Cisco Advanced Malware Protection for Endpoints:

– Malicious Activity Protection (защита от вредоносной активности)

Обзор

В настоящем документе рассказывается о новом модуле защиты от вредоносной активности, добавленном к решению Cisco® Advanced Malware Protection for Endpoints в рамках версии 6.1.5 Коннектора AMP для Windows – Malicious Activity Protection. Цель документа – объяснить технологию, а также помочь в проведении оценки ценности модуля защиты от вредоносной активности как дополнения к текущему комплекту механизмов безопасности, поставляемых с продуктом. Здесь описывается порядок работы модуля, а также представлено краткое руководство для проверки и демонстрации доказательства его ценности.

Введение

Атаки программ-вымогателей могут принимать самые разные формы. Программы-вымогатели – это вид вредоносного ПО, которое, как правило, стремится зашифровать файлы на компьютере жертвы. В случае успешного шифрования такие программы требуют заплатить за расшифровку данных и возврат жертве доступа к ним. Атаки программ-вымогателей обычно происходят с использованием вредоносной полезной нагрузки, которая распространяется как легитимный файл. Этот файл направляется в приложении к электронному письму и обманным путем заставляет пользователя скачать или открыть его. Однако существуют примеры атак программ-вымогателей, которые распространяются без взаимодействия с пользователем. Злоумышленники, использующие программы-вымогатели, почти всегда желают получить деньги, и в отличие от атак других типов, жертву, как правило, уведомляют о том, что атака произошла. Затем жертве дают указания в отношении того, как избавиться от последствий атаки. Оплату часто требуют в виртуальной валюте, чтобы вычислить личность киберпреступника было не так просто. Важным моментом здесь является то, что совершение оплаты в пользу вымогателя не гарантирует расшифровки данных и, кроме того, спонсирует разработку следующего поколения программ вымогателей. Чтобы узнать больше о примерах недавних атак программ-вымогателей и основополагающих рекомендациях для минимизации рисков таких атак, посетите веб-сайт Cisco Talos™ (talosintelligence.com).

Модуль AMP for Endpoints Malicious Activity Protection (MAP), включенный в версию 6.1.5 Коннектора AMP для Windows, защищает ваши оконечные устройства посредством мониторинга системы и выявления процессов, демонстрирующих вредоносную активность при выполнении, и прекращает их выполнение. Поскольку модуль MAP обнаруживает угрозы, наблюдая за поведением процесса при его выполнении, он способен по образцу определить, была ли система атакована новым вариантом программы-вымогателя или вредоносного ПО, который смог обойти прочие продукты безопасности и технологии обнаружения, такие как традиционные системы обнаружения вредоносного ПО на основе сигнатур. Первый выпуск модуля MAP направлен на обнаружение, блокировку и помещение в карантин атак программ-вымогателей на оконечных устройствах.

Содержание

Обзор

Введение

Защитная структура AMP for Endpoints

Технология защиты от вредоносной активности

- Принцип действия
- Производительность и совместимость
- Исключения

Решение в действии

Приложение

- Часто задаваемые вопросы

Заключение

Защитная структура AMP for Endpoints

Средства защиты в рамках AMP for Endpoints включают несколько совместно работающих технологий для предотвращения попадания вредоносных кодов на оконечные устройства, их обнаружения и устранения. Основные технологии предотвращения в памяти включают:

- **Предотвращение атак эксплойтов (Exploit Prevention)** защищает оконечные устройства от атак путем внедрения в память, которые обычно используются вредоносным ПО или в рамках атак «нулевого дня» при наличии неисправленных программных уязвимостей в защищенных процессах.
- **Защита системных процессов (System Process Protection)** защищает критически важные системные процессы Windows от компрометации атак путем внедрения в память других процессов.

