УДК 004.056.2

СТЕЖЕННЯ ЗА ГРОМАДЯНАМИ СПЕЦСЛУЖБАМИ В РІЗНИХ КРАЇНАХ

Реснянський С.О., студ. гр. КБ-171
Мехед Д.Б., к.пед.н, доцент кафедри
Чернігівський національний технологічний університет

Приватність? Мені нічого приховувати.

Останнім часом, коли я обговорюю це питання, кожний раз з'являється хтось, хто каже "Я не турбуюсь про вторгнення в особисте життя, тому що мені нічого приховувати". Я завжди кажу одне й те саме до всіх. Я беру ручку, записую мій адрес електронної пошти та кажу "Ось моя електронна скринька. Коли повернешся додому, відправ мені паролі від УСІХ твоїх акаунтів. Як робочих, так і особистих, щоб я мав змогу подивитися чим ти займаєшься, дізнатися все про тебе та опублікувати те, що вважатиму за потрібне. Зрештою, якщо ти законослухняний громадянин, який не робить нічого поганого, тобі нічого приховувати?". Жоден з них не прийняв цієї пропозиції. — *Глен Грінвальд, Why privacy matters - TED Talks.*

Що потрібно знати про сервіси з Великобританії і США?

Угода про радіотехнічну розвідувальну діяльність Великобританія-США — або UKUSA Signals Intelligence agreement — угода між Великобританією, США, Австралією, Канадою і Новою Зеландією по спільному збору, аналізу та обміну розвідувальної інформації. Члени цієї групи, відомі як "П'ять очей", займаються збором і аналізом даних в різних частинах світу. Незважаючи на те, що країни "П'яти очей" домовилися не шпигувати один за одним, витік інформації від Едварда Сноудена продемонструвала, що деякі члени проводили стеження за громадянами інших країн групи, щоб уникнути порушення національного законодавства, що забороняє стеження за своїми громадянами. Альянс "П'яти очей" також співпрацює з групою третіх країн для обміну інформацією (т. зв. альянси "Дев'яти очей" і "чотирнадцяти очей"), проте "П'ять очей" і треті країни також можуть здійснювати і здійснюють шпигунство щодо один одного. У діяльності альянсу беруть участь наступні спецслужби:

- США — Агентство національної безпеки
- Великобританія — Центр урядового зв'язку (MI5 та MI6)
- Австралія — Управління радіотехнічної оборони
- Нова Зеландія — Служба безпеки урядових комунікацій
- Канада — Центр безпеки комунікацій

Одним з найбільш відомих проектів, здійснюваних під егідою UKUSA, є створення та експлуатація глобального комплексу радіоелектронної розвідки ECHELON. Це глобальна система радіоелектронної розвідки, головним оператором якої є Агентство національної безпеки США. «Ешелон» являє собою розгалужену інфраструктуру, яка включає в себе станції наземного спостереження, розташовані по всьому світі. В системі «Ешелон» беруть участь вищезазначені країни.

П'ять очей	Дев'ять очей	Чотирнадцять очей
1. Австралія	6. Данія	10. Бельгія
2. Канада	7. Франція	11. Німеччина
3. Нова Зеландія	8. Нідерланди	12. Італія
4. Великобританія	9. Норвегія	13. Іспанія
5. Сполучені Штати Америки		14. Швеція

Чому не варто використовувати сервіси, розташовані в США?

Я не рекомендую використовувати американські сервіси через державні програми стеження і заборони для компаній на публікацію запитів, що стосуються національної безпеки (т. зв. "gag orders"). Така зв'язка дозволяє державним структурам отримувати необмежений доступ до даних користувача без їх відома і використовувати компанії як засоби масової стеження.

Гучним інцидентом стала справа Lavabit - вже не активного безпечного поштового сервісу, створеного Ладаром Левісоном. ФБР зажадало надати дані Сноудена, що був одним з користувачів сервісу. Оскільки в Lavabit не зберігалися логи, а усі листи користувачів були зашифровані, ФБР скористалося правом "gag order" і зажадало надати SSL-ключі, які дозволяли їм отримати повний доступ до незашифрованих даних користувача в реальному часі, причому не тільки Сноудена, але і всіх інших користувачів.

Левісон відмовився надати ключі і закрив сервіс, що було трактовано урядом США як порушення постанови вироку з загрозою арешту для автора.

Що таке "свідоцтво канарки"?

