Защита от усовершенствованного вредоносного ПО:

руководство покупателя

Защита от усовершенствованного вредоносного ПО: руководство покупателя

Об этом документе

В этом документе описывается, какие функции необходимы современным решениям для защиты от вредоносного ПО, перечисляются основные вопросы, которые покупателю необходимо задать поставщику, и рассказывается, как решения Cisco помогают успешно противостоять атакам, используя следующие четыре метода:

- Углубленный анализ.
- Коллективная глобальная аналитика угроз безопасности.
- Применение средств защиты для разных форм-факторов (сети, оконечные устройства, мобильные устройства, защищенные шлюзы и виртуальные системы).
- Непрерывный анализ и ретроспективная защита.

Введение

Не секрет, что у современных злоумышленников достаточно средств, опыта и упорства, чтобы обойти систему ИТ-безопасности в любой организации — нужно только время. Традиционные средства защиты, включая межсетевые экраны и антивирусное ПО для оконечных устройств, больше не справляются с такими атаками. Процесс обнаружения и устранения вредоносного ПО необходимо совершенствовать — и при этом быстро. Обнаружение вредоносного ПО и целенаправленных, непрерывных атак, которые оно осуществляет, — слишком сложная задача, чтобы ее можно было эффективно решить исключительно с помощью технологии или продукта, действующих в определенный момент времени. Для защиты от усовершенствованного вредоносного ПО требуются интегрированный набор средств контроля и непрерывный процесс обнаружения, подтверждения, отслеживания, анализа и устранения подобных угроз до, во время и после атаки.

Вопросы, которые следует задать поставщику

- Как вы используете большие данные для непрерывного обнаружения вредоносного ПО?
- Как проводится анализ вредоносного ПО для выявления выполняемых им действий?
- Могут ли ваши средства анализа вредоносного ПО автоматически обновлять возможности обнаружения?
- Как вы получаете информацию о новых угрозах вредоносного ПО?
- Каким образом вы выполняете непрерывный анализ для ретроспективного обнаружения вредоносного ПО?

Эта проблема может еще усугубиться в будущем. Распространение полиморфного вредоносного ПО привело к тому, что организации сталкиваются с десятками тысяч новых образцов вредоносного ПО в час, а для успешной компрометации устройства достаточно иметь в распоряжении простейшие вредоносные программные средства. Подход, основанный на черных списках, по которым файлы сопоставляются с сигнатурами известных вредоносных программ, уже не в состоянии решить эту проблему, а новые приемы обнаружения (например, перемещение подозрительных файлов в изолированные среды) не обладают стопроцентной эффективностью.

Углубленный анализ и коллективная аналитика безопасности

Пытаясь улучшить обслуживание заказчиков в условиях экспоненциального роста известных типов вредоносного ПО, поставщики традиционных средств защиты для оконечных устройств представили на рынке «облачный антивирус», который фактически перенес базы данных сигнатур в облако. Эта технология устранила потребность в распространении миллиардов сигнатур вирусов на каждое оконечное устройство каждые пять минут, но не решила проблему изощренных атак, ориентированных на преодоление систем обнаружения на основе сигнатур.

Разрабатывая вредоносное ПО, которое терпеливо ждет подходящего момента для атаки, злоумышленники использовали еще один недостаток модели облачного антивируса: большинство технологий защиты от вредоносного ПО действует непостоянно и без учета контекста. Они ориентируются исключительно на обнаружение файла в момент его появления (в определенный момент времени). Однако файл, безопасный сегодня, легко может стать вредоносным завтра. Полноценную защиту можно обеспечить только путем непрерывного анализа. Постоянный мониторинг всего трафика помогает сотрудникам отдела безопасности отследить заражение, вплоть до его источника, если поведение файла изменилось.