Основные технологии обнаружения на диске включают:

- **Облако AMP (AMP Cloud)** предоставляет доступ к глобальной базе аналитических данных, которая постоянно обновляется и дополняется новыми обнаружениями, а также предоставляет огромный массив знаний для Коннектора AMP посредством поиска хеша «один к одному», модуля универсальных сигнатур, а также модуля машинного обучения.
- **TETRA** – это традиционный антивирусный модуль на основе сигнатур, который располагается на оконечном устройстве и обеспечивает возможность обнаружения вредоносного ПО на диске; TETRA является частью Коннектора AMP для Windows (ClamAV – это оффлайн-модуль для Mac и Linux).
- **Защита от вредоносной активности (Malicious Activity Protection)** обеспечивает обнаружение и блокирование ненормального поведения выполняемой программы на оконечном устройстве в процессе ее выполнения (например, поведения, связанного с программами-вымогателями).
- **Пользовательский поиск (Custom Detections)** служит для целей предоставления администратору по безопасности реальных возможностей контроля посредством определения пользовательских сигнатур и создания «черных списков».

Рисунок 1. Защитная структура AMP for Endpoints

Основныетехнологии обнаружения после заражения включают:

- **Когнитивный анализ угроз (Cognitive Threat Analytics)** использует машинное обучение и искусственный интеллект для корреляции трафика, генерируемого пользователями, чтобы с высокой степенью надежности обнаруживать трафик к командным серверам управления, утечку данных и потенциально нежелательные приложения, которые уже работают в среде; для этого требуется прокси-сервер, предоставляющий веб-журналы, или анализатор потоков Cisco Stealthwatch® Flow Collector, предоставляющий данные NetFlow.
- **Корреляция потоков от устройств (Device Flow Correlation)** позволяет отслеживать сетевую активность и определяет, какие действия должен совершать Коннектор AMP в случае обнаружения подключений к вредоносным узлам.
- **Облако индикаторов компрометации (Cloud Indication of Compromise (IOC))** – это функция, которая позволяет обнаруживать подозрительное поведение, наблюдаемое на оконечных устройствах, а также ищет шаблоны вредоносного ПО и предупреждает о них; облако IOC не подразумевает активной блокировки.
- **Индикаторы компрометации на оконечных устройствах (Endpoint IOC)** – это мощный инструмент реагирования на инциденты для сканирования индикаторов после компрометации на большом количестве компьютеров; его можно импортировать из открытых файлов на основе IOC, которые написаны с учетом срабатывания на свойства файла. Перечисленные функции безопасности формируют основу для общего подхода для защиты от современного вредоносного ПО. Хотя Cisco рекомендует использовать все эти модули совместно для получения ценности продукта в полном объеме, клиенты могут сами решить, какие из указанных функций активировать, а какие – нет, посредством соответствующей политики. Модуль MAP, которому уделяется основное внимание в настоящем документе, сам по себе является лишь одним из важных функциональных элементов, предоставляемых AMP for Endpoints. Несмотря на то, что эти технологии перечислены по отдельности, они работают совместно, образуя структуру обнаружения, для обеспечения улучшенного мониторинга и дополнительного контроля на всем протяжении атаки.

Дополнительные функции AMP for Endpoints, такие как динамический анализ и ретроспективное обнаружение, подробно описаны в руководстве пользователя, представленном по ссылке: docs.amp.cisco.com.

Технология защиты от вредоносной активности

Модуль MAP представляет собой модуль обнаружения на основе поведения, который выявляет вредоносные действия, происходящие на оконечном устройстве в процессе выполнения. После проведения масштабных исследований с изучением образцов программ-вымогателей в различных вариантах, наблюдаемых на практике, группа AMP for Endpoints по проведению исследований и разработок определила общие типы поведения, связанные с такими угрозами, что позволило сформулировать набор правил, ставший частью модуля, который размещен на Коннекторе AMP.

