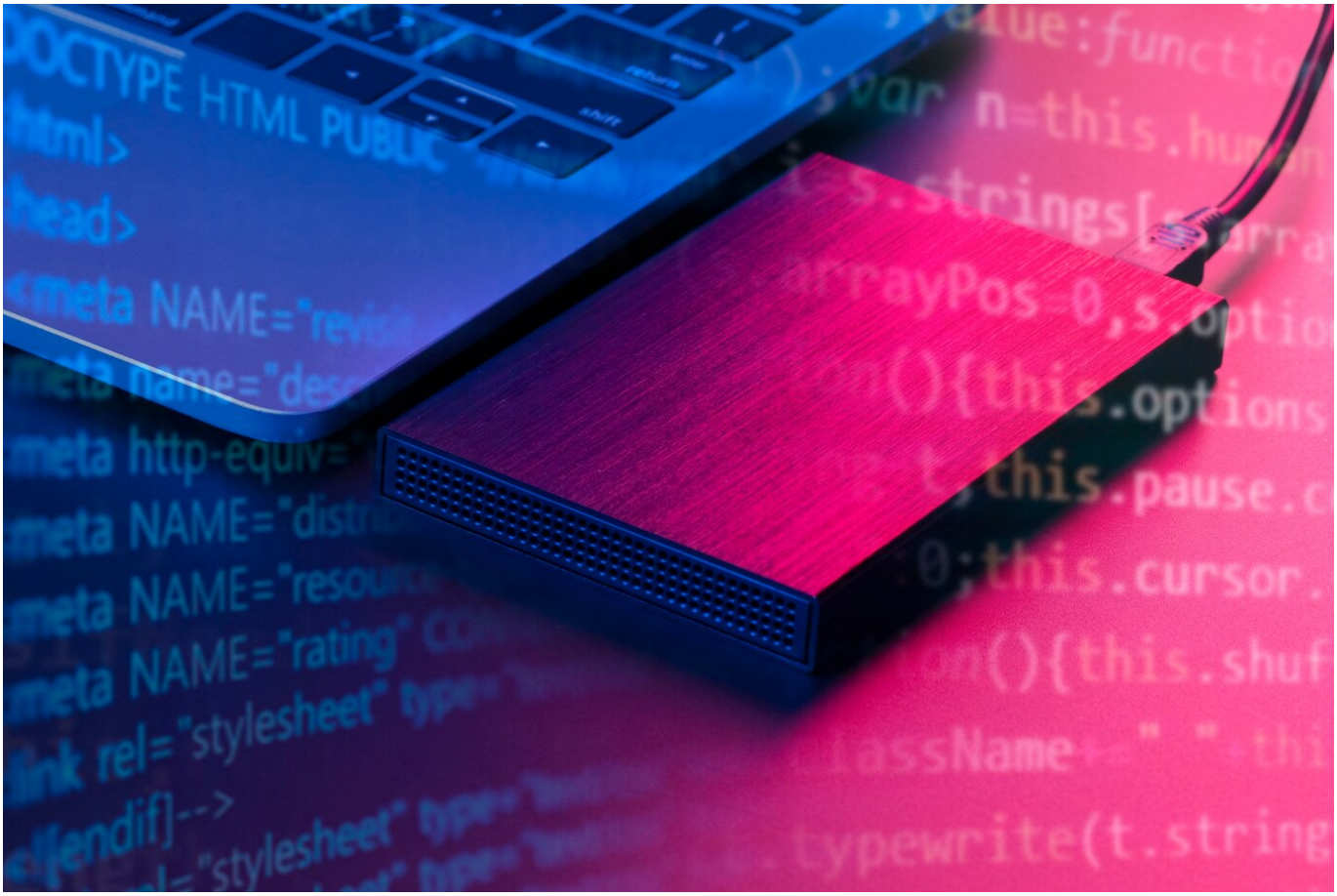
Как защитить программное обеспечение от пиратства: возможности Sentinel LDK Envelope



Как это работает

Пакеры — определение и использование
Пакер, как следует из названия, представляет собой инструмент, который модифицирует исполняемые файлы и создает новые эквивалентные файлы с целью сжатия или в качестве метода защиты от реверс-инжиниринга. В процессе упаковки к исходному исполняемому файлу добавляется защитный код, который «распаковывает» программу или ее части перед выполнением на ПК. Этот код, далее именуемый LDK Envelope Runtime, необходим для запуска защищенного приложения и отвечает за такие задачи, как защита от отладки, обнаружение трассировки, управление лицензиями и проверка анкетных данных.
Инструмент сочетает в себе шифрование и обфускацию кода для максимальной эффективности решений по упаковке файлов для защиты от копирования и защиты интеллектуальной собственности.

Sentinel LDK Envelope — простое в использовании решение, работающее в один клик
Sentinel LDK Envelope защищает приложение, добавляя “щит”, отвечающий за привязку приложения к аппаратным, программным или облачным ключам защиты (ключи HL, SL и CL соответственно).
Защита приложения с помощью Sentinel LDK Envelope — это процедура, которая занимает всего несколько секунд и предоставляет чрезвычайно мощное решение для поставщиков программного обеспечения практически без каких-либо усилий.
Пакеры также могут использоваться дистрибьюторами ПО, которые не имеют доступа к исходному коду приложения. Например, продавец ПО может защитить приложение, не привлекая разработчиков к защите программного обеспечения. Такая схема может быть использована дистрибьюторами и реселлерами, которые хотят защитить программное обеспечение для своего местного рынка, а ПО разрабатывается в другой стране.
При запуске защищенного приложения LDK Envelope Runtime пытается войти в систему с помощью лицензии LDK и, в случае успеха, использует шифрование ключей защиты HL, SL или CL для расшифровки приложения или его частей в памяти. Если ключ защиты Sentinel отсутствует или лицензия недействительна, бинарный файл не может быть расшифрован в памяти, и приложение не может запуститься. Если ключ или лицензия становятся недействительными во время выполнения, приложение останавливается - таким образом, нельзя запустить ПО несколько раз на разных ПК с одним и тем же ключом.
Sentinel LDK Envelope — это автоматический упаковщик файлов, который обеспечивает защиту от реверс-инжиниринга программного обеспечения посредством шифрования файлов с помощью технологии « », запутывания кода и защиты от отладки. Процесс упаковки (или обертывания) двоичных файлов (исполняемых файлов и библиотек) создает прочную связь между системой лицензирования и приложением, обеспечивая максимальную защиту от копирования.

Утилита шифрования файлов данных

Помимо защиты исполняемого файла приложения (например, EXE), также доступно и шифрование файлов с данными, к которым обращается приложение. Это обеспечивает защиту интеллектуальной собственности и создает дополнительный уровень безопасности между взломщиком (хакером, который пытается снять защиту) и интеллектуальной собственностью программного обеспечения. Утилита Sentinel LDK Data Protection в сочетании с Sentinel LDK Envelope использует шифрование файлов данных для предварительного шифрования, которые затем шифруются или дешифруются защищенным приложением. После этапа шифрования (выполняемого с помощью утилиты Sentinel LDK Data Protection) доступ к файлам данных возможен только при наличии подходящего ключа защиты для приложения, защищенного Envelope, во время его выполнения.
Для расшифровки определенных файлов данных могут потребоваться специальные лицензии, что дает поставщику или разработчику контента возможность лицензировать документы, медиафайлы и другой контент независимо от лицензирования самой программы.

Описание

Sentinel LDK Envelope обеспечивает надежную защиту интеллектуальной собственности от реверс-инжиниринга благодаря использованию таких передовых функций, как шифрование файлов,

обфускацию кода, защита от отладки, AppOnChip (выполнение части кода на ключе) и другие. Реализация этих дополнительных технологий защиты делает взлом защиты очень сложным и трудоемким для хакеров, тем самым обеспечивая прочную привязку программного кода к лицензии конечного пользователя. Каждая функция борется с различными методами, которые хакеры используют при попытке обойти защиту приложения.

Защита самого слабого места

Самым уязвимым местом в приложении, защищенном любым механизмом упаковки, является стык между файлом приложения и добавленным кодом защиты. Это место, которое, после обхода, разорвет связь с ключом защиты, содержащим лицензию, оставив приложение полностью незащищенным. Следовательно, это место, которое большинство злоумышленников будут пытаться атаковать. Злоумышленники изучают защищенный файл, анализируя код защиты и то, как он связан с ключом защиты. Как только они поймут код и определят его нахождение, они могут попытаться действовать одним из следующих способов:

1. Взлом конкретного приложения — разрыв связи защиты для конкретного файла приложения.
2. Общий взлом — создание поддельной лицензии, которая работает со всеми приложениями, зависимыми от нее для выполнения, или разрыв связи защиты для всех других файлов, защищенных тем же механизмом, если в них повторяется один и тот же метод. Поэтому очень важно, чтобы соединение между защищенным файлом и добавленным кодом защиты было неоднозначным и неотслеживаемым, что требует длительной и утомительной процедуру для любого, кто пытается понять механизм защиты. Одной из самых сильных сторон Sentinel LDK Envelope является его способность защищать это соединение и создавать препятствия и ловушки, которые не позволяют разорвать описанную выше связь.

