більш ефективного використання цього новітнього інформаційного ресурсу в поліцейській діяльності.

Бібліографічні посилання:

1. Доручення НПУ від 29.01.2019 № 137/02/14-2019 «Про віднесення об’єктів транспортної інфраструктури до підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи ІПНП»
2. Інформаційне забезпечення професійної діяльності: навч. посіб. / І.В.Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2018. – 218 с.

Махницький О. В.
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

МОБІЛЬНІ ДОДАТКИ ДЛЯ БОРОТЬБИ З COVID 19. ЗАРУБІЖНИЙ ДОСВІД

У даній статті представлений огляд додатка eRouška - Part of Smart Quarantine, розробленого урядом Чехії для контролю і попередження поширення COVID19.
eRouška - це офіційний чеський додаток з повідомленнями про вплив, розроблене Міністерством охорони здоров'я і NAKIT (Національним агентством інформаційних і комунікаційних технологій). Для боротьби з епідемією COVID-19, додаток направлено на повідомлення користувачів, які піддаються ризику передачі вірусу. Грунтуючись на історії контактів з іншими потенційно заразними користувачами, додаток дає інструкції, як діяти, щоб мінімізувати поширення епідемії. Однак програма не є діагностичним або медичним інструментом.

У додатку використовується технологія Bluetooth Low Energy , яка зводить до мінімуму споживання енергії, і воно не збирає дані про геолокації , включаючи дані GPS. Додаток розроблено і випущено в повній відповідності з вимогами « Політики API » повідомлень про розкриття інформації, повністю відповідає GDPR і не збирає і не обробляє будь-які особисті дані, які можуть ідентифікувати користувача або його мобільний пристрій, такі як його ім'я, адреса або номер телефону. eRouška може визначити, що два користувача були в контакті, не знаючи, хто ці користувачі і де сталася зустріч.

Що б не перевантажувати огляд технічними термінами не аналізуватимемо вихідний код і обмін додатки з сервером. Практично вся робота відбувається на сервері Google, через сервіси Google Play. Сервер чеського МОЗ задіюється тільки в тому випадку, якщо є позитивний результат тесту на COVID-19.

Використання технології Bluetooth. Система побудована на базі «маяків» BLE (Bluetooth Low Energy Beacon). Спочатку ця технологія проектувалася для захисту предметів від втрати-крадіжки, а також для навігації в приміщеннях. У 2013 році

Apple представила свою технологію iBeacon , а в 2019, з релізом iOS 13, задіяла ці маяки для пошуку пристроїв через Find My . Рік тому ніхто не думав, що ці маяки будуть використовувати для боротьби з вірусом. Bluetooth пристрій при цьому працює в broadcast режимі, передаючи в ефір певні дані. Пристрої, що знаходяться поруч, можуть ці дані прочитати і якось використовувати, в тому числі і передати далі. Ось такими віртуальними рукостисканнями і обмінюються пристрої, відстежуючи контакти з зараженими COVID-19.

Як забезпечується приватність. Звичайно ж, в новому додатку вже немає номера телефону і SMS- ки для активації. Все, що потрібно зробити, це запустити додаток і дозволяти пристрою використовувати API Exposure Notifications . У будь-який момент додаток можна поставити на паузу. Кожен день на пристрої генерується Temporary Exposure Key (TEK) - абсолютно випадковий набір з 16 байт. Але і він не передається в ефір, щоб виключити атаку з перехопленням коду і його емуляцією на іншому пристрої. В ефір передається Rolling Proximity Identifier (RPI). Цей ідентифікатор змінюється кожні 10 хвилин, що робить перехоплення трафіку безглуздим. Спочатку з TEK за допомогою алгоритму HKDF генеруються два ключі, шифрування: RPI Key і AEM Key . Ключем RPI ми шифруємо поточний час, що вимірюється в 10-хвилинних інтервалах. А ключем AEM шифруємо метадані. metadata у цьому процесі поки не використовується і є резервним параметром для майбутніх версій. Далі програма бере поточний час, додає до нього ще кілька байт padding -а і шифрує його нашим RPI ключем. Провести зворотне перетворення з RPI в TEK практично неможливо, теоретично це займе багато мільйонів років навіть з використанням всіх комп'ютерних потужностей на планеті. TEK залишається секретним до того моменту, коли потрібно повідомити про те, що людина заражена COVID19. Після цього, за згодою користувача, його ключ публікується в базі. Ця база зберігається на серверах Google Play і додаток робить запити для її отримання Рис.1:

