Евгения Красавина

Руководитель отдела продвижения и развития продуктов

PT MultiScanner: перезагрузка

Плохие новости — жить все еще страшно

Но почему все так

POSITIVE TECHNOLOGIES

2 квартал 2017 года:

Использование вредоносного ПО

150 Стран жертв массовых атак шифровальщиков

1M+ Зараженных устройств

$1B+ Ущерб

Источник: «Актуальные киберугрозы 2 квартала 2017 года», Positive Technologies
www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2017-rus.pdf

Время против нас

Растет разрыв между моментом компрометации и обнаружением

POSITIVE TECHNOLOGIES

62% результативных атак являются целевыми

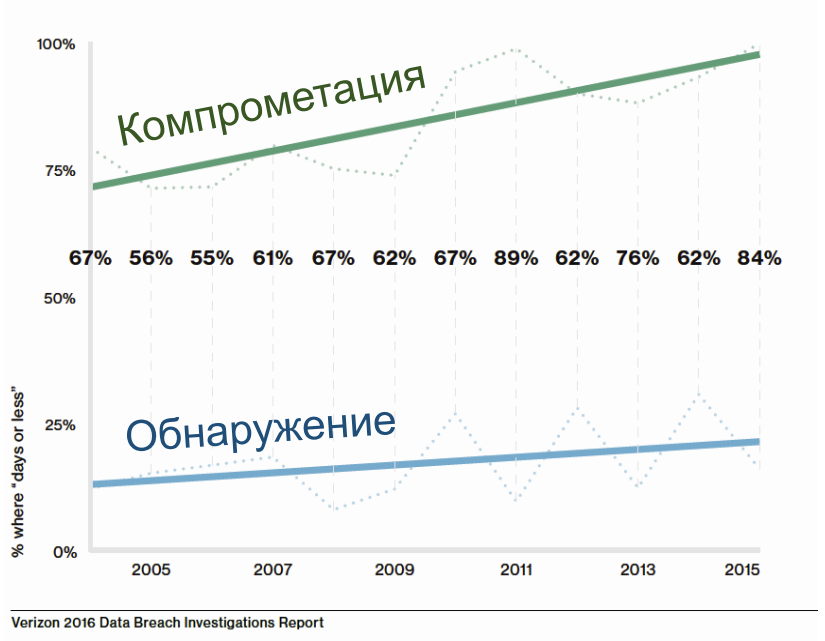
3 года в среднем злоумышленник присутствует в системе

10% атак выявляются самими жертвами

Источник: «Кибербезопасность 2016–2017: от итогов к прогнозам», Positive Technologies
www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf

Дни, часы, минуты
занимает компрометация

Недели, месяцы
проходят до обнаружения



Хорошие новости — мы знаем, в чем беда

Почему возникают сложности в выявлении заражений

POSITIVE TECHNOLOGIES

Сложность локализации угрозы заражения в инфраструктуре, как в настоящем, так и в прошлом

Отсутствие мультивендорного подхода для повышения вероятности детектирования

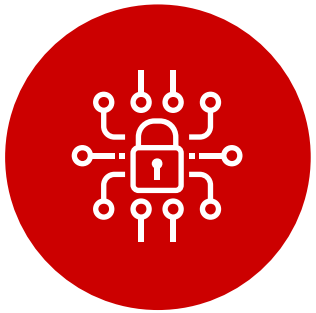
Отсутствие единой точки мониторинга всех вредоносных и не только объектов

Сложность создания одной точки мониторинга и выявления ВПО во всех возможных потоках распространения

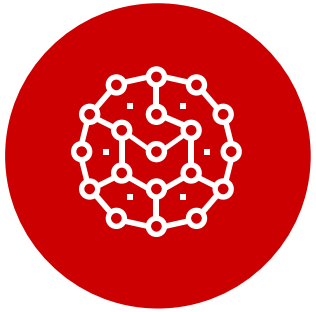

PT MultiScanner
SCANNING

PT MultiScanner — универсальное средство защиты от ВПО

POSITIVE TECHNOLOGIES



Локализация и предотвращение распространения заражения в инфраструктуре



Мультивендорная проверка передаваемых объектов на наличие ВПО

Единая точка хранения объектов, мониторинга и расследования распространения ВПО в инфраструктуре

Ключевые преимущества

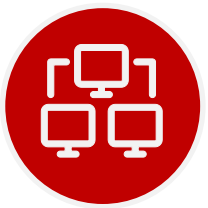
POSITIVE TECHNOLOGIES

ЭФФЕКТИВНО

- Выявление и блокирование массовых заражений за счет агрегации сканирований
- Гарантированный прирост детекта за счет AV-движков, репутационных списков, статического анализа
- Высокая скорость сканирования — до 150.000 объектов в час
- Умные вердикты на базе собственной классификации ВПО
- Ретроспективный анализ объектов для выявления скрытых угроз

