Cisco Advanced Malware Protection

Усовершенствованная защита Cisco® от вредоносного ПО (AMP) предлагает единственную систему усовершенствованной защиты от вредоносного ПО, охватывающую весь период атаки: до ее начала, во время ее проведения и после завершения. Система обеспечивает непрерывный анализ и расширенную аналитику, поддерживающие возможности ретроспективной безопасности Cisco. Ретроспективная безопасность дает администраторам возможность вернуться в прошлое для изучения угроз в системе с помощью таких инструментов как ретроспекция, взаимосвязь элементов цепочки атаки, поведенческие признаки вторжения (интегрированный центр управления), траектория и поиск нарушений. Благодаря этим инструментам ретроспективной безопасности можно определить масштабы, установить контроль в случае нарушения. Это позволяет команде по обеспечению безопасности быстро и эффективно устранять все угрозы в среде, прежде чем станет слишком поздно.

Почему точечная защита недостаточна для защиты вашей среды

Одни лишь точечные проверки никогда не будут эффективными на 100 процентов. Чтобы преодолеть защиту и нарушить вашу среду, достаточно лишь одной угрозы. Используя адресное, вредоносное ПО с учетом контекста, опытные злоумышленники имеют достаточно ресурсов, опыта и настойчивости, чтобы обойти средства точечной защиты и в любой момент создать угрозу для любой организации. Кроме того, средства точечной защиты совершенно неспособны определить масштабы и глубину нарушения после того, как оно возникло.

Функции Cisco AMP

В таблице 1 показаны функции Cisco AMP для сетей, AMP для оконечных устройств и AMP для содержимого. Основные функции обсуждаются в следующем разделе.

Таблица 1. Функции Cisco AMP

Характеристики	Контент	Сеть	Оконечное устройство
Репутация файла	✓	✓	✓
Изолированная среда	✓	✓	✓
Ретроспективное обнаружение	✓	✓	✓
Признаки вторжения		✓	✓
Анализ файлов		✓	✓
Траектория файла		✓	✓
Траектория устройства			✓
Гибкий поиск			✓
Контроль «эпидемии»			✓

Точечная защита

- **Репутация файла:** AMP получает сигнатуру каждого файла, поступающего на шлюз, и отправляет ее в аналитическую облачную сеть AMP для оценки его репутации, проверяемой на соответствие эксплойтам нулевого дня.
- **Изолированная среда для файлов:** при обнаружении вредоносного ПО AMP тщательно собирает мельчайшие детали о поведении файла. Затем AMP объединяет эти данные с подробным человеческим и автоматическим анализом, чтобы определить уровень угрозы файла в изолированной среде.

Ретроспективная безопасность

- **Непрерывный анализ:** возможности ретроспекции применяют непрерывный анализ и расширенную аналитику для того, чтобы заглянуть в прошлое и отследить процессы, активность файлов и связи, чтобы понять весь объем заражения, выявить исходную причину и произвести восстановление. Потребность в ретроспективном анализе возникает в случае каких-либо признаков нарушения, например при срабатывании триггера события, изменении в расположении файла или при срабатывании триггера интегрированного центра управления.

- **Мониторинг и контроль:** AMP решает проблему вредоносных файлов или угроз, не выявленных точечной защитой, благодаря тому, что постоянно анализирует и отслеживает поведение и деятельность сети. AMP предоставляет инструментальные панели и отчеты, которые быстро показывают место и объем нарушения, а также хронологию и основную причину заражения.

Collective Security Intelligence

Функции коллективной информационной безопасности от аналитического центра Cisco в сфере информационной безопасности и группы исследования уязвимостей (VRT) Sourcefire предоставляют самый большой в отрасли набор аналитической информации об угрозах в режиме реального времени с самым обширным мониторингом, объемом и возможностью использования через различные платформы обеспечения безопасности. (Sourcefire теперь является частью корпорации Cisco.) Например, у нас есть 1,6 млн датчиков, установленных по всему миру. Ежедневно мы получаем 100 ТБ данных и свыше 180 тыс. образцов файлов, а также имеем возможность отслеживать 35 процентов мирового трафика электронной почты. Над анализом этой информации, а также над публичной и частной передачей данных об угрозах работает свыше 600 инженеров, технических специалистов и исследователей, говорящих на 40 языках. Работа ведется круглосуточно, без перерывов и выходных. Постоянное взаимодействие с сообществами FireAMP™, Snort и ClamAV, а также участие в программе Sourcefire Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) позволяет нам делиться передовыми методами анализа угроз и восстановления. Благодаря этому мы лучше подготовлены к защите от будущих атак.

Основные преимущества AMP

- **Обеспечивает непрерывный анализ и последующие ретроспективные уведомления:** AMP информирует пользователей о зараженных файлах в случае изменения обнаружения вредоносного ПО после первоначального анализа. Решение отслеживает, анализирует и сопоставляет активность, чтобы обеспечить сотрудников отдела безопасности с результатами автоматизированного анализа и классификации рисков.
- **Защищает до и во время атаки:** интернет-репутация и интеллектуальные средства мониторинга угроз нулевого дня от аналитического центра Cisco в сфере информационной безопасности останавливают угрозы до того, как они проникнут в сеть. Репутация файла и изолированная среда позволяют обнаружить угрозы во время атаки.
- **Обеспечивает анализ и восстановление после атаки:** ретроспективная безопасность обеспечивает ретроспекцию, возможность использовать интегрированный центр управления, обнаружение вторжения, отслеживание, анализ и оперативную ликвидацию последствий после атаки, когда вредоносное ПО смогло ускользнуть от других средств защиты. Ретроспективные уведомления информируют о любом изменении ситуации, в том числе о том, кто и когда в сети мог быть заражен. Инструментальные панели точно показывают, где возникла угроза, что это была за угроза, и каковы ее основные причины, чтобы вы могли быстро сдержать и устранить ее.
- **Простые и гибкие возможности развертывания:** AMP можно активировать в решениях Email и Web Security Cisco всего лишь одним нажатием. Кроме того, в целях улучшения контроля AMP можно развернуть во встроенном режиме в качестве специального сетевого устройства, а также на оконечном устройстве в качестве небольшого коннектора.

Преимущества решений Cisco

Cisco предлагает высокий уровень защиты и гибкости развертывания, не имеющих себе равных в отрасли. Наши системы точечной и ретроспективной защиты вместе с комплексными коллективными мерами по информационной безопасности включают в себя уникальный и высокоинтеллектуальный набор преимуществ в постоянной борьбе с повышенными угрозами.

Дальнейшие шаги

Узнайте больше об усовершенствованной защите Cisco от вредоносного ПО. Для получения дополнительной информации обратитесь к торговому представители или торговому партнеру Cisco, или посетите http://www.cisco.com/c/en/us/solutions/enterprise-networks/advanced-malware-protection/index.html.

C45-731876-00 05/14