McAfee Advanced Threat Defense

Обнаружение сложных вредоносных программ

McAfee® Advanced Threat Defense дает организациям возможность выявлять сложные трудноуловимые вредоносные программы и немедленно преобразовывать информацию об угрозах в неотложные меры реагирования и обеспечения безопасности. В отличие от традиционных изолированных сред («песочниц») в него включены дополнительные средства проверки, расширяющие возможности обнаружения угроз и выявления методов обхода защиты. Тесная взаимосвязь решений для защиты сетей, конечных точек и проведения расследований и т. д. обеспечивает мгновенный обмен информацией об угрозах в масштабах всей среды. Это позволяет укрепить защиту и оптимизировать процессы расследования инцидентов. Гибкие варианты развертывания позволяют интегрировать данный продукт в любую сеть.

Наша технология преобразила процесс обнаружения угроз, объединив функции анализа сложного вредоносного ПО с существующими средствами защиты, расположенными в разных точках сети (от периферии до конечных точек), и обеспечив обмен информацией об угрозах в рамках всей ИТ-среды. Благодаря обмену информацией об угрозах в масштабах всей экосистемы интегрированные защитные решения взаимодействуют между собой, позволяя моментально блокировать доступ удаленного центра управления к взломанным системам, помещать их в карантин, блокировать другие экземпляры таких же или похожих угроз, оценивать размер возможного ущерба и принимать необходимые меры.

McAfee Advanced Threat Defense: обнаружение угроз повышенной сложности

Благодаря использованию новаторского многоуровневого подхода решение McAfee Advanced Threat Defense способно обнаруживать современные скрытые вредоносные программы «нулевого дня». Решение совмещает в себе автоматические аналитические модули, такие как средства анализа антивирусных сигнатур, репутации и эмуляции в режиме реального времени с функциями динамического анализа («в песочнице»), что позволяет анализировать реальное поведение. Затем проводится глубокий статический анализ кода, позволяющий проверить все атрибуты

Основные отличительные качества McAfee Advanced Threat Defense

Широкие возможности интеграции решения

- Интеграция с другими решениями McAfee, шлюзами для электронной почты сторонних поставщиков и прочими продуктами, поддерживающими открытые стандарты
- Сокращение разрыва между обнаружением атаки и ее сдерживанием и обеспечением защиты в масштабе всей организации
- Оптимизация рабочих процессов, позволяющая быстрее реагировать на угрозы и быстрее их устранять
- Автоматизация процессов

Подписаться

файлов и наборы инструкций с целью выявления его фактических намерений и используемых в нем способов уклонения. Такой анализ позволяет оценить степень сходства кода с известными семействами вредоносного ПО. В завершение McAfee Advanced Threat Defense проводит проверку на наличие вредоносных признаков, выявленных с помощью методов машинного обучения на базе глубокой нейронной сети. В комплексе мы получаем самую надежную из представленных на рынке систем защиты от сложных вредоносных программ, позволяющую найти удачный баланс между необходимостью детальной проверки и быстродействием среды. Использование автоматических методов анализа, таких как сигнатуры и эмуляция в режиме реального времени, упрощает обнаружение известных вредоносных программ и положительно сказывается на быстродействии; а глубокий статический анализ кода и информация, полученная с помощью методов машинного обучения, в дополнение к технологии «песочницы» позволяют обеспечить защиту от более широкого спектра чрезвычайно замаскированных, трудноуловимых угроз. Для обнаружения вредоносных признаков, не проявляющих себя в динамической среде, используется распаковка, глубокий статический анализ кода и сбор информации методами машинного обучения.

Упаковка кода дает разработчикам вредоносных программ возможность изменять состав кода или скрывать его с целью избежания обнаружения. Большинство продуктов не может правильно распаковывать весь исходный исполняемый код, подлежащий анализу. В McAfee Advanced Threat Defense включены мощные функции распаковки, позволяющие «распутать» код и добраться до исходного исполняемого кода. Это дает возможность с помощью глубокого статического анализа кода искать аномалии за пределами высокоуровневых файловых атрибутов, анализируя атрибуты и наборы инструкций с целью выявления его намерений.

Глубокий статический анализ кода, методы машинного обучения и динамический анализ файлов, используемые в совокупности, позволяют провести полную и подробную оценку ПО, подозреваемого во вредоносности. Уникальные результаты анализа помогают формировать сводные отчеты, которые дают полное представление о текущей ситуации и позволяют приоритизировать действия, а кроме того, обеспечивают предназначенные для аналитиков более подробные отчеты, содержащие данные о вредоносных программах.