НАДЕЖНО

- Поддержка офлайн обновлений антивирусных баз
- Обновление базы знаний и системы через сервер PT
- Шифрование хранимых в системе объектов
- Как результат — предотвращение возможных утечек конфиденциальных данных



УНИВЕРСАЛЬНО

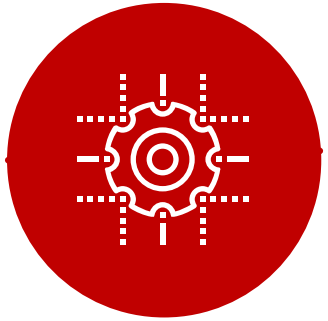
- Упрощенная интеграция в существующую архитектуру за счет поддержки ICAP/TAP/REST API
- Единое хранилище всех объектов, передаваемых в сети
- Быстрое конфигурирование
- Логичное встраивание в процесс расследования ИБ-инцидентов

Ретроспективный анализ — взгляд в прошлое

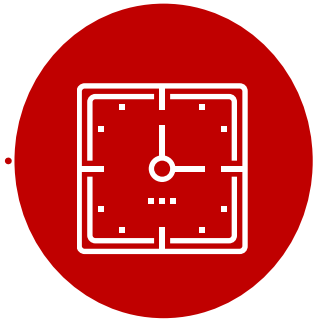
POSITIVE TECHNOLOGIES

При обновлении движков и репутационных списков

Единое хранилище проанализированных объектов



Автоматическое пересканирование без нагрузки на систему



Неограниченное по времени хранение файлов и метаданных

Закрытие актуальных потоков распространения

POSITIVE TECHNOLOGIES

Мониторинг и блокировка

ТРАФИК НА ВЕБ-ПОРТАЛЫ

СЕТЕВОЙ ТРАФИК

ФАЙЛОВЫЕ ХРАНИЛИЩА

ПОЧТА

ПОЛЬЗОВАТЕЛЬСКИЙ ВЕБ-ТРАФИК

Дополнительные «плюшки»

Услуга от PT ESC по расследованию инцидентов на базе PT MultiScanner

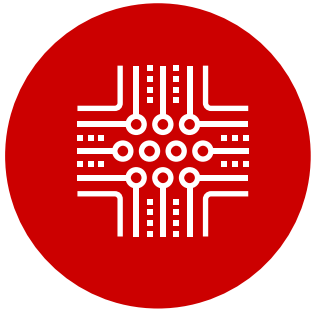
Периодическая экспертная верификация и оценка критичности найденных объектов

Внутренний пользовательский сервис для повышения уровня осведомленности пользователей в вопросах ИБ

Подход к пилотам — молниеносность

POSITIVE TECHNOLOGIES

Быстрое развертывание с новым инсталлятором, встроенными движками



Не после, не до, а вместе с существующими средствами защиты для демонстрации эффективности

Отправка демонстрационного ПО с сигнатурами вирусов, в случае если в живом трафике не нашли ничего серьезного, для наглядности

Подход к пилотам — подробности

POSITIVE TECHNOLOGIES

Исполнение

- PT Unified Chassis
- Виртуальные машины (Vmware/KVM/ Hyper-V)

Лицензия

- Софтверный ключ

Ресурсы

- 2 недели – 1 месяц
- Минимум 4 Core, 12GB 7200FPH

Лицензионная политика

POSITIVE TECHNOLOGIES

1 Исполнение

- PT Unified Chassis
- Виртуальные машины (Vmware/KVM/ Hyper-V)

2 Основные лицензии

- Мониторинг (3k / 7k / 25k / 50k / 150k FPH)
- Блокировка (3k / 7k / 25k / 50k / 150k FPH) +пассивный кластер
- Ручная загрузка (1k FPH)

3 Дополнительные лицензии

- Централизованное обновление
- Управление и консолидация

4 Сервисы PT ESC

- Мониторинг раз в неделю
- Мониторинг раз в месяц
- Одно расследование в год

Достаточно слов!
Теперь демо!

Контакты

POSITIVE TECHNOLOGIES

Евгения Красавина
Руководитель отдела продвижения и развития продуктов
ekrasavina@ptsecurity.com

Вместо тысячи слов
Записаться на бесплатный пилот
www.ptsecurity.com/ru-ru/products/multiscanner/#content-test