Всё это достигается путем изменения частей кода приложения, чтобы во время выполнения требовался код LDK Envelope Runtime. Удаление LDK Envelope Runtime помешает правильной работе приложения, а его дебаг чрезвычайно затруднён, поскольку схема сильно запутывает и использует проверки целостности, которые предотвращают модификацию.
Кроме того, при защите приложений .NET и Java Sentinel LDK Envelope обеспечивает защиту на уровне методов, где методы дешифруются во время выполнения, точно в нужное время. Это может быть применено к любому количеству методов, используемых хакерами, и обойти это чрезвычайно трудоёмко.
Sentinel LDK Envelope автоматически выбирает для защиты только те методы, которые с меньшей вероятностью повлияют на производительность, а разработчик может переопределить и отменить выбор или выбрать определенные методы или классы в случае особых требований к безопасности или производительности. Для нативных бинарных файлов Envelope использует другой подход, если производительность критична, позволяя поставщику программного обеспечения настраивать процент кода, который шифруется. Однако обычно это не является проблемой, и защищенные нативные приложения работают так же быстро, как и их незащищенные версии.
Sentinel LDK Envelope также обеспечивает еще один уровень защиты для этих приложений — шифрование на уровне сборки (защита оболочки Windows) и шифрование на уровне классов для Java. Это дает преимущество в виде обезвреживания декомпиляторов и других инструментов реверс-инжиниринга (РИ), поскольку зашифрованные файлы больше не распознаются инструментами РИ как корректные сборки .NET или файлы классов Java.
Защищенные файлы не имеют никакого сходства между собой, даже если исходные файлы полностью идентичны.

Код LDK Envelope создается динамически во время защиты. Он содержит секретные данные разработчика и каждый раз зашифрован по-разному. Это значительно затрудняет “ковыряние” кода злоумышленниками и делает бесполезным использование дисассемблеров для анализа механизма защиты или дисассемблированного кода.
Код Envelope Runtime может увеличить размер бинарника, но в большинстве случаев это увеличение незначительно по сравнению с исходным размером. В некоторых случаях сжатие файла от Envelope может даже уменьшить размер двоичного файла.
Благодаря шифрованию двоичного файла, добавлению проверок лицензий, обнаружению и пресечению попыток взлома, а также реализации мер, затрудняющих анализ защищенных программ, Sentinel LDK Envelope является инструментом выбора для защиты программного обеспечения от неправомерного использования и защиты ценных алгоритмов и коммерческой тайны от посторонних глаз.

Методы защиты от отладки и отслеживания

Обычно отладчики используются разработчиками программного обеспечения для устранения ошибок и отслеживания проблем в процессе разработки приложений. Однако взломщики, пытающиеся получить незаконный доступ к программному обеспечению, используют те же отладчики для обнаружения и отслеживания встроенного защитного кода с конечной целью его изменения, отключения или полного удаления.
Чрезвычайно мощной функцией Sentinel LDK Envelope является его механизм защиты от отладки, который постоянно находится “начеку” в поисках активных отладчиков. Приложения, работающие под контролем отладчика, ведут себя немного иначе. Envelope обнаруживает и использует этот факт, делая отладчики неэффективным инструментом для анализа приложения с целью удаления защиты. Sentinel LDK Envelope разработан таким образом, чтобы обнаруживать запуск инструментов противодействия отслеживанию и при необходимости останавливать работу защищенного приложения.
Поскольку и взломщики, и разработчики используют одни и те же инструменты отладки, Sentinel LDK Envelope должен иметь возможность различать отладочную деятельность легитимного разработчика и деятельность лица, намеревающегося нанести вред. Это достигается путем отображения сообщения о том, что обнаружен отладчик, и предотвращения загрузки защищенного приложения. Разработчик не будет пытаться обойти это сообщение, а вместо этого будет использовать незащищённое приложение для легитимной отладки. Однако, если эта проверка отладчика обойдена, то это явно является действиями злоумышленника, пытающегося снять защиту ПО, и, следовательно, приложение останавливается.

