PT NETWORK ATTACK DISCOVERY ПОВЫШАЕТ ЗАЩИЩЕННОСТЬ ИНФРАСТРУКТУРЫ ВГТРК

«Для эффективной борьбы с постоянными киберугрозами нам нужен был инструмент, позволяющий быстро анализировать проблемы, возникающие в различных точках подключения, отслеживать общую ситуацию в сети или действия конкретной машины. Благодаря внедрению PT Network Attack Discovery мы смогли решить проблему контроля вредоносной активности в сетевом трафике, а также провели подготовку к выполнению требований регулирующих органов».

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 Network Attack Discovery для глубокого анализа сетевого трафика, выявления вредоносной активности в сетевом трафике, расследования инцидентов и выполнения требований регуляторов

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

ЗАДАЧА

Число целенаправленных атак на компании растет с каждым годом — в 2017 году с ними столкнулась уже каждая вторая организация[1]. Выявление и отражение этих атак становится крайне трудоемкой задачей: злоумышленники все чаще используют множественные векторы проникновения в инфраструктуру и сложное вредоносное ПО. В таких условиях процесс выявления скрытых угроз может тянуться от нескольких недель до нескольких лет.

Отдельным слабым звеном в защищенности компании является ее персонал: загружая вредоносные файлы и переходя по подозрительным ссылкам в интернете, сотрудники нередко провоцируют заражение всей инфраструктуры и компрометацию важных данных.

Как крупная медийная компания ВГТРК часто сталкивается с подобными угрозами. Осознавая существующие риски, отдел защиты информации (ОЗИ) ВГТРК принял ряд мер по повышению корпоративной защищенности. Эти меры включали внедрение системы сетевой безопасности для глубокого анализа взаимодействия компонентов сети и поиска аномалий в сетевых соединениях. Для решения этих задач требовался продукт, предоставляющий:

- агрегацию всех данных о сетевых взаимодействиях в инфраструктуре компании;
- возможность сбора и хранения сырого трафика и метаданных;
- инструменты ретроспективного анализа данных для поиска аномалий в трафике, происходивших в прошлом.

РЕШЕНИЕ

ОЗИ ВГТРК выбрал PT Network Attack Discovery (PT NAD) — комплексное решение сетевой безопасности, предназначенное для анализа сетевого трафика, выявления и расследования инцидентов ИБ.

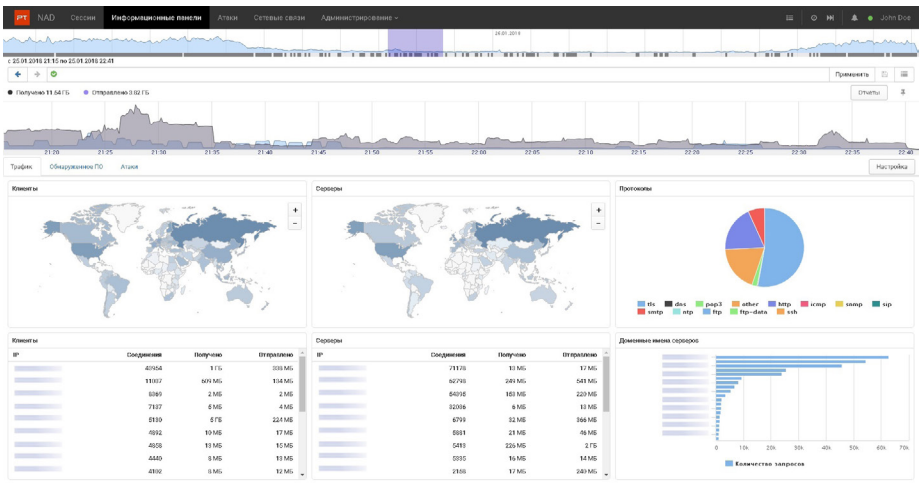
В ходе работы PT NAD захватывает, обрабатывает и хранит большие объемы сырого трафика. Разбирая протоколы до уровня L7, система на лету извлекает и сохраняет метаданные с уникальными параметрами каждого сетевого соединения: IP-адресами и значениями полей протоколов, репутацией передаваемых объектов, задействованными портами, приложениями.

1 Обзор «Кибербезопасность (2017–2018): цифры, факты, прогнозы», Positive Technologies.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- **Хранение сырого трафика и метаданных.** Гарантированный захват трафика скоростью до 10 Гбит/с, индексация и запись в файлы формата PCAP.
- **Реконструкция сессий.** Детальный разбор протоколов и извлечение метаданных о параметрах сетевых соединений, мощные механизмы поиска и фильтрации для быстрой навигации в больших массивах сохраненных данных.
- **Извлечение файлов.** Автоматизированное извлечение объектов, передаваемых через протоколы прикладного уровня: HTTP, FTP, POP3, SMTP, SMB, NFS и др.
- **Ретроспективный анализ.** Импорт файлов в формате PCAP из внешних источников для углубленного анализа и выявления не обнаруженных в прошлом атак.
- **Визуализация данных.** Подробная статистика событий безопасности, настраиваемые формы отчетов и графиков, наглядная карта сетевых взаимодействий.

Среди других решений класса Network Forensics продукт выделяет наличие встроенной системы пассивного выявления атак с помощью сигнатурных методов и поведенческого анализа. Кроме того, PT NAD поддерживает загрузку файлов с трафиком из внешних источников для проведения ретроспективного анализа. Анализ трафика в реальном времени в сочетании с ретроспективой позволяет не только выявлять текущую скрытую вредоносную активность, но и отслеживать векторы развития и хронологию атак.



РЕЗУЛЬТАТЫ

Уже в ходе пилотного проекта с помощью PT NAD специалистам ОЗИ ВГТРК удалось обнаружить в корпоративной сети несколько действующих ботнетов и другую скрытую вредоносную активность. Вскоре после перехода на боевую систему было выявлено и оперативно ликвидировано несколько программ-майнеров.

В результате проекта ВГТРК получила удобный инструмент для контроля вредоносной активности в сетевом трафике и возможность для выполнения требований регуляторов — в частности, новых требований к операторам связи и интернет-проектам, предусмотренных Федеральным законом № 35-ФЗ «О противодействии терроризму».

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