Кейс. Расследование атаки: нелегальный «пентест» с кражей данных

›› Расследование и реагирование

ЖЕРТВА АТАКИ

Дочерняя компания крупной медицинской организации

Цель атаки:
Финансовая выгода

Уровень атаки:
Кибермошенники

Способ проникновения:
Взлом через публично доступный сервис выдачи пропусков

Получение доступа с помощью скомпрометированного open-source-менеджера паролей

ДЕТАЛИ АТАКИ

1. Атакующие сообщили о взломе и потребовали выкуп за «отчет по пентесту»

2. Действия жертвы: отказ платить и безуспешное расследование собственными силами

3. Итог: украдена часть чувствительных данных компании и переписка пользователей

4. Чудесное спасение: ошибка атакующих на последнем этапе спасла от шифрования всей сети

СХЕМА ХРОНОЛОГИИ АТАКИ

Указана на следующем слайде

SOLAR | 4RAYS by SOLAR

РЕШЕНИЕ

Расследование и реагирование на инциденты (DFIR)

ДЕТАЛИ РАССЛЕДОВАНИЯ

[01] Компания X использовала open-source-решение для выдачи пропусков. Атакующие через уязвимость этого решения получили доступ к удаленному выполнению команд на сервере

[02] Атакующие получили доступ к сервису хранения паролей, который также имел уязвимость. Получен доступ ко всему, что можно зашифровать

[03] Атакующие потребовали выкуп за предоставление доступов и «отчета» об найденных уязвимостях

[04] Заказчик провел расследование своими силами, но не смог обнаружить, что сервис для хранения паролей скомпрометирован. У атакующих остался доступ внутрь инфраструктуры заказчика, и они присутствовали в ней несколько месяцев. Далее они запустили шифрование

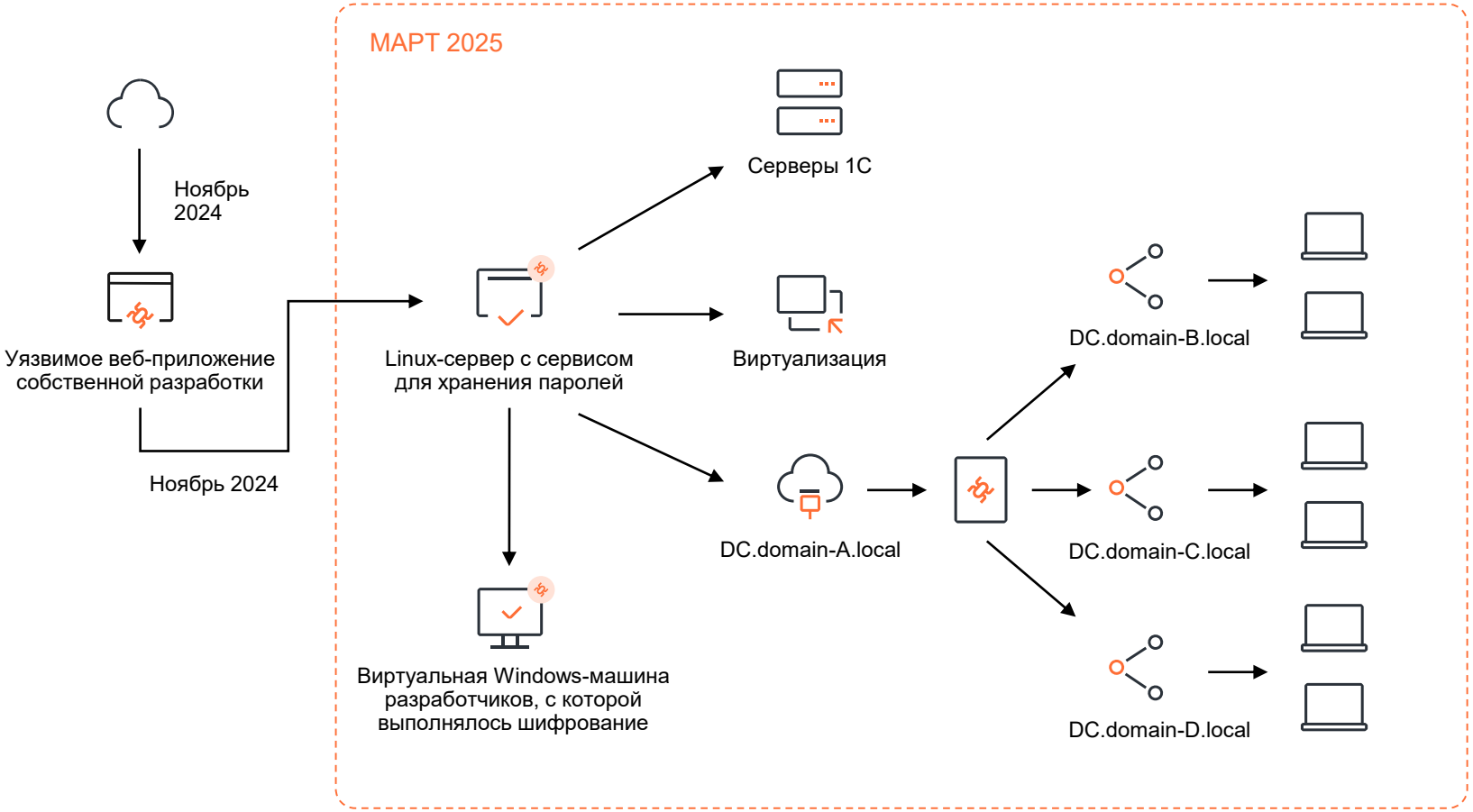
[05] Привлечение команды Solar 4RAYS помогло обнаружить следы атакующих, локализовать инцидент и сформировать рекомендации по его недопущению в дальнейшем

КЕЙС. РАССЛЕДОВАНИЕ АТАКИ: НЕЛЕГАЛЬНЫЙ «ПЕНТЕСТ» С КРАЖЕЙ ДАННЫХ

SOLAR | 4RAYS by SOLAR

›› Расследование и реагирование

ХРОНОЛОГИЯ АТАКИ



РЕКОМЕНДАЦИИ

по возможной остановки атаки и ее предотвращению

- Соблюдение базовых правил кибергигиены Подробнее
- Периодическая оценка защищенности инфраструктуры (пентесты, киберучения и т. п.)
- Подключение к мониторингу и анализу инцидентов (SOC), потокам данных TI Feeds*
- Мониторинг DNS-трафика, блокировка вредоносных и фишинговых доменов
- Проведение Compromise Assessment при подозрении на атаку

* *Многие индикаторы компрометации уже были известны и могли бы заблокировать атаку*