Обнаружение попыток взлома

Sentinel LDK Envelope использует дополнительные методы для обнаружения попыток взлома. Например, Envelope оставляет в двоичном файле «ловушки», которые включают код, который в обычной работе никогда не выполняется. Если взломщик прощупывает эти пути выполнения кода, это является явным признаком взлома, который может привести к отключению ключа или приложения.

Особенности и преимущества Sentinel LDK Envelope:

1. Автоматический упаковщик файлов — обеспечивает надежную защиту от обратной разработки программного обеспечения посредством шифрования файлов шифрование файлов и запутывание кода.
2. Безопасный канал связи — Sentinel LDK Envelope исключает атаки типа «человек посередине (MITM)», обеспечивая безопасный канал связи между защищенным приложением и ключом защиты.
3. Расшифровка во время выполнения — функции расшифровываются во время выполнения, точно в нужное время, что гарантирует, что приложение не может быть полностью скопировано из памяти.
4. Поддержка нескольких платформ — Sentinel LDK Envelope обеспечивает безопасность ваших приложений, гарантируя надежную защиту от копирования и защиту от реверс-инжиниринга на нескольких платформах: Windows (x86, x86_64); Linux (x86, x86_64, ARM), Mac (x86_64).

Приложения .NET и Java поддерживаются на нескольких операционных системах.
Sentinel LDK Envelope позволяет поставщикам программного обеспечения шифровать определенные части приложения или весь файл приложения — это одна из многих опций настройки, которая позволяет поставщикам программного обеспечения адаптировать защиту к своим индивидуальным потребностям.
Защищенное приложение подписывается цифровой подписью. Во время выполнения подпись проверяется, чтобы убедиться, что весь двоичный файл (как код, так и ресурсы) не были изменены.

Защита целостности программы

Envelope совместима с подписями Microsoft Authenticode. Обе могут применяться к бинарному файлу без взаимной интерференции.

Автоматическое отключение ключа

Очень эффективным ответом на попытку взлома является отключение ключа защиты, что останавливает взломщиков. Эта функция поддерживается ключами Sentinel HL Driverless и CL и может быть отменена поставщиком — ключ может быть повторно включен, если пользователь предоставит убедительную причину для повторного доступа к ключу, после чего поставщик предоставляет файл обновления с цифровой подписью, который повторно включает ключ. Хотя отключение ключа не включено по умолчанию, его настоятельно рекомендуется использовать для повышения безопасности. По опыту Thales, отключение ключа крайне редко приводит к ложному срабатыванию системы обнаружения — за годы с момента внедрения этой функции не было зарегистрировано ни одного такого случая.

Автоматическое отключение приложения

Для ключей Sentinel SL, где отключение ключей не может быть эффективно реализовано, Sentinel LDK Envelope использует альтернативную технику. При обнаружении попытки взлома (например, с помощью проверки целостности) поведение программного обеспечения искажается (добавляется задержка), что нарушает логическую связь между «причиной» и «следствием». Задержка реакции сбивает взломщика с толку, затуманивая истинную логическую связь между попыткой взлома и отрицательной реакцией программного обеспечения на эту конкретную попытку (например, приложение может завершить работу с внутренней ошибкой).

Библиотеки API, специфичные для производителя

Большинство поставщиков средств защиты программного обеспечения предоставляют всем клиентам одну и ту же библиотеку API, что делает эту библиотеку единственной точкой отказа в случае

нарушения безопасности. Thales использует гораздо более безопасное решение — библиотеки API, специфичные для каждого поставщика. Эти библиотеки API создаются и настраиваются на серверах, вдали от посторонних глаз взломщиков. Они гарантируют, что каждый поставщик получает структурно отличающийся компонент для интеграции в свое приложение. В рамках этого процесса библиотеки API, которые настраиваются индивидуально для каждого поставщика программного обеспечения, дополняются уникальными секретами криптографии «белого ящика» и, наконец, проходят через обфускацию кода и другие методы защиты. Полученные в результате библиотеки API практически невосприимчивы к общим взломам и гарантируют, что, как правило, взломщики не могут добиться успеха, взломав библиотеку API одного поставщика, и затем рассчитывать на успех в отношении других поставщиков. Sentinel LDK Envelope извлекает эти специфичные для поставщика библиотеки API из копии загруженных API на компьютере разработчика и связывает их с приложением во время защиты. Эти надежно защищенные специфичные для поставщика API затем используются Envelope во время выполнения, чтобы обеспечить законный доступ защищенного приложения к ключу защиты.

