Обнаружение и скрытие процессов

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цели урока

- Узнать про EDR — систему обнаружения вредоносной активности
- Разобрать, как писать YARA-правила для выявления вредоносных программ
- Узнать, как скрывать процесс

EDR

Endpoint Detection & Response (EDR) — класс решений для обнаружения и изучения вредоносной активности на конечных точках: подключённых к сети рабочих станциях, серверах, устройствах.

Правила для поиска

YARA — это инструмент для поиска и классификации вредоносных программ.

Утилита выполняет сигнатурный анализ на основе заранее сформулированных правил — YARA-описаний.

Правила для YARA

Правила хранятся в текстовом формате в файле .yar и состоят из двух секций:

- секции определений (strings)
- секции условия (condition)

```
rule SomeMalwareName {

meta:
author = "AuthorName"

strings:
…

condition:
…
}
```

MIMIC

MIMIC — инструмент для сокрытия процессов.

Преимущества MIMIC:

- может запустить «зловредную» программу и сделать её похожей на любую другую «легальную» программу
- не требует разрешений — может использоваться кем угодно

Выводы урока

- Для обнаружения и изучения вредоносной активности используется система EDR
- Найти вредоносные программы можно с помощью YARA-правил
- Вредоносные процессы можно скрыть с помощью MIMIC

Итоги модуля

- Процессы могут быть фоновые, интерактивные и демоны
- Один процесс может породить другой, он станет родительским по отношению к созданному процессу, а созданный процесс станет дочерним
- У каждого процесса есть свой PID, по которому команды ps и top могут отслеживать процессы
- На приоритетность процессов можно влиять при необходимости
- Вредоносные процессы (бэкдоры) нужно выявлять и скрывать при помощи EDR, YARA и MIMIC