Защита SWIFT-инфраструктуры с помощью DECEPTIONGRID™ (Сеть обнаружения атак)

Защита SWIFT-инфраструктуры, связанных сетевых активов и Back-office систем

За прошедший год финансовая сеть SWIFT подвергалась целенаправленным кибератакам, в результате чего у банков по всему миру было похищено более $ 100 млн. Аналитики прогнозируют, что атаки на финансовые сети будут продолжаться и SWIFT остается приоритетной мишенью для взломщиков. Традиционные продукты безопасности, ориентированные на защиту периметра или обнаружение вредоносных программ относительно легко преодолеваются квалифицированными хакерами.

Новые технологии, такие как Deception, или использование «ложных» ИТ-систем, являются важным компонентом в борьбе с современными атаками. DeceptionGrid полностью автоматизирует создание и развертывание сигнальной сети замаскированных ловушек TrapX («ложные» ИТ-объекты) и токенов (приманок к ним). Таким образом, разворачивается своеобразное «минное поле» для хакеров.

Ловушки имитируют системы, которые могут представлять различные реальные ИТ-активы, в том числе SWIFT Alliance SAG, SWIFT Alliance SAA, и SWIFT Alliance Web Platform для Linux и Windows. Эти ловушки фактически идентичны реальным SWIFT активам и могут быть развернуты по всей сети заказчика, создавая разветвленную сигнальную инфраструктуру, смешанную с реальной ИТ-инфраструктурой.

Взломщики, используя скомпрометированные ПК для разведки и скрытого распространения, наталкиваются на фальшивые данные (приманки), такие как сохраненные RDP-сессии, историю и закладки в браузере для Alliance Web Platform, ложные SWIFT-сообщения и ложные учетные записи. Эти приманки приводят атакующего в развернутые ловушки, что дает возможность их обнаружить и, в то же время, отвлечь от реальных SWIFT систем.

Таким образом, реальные активы SWIFT покрываются сигнальной сетью «ложных», которые выглядят относительно уязвимыми и привлекают взлом-

Преимущества для пользователей SWIFT

- DeceptionGrid обнаруживает и отвлекает атаки, нацеленные на SWIFT, создавая новый защитный слой вокруг инфраструктуры SWIFT.

- Внедрение высокоэффективных методов противодействия обеспечивают защиту SWIFT от самых современных и совершенных методов мошенничества.

- Быстрый способ радикально снизить уровень рисков информационной безопасности для SWIFT-инфраструктуры

- Помогает команде безопасности защитить периметр сети от будущих атак за счет использования достоверной и полной аналитики обнаруженных угроз

- Защищает другие финансовые и ИТ-активы, в том числе ключевые приложения, рабочие станции, сетевое оборудование, серверы и многое другое.

DeceptionGrid полностью автоматизирует развертывание сигнальной сети замаскированных ловушек и приманок TrapX.

щиков. Благодаря такому комплексному подходу с использованием «ловушек» и «приманок» DeceptionGrid создает новый слой защиты инфраструктуры SWIFT.

Детальный анализ подозрительных компьютеров производится с помощью дополнительного модуля автоматизированного реагирования на инциденты (AIR) входящего в состав платформы DeceptionGrid. Память и другие компоненты подозрительных компьютеров автоматически анализируются, результаты обобщаются и передаются в виде детального отчета.

Интегрированное управление событиями и ИБ-аналитика

Информация, полученная в результате анализа, автоматически передается в систему управления с уникальным ID и потом хранится в интегрированной базе данных управления событиями. Встроенные механизмы анализа коррелируют эту информацию с данными об угрозах для того, чтобы предотвратить будущие атаки. Ботнет-детектор (DeceptionGrid Network Intelligence Sensor) анализирует исходящую активность настоящих пользователей на основе информации, собранной о вредоносной активности, которая была замечена в ловушках.

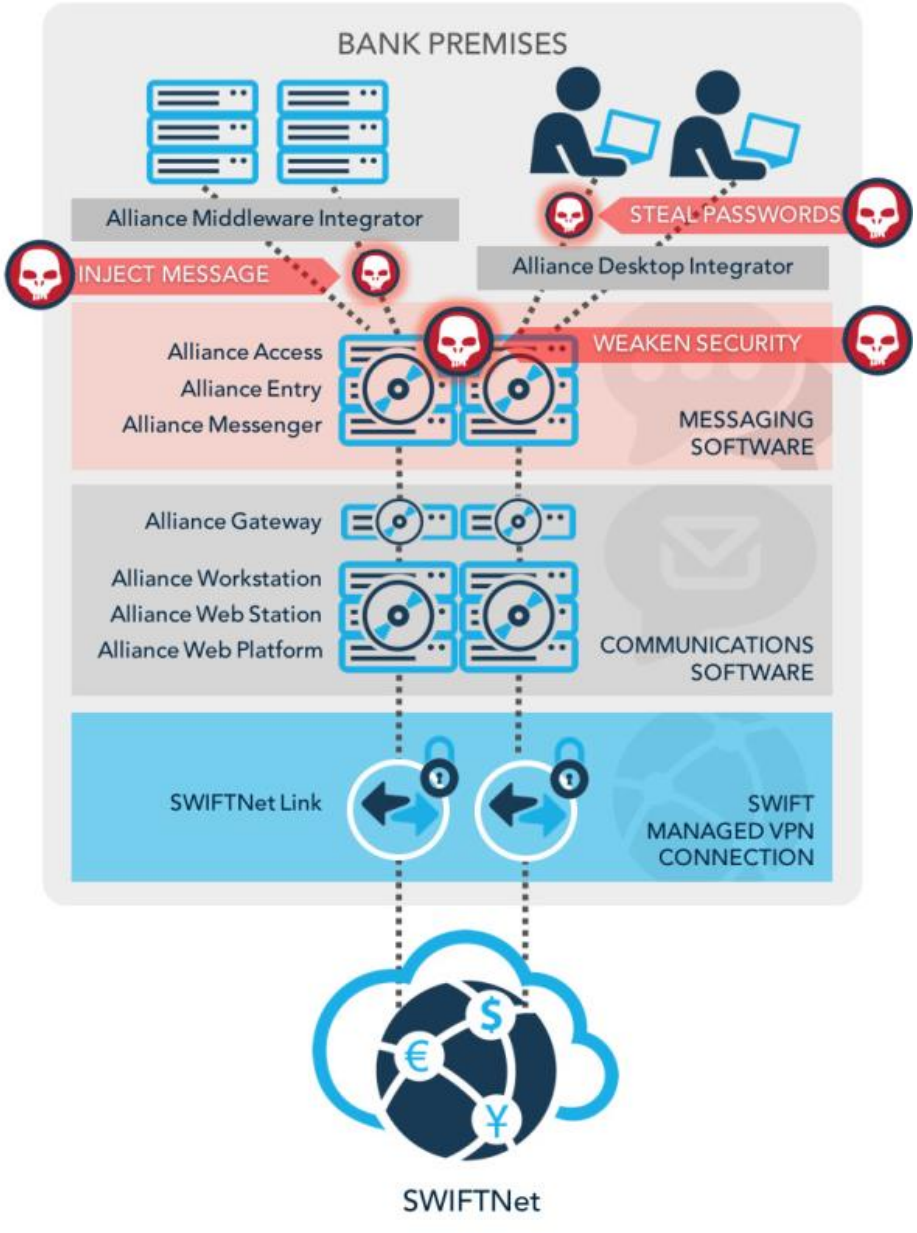

Рис.1. Векторы атак на инфраструктуру SWIFT

Выгоды использования DeceptionGrid

- Технология DeceptionGrid обнаруживает атаки, которые не фиксируются другими решениями.
- Ловушки минимизируют риск экономических потерь за счет значительного сокращения времени, необходимого для обнаружения взлома.
- Практически нулевой процент ложных срабатываний позволяет сосредоточить внимание на реальных угрозах.
- Автоматический анализ предоставляет все необходимые данные для ликвидации атаки в SOC.
- Имитируемые «ложные» объекты (ловушки) и встроенные «приманки» (токены) создают уникальный защитный слой для всех ИТ-активов предприятия.
- Имитация, а не использование реальных активов, позволяет строить широкомасштабные сигнальные сети с высокой экономической эффективностью
- Максимизация эффекта и сохранение инвестиций за счет интеграции с существующими средствами ИБ от других поставщиков и партнеров

Особенности TrapX DeceptionGrid

- Достоверная имитация широкого ряда устройств (SWIFT, медицинские приборы, банкоматы (ATM), POS-устройства и многое другое).
- Обнаружение злоумышленников в реальном времени, в любом месте сети.
- Уровень точности обнаружения атак - 99%
- Всесторонний автоматический анализ вредоносных программ и инструментов атакующего.
- Модуль AIR обеспечивает автоматический анализ памяти подозрительной рабочей станции.
- Возможность быстрого развертывания DeceptionGrid в масштабах всего предприятия.
- Центр анализа угроз использует результаты анализа и сформированные IoC (Indicator of Compromise) для улучшения защиты в целом.
- Наше стратегическое партнерство с другими производителями в области ИБ обеспечивает широкие возможности интеграции и защиту Ваших инвестиций.