Множественные вызовы ключа защиты Sentinel, автоматически интегрированные Sentinel LDK Envelope

Изобретательность Sentinel LDK Envelope заключается в том, что он применяется к скомпилированному файлу, что гарантирует отсутствие необходимости в изменении исходного кода приложения. Вызовы ключа защиты периодически выполняются кодом защиты (LDK Envelope Runtime), который добавляется к файлу приложения. Envelope позволяет интегратору безопасности поставщика ПО указывать и настраивать интервалы времени, с которыми проверяются ключи защиты Sentinel, проверяя их наличие с помощью криптографических средств. Это лишь один из многих параметров, которые поставщик может полностью настроить для использования на этапе защиты.

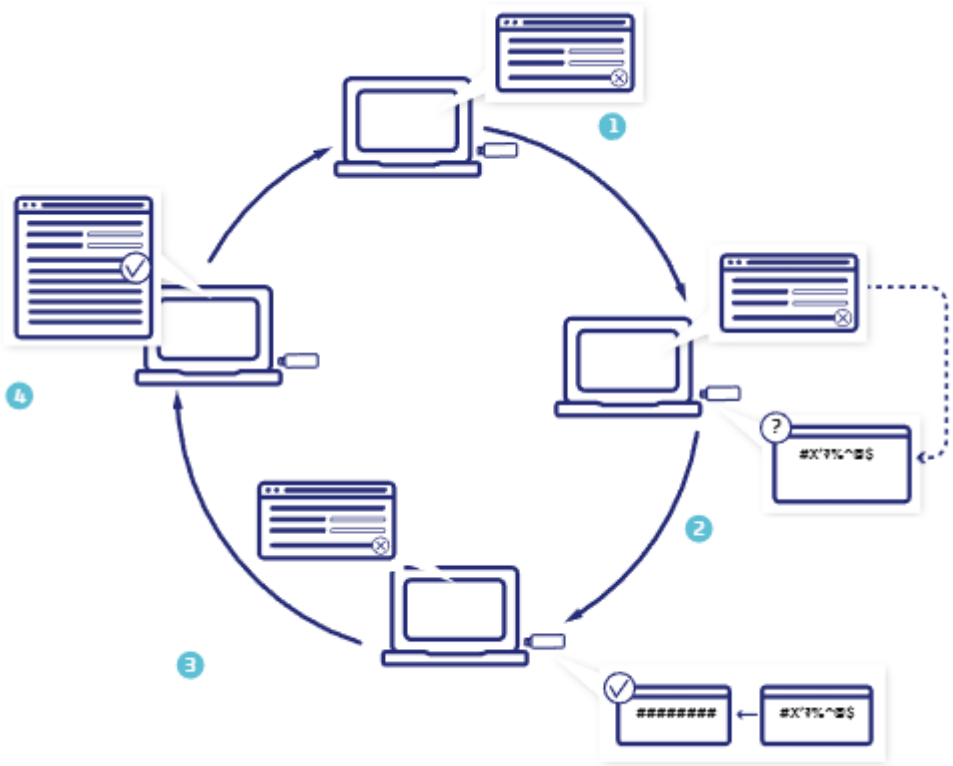
Криптография White-Box

Thales является первопроходцем в отрасли по использованию криптографии White-Box для полного шифрования канала связи в качестве средства предотвращения понимания злоумышленниками связи между защищенным приложением и ключом защиты. Безопасная связь по каналу на основе White-Box использует компоненты, специфичные для поставщика, гарантируя, что ключ шифрования безопасного канала не может быть извлечен из защищенных двоичных файлов, независимо от того, используется ли динамическая или статическая атака.

AppOnChip

Одна из самых передовых и инновационных функций Sentinel LDK Envelope от Thales, AppOnChip, обеспечивает практически неразрывную связь аппаратного ключа Sentinel с приложением, предоставляя поставщикам программного обеспечения самое безопасное из доступных решений для защиты программного обеспечения.
Этот (полностью автоматизированный) процесс предоставляет поставщику программного обеспечения список функций из его приложения, содержащих блоки кода, совместимые с функцией AppOnChip. Защищенные блоки кода, зашифрованные и подписанные, могут затем загружаться и выполняться на самОм аппаратном ключе. Эта дополнительная мера безопасности делает его самым безопасным решением для лицензирования программного обеспечения на рынке. Особенности и преимущества AppOnChip включают в себя повышенную безопасность, простоту внедрения и отсутствие нагрузки ОС, поскольку зашифрованный код отправляется на ключ для выполнения во время работы и не требует предварительной загрузки.
Функция AppOnChip доступна в Windows для нативных и .NET-приложений, защищенных с помощью ключей HL Driverless. Доступен автоматический профилировщик производительности во время

выполнения, который помогает поставщикам найти баланс между безопасностью и производительностью интеграции AppOnChip.



