Анализ зашифрованного трафика с помощью новых сетевых решений Cisco и Stealthwatch

Повышение надежности зашифрованного трафика без ущерба для конфиденциальности данных

Быстрый рост зашифрованного трафика меняет ландшафт угроз. Цифровые компании, сложность которых все увеличивается за счет роста числа устройств и приложений, работающих в их сети, все чаще используют шифрование для защиты информации. Согласно отчетам за 2017 год, практически половина всего интернет-трафика защищена протоколом HTTPS[1]. И объем зашифрованного трафика в сети будет только продолжать расти.

Шифрование обеспечивает большую конфиденциальность и безопасность, что особенно необходимо для мобильных, облачных и веб- приложений. Однако злоумышленники также применяют шифрование для маскировки вредоносных программ и обхода систем обнаружения, используемых в традиционных продуктах безопасности. Таким образом, протокол, считавшийся раньше надежным и безопасным, теперь сам стал инструментом для киберпреступников. Взлом данных очень отрицательно сказывается на организации в целом. Согласно результатам исследований, в среднем обнаружение проникновения в сеть занимает около 200 дней, а средние издержки, понесенные в результате проникновения, составляют примерно 3,62 млн долл. США[2]. К сожалению, у большинства организаций нет возможности обнаруживать вредоносную активность в зашифрованном трафике, не дешифровав его.

К 2019 году:

всего трафика будет зашифровано

сетевых атак будет использовать шифрование

Источник: Gartner

Преимущества решения

- **Расширенный мониторинг.** Получение детальной информации об угрозах в зашифрованном трафике с использованием сетевой аналитики и машинного обучения. Получение контекстной информации от интеллектуальных средств исследования угроз с данными анализа в реальном времени, соотнесенными с информацией о пользователях и устройствах.
- **Криптографическая оценка.** Позволяет гарантировать соответствие корпоративных требований криптографическим протоколам и обеспечивать мониторинг и понимание не только того, какой трафик в сети зашифрован, но и какова степень этого шифрования.
- **Ускорение реагирования.** Быстрая нейтрализация зараженных устройств и пользователей за счет обнаружения угроз в зашифрованном трафике в реальном времени, без необходимости использования дешифрования, занимающего много времени.
- **Экономия времени и средств.** Использование сети как основы для оценки состояния безопасности с извлечением выгоды из инвестиций в безопасность сети.

«Идентификация угроз, скрытых в зашифрованном сетевом трафике, представляет собой уникальный набор задач. Важно не только выполнять мониторинг трафика на наличие угроз и вредоносных программ, но при этом не нарушать целостность шифрования»[3].

– Блейк Андерсон (Blake Anderson), Advanced Security Research Group

Принципы работы

Элементы решения:

- Корпоративные коммутаторы. Платформа коммутации Cisco® Catalyst® 9000 (начиная с ПО Cisco IOS® XE, версия 16.6.1)
- Маршрутизаторы филиалов. Cisco ASR серии 1000, ISR серии 4000, маршрутизаторы серии 1000, маршрутизатор Cloud Services Router 1000V и виртуальный маршрутизатор с интеграцией сервисов (начиная с ПО Cisco IOS XE, версия 16.6.2)
- Мониторинг сети и аналитика безопасности. Cisco Stealthwatch® Enterprise (начиная с версии 6.9.2)

Необходимость определения степени доверенности зашифрованного трафика стала слишком сложной задачей для большинства групп реагирования на инциденты. Традиционная проверка на наличие угроз с использованием массовой расшифровки, анализа и повторного шифрования не всегда является практичной или выполнимой из-за снижения производительности и значительной загрузки ресурсов. Но даже если такая проверка возможна, решения для расшифровки сетевого трафика снижают уровень конфиденциальности пользовательских данных и работают не со всеми типами шифрования.

Аналитика зашифрованного трафика

Компания Cisco, имея огромный опыт работы на рынке сетевой инфраструктуры, провела обширное исследование и представила инновационную и революционную технологию для анализа зашифрованного трафика Encrypted Traffic Analytics (ETA). С ее помощью можно заглянуть в каждый уголок зашифрованного трафика, не расшифровывая его, а используя новые типы элементов данных или телеметрию, независимую от деталей протоколов.

