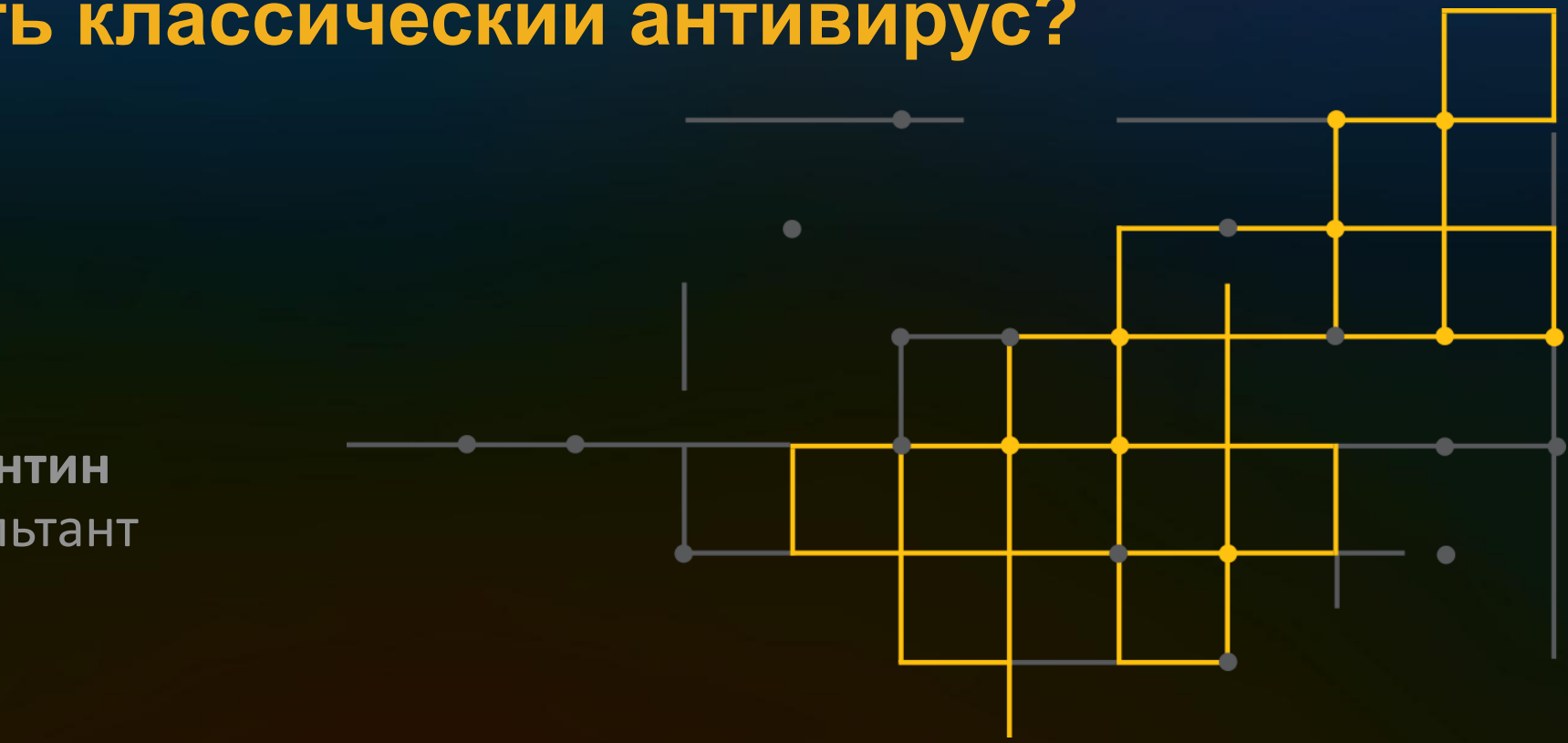
Чем заменить классический антивирус?