Усиление защиты

Благодаря тесной интеграции между McAfee Advanced Threat Defense и защитными устройствами, расположенными в разных точках сети (от периферии до конечных точек), интегрированные защитные устройства могут принимать меры реагирования сразу, как только McAfee Advanced Threat Defense классифицирует тот или иной файл как вредоносный. Такая тесная автоматическая интеграция средств обнаружения и защиты имеет ключевое значение.

Эффективные функции обнаружения угроз

- Сочетание методов глубокого статического анализа кода, функций динамического анализа файлов и технологии машинного обучения, позволяющее с большей точностью обнаруживать угрозы, используя уникальные аналитические данные
- Передовые функции обеспечивают поддержку центра управления безопасностью и предоставляют возможность расследовать инциденты

Гибкое централизованное развертывание

- Сокращение затрат благодаря централизованному развертыванию с поддержкой множества протоколов
- Гибкие варианты развертывания позволяют интегрировать данный продукт в любую сеть

McAfee Advanced Threat Defense интегрируется разными способами: напрямую (в случае некоторых защитных решений), посредством McAfee Threat Intelligence Exchange и посредством McAfee Advanced Threat Defense Email Connector.

Прямая интеграция дает защитным решениям возможность принимать необходимые меры в отношении файлов, проанализированных с помощью McAfee Advanced Threat Defense. Возможность немедленно встроить информацию об угрозах в существующие процессы применения политик позволяет не допускать в сеть другие экземпляры таких же или похожих файлов.

Результаты анализа, проведенного McAfee Advanced Threat Defense, отображаются в журналах интегрированных продуктов и на их панелях мониторинга, как если бы весь анализ был выполнен самими этими продуктами. Это оптимизирует рабочие процессы и дает администраторам возможность эффективно управлять оповещениями, работая через один-единственный интерфейс.

Интеграция с McAfee Threat Intelligence Exchange дает дополнительным защитным продуктам (включая McAfee Endpoint Protection) возможность использовать функции McAfee Advanced Threat Defense. Таким образом, широкий спектр интегрированных защитных решений получает доступ к результатам анализа и признакам взлома. Когда McAfee Advanced Threat Defense признает файл вредоносным, McAfee Threat Intelligence Exchange передает информацию об угрозах всем имеющимся в организации интегрированным средствам защиты путем обновления данных о репутации.

Конечные точки, подключенные к McAfee Threat Intelligence Exchange, получают возможность заблокировать первоначальную установку вредоносных программ и обеспечить упреждающую защиту на случай, если они столкнутся с этим файлом в будущем. А шлюзы, подключенные к McAfee Threat Intelligence Exchange, не допустят этот файл внутрь организации. Кроме того, подключенные к McAfee Threat Intelligence Exchange конечные точки получают результаты анализа файлов даже будучи отключенными от сети. Это позволяет избавиться от белых пятен, возникающих в результате внеполосной доставки полезной нагрузки.

Соединительный модуль McAfee Advanced Threat Defense Email Connector дает McAfee Advanced Threat Defense возможность получать от почтового шлюза подлежащие анализу вложения из сообщений электронной почты. McAfee Advanced Threat Defense анализирует файлы во вложениях и сообщает свое заключение всем активным почтовым шлюзам внутри заголовка пересылаемого сообщения. Получив заключение, почтовый шлюз может принять меры в соответствии с политиками безопасности, например, удалить соответствующее вложение или поместить его в карантин, предотвращая тем самым распространение вредоносного ПО и заражение внутренней сети организации. Автономный режим позволяет доставлять электронные письма с вложениями конечному пользователю, одновременно выполняя их сканирование с помощью McAfee Advanced Threat

Интегрированные решения

- McAfee® Active Response
- McAfee® Advanced Threat Defense Email Connector
- McAfee® Enterprise Security Manager
- McAfee® ePolicy Orchestrator®
- McAfee® Network Security Platform
- McAfee® Threat Intelligence Exchange
  - McAfee® Application Control
  - McAfee® Endpoint Protection
  - McAfee® Security for Email Servers
  - McAfee® Server Security
- McAfee® Web Gateway
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

Defense. Почтовым шлюзам не требуется ждать заключения по анализу вложения. Администраторы просматривают результаты сканирования в McAfee Advanced Threat Defense или McAfee Threat Intelligence Exchange. Для оптимизации защиты почтового сервера McAfee Advanced Threat Defense интегрируется с McAfee Security for Email Servers с помощью службы McAfee Threat Intelligence Exchange.

