История успеха

GROUP-IB И SIMPLE:

**не только вино,
но и технологии**

simple group

GROUP IB

80+
городов России

2000
высококвалифицированных сотрудников

>500
эксклюзивных поставщиков

Группа компаний Simple

Группа компаний Simple – один из ведущих импортеров, национальный дистрибьютор и ритейлер с динамично развивающейся собственной сетью винотек и онлайн-витриной под розничным брендом SimpleWine.

За более чем 25 лет работы Simple сумели завоевать доверие лучших винодельческих домов Старого и Нового Света.

Миссия Simple — повышать качество жизни людей через возрождение российской винной культуры.

Шаг за шагом реализовать эту миссию помогает интегрированный подход к ведению бизнеса: винные рестораны и бары Grand Cru и Simple Bar, издательство Simple Media (Simple Wine News, swn.ru), школа вина «Энотрия».

Год основания:

1994

Отрасль:

АЛКОГОЛЬНАЯ

Деятельность:

ИМПОРТ И ДИСТРИБУЦИЯ ВЫСОКОКАЧЕСТВЕННОЙ АЛКОГОЛЬНОЙ ПРОДУКЦИИ В РОССИИ, РИТЕЙЛ

Количество сотрудников:

2000

simple group

Предпосылки внедрения

Миссия Simple — повышать качество жизни людей через возрождение российской винной культуры. Шаг за шагом реализовать эту миссию помогает интегрированный подход к ведению бизнеса: винные рестораны и бары Grand Cru и Simple Bar, издательство Simple Media (Simple Wine News, swn.ru), школа вина «Энотрия». Неотъемлемой частью успеха компании Simple сегодня является продвинутая ИТ инфраструктура. Благодаря уникальным ИТ-системам и высоким требованиям к информационной безопасности Simple предоставляет своим партнерам и клиентам качественный и надежный сервис.

Всегда с ростом бизнеса увеличивается уязвимость любой компании, становится сложнее управлять всеми программным и аппаратными средствами, следить за своевременными обновлениями. А в ритейл-индустрии ещё накладывается уязвимость со стороны кассового оборудования, которое не всегда имеет самое свежее программное обеспечение.

> Мы используем сразу несколько традиционных средств защиты, но иногда встречали ложные срабатывания или не выявленное вредоносное ПО. И одним из самых уязвимых мест в нашей инфраструктуре являются именно кассовые аппараты. На них часто не выходят обновления от производителей операционных систем, да и сами ОС, как правило, имеют версионность на несколько поколений назад. Прошлый продукт, который использовался для защиты от сложных угроз, показал себя неэффективным и не смог решить всех поставленных задач. Именно поэтому мы решили найти более действенное, удобное в управлении и масштабируемое решение.
>
> **Владимир Бондарев,**
> Руководитель управления инфраструктуры и поддержки, Дирекция информационных технологий Simple

Почему выбрали Group-IB

Перед департаментом IT-безопасности Simple была поставлена задача найти комплексное и качественное решение, которое поможет усилить защиту корпоративной сети и будет выявлять вредоносные файлы. Но нужна была не только возможность обнаруживать аномальный сетевой трафик внутри сети, но и проводить поведенческий анализ зараженных файлов в изолированной среде.

Среди претендентов для пилотирования было выбрано несколько компаний с их решениями класса Anti-APT (англ. Advanced Persistent Threat — «развитая устойчивая угроза», целевая кибератака), позволяющие проводить поведенческий анализ вредоносных файлов в, так называемой, «песочнице» — изолированной от основной сети среде. Но стоит отметить, что предложенное решение компанией Group-IB опережало конкурентов за счет изменения технологий и средств непосредственного анализа файлов.

В ходе тестирований решением Group-IB было обнаружено несколько зловредных файлов, которые пропустились другими решениями. В основном пропускались письма с запароленными архивами и файлы с вредоносным ПО, которое запускает отложенные задачи.

Также, ключевую роль в выборе поставщика сыграл большой опыт Group-IB в расследовании киберпреступлений, отслеживании реальных преступных группировок и анализу информации по ним.

> Для крупной компании, такой как Simple, наличие качественного решения для защиты от сложных атак очень важно. Современные APT-группировки находят различные техники заражения корпоративных сетей, что может вести, как к краже данных клиентов, их денег, так и к репутационным и финансовым потерям самой компании. В данном проекте мы, совместно со специалистами Simple, реализовали комплексный проект, позволяющий, как выявлять современные атаки, так и защищаться от них, а совместная работа экспертов Group-IB со специалистами по реагированию Simple позволила достичь действительно высокого уровня обеспечения безопасности.
>
> **Станислав Фесенко,**
> Руководитель департамента системных решений Group-IB

Решение Group-IB

Высокотехнологичная система раннего выявления кибератак Group-IB Threat Hunting Framework, модули Sensor и Polygon.

