

УДК 004.744:001.103.2
DOI: 10.31733/15-03-2024/2/322-323

Олександр КОСИЧЕНКО
доцент кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

МЕТАДАНИ ЯК ЗАГРОЗА КОНФІДЕНЦІЙНОСТІ ОСОБИСТІЙ ІНФОРМАЦІЇ

Зручність, що надається сучасними інформаційними технологіями, має свої переваги, але водночас вона збільшує ризик доступу кіберзлочинців до інформації, де б вона не знаходилася. У міру зростання нашої залежності від мобільних пристроїв зростає і цінність даних, що зберігаються на них або яких вони отримують доступ. Цілком логічно, що мотивація кіберзлочинців створювати більш потужні та складніші загрози для мобільних пристроїв також зростатиме. Щоб захистити всі мобільні пристрої та важливі дані, важливо зрозуміти, як працюють ці загрози, і вжити простих заходів, які зупинять їх, перш ніж вони завдадуть будь-якої значної шкоди. Інформація може бути цінною як для організації, так і для окремої людини, але розглянемо лише захист особистих даних, оскільки будь-яка людина, згідно з Конституцією України, має право на недоторканність приватного життя та заборону на збір інформації про неї без її згоди. Деякі люди можуть замислюватися про приховування або видалення своїх персональних даних від сторонніх очей, але не всі, надсилаючи зображення або якийсь документ, навіть не маючи з ними чогось спільного, замислюються про те, що такі файли можуть містити інформацію у формі метаданих яка може бути конфіденційною. Метадані – це дані про дані, які можуть включати ім'я автора файлу, час створення або останньої зміни, назву пристрою, за допомогою якого був створений файл, і навіть геолокацію. Якщо такі дані потрапляють до рук зловмисників чи ворогів держави, власник файлу ставить під загрозу як конфіденційність своїх даних, а й, можливо, своє життя, і навіть державну безпеку [1-3].

Можна сказати, що метадані – це формально описані відомості, що характеризують властивості того чи іншого об'єкта даних і дозволяють керувати ним. Як правило, вони записуються у вигляді «атрибут: значення» відповідно до певного стандарту. Текстовий документ міститиме, наприклад, формат документа, дату його створення, останньої зміни, додаток, за допомогою якого він був створений та змінений. Для зображення або відео метаданими можуть бути назва пристрою, за допомогою якого була проведена зйомка та її дата, формат файлу та геолокація. Також як метадані для будь-якого файлу можуть виступати ім'я або нікнейм (логін) автора. Всі ці відомості становлять загрозу конфіденційності людини, яка створила і виклала в Інтернет той чи інший файл.

Можна продемонструвати, наскільки легко знайти профіль людини в соціальних мережах за метаданими файлу фотографії. В Інтернеті є безліч сайтів, які надають послуги пошуку людей у соціальних мережах за заповненою формою з ім'ям та прізвищем. Скориставшись одним із таких сайтів, можна з'ясувати, що людина з таким ім'ям та прізвищем має профіль, наприклад, лише в соціальній мережі «Інстаграм». Натиснувши на готове посилання, можна перейти у профіль і дізнатися докладнішу інформацію про автора зображення.

Ситуація може звичайно значно ускладнитися, якщо у шуканої людини будуть тетки і однофамільці, в цьому випадку знадобиться більше уточнюючої інформації, яку досвідченому зловмиснику не важко знайти.

Переважно у соціальних мережах публікується інформація, безпосередньо пов'язана з користувачем або його інтересами, наприклад сім'я, улюблена їжа або захоплення. Навіть таку, на перший погляд, невинну інформацію не варто публікувати у своєму профілі, тому що вона може бути використана злочинцями як відповідь на секретне запитання, наприклад, для підбору пароля профілю.

Одним із найбільш надійних та гарантованих способів захисту особистих відомостей є видалення метаданих файлів. Найпростіший спосіб видалення метаданих через

властивості файлу. Якщо в будь-якому файловому менеджері (наприклад, «Провідник» або «Total Commander») натиснути правою кнопкою миші на файл і перейти на вкладках «Властивості» – «Докладно», то в самому низу віконця буде напис «Видалення властивостей та особистої інформації», натиснувши на яку можна видалити, або всі метадані, або вибрати ті, які необхідно видалити. В результаті буде видалена інформація, що містить параметри та модель фотоапарата та ім'я автора знімка.

Другим способом видалення метаданих є використання спеціальних програм-утиліт, наприклад ExifTool. Крім звичайного перегляду метаданих, програма дозволяє видалити, змінювати або додавати нові. Використання функції видалення метаданих утилітою дозволяє видалити не тільки інформацію, пов'язану з автором знімка, але й налаштовані параметри фотоапарата.

Наступний спосіб видалення метаданих базується на використанні он-лайн сервісів. Для цього достатньо створити відповідний запит в Інтернеті і вибрати сайт, що сподобався. Як приклад можна розглянути, як працює інструмент під назвою metaClean від іспанської компанії Adarsus, що спеціалізується на захисті конфіденційної інформації.

Видалення метаданих засобами операційної системи Windows через властивості файлу дійсно не викликає труднощів з боку користувачів, проте частина метаданих, наприклад, геолокація, все одно залишається недоторканими, а значить, є ризик порушення конфіденційності людини. Використання утиліт потребує певних навичок роботи, тому не всі користувачі зможуть скористатися ними. Крім того, багато утиліт не підтримують зміну або видалення метаданих деяких форматів файлів, в даному випадку .mp3 і .docx. Але незважаючи на це, цей спосіб дозволяє затерти більшу частину метаданих, залишивши тільки ті, які безпосередньо пов'язані вже з файлом на пристрої іншої людини або навіть злочинця.

Он-лайн сервіси надають користувачеві зручний інтерфейс, що вимагає мінімальних дій з їхнього боку для завантаження файлу. Проте на деяких таких сервісах є обмеження на завантаження, тому у великих файлах, в даному випадку у відео, неможливо видалити метадані. Крім того, є можливість потрапити на сайт, де завантажуваний файл разом із метаданими зберігається на сервері, де порушник зможе ними скористатися.

Локальні програмні засоби видалення метаданих також представляють зручний інтерфейс користувача з наочним представленням файлів і інструментів для роботи з ними. Крім цього, результат видалення метаданих не гірший, ніж у утиліт та он-лайн сервісів, при цьому виключаються їхні недоліки. Тому можна зробити висновок, що найзручнішим та найефективнішим способом видалення метаданих є використання локальних програмних засобів. Цінною властивістю програм для зміни метаданих є можливість не тільки видалити метадані. Іноді для введення противника в оману слід не видалити метадані, а просто їх змінювати, тобто робити дезінформаційні зміни метаданих.

Отже, можна дійти висновку, що у сучасній епісі захист особистих даних є важливим аспектом безпеки. І незважаючи на те, що метадані можуть бути менш видимими, ніж самі дані, вони мають цінність для зловмисників та ворогів. Тому в якості захисту відомостей, пов'язаних з людиною, було обрано метод видалення метаданих. Крім того, не варто обмежуватись лише видаленням метаданих для забезпечення своєї конфіденційності. При передачі даних потрібні інші інструменти захисту інформації, а також інші техніки знеособлення.

1. Privacy is Power: Why and How You Should Take Back Control of Your Data. Carissa Veliz. London: Bantam Press, 2021. 288 pages.

2. Kosyuchenko O.O., Klynytskyi I.I. Analysis of information security threats related to the use of metadata documents. Dnipropetrovsk State University of Internal Affairs. Scientific journal «Philosophy, Economics and Law Review». Volume 1, no. 1, 2023. p. 152-161

3. Косиченко О.О., Рибальченко Л.В. Загрози та ризики інформаційної безпеки, пов'язані з метаданими. III Міжн. наук.-практ. конф. «Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення», 16 червня 2023 року, Дніпровський гуманітарний університет, м. Дніпро, с.148-151.