Принцип действия

Модуль MAP непрерывно проверяет защищаемую систему на определенные изменения (о которых будет рассказано далее), чтобы выявить процессы, которые следует считать виновными в случае обнаружения видов активности, перечисленных в наборе поведенческих правил. В отношении процессов, обнаруженных MAP, можно предпринять следующие действия, в соответствии с конфигурацией политики:

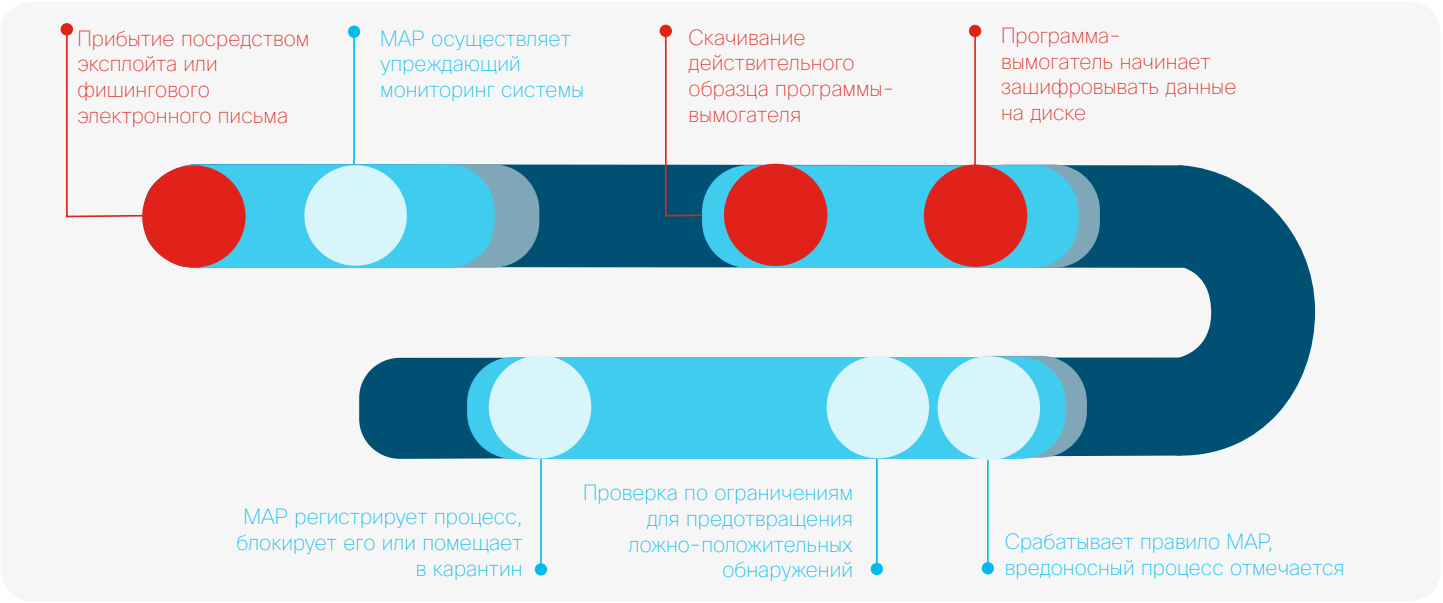
- Зарегистрировать обнаружение: В этом режиме обнаруженный вредоносный процесс не блокируется MAP, а регистрируется в консоли AMP for Endpoints. (Это режим аудита, когда блокировка или помещение в карантин не осуществляются, но обнаружение регистрируется.)
- Заблокировать выполнение процесса: В этом режиме вредоносный двоичный файл обнаруживается и блокируется, а его дальнейшее выполнение запрещается (по аналогии с функцией блокировки приложения).
- Пометить процесс в карантин: В этом режиме процесс-нарушитель прекращается, а соответствующие файлы помещаются в карантин.

Набор правил обнаружения в модуле MAP направлен на поиск аномалий в системе. Например, если процесс читает, записывает и переименовывает набор файлов в течение короткого промежутка времени, правило может запустить определенное действие в отношении такого процесса. В качестве альтернативы, если процесс читает и записывает содержание файла в другой файл, а затем стирает исходные файлы, модуль MAP может запустить определенное действие согласно политике. Это лишь несколько примеров правил, входящих в указанный набор. Правила предназначены для внутреннего использования разработчиками и никогда не раскрываются пользователям, а также не могут конфигурироваться пользователями. Инженерные и исследовательские группы AMP for Endpoints непрерывно оценивают методы, используемые вредоносным ПО и программами-вымогателями на практике, чтобы повысить ожидаемые уровни защиты.

Для борьбы с ложно-положительными обнаружениями процессы, определенные модулем MAP как демонстрирующие вредоносную активность, проверяются по ограничениям для предотвращения случайной блокировки или помещения в карантин легитимных приложений и компонентов операционной системы.

Несмотря на то, что Коннектор AMP способен обнаружить программы-вымогатели и не допустить полной компрометации данных в системе, существует возможность того, что некоторые файлы будут зашифрованы процессом-нарушителем до тех пор, пока модуль MAP не определит, что процесс отвечает критериям для его обозначения в качестве вредоносного. Коннектор AMP сообщит, какие файлы были изменены процессом-нарушителем, чтобы их можно было быстро восстановить из резервных копий при необходимости. Эта информация об истории файлов располагается в данных о событии MAP в консоли AMP for Endpoints.

Рисунок 2. Схема обнаружения модулем MAP



MAP является частью коннектора AMP for Endpoints для Windows. Сведения относительно поддерживаемых операционных систем можно найти в примечаниях к выпуску.

Производительность и совместимость

Воздействие на производительность определяет значительную часть критериев выбора средств безопасности для оконечных устройств. AMP for Endpoints создает небольшую нагрузку на систему с точки зрения ее производительности. Активация модуля MAP не подразумевает существенного снижения производительности или каких-либо изменений в качестве для конечного пользователя. Ожидаемое увеличение загрузки ЦП, связанное с активацией модуля MAP, составляет приблизительно 5 %, при этом воздействие на производительность памяти, диска и сети практически равно нулю.

Совместимость с программным обеспечением, установленным на оконечном устройстве, является определяющим аспектом с точки зрения любого решения для оконечных устройств. Модуль MAP не имеет каких-либо известных проблем в части совместимости с программным обеспечением сторонних поставщиков. Для получения подробной информации об известных проблемах в части совместимости обратитесь к руководству пользователя AMP for Endpoints.

Исключения

Используемые в пользовательской среде легитимные приложения, которые демонстрируют поведение, аналогичное поведению программ-вымогателей, может потребоваться исключить из мониторинга MAP. Простым примером таких приложений служат программы-архиваторы. Исключения из процесса можно применять для предотвращения мониторинга приложений и, в некоторых случаях, их дочерних процессов на предмет присутствия вредоносной активности модулем MAP в рамках AMP for Endpoints. Обратите внимание на то, что дочерние процессы, создаваемые исключенным процессом, не исключаются по умолчанию.

В целом, исключения также можно использовать для разрешения конфликтов с другими продуктами безопасности или для минимизации проблем с производительностью посредством исключения каталогов, где располагаются большие файлы, в которых часто производятся записи, такие как базы данных. Для получения более подробной информации обратитесь к руководству пользователя AMP for Endpoints.

Решение в действии

Несмотря на то, что модуль MAP способен останавливать программы-вымогатели по образцу во время выполнения (без учета вектора использования, способности к распространению, хеша образца, целевых файлов, расширений файлов и т.д.), для целей тестирования может быть полезным рассмотреть несколько примеров атак, которые могут быть заблокированы модулем или помещены им в карантин. Тестирование проводилось с использованием инфраструктуры, автоматизированной для тестирования с использованием различных сред виртуализации, а также машин с поддерживаемыми операционными системами. Инженерные и исследовательские группы AMP for Endpoints непрерывно оценивают методы, используемые авторами программ-вымогателей, чтобы повысить уровни защиты.

В число семейств программ-вымогателей, заблокированных MAP или помещенных им в карантин во время выполнения, входят SamSam, WannaCry, JigSaw, Jaff, Cerber, TeslaCrypt, CryptoFortress и многие другие.

Поскольку модуль MAP использует защиту на основе поведения для поиска вредоносной активности, невозможно избежать обнаружения простых изменений в хешах файлов или обфускации с использованием упаковщиков.

Трансляцию можно посмотреть здесь.

Приложение

Часто задаваемые вопросы

Вопрос. Если процесс был ошибочно помещен в карантин, можно ли восстановить его нормальную работу?

Процесс, который был ошибочно признан нарушителем и помещен в карантин в результате этого, может быть восстановлен с использованием обычной процедуры восстановления AMP for Endpoints. После этого его нужно поместить в «белый список» или исключить из проверки AMP с помощью консоли AMP for Endpoints; о каждом таком происшествии также следует сообщать инженерной группе через Центр технической поддержки Cisco.

Вопрос. Может ли MAP помочь в том случае, когда вредоносный код был внедрен в легитимный процесс и использовал его для шифрования данных?

Поскольку в Коннектор AMP встроены определенные ограничения, они могут защитить легитимный процесс от признания его нарушителем модулем MAP (даже если он может содержать вредоносный код в результате использования процедуры создания полостей или иного метода внедрения кода). Использования различных методов внедрения кода можно избежать посредством модулей предотвращения атак эксплойтов и защиты системных процессов, которые можно активировать с помощью политики AMP.

Вопрос. Способен ли модуль MAP остановить программы-вымогатели, запущенные с подключенного USB накопителя?

Да, модуль MAP отслеживает подключенные USB накопители и блокирует/помещает в карантин запущенные с них процессы программ-вымогателей.

Вопрос. Существует ли гарантия того, что действующие образцы программ-вымогателей будут заблокированы модулем MAP или помещены им в карантин?

Такая гарантия никогда не предоставляется. Однако группы AMP по проведению исследований и разработок непрерывно проводят испытания эффективности и осуществляют постоянные инвестиции в разработку функции, обеспечивающей более высокие уровни защиты для клиентов.

Заключение

Атаки программ-вымогателей оказывают значительное влияние на многие организации по всему миру. С течением времени масштабы этого бизнеса существенно возросли, а самые распространенные атаки программ-вымогателей прошлого дают хорошее представление о том, как происходило это развитие. Во многих случаях вину за такие взломы можно возложить на способ формирования и поддержания организациями своей ИТ инфраструктуры. Кроме того, всегда присутствует человеческий фактор: многие атаки программ-вымогателей начинаются с простого фишингового письма по электронной почте, которое даже не во всех случаях имеет конкретную цель и подготовлено злоумышленниками должным образом.

MAP внедряет иной подход к защите от вредоносного ПО и программ-вымогателей, который в большей степени сосредоточен на обнаружении во время выполнения с целью блокировки и помещения в карантин. Это лучший подход к обнаружению различных вариантов программ-вымогателей во время выполнения, не зависящий от сигнатур и не требующий предварительных знаний о том, как сформировалась угроза. Cisco настоятельно рекомендует использовать эту возможность совместно с архитектурным подходом к безопасности, а также передовой практикой обеспечения информационной безопасности, что поможет сформировать эффективное решение для предотвращения или серьезного ограничения воздействия таких угроз. Наличие продуманной многоуровневой стратегии углубленной защиты гарантирует, что организации смогут ограничить распространенные сбои в работе систем, а также обнаруживать случаи компрометации систем в своей среде и реагировать на них, чтобы минимизировать возможные последствия таких атак.

Узнайте больше об AMP for Endpoints

Чтобы получить более подробную информацию об AMP for Endpoints и обеспечиваемой этим решением защите от современных угроз, посетите веб-сайт https://cisco.com/go/endpoints

Демонстрационное видео об AMP for Endpoints представлено по ссылке: https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html?socialshare=lightbox-hero2

C11-740980-00 07/18