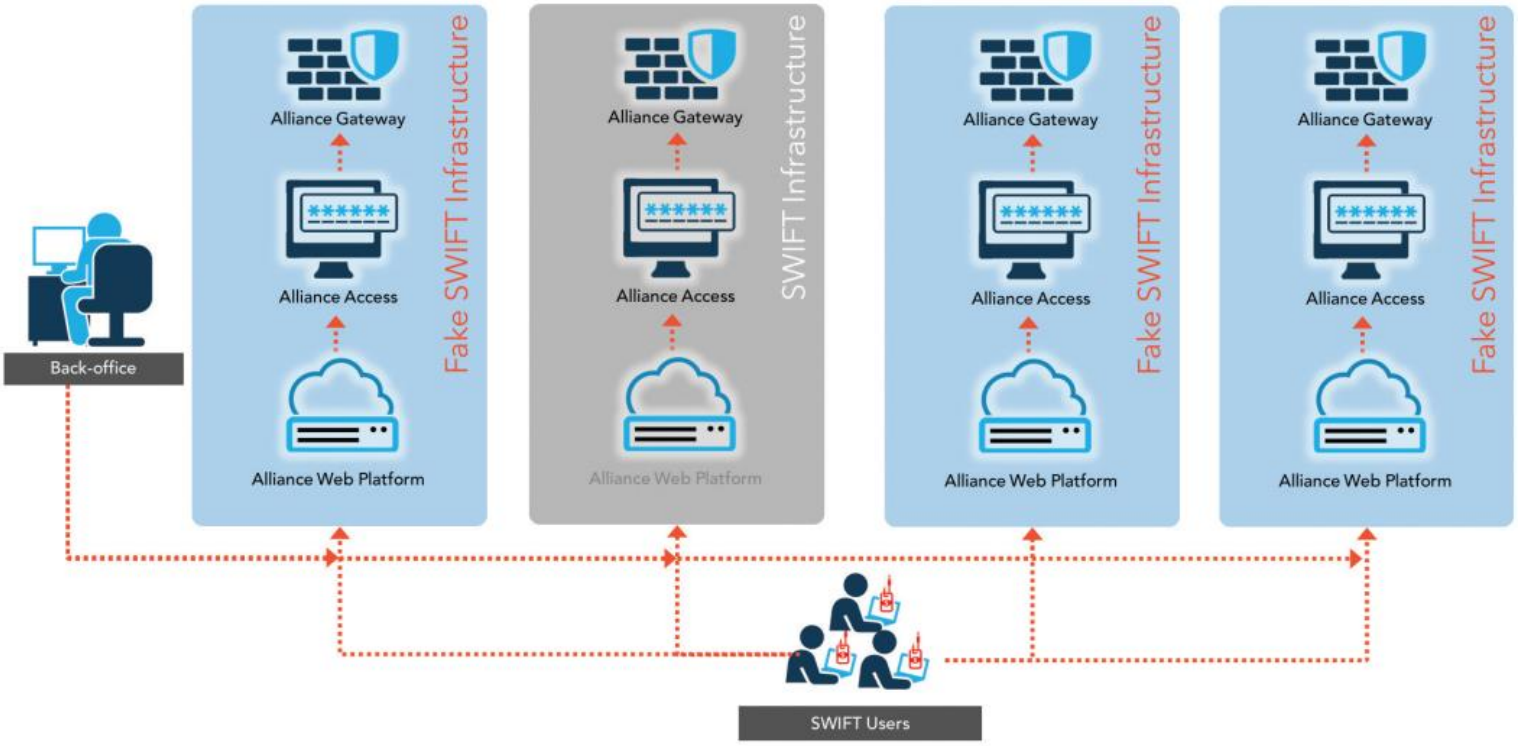

Рис. 2. DeceptionGrid формирует новый защитный слой SWIFT-инфраструктуры

Гибкие возможности развертывания

DeceptionGrid разработан для быстрого развертывания в крупных корпоративных сетях, без необходимости изменения существующей ИТ-инфраструктуры. Наши встроенные средства автоматизации позволяют выполнить полное внедрение всего за несколько часов.

Теперь DeceptionGrid защищает и финансовую сеть SWIFT. DeceptionGrid повышает уровень защищенности сетей, обслуживающих приложения SWIFT. Это обеспечивает бесперебойность бизнес-процессов и успешное прохождение SWIFT аудитов.

Функционал DeceptionGrid для SWIFT

DeceptionGrid автоматизирует развертывание сотен или тысяч ловушек во внутренней сети компании. Эти ловушки предназначены чтобы обмануть злоумышленников, которые не были обнаружены традиционными защитными системами.

Типичные ловушки представляют собой эмуляции различных рабочих станций Windows, серверов Windows и Lunix, сетевого оборудования. Кроме того, специализированные ловушки, такие как медицинское оборудование, PoS-устройства, банкоматы, SCADA системы могут быть сконфигурированы и развернуты простым нажатием кнопки.

Для повышения вероятности срабатывания ловушек также разворачивается сеть «приманок» в виде файлов, учетных записей, закладок, которые размещаются на реальных IT объектах.