ЧЁЛУШКИН Константин
технический консультант
Symantec в России

Когда “умер” классический антивирус?

Брайан Дай, тогда старший вице-президент Symantec, в первых числах **мая 2014 года** в интервью WSJ сообщил, что “антивирус умер”

Некоторые СМИ тогда позволили себе интерпретировать его слова так, будто Symantec выходит из "антивирусного бизнеса"

Однако, мысль Брайна заключалась в том, что эффективность классического антивируса очень низка, что он может детектировать лишь 45% атак и поэтому **ОДНОГО антивируса недостаточно для защиты от современных угроз**

Цепи атаки современных угроз

ВТОРЖЕНИЕ

- Интернет
- Эл. почта
- Доверен. приложения
- Устройства

Множество векторов атаки

ИНФЕКЦИЯ

- Файлы
- Макросы
- Мониторинг Памяти
- Мониторинг Сети
- Шифровальщики
- Руткиты

Разнообразные инструменты

ПОРАЖЕНИЕ

- Скрытие от обнаружения
- Связь с центром управления
- Распространение
- Несанкцион. запуск

ВАКЦИНА

- Карантин файлов и конечных точек
- Удаление и восстановление
- Повышение уровня защиты

Быстрое заражение

Необходимы технологии защиты конечных точек по всей цепи атаки

Что такое классический антивирус?

Классический антивирус **работает только с файлами** и детектирует наличие вируса путём анализа содержимого файла, сравнивая его с базой вирусных сигнатур

Такой метод детектирования позволяет точно идентифицировать угрозу, определить ее тип и среагировать на основании типа обнаруженной угрозы: игнорировать, уведомить, переместить в карантин, удалить, очистить вирус, если это доступно.

ДОСТАТОЧНО ЛИ ЭТОГО ДЛЯ БОРЬБЫ С СОВРЕМЕННЫМИ УГРОЗАМИ?

Основные технологические проблемы классического антивируса

Необходимость наличия достаточного количества **вычислительных ресурсов** для анализа контента файлов, что не позволяет использовать эту технологию в режиме реального времени на платежных терминалах и банкоматах, где ресурсов очень мало, а также на высоконагруженных серверах, где нет свободных ресурсов

Необходимость регулярного **обновления базы сигнатур** на агенте, которая становится все больше с каждым днем. Обновление базы на агенте затруднительно реализовать для ПК со слабым каналом связи, а также для VDI, когда при каждом обновлении огромной базы сигнатур на множестве виртуальных машин необходимо выполнить большое число операций ввода-вывода

Почему эффективность ОДНОГО классического антивируса низка?

Полиморфное вредоносное ПО быстро изменяет свой контент

Упаковщики позволяют злоумышленникам быстро создавать новые уникальные экземпляры вредоносного ПО

Реагирование на новое вредоносное ПО затруднительно, так как всё, что есть в Вашем распоряжении при классическом подходе – это база вирусных сигнатур и в нее необходимо как-то добавить новую сигнатуру

Нужно ли заменять классический антивирус?

Лучший подход – не замена классического антивируса, а дополнение его новыми технологиями защиты и создание таким образом **эшелонированной защиты**

Новые технологии позволят достичь наилучшего результата, как с точки зрения **оптимальной производительности** и низкого процента ложных срабатываний, так и с точки зрения **эффективности защиты** и высокого процента детектирования

В некоторых случаях, таких как банкоматы и высоконагруженные сервера, технология классического антивируса не применима и требуются другие технологии, однако это не означает, что она не эффективна там, где ее можно применить и что от нее стоит вовсе отказаться

Классы новых технологий

Технологии защиты, которые повышают производительность конечной точки и эффективность защиты

Технологии обнаружения и реагирования (EDR), которые позволяют обнаружить скрытые и направленные атаки (APT) и сократить время реагирования и исправления защиты

Новые технологии защиты

Сетевой фильтр и **управление устройствами**, чтобы ограничить доступные сетевые протоколы и сузить возможности вторжения

