PT MULTISCANNER В ВГТРК: ВНУТРЕННИЕ ПОЛЬЗОВАТЕЛЬСКИЕ СЕРВИСЫ ДЛЯ ВЫЯВЛЕНИЯ ВРЕДОНОСНОГО ПО

«Мы осознаем, насколько высока вероятность заражения вредоносным ПО в такой крупной компании, как ВГТРК. Для эффективного противостояния этой угрозе нам потребовалось одновременно надежное и максимально гибкое решение, способное легко адаптироваться под наши нужды. Именно таким решением стал PT MultiScanner — продукт, который объединил в себе глубокую экспертизу Positive Technologies и многолетний опыт AV-вендоров».

Дмитрий Сафронов,
начальник отдела защиты информации ВГТРК

ВГТРК
ТЕЛЕВИДЕНИЕ И РАДИО

ПРОФИЛЬ КОМПАНИИ

- **Название:** ФГУП ВГТРК
- **Отрасль:** СМИ
- **Состав компании:** федеральные каналы «Россия-1», «Россия — Культура» и «Россия-24», международный канал «РТР-Планета», русская версия канала «Евроньюс», более 80 региональных телерадиокомпаний, четыре радиостанции («Радио России», «Маяк», «Культура», «Вести FM»), интернет-канал «Россия»

- **Решение:** PT MultiScanner для комплексной антивирусной проверки файлов сотрудников, снижения трудозатрат отдела защиты информации и повышения осведомленности пользователей в вопросах ИБ

Всероссийская государственная телевизионная и радиовещательная компания (ВГТРК) — крупнейшая медиакорпорация России. ВГТРК является лидером на рынке национального вещания и одним из ведущих производителей программ.

ЗАДАЧИ

Использование вредоносного ПО остается наиболее распространенным способом атаки[1]. Сотрудники компаний являются удобной потенциальной точкой входа для злоумышленников — вредоносное ПО, загруженное вместе с файлами из интернета или полученное по почте, может стать причиной массового заражения инфраструктуры или утечки данных.

С подобной проблемой столкнулся отдел защиты информации (ОЗИ) ВГТРК. Как крупнейшая в России медийная корпорация, ВГТРК постоянно подвергается атакам, направленным на нарушение работы многочисленных медиасервисов или получение конфиденциальной информации. Одна из наиболее популярных целей для атак — личная и корпоративная почта сотрудников, куда злоумышленники регулярно рассылают письма с вредоносными вложениями. Кроме того, нередки случаи заражения после загрузки сотрудниками подозрительных файлов из интернета и с внешних носителей.

Изначально для борьбы с вирусными угрозами ОЗИ использовал набор отдельных AV-средств, но этот подход породил ряд проблем. «Организовать эффективное управление таким количеством разнородных систем очень сложно. Без централизованного решения для координации AV-решений мы столкнулись с трудностями при анализе разнородных отчетов о сканировании и множеством ложных срабатываний», — отмечает Дмитрий Сафронов, начальник ОЗИ ВГТРК. Также ОЗИ создал специализированный электронный адрес, куда сотрудники компании могли переправлять письма с подозрительным содержимым. Все сообщения обрабатывались вручную специалистами ОЗИ; этот метод выявления вредоносного ПО оказался эффективным, но потребовал существенных трудозатрат.

В связи с этим ОЗИ потребовалось решение, которое позволило бы автоматизировать и сделать более надежным анализ файлов, снизить трудозатраты, а также повысить уровень осведомленности пользователей в вопросах ИБ, предоставив им сервис для самостоятельной проверки.

РЕШЕНИЕ

Для решения этих задач ВГТРК выбрал PT MultiScanner — многоуровневую систему защиты от вредоносного контента. Выбор определили следующие особенности продукта:

- проверка объектов с помощью нескольких антивирусных движков, статического анализа и репутационных списков — без отправки конфиденциальных данных за пределы периметра компании;
- ретроспективный анализ, позволяющий обнаруживать скрытые угрозы, отслеживать распространение вредоносного ПО в инфраструктуре и расследовать инциденты ИБ;
- агрегация данных обо всех угрозах в разных потоках данных;
- простота и скорость развертывания системы;
- масштабируемость и устойчивость к нагрузкам;
- интуитивно понятный и удобный интерфейс.

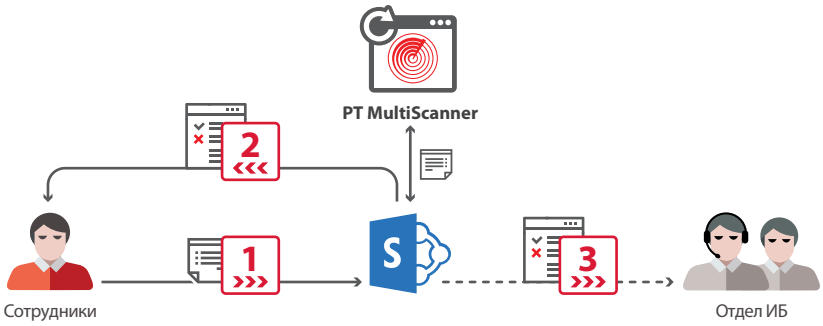
1 Исследование «Актуальные киберугрозы: IV квартал 2017 года», Positive Technologies.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

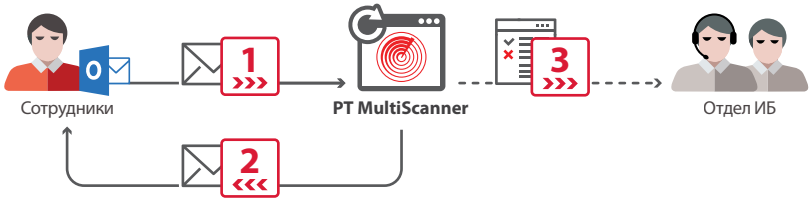
- Комплексная проверка файлов с помощью набора антивирусных движков, статического анализа и репутационных списков Positive Technologies
- Ретроспективный анализ файлов, позволяющий выявлять скрытое присутствие вредоносного ПО и целенаправленные атаки (APT), а также расследовать инциденты ИБ
- Агрегация сведений обо всех обнаруженных угрозах в различных потоках данных компании
- Поддержка стандартных интерфейсов взаимодействия (SPAN, MTA, ICAP, REST API), обеспечивающая простоту внедрения
- Повышение осведомленности пользователей в вопросах информационной безопасности

На базе PT MultiScanner реализуются два варианта проверки файлов.

- **Локальный пользовательский сервис (интеграция с внутренним порталом).** Благодаря интеграции PT MultiScanner с внутренним порталом на SharePoint (через REST API) реализуется пользовательский сервис для самостоятельной проверки файлов. При получении подозрительного сообщения сотрудники могут загрузить его на проверку и получить данные сканирования с помощью специальной кнопки в интерфейсе SharePoint.



- **Интеграция с почтовым клиентом.** Благодаря интеграции PT MultiScanner с корпоративным почтовым клиентом пользователи могут отправлять подозрительные файлы на проверку с помощью специальной кнопки в интерфейсе самого почтового клиента.



Оба варианта подразумевают отправку уведомления специалистам по ИБ при обнаружении вредоносного ПО; это помогает ОЗИ оперативно принять необходимые меры безопасности, отследить распространение «вредоноса» в инфраструктуре и ликвидировать угрозу.

РЕЗУЛЬТАТЫ

«PT MultiScanner — очень гибкая система. Она легко адаптируется к любым нашим нуждам, а поддержка разных интерфейсов взаимодействия заметно упрощает интеграцию с существующими системами. Благодаря PT MultiScanner мы решили проблему эффективной антивирусной защиты», — отмечает Дмитрий Сафронов.

В результате внедрения PT MultiScanner ВГТРК получил удобные внутренние сервисы, которые позволили вдвое сократить трудозатраты специалистов по ИБ на ручные проверки файлов и повысили уровень защищенности инфраструктуры от вредоносного ПО. В дальнейших планах ВГТРК — расширение набора используемых антивирусных движков и интеграция с другими корпоративными системами для обеспечения всесторонней защиты.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays