ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

СТЕГАНОГРАФІЯ ТА СТЕГОАНАЛІЗ/ STEGANOGRAPHY & STEGANALYSIS

DOI: 10.18372/2225-5036.30.18617

СЦЕНАРІЇ АТАК НА ВІДЕОХОСТИНГ

Олександр Кіреєнко

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

КІРЕЄНКО Олександр Володимирович, асистент
Рік та місце народження: 1993 рік, м. Київ, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2016 рік.
Посада: асистент спеціальності «Кібербезпека» Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Наукові інтереси: інформаційна безпека, теорія ігор.
Публікації: більше 3 наукових публікацій, серед яких наукові статті.
E-mail: kirealex12@gmail.com.
Orcid ID: 0000-0001-9184-6738.

***Анотація**. Розробка моделей порушника та загроз необхідна для захисту інформаційної системи від потенційного шкідливого впливу. Шкідливий вплив на систему можуть чинити як випадково (її законні користувачі) так і з відповідним наміром (зловмисники). Кожна модель є абстракцією, а рівень цієї абстракції залежить від декількох критеріїв, одним із яких є об'єкт захисту. Найбільш деталізовані моделі можливо проектувати під конкретну систему, менше загальні - під деякий тип систем, ще менш загальні - під системи, що відносяться до деякої галузі, і найменш загальні - без прив'язки до системи взагалі. В будь-якому випадку, атаки, що включають до моделі, обирають із деякої множини. Специфіка функціонування відеохостингу передбачає роботу з великими відеофайлами і значну кількість зловживань його основними функціями з боку законних користувачів, а відкритість даного сервісу означає, що атаками будуть послідовності дій користувачів, які заборонені лише на організаційному рівні і не блокуються самою системою.*

***Ключові слова**: відеохостинг, стрімінг, стеганографія, список відтворення, thumbnail/мініатюра, password sharing, субтитри.*

Постановка проблеми

Відеохостинг є інтернет-ресурсом, який надає користувачам можливість завантажувати та переглядати файли в форматі відео. Часто відеохостинги мають безліч додаткових функцій, кожна з яких створює додаткову поверхню атаки.

Багато сучасних відеохостингів подібні до соціальних мереж, так як крім своєї основної функції - зберігання відео, містять функції оцінювання користувачів, які цей контент завантажують (лайки і дизлайки), функції обговорення контенту (коментарі), сповіщень про появу нового контенту (нове відео на каналі, на який ви підписані), соціальних зв'язків (рекомендації відео, які сподобалися вашим друзям, рекомендації відео, які відповідають вашому профілю користувача з вашими інтересами, віком, статтю, геолокацією).

Як і соціальні мережі, відеохостинги часто стають об'єктом атак, які можуть бути спрямовані як безпосередньо на відеохостинг, так і на його користувачів. Для захисту відеохостингу нам потрібно розуміти, які сценарії атак, крім загальних для веб-ресурсів, можуть бути реалізовані для нашої системи.

Аналіз останніх досліджень і публікацій

На даний момент підходи до захисту відеохостингу мало чим відрізняються від захисту інших ресурсів, до яких може бути здійснено віддалений доступ. Класичний підхід означає перевірку завантажуваних файлів на наявність шкідливого ПЗ, запобігання XSS атакам (в секції коментарів під відео), directory traversal для несанкціонованого доступу до інших ресурсів сервера, на якому розміщено даний ресурс, створення резервних копій та балансування навантаження для запобігання атакам на відмову в обслуговуванні.

Специфіка функціонування відеохостингу при цьому практично не враховується. Кількість та розмір відеофайлів не дозволяють здійснювати їх резервне копіювання, бо в системі просто не вистачить для цього ресурсів. Розмір файлів також не дозволяє застосовувати до них безпосередньо алгоритми цифрового підпису (підписувати доводиться хеш файлу).

Небажаний контент, розміщений саме у форматі відео не може бути виявлений простим пошуком послідовності байтів у файлі, для цієї задачі потрібно застосовувати Optical Character Recognition, штучний інтелект або залучати людей-модераторів.

Мета та постановка завдання

У цій роботі пропонується опис сценаріїв атак на відеохостинг, де крім класичних кібератак із використанням шкідливого ПЗ розглянуто широке коло порушень та зловживань пов'язаних із контентом, а також із нецільовим використанням основних та допоміжних сервісів відеохостингу. Запобігання цим атакам дозволить знизити рівень матеріальних та репутаційних втрат.

