История успеха «Абсолют Банк»

Абсолют Банк

«Абсолют Банк» защитил веб-кабинет от вредоносных программ с помощью PT MultiScanner

Задача

Согласно исследованиям Positive Technologies, в России кредитно-финансовая отрасль входит в тройку наиболее атакуемых кибермошенниками[1]. Как правило, цель злоумышленников — быстро проникнуть в сеть и быстро вывести деньги, поэтому они предпочитают простые способы — в основном применяют вредоносное ПО. Например, они могут загрузить зараженный файл в веб-форму на сайте, разослать электронные письма, содержащие вредоносную программу, или провести фишинг.

АКБ «Абсолют Банк» — крупный федеральный банк с фокусом на высокотехнологичное развитие в приоритетных направлениях бизнеса. Банк специализируется на работе в сегментах с высоким уровнем экспертизы и уникальными IT-решениями — ипотеке, автокредитовании, а также на обслуживании малого и среднего бизнеса в цифровом формате, на системном обслуживании компаний холдинга ОАО «РЖД», на комплексных решениях в private banking.

В экосистему веб-сервисов «Абсолют Банка» входит веб-кабинет оформления банковских гарантий для организаций и индивидуальных предпринимателей. После регистрации на портале можно оформить заявку, предоставить необходимый пакет документов и получить банковскую гарантию без посещения офиса банка. Этот сценарий использования портала связан с угрозой для инфраструктуры банка: через форму для отправки документов клиент может случайно отправить зараженные файлы, а злоумышленник — целенаправленно загрузить вредоносное ПО.

Чтобы защитить инфраструктуру банка от возможных рисков, служба информационной безопасности «Абсолют Банка» решила внедрить систему, способную анализировать загружаемые на портал файлы и блокировать их при наличии угрозы.

Решение

В качестве решения «Абсолют Банк» выбрал многоуровневую систему защиты от вредоносных программ PT MultiScanner. Продукт анализирует файлы, которые попадают в корпоративную сеть в сетевом и почтовом трафике, загружаются в веб-приложения и файловые хранилища компании. Каждый файл проверяется с помощью нескольких антивирусов и уникальных правил PT Expert Security Center. Это позволяет защититься как от массовых угроз, так и от целевых атак хакерских группировок.

По данным независимого исследовательского института AV-TEST, в мире ежедневно регистрируется более 350 000 новых вредоносных программ. А как показывают исследования Positive Technologies, загрузка произвольных файлов через веб-приложения входит в топ-5 наиболее распространенных уязвимостей на сетевом периметре организаций.

1 «APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник», Positive Technologies.

Руслан Ложкин
Руководитель
службы информационной
безопасности

Абсолют Банк

«Внедрение PT MultiScanner было логичным этапом в процессе выстраивания комплексной защиты банка от киберугроз. **Тесная интеграция с межсетевым экраном PT Application Firewall и подтвержденная эффективность продукта стали ключевыми факторами выбора PT MultiScanner**, который позволил нам решить задачу по защите банковских веб-ресурсов от вредоносного ПО»

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ PT MULTISCANNER

- **Надежная защита.** PT MultiScanner проверяет файлы с помощью нескольких антивирусов и уникальных правил, поставляемых экспертами Positive Technologies по итогам расследований инцидентов ИБ в крупных компаниях и исследования деятельности хакерских группировок.
- **Точная локализация.** PT MultiScanner предоставляет подробные данные обо всех пораженных узлах сети и позволяет локализовать угрозу.
- **Выявление атак, не замеченных в прошлом.** С помощью автоматического ретроспективного анализа продукт обнаруживает вредоносное ПО, которое не было выявлено ранее.

Еще один сценарий использования PT MultiScanner — внутренний веб-портал, на котором можно проверить любой файл, просто переместив его в специальную форму. Эта функция полезна и удобна для сотрудников фронт-офиса банка, которые ежедневно имеют дело с многочисленными файлами от разных клиентов.

Проект по внедрению PT MultiScanner выполнял авторизованный партнер Positive Technologies — системный интегратор «ДиалогНаука».

К моменту внедрения в «Абсолют Банке» уже использовался межсетевой экран уровня веб-приложений PT Application Firewall, обеспечивающий защиту веб-приложений. Поэтому основной задачей было выполнить интеграцию PT MultiScanner с межсетевым экраном. PT MultiScanner поддерживает множество интерфейсов взаимодействия (SPAN, BCC, MTA, ICAP, REST API), это позволило бесшовно интегрировать продукты и быстро наладить процесс проверки файлов, загружаемых на портал РКО.

PT Application Firewall перенаправляет на анализ все загружаемые на веб-ресурс файлы. Далее PT MultiScanner проводит комплексную проверку каждого файла; система способна анализировать десятки тысяч файлов в час. PT MultiScanner возвращает вердикт в PT Application Firewall, и в зависимости от вердикта межсетевой экран пропускает файл в инфраструктуру или блокирует его.

Результаты

Внедрение PT MultiScanner позволило службе ИБ «Абсолют Банка» контролировать поступающий извне контент и решить задачу оперативного обнаружения и блокирования вредоносного ПО. Интеграция с межсетевым экраном PT Application Firewall повысила защищенность веб-портала от случайных заражений, спровоцированных пользователями, и от целенаправленных атак с применением вредоносных программ.

PT-MS_Absolut Bank_SS_A4.RUS.0001.02.JAN.15.2020