Этот всесторонний подход с использованием ловушек и приманок обеспечивает быстрое обнаружение и отвлечение злоумышленников на разных этапах атаки.

Специализированные ловушки, такие как SWIFT серверы, Point of Sale (PoS) системы, банкоматы (ATM) и другие могут быть сконфигурированы и запущены несколькими кликами мышки

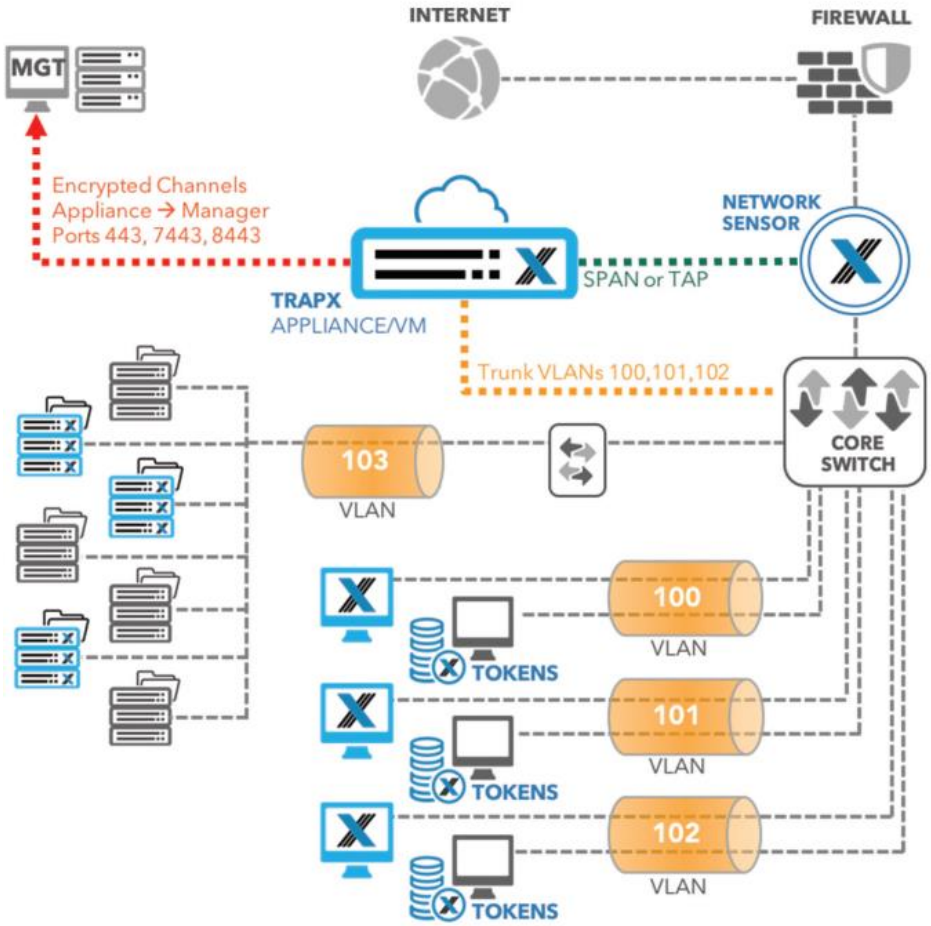

Рис.3. Архитектура сигнальной сети

Атакующие, которые используют захваченные рабочие станции для разведки и скрытого распространения, неминуемо сталкиваются с приманками и ловушками

Автоматические экспертизы

Средства автоматизации в реальном времени обнаруживают и изолируют применяемые взломщиком инструменты, затем направляют их для проведения всестороннего анализа в «песочницу» Клиента или облачный сервис TrapX.

Дополнительная аналитика угроз, полученная от этих систем, коррелируется с поведением ловушек и Ваш Центр обеспечения безопасности (SOC) получает исчерпывающий аналитический отчет. Дополнительный модуль анализа сетевой активности (NIS) в составе DeceptionGrid выполняет анализ исходящего трафика и вместе с информацией, полученной от ловушек, позволяет создать полную картину скомпрометированных активов и внешней сетевой активности атакующего.

О TrapX

TrapX Security – лидер в сфере киберзащиты на основе технологии «ложных» ИТ-систем. Наши продукты быстро определяют, анализируют и нейтрализуют новейшие APT-атаки и атаки «нулевого» дня в режиме реального времени. DeceptionGrid обеспечивает автоматизированный, тщательный анализ вредоносного ПО и подозрительных активностей, невидимых для других средств киберзащиты. Мы следуем проактивной концепции безопасности, в корне меняя экономический аспект киберзащиты. Для хакеров атаки становятся дороже. Услугами TrapX Security уже пользуются 2000 коммерческих и правительственных структур в сферах защиты, здравоохранения, финансов, энергетике, потребительских товаров и многих других ключевых отраслей по всему миру.