EDR – обнаружение и реагирование

Роман Ванерке, *технический директор АО "ДиалогНаука"*

Целенаправленные атаки злоумышленников продолжают наносить финансовый и репутационный ущерб, несмотря на то, что многие из компаний, подвергшихся нападению, уже использовали у себя средства защиты, а также соответствовали тем или иным стандартам безопасности. В настоящей статье будет рассмотрен один из относительно новых типов средств защиты информации – EDR (Endpoint Detection and Response), который предназначен для более эффективной защиты от целенаправленных атак и для реагирования на выявляемые инциденты информационной безопасности.

EDR дополняет установленную EPP, расширяя возможности по защите конечных устройств. При этом решения класса EPP обеспечивают защиту от известных типов атак, а EDR – другие этапы жизненного цикла инцидента: детектирование, реагирование и расследование, а часто и функции по анализу эффективности работы EPP для выявления слабых мест в защите. В настоящее время наблюдается сближение этих систем – в EDR-платформах появляется функционал EPP и наоборот.

Защита не работает?

Для того чтобы понять, почему атаки все еще успешны, разберем несколько примеров. Так, Symantec опубликовала отчет об атаках, связанных с деятельностью хакерской группировки Thrip. Symantec проводит исследование группировки Thrip с 2013 г. и подробно изучила ее действия. Характерной особенностью группы является использование для взлома легитимного ПО. В частности, для запуска удаленных процессов хакерами были использованы легитимные утилиты PsExec и LogMeIn, а для воровства файлов – легальный FTP-клиент WinSCP. Использование легитимных утилит позволяет хакерам ускользать от всевидящего ока антивирусов, т.к. легитимные программы не могут помечаться как вредоносные, даже если их используют хакеры для своих целей. Контроль приложений здесь тоже не помогает – эти утилиты, как правило, разрешены для использования в организациях.

Впрочем, хакеры группировки Thrip используют для повышения полномочий утилиту Mimikatz, обычно определяемую как вредоносный код, что может позволить выявить их вредоносную активность. Однако злоумышленники обходят и эту защиту, изменяя файл таким образом, чтобы сигнатуры антивируса не срабатывали. Нужно также иметь в виду, что вредонос присутствует в системе очень короткое время – после получения административных полномочий хакеры удаляют его и опять пользуются только легальным ПО. Антивирусы, обновившие свои сигнатуры, не всегда могут обнаружить подобные вредоносные коды, что и позволяет хакерам долго скрывать свое присутствие в системе. Аналогичным свойством обладают и бесфайловые вредоносы – они располагаются только в памяти и при включении компьютера удаляются, и антивирусам, которые сканируют только файловую систему, они также не видны.

Если же рассмотреть материалы комиссии Роберта Мюллера по взлому сетей демократического комитета по выборам в Конгресс США (DCCC) и комитета демократической партии (DNC), то и в этом случае классические антивирусы, рассчитанные на обнаружение массовых вредоносных программ, также оказались бессильны. Как следует из пресс-релиза окружного суда штата Колумбия, первоначальное проникновение было выполнено с помощью фишингового перехвата учетных данных одного из сотрудников штаба, который нарушил политику безопасности и использовал в рабочей переписке публичные почтовые ресурсы. Далее по контрагентам электронной почты хакерами был разослан специально разработанный вредонос, который получил наименование X-Agent, и с помощью него и были произведены утечки конфиденциальных данных. Понятно, что специализированный вредонос детектироваться массовыми антивирусами не будет. А даже если и будет, то хакеры могут быстро обновить его коды, чтобы вывести свой код из-под подозрений антивируса.

EDR vs EPP

Из приведенных выше примеров следует, что антивирусные платформы, которые получили наименование EPP (Endpoint Protection Platform – платформы для защиты конечных устройств), не могут обнаружить нестандартную вредоносную активность, для которой отсутствуют сигнатуры. В качестве примера такой активности можно привести:

- поведение пользователей и программ, если к их учетным данным получили доступ злоумышленники;
- поведение легальных пользователей, обманутых с помощью различных методов социальной инженерии;
- поведение ранее неизвестных вредоносных программ, код которых не был ранее доступен в антивирусной лаборатории и для которых отсутствуют сигнатуры;
- поведение бесфайловых вредоносов, которые не сохраняют своего тела в файловой системе.

Для того чтобы дополнить функциональные возможности антивирусов, появился целый класс решений, которые позволяют обобщить сведения о вредоносной активности на всем предприятии, обнаружить подозрительные действия, выявить подверженные атаке устройства, а также локализовать вредоносную активность. Такие решения позволяют также провести ретроспективное расследование проникновения и выявить причины возникновения инцидента, которые необходимо устранить для предотвращения подобных атак в будущем. Этот класс средств защиты получил наименование EDR (Endpoint Detection

Хакеры группировки Thrip используют для повышения полномочий утилиту Mimikatz, обычно определяемую как вредоносный код, что может позволить выявить их вредоносную активность. Однако злоумышленники обходят и эту защиту, изменяя файл таким образом, чтобы сигнатуры антивируса не срабатывали. Нужно также иметь в виду, что вредонос присутствует в системе очень короткое время – после получения административных полномочий хакеры удаляют его и опять пользуются только легальным ПО. Антивирусы, обновившие свои сигнатуры, не всегда могут обнаружить подобные вредоносные коды, что и позволяет хакерам долго скрывать свое присутствие в системе. Аналогичным свойством обладают и бесфайловые вредоносы – они располагаются только в памяти и при включении компьютера удаляются, и антивирусам, которые сканируют только файловую систему, они также не видны.

and Response – обнаружение атак на конечные устройства и реагирование на них). Подобные решения с помощью специального агента, установленного на конечные устройства, собирают информацию об активности пользователей и программ, анализируют ее для обнаружения признаков компрометации (IoC), помогают выявлять и локализовать скомпрометированные устройства, провести расследование и усилить защиту.

Таким образом, EDR по сути дополняет установленную EPP, расширяя возможности по защите конечных устройств. При этом решения класса EPP обеспечивают защиту от известных типов атак, а EDR – другие этапы жизненного цикла инцидента: детектирование, реагирование и расследование, а часто и функции по анализу эффективности работы EPP для выявления слабых мест в защите. В настоящее время наблюдается сближение этих систем – в EDR-платформах появляется функционал EPP и наоборот.

EDR и все, все, все...

С точки зрения корпоративной системы защиты EDR является дополнительным элементом безопасности, который позволяет выявлять действия злоумышленника, когда он уже смог преодолеть все имеющиеся средства защиты. Кроме того, EDR позволяет с помощью выявления аномалий обнаружить подозрительные файлы и направить их на исследование в "песочницу" – виртуальную среду, используемую антивирусными аналитиками для выявления вредоносной активности кодов и приложений.

Именно поэтому сейчас производители антивирусных решений с одной стороны и разработчики сетевых средств защиты с другой стараются встроить функции EDR в свои продукты. В качестве примера рассмотрим два решения класса EDR: FireEye HX и Kaspersky EDR.

Компания FireEye, специализирующаяся на разработке "песочниц", выпустила EDR-решение FireEye Endpoint Security (серия получила наименование HX), которое включает в себя в том числе следующие технологии:

- обнаружение и блокирование эксплойтов без использования сигнатур (защита от угроз нулевого дня);
- расширение киберразведки FireEye на конечные устройства для всеобъемлющей защиты от современных угроз;
- получение результатов анализа в "песочницах" FireEye (индикаторов) с последующей их проверкой на конечных узлах;
- Triage Viewer и Audit Viewer для отслеживания и анализа индикаторов угроз (детектирование);
- Enterprise Search для быстрого поиска на всех конечных узлах индикаторов и проведения расследования с целью дальнейшего устранения последствий (расследование);
- Forensic Data Acquisition позволяет выполнить сбор данных с устройства для тщательной проверки и анализа (анализ);
- изолирование угроз и скомпрометированных устройств (реагирование).

Продукт интегрирован с другими разработками FireEye, что позволяет в случае обнаружения атак на конкретные устройства оперативно локализовать нападение и не дать вредоносам продолжить свою деятельность в системе. Кроме этого в состав агента FireEye входит дополнительный антивирус, который выполняет дополнительную проверку подозрительных объектов.

В 2018 г. компания "Лаборатория Касперского" выпустила свой продукт под названием Kaspersky EDR, который позволяет решать следующие задачи:

- улучшить контроль рабочих мест и оптимизировать обнаружение угроз с помощью передовых технологий, включая машинное обучение, "песочницу", аналитику угроз и проверку на индикаторы компрометации (IoC) (детектирование);
- автоматизировать выявление угроз и реагирование на них во избежание потерь и простоев (реагирование);
- создать постоянно совершенствующуюся систему защиты на базе простого в использовании корпоративного решения по нейтрализации и расследованию угроз (расследование);
- наладить эффективные процессы обнаружения угроз, управления инцидентами и реагирования на них (процесс модернизации защиты).

Особенностью решения Kaspersky EDR является его интеграция с другими продуктами "Лаборатории Касперского" – антивирусом и Kaspersky KATA.

Таким образом, сейчас рынок EDR – это поле для конкуренции между производителями антивирусов, которые хотят стать полноценными корпоративными средствами защиты от целенаправленных атак, и разработчиками "песочниц", которые выходят на рынок защиты конечных устройств.

Заключение

Рынок EDR сейчас только начинает формироваться и имеет хорошие перспективы для дальнейшего развития. Тем не менее производителей данных инструментов уже достаточно как минимум для обзоров аналитических компаний. Так, Gartner, Forrester и IDC уже выпустили несколько отчетов по данному рынку и сравнили его перспективность с устоявшимся рынком EPP. Первый опыт внедрения решений класса EDR продемонстрировал их высокую эффективность и способность реально повысить уровень защиты, в том числе и от целенаправленных атак злоумышленников. ●

Сейчас рынок EDR – это поле для конкуренции между производителями антивирусов, которые хотят стать полноценными корпоративными средствами защиты от целенаправленных атак, и разработчиками "песочниц", которые выходят на рынок защиты конечных устройств.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru