Мониторинг и контроль для повсеместного предотвращения, обнаружения и устранения усовершенствованного вредоносного ПО

Обзор

Сегодня для успешного противодействия вредоносному ПО мало использовать только точечные решения. Чтобы преодолеть защиту и нарушить вашу среду, достаточно лишь одной угрозы. Кроме того, обнаружение в отдельный момент времени не позволяет оценить масштаб возникшего нарушения, а следовательно, и определить способ отражения и сдерживания угрозы.

Решение Cisco® для защиты от усовершенствованного вредоносного ПО (AMP) действует иначе. Это интегрированное решение предоставляет следующие преимущества.

- Доступ к базе глобальных аналитических данных по угрозам для усиления защиты сети.
- Модули углубленного анализа для блокировки вредоносных файлов в реальном времени.
- Возможность непрерывного анализа поведения файлов и трафика для быстрого обнаружения угроз.

Все эти возможности позволяют не только надежно обнаруживать потенциально опасную активность, но и быстро локализовать и устранять вредоносное ПО. Пользователь получает интегрированную защиту всей сети до, во время и после атаки.

Мир полон угроз

Киберпреступность проникает повсюду, деятельность хакеров прекрасно организована, а вредоносное ПО стало изощренным, незаметным и действует очень быстро

Хакерство – это индустрия, которая поддерживается сообществом профессиональных, предприимчивых и изобретательных киберпреступников. Они делятся друг с другом приемами, пользуются солидным финансированием и сообща достигают своих целей. Упорные и безжалостные, хакеры организуют автоматизированные, многовекторные атаки против определенных организаций.

Это динамичное и эффективное криминальное сообщество применяет разнообразные систематические методы с использованием усовершенствованного вредоносного ПО. Подобный код, включая полиморфные и адаптирующиеся к условиям программы, прекрасно маскируется и обходит традиционные средства защиты.

> Вопрос больше не в том, *возможно* ли нарушение безопасности, а в том, *когда* оно произойдет.

Так что вопрос больше не в том, *возможно* ли нарушение безопасности, а в том, *когда* оно произойдет. Вот лишь несколько цифр: 95 % организаций были атакованы вредоносным ПО.[1] Кража 60 % корпоративных данных совершается за несколько часов после атаки; 54 % нарушений безопасности остаются незамеченными многие месяцы, а 55 % организаций даже не могут определить источник атаки.[2] Чем дольше вредоносное ПО остается необнаруженным, тем больший ущерб оно причиняет: средний размер убытков от взлома в 2014 г. составил 5,9 млн долларов США, и этот показатель продолжает расти.[3]

Средства защиты от усовершенствованного вредоносного ПО не справляются со своей задачей

Если 54 % нарушений остаются незамеченными несколько месяцев и 55 % компаний даже не могут выявить причину нарушения, ясно, что используемые средства ИТ-безопасности неэффективны против современных угроз.

> 54 % нарушений безопасности остаются незамеченными многие месяцы.

Что же происходит?

Многие организации развертывают только антивирусные решения, традиционные межсетевые экраны и устаревшие системы предотвращения вторжений (IPS) для защиты своей среды. Эти точечные средства проверяют файл, как только он попадет в расширенную сеть, и сопоставляют его репутацию со списком известных вредоносных файлов. Заведомо вредоносные файлы блокируются. Если файл идентифицирован как безопасный или в базе нет сведений о нем, передача файла в сеть разрешается.

К сожалению, на этом анализ прекращается, и у организации возникают проблемы.