Анализ содержимого сетевых пакетов по сигнатурам (IPS), чтобы предотвратить использование какой-либо известной уязвимости сетевого приложения или протокола (например, Heartbleed, EternalBlue), а также блокировать трафик нежелательного типа (например, P2P). Очень эффективная технология, помогла предотвратить WannaCry

Анализ репутации файла, что требует существенно меньшего количества вычислительных ресурсов по сравнению с антивирусной проверкой, благодаря чему повышается производительность системы. Кроме этого, проверка репутации позволяет выявить подозрительные файлы и применить к ним дополнительные средства контроля, такие как мониторинг поведения

Новые технологии защиты (продолжение)

Анализ статических атрибутов файла на основе данных машинного обучения, что позволяет выявить потенциально опасное ПО, требует мало вычислительных ресурсов и не требует большой базы сигнатур на агенте

Эмуляция запуска процесса, что позволяет повысить эффективность детектирования упакованного вредоносного ПО

Защита от эксплойтов в памяти. Блокировка использования известных методов эксплуатации уязвимостей, такие как SEHOP, Java Security Manager, HeapSpray, ForceDEP и др.

Мониторинг поведения подозрительных процессов, чтобы на основании их действий детектировать атаку и блокировать её

Новые технологии защиты (продолжение)

Блокировка запуска процессов по белому или черному списку

Блокировка изменения конфигурации средств защиты

Контроль процессов на уровне доступа к файлам, к реестру, к процессам, к сети. Например, блокировка создания исполняемых файлов, блокировка запуска системных служб с сетевых томов, блокировка запуска процессов из папки «recycle.bin» и т.п.

Харденинг системы: запуск системных и пользовательских процессов таким образом, чтобы они могли действовать только в рамках необходимых им полномочий

Эшелонированная защита по всем цепям атаки



	ВТОРЖЕНИЕ	ЗАРАЖЕНИЕ	ПОРАЖЕНИЕ	ЭКСФИЛЬТРАЦИЯ
Анализ по атрибутам и поведению		Анализ репутации Анализ статических атрибутов Мониторинг поведения		
Контроль сети	Сетевой IPS Сетевой экран		Сетевой IPS Сетевой экран	
Контроль процессов	Белые и черные списки Контроль приложений и устройств	Защита от эксплойтов в памяти		
Анализ по сигнатурам		Антивирус Эмулятор		

Зачем нужны технологии обнаружения и реагирования?

Опыт последних лет показывает, что недостаточно только технологий защиты, так как в случае направленных атак используется либо уникальное вредоносное ПО либо вообще не используется вредоносное ПО

Детектирование направленных атак может занимать недели и месяцы, а после детектирования уходят дни и недели, чтобы **среагировать** и внести исправления в конфигурацию средств защиты

Технологии обнаружения

«Ловушки» для вредоносного ПО, имитация наличия антивирусного ПО или файлов с конфиденциальной информацией и детектирование попыток обращения к ним

Создание базы данных событий активности на конечных точках, которые могут быть полезны при расследовании инцидентов (хэш файла, изменения ключей реестра, установка сетевых подключений, запуск и остановка процессов, создание исполняемых файлов, запуск скриптов powershell и др.)

Использование «песочниц» для анализа потенциально вредоносного ПО и поиск индикаторов компрометации (IoC) в базе событий активности и непосредственно на конечных точках

Корреляция событий детектирования вредоносной активности, создание и управление инцидентами

Технологии реагирования

Контроль конфигурации системы и приложений и автоматическое реагирование на нарушения политик безопасности

Локальная база репутации

Блокировка запуска процессов по черному списку

Контроль действий процессов

Удаление вредоносного ПО

Изоляция атакованных или зараженных конечных точек

Спасибо!

ЧЁЛУШКИН Константин

konstantin_chelushkin@Symantec.com