ATHENA

Система зищиты от
целенаправленных атак

Техническое описание

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:

- Возможность бесшовной интеграции с внешними антивирусными движками
- 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 10 - 7
· Windows Server (2008 R2 - 2019)
· Linux:
· Astra Linux
· Debian 9.8 (Stretch)
· openSUSE Leap 15
· CentOS 7.6.1810
· Ubuntu 18.10
· 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.

Режим работы

Система ATHENA имеет два режима работы: автоматический и экспертный.

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

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

- Загрузку вручную любых файлов в систему, в т.ч. посредством telegram-bot
- Выбор файла и «песочницы»
- Настройку параметров исследования и запуск файла
- Наблюдение за исследованием
- Участие в имитации работы пользователя в «песочнице»

Матрица производительности

Файлы до 10 МБ

Статика

Время	1 час			
Хранение данных	Безопасные удаляются			

*Срок хранения файлов 3 месяца.

Кол-во файлов	6 000	60 000	120 000	260 000
CPU	16 ядер	160 ядер	320 ядер	640 ядер
RAM	128 GB	265 GB	512 GB	1 TB
HDD	10 TB	100 TB	200 TB	900 TB
SSD	4 TB	40 TB	80 TB	264 TB

Статика + Динамика

Время	1 час			
Хранение данных	Только вредоносные			

*Срок хранения файлов 3 месяца.

Кол-во файлов	6 000	60 000	120 000	260 000
CPU	80 ядер	800 ядер	1 600 ядер	3 200 ядер
RAM	300 GB	2 TB	4 TB	8 TB
HDD	20 TB	200 TB	400 TB	900 TB
SSD	6 TB	60 TB	120 TB	264 TB

Техническая спецификация

Оборудование

Модель процессора	Intel(R) Xeon(R) CPU E5-2603 v4 @1.7GHz
Количество процессоров	2
Количество ядер процессоров	6
Количество потоков на ядро	2
Оперативная память	128 ГБ
Диск	SSD 500 ГБ x2 RAID1 HDD 500 ГБ x2 RAID1 SAS 1 ТВ x 8 RAID10
Сеть	10/100/1000 Мбит/с (2 шт.)