За пределами возможностей «песочницы»: повышение безопасности от периметра до оконечного устройства

Об этом документе

На протяжении многих лет все мы слышали о простых и, казалось бы, волшебных технологиях для решения проблем безопасности. Например, утверждалось, что, используя одну лишь технологию «песочницы», можно успешно противостоять усовершенствованному вредоносному ПО и направленным угрозам.

Эта статья дает ответы на следующие вопросы:

- Какое место занимает технология «песочницы» сегодня.
- Почему она не отвечает требованиям организаций.
- Что нужно для эффективного анализа вредоносного ПО.

Обзор

Веб-угрозы становятся все изощреннее, и их все сложнее обнаружить. Киберпреступники организуют атаки по разным направлениям. Их мишенями в том числе становятся приложения, которые пользователи считают надежными и безопасными. Число направленных атак растет, и в организациях постоянно присутствуют скрытые угрозы. Исследования Cisco показывают, что в 75 % случаев сама атака, направленная на кражу данных, занимает всего несколько минут, зато ее обнаружение занимает гораздо больше времени. Более 50 % всех атак остаются незамеченными на протяжении нескольких месяцев или даже лет. И если вторжение обнаружено, до полной локализации и устранения последствий может пройти несколько недель. За это время хакеры могут нанести серьезный ущерб.

Почему же обнаружение утечки данных занимает так много времени? Многим организациям недостает навыков, процессов и технологий для обнаружения и реагирования на инциденты. Для определения источника и масштаба атаки обычно требуется вручную провести анализ нарушения. Но решить эту проблему, просто увеличив штат специалистов по информационной безопасности, не получится: согласно годовому отчету Cisco по информационной безопасности за 2014 год, мировой дефицит таких работников составляет около миллиона человек.

Чтобы помочь отражать угрозы, проникшие в сеть, были созданы средства для динамического анализа образцов предполагаемого вредоносного ПО в безопасной среде («песочнице»). По мере развития этой технологии выделились три типовых способа развертывания решений на основе «песочницы»:

- Автономное решение, которое обычно установлено на сетевом тест-порте или порте анализатора. Оно самостоятельно получает образцы для анализа и не зависит от других продуктов для обеспечения безопасности.
- Распределенная система с датчиками, при котором возможности «песочницы» интегрированы в межсетевые экраны, систему предотвращения вторжений (IPS) или решения для унифицированного управления угрозами (UTM).
- Интеграция в защищенные шлюзы контента, например шлюзы веб-трафика или электронной почты.

Хотя у каждого варианта развертывания свои достоинства и недостатки, традиционные технологии «песочницы» обычно работают аналогичным образом и имеют одинаковые ограничения: они создают лавинный поток оповещений; их может обойти вредоносное ПО, отслеживающее окружающую обстановку; для получения отчетов требуются дополнительные ручные операции, а для интерпретации результатов анализа – опыт; недостаточные возможности восстановления. Пора усовершенствовать традиционные технологии «песочницы», дополнив ее автоматизацией, функциями учета контекста и поддержкой развертывания от периметра до оконечного устройства.

Что сегодня могут «песочницы»

На протяжении многих лет все мы слышали об универсальных технологиях для решения проблем безопасности. Например, утверждалось, что достаточно лишь «песочницы», чтобы успешно противостоять усовершенствованному вредоносному ПО и направленным угрозам. Неудивительно, что множество поставщиков систем безопасности включились в конкурентную борьбу и создали новый рыночный сегмент решений, направленных на обнаружение более изощренных атак (с которыми традиционные средства защиты уже не справлялись). Цель «песочницы» – организовать безопасную среду для обнаружения большего числа угроз, проникающих в сеть, и ускорить их анализ, чтобы эффективнее противодействовать им и снижать возможный ущерб. Но в реальности использование «песочницы» не всегда эффективно, и это доказывают несколько громких случаев взлома. В чем причина?

- Согласно полугодовому отчету Cisco по безопасности за 2015 год, разработчики вредоносного ПО научились обнаруживать «песочницы» и виртуальные машины. Для этого они используют специальные макросы, проверяют имена BIOS и некоторых файлов. Если вредоносное ПО распознает наличие «песочницы», оно выполняет маневр для самосокрытия и обхода этих средств защиты. Технологии «песочницы» генерируют множество оповещений, которые сложно упорядочить по приоритету, что может замедлить реагирование на критически важные угрозы.
- Не все подходы к «песочнице» одинаковы. Некоторые могут быть весьма дорогостоящими и сложными в масштабировании. Кроме того, они различаются по диапазону поддерживаемых операционных систем и файлов на целевых оконечных устройствах.

© Компания Cisco и/или ее дочерние компании, 2015. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

- «Песочница» является хорошим источником исходных данных, но подходит преимущественно для исследований. Как правило, она лишена удобных для пользователя возможностей отчетности. Данные необходимо подвергнуть экспертному анализу и коррелировать вручную, чтобы получить сведения об угрозе и оценить ее серьезность.
- Согласно результатам исследований Ponemon Institute, 41 % организаций не имеет автоматизированных средств для сбора аналитических данных и оценки реальной угрозы вредоносного ПО.

Учитывая этот факт, эксперты в области безопасности соглашаются в том, что «песочница» — не панацея. Некоторые поставщики решений для ИТ-безопасности понимают, что механизм «песочницы» лучше встраивать в другие свои продукты, чтобы они действовали как дополнительный уровень анализа и обнаружения. Такая система проверяет файлы уже после средств защиты от вредоносного ПО, систем IPS, защищенных шлюзов веб-трафика и межсетевых экранов. Для некоторых поставщиков «песочница» — лишь один из компонентов систем безопасности, который помогает выявлять вредоносные файлы. Другие поставщики сосредоточены исключительно на технологии «песочницы», предлагая заказчикам еще один отдельный продукт, неспособный взаимодействовать с множеством уже развернутых средств ИТ-безопасности.

Конечно, свою задачу «песочница» выполняет, но она не может быть источником актуальной информации о вредоносном коде. Она должна не увеличивать объем работы, а сокращать его. По-настоящему эффективный анализ вредоносного ПО дает возможность аналитикам первого уровня самостоятельно справиться с большим числом угроз без эскалации на третий уровень. Это требует интегрированного подхода, который повышает надежность за счет проверки данных и предусматривает автоматизацию для ускорения реагирования.

Почему существующий подход неэффективен

Хакерство уже превратилось в индустрию — киберпреступники становятся настоящими предпринимателями и профессионалами. Хакерам платят за взлом конкретных организаций и выполнение определенных задач, поэтому они демонстрируют невероятную целеустремленность и постоянно атакуют сразу с нескольких сторон. Они выбирают путь наименьшего сопротивления, но, потерпев неудачу, упорно продолжают совершенствовать приемы для достижения своих целей.

Традиционные «песочницы» не предназначены для современного мира динамических угроз. Это связано с тем, как они работают:

- Открывают файл в виртуальной среде, которая легко обнаруживается вредоносным ПО, отслеживающим окружающую обстановку.
- В качестве ответных действий просто добавляют угрозу в черный или белый список (то есть сообщают, является ли файл безопасным или вредоносным, но не дают контекста и не определяют, нужно ли продолжить отслеживание и мониторинг подозрительного файла).
- Не анализируют файлы, которые уже были обнаружены ранее.
- Легко вводится в заблуждение вредоносным ПО: оно может либо просто активироваться лишь через некоторое время после проникновения, либо сначала проверять характеристики хоста, а потом запускаться только в безопасных для себя условиях.