Учитывая то, что нам известно об усовершенствованном вредоносном ПО, файлы, считающиеся безопасными или поступившие из неизвестного источника, могут оказаться вредоносными, и точечные средства могут не выявить это. Сигнатура или аналитические данные по угрозам, указывающие на вредоносность файла, могут отсутствовать, либо код настолько эффективно маскируется под безвредный, что не поддается обнаружению. Даже при развертывании изолированной среды («песочницы») усовершенствованное вредоносное ПО может обойти ее при помощи полиморфизма или отложенной активации. Когда вредоносный код только проникает в сеть, точечные средства после первоначального обнаружения не позволяют оценить активность угроз. В результате у специалистов по ИТ-безопасности нет возможности продолжить мониторинг этих файлов и принять необходимые меры, если в дальнейшем файлы проявят вредоносное поведение.

1. Годовой отчет Cisco по безопасности за 2014 год
2. 2014: A Year of Mega Breaches («2014: год крупномасштабных нарушений безопасности»), Ponemon Institute.
3. Cost of a Data Breach, 2013/2014 («Цена утечки данных, 2013–2014 гг.»), Ponemon Institute.

Мониторинг и контроль для повсеместного предотвращения, обнаружения и устранения усовершенствованного вредоносного ПО

Использование нескольких различных средств обеспечения безопасности лишь ухудшает положение

Несмотря на недостатки точечных инструментов, организации используют все больше таких средств. Приобретая все новые и новые системы защиты, нередко организация накапливает по 40–60 различных решений для обеспечения безопасности, которые не работают и не могут работать вместе.

Разнородные продукты не всегда совместимы друг с другом. Это ухудшает обмен информацией до, во время и после атаки, а следовательно, и возможность оперативно обнаружить угрозы. Вместо того, чтобы сопоставлять данные и приоритизировать нарушения, помогая специалистам по безопасности выявлять наиболее серьезные и важные угрозы, подобные разнотипные средства ежедневно выдают сотни разрозненных или повторяющихся предупреждений, заставляя персонал выполнять ненужную работу. Средства безопасности должны работать сообща, помогая принимать более обоснованные решения и отсеивать ложные сигналы, а не увеличивать их число.

Кроме того, в среде с использованием нескольких продуктов требуется взаимодействие с несколькими поставщиками и несколько систем управления, одновременно обслуживаемых специалистами по ИТ-безопасности. В результате обнаружение угроз занимает больше времени, повышаются капитальные и эксплуатационные затраты и усложняется администрирование. В конце концов такой разрозненный подход не обеспечивает мониторинг, контроль и удобство управления для быстрого обнаружения и устранения угроз до того, как они нанесут ущерб.

Обнаружение вредоносного ПО и целенаправленных, непрерывных атак, которые оно осуществляет, — слишком сложная задача, чтобы ее можно было решить с помощью традиционных средств защиты или набора фрагментированных продуктов. Организациям необходим совершенно иной подход к проблеме безопасности. Защита от усовершенствованного вредоносного ПО должна иметь широкое распространение, как и вредоносное ПО, которому она противостоит.

Для отражения современных атак требуется интегрированный, расширенный подход к безопасности

Максимальное предотвращение

Итак, как решить проблему? Прежде всего предотвратите все возможные нарушения. Расширьте базу аналитических данных по угрозам, чтобы усилить защиту сети и блокировать больше заведомо вредоносных файлов. Примите меры против большинства вредоносных программ, атакующих вашу организацию. Оптимизируйте работу средств обнаружения, чтобы повысить их эффективность и быстрее выявлять угрозы. Несмотря на недостатки обнаружения в определенный момент времени, оно по-прежнему играет важную роль в устранении большинства потенциальных угроз.

Но следует смотреть правде в глаза: использование одной лишь стратегии предотвращения в конечном итоге приведет к провалу. Ни один метод обнаружения не является стопроцентно эффективным, поскольку злоумышленники постоянно совершенствуют свои приемы, чтобы обойти средства защиты на переднем крае. И в каком-то случае атака обязательно увенчается успехом.

Потребность в скорости: быстрое обнаружение, реагирование и восстановление

Кража **60 %** корпоративных данных совершается за несколько часов после атаки.