Оптимизация и автоматизация расследований благодаря обмену информацией об угрозах

Для расследования и устранения последствий атак организациям необходимо иметь комплексное представление о происходящем, подкрепленное информацией об угрозах и позволяющее принимать более обоснованные решения и адекватно реагировать на угрозы. McAfee Advanced Threat Defense предоставляет подробную информацию об угрозах, доступную в масштабе всей вашей среды, что позволяет оптимизировать и автоматизировать процессы расследования. Поддержка уровня обмена данными Data Exchange Layer (DXL) и интерфейсов прикладного программирования (API), реализованных при помощи REST (Representational State Transfer) обеспечивает возможность интеграции с другими продуктами и широко используемыми стандартами обмена информацией об угрозах, такими как Structured Threat Information eXpression (STIX)/ Trusted Automated eXchange of Indicator Information (TAXII), что дает организациям более широкие возможности при создании, поддержке и расширении единой экосистемы безопасности.

Сопоставляя получаемые из McAfee Advanced Threat Defense и других систем безопасности подробные данные о репутации файлов и событиях выполнения файлов, McAfee Enterprise Security Manager в рамках экосистемы McAfee генерирует расширенное представление данных за текущий и прошлые периоды, дающее администраторам возможность лучше ориентироваться в угрозах безопасности, приоритизировать риски и контролировать ситуацию в режиме реального времени. Информация о признаках взлома, получаемая из McAfee Advanced Threat Defense, дает McAfee Enterprise Security Manager возможность искать признаки наличия таких артефактов во всех сохраненных им данных о сети и системах за период до шести месяцев. Это позволяет выявлять системы, ранее обменивавшиеся данными с только что выявленными источниками вредоносного ПО. Тесная интеграция с McAfee Endpoint Protection, McAfee Threat Intelligence Exchange и McAfee Active Response позволяет оптимизировать скорость реагирования на инциденты и эффективность мер по обеспечению безопасности благодаря наличию информации о происходящем и возможности выполнять такие действия по упреждающему снижению риска, как создание новых конфигураций, внедрение новых политик, удаление файлов и развертывание обновлений программного обеспечения. Автоматическое выявление зараженных конечных точек по всей сети организации с помощью McAfee Active Response и включение их в отчеты McAfee Advanced Threat Defense позволяют быстро принимать меры на основе фактической информации.

Просмотр этих подробных отчетов в единой рабочей среде McAfee Active Response увеличивает эффективность работы аналитиков.

Расширенные возможности проведения расследований

McAfee Advanced Threat Defense включает в себя целый ряд дополнительных функций:

- **Настраиваемая поддержка операционных систем и приложений.** Подстройка образов, используемых для анализа, с помощью отдельных переменных среды позволяет повысить точность обнаружения угроз и скорость проведения расследований.
- **Интерактивный пользовательский режим** дает аналитикам возможность напрямую взаимодействовать с образцами вредоносных программ.
- **Широкий набор функций распаковки** позволяет сократить время расследования инцидентов с нескольких дней до нескольких минут.
- **Полный логический путь** позволяет проводить более глубокий анализ образцов, вынуждая код выполнять дополнительные логические пути, не выполняемые в стандартных изолированных средах.
- **Отправка образца в несколько разных виртуальных сред** повышает скорость проведения расследований, поскольку позволяет определить, какие переменные среды необходимы для выполнения анализируемого файла.
- **Подробные отчеты** содержат критически важную для хода расследования информацию, включая сведения из базы MITRE ATT&CK™, результаты дизассемблирования, дампы памяти, графические диаграммы вызова функций, информацию о встроенных и сброшенных файлах, журналы API пользователя и информацию, полученную с помощью PCAP. Временная шкала угроз позволяет визуализировать этапы реализации атак.
- **Интеграция с Bro Network Security Monitor.** Используйте датчик Bro для мониторинга подозрительного сегмента сети, который позволяет отслеживать и захватывать трафик, затем передавая файлы McAfee Advanced Threat Defense для их последующего анализа.

Развертывание

Несколько вариантов развертывания системы анализа угроз повышенной сложности позволяют интегрировать данный продукт в любую сеть. McAfee Advanced Threat Defense предлагается как в виде аппаратного устройства, так и в виртуальной форме с поддержкой и частного, и публичного облака на платформе Azure Marketplace.