Згідно із Патріотичним Актом (The Patriot Act), уряд США може направити секретний ордер інтернет-компанії на стеження за користувачем. Закон забороняє компанії розголошувати факт існування такого ордера (так званий «виверт 22»), проте компанія може обійти цю заборону, не порушивши при цьому закону: компанія може регулярно повідомляти користувача про те, що за ним у даний момент не ведеться прихованого спостереження — така фраза може бути вказана в будь-якому звіті компанії користувачеві. Якщо ж компанія

отримає ордер, такого повідомлення у звіті не буде. Така ідея передачі повідомлень була запропонована відносно недавно у зв'язку з проблемою масового стеження в Інтернеті в умовах секретності.

Закони про розкриття ключів шифрування

Закони про примусове розкриття ключів вимагають від користувачів передачі ключів шифрування правоохоронним органам під час розслідування злочину. Реалізація законів (визначення сторін, які відповідно до закону зобов'язані допомагати слідству) відрізняється в різних країнах, але зазвичай потрібно ордер. Захистом від таких законів може служити стеганографія і шифрування даних таким способом, щоб воно задовольняло принципу правдоподібного заперечення.

Стеганографія полягає в приховуванні конфіденційної інформації всередині неконфіденційних даних - наприклад, розміщення зашифрованого конфіденційного зображення всередині аудіофайлу. **Правдоподібне заперечення** в криптографії - метод, при якому вимагаюча сторона не має можливості довести, що необхідна інформація існує взагалі - прикладом може бути зашифрований файл, який при використанні одного ключа розшифровує неважливу інформацію, а при використанні іншого ключа на ньому ж - конфіденційну.

Застосовуються	Можуть бути застосовані	Не застосовуються
1. Антигуа і Барбуда	1. Бельгія*	1. Німеччина
2. Австралія	2. Нідерланди*	2. Польща
3. Великобританія	3. Нова Зеландія (немає чіткої позиції)	3. Чехия
4. Індія	4. США	
5. Ірландія	5. Фінляндія*	
6. Канада	6. Швеція	
7. Норвегія		
8. Росія		
9. Франція		
10. ПАР		

* (закон застосовується до тих, у кого є доступ до системи, однак, непридатний до підозрюваного і членів його сім'ї)

Що потрібно знати про Windows 10

Microsoft представила багато нового в Windows 10 - наприклад, голосову помічницю Кортану. Тим не менш, більшість новинок порушують користувацьку приватність.

1. Синхронізація даних за замовчуванням включена.
2. Для кожного користувача за замовчуванням генерується унікальний ідентифікатор одержувача реклами".
3. Кортана збирає великий набір даних, в тому числі:
    a. Натиснуті клавіші, пошукові запити і записи з мікрофона
    b. Поточне місце розташування
    c. Дані календаря
    d. Твою улюблену музику
    e. Дані про кредитні картки
    f. Покупки
4. Крім того, Microsoft окремо збирає й інші дані, такі як:
    a. Збережені паролі
    b. Демографічні дані
    c. Звички та інтереси
    d. Статистику використання
    e. Дані про контакти
    f. Дані про місцезнаходження
    g. Контентні дані (пошта, повідомлення, історія дзвінків, аудіо - та відеозапису)
5. Дані можуть і будуть передані третім особам.

Підсумки. Так чи інакше, майже усі країни стежать за своїми громадянами. Використовуючи інтернет неможливо не залишати слідів. Якщо ви хочете почувати себе в відносній безпеці, треба використовувати додаткове програмне забезпечення, як то VPN, браузери з мінімумом або повною відсутністю стеження, захищені сервіси, які не знаходяться в країнах П’яти очей, анонімні мережі або ж зовсім не використовувати Інтернет.

Фраза "Мені наплювати на право на особисте життя, тому що мені нічого приховувати" по суті еквівалентна фразі "Мені наплювати на свободу слова, тому що мені нічого сказати" (Едвард Сноуден)

Список використаних джерел

1. UKUSA Agreement - https://en.wikipedia.org/wiki/UKUSA_Agreement
2. ECHELON - https://en.wikipedia.org/wiki/ECHELON
3. Warrant canary - https://en.wikipedia.org/wiki/Warrant_canary
4. Warrant Canary Frequently Asked Questions - https://www.eff.org/deeplinks/2014/04/warrant-canary-faq
5. Key disclosure law - https://en.wikipedia.org/wiki/Key_disclosure_law
6. Steganography - https://en.wikipedia.org/wiki/Steganography
7. Plausible deniability - https://en.wikipedia.org/wiki/Plausible_deniability