Необходимо принять тот факт, что взлом неизбежен. Вредоносное ПО стало изощренным, хакеры — продвинутыми, а атака может обойти средства первоначального обнаружения и другие превентивные меры. После возникновения нарушения стоит задача сократить время его обнаружения (TTD) и восстановления среды (TTR). Вредоносный код действует быстро, ставя под угрозу ваши конфиденциальные данные и критически важные системы. За несколько часов после взлома совершается кража 60 % данных. Чем дольше вредоносное ПО остается незамеченным в среде, тем больший ущерб будет причинен. Поэтому важно не только обнаружить, локализовать и устранить вредоносный код, но и сделать это максимально быстро.

Однако известно, что большинству организаций не удается отслеживать угрозы в своей среде. Не видя усовершенствованные угрозы, как можно обнаружить и устранить их? Как не попасть в заголовки завтрашних новостей?

Требуется постоянный и повсеместный мониторинг и контроль

Необходимо выйти за рамки возможностей точечных решений. Нужно быстро и эффективно обеспечить мониторинг и контроль: мониторинг — чтобы знать текущую обстановку в ИТ-среде, контроль — чтобы нейтрализовать обнаруженный вредоносный код. Но это недостижимо при использовании стратегии защиты в определенный момент времени. Мониторинг и контроль должны быть повсеместными и постоянными: для всех направлений атаки (оконечные устройства, мобильные устройства, Интернет, электронная почта, сеть) и на протяжении всего цикла атаки (до, во время и после нее).

Чтобы добиться этого, необходимо непрерывно собирать и анализировать телеметрические данные, не ограничиваться сигнатурами для выявления известных атак и на основе поведения файлов обнаруживать индикаторы компрометации, которые иначе остались бы незамеченными. Локальные данные нужно связать с глобальной аналитической базой для получения более полной информации о природе атаки. Эту информацию необходимо распространять среди многочисленных контрольных точек в среде, чтобы ускорить обнаружение и принятие надлежащих мер до того, как угроза будет реализована. Оконечные устройства должны взаимодействовать с сетевым устройством, оно в свою

очередь должно взаимодействовать с межсетевым экраном и т. д. Например, сетевые датчики могут автоматически проанализировать или заблокировать предположительно вредоносное ПО, обнаруженное на оконечном устройстве. Если одно средство обнаружило что-то подозрительное, все остальные компоненты тоже должны заметить это.

Зная, как действуют файлы и что именно они делают, можно идентифицировать их как вредоносные даже после атаки. Затем потребуется технология, способная быстро локализовать файлы и удалить их. Ответные меры могут быть различными, например выявление основной причины атаки, приоритизация событий по их масштабу и серьезности для более быстрой нейтрализации реальных угроз, одновременная деактивация всех точек компрометации и мест проникновения заражения для предотвращения обходных маневров злоумышленника. Все это нужно сделать очень быстро, чтобы свести ущерб к минимуму.

Повсеместный и постоянный мониторинг и контроль жизненно необходимы для реализации более системного и комплексного подхода к защите от угроз и эффективного обеспечения безопасности организации.

Представляем решение Cisco для защиты от усовершенствованного вредоносного ПО

Технология Cisco для защиты от усовершенствованного вредоносного ПО (AMP) реализует интегрированный, расширенный подход к безопасности, который вам нужен. Cisco AMP обеспечивает мониторинг и контроль не только для предотвращения нарушений и блокировки известных и новых угроз, *но и* для быстрого обнаружения, локализации и устранения вредоносного ПО, атаковавшего обширную сеть по нескольким направлениям. (См. рис. 1.)

Рис. 1. Непрерывный мониторинг и контроль

Защита организации до, во время и после атаки

ДО. Cisco AMP улучшает защиту до атаки благодаря лучшим **средствам анализа угроз и расширенной аналитике**. Располагая обширной библиотекой аналитических данных, известных вредоносных файлов и моделей поведения, можно выявить больше угроз при наблюдении, улучшить средства защиты и принимать более эффективные решения по обеспечению безопасности.