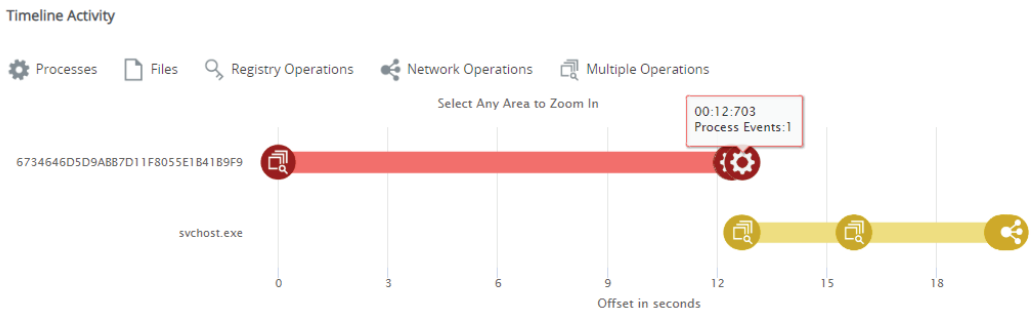

Рис. 1. Этапы выполнения анализируемой угрозы отображаются на временной шкале.

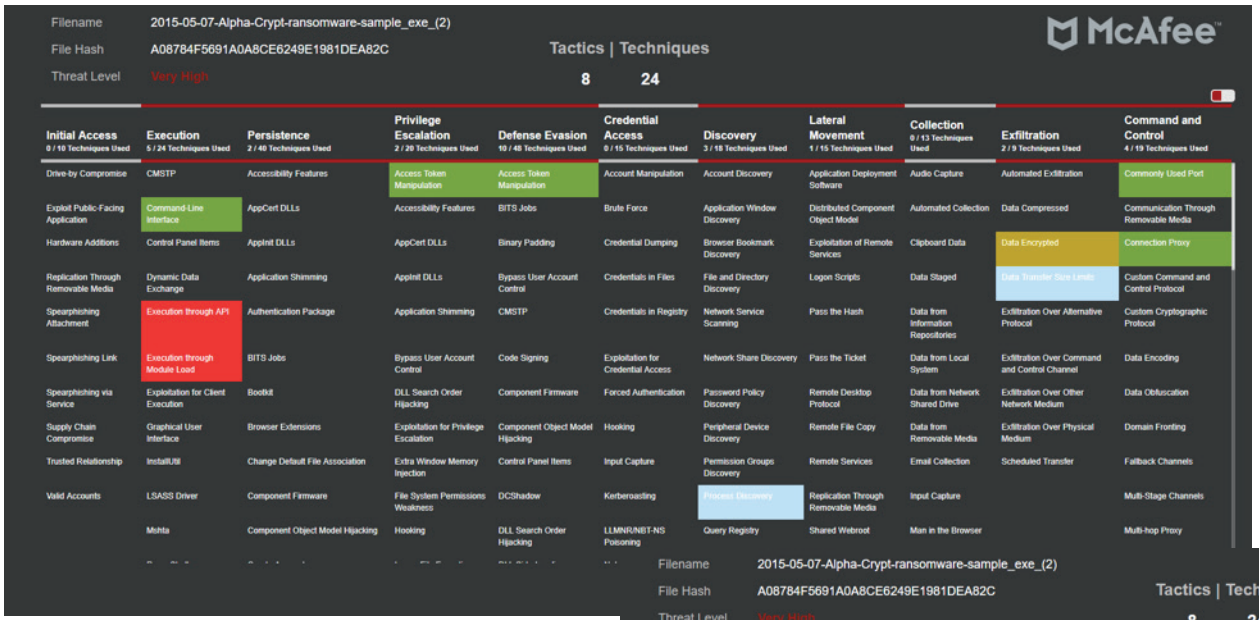

Рис. 2. Результаты сопоставляются с информацией из базы MITRE ATT&CK™.

