 쉽다

- $ yara [Options] Rules-File Target-File

3. 빠르다 (시간)

- YARA 는 아무리 큰 파일 들도 간단한 command으로 scanning을 할수있다 (regardless of size)

- 엄청 큰 파일 안에서 string 하나만 찾고싶은 경우에는 간단하게 YARA 한태 찾으라고 하면 엄청난 시간을 아낄수 있다.

- 행위 분석 (behavior analysis) 은 시간 이랑 resource (money, CPU, etc.) 가 많이 필요한 방식이다. 그래서 YARA 를 이용해서 의심이 되는 파일 이나 로그 들만 찾은 다음에 행위 분석을 하면 시간을 저축할수 있지 않을가.. 라고 생각 합니다.

YARA Cons (단점) -

1. 정확하지가 않다

- False Positive (의미 없는 결과) 나오는 경우 가 있다.

- 중요한 string들을 놓지는 경우 가 있다 (Rule안에 안써서).

- YARA rule 은 사고후 (사후) 로그 를 통해서 만 작성을 할수 있다.

2. Binary 파일 만 읽을수 있다.

3. YARA rule들은 시간이 흐를수록 뒤떨어져서 항상 새로운 rule들을 쓰고 update해야 된다.

- Malware, SQLi, 또는 Ransomeware 들은 항상 변합니다. 변할때 마다 rule 을 써야되요.

4. Open-source라서 해커들이 rule을 보고 새로운 방식을 찾아낼수있다.

5. Malware를 막지는 못하고 탐지 만 할수있다. Malware의 pattern & strings들을 찾아서 해커들의 발걸음을 따라가는 것이다.

6. Raw data를 핸들 할수가 없다.

7. Plura가 가는 방향에서 방해 되지가 않을가 싶습니다.

8. 요즘 은 행위 분석 을 주로 사용하고 signature matching 은 별로 안씁니다.

9. 결론은 생각보다 눈과 손이 많이 가는 tool 입니다.

YARA 가 어떡해 실행 하는지 예를 들겠습니다.

요즘 SQL Injection 에 대한 YARA Rule 작성 을 했고 Apache2 에 있는 Log File 을 YARA 한태 보내봤습니다 ($ yara Rule.yar Log\_File).

결과는 이렇게 나왔습니다 (짧은 version): @ 터미널

matthew@matthewjang ~/Yara Tests/Email Project $ yara -s -f Rule.yar Log\_File

Rule Log\_File (Rule이랑 Log\_File 이 match 됬다)

0x392:$char2: – (0x392: line 위치)

0x66:$char3: #

0x5f9b:$str1: CONCAT (“CONCAT” 라는 string 이랑 match 됬다)

0x10d53:$str2: CHAR

0x65c1f:$str9: MD5

0x10d37:$str12: CAST

0x3a75d:$str13: CONVERT

0x10783:$str17: VERSION

0x385:$str18: WHERE

0x11b87:$str19: LIMIT

0x3a6:$str20: EXEC

0x65c09:$str25: BENCHMARK

0x2fb:$str37: UNION

Log\_File에 담겨진 CONCAT, CHAR, 또는 UNION (등등) 이란 string 들을 YARA 가 발견 한 겁니다. 발견된 string들은 SQL Injection할때 많이 보이는 string입니다. 하지만 발견되지 않은 string들도 분명히 있을거고 발견된 string 들이 false positive인지 아닌지 모릅니다.

더 중요한 것은YARA 가 Plura 에 도움이 될지 안될지 아직 모르겠습니다. Plura안에서 언제 어디서 써야되는지 도 모르겠습니다.

현재 YARA 랑 비슷한 역할 을 하는 script 가 Plura안에 있다고 들었는데 YARA를 대신 쓸수는 있겠지만 제 생각에는 큰 의미나 변화는 없을 것 같습니다.

SQL Injection 이랑 Ransomware 탐지 하는 경우에는 아직 YARA 가 많이 부족할 것 같고 장점을 살리기는 조금 힘들 것 같습니다.

구체적인 결과 같은게 아나와서 죄송합니다. 저랑 같이 고민을 하고 방향 이나 결론 을 찾았으면 좋겠습니다.

감사합니다!