Разработчики усовершенствованного вредоносного ПО самыми разными способами маскируют его сущность и затрудняют его обнаружение. К подобным приемам относятся полиморфное изменение файлов, которого достаточно для того, чтобы обмануть модули сигнатур, интеллектуальные программы загрузки, которые получают вредоносное ПО по требованию из сетей управления и контроля, а также стираемые «трояны», которые удаляют собственные компоненты, усложняя экспертам-криминалистам задачи поиска и анализа вредоносного ПО. И это далеко не всё.

Поскольку вредоносное ПО больше нельзя идентифицировать по внешним признакам, для эффективной защиты требуются новые техники, с помощью которых можно будет зафиксировать и проанализировать все этапы жизненного цикла подобного ПО. Эта новая модель упреждающей информационной безопасности позволит понять, что делает вредоносный код и куда он перемещается. Технологии обнаружения, действующие в определенный момент времени, могут не распознавать современные угрозы, и вредоносные действия и признаки вторжения могут появиться значительно позднее периода первоначального обнаружения.

Средства защиты от вредоносного ПО должны адаптироваться так же быстро, как угроза. Для решения этих проблем обнаружения вредоносного ПО компания Cisco применила новый, более комплексный подход. Благодаря глобальной базе, в которую входят тысячи предприятий и миллионы оконечных устройств, мы ежемесячно собираем несколько миллионов образцов вредоносного ПО. Десятки тысяч программных атрибутов проходят анализ в наших модулях анализа Threat Grid, в группе по информационной безопасности и исследованиям Cisco Talos (Talos) и в облаке коллективной информационной безопасности (CSI) в целях отделения вредоносного ПО от безопасного. Также анализируются характеристики сетевого трафика, чтобы идентифицировать вредоносное ПО, выполняющее поиск сетей управления и контроля. Для сравнения мы используем свою обширную базу установленных решений по защите от усовершенствованного вредоносного ПО (AMP) в разных линейках продуктов[1], чтобы определить нормальное поведение файлов и сетей, как глобальное, так и характерное для отдельных организаций.

1. Возможности AMP теперь предлагаются как дополнительно лицензируемый компонент в решениях Cisco для обеспечения безопасности электронной почты и веб-трафика. Узнайте больше, посетив веб-сайт http://www.cisco.com/go/amp.

Защита от усовершенствованного вредоносного ПО: руководство покупателя

Для обнаружения вредоносного ПО, созданного для противодействия традиционным тактикам обнаружения, требуется дальнейшее развитие технологий. Cisco использует специализированные модели, которые идентифицируют вредоносное ПО по его действиям, а не по внешним признакам. Это позволяет обнаруживать новые типы атак, даже атаки «нулевого дня». Чтобы не отставать от темпов развития вредоносного ПО, эти модели автоматически обновляются в режиме реального времени на основе данных о новых методах атак, полученных нашими аналитическими модулями Threat Grid и группой по информационной безопасности и исследованиям Talos.

Интеграция нашей технологии Threat Grid в AMP расширяет аналитику угроз и позволяет использовать как статические, так и динамические («песочница») механизмы анализа вредоносного ПО. Встроенный в AMP компонент Threat Grid (также доступный как отдельное решение) предоставляет отделам безопасности дополнительную базу знаний по вредоносному ПО, которая пополняется данными со всего мира. Организации получают в свое распоряжение контекстные каналы аналитических данных в стандартных форматах, которые легко интегрируются с существующими технологиями обеспечения безопасности. Анализ миллионов образцов вредоносного ПО более чем по 350 поведенческим индикаторам каждый месяц позволяет выявить миллиарды артефактов и создать простую для понимания систему оценки угроз, чтобы помочь службам информационной безопасности правильно расставить приоритеты. Модули анализа Threat Grid обнаруживают деятельность вредоносного ПО, включая связанный трафик HTTP и DNS, потоки TCP/IP, процессы, которые оно затрагивает, и операции с реестром, благодаря чему группы обеспечения безопасности владеют всей полнотой информации о потенциальных угрозах в своих сетях.

