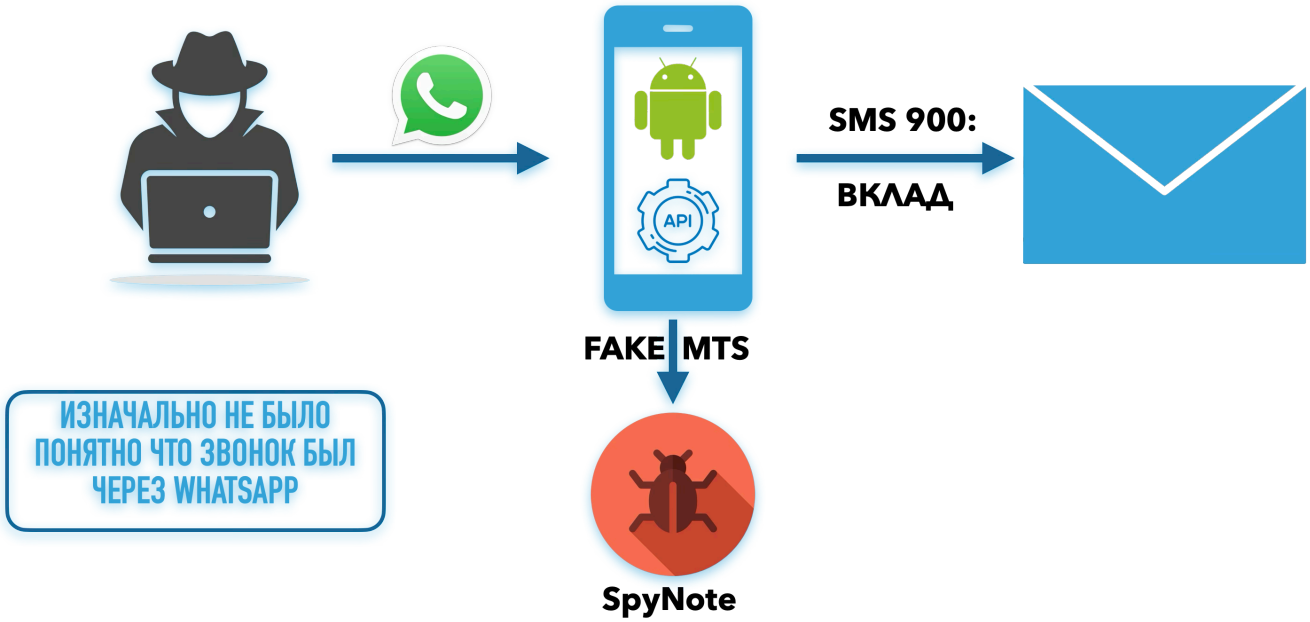
Попытка кражи денежных средств с Android телефона

Оглавление

Схема инцидента



Общее описание работы

Последнее время стал активно распространяться троян Android.SpyNote (https://xakep.ru/2024/10/23/spynote-attacks/)

Вам в задании необходимо рассмотреть представленный кейс из реальной жизни, дать свое представление о дальнейшем развитии событий и разложить весь инцидент по модели Cyber-Kill Chain

---

Кейс инцидента

1. Участвующее лицо - пожилой человек
2. На телефон по средствам WhatsApp поступает звонок якобы от тех поддержки МТС с информацией о том, что баланс телефона отрицательный.
3. Они предлагают помочь пополнить баланс и человек соглашается

4. Далее происходит несколько возможных вариантов ввиду того, что нет понимая как было конкретно
   1. Они объясняют человеку как из play market поставить приложение для удаленного управления
   2. Или они объясняют как разрешить установку приложения из недоверенных источников (Whatsapp)
5. В результате данных действий на телефоне появилось два приложения
   1. Первое - фейковое MTS с трояном внутри SpyNote, при этом данное приложение не отражается в библиотеке приложений
   2. Некое второе приложение возможно вида удаленного помощника (Возможно управление происходит через фейковое приложение MTS на основе возможностей SpyNote)
6. Далее происходит отправка СМС сообщения на номер 900 с текстом "вклад" для выяснения наличия средств на банковских счетах (данную операцию производится либо посредствам трояна, либо удаленного помощника)
7. На фоне происходящего человек включает авиа режим на телефоне и соответсвенно все операции прекращаются и денежные средства в безопасности

Структура ответа

1. Кратко дать описание трояна SpyNote и как он функционирует
2. Найти примеры зловредных средств удаленного помощника, которые могут быть также установлены на телефон по типу SpyNote
3. Дать приблизительное описание как произошла отправка СМС (троян или удаленный помощник)
4. Дать возможное описание развития событий по краже денежных средств (смс или сбербанк онлайн)
5. Разложить весь инцидент по модели Cyber-Kill Chain