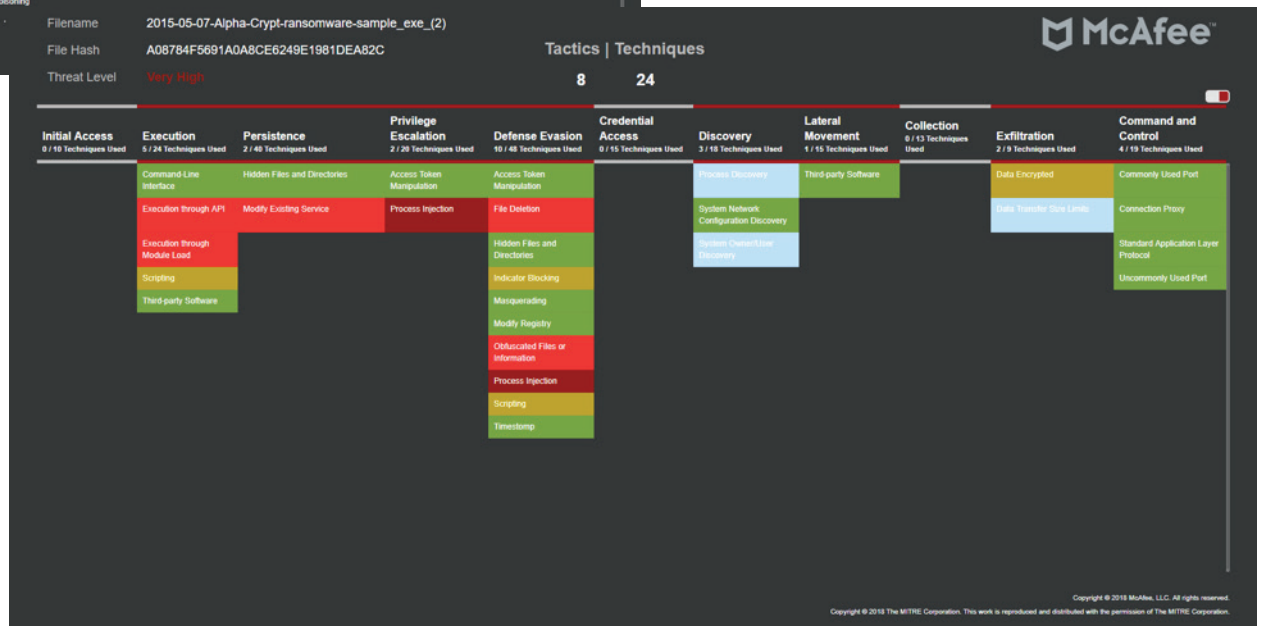

Рис. 3. Фильтрация результатов, показанных на рис. 2, позволяет отобразить в отчете только выявленные методы атаки.

Технические характеристики McAfee Advanced Threat Defense		
Вариант аппаратного устройства	ATD-3200 Корпус 1RU для монтажа в стойку	ATD-6200 Корпус 1RU для монтажа в стойку
Вариант виртуального устройства	v1008 ESXi 5.5, 6.0, 6.5, 6.7 Hyper-V Windows Server 2012 R2, Windows Server 2016	
Обнаружение		
Поддерживаемые типы образцов файлов	PE-файлы, файлы Adobe, файлы Microsoft Office, файлы изображений, архивные файлы, файлы Java, файлы Android Application Package, URL-адреса	
Методы анализа	McAfee Anti-Malware Engine, оценка репутации файлов, URL-адресов и IP-адресов с помощью технологии GTI, Gateway Anti-Malware (эмуляция и анализ поведения), динамический анализ (в «песочнице»), детальный анализ кода, пользовательские правила для YARA, машинное обучение	
Поддерживаемые операционные системы	Windows 10 (64-разрядняя версия), Windows 8.1 (64-разрядняя версия), Windows 8 (32- и 64-разрядные версии), Windows 7 (32- и 64-разрядные версии), Windows XP (32- и 64-разрядные версии), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003; Android Поддержка операционной системы Windows на всех языках	
Форматы вывода данных	STIX, OpenIOC, XML, JSON, HTML, PDF, текст	
Методы предоставления	Посредством интеграции со специализированными решениями, через API-интерфейсы на основе REST, вручную и через McAfee Advanced Threat Defense Email Connector (SMTP)	

Дополнительная информация

За дополнительной информацией о McAfee Advanced Threat Defense или для получения пробной версии решения просим обращаться к своему представителю или к странице **www.mcafee.com/ru/products/advanced-threat-defense.aspx**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru

McAfee и логотип McAfee являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. MITRE ATT&CK и ATT&CK являются товарными знаками корпорации MITRE Corporation. Copyright © 2020 McAfee, LLC. 4616_0920
Сентябрь 2020 г.