«Песочницы» делают среды более сложными и фрагментированными. Многие организации по мере необходимости устанавливают дополнительные инструменты защиты, накапливая по 40–60 разнотипных решений. Традиционные «песочницы» только усугубляют проблему, поскольку по своей природе создают слабые места в контроле и защите:

- В большинстве случаев «песочница» практически бесполезна: если это автономное или слабоинтегрированное решение (например, компонент межсетевого экрана), она не дает особых преимуществ для всей экосистемы безопасности.
- Некоторые подходы к защите от вредоносного ПО, основанные на «песочнице», весьма затратны и сложны в масштабировании:
  - Устройства большинства поставщиков необходимо устанавливать на каждой точке входа — только так они могут обеспечить полное покрытие сети.
  - Поскольку для каждого устройства существует свой вектор атаки, приходится развертывать несколько устройств для защиты веб-трафика, электронной почты, сети и оконечного оборудования. Заказчики, по сути, создают еще одну сеть, затратную в развертывании и сложную в управлении.
- «Песочницы» предоставляют не так уж много данных — обычно это лишь информация об угрозах и список вредоносных IP-адресов. Они не дают общего представления об обстановке, поэтому не позволяют выявлять тенденции и узнавать об угрозах заранее. А поскольку эти решения не являются интегрированными, они неспособны сопоставлять локальные аналитические данные или результаты анализа корпоративной инфраструктуры, что не дает возможности определить масштабы атаки и ее серьезность для организации.

© Компания Cisco и/или ее дочерние компании, 2015. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Новая эра в анализе вредоносного ПО

Эти недостатки могут иметь серьезные последствия для компаний, но чтобы преодолеть их, требуется более эффективный подход к анализу вредоносного ПО. Он должен объединять лучшее из традиционных методов и передовые технологии, помогая организациям успешно противостоять злоумышленникам, которые пользуются солидным финансированием и постоянно совершенствуют свои приемы.

Оптимизированный рабочий процесс

Схема рабочего процесса приведена на следующем рисунке. Система защиты в этом процессе должна выполнять следующие функции:

Рис. 1. Рабочий процесс анализа вредоносного ПО

1. Автоматизировать отправку сведений из нескольких точек мониторинга безопасности, включая сеть и оконечные устройства.
2. Открывать подозрительные файлы в защищенной виртуальной или эмулированной среде для установления истинного назначения файла.
3. Эффективно использовать приемы статического и динамического анализа и последующей обработки для обеспечения максимально возможного качества данных.
4. Интегрироваться в существующую экосистему безопасности с помощью API-интерфейсов, охватывая множество направлений атаки, обеспечивая автоматическое реагирование и реализуя подход к защите, ориентированный на угрозы.
5. Обеспечивать простое извлечение и использование данных другими средствами мониторинга и анализа.
6. Обеспечивать баланс между точностью и масштабируемостью данных, поддерживая растущее число методов анализа, образцов и данных без увеличения времени обработки.
7. Проводить анализ в удобном формате с учетом контекста для определения приоритетов ответных мер.
8. Сопоставлять текущие угрозы со статистическими данными для разработки более эффективных планов и средств реагирования.

Важность контекста

Значение контекста невозможно переоценить. Когда организация подвергается атаке злоумышленников, контекст исключительно важен для того, чтобы локализовать реальную угрозу и ускорить ответные меры. Контекст помогает выявить вредоносное ПО, которое способно обходить традиционные «песочницы» и может сохраняться в организации незамеченным многие месяцы или даже годы. Традиционная технология «песочницы» учитывает далеко не все происходящее в инфраструктуре организации или в окружающем мире. Это просто среда для проверки и анализа подозрительных файлов. Однако добавление контекста помогает отделу безопасности получить более полную картину и быстрее принять решительные меры.

Преимущества контекстного анализа вредоносного ПО:

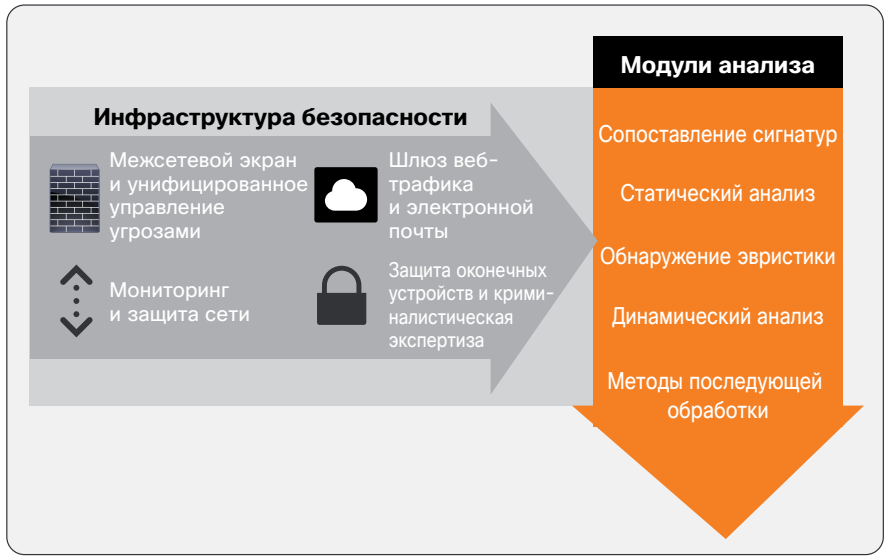
- Анализ структуры кода файла и его запуск в виртуальной среде.
- Исключение тех характеристик виртуальной машины, которые могут обнаруживаться вредоносным ПО, оценивающим окружающую обстановку.
- Анализ каждого образца, даже если его контрольная сумма уже известна, что позволяет отслеживать изменения со временем.
- Предоставление контекстной информации для образца на основе региона или сходства с другим вредоносным ПО.
- Обеспечение оценки угроз и степени их опасности для определения серьезности по отношению к конкретной среде.
- Объединение глобальной коллективной аналитики, поведенческих индикаторов компрометации, каналов аналитической информации по угрозам и других ресурсов для идентификации образца как вредоносного, подозрительного или безопасного.
- Комплексное противодействие угрозам до, во время и после атаки.

Четвертый вариант развертывания: от периметра до оконечного устройства

Основу оптимизированного рабочего процесса и контекстного анализа вредоносного ПО составляет интегрированный, ориентированный на угрозы подход к безопасности. В этом случае анализ вредоносного ПО является неотъемлемым компонентом архитектуры безопасности. Решение охватывает все уровни – от межсетевого экрана до защищенных шлюзов электронной почты и веб-трафика, систем защиты сети и средств обеспечения безопасности оконечных устройств. В процессе передачи файла в место назначения выполняется несколько проверок. Есть несколько вариантов развертывания: ПО как услуга, лицензированный программный продукт, который можно установить на существующем устройстве обеспечения безопасности, или автономное устройство для анализа вредоносного ПО. (См. рис. 2.)

© Компания Cisco и/или ее дочерние компании, 2015. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Рис. 2. Анализ вредоносного ПО от периметра до оконечного устройства



В каждой точке своего пути, от межсетевого экрана до оконечного устройства, файл подвергается проверке. Здесь возможно несколько результатов: файл определяется как вредоносный (блокируется), как заведомо безопасный (доставляется конечному пользователю) или как неизвестный (передается в следующую контрольную точку). Если, достигнув оконечного устройства, файл по-прежнему считается неизвестным, он автоматически направляется на анализ вредоносного ПО, который проводят несколько модулей. Кроме того, в фоновом режиме запускается функция для проверки поведенческих признаков с использованием глобальной аналитики и статистических данных. Если файл, ранее считавшийся безопасным, теперь идентифицирован как вредоносный, пользователь получает уведомление.

Система возвращает решение с оценкой угрозы, помогая определить ее серьезность и назначить приоритеты для ответных действий. Если файл определен как заведомо вредоносный, он автоматически блокируется и заносится в черный список. Если файл прошел все предыдущие проверки и позднее был идентифицирован как вредоносный, то интегрированный, ориентированный на угрозы подход к безопасности позволяет проследить траекторию файла, поместить в карантин все зараженные устройства, выполнить восстановление в автоматическом режиме или вручную, а затем снова подключить устройства к сети. Эта возможность, называемая ретроспективной защитой, играет важную роль в сокращении времени обнаружения (TTD) и ускорении восстановления.