Рис. 1. Технология Cisco обеспечивает защиту до, во время и после атаки, охватывает множество направлений атак и дополняет традиционные приемы обнаружения в определенный момент времени возможностями непрерывного анализа и ретроспективной защиты.

К дополнительным преимуществам можно отнести облачную систему анализа, которая оценивает файлы за продолжительный период времени. Наши решения AMP могут уведомлять пользователя об угрозах в течение длительного времени после первоначального анализа файла, даже если он прошел через точку обнаружения.

Наконец, эти преимущества предоставляются всему сообществу пользователей Cisco AMP. Его участники получают от AMP уведомление каждый раз при изменении поведения файла. В этой ситуации все организации, применяющие Cisco AMP, мгновенно информируются о вредоносном файле – таким образом, возможности облака обеспечивают им «коллективный иммунитет».

Ретроспективная защита тормозит развитие атак злоумышленников и возвращает их на шаг назад

Злоумышленники не дремлют. Они непрерывно оценивают имеющиеся средства обеспечения безопасности и меняют тактику, чтобы оставаться на шаг впереди системы защиты. Фактически большинство разработчиков вредоносного ПО проверяет, может ли их продукт противостоять ведущим системам защиты, прежде чем осуществить атаку. Поскольку эффективность черных списков снижается, все больше компаний по обеспечению безопасности решают задачи по обнаружению и изучению вредоносного ПО при помощи динамического анализа, основанного на виртуальных машинах (ВМ). Злоумышленники, в свою очередь, подкорректировали тактику: теперь они либо не выполняют никаких действий, либо откладывают атаку на срок в несколько часов (или дней), если вредоносный код запускается в ВМ. Они предполагают, что в этом случае вредоносный файл не будет обнаружен, поскольку в период оценки он не является источником вредоносных действий. Конечно, по завершении периода ожидания устройство будет взломано.

К сожалению, технологии, действующие в определенный момент времени, не выполняют повторный анализ файлов. Статус файла, идентифицированного как безопасный, впоследствии не меняется, даже если приемы обнаружения с тех пор были усовершенствованы или данный файл демонстрирует вредоносное поведение. Что еще хуже, если вредоносное ПО не было выявлено, средства обеспечения безопасности не могут отследить его распространение в среде, определить первопричины или выявить потенциальные шлюзы для проникновения вредоносного ПО (системы, которые периодически заражаются вредоносным ПО или являются отправными точками для более широкого распространения заражения).

Ретроспективная защита

Непрерывный анализ поведения файлов, отслеживание процессов, действий файлов и связи с течением времени с целью понять весь масштаб заражения, выявить основные причины и выполнить восстановление. Это позволяет повернуть время вспять и затормозить развитие новых атак. Потребность в ретроспективной защите возникает в случае каких-либо признаков нарушения, например срабатывания триггера события, изменения в поведении файла или срабатывания триггера индикатора компрометации.

Лучше всего предположить, что ни одно средство обнаружения не может быть на 100% эффективным. Верить в то, что одни только средства обнаружения могут обеспечить системе полную защиту, значит переоценивать свои возможности защиты важных ресурсов и в то же время недооценивать возможности злоумышленников. Организации должны предполагать, что их средства защиты уязвимы. Они должны иметь возможность определить масштаб и контекст заражения, быстро локализовать и устранить угрозу, ее первопричины и шлюзы для вредоносного ПО. А для этого требуется ретроспективная защита.

Наша ретроспективная технология обеспечения безопасности позволяет вернуться в прошлое и определить, какие устройства были заражены вредоносным ПО, вне зависимости от времени идентификации вредоносного файла. Такую возможность обеспечивают два компонента: траектория файла и индикаторы компрометации. Траектория файла отслеживает каждый файл, попадающий в защищенную сеть, и предоставляет доступ к полной истории действий, выполненных на каждом защищаемом устройстве. Индикаторы компрометации используют информацию, полученную из траектории файла, для создания поведенческого шаблона, при помощи которого можно искать вредоносное ПО, присутствующее в системе, но не обнаруженное.

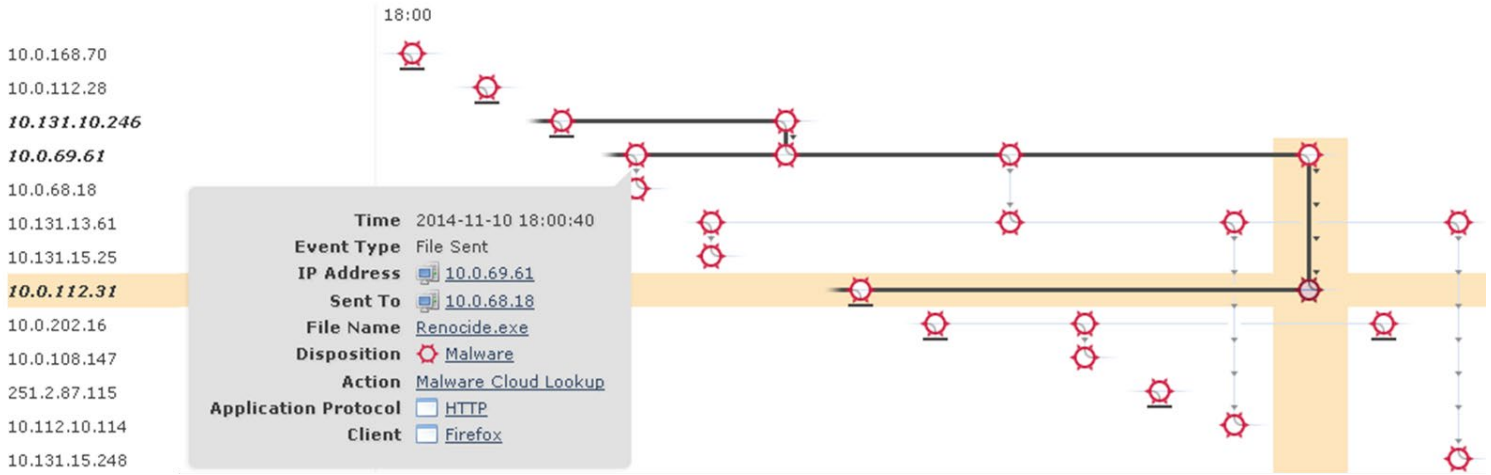
Отслеживание вредоносного ПО по траектории

В случае использования традиционных средств защиты от вредоносного ПО при идентификации файла как вредоносного в тот или иной момент в будущем возможности пользователя ограничены. Он не может воспользоваться машиной времени и заблокировать этот файл в точке вхождения. Файл уже находится в среде, и неизвестно, насколько далеко он распространился и какой ущерб нанес. В такой ситуации большинство средств защиты от вредоносного ПО становятся бесполезными, не позволяя оценить весь масштаб проблемы и решить ее.

Именно на этом этапе большие данные и расширенная аналитика, на которых базируется AMP, приносят свои плоды. Функция траектории помогает точно отследить перемещение вредоносного ПО по организации. В некоторых случаях можно мгновенно и автоматически удалить его с зараженных устройств. Траектория дает наглядное представление о перемещении файлов по организации и их действиях в системе. Но пользователь не просто получает общую картину действий файла во всей сети. AMP также предоставляет подробные сведения об активности каждого исполняемого файла на отдельном оконечном устройстве, независимо от поведения файла. Получив эту информацию, можно узнать, на какие другие оконечные устройства в сети распространились вредоносные файлы. Это обеспечивает специалистам по обеспечению безопасности высокий уровень контроля. Еще важнее то, что, поскольку система AMP отслеживает все события использования для каждого файла, организации могут выявить «нулевого пациента» (первую жертву вредоносного ПО) и все остальные зараженные устройства, что гарантирует полное устранение заражения. Хорошо известно, что, если после очистки в системе останется хотя бы один экземпляр вредоносного ПО, повторное заражение весьма вероятно.