Технология Cisco AMP основана на непревзойденной базе аналитики угроз, данные для которой поступают от отдела информационной безопасности Cisco, группы по информационной безопасности и исследованиям Talos, а также по каналам Threat Grid. Cisco проверяет 35 % мирового трафика электронной почты, сканирует 100 Тбайт данных и 1,1 млн образцов вредоносного ПО в день и располагает группой аналитиков и исследователей угроз, которые круглосуточно снабжают AMP самыми свежими данными. Cisco AMP сопоставляет файлы, поведение, телеметрические данные и действия с этой обширной контекстной базой знаний, помогая быстро обнаруживать вредоносное ПО, лучше понять ситуацию, расставить приоритеты и блокировать сложные атаки.

ВО ВРЕМЯ. Cisco AMP объединяет аналитику с проверенными методами обнаружения, чтобы перевести **точечные средства защиты** на новый уровень. Проверка репутации файлов, сопоставление сигнатур, распознавание идентификационных отпечатков методами нечеткой логики, статический и динамический анализ с помощью технологии «песочницы» — все это входит в Cisco AMP в качестве первой линии обороны. Эти средства позволяют организациям автоматически блокировать максимум известных и новых угроз до их проникновения в сеть. При постоянном поступлении новых аналитических данных по угрозам система может блокировать известные вредоносные программы, типы файлов, нарушающие политику безопасности, динамические подключения из черного списка, о которых точно известно, что они вредоносные, а также блокировать попытки загрузки файлов с веб-сайтов и из доменов, отнесенных к категории вредоносных.

Но ни один метод обнаружения вредоносного ПО на определенный момент времени не обеспечит стопроцентную эффективность. Хотя такой подход играет важную роль, для современных решений по обеспечению безопасности его недостаточно. Cisco AMP не ограничивается проверкой в определенный момент времени, позволяя быстро обнаружить, локализовать и устранить даже самое неуловимое вредоносное ПО, если ему удалось обойти средства защиты на переднем крае.

ПОСЛЕ. в отличие от любой другой современной технологии Cisco AMP обеспечивает **непрерывный анализ и ретроспективную защиту**, помогая обнаружить вредоносное ПО даже после его проникновения в сеть. После того как файл пройдет через точку контроля безопасности, будет идентифицирован точечными средствами как безопасный или неизвестный и пропущен в сеть, система AMP продолжит следить за ним, тщательно анализируя каждое его перемещение в среде.

Мониторинг и контроль для повсеместного предотвращения, обнаружения и устранения усовершенствованного вредоносного ПО

AMP непрерывно ведет мониторинг, анализ и запись действий и коммуникаций всех файлов на оконечных устройствах, мобильных устройствах и в сети, что позволяет быстро выявить файлы с подозрительной активностью. При первом признаке проблемы система AMP ретроспективно предупреждает службу информационной безопасности, сообщая подробные сведения о специфике угрозы – как произошел инцидент, откуда поступило вредоносное ПО, где в сети оно успело побывать и какие действия пытается совершить. И самое главное, AMP затем дает возможность блокировать вредоносное ПО. На основании собранных и проанализированных доказательств можно классифицировать файл как вредоносный и удалить его.

Эта уникальная возможность Cisco AMP называется **ретроспективной защитой**. Она позволяет регистрировать действия каждого файла в системе. Если предположительно безопасный файл становится вредоносным, можно просмотреть записанную историю действий, чтобы определить источник угрозы и ее поведение с течением времени. Затем встроенные в AMP функции реагирования позволяют принять меры. Кроме того, система AMP фиксирует всю поступающую информацию – от сигнатуры угрозы до поведения файла – и заносит ее в базу данных аналитики угроз для усиления передней линии защиты. Этот вредоносный файл и ему подобные в следующий раз не останутся незамеченными.

