POSITIVE TECHNOLOGIES

Атака через «дочку»

История одного расследования

Виктор Рыжков
Руководитель группы систем защиты от целенаправленных атак

ptsecurity.com

План вебинара

1 Вводная

- Целенаправленная атака (APT)
- APT сегодня: статистика;
- Тренд APT: компрометация сторонней организации.

2 Расследование

- Инструмент расследования;
- Разбор кейса;
- Ответы на вопросы.

Основные определения

Advanced persistent threat (APT)

Определение

Любая атака, которая обходит имеющиеся средства защиты, остается незамеченной и продолжает наносить ущерб*

* Defining the advanced persistent threat, Gartner Blog Network

Основные определения

Advanced persistent threat (APT)

Определение

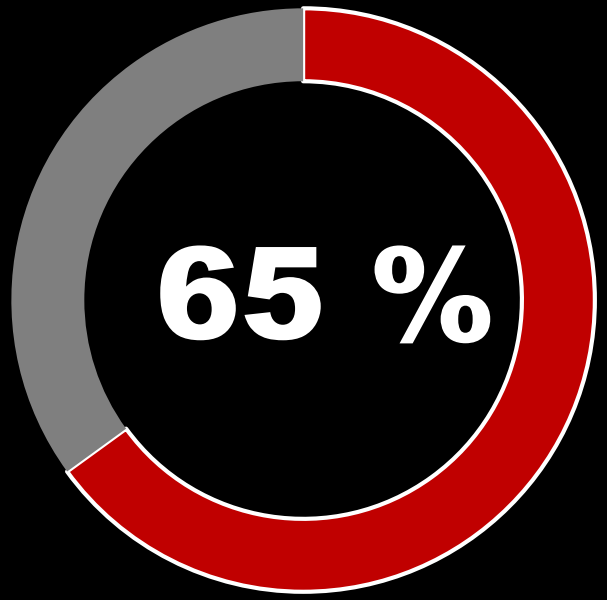
Любая атака, которая обходит имеющиеся средства защиты, остается незамеченной и продолжает наносить ущерб*

Сегодня

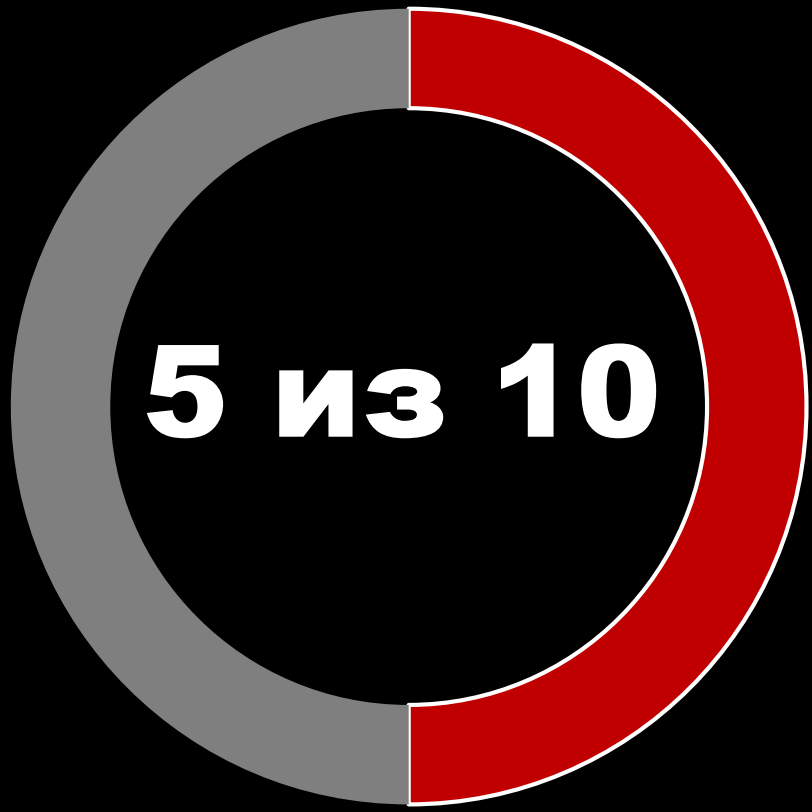
- многофазные;
- распределены по времени;
- могут готовиться под конкретную инфраструктуру;

* Defining the advanced persistent threat, Gartner Blog Network

APT сегодня



атак были целенаправленными
в Q3 2019*



группировок начинают атаку с компрометации
ресурсов сторонних организаций**

- Актуальные киберугрозы: III квартал 2019 года, Positive Technologies

** APT-атаки на топливно-энергетический комплекс России: обзор тактик и техник, Positive Technologies

Расследование

Компания

Invulnerable corp.

- 10 000+ сотрудников;
- 5+ дочерних организаций;

Invulnerable child

- 250+ сотрудников;
- существуют с 2011 г.;
- стали ДЗО в 2019 г.;

Расследование

Компания

Invulnerable corp.

- 10 000+ сотрудников;
- 5+ дочерних организаций;

Invulnerable child

- 250+ сотрудников;
- существуют с 2011 г.;
- стали ДЗО в 2019 г.;

Инцидент

Когда

- Июль 2019;

Условия воспроизведения

- Часть, согласованная с заказчиком;
- Воспроизведено в нашей лаборатории;
- IP, DNS-имена, ссылки заменены;

Расследование

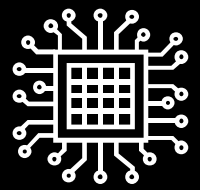
Компания

Invulnerable corp.

- 10 000+ сотрудников;
- 5+ дочерних организаций;

Invulnerable child

- 250+ сотрудников;
- существуют с 2011 г.;
- стали ДЗО в 2019 г.;



PT Network
Attack Discovery

Инцидент

Когда

- Июль 2019;

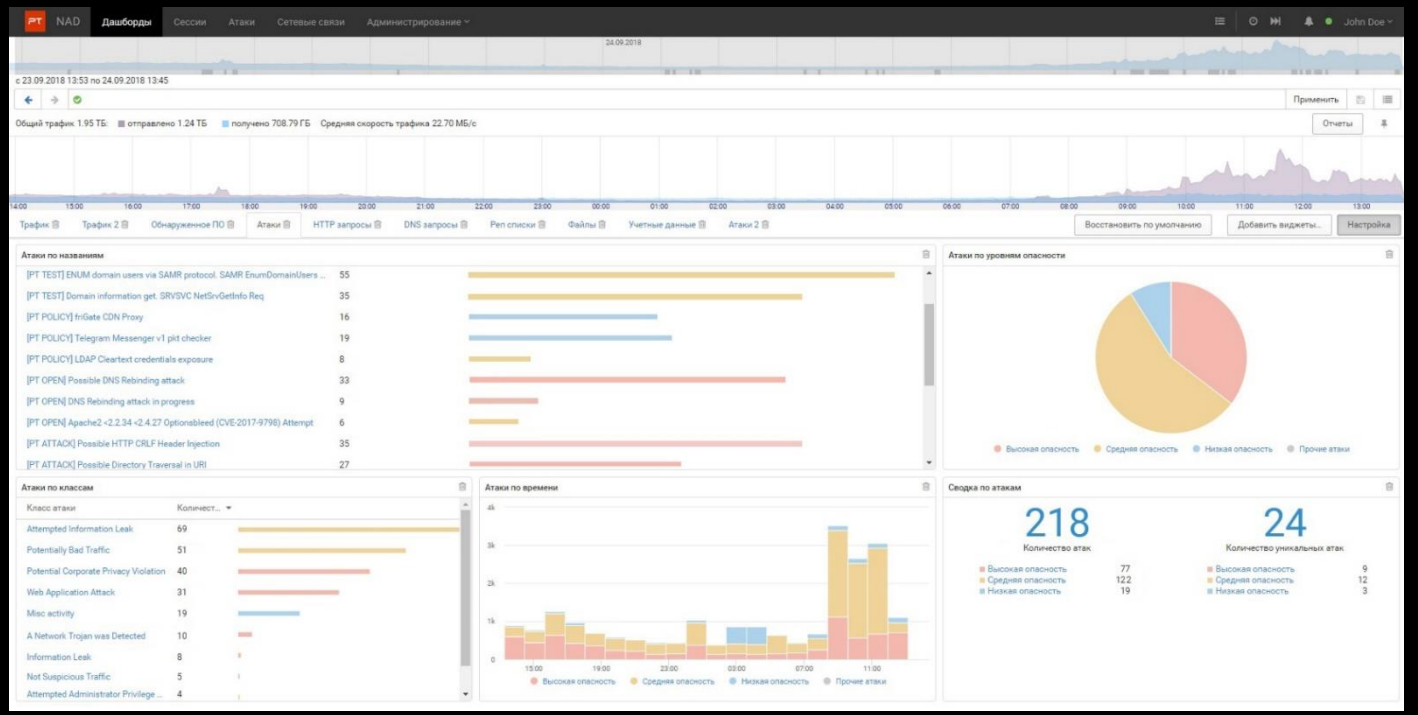
Условия воспроизведения

- Часть, согласованная с заказчиком;
- Воспроизведено в нашей лаборатории;
- IP, DNS-имена, ссылки заменены;

PT Network Attack Discovery

PT NAD — система глубокого анализа сетевого трафика (NTA) для выявления атак на периметре и внутри сети.

Система знает, что происходит в сети, обнаруживает активность злоумышленников даже в зашифрованном трафике и помогает в расследованиях.



NTA — решения класса Network Traffic Analysis

Видео…

Что было сделано

В основной организации

На Domain controller

- Смена паролей;
- Запрет на полное делегирование (Full-delegation across trusts)

На рабочих станциях сотрудников

- Чистка файлов.

В дочерней организации

На сервере Exim

- Обновлена версия Exim;
- Удален загруженный файл(в т.ч. из автозапуска)

На сервере MS Exchange

- Отключение возможности Relay в реестре;
- Правка набора прав учётной записи MS Exchange на DC.

Рекомендации

Анализ трафика

Внешнего

- для выявления внешних злоумышленников.

Внутреннего

- для выявления внутренних злоумышленников.

Хранение и индексация

Индексация всего трафика

- Для проведения расследований;
- Независимо от обнаружений;

Хранение сырого трафика

- Для доказательной базы
и детального ручного анализа;

Полезная нагрузка

Про уязвимости

CVE-2019-10149 (Exim)

- CVE-2019-10149
- github.com/dhn/exploits/tree/master/CVE-2019-10149

CVE-2018-8581 (MS Exchange)

- CVE-2018-8581
- dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/
- github.com/ptresearch/AttackDetection

Printer Bug harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/

Полезная нагрузка

Про PT NAD

Пропилотировать ptsecurity.com/ru-ru/products/network-attack-discovery/

Чат в телеграм t.me/PTNADChat

Вебинары

- Про контроль сетевого комплаенса - ptsecurity.com/ru-ru/research/webinar/298584/
- Про выявление малварей в шифрованном трафике - ptsecurity.com/ru-ru/research/webinar/298091/
- Про обнаружение атак на AD - ptsecurity.com/ru-ru/research/webinar/290582/
- Кейсы threat hunting с PT NAD - ptsecurity.com/ru-ru/research/webinar/302112/

POSITIVE TECHNOLOGIES

Ваши вопросы?

Буду рад ответить

Виктор Рыжков
Руководитель группы систем защиты от целенаправленных атак
vryzhkov@ptsecurity.com
t.me/PTNADChat

ptsecurity.com