Кроме того, функция траектории не просто анализирует данные, связанные с активностью файлов. Она также отслеживает информацию о прохождении файла в системе, использовании, зависимостях, связях, протоколах. Кроме того, траектория выявляет файлы, которые устанавливают вредоносное ПО, чтобы быстро выполнить анализ первопричин попадания обнаруженного вредоносного ПО в систему или возникновения подозрительных действий. Благодаря этому сотрудники отдела безопасности могут мгновенно переключиться с обнаружения на управление в ходе атаки, быстро определив масштаб вторжения и его основные причины для эффективного пресечения дальнейшего распространения заражения.

Рис. 2. Экран с траекторией файла, показывающий распространение вредоносного ПО с информацией о точке проникновения, активности вредоносного ПО и зараженных оконечных устройствах.



При наличии большого числа событий обнаружения, особенно вредоносного ПО, очень трудно определить, какое событие действительно имеет высокий приоритет и требует принятия немедленных мер. Одно событие, даже если это блокировка вредоносного файла на оконечном устройстве, не всегда свидетельствует о компрометации. Но когда несколько событий, даже на первый взгляд безобидных, сопоставляются, может значительно увеличиться риск заражения системы и вероятность того, что нарушение безопасности неминуемо или уже произошло.

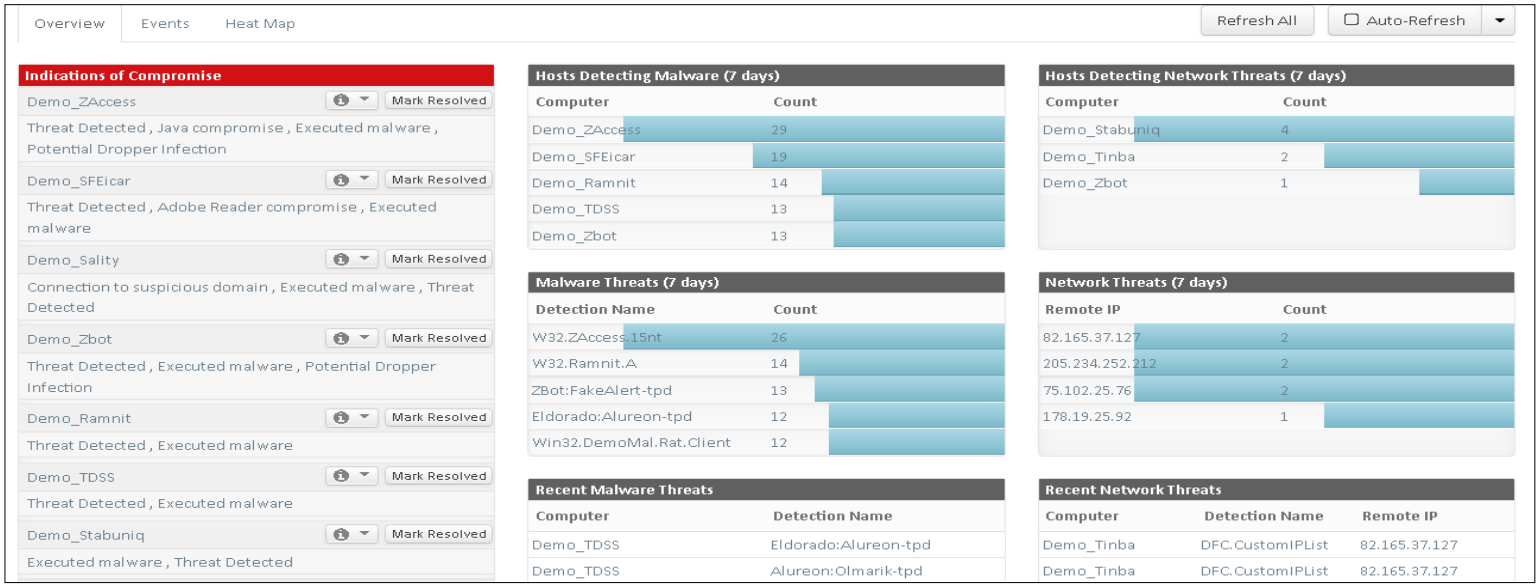
Индикаторы компрометации помогают выявить шаблоны, а не конкретные признаки.