Анализ вредоносного ПО в действии в Центре интернет-безопасности

Центр интернет-безопасности (CIS), на базе которого действует Межрегиональный центр обмена информацией и анализа (MS-ISAC), – это некоммерческая организация, которая круглосуточно предоставляет услуги по кибербезопасности своим 19 000 участникам, включая региональные, территориальные и другие органы власти. С ростом числа атак со стороны государственных субъектов CIS потребовалось решение, способное помочь Центру предоставлять услуги по автоматическому анализу вредоносного ПО в больших масштабах с учетом контекста, чтобы идентифицировать образец как вредоносный, подозрительный или безопасный и определить причины той или иной оценки. Участникам CIS нужно было автоматически анализировать вредоносное ПО в надежной среде, не отправляя образцы в общедоступный домен, за которым злоумышленники могут следить и изменить свои методы, узнав о ведущемся расследовании.

Масштабируемая инфраструктура должна была иметь возможность обрабатывать образцы вредоносного ПО, полученные от тысяч организаций по всей стране. Используя многофункциональный API-интерфейс, CIS организовал особый портал для решения Cisco AMP Threat Grid с эффективными средствами управления доступом. Центр создал сообщества, чтобы группы реагирования на инциденты могли получать полную картину угроз для конкретных образцов вредоносного ПО, не распространяя информацию среди более широкой аудитории. Специалисты могут провести поиск по множеству разных типов признаков и отобрать все образцы с одним и тем же индикатором. За несколько минут участники CIS получают контекст, который помогает им определить, что именно будет выполнять вредоносное ПО, а также оценить масштабы угрозы и выработать способы защиты.

© Компания Cisco и/или ее дочерние компании, 2015. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Контрольный список оценки технологий для анализа вредоносного ПО

При оценке технологии «песочницы» следует обдумать следующие аспекты, чтобы выбрать более эффективный подход к анализу вредоносного ПО, обеспечивающий оптимизированный рабочий процесс, учет контекста и гибкость развертывания, а в конечном итоге действенную защиту.

- **Варианты развертывания.** Для использования «песочницы» нужны и облачные, и локальные средства анализа, поскольку в строго регулируемых отраслях предъявляются более высокие требования к конфиденциальности и соблюдению нормативов. Следует искать решения, обеспечивающие гибкость развертывания в соответствии с потребностями вашей организации.
- **Масштабируемость.** Организации, решающие вопрос развертывания технологий «песочницы», должны оценить масштабируемость каждого потенциального решения. Если для него требуется создавать дополнительную наложенную сеть, развертывание и администрирование такого решения могут быть дорогостоящими и сложными.
- **Эффективность.** Необходимо понять, какие средства потребуются для максимально эффективного использования технологии для ускорения обнаружения, анализа и восстановления.
- **Пригодность.** Организации должны убедиться, что потенциальные поставщики технологии могут воссоздать ключевые компоненты и конфигурации оконечных устройств и изучить типы файлов, которые используются в корпоративной среде.
- **Интеграция.** Следует понять, как решение интегрируется и обменивается информацией с другими системами ИТ-безопасности в корпоративной среде. Это поможет не только ускорить обнаружение и реагирование во время и после атаки, но и предотвратить аналогичные атаки путем автоматического обновления политик.

Заключение

Злоумышленники не ограничиваются единственным приемом для достижения своих целей. Поэтому и специалисты по безопасности не должны полагаться исключительно на динамический анализ вредоносного ПО («песочницу») для защиты среды. Однако можно повысить эффективность каждого компонента защиты, сделав его неотъемлемой частью подхода к безопасности, ориентированного на угрозы.

Главными составляющими стратегии защиты должны быть мониторинг, учет контекста на основе локальных и глобальных аналитических данных по угрозам и контроль с помощью анализа и автоматизации. Это обеспечит защиту от угроз независимо от того, где и когда они будут обнаружены.

Дополнительная информация

Для получения дополнительных сведений о решении Cisco для защиты от усовершенствованного вредоносного ПО посетите веб-сайт: http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html.

Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками компании Cisco и/или ее дочерних компаний в США и других странах. Чтобы просмотреть список товарных знаков Cisco, перейдите по ссылке www.cisco.com/go/trademarks. Товарные знаки сторонних организаций, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает отношений партнерства между Cisco и любой другой компанией. (1110R)

C96-735492-00 07/15