Аналитика зашифрованного трафика опирается на четыре основных элемента данных.

1. **Последовательность времени и длины пакетов (Sequence of Packet Lengths and Times, SPLT).** SPLT передает длину (число битов) прикладных полезных данных каждого пакета для нескольких первых пакетов потока вместе с промежутками времени между прибытием этих пакетов.
2. **Исходный пакет данных (Initial Data Packet, IDP).** IDP используется для получения данных пакета из первого пакета в потоке. Это позволяет извлечь необходимые данные, такие как URL-адрес HTTP, имя/адрес DNS-узла и другие элементы данных.
3. **Распределение байтов.** Распределение байтов представляет вероятность того, что определенное значение байта появится в полезных данных пакета в потоке.
4. **Функции, относящиеся к TLS.** Квитирование TLS состоит из нескольких сообщений, содержащих необходимые незашифрованные метаданные, используемые для извлечения элементов данных, таких как комплекты шифров, версии TLS и длины открытого ключа клиента.

Используя эти элементы данных или расширенную телеметрию, технология ETA позволяет идентифицировать вредоносный код в зашифрованном трафике, применяя передовые средства анализа безопасности. В то же время целостность зашифрованного трафика поддерживается благодаря отсутствию необходимости в массовом дешифровании/расшифровании.

Обнаружение вредоносных программ, скрытых в зашифрованном трафике

Расширенная сетевая телеметрия с последних маршрутизаторов и коммутаторов Cisco собирается с помощью устройства Cisco Stealthwatch Enterprise – средства, обеспечивающего комплексный мониторинг сети и предоставляющего аналитические данные безопасности. Это средство использует расширенное моделирование сущностей и многоуровневое машинное обучение для постоянного определения тех, кто находится в сети, и того, что они там делают, а также для выявления аномального поведения в реальном времени для обнаружения угроз. С его помощью можно также составить глобальную карту угроз для идентификации известных глобальных угроз и их корреляции с локальной средой. Таким образом, впервые в отрасли значительно повышается точность обнаружения вредоносных программ в зашифрованном трафике и в то же время обеспечивается полная конфиденциальность и целостность каналов передачи благодаря отсутствию дешифрования /расшифрования.

Заключение

Группы по обеспечению безопасности и по сетевым технологиям должны работать совместно, чтобы иметь полное представление обо всем корпоративном трафике. Интуитивная сеть Cisco поможет обнаружить скрытые угрозы безопасности даже в зашифрованном трафике. Более подробную информацию о том, как решения Cisco по безопасности позволят вам получить полное представление обо всех областях своей сети, см. по ссылке https://www.cisco.com/go/eta.

Источники:

1. Electronic Frontier Foundation, февраль, 2017 г., https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web.
2. Ponemon Institute, июнь 2017 г.
3. Блог: Обнаружение зашифрованного вредоносного трафика без дешифрования, июнь 2017 г.

Обеспечение соответствия криптографическим протоколам

Используя шифрование для обеспечения конфиденциальности и защиты данных, организация должна ответить на следующие вопросы. Какая часть нашего цифрового бизнеса использует надежное шифрование? Насколько это шифрование качественное? Эту информацию чрезвычайно важно знать, чтобы в первую очередь помешать злоумышленникам проникнуть в зашифрованный поток данных. На сегодняшний день единственный способ, гарантирующий соответствие зашифрованного трафика заданным политикам, заключается в периодическом проведении аудита на предмет выявления любых нарушений протокола TLS. Однако это не самая удачная стратегия из-за большого количества устройств и объема трафика, проходящего через предприятие. Cisco ETA обеспечивает непрерывный мониторинг без затрат времени и средств, присущих мониторингу с использованием дешифрования. Используя собранную расширенную телеметрию, Stealthwatch Enterprise предоставляет возможность просмотра и поиска по таким параметрам, как обмен ключами шифрования, алгоритм шифрования, длина ключа, версия TLS/SSL и т. д., чтобы обеспечить соответствие криптографическим протоколам.

C45-740079-00 12/17