Виклад основного матеріалу дослідження

Функції відеохостингу

Існує декілька видів веб-сервісів, пов'язаних із розміщенням відеоматеріалів. Відеофайли можуть зберігатися на ftp серверах, хоча в роботі самого серверу немає жодних суттєвих обмежень на тип файлу. Подібну функцію можуть виконувати і бази даних. Але бази даних та ftp сервери є менш спеціалізованими системами, що дозволяють зберігати інформацію довільного вигляду, а доступ до неї здійснюється в основному методом завантаження файлу з сервера на клієнт і його переглядом на клієнті. Стрімінгові платформи (наприклад netflix) надають доступ до контенту із деякої бібліотеки (наприклад вибірка фільмів та телесеріалів), але вони не дозволяють звичайним користувачам самостійно завантажувати свої відео на платформу. Відеоконференції можуть містити архів, в якому зберігаються записи минулих конференцій, з можливістю переглядати їх пізніше. В цьому випадку користувачі навпаки є авторами всього контенту, бо вони і були учасниками конференції, яка записувалася. Ці веб-сервіси відрізняються від більш звичного для простого користувача відеохостингу (наприклад, Youtube).

Особливий інтерес представляють сценарії атак, в яких порушниками є звичайні користувачі системи, а порушення є зловживанням наданих системою дозволів. Захист від подібних атак необхідний, щоб знизити навантаження на працівника-модератора, який обслуговує систему.

Відеохостинг зручно представляти у вигляді множини, елементами якої є окремі відеофайли разом із усією допоміжною інформацією про них (метадані, субтитри, вбудована реклама, thumbnail /мініатюра, лічильники лайків та дизлайків, список коментарів, теги, що визначають тематику відео та ін.):

$$H = \{< V1, M1 >, < V2, M2 > \cdots < Vn. Mn >\}, \quad (1)$$

де Vi – відеофайл, Mi – метадані та інша службова інформація. Mi можна більш детально представити у вигляді кортежу значень <md, sub, b_in_adv, thumb, like_amount, dislike_amount, comment_list, topic1, topic2, ..., topick, etc>.

Кожен обліковий запис або акаунт користувача є в такому випадку деякою підмножиною, що містить відеофайли, які "належать" даному користувачу:

$$\forall i, Acc\_i \subset H, \quad (2)$$

$$\bigcup_i Acc\_i \subset H. \quad (3)$$

Зверніть увагу, що в загальному випадку відеохостинг може містити відео, що не належать до жодного облікового запису (відео без власників)

Описані в даній статті атаки можна поділити на дві підмножини. В перших двох розділах описані атаки, що є зловживаннями з боку користувачів системи. Ці атаки використовують дуже спрощений життєвий цикл. Так як в більшості випадків такі атаки складаються з однієї чи двох шкідливих дій, проводити детальну розвідку нема потреби. Порушник просто починає атаку із спроби виконати відповідну дію. Методом доставки є клієнтська частина відеохостингу, замість шкідливого ПЗ порушник використовує відеофайл, який тим або іншим способом порушує правила відеохостингу, відповідно нема потреби в установленні шкідливого ПЗ та подальшої взаємодії із цим шкідливим ПЗ. Можливим є замітання слідів в якості останнього етапу атаки, якщо це не суперечить меті атаки. Для кібератак, що описані в розділах 3 та 4, можна застосовувати класичний підхід.

Завантаження відеофайлів

Тут можливі декілька сценаріїв атаки:

а) завантаження файлів, що порушують вимоги відеохостингу стосовно контенту. Сюди можна віднести будь-які матеріали, що містять сцени реального насильства, розпалювання ворожнечі та ін;

б) завантаження файлів, що порушують технічні вимоги відеохостингу. Сюди можна віднести завантаження файлів, що є занадто великими або малими за розміром, файлів із відсутніми метаданими або некоректно вказаними метаданими, файлів в неправильному форматі;

в) завантаження файлів, що порушують вимоги відеохостингу стосовно авторського права. Розміщення матеріалів, власником яких користувач системи не є, може потребувати дозволу від власника контенту;

г) завантаження файлів, що містять вбудовану у відеоряд рекламу. Дане обмеження важливе в тому випадку, коли сам відеохостинг має вбудований механізм додавання реклами до відео. Якщо відео має рекламу, що була вбудована безпосередньо, може виникнути ситуація, коли при перегляді одного відео, користувачі побачать рекламу конкуруючих брендів, що може бути порушенням правил розміщення реклами, визначених керівництвом відеохостингу та рекламодавцем;

д) завантаження інформації, яку можна описати як "недостовірну/псевдонаукову". Відеоматеріали, що стосуються теорій змови, плоскої Землі, древніх прибульців и подібний контент можуть бути або повністю заборонені, або дозволені лише за наявності відповідного маркування (або дисклеймеру на початку відео);

е) інформація відеоуроків, якщо представлені в ній матеріали можуть заподіяти шкоду здоров'ю/ життю людини, або завдати значних матеріальних збитків (неякісні рецепти кулінарних відео, небезпечні відео збору електротехніки, що можуть призвести до короткого замикання, відео, що стосуються самолікування та ін.);

є) навіть якщо відеоматеріали є коректними та відповідають дійсності, вони все ще можуть бути заборонені. Власник торгової марки може бути проти того, щоб на відеохостингу розміщували уроки з ремонту його техніки в домашніх умовах. Аналогічна заборона може поширюватися на матеріали, що пояснюють механізм обходу DRM (digital rights management) для програмного забезпечення;

ж) окремо можна розглянути і заборону на відеоматеріали, які можуть спричиняти прямий вплив на психічний стан людини. Відео із мерехтінням екрану може спричиняти епілептичні напади. Під забороною можуть бути і відео, що містять так званий 25-ий кадр або будь-який інший механізм впливу на людину на підсвідомому рівні.

Завантаження відеофайлу, як дозволеного, так і забороненого є додаванням елементу <Vk,Mk> до однієї/декількох/всіх підмножин:

$$Acc\_i' = Acc\_i \cup < \mathrm{Vk}, \mathrm{Mk} > . \quad (4)$$

Атакою дана дія вважатиметься тоді, коли завантаження подібного файлу тим чи іншим способом порушує правила відеохостингу.

Як бачимо, навіть серед інформації, що не є шкідливим програмним забезпеченням, є багато шкідливої та небезпечної, і розміщення подібної інформації потрібно відслідковувати.

Зберігання файлів

Почнемо з того, що зберігання файлу саме по собі вже потребує ресурсів, тому відеохостинги можуть запроваджувати обмеження на кількість інформації, що може зберігатися безкоштовно (якщо така взагалі є), і допускати збереження більшої кількості інформації для користувачів із преміум-акаунтами.

Також рішення щодо збереження інформації можуть бути продиктовані характеристиками даної інформації - її позитивним рейтингом (кількість нових лайків за деякий проміжок часу), негативним рейтингом (аналогічно для дизлайків), загальним рейтингом (співвідношення лайків та дизлайків), кількістю переглядів за деякий період часу, кількістю переглядів в повному обсязі за деякий період часу, кількістю переглядів, що викликали реакцію (лайк/дизлайк), кількістю переглядів, що викликали обговорення (коментарі під відео), або деякою комбінацією перерахованих вище критеріїв.

Ще можливим є присвоєння відеофайлу деякої мітки чи категорії, і використання вище описаних критеріїв з урахуванням категорії, тобто застосування різних правил для різних типів відео (один набір критеріїв для навчальних відео, другий для розважальних, третій для політичних і т.д.).

Інформацію про час, протягом якого слід зберігати файл, можна зберігати як в кортежі <V,M>серед значень, що входять до M, або розраховувати кожен раз, коли необхідно здійснити перевірку умови видалення файлу. В другому випадку в кортежі зберігаються параметри функції, результат виконання якої і буде булевим значенням, відповідно до якого файл залишають або видаляють. Очевидним недоліком є навантаження на відеохостинг, так як при зростанні кількості файлів, такі розрахунки потрібно буде проводити у великих обсягах.