Индикаторы компрометации APM предназначены для углубленного анализа и обнаружения систем, демонстрирующих симптомы активного заражения. По возможностям эта функция значительно превосходит технологии обнаружения в определенный момент времени, поскольку после первого анализа продолжает собирать, анализировать и сопоставлять данные о действиях, связанных с вредоносным ПО, автоматически предоставляя результаты анализа и сведения о приоритетности рисков.

Наконец, если вредоносное ПО уже обосновалось в среде, оно обычно пытается наладить связь с серверами управления и контроля или в случае прямого контроля со стороны злоумышленника проводит разведку, чтобы приблизиться к предполагаемой цели.

Cisco AMP отслеживает операции связи на защищенных оконечных устройствах и сопоставляет их с базой данных коллективной аналитики безопасности, чтобы выявить возможное заражение, а затем заблокировать связь и распространение вредоносного ПО на оконечных устройствах. Это обеспечивает отделу безопасности явное преимущество за счет контроля над распространением вредоносного ПО на оконечных устройствах, которые могут быть недоступны для средств защиты корпоративной сети, как, например, системы, используемые удаленными или мобильными сотрудниками. Кроме того, функции траектории и индикаторов компрометации используют собранные сведения о действиях в сети для ускорения расследования и назначения приоритета угрозам.

Рис. 3. Экран панели управления Cisco AMP с индикаторами компрометации в системе.



Защита от усовершенствованного вредоносного ПО: руководство покупателя

Вместе – лучше: внедрение в сети, на защищенном шлюзе, на физических и виртуальных оконечных устройствах, а также на мобильных устройствах.

Ни одно средство обеспечения безопасности не может существовать в вакууме. Для защиты от усовершенствованного вредоносного ПО требуется максимальная координация между средствами обеспечения безопасности сети, шлюза и оконечных устройств. Чтобы ускорить обнаружение и устранение угроз и перехватывать вредоносное ПО до возникновения масштабных нарушений безопасности, средства защиты должны согласованно работать, обмениваться информацией и сопоставлять события. Также требуется централизованная консоль управления, с помощью которой отслеживаются угрозы и выполняются операции по восстановлению на всех уровнях. Cisco предлагает интегрированную систему, использующую облачную базу данных информационной безопасности, средства углубленного анализа сети и несколько точек контроля. Такая система гарантирует, что усовершенствованное вредоносное ПО будет обнаружено при попытке проникновения в организацию.

Широкие возможности решения Cisco AMP начинаются на уровне сети, где оно обнаруживает и блокирует вредоносное ПО в момент проникновения. Когда каждый файл входит в сеть (или покидает ее), решение AMP for Networks создает для него идентификационный отпечаток, а затем обращается к центру управления Cisco FireSIGHT®, чтобы определить, был ли этот файл идентифицирован как вредоносный.

Если сведения о файле отсутствуют в центре управления, система обращается к коллективной аналитике безопасности и определяет, был ли подобный файл зафиксирован в сети информационной безопасности. Такая проверка требует немного ресурсов, отличается повышенной масштабируемостью и не влияет на задержку, в отличие от помещения каждого файла в сети в изолированную среду (метод «песочницы»). По отношению к файлам, идентифицированным как вредоносные, центр управления применяет возможности отслеживания траектории файлов, чтобы определить контекст и масштаб заражения.

