Корпоративная защита от передовых угроз и целенаправленных атак: как не купить «кота в мешке»

Яна Шевченко

Менеджер по развитию направления
защиты от передовых угроз

KASPERSKY lab

ПОЧЕМУ?

- Целенаправленная атака это непросто
- Недостаточно традиционных средств защиты
- Необходимы специализированные решения
- Важен комплексный подход

ЦЕЛЕНАПРАВЛЕННАЯ АТАКА

- **Направленна не только на крупные, но и на средние государственные и коммерческие структуры**

На всякую рыбу есть едок

- **Имеет конкретную цель, для достижения которой используются необходимые инструменты**

Бессмысленно выпускать стрелу без цели

Цель оправдывает средства

- **Тщательно подготовленный и продолжительный процесс**

Какие труды, такие и плоды

KASPERSKY lab

ЦЕЛЕНАПРАВЛЕННАЯ АТАКА

Одна дверь на замок, другая настежь

В атаке и граната-товарищ

В тихом омуте черти водятся

Применяется мультивекторный подход

Используются разные средства к построению

Может не создавать негативный фон и оставаться незамеченной длительное время

KASPERSKY lab

НЕМНОГО СТАТИСТИКИ

В 2017 году доля целевых атак выросла на 10% по сравнению с 2016 годом и составила **23%**, что поставило их в ряд самых стремительно развивающихся угроз*

В 2017 году каждая **4** крупная организация стала жертвой целенаправленной атаки*

22% всех опрошенных в России компаний подозревают, что стали жертвой не случайно, а целенаправленно*

*По данным исследования «Информационная безопасность бизнеса» (Kaspersky Lab Corporate IT Security Risks Survey) аналитического агентства B2B International по заказу «Лаборатории Касперского», апрель 2017 г.

К ЧЕМУ ПРИВОДЯТ УСПЕШНЫЕ ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ

- компрометация данных ключевых персон
- утеря критичных данных
- кража коммерческой тайны
- уничтожение ИТ инфраструктуры
- прерывание бизнес-процессов
- недоступность предлагаемых сервисов
- кража денежных средств

→ **К прямым и косвенным денежным потерям**

- ухудшение репутации
- потеря конкурентного преимущества
- утеря доверия клиентов
- уменьшение занимаемой доли на рынке

KASPERSKY lab

ПРЯМЫЕ И КОСВЕННЫЕ ПОТЕРИ

Прямые потери

Восстановление

- IT консалтинг
- Аудиторы
- PR активности
- Юристы

+

Потерянные возможности

- Потерянные сделки
- Упущенная прибыль

+

Простои

- Сокращение доходов

+

Последующие траты

Решения

- Закрытие имеющихся уязвимостей в инфраструктуре
- Замена систем
- Закупка дополнительных средств ИБ

+

Кадры

- Наем дополнительного штата специалистов
- Пересмотр бизнес процессов

+

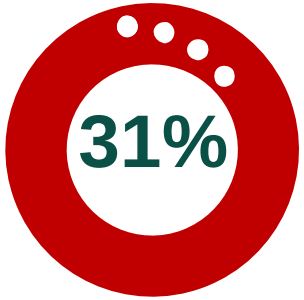
Обучение

- Повышение осведомленности сотрудников
- Улучшение экспертизы служб ИБ

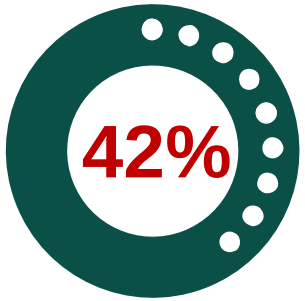
Для исключения повторения инцидентов

KASPERSKY lab

НЕМНОГО СТАТИСТИКИ



Опрошенных признали, что их организация не понимает, какая стратегия по борьбе с целевыми атаками и подобными им угрозами является эффективной*



Руководителей служб ИБ не уверены в эффективности существующей стратегии защиты против передовых угроз*

Компаний считают, что защита их организаций рано или поздно будет взломана*

*По данным исследования «Информационная безопасность бизнеса» (Kaspersky Lab Corporate IT Security Risks Survey) аналитического агентства B2B International по заказу «Лаборатории Касперского», апрель 2017 г.

KASPERSKY lab

ПОЧЕМУ НЕДОСТАТОЧНО ТРАДИЦИОННЫХ СИСТЕМ ЗАЩИТЫ

Во-первых

Из-за специфики целенаправленных атак и подготовки к ним, таких как:

