Також вдалось розробити програмне забезпечення, яке дозволяє завантажити будь-яку кількість захищеного авторським правом контенту. Додаток був розроблений у вигляді JavaScript скріпта, що дозволяє використовувати його як основу для легкої побудови розширення для браузера, мобільного або веб додатку.

Немає технічної проблеми реалізувати веб додаток, який буде використовувати YouTube як джерело даних, чим буде порушувати авторські права.

Зростання різноманітних засобів розповсюдження інформації та зміщення фокусу з класичних додатків в бік веб додатків, чому свідчіть зростання кількість вакансій веб розробників на ринку праці [7], підвищує необхідність розробки нових засобів та методів розробки веб додатків. Ці засоби та методи розробки повинні дозволяти не тільки захистити авторів від випадкового, але й від цілеспрямованого піратства. Це питання потребує більш детального дослідження та розробки прототипів.

Список використаних джерел:

1. Alexa «The top 500 sites on the web» [Електронний ресурс]. – Режим доступу: https://www.alexa.com/topsites, дата візиту: 28.10.2018.

2. Popvideo [Електронний ресурс]. – Режим доступу: https://www.popvideo.com, дата візиту: 28.10.2018.

3. BBC News [Електронний ресурс]. – Режим доступу: https://www.youtube.com/user/bbcnews, дата візиту: 28.10.2018.

4. Vevo [Електронний ресурс]. – Режим доступу: https://www.youtube.com/user/VEVO, дата візиту: 28.10.2018.

5. Vevo [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Vevo, дата візиту: 28.10.2018.

6. w3schools «Browser Statistics» [Електронний ресурс]. – Режим доступу: https://www.w3schools.com/browsers, дата візиту: 28.10.2018.

7. Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, Web Developers [Електронний ресурс]. – Режим доступу: https://www.bls.gov/ooh/computer-and-information-technology/web-developers.htm, дата візиту: 28.10.2018.

Томайли Д.О.

аспірант,

Національний авіаційний університет

ВРАЗЛИВОСТІ ЕКОСИСТЕМИ НАЙПОПУЛЯРНІШОЇ МОБІЛЬНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

Сучасний світ важко уявити без мобільних додатків. Мобільний трафік у мережі інтернет вже перевищив трафік з персональних комп'ютерів [1; 2]. Кількість додатків в екосистемах, на кшталт, екосистемі Android вже перевищив 2.7 мільярди одиниць [3]. Google Play це основне джерело розповсюдження додатків в екосистемі Android, воно змушує розробників додатків дотримуватися деяких правил [4]. Всі додатки проходять автоматичну

валідацію, але тільки деякі додатки потрапляють до ручної варіації, де людина може перевірити відповідність опису додатку та його реальну ціль [5]. В клієнт Play Store вбудовано антивірус, який сканує додатки на наявність шкідливого програмного забезпечення [6]. Але цей захист не здатен захистити від додатків які створені для витоку інформації або для пере направлення/крадіжки трафіку. Прямо зараз можна переконатись в тому, що є велика кількість додатків, які намагаються мімікрувати відомий додаток, чим не тільки здійснюють крадіжку трафіку, але й, потенційно, можуть містити інші шкідливі функції [7].

Під час дослідження було виявлено декілька небезпечних особливостей та вразливостей екосистеми Android.

Перша небезпечна особливість полягає в великій кількості ресурсів, які автоматично після публікації додатку до магазину додатків Google Play копіюють як додаток, так і весь опис додатку для розміщення у власних магазинах або каталогах додатків. З першої сторінки пошукової системи можна знайти автоматичні агрегатори додатків, такі як: a2zapk.com, apk.support, apkpure.com, androidappsapk.co, appbrain.com, apkgk.com, apkname.com та інші. Якщо додаток з часом пройде ручну валідацію та буде видалений з магазину додатків Google Play з агрегаторів цей додаток видалений не буде. Подібних агрегаторів можна знайти десятки за дуже короткий строк. Зазвичай використання подібних ресурсів обумовлено неможливістю встановити додаток з магазину додатків Google Play по різним причинам, наприклад якщо розробник додатку заборонив розповсюджувати додаток в країні користувача. Ця особливість екосистеми Android несе велику загрозу, адже зловмиснику необхідно тільки опублікувати шкідливий додаток до Google Play і він одразу з’явиться у десятках магазинів або каталогів додатків. Чим більша кількість подібних агрегаторів додатків, тим більша кінцева розповсюдженість будь-якого додатку і тим буде більша кількість заражених пристроїв.

Наступна вразливість полягає у форматі розповсюдження додатків, а саме у структурі.apk пакету. Кожен додаток має унікальне ім’я, яке визначається при створенні додатку. Це ім’я використовується при публікації до магазину додатків Google Play, при роботі з додатком та повинно бути унікальним. Під час дослідження було виявлено, що не зважаючи на те, що унікальне ім’я додатку використовується в багатьох частинах додатку при роботі з пакетом додатку як сама система Android, так й магазин додатків Google Play використовує інформацію з скомпільованого файлу маніфесту (короткий опис додатку). Вдалося реалізувати програмне забезпечення, яке змінює унікальну назву додатку в скомпільованому файлі маніфесту не порушуючи цілісність пакету додатку. Це дозволяє, наприклад, встановлювати будь-яку кількість копій одного й того ж самого додатку, просто змінюючи унікальне ім’я додатку. Але в зміні ім’я додатку є більш небезпечний наслідок. Зловмисник здатен розробити додаток, який здатен повноцінно мімікрувати будь-який інший додаток. Наприклад, користувач встановлює звичайний калькулятор, який в собі містить повний клон розповсюджених додатків банківських клієнтів. При першому використанні цього шкідливого додатку додаток зробить запит до системи на встановлення нового шкідливого додатку. З точки зору користувача та системи це буде просте

оновлення існуючого додатку. Але після такого оновлення користувач може лишитися коштів з банківського рахунку.

Наступна вразливість тісно пов'язана з попередньою і полягає в системі електронного підпису пакету. Як система Android, так й магазин додатків Google Play не дозволяють використовувати додатки, які не мають цифрового підпису розробника. І при будь якій модифікації пакету додатку необхідно оновити підпис. Тим самим розробники екосистеми заклали дуже потужний інструмент захисту користувачів від підробок та модифікованих додатків. Але проблема полягає в тому, що механізму перевірки довіреності сертифікату в цей момент не існує. Тому система Android не зможе відрізнити офіційний додаток банківського клієнту від додатку, який намагається мімікрувати під офіційний.

Не зважаючи на зростання загальної захищеності екосистеми Android провівши дослідження можна стверджувати, що кількість різноманітних векторів атаки ще досі дуже велика. Не було виявлено засобів захисту від знайдених векторів атак. Враховуючи розповсюдженість мобільних пристроїв в наш час під загрозою знаходяться не тільки кінцеві користувачі мобільних пристроїв, але й компанії. Питання захисту від шкідливих додатків стоїть дуже гостро й потребує подальшого дослідження.

Список використаних джерел:

1. StoneTemple «Mobile vs Desktop Usage in 2018: Mobile takes the lead» [Електронний ресурс]. – Режим доступу: https://www.stonetemple.com/mobile-vs-desktop-usage-study, дата візиту: 29.10.2018.

2. SmartInsights «Mobile Marketing Statistics compilation» [Електронний ресурс]. – Режим доступу: https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics, дата візиту: 29.10.2018.

3. Appbrain «Number of Android applications» [Електронний ресурс]. – Режим доступу: https://www.appbrain.com/stats/number-of-android-apps, дата візиту: 29.10.2018.

4. Google Play «Let's build the world's most trusted source for apps and games» [Електронний ресурс]. – Режим доступу: https://play.google.com/intl/en-US/about/developer-content-policy/index.html#!?modal_active=none, дата візиту: 29.10.2018.

5. Google Play «Launch checklist» [Електронний ресурс]. – Режим доступу: https://developer.android.com/distribute/best-practices/launch/launch-checklist, дата візиту: 29.10.2018.

6. Android «Google Play Protect: Securing 2 billion users daily» [Електронний ресурс]. – Режим доступу: https://www.android.com/play-protect, дата візиту: 29.10.2018.

7. Google Play Search [Електронний ресурс]. – Режим доступу: https://play.google.com/store/search?q=%D0%B0%D0%BB%D0%B8%D1%81%D0%B0&c=apps, дата візиту: 29.10.2018.