На каждое защищаемое устройство также можно установить компактный агент Cisco для защиты от вредоносного ПО (коннектор Cisco AMP™), который будет сопоставлять все действия файлов с данными коллективной аналитики безопасности и списком известных вредоносных файлов. Решение AMP for Endpoints не только ищет вредоносные файлы, но также выявляет и блокирует поведение вредоносного ПО на устройстве. Даже если сведения о файле отсутствуют в базе данных, оконечные устройства будут защищены от совершенно новых атак. Решение AMP for Endpoints также использует вышеупомянутые функции ретроспективной защиты и траектории для определения масштабов любого вторжения и выявления устройств, требующих немедленного восстановления.

Если файл окажется подозрительным, AMP подвергнет его более глубокому анализу. Как указано выше, облачная система анализа Cisco точно определяет, какие действия выполняет файл, и, если он окажется вредоносным, составляет профиль атаки. Интеграция данной технологии в AMP for Endpoints предоставляет дополнительные каналы аналитики и механизмы статического и динамического анализа для более тщательного изучения вредоносного ПО. В этом процессе формируются индикаторы компрометации для обнаружения вредоносного ПО, которое может уже присутствовать в сети.

С помощью профилей вредоносного ПО AMP предоставляет организации возможность заблаговременно принять меры для защиты от вторжения. Если файл был идентифицирован как вредоносный постфактум (с помощью функции ретроспективной защиты) или выявлен в другой среде сообщества Cisco AMP, облако CSI передает обновленные сведения о нем в центр управления вашей организации, чтобы вы смогли заблокировать вредоносное ПО на уровне сети или оконечного устройства. Таким образом, вы и все остальные участники сообщества Cisco AMP получаете коллективный иммунитет. Помимо этого, организации могут задать индивидуальные правила для блокировки определенных файлов и IP-адресов, если локальные администраторы обнаружат локализованную атаку, требующую незамедлительного принятия мер.

Решение Cisco AMP for Endpoints также применяется для защиты мобильных устройств. Мобильный коннектор AMP применяет все ту же облачную базу данных информационной безопасности для быстрого анализа приложений Android на наличие возможных угроз в реальном времени. Благодаря мониторингу мобильных устройств можно быстро понять, какие устройства заражены и какие приложения являются источниками вредоносного ПО. Для прекращения атаки предусмотрены эффективные средства блокировки (занесения в черный список) конкретных приложений, чтобы можно было разрешить или запретить использование тех или иных приложений на мобильных устройствах, обладающих доступом к корпоративным ресурсам.

Возможности AMP теперь также доступны на шлюзах Cisco для обеспечения безопасности электронной почты и веб-трафика, в облачной системе защиты веб-трафика Cisco Cloud Web Security и на многофункциональных устройствах защиты Cisco ASA с сервисами FirePOWER. Функции AMP, добавленные на эти устройства, улучшают обнаружение и блокировку усовершенствованного вредоносного ПО в потенциальных точках вторжения. Основные возможности AMP включают анализ репутации файлов и помещение файлов в «песочницу», описанное выше. Кроме того, ретроспективное оповещение обеспечивает непрерывный анализ файлов, проникнувших через шлюзы, используя обновления в режиме реального времени из облака CSI. Это позволяет отслеживать изменение уровней угроз. Если файл распознается как вредоносный, система AMP предупреждает администратора и позволяет определить, какие области и приложения в сети были заражены и когда. В результате пользователи могут оперативно выявить атаку и принять меры еще до того, как она начнет распространяться.

Как уже говорилось, вредоносное ПО может проникнуть в организацию самыми разными способами. Поэтому очень важен мониторинг всех действий на всех уровнях организации. Благодаря глобальной сети информационной безопасности и возможности выявлять, блокировать, отслеживать, исследовать и прекращать вторжения на шлюзе, в сети, на оконечных устройствах, на мобильных устройствах и в виртуальных системах организации могут устранить «белые пятна», характерные для всех остальных средств обеспечения безопасности, неспособных обеспечить широкомасштабную защиту.

