AVSOFT LOKI

ОПИСАНИЕ ПРОБЛЕМЫ

Кибератаки могут атаковать любой тип устройства в ИТ-инфраструктуре организации и быстро распространиться по сети, молниеносно заражая или уничтожая информационные ресурсы.

РЕШЕНИЕ

LOKI – система имитации ложной ИТ-инфраструктуры для обнаружения кибератак на различные типы устройств. Система относиться к классу систем Deception - платформ ложных распределенных целей для инициации активного взаимодействия с кибератакой.

Система осуществляет обнаружение, детальный анализ и предупреждение о кибератаках на общекорпоративные сервисы, оборудование IoT и IIoT. Основные функции:

- сканирование сети ИТ-инфраструктуры и определения зарегистрированных в ней устройств и сетевых сервисов
- развертывание сети ловушек, имитирующие общекорпоративные сервисы, оборудование IoT и IIoT (ICS/SCADA)
- развертывание «песочниц» на базе ОС Windows/Linux/Android с различными архитектурами
- сбор индикаторов сетевых атак
- перенаправление внешних соединений из сети ловушек в «песочницы»
- сбор поведения злоумышленника в интерактивных средах
- сбор образцов вредоносного программного обеспечения и анализ их поведения в «песочницах» с различными операционными системами
- оповещение об атаках на ловушки и сетевые сервисы по электронной почте и в системы мониторинга по протоколу SYSLOG

ТИПЫ ЛОВУШЕК

Наименование типа	Описание
Низкоинтерактивные	Имитируют сетевые протоколы взаимодействия устройства.
Высокоинтерактивные	Имитируют операционную систему устройства, сервисы и протоколов сетевого взаимодействия.

ВИДЫ ЛОВУШЕК

Ловушки могут имитировать любые объекты ИТ-инфраструктуры

- WEB-сервер
- FTP-сервер
- почтовый сервер
- рабочее место
- межсетевой экран
- операционную систему
- маршрутизатор
- коммутатор
- сеть приманка
- IoT/IIoT
- медицинское оборудование

Для обеспечения максимального охвата поддерживаемого оборудования организации в ложной инфраструктуре ловушки поддерживают следующие архитектуры процессоров:

- Intel x86-based
- AMD64
- ARM

- MIPS
- Power Systems
- Эльбрус

Все ловушки осуществляют сбор сетевой телеметрии, дополнительных данных в соответствии с имитируемым протоколом:

- IP-адрес источника
- порт источника
- порт получателя
- протокол
- информацию по email (адрес отправителя, адреса получателей, заголовок и текст письма, вложения)
- информацию по HTTP/HTTPS соединениям (тип, адрес, user-agent, данные запроса)
- информацию по запросам к СУБД (текст запроса, ответ на запрос)
- учетные данные при наличии в соответствующем протоколе

Ловушки также осуществляют сбор собственного сетевого трафика для последующего анализа перехватываемых сетевых атак.

Перечень протоколов, по которым осуществляется сбор учетных данных:

Наименование сервера	**Предположительный порт**
SMTP	25
POP3	110
POP3S	995
IMAP	143
IMAPS	993
HTTP	80
HTTPS	443

Наименование сервера	Предположительный порт
SSH	22
Telnet	23
RDP	3389
VNC	5900
FTP	21
TFtp	69
SMB	139
MySQL	3306
PostgreSQL	5432
MongoDB	27017
Socks5	1080
SIP	5060

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

Развертывание LOKI на 1 сервере (10 ловушек)

Параметры	Минимальные требования
Количество ядер процессора	6
Оперативная память	15 GB
Диск	SSD 1 TB x 2 (RAID1)
Сеть	10/100/1000 Мбит/с (2 шт.)

Развертывание LOKI на нескольких серверах

Параметры	Минимальные требования
Сервер	
Количество ядер процессора	4
Оперативная память	12 GB
Диск	SSD 256 GB x 2 (RAID1)
Сеть	10/100/1000 Мбит/с (2 шт.)
Сенсор (10 ловушек)	
Количество ядер процессора	2
Оперативная память	3 GB
Диск	SSD 100 GB x 2 (RAID1)
Сеть	10/100/1000 Мбит/с (2 шт.)

Варианты инфраструктуры развертывания

Развертывание системы LOKI можно осуществлять, как на виртуальных машинах, так и физических машинах.

СХЕМА РАБОТЫ

Схема интеграции ловушек в ИТ-инфраструктуру организации.