1. Приложение работает в обычном режиме, пока не доходит до функции, защищенной AppOnChip;
2. Приложение динамически загружает защищенный код, а затем безопасно выполняет его на ключе;
3. AppOnChip возвращает результаты выполненного кода обратно в приложени;
4. Приложение использует результаты в рамках своего нормального потока.

Защита исходной точки входа (OEP)

Оригинальная точка входа (original entry point, OEP) — это адрес запуска любого приложения, с которого операционная система (ОС) начинает выполнять приложение. Чтобы распаковать защищенное приложение, взломщики должны найти этот адрес, удалить код упаковщика и попытаться запустить приложение из оригинальной точки входа приложения.
В отличие от многих упаковщиков, Sentinel LDK Envelope удаляет инструкции исходной точки входа из их стандартного местоположения и распределяет их по коду LDK Envelope Runtime. Взломщик, пытающийся найти и восстановить исходную точку входа из распределенных фрагментов, столкнется с затруднением, поскольку это практически невозможно, учитывая случайность расположения и размера фрагментов.

Защита на уровне методов

Sentinel LDK Envelope усиливает защиту двоичных файлов .NET и Java, определяя защиту на уровне методов. Когда для защиты выбирается сборка .NET или архив Java, Envelope автоматически определяет методы, доступные для индивидуальной защиты. Это позволяет поставщику выбирать, какие методы защищать и как, что обеспечивает максимальный уровень защиты при минимальном влиянии на производительность.
Sentinel LDK Envelope обеспечивает готовую к использованию первоклассную безопасность, не требуя от вас затрат времени и усилий на разработку решения с нуля, позволяя вашим инженерным командам сосредоточиться на своих основных компетенциях.

Удаление таблицы импортных адресов

Дополнительным средством обхода попыток взлома native-бинарников Windows является удаление таблицы импортных адресов, которая содержит адреса функций во внешних DLL, используемых защищенным приложением. В процессе упаковки исходного приложения таблица импортных адресов удаляется, так что она не существует ни на диске, ни в памяти, а эта информация распределяется внутри LDK Envelope Runtime. Это означает, что каждая операция импорта адреса защищена и обрабатывается внутренне Envelope. Кроме того, каждая операция импорта разрешается в другое место памяти с другим запутывающим кодом, так что взломщик должен анализировать и понимать каждую операцию импорта отдельно, чтобы получить кусочек головоломки. В традиционных упаковщиках защиты таблица импортных адресов позволяет взломщикам определять, когда они закончили анализ каждой записи в таблице. В Sentinel LDK Envelope таблица импортных адресов не используется, поэтому инструменты, которые взломщик обычно использует для восстановления этой таблицы, становятся бесполезными. Кроме того, Envelope использует различные методы для скрытия импортов, которые приводят к сбою взломанного приложения на более позднем этапе, делая «успешно взломанное» приложение частично неработоспособным и, следовательно, ненадежным.

Прочная связь между исходным кодом и кодом Envelope

Во многих распространенных упаковщиках нет связи между исходным кодом приложения и кодом упаковщика. Sentinel LDK Envelope усиливает виртуальную связь между упаковщиком и защищенным приложением, интегрируясь в поток приложения на основе анализа потока кода, выполняемого во время защиты. Это позволяет незаметно интегрировать меры защиты в приложение, предотвращая его удаление злоумышленником. Во время выполнения, как только поток управления достигает этих назначенных адресов, явная последовательность выполнения выполняет различные операции проверки и верификации, продолжая при этом выполнение исходного кода приложения. Если поток не поврежден, приложение будет работать; в противном случае, если целостность приложения под вопросом, процесс останавливается.