Полный перечень вариантов развертывания AMP и их возможностей см. на веб-сайте http://www.cisco.com/go/amp

AMP в действии

Лучший способ изучить возможности интегрированной системы защиты от усовершенствованного вредоносного ПО – рассмотреть реальный пример. Система AMP обнаружила совершенно новую Java-атаку за 48 часов до того, как информация об этой атаке была обнародована. В этом случае решение AMP for Endpoints зарегистрировало на нескольких устройствах нестандартную активность. С помощью облака CSI заказчик провел анализ подозрительных файлов и, безусловно, идентифицировал их как вредоносные.

Следующим шагом стало определение масштаба атаки и максимально быстрое ее прекращение. С помощью функции определения траектории заказчик выяснил, какие устройства были заражены вредоносными файлами или продемонстрировали поведенческие модели атаки. После очистки зараженных устройств заказчик настроил индивидуальные правила блокировки выявленных вредоносных файлов, а также индикаторов компрометации.

Однако эти правила понадобились лишь на короткое время. После инцидента все пользователи AMP получили профиль вредоносного ПО и иммунитет к этой конкретной атаке. Поскольку обнаруженные файлы и индикаторы были добавлены в модуль анализа больших данных, каждый экземпляр этой атаки был заблокирован до проникновения на устройство или в сеть. Заказчики также получили оповещение об атаке, что позволило им провести поиск угрозы в собственной среде. Таким образом, единственное действие обеспечило глобальную защиту всем пользователям Cisco AMP еще до того, как информация о новой атаке была обнародована.

Заключение

Хотя отрасль признает, что атаки усовершенствованного вредоносного ПО требуют инновационных решений для обнаружения и устранения, слишком много организаций предпочитают сосредоточить все усилия на обнаружении, вне зависимости от того, применяют ли они традиционные средства для защиты оконечных устройств или новые универсальные системы обеспечения безопасности. Это гарантированный путь к провалу, что регулярно подтверждают новости об очередной потере данных или взломе.

Чтобы иметь хотя бы минимальный шанс на эффективную защиту от современных атак, решение должно применять непрерывный анализ и анализ больших данных для отслеживания взаимодействия и действий файлов в сети, в физических и виртуальных средах, а также на защищаемых оконечных устройствах и мобильных устройствах. С учетом того, что многие атаки в период традиционного обнаружения пребывают в скрытом состоянии, возможность вернуться в прошлое и ретроспективно изменить статус файлов на вредоносный, а затем отследить их траекторию и индикаторы компрометации в организации позволяет более эффективно сдерживать изощренные атаки и устранять нанесенный ими ущерб.

Наконец, защита от усовершенствованного вредоносного ПО должна распространяться не только на оконечные устройства, но и на сети, мобильные устройства и виртуальные системы, чтобы гарантировать повсеместную и согласованную защиту в условиях, когда цель следующей атаки невозможно спрогнозировать.

Преимущества AMP следующие.

- Гибкое развертывание с применением согласованной политики на оконечных устройствах, в сети, на мобильных устройствах, на защищенных шлюзах и в виртуальных системах.
- Выявление и анализ атак на первых этапах, еще до того, как о них станет известно в отрасли,
  с помощью облака CSI.
- Возможность ретроспективно идентифицировать вредоносное ПО и отслеживать его траекторию для выявления всех его экземпляров в организации до начала распространения.
- Коллективный иммунитет для всех участников глобального сообщества Cisco AMP благодаря доступу к исследованиям на базе информации, полученной группой Talos, и образцов файлов, выявленных миллионами агентов AMP.

Чтобы включить решения Cisco AMP в свою программу оценки средств защиты, посетите веб-сайт http://www.cisco.com/go/amp.