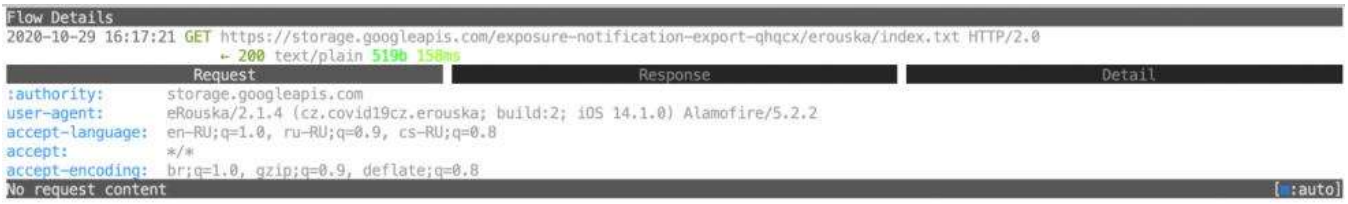

Рис. 1

Ім’я Файлу - це часовий проміжок, рівний однієї доби. Усередині зіп архіву знаходяться два файли: export.bin і export.sig . Перший файл містить protobuf зі структурою, в яку входить трохи службової інформації і, власне, список ключів TEK. Для кожної людини тут буде до 14 ключів, так як мається на увазі, що за 2 тижні до позитивного тесту він міг бути носієм зарази. Аналіз структури показав, що кожен ключ займає 31 байт, тому за розміром файлу можна приблизно прикинути, скільки заражених система виявила за день.

У разі визначення контакту з зараженим виконуються наступні дії. На пристрої у нас є свіжі бази TEK, а також величезна колекція RPI разом з інформацією про рівень сигналу Bluetooth , за яким приблизно можна визначити

відстань. Ці дані, до речі, інтерпретуються так, як вибере МОЗ тієї країни, в якій запроваджено систему. Наприклад, автори програми eRouška стверджують, що в Чехії небезпечним вважається контакт тривалістю більше 15 хвилин на відстані менше, ніж 2 метри. В інших країнах це може бути по-іншому. Перевірка контактів здійснюється виключно в самому додатку і ці дані нікуди не передаються. Додаток просто повідомляє користувачеві про можливий контакт з зараженим . Для перевірки додаток бере все викачані TEK і повторює для них ту ж процедуру, яку я описував в розділі «Як здійснюється приватність». Тобто, ми беремо TEK, час, метадані та заново вважаємо все RPI, які міг передати в ефір телефон зараженого . Далі проста процедура порівняння і фільтрація по часу контакту і відстані.

Користувач ставить додаток і забуває про нього. Все працює в фоновому режимі. До тих пір, поки не виникне дві ситуації:

Система виявила можливий контакт з зараженим. Буде просто попередження від програми. Додаток нікому про це не повідомляє, крім користувача. Далі вже користувач сам вирішує, що йому робити. Він може піти здати тест, може обмежити на час контакти з іншими людьми, може взагалі нічого не робити. Це його соціальна відповідальність.

Користувач з якої-небудь причини здав тест, і він виявився позитивним. У цьому випадку на телефон користувача приходить два SMS повідомлення: про те, що тест позитивний, і код верифікації для додатка eRouška . Далі знову ж рішення за користувачем. Він може просто проігнорувати цей код і нічого за це не буде. Або може опублікувати свої анонімні ключі в базі. Для цього він просто вводить отриманий код в додаток, і воно передає ключі на сервер.

Висновки

Система зроблена дуже грамотно і дійсно забезпечує анонімність. Поставити додаток нескладно, і воно абсолютно ні до чого не зобов'язує. Використання BLE маяків не призводить до істотного витрати батареї. І можливо, комусь буде спокійніше психологічно бачити, що контактів з зараженими не було. Але, з іншого боку, доведеться понервувати, якщо з'ясується, що контакт був.

Згідно з даними Google Play , додаток для Андроїда скачали більше мільйона жителів Чехії. Для iOS таких даних немає. Таким чином, програма встановлена приблизно у 12-15% чехів. Звичайно ж, дуже цікаво, скільки в базі заражених. Отже, в день, коли офіційна статистика говорила про 15664 позитивних тестах, в базу потрапило близько 500 ключів користувачів. З цього складно зробити якийсь висновок, але видно, що далеко не всі користувачі програми публікують свої ключі.

А тепер подивимося на цей додаток з точки зору подвійного призначення. А саме як теоретично можна використовувати цю систему для розслідувань. Ну або як це можуть використовувати «погані хлопці». В системі все добре до тих пір, поки в наших руках не виявилося сам пристрій. Або, ще краще, два пристрої від двох підозрюваних. Наприклад, вони кажуть, що взагалі один одного не знають і ніколи не бачили. Але на пристрої є маса інформації, яка може довести, що це не так. Як відомо, iPhone зберігає внутрішню базу координат, з якої можна визначити місце розташування телефону в певний момент часу. Більш того, наш підозрюваний може ще користуватися фітнес трекера , які визначають навіть кількість кроків. Але GPS координати не так точні, щоб зробити висновок, що люди перебували поруч один з

одним. А ось ті самі RPI, отримані через BLE beacons , скажуть нам, що люди були дуже близько один до одного. Плюс, ми самі можемо визначити, чи були у підозрюваного контакти із зараженими COVID19 , хоча для криміналістики це не така суттєва інформація. Звичайно ж, на всіх сучасних пристроях інформація захищена від несанкціонованого доступу. Але є дуже багато вразливостей, якими успішно користуються як експерти-криміналісти, так і кримінал. Більш того, користувач може сам залишити свій пристрій відкритим, достатньо не встановити на нього пароль доступу. І навіть якщо він стоїть, пристрій може бути вилучено у розлоченому вигляді.

Тому бережіть свої дані. Користуйтеся сучасними пристроями, ставте стійкі паролі, не залишайте розблокувати пристрій без нагляду. Ця рада універсальний і стане в нагоді в будь-якій ситуації.

Мельнікова О.О. кандидат юридичних наук, викладач кафедри кібербезпеки та інформаційного забезпечення факультету підготовки фахівців для підрозділів кримінальної поліції Одеського державного університету внутрішніх справ
Гагауз В.Ф. студент 3 курсу 4 групи факультету №1 ННІПКБ Одеського державного університету внутрішніх справ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Стрімкий розвиток інформаційних технологій в Україні, який спостерігається останнє десятиріччя, супроводжується динамічним розвитком злочинів у сфері інформаційних технологій .

«Кіберзлочинність», «хакери», «комп'ютерний злом» – ці терміни вже перестали бути новелою в нас час. На сьогодні кіберзлочини – це одна з динамічних груп суспільно небезпечних посягань. Швидко збільшуються показники поширеності даних злочинів, а також постійно зростає їх суспільна небезпечність [4].

З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті є одними з найчисельніших.

Інформаційний злочин(кіберзлочин) — це незаконні дії спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань.

Правове підґрунтя інформаційної безпеки України створюють: Конституція України, Кримінальний кодекс України, закони України "Про основні засади