Украденные байты

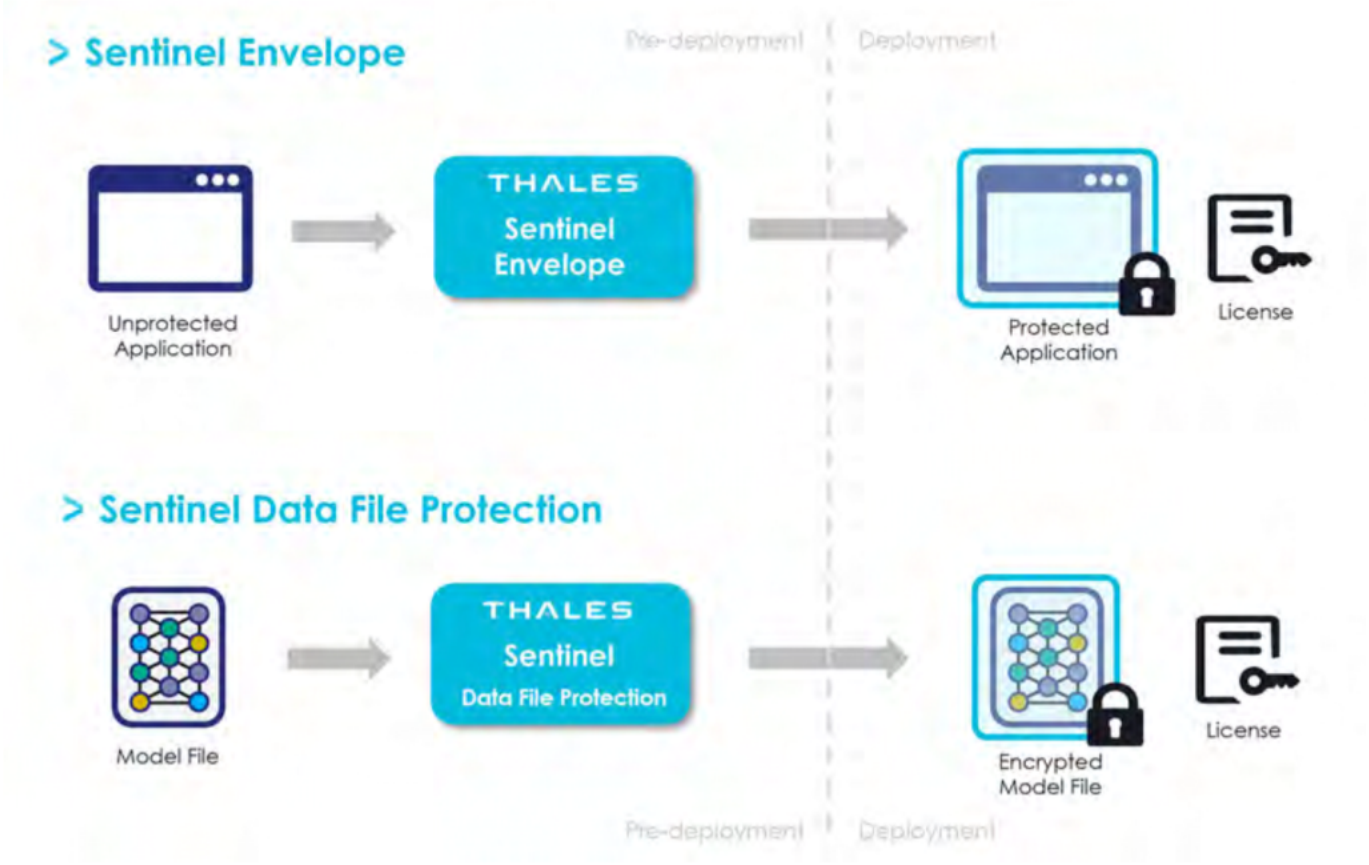
Снимки памяти и дампы — это широко используемые методы, которые в некоторых случаях могут дать взломщикам представление о логике исходного приложения. Это важный первый шаг для любого взломщика, пытающегося обойти защиту приложения, и именно в этом заключается задача успешного решения для защиты от взлома.

Концепция «украденных байтов» относится к усилению зависимости между защищенным приложением и кодом Envelope. Кража байтов означает выбор случайных блоков байтов из разных мест исходного двоичного файла и их случайное распределение внутри кода Envelope. Эти блоки кода (украденные байты) выполняются в новых случайных местах во время выполнения исходного кода защищенного приложения. Этот механизм усиливает зависимость исходного кода приложения от кода LDK Envelope Runtime, размывая границу между исходным кодом приложения и кодом Envelope.