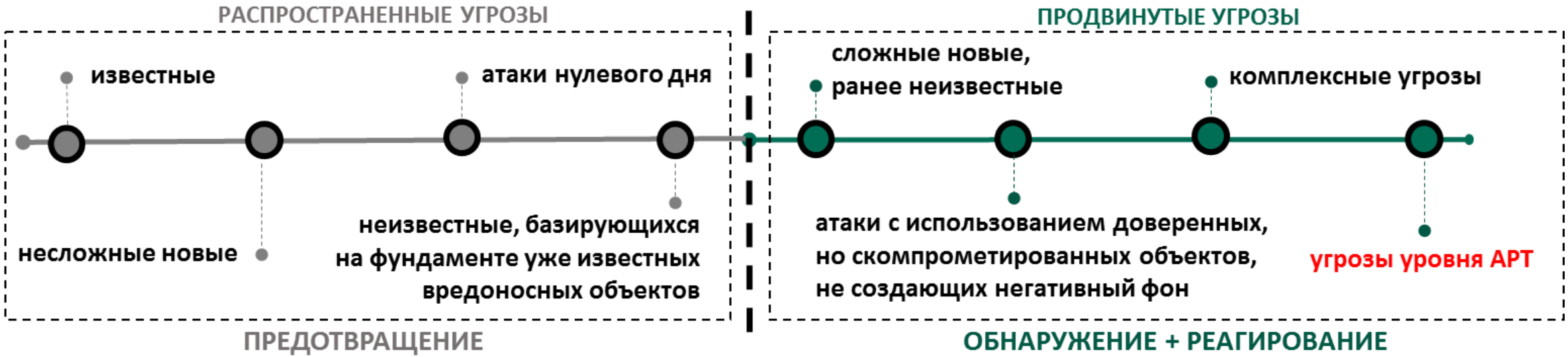
- детальное изучение используемых средств защиты с целью их обхода;
- написание уникального ПО и закрепление его в инфраструктуре цели;
- использование в атаках доверенных, но скомпрометированных объектов, не создающих негативный фон;
- применение мультивекторного подхода к проникновению;
- скрытность и пр.

Во-вторых

Из-за присущих традиционным средствам защиты технологических ограничений:

- обнаружение направлено только на распространённые (несложные) угрозы, уже известные уязвимости и методы;
- нет встроенного сопоставления и корреляции детектов в единую цепочку событий;
- нет технологий выявления отклонений в нормальных активностях и анализа работы легитимного ПО.

ПОЧЕМУ НЕОБХОДИМ КОМПЛЕКСНАЙ ПОДХОД



✓ **использование традиционных решений эшелонированной защиты (NGFW, EPP):**

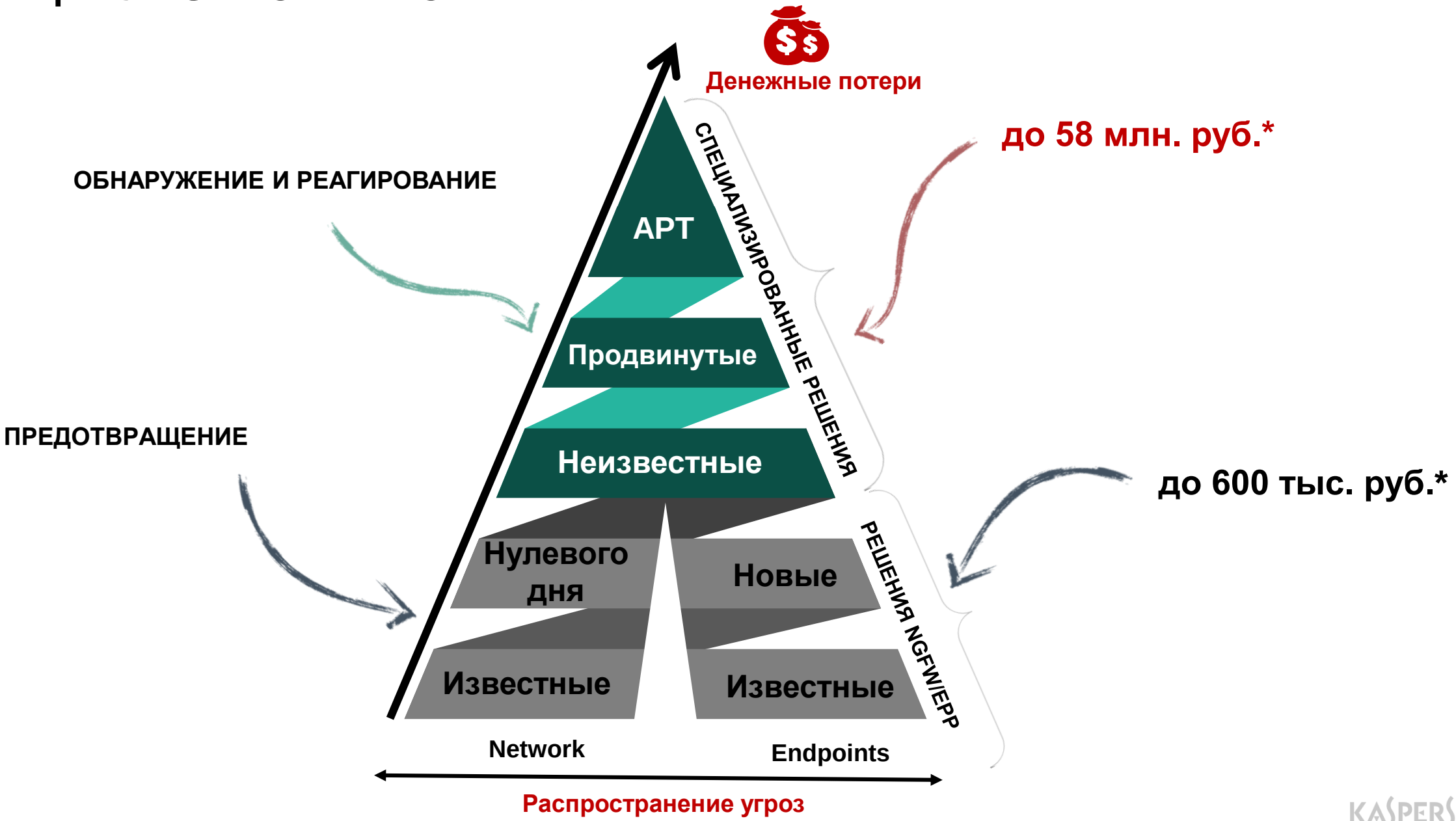
- эффективная борьба против классифицированных типов (несложных) угроз;
- автоматическое блокирование, без необходимости расследования инцидентов;
- исключение из спектра анализа распространённых угроз;
- сокращение объема поиска, помощь в анализе продвинутых угроз.

✓ **использование специализированных решений:**

- обнаружение сложносоставных атак, с сопоставлением различных событий в единый инцидент;
- ретроспективный анализ;
- многоуровневые механизмы обнаружения на базе динамического машинного обучения и поведенческого анализа;
- отправка вердиктов в NGFW, EPP.

KASPERSKY lab

СПЕЦИАЛИЗИРОВАННОЕ РЕШЕНИЕ



*Стоимость одного незакрытого инцидента по данным Kaspersky Lab Report 2017. Analyzing the state of IT Security

ЧТО НЕОБХОДИМО УЧИТЫВАТЬ ПРИ ВЫБОРЕ РЕШЕНИЯ

KASPERSKY lab

ЧТО НЕОБХОДИМО УЧИТЫВАТЬ В КОМПЛЕКСНОМ ПРОЕКТЕ

Защита рабочих мест

Сетевые решения защиты

Специализированное решение по обнаружению

Специализированное решение по реагированию

Расширенная техническая поддержка

Выделенный эксперт по ИБ

Локальная репутационная база угроз для изолированных сред

Профессиональные сервисы

- сервисы по активному поиску угроз
- цифровая криминалистика
- портал аналитических отчетов об угрозах
- анализа событий ИБ и реагирования на инциденты

- Обучение IT администратора
- Тренинг по работе с системами
- Обучение по расследованию инцидентов
- Тренинг по Yara-правилам

KASPERSKY lab

ВЛОЖЕННЫЕ ИНВЕСТИЦИИ

Вложенные инвестиции в решения по противодействию целенаправленным атакам и передовым угрозам нацелены на:

- **предотвращение прямых потерь** и **последующих трат** за счет раннего обнаружения признаков компрометации инфраструктуры и принятия соответствующих мер;

- **сокращение трудозатрат** высокооплачиваемых специалистов на ручные рутинные операции;

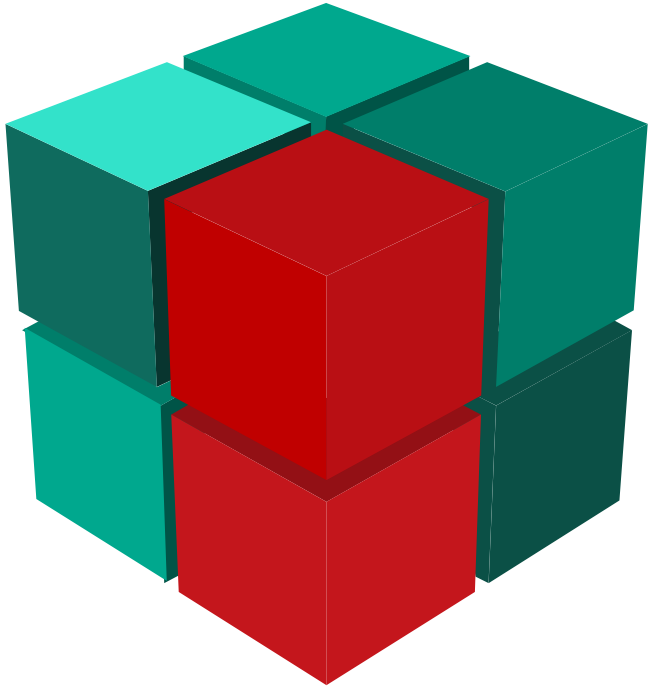
- **увеличение продуктивности** сотрудников службы ИБ, без необходимости расширения штата: качественное выявление скрытых угроз, повышение скорости и точности реагирования;

- **оптимизация затрат** на процесс расследования инцидентов, уменьшения степени вовлечения сторонних департаментов;

- **повышение общего уровня информационной безопасности**, с сохранением ранее вложенных инвестиций;

- автоматизация процессов расследования инцидентов в **соответствии с внутренними/внешними требованиями**.

СПАСИБО!



LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com