AVSOFT ATHENA

ОПИСАНИЕ ПРОБЛЕМЫ

Целенаправленные кибератаки быстро совершенствуются уже более 14 лет. Одним из распространенных способов их осуществления является использование вредоносного ПО нулевого дня, которое не обнаруживается антивирусными средствами.

РЕШЕНИЕ

Система выявления и анализа вредоносного программного обеспечения ATHENA защищает организации от целенаправленных кибератак и угроз нулевого дня, комбинируя два многоуровневых вида анализа: статический и динамический в сочетании с технологией машинного обучения. Каждый метод анализа включают в себя несколько направлений проверки.

Статическое направление проверки включает в себя:

- проверку файлов в более 20 различных локальных антивирусах
- детальный анализ структуры и содержимого файлов
- проверку во внешних аналитических ресурсах и репутационных базах
- анализ определенных типов файлов в соответствующих нейронных сетях
- распаковку архивов, включая многотомные и защищенные паролем

Динамическое направление проверки дополняет статическое направление. т.к. антивирусные базы данных не всегда содержат сигнатуры нового вируса. Оно включает в себя исследование поведения ПО в изолированных виртуальных и физических средах («песочницах»), имитирующих компьютер или мобильное устройство. Внутри «песочниц» установлен контент и автоматическая имитация работы пользователя. Вердикт динамического анализа выносится на основании зафиксированных подозрительных или вредоносных действий исследуемого файла в имитационной среде – «песочнице».

В операционной системе «песочниц» присутствует пользовательский контент и выполняется имитация работы пользователя. Они могут быть кастомизированы под контент и состав ПО реального предприятия.

В динамическом анализе осуществляется также фиксация потребляемых ресурсов, что позволяет выявить ПО, расходующее ресурсы ОС для майнинга. После сбора событий о поведении ПО внутри «песочницы» происходит их анализ и определение вердикта.

После определение вердиктов обоими видами анализа формируется общий вердикт.

Система ATHENA имеет широкую линейку поддерживаемых операционных систем в динамическом анализе:

- MS Windows XP - 10
- Windows Server (2003 - 2019)
- ОС на базе ядра Linux (Astra Linux, CentOS, Debian, Fedora, openSUSE, RedHat, Ubuntu, РЕД ОС, др.)
- Android (5-9)

Система ATHENA способна принимать любые типы файлов на проверку:

- исполняемые;
- офисные;
- мобильные приложения;
- архивы, включая многотомные и закрытые паролем;
- скрипты и др.

В системе ATHENA реализован прием файлов на анализ из следующих источников:

- веб-трафик;
- почтовый трафик;
- межсетевые экраны (ViPNet xFirewall, EtherSensor, UserGate, др.);
- мобильные устройства;
- съемные носители;
- ATHENA_Bot (Telegram-бот, WhatsApp-бот);
- ручная загрузка;
- API;
- ICAP.

РЕЖИМЫ РАБОТЫ

Система ATHENA имеет два режима работы: автоматический и экспертный.

Автоматический режим заключается в перехвате и проверке файлов из интернет-трафика, почтовых вложений, межсетевых экранов, мобильных устройств и API/ICAP.

Экспертный режим позволяет пользователю детально настраивать динамическую среду по интересующим его направлениям исследования, включая:

- загрузку вручную любых файлов в систему, в т.ч. посредством ATHENA_Bot;
- выбор файла и «песочницы»;
- гибкую настройку параметров исследования и запуск файла;
- наблюдение за исследованием;
- участие в имитации работы пользователя в «песочнице».

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

ATHENA	
Оборудование	
Модель процессора	Intel(R) Xeon(R) CPU E5-2603 v4 @1.7GHz
Количество процессоров	2
Количество ядер процессора	6
Количество потоков на ядро	2
Оперативная память	128 ГБ
Диск	SSD 500 ГБ x2 RAID1 HDD 500 ГБ x2 RAID1 SAS 1 TB x 8 RAID10
Сеть	10/100/1000 Мбит/с (2 шт.)
Замеры	
Файлы *	2 000
Формат	
exe	100 файлов
pdf	850 файлов
office	1000 файлов
apk/zip/rar/7z	50 файлов
Количество одновременно запущенных виртуальных машин	10
Время	1 час 00 минут

* все файлы прошли проверку статическим и динамическим анализом.

ОСОБЕННОСТИ

Охват множества источников поступления файлов, анализ любого типа файла, а также гибкость подключения/отключения модулей делают комплекс универсальным для организации любого масштаба и структуры.

Компании могут использовать систему ATHENA как экспертную, что позволит им выполнять исследования, поднимать компетенции своих специалистов и создавать аналитические правила выявления вредоносного ПО.

Сочетание двух многоуровневых видов анализа обеспечивает высокую степень детектирования вредоносного ПО.