Скрытие символов и кода

Запутывание символов — это процесс преобразования значимых строк в случайные строки букв или цифр. Используя Sentinel LDK Envelope, поставщик программного обеспечения может применять запутывание в качестве меры безопасности против обратной инженерии. По умолчанию все имена символов с частной видимостью запутываются в защищенных сборках .NET. Кроме того, поставщики программного обеспечения могут выбрать запутывание кода выбранных методов. Поскольку запутывание кода может замедлить работу приложения, по умолчанию оно не выбирается. Поставщики могут применять запутывание кода к методу независимо от того, выбран ли он для запутывания символов или шифрования в списке методов, подлежащих защите.

Защита python-скриптов и нейросетевых моделей



Продукт Sentinel Envelope поддерживает защиту скриптов, выполняемых как на Windows, так и на Linux. Скрипты защищаются самим производителем софта, а исполняемые библиотеки обеспечивают автоматическую расшифровку и безопасное выполнение на машине пользователя.
Также Envelope позволяет защищать приложения на Пайтоне скомпилированные в С при помощи Cython, что позволяет обеспечить дополнительный уровень защиты (который рассматривался чуть выше по тексту) к коду, написанному на этом языке.
Для производителей софта для ИИ-рынка Envelope предлагает защиту моделей и автоматическую шифровку-дешифровку. Это позволяет защитить модели от несанкционированного изменения,

“отравления” кода и пиратства и поддерживается TensorFlow и PyTorch. При распаковке такой модели Envelope гарантирует подлинность кода и модулей и занимается шифровкой-дешифровкой “на лету”.

Возможности

Позволяя поставщикам программного обеспечения настраивать защиту своих приложений и выбирать технологии защиты для интеграции, Sentinel LDK Envelope может удовлетворить различные индивидуальные потребности, предоставляя все инструменты для реализации самой надежной защиты от копирования. Безопасность может быть достигнута за счет некоторого снижения производительности и удобства использования. Поэтому крайне важно, чтобы поставщик правильно оценил требуемый уровень безопасности на основе уровня угрозы (то есть ценности того, что необходимо защитить) в сочетании с предполагаемыми убытками, связанными с игнорированием потенциальных рисков.
Помимо защиты от копирования, активно препятствуя доступу конкурентов к коммерческой тайне и ноу-хау, поставщик программного обеспечения может помешать промышленному шпионажу и сохранить конкурентное преимущество. Технология сочетает в себе шифрование и обфускацию нативного кода, чтобы обеспечить надежную защиту вашей ценной интеллектуальной собственности.
Sentinel LDK Envelope разработан с учётом простоты использования и обеспечивает высочайший уровень безопасности без необходимости тратить время и усилия на разработку решения для защиты с нуля, позволяя вашим инженерным командам сосредоточиться на своих основных компетенциях.
Загрузите БЕСПЛАТНЫЙ демонстрационный комплект Sentinel LDK, который включает Sentinel LDK Envelope.
Thales — лидирующий на рынке поставщик решений по лицензированию программного обеспечения и управлению правами для поставщиков локального, встроенного и облачного программного обеспечения. Thales Sentinel — один из самых надёжных брендов в индустрии программного обеспечения, предлагающий безопасные, гибкие и перспективные решения по монетизации программного обеспечения.
Простые в интеграции и использовании, инновационные и ориентированные на функциональность, решения “Sentinel Software Monetization Solutions” разработаны для удовлетворения уникальных требований любой организации к лицензированию, обеспечению соблюдения и управлению, независимо от ее размера, технических требований или организационной структуры. С Thales клиенты могут решать все аспекты жизненного цикла монетизации программного обеспечения — от защиты копий и интеллектуальной собственности до управления каталогом продуктов и постоянного улучшения пользовательского опыта.
Благодаря проверенной истории адаптации к новым требованиям и внедрению новых технологий для реагирования на меняющиеся рыночные условия, клиенты Thales по всему миру знают, что, выбирая Sentinel, они выбирают свободу развивать свой бизнес сегодня, завтра и в будущем.
Люди, на которых вы полагаетесь в вопросах защиты своей конфиденциальности, полагаются на Thales в вопросах защиты своих данных. Когда речь заходит о безопасности данных, организации сталкиваются с всё возрастающим числом решающих моментов. Будь то разработка стратегии шифрования, переход в облако или выполнение требований по обеспечению соответствия, вы можете положиться на Thales в вопросах обеспечения безопасности вашей цифровой трансформации.