Описание решения Group-IB Threat Hunting Framework (THF)

Group-IB THF — комплексное решение, предназначенное для выявления целевых атак и неизвестных угроз, охоты за угрозами как внутри защищаемого периметра, так и за его пределами, реагирования на инциденты и их расследования.

Применение Group-IB THF позволяет определять заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений.

Group-IB THF Sensor – модуль продукта Group-IB THF, предназначенный для анализа входящих и исходящих пакетов данных. Используя собственные сигнатуры и поведенческие правила Group-IB, THF Sensor позволяет выявлять взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств. Модуль также позволяет извлекать объекты анализа из различных источников для передачи в Group-IB THF Polygon.

Group-IB THF Polygon представляет собой модуль для детонации файлов в изолированных средах, извлечения индикаторов и обогащения их. Главной задачей Group-IB THF Polygon является всеми возможными способами обнаружить вредоносный код в почтовых вложениях, скачиваемых файлах и ссылках.

> Технология глубокого анализа файлов и детонации вредоносных нагрузок Group-IB Polygon позволяет существенно поднять защищенность любого предприятия по ключевым векторам начального проникновения. Мы очень рады, что наша технология и формат ее поставки в виде облачного сервиса Polygon Cloud были по достоинству оценены и приняты на вооружение таким интересным клиентом, как Simple.
>
> **Никита Кислицин,**
> Руководитель Департамента сетевой безопасности Group-IB

Результаты работы

Решение полностью оправдало ожидания. Его интеграция в существующую инфраструктуру винного поставщика заняла всего неделю, специалисты обеих компаний взаимодействовали плодотворно.

Количество ложных срабатываний снизилось в несколько раз, а департамент IT-безопасности Simple своевременно получает полный анализ событий по выявленным инцидентам. Также THF выводит сводную информацию по текущему состоянию системы на ТВ-панель для более быстрого реагирования на инциденты.

THF Sensor находит подозрительные события, он дополнительно проверяет их на сопутствующих системах: firewall, почтовые web шлюзы и т.д. В случае обнаружения вредоносные файлы отправляются на анализ в THF Polygon. В свою очередь, THF Polygon запускает зараженные файлы в изолированной среде для анализа вредоносности. Если файл не запустился в выбранной среде, осуществляется его перезапуск в новой среде.
В модуле используются различные методы сокрытия факта виртуализации. После помещения анализируемого объекта в выбранную виртуальную среду, реализуется большой спектр возможных действий реального пользователя операционной системы – от движения мыши и нажатия клавиш до перехода по ссылкам, скачивания и открытия/запуска файлов. Помимо этого, ведется полное логирование и видео исполнения файла.

> Мы иногда даже забываем, что у нас стоит система THF, так мало ложных срабатываний! И хотим выразить отдельную благодарность за столь продуманный пользовательский интерфейс. Не нужно много ресурсов, чтобы научиться полноценно управлять системой, всё интуитивно понятно и на своём месте. За те месяцы, что пользуемся THF, у нас значительно увеличилось время ИБ-специалистов, которое, наконец, они могут потратить на развитие всей инфраструктуры, внедрение новых технологий и обучению и повышению квалификации.
>
> **Владимир Бондарев,**
> Руководитель управления инфраструктуры и поддержки, Дирекция информационных технологий Simple

GROUP-IB

Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защиты интеллектуальной собственности в сети.

По версии **Gartner, IDC и Forrester,** Group-IB является одним из ключевых поставщиков Threat Intelligence в мире, в базе которой хранится 100 000+ профайлов киберпреступников.

Клиентами Group-IB являются крупнейшие банки и финансовые организации, промышленные и транспортные корпорации, ИТ и телеком провайдеры, ритейл и FMCG компании в 60 странах мира.

60 000+
часов реагирования

1000+
успешных расследований по всему миру

EUROPOL INTERPOL **Официальный партнер**

OSCE **Рекомендована Организацией по Безопасности и Сотрудничеству в Европе (ОБСЕ)**

Узнать больше о Threat Hunting Framework

group-ib.ru/thf
thf@group-ib.com