Система AMP действует повсеместно, комплексно и во взаимосвязи с другими компонентами

Всесторонний мониторинг и контроль – именно то, что нужно для быстрого обнаружения и устранения скрытого вредоносного ПО. Но, кроме того, требуется отслеживать множество направлений атаки и распространять информацию между всеми элементами инфраструктуры безопасности для принятия быстрых и эффективных мер.

Технология Cisco AMP действует повсеместно. Ее можно развернуть в масштабе всей инфраструктуры безопасности или в определенных стратегических контрольных точках в зависимости от конкретных потребностей в защите. Есть множество способов использования данной технологии: на оконечных устройствах, в сети, на мобильных устройствах и в виртуальных средах. (См. табл. 1).

Здесь важно отметить взаимосвязанность, интеграцию всех этих решений и информационный обмен между ними. Это не отдельные изолированные продукты. Развернутые в комплексе, они совместно работают, обеспечивая интегрированную защиту для систематического и оперативного реагирования на угрозы. Создается целостная экосистема, посредством которой решения AMP автоматически распространяют аналитические данные по угрозам, индикаторы компрометации, информацию о событиях и карантине между всеми компонентами. Благодаря всеобъемлющему контролю, который обеспечивает AMP, организации могут существенно сократить TTD и TTR.

Таблица 1. Варианты развертывания

Решение	Развертывание
AMP for Endpoints	Защита компьютеров под управлением Windows, Mac, мобильных устройств на платформе Android, систем Linux и виртуальных сред с использованием компактного коннектора AMP, который не влияет на скорость работы пользователей.
AMP for Networks	Развертывание AMP как сетевого решения, интегрированного в устройства обеспечения безопасности Cisco FirePOWER™ NGIPS.
AMP на ASA с сервисами FirePOWER	Интеграция возможностей AMP в межсетевой экран Cisco ASA.
Виртуальное устройство AMP для частных облаков	Развертывание как локального изолированного решения, специально созданного для организаций с высокими требованиями к конфиденциальности, которые ограничивают использование общедоступного облака для поиска характеристик файла.
AMP на устройствах Email Security Appliance (ESA), Web Security Appliance (WSA) и Cloud Web Security (CWS)	В облачной системе защиты веб-трафика Cisco Cloud Web Security (CWS), на устройствах обеспечения безопасности электронной почты Email Security Appliance (ESA) и веб-трафика Web Security Appliance (WSA) функции AMP можно использовать для ретроспективного анализа вредоносного ПО.
AMP Threat Grid	AMP Threat Grid – это автономное решение для анализа вредоносного ПО и угроз, которое можно развернуть в облаке или в локальной среде. Аналитические данные по угрозам и средства углубленного анализа вредоносного ПО, предоставляемые Threat Grid, в разной степени встроены в другие варианты развертывания AMP.

Заключение

Для эффективной защиты от современных изощренных угроз требуется решение, которое отслеживает множество направлений атаки, обменивается информацией, снижает уровень сложности, повышает удобство управления и в конечном итоге обеспечивает организации тщательный мониторинг и контроль, необходимые не только для предотвращения нарушений безопасности, но и для быстрого обнаружения, локализации и устранения вредоносного ПО, если оно проникло в систему. Эти возможности предоставляет решение Cisco для защиты от усовершенствованного вредоносного ПО, обеспечивающее защиту организации до, во время и после атаки.

Дополнительная информация

Чтобы узнать больше о решении Cisco для защиты от усовершенствованного вредоносного ПО и о его преимуществах для вашей организации, посмотрите этот краткий видеообзор, ознакомьтесь с краткой или подробной демонстрацией технологии, послушайте мнение заказчиков, посмотрите сравнение AMP с конкурентами или свяжитесь с торговым представителем Cisco для планирования оценки с участием специалиста по Cisco AMP.

C11-735641-00 08/15