УДК 004.492.3

Євгеній Романович Лоцман,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Методи деанонімізації як засіб виявлення правопорушників

Звичайний користувач не підозрює наскільки глибоко Всесвітня мережа вбудована в суспільство, і що, крім усього корисного, Інтернет несе об'єктивні ризики для користувацької безпеки. Кожен намагається зберегти свої дані в недосяжному для інших вигляді, через це збільшується кількість методів анонімізації і людей які намагаються нею скористатися. Серед звичайних користувачів можуть бути і зловмисники, тому правоохоронним органам дуже важливо мати в своєму арсеналі інструмент для деанонімізації.

Якщо говорити про анонімізацію, то – це спосіб ухилення від автентифікації [1], а визначення для деанонімізація – процес встановлення особи користувача в мережі або справжнього місця виходу в мережу. Розкриття проявляється в публікації особистих даних, найчастіше під цим розуміється публікація реальних фотографій анонімуса, в інших випадках – це публікація повних відомостей про людину.

В мережі Інтернет зловмисники захищені програмними засобами забезпечення анонімності. Більшості користувачів це надає відчуття безпеки і впевненості в тому що, до них не дістатися правоохоронцям і вони не будуть покарані за їх проступки. Наступні методи деанонімізації допомогли правоохоронним органам спростувати теорію безкарності:

1. Фізичний доступ і комп'ютерна криміналістика – шляхом фізичного доступу можна отримати багато інформації про носії і власника інформації. Сучасні засоби дозволяють правоохоронцям відновлювати видалені дані з оперативної пам'яті. Далі в хід йде аналіз отриманих даних і зіставлення їх з уже наявними зачіпками з мережі.

2. Поштова система – головною проблемою чорного ринку донині залишається спосіб доставки. Придбані наркотики і зброю потрібно десь і якось забрати, що представляє в своєму роді велику проблему.

Відомо, що улюбленим поштовим сервісом Сноудена був Lavabit. Уряд США зажадав від творця Lavabit Ладара Левісона передати ключ шифрування за протоколом SSL, який використовувався для криптографічного захисту даних на серверах Lavabit. Творець сервісу Ладар Левісон зволів закрити Lavabit, а не виконувати вимогу американських правоохоронців про стеження за своїми користувачами [2].

3. Операції під прикриттям – завдяки стрімкому розвитку засобів анонімізації і головному правилу в даркнета – анонімність перш за все, визначити хто на тому, протилежному, кінці мережі представляє велику трудність. Ця трудність дозволяє силовикам займати позицію продавця або покупця в мережі і тим самим деанонімізувати зловмисника.

4. Хакерство – в мережі існують білі і темні хакери. Новим напрямком в боротьбі є – взяття під контроль сайту з продажу або наприклад сайту з дитячою порнографією. Найгучнішим прикладом є операція голландських поліцейських, які взяли під контроль майданчик торгівлі наркотиками і жили життям донорів протягом декількох місяців, це дозволило їм виявити велику кількість IP-адрес і деанонімізувати більшу частину як користувачів так і постачальників.

5. Відкрита інформація – жити повним життям в реальності і залишатися анонімним в мережі нереально. Кожна дія, кожен запит в браузері, кожен клік – все це фіксується особливо у соціальних мережах Instagram або Facebook.

6. Телеметрія – це спосіб збору інформації про користувача для поліпшення якості додатку. Тільки грань між телеметрією і кібершпіонажем занадто тонка. Телеметрія – це коли всі дані користувача збираються без прив'язки до особистих даних та геопозиціїнування.

7. Трекінг – це визначення місця розташування рухомих об'єктів в часі за допомогою зібраних даних. Існують випадки коли відомий лише MAC-адрес ноутбука зловмисника. В такому випадку сильно допомагає трекінг пристроїв.

З причини мережної загрози і активності країн світових лідерів в Інтернет просторі, кіберполіція в Україні починає стрімко розвиватися. Цей орган має величезний потенціал і вже розкрив велику кількість злочинних організацій. Яскравим прикладомі є викриття міжнародного хакерського угрупування «Cobalt». Працівники Київського управління кіберполіції Департаменту кіберполіції встановили причетність 30-річ-

ного мешканця Києва до розробки вірусів, кібершпигунства та продажу персональних даних громадян з усього світу [3].

Деанонімізація є потужною зброєю в руках поліцейських та хакерів. Вона дозволяє викрити зловмисників, але також дозволяє зловмисникам красти і продавати дані користувачів мережі Інтернет. Уряд України вчасно усвідомив важливість даного напрямку і збільшив фінансування служб інформаційної безпеки, що призвело до часткової нормалізації Інтернет простору.

Кожен користувач бажає залишатися анонімним тим самим дозволяє зловмисникам ховатися в натовпі, це розсіює увагу кіберполіції. Більш тісне співробітництво з іноземними службами інформаційної безпеки дозволяє українським правоохоронцям перейняти досвід і навести лад у кіберпросторі власної держави.

Список бібліографічних посилань

1. Анонимность, безопасность и цензура в Интернете // SecureVPN : сайт. 16.02.2017. URL: https://www.securevpn.pro/rus/blog/view/4 (дата звернення: 24.10.2019).
2. Бонларэв О. До біса ЦРУ! Легендарний сервіс електронної пошти Lavabit воскрес і готовий стати кошмаром спецслужб // НВ : сайт. 24.01.2017. URL: https://techno.nv.ua/ukr/gadgets/do-bisa-tsru-legendarnij-servis-elektronnoji-poshti-lavabit-voskres-i-gotovij-stati-koshmarom-spetssluzhb-530178.html (дата звернення: 24.10.2019).
3. Кіберполіція викрила українського хакера у взламі комп'ютерів світових банків та готелів // Національна поліція : офіц. сайт. 26.03.2018. URL: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-ukrajinskogo-xakera-u-vzlami-komp-yuteriv-svitovix-bankiv-ta-goteliv/ (дата звернення: 24.10.2019).

Одержано 26.10.2019