Проблему зберігання відео можна розділити на дві великі підкатегорії:

А) зберігання відео, яке вже не потрібно зберігати, тобто наявність зайвих елементів $< \mathrm{V}, \mathrm{M} > \in$ Нта;

Б) дублювання відео, коли той самий файл завантажується повторно, щоб обнулити таймер. Навіть якщо оригінальне відео буде видалено, його фактична копія залишається на сервері, навіть якщо це порушує правила відеохостингу. $< \mathrm{V1}, \mathrm{M1} > \notin H, < \mathrm{V2}, \mathrm{M2} > \in \mathrm{H}, V1 = V2, M1 \neq M2;$

В) припинення зберігання відео, яке все ще треба було зберігати, коли ми можемо спостерігати нестачу елемента $< \mathrm{V}, \mathrm{M} > \notin \mathrm{H}$.

Якщо відеофайл порушує один із описаних вище критеріїв, може бути прийняте рішення стосовно його видалення із нашого сервера, але користувачам не подобається, коли їх файли видаляють. Порушники можуть застосовувати різні методи для обходу даної проблеми.

Для уникнення дублікатів повинен бути реалізований механізм перевірки файлів на збіги. Це можна зробити за допомогою контрольної суми або цифрового підпису. Проблема такого підходу в тому, що застосування цифрового підпису до відеофайлів є дуже ресурсоємним процесом, так як цифровий підпис реалізують засобами асиметричної криптографії. Можна звісно замість самого відеофайлу підписати хеш, і операція взяття хешу є досить легкою в плані обчислень, але довжина хешу буде меншою ніж довжина файлу, а це може призвести до колізій. Особливо суттєвою ця проблема стає для великих відеохостингів, де зберігається багато файлів. Ще однією проблемою даного підходу є те, що операція взяття хешу дуже чутлива до будь-яких, навіть мінімальних змін. Порушник може завантажити копію відео, змінивши в ньому один кадр, або навіть декілька пікселів на одному із кадрів і це призведе до лавинного ефекту при розрахунку хешу. Перевірка подібності відео по деякій випадковій вибірці кадрів із відео теж не є надійним рішенням проблеми, тому що порушник може мінімально модифікувати кожен кадр. Наприклад відео можна віддзеркалити, і цього буде достатньо, щоб всі кадри нового відео відрізнялися від оригінального, але із них можна було легко відновити оригінальне відео, застосувавши віддзеркалення повторно.

Окремо слід розглянути випадок, коли копію файлу завантажують на сервер з іншого акаунта:

$$\begin{gathered} \forall i \neq j, < Vi, Mi > \in Acc_t, < Vj, Mj > \\ \in Acc_t, Vi \neq Vj \\ \text{але} \\ \exists < Vi, Mi > \in Acc_t, \exists < Vj, Mj > \in Acc_r : \\ Vi = Vj, Mi \neq Mj. \end{gathered} \quad (5)$$

Для економії ресурсів бажано заборонити завантаження дублікатів файлів, навіть якщо це роблять різні користувачі.

Частково проблему завантаження дублікатів з одного акаунта можна вирішити, встановивши обмеження на кількість завантажень в день. В цьому випадку порушник все ще може завантажувати дублікати, але не для кожного відео. Тобто ми встановлюємо для нього квоту на кількість завантажень:

$$Acc^{(n+1)} \subseteq Acc^{(n)} \cup_{i=1}^{u} < Vi.Mi >, \quad (6)$$

де (n+1) та (n) позначають два послідовні стани облікового запису (наприклад вчора і сьогодні). В такому варіанті користувач може "накопичувати" право на зміну, не додаючи нові файли протягом деякого періоду часу, щоб потім додати одразу велику їх кількість:

$$Acc^{(n+1)} \in Acc^{(1)} \cup_{i=1}^{u} < Vi.Mi >. \quad (7)$$

В цьому варіанті існує обмеження на загальну кількість файлів, які може завантажити користувач в межах одного облікового запису. При цьому відсутня перевірка на дублікати. Але кожен дублікат займає місце одного файлу з квоти.

При завантаженні файлу порушник може в мета даних вказати дату завантаження "із майбутнього", для того, щоб відлік часу до видалення файлу почався саме з цієї дати, а не з дати завантаження. Використання власних метаданих для збереження інформації про час завантаження файлу дозволить цього уникнути, але потребує витрат додаткових ресурсів.

Також порушник може спробувати впливати на критерій, за яким ми приймаємо рішення, щодо видалення відео. Накрутка лайків, обговорення відео в коментарях із декількох акаунтів, автоматичний перегляд відео без особистої присутності перед екраном і т.д. Для цих дій може використовуватися ботнет, або просто декілька користувачів діють в змові як одна команда для збереження відеофайлів кожного із них.

Видалення відео з хостингу може відбуватися в один крок (одразу видаляємо файл) так і поетапно (перший етап - блокування відео, другий етап - видалення). Заблоковане відео не можна переглядати, але у користувачів залишається доступ до метаданих, тобто можливість переглянути кількість лайків/дизлайків, прочитати коментарі до відео, подивитися, який у відеофайлу був заголовок (щоб полегшити пошук цього відео на інших відеохостингах) та метадані (дата створення, автор і т.д.). Блокування відео означає перенесення його до спеціальної підмножини елементів в межах даного облікового запису:

$$Acc = Acc_{blocked} \cup Acc_{available}$$
$$Acc_{blocked} \cap Acc_{available} = \emptyset. \quad (8)$$

Можна також передбачити спеціальні правила для випадку $Acc = Acc_{blocked}$, коли всі відео деякого користувача заблоковані. Наприклад можна автоматизувати процес видалення такого облікового запису. Для збереження запису потрібно або розблокувати одне із заблокованих відео або додати нове відео, що не буде заблокованим:

$$Acc_{blocked}{}' = Acc_{blocked} / < Vi, Mi >, Acc_{available}{}' = Acc_{available} \cup < Vi, Mi >$$
та
$$Acc_{blocked}{}' = Acc_{blocked}, Acc_{available}{}' = Acc_{available} \cup < Vi, Mi > \text{відповідно.} \quad (9)$$

Тепер розглянемо ситуацію, коли порушник бажає припинити зберігання відео, яке йому не подобається з особистих/економічних/ідеологічних або будь-яких інших причин.

Для відео, що мають малу кількість переглядів можливим є вплив на його оцінку (дизлайки та негативні коментарі), для більш популярних відео можна застосовувати той же підхід, але із залученням ботнету.

Можливим є і сценарій із "класичними" кібератаками, коли порушник із використанням шкідливого ПЗ отримує доступ до сервера, і видаляє відео, або він може отримати доступ до акаунта користувача, якому належить дане відео і вже від його імені видалити його. Механізми захисту, які ми впроваджуємо на відеохостингу можуть захистити нас від першого типу атак, але наші можливості будуть суттєво обмежені для другого типу. Якщо порушник скомпрометував персональний комп'ютер іншого користувача, який не є частиною нашої інформаційної системи, а лише засобом доступу до інформації, то ми, в загальному випадку, не в змозі відрізнити скомпрометованого користувача від звичайного. Ми можемо використовувати механізми захисту, що реагують на аномалії в поведінці, але вони будуть захищати лише деякий набір відеофайлів. Видалення окремого відео не є достатньою аномалією в поведінці, хоча видалення одного відеофайлу може бути повноцінною атакою. Крім механізмів захисту, що відслідковують поведінку, ми можемо запровадити додаткові механізми захисту окремих відео. Наприклад у нас можуть бути відео, захищені паролем, що відрізняється від пароля прив'язаного до акаунту користувача, який дане відео завантажив. Тобто в користувача є один пароль для роботи із системою, і по одному паролю на кожне відео, яке необхідно захистити від несанкціонованої модифікації чи видалення. В цьому випадку, навіть при компрометації персонального комп'ютера користувача, його відео можуть бути захищені просто тому, що паролі, необхідні для їх видалення могли зберігатися на іншому комп'ютері, або взагалі за межами інформаційної системи (записані на папірці). Проблема в тому, що захищаючи відео окремими паролями, ми захищаємо його і від законного користувача, який не зможе його видалити, якщо забуде пароль.

Також потрібно прийняти рішення про зберігання відео, в яких більше немає власника. Якщо при видаленні акаунту, з якого було завантажено відео, видаляється і відео, навіть в умовах, коли воно було захищене паролем, то цей тип захисту просто не працює. Якщо ж відео не можна видалити без пароля, навіть при відсутньому власнику, то потрібно передбачити механізм призначення власника і скидання паролю. Цим неодмінно спробує скористатися порушник.

Видалення акаунту означає перенесення всіх елементів відповідної підмножини в спеціальну підмножину, яка є "відсутністю акаунта":

$$Acc' = Acc / \bigcup_{i=1}^{u} < Vi, Mi >, NoAcc' = NoAcc \cup \bigcup_{i=1}^{u} < Vi, Mi >. \quad (10)$$

Ще одним способом видалення відео є маніпулювання підсистемою перевірки на дублікати. Для цього порушник завантажує копію відео із підробленими метаданими, які вказують, що його відео є більш старим (завантажено раніше), тоді оригінальне відео будуть вважати дублікатом, який необхідно видалити. Після цього порушнику залишається видалити свою версію відео і атака буде успішною:

$$< Vi, Mi > \in Acc_l, \quad Acc_v{}' = Acc_v \cup < Vi, Mj >,$$
$$Acc\_l' = Acc_l{}' / < Vi, Mi >, \quad (11)$$
$$Acc\_v'' = Acc_v,$$

де l позначає акаунт законного користувача, v–акаунт порушника.

Порушник може спробувати модифікувати відео, щоб воно почало порушувати вимоги нашого відеохостингу. В цьому випадку, навіть якщо видалити відео самостійно він не може, це замість нього зробить наша інформаційна система.

Якщо порушник не може досягнути своєї основної мети (видалення відео), він все ще може спробувати досягти його тимчасового блокування, написавши в службу підтримки, що таке відео порушує правила розміщення на відеохостингу. В таких випадках відео блокують, але не видаляють, до моменту, коли скарга буде розглянута модератором:

$$Acc_{blocked}{}' = Acc_{blocked} \cup < Vi, Mi >, Acc_{available}{}' = Acc_{available} /< Vi, Mi > \quad (12)$$

Скачування відео для його збереження локально

Деякі відеохостинги радикально проти подібного функціоналу, тому що тоді у користувачів не буде мотивації переглядати це відео на нашому ресурсі повторно, що зменшує кількість відвідувань сайту і прибуток від реклами. Можливою є ситуація, коли скачування відео доступне лише користувачам із преміум-акаунтами. Обмеження може стосуватися і відеофайлів, що захищені авторським правом. Як і у випадку із видаленням, відео може бути захищене від скачування паролем, коли лише ті користувачі, які отримали пароль, можуть скачати дане відео.

Для обходу подібних обмежень порушник може використовувати стороннє програмне забезпечення, яке дозволяє записувати відео та аудіо з екрану. Подібний спосіб копіювання відео важко заблокувати, так як ми не контролюємо пристрої, з яких користувачі здійснюють доступ. Ми можемо нав'язати використання нашого додатку, в якому будуть функції моніторингу, що перевірятимуть, чи не запущено на клієнті процес, який відповідає подібному ПЗ. Але дане рішення буде малоефективним. По-перше багато користувачів просто відмовляться від використання нашого відеохостингу, і перейдуть до конкурентів, які дозволяють доступ через звичайний браузер. По-друге, подібний моніторинг програмного забезпечення на клієнті вже сам по собі може бути порушенням прав користувачів, особливо в тих випадках, коли він здійснюється приховано. Нас можуть звинуватити у використанні шпигунського програмного забезпечення. Також подібний підхід ніяк не захищає від копіювання відео за допомогою відеокамери, встановленої перед екраном, на якому відео відтворюється. Звісно в цьому випадку якість буде нижчою, але цього може виявитися достатньо для порушника. Якщо ми хочемо запобігти скачуванню відео методом запису його з екрану, ми повинні переконатися, що даний процес потребуватиме постійного нагляду зі сторони порушника. Тобто ми не хочемо, щоб порушник запустив програмне забезпечення для запису екрану, ввімкнув відтворення відео і пішов займатися іншими справами. Ми можемо перевіряти, чи знаходиться користувач перед екраном, зупиняючи відео у випадкові моменти часу із проханням підтвердити, що користувач все ще тут. Це може бути проста форма із підтвердженням, або така ж форма, але з CAPTCHA. Додавання watermark до відео теж може допомогти, так як за допомогою watermark можна буде встановити, що відео було скачане методом запису з екрану з нашого відеохостингу. Ще однією ознакою скачування відео є тривала буферизація перед початком його відтворення. Це робиться для того, щоб під час запису відео не зупинялося.

Загрози пов'язані із завантаженням, збереженням та скачуванням відео можна віднести до основних. Ці загрози стосуються безпосереднього функціонування відеохостингу. Але крім них є ще і опосередковані загрози. порушник може використовувати наш відеохостинг не за призначенням.

Опосередковані загрози

Першим прикладом використання відеохостингу не за призначенням є його використання для збереження файлів, що не є відеофайлами. Фактично, порушник бажає використовувати наш відеохостинг як зовнішній жорсткий диск для всіх файлів, які в нього не поміщаються локально. Для цього порушник може завантажувати файл, підміняючи його розширення, наприклад замість .rar вказувати .mkv або .avi.

Перевірка розширень завантажуваних файлів повинна здійснюватися в будь-якому випадку, але цією перевіркою не можна обмежуватися. Вміст файлу може вказувати на його тип так само, як і його розширення. При цьому визначення типу файлу можна перекласти на третю сторону. Будь-який файл, який намагаються завантажити на наш відеохостинг, наша система може спочатку відправляти на інший ресурс, який займається конвертацією файлів, з завданням конвертувати дане відео з одного формату в інший. Якщо файл не є відеофайлом, то при його конвертації скоріше за все виникнуть помилки, і конвертація не буде виконана. Такий підхід добре працює для малих відеохостингів і абсолютно не прийнятний для великих, так як сторонній ресурс, що займається конвертацією файлів може швидко занести нашу систему до чорного списку за підозрою в DOS-атаці. Можна використовувати спеціалізовані ресурси, які займаються саме визначенням типу файлу, а не його конвертацією з одного формату в інший. Але і такі ресурси можуть мати обмежену пропускну здатність. Тому для нашого відеохостингу необхідно використовувати систему розпізнавання формату файлів, яка працює локально.

На жаль, всі ці зусилля будуть марними, якщо порушник використає більш інтелектуальний підхід і, замість завантаження довільних файлів зі зміненим розширенням, почне завантажувати коректні відеофайли, в яких закодована інформація. Кожен кадр відео містить деяку кількість пікселів, кожен піксель містить дані в форматі RGB + brightness, тобто 4 байти (по одному байту на кожен із кольорів і 1 байт на яскравість). В такому випадку відеофайл є коректним і без помилок конвертується в інші формати, але зберігати такий відеофайл ми не хочемо, тому що ми не отримаємо жодного прибутку від його перегляду (він в більшості випадків цікавить лише власника).

Також порушник може застосовувати засоби стеганографії для зберігання меншого обсягу заборо-

неної інформації у завантажених відеофайлах. Виявлення прихованих повідомлень, як і криптоаналіз, є ресурсоємною задачею і застосовувати його до кожного відео економічно недоцільно. Застосування фільтрів та перетворень, що трохи змінюють відео, стираючи будь-які приховані повідомлення є можливим, але це впливатиме на якість відео, що може викликати невдоволення серед законних користувачів. При відсутності дублікатів ми також не можемо порівняти оригінальне відео із відео, що, можливо, є стегоконтейнером.

Субтитри

Для відеохостингу, який розрахований на міжнародну аудиторію, важливим є і механізм субтитрів. Субтитри для відео є особливим форматом файлу, який підключається окремо. Порушник може підмінити субтитри відео для розміщення забороненого контенту (заклики до насильства, розпалювання ворожнечі, посилання на заборонені ресурси в darkweb та ін.).

Наш відеохостинг повинен перевіряти, що субтитри відповідають відео, до якого їх додали. В найпростішому випадку можна перевірити, чи відповідає довжина відео, довжині файлу із субтитрами. Цей підхід працює лише в тих випадках, коли субтитри відображаються протягом всього відео (чи потрібно відображати субтитри, коли на відео тиша?). Дана перевірка є досить тривіальною і порушник може легко доповнити субтитри до бажаної довжини, щоб вони співпадали з відео.

Навіть якщо субтитри не містять закликів до насильства (крім випадків, коли вони звучать і в самому відео), вони можуть містити несанкціоновану рекламу, що буде конфліктувати із рекламою, прикріпленою до самого відео на нашому хостингу. Важливо розглянути і ситуацію, коли субтитри є вбудованими в саме відео. В цьому випадку їх не можна підмінити, бо текст "надруковано" безпосередньо на кожному кадрі самого відео. Прив'язка субтитрів таким способом робить їