Подготовка 1

Установить контакты, выработать процедуры, собрать информацию для оптимизации временных затрат во время инцидента.

- Служба поддержки должна иметь формализованный процесс на случай выявленного заражения мобильного устройства: заменить инфицированный мобильный терминал и изолировать его для анализа и криминалистического расследования.

- Заручиться хорошим знанием стандартных процессов и основных программ мобильного терминала. В случае необходимости, обратиться за помощью к специалисту по мобильным устройствам и ОС.

- Проверить мобильный терминал на предмет выявления аномальной сетевой (большие объемы данных) или телефонной (крупные счета) активности.

Обнаружение 2

Обнаружить проблему, определить затрагиваемый периметр, привлечь заинтересованных лиц.

Признаки заражения мобильного терминала:

- Регулярные оповещения антивируса;
- Аномальная активность системы; медленное выполнение заданий;
- Аномальная сетевая активность; медленное Интернет соединение.
- Система перезагружается или выключается без видимой причины;
- Самопроизвольное прекращение работы некоторыми программами;
- Пользователь получает необычные SMS, или MMS сообщения;
- Аномально высокие счета за пользование телефоном или большие объемы использованного Интернет траффика;
- Необычные звонки на незнакомые телефонные номера, совершенные в необычное время суток.

Необходимо собрать данные о посещенных веб-ресурсах..

Осведомитесь у пользователя о привычках использования мобильного терминала: посещаемые веб ресурсы, установленные программы “не-из-коробки”. Сверить полученную информацию с корпоративной политикой использования мобильных терминалов.

Сдерживание 3

Минимизировать последствия инцидента

- Снабдить пользователя временным терминалом на время проведения расследования.
- Произвести резервное копирование данных на мобильном терминале.
- Физически удалить батарею для пресечения любых соединений (Wi-Fi, Bluetooth).
- Произвести антивирусную проверку мобильного терминала подсоединив к стационарному компьютеру.

- Передать инфицированный терминал со всеми аксессуарами (SIM карта, аккумулятор, сетевой кабель, карты памяти) вашей команде безопасности. Данная команда изолирует и передаст вредоносные компоненты компьютерным криминалистам, антивирусным лаборато-риям и т.д.

Устранение 4

Принять меры по устранению угрозы и избежанию схожих инцидентов в будущем.

В случае использования на мобильном терминале пароля или шифрования, постараться получить их или обойти данные способы защиты. В противном случае расследование может столкнуться с серьезными ограничениями.

Для проведения криминалистического расследования терминала понадобится использование специализированного оборудования и ПО, например:

Бесплатное ПО: iPhone Analyzer (iOS), Katana Forensics Latern Lite (iOS), SAFT (Android), XDA Utils (Multiplatform), Mobile Internal Acquisition Tool (Symbian, Windows Mobile), TULP2G, viaForensics (Android).

Коммерческое ПО: Blacklight (iOS), Cellebrite Mobile Forensics, Micro Systemation XRY, Oxygen, Paraben и др.

Порядок действий:

- Удалить SIM-карту
- Восстановить историю звонков, посещения сайтов и все доступные логи;
- Восстановить все логии серверных соединений;
- Идентифицировать и удалить вредоносный код и сопряженные файлы;
- Если вредоносное ПО интегрировано или закамуфлировано под определенное приложение, идентифицировать и удалить приложение.

Восстановление 5

Восстановить систему до состояния нормального функционирования

Если пользователь нуждается в восстановлении потенциально инфицированных данных, используйте антивирус для изоляции и безопасного удаления вредоносных компонентов.

Восстановить все необходимые данные из резервной копии или иного надежного источника.

По окончанию расследования отформатировать (wipe/hard reset) мобильный терминал и откатить к заводским настройкам с актуализованной версией firmware.

После инцидента 6

Задокументировать детали инцидента, обсудить извлеченные уроки, оптимизировать процессы защиты.

Отчет

Написать отчет об инциденте заражения; сделать отчет доступным причастным лицам. Раскрыть следующие темы:

- Причины инфекции
- Действия и сроки
- Верные действия
- Неверные действия
- Стоимость инцидента

Капитализация опыта

Формализовать и задокументировать опыт, накопленный в результате управления инцидентом с целью увеличения эффективности будущих действий.

Разобрать инцидент с пользователем для повышения уровня осведомленности о проблемах безопасности.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

cert.sg@socgen.com / cert.societegenerale.com / @certsg

IRM #9

Вредонос на мобильных платформах

Анализ зараженных мобильных терминалов

Автор IRM: CERT SG

Версия IRM: 1.2 (RU)

Об IRM

Данная методология по реагированию на инциденты ИБ является кратким руководством, предназначенным вниманию специалистов, работающих над проблемами безопасности:

- Системные администраторы
- Члены Security Operation Centers
- Начальники и представители отделов ИБ
- Представители CERT/CSIRT/IRT

Распространение IRM возможно в рамках SG Group.

В случае обнаружения признаков инцидента, следуйте рекомендациям IRM, делайте заметки, не поддавайтесь панике и немедленно оповестите свой CERT.

Фазы управления инцидентами ИБ

Шесть фаз управления инцидентами ИБ:

- **Подготовка**: подготовится к управлению инцидентом
- **Обнаружение**: идентифицировать проблему
- **Сдерживание**: ограничить негативный эффект
- **Устранение**: ликвидировать угрозу
- **Восстановление**: восстановить до нормального
- **После инцидента**: формализация и совершенствование процесса управления инцидентом

IRM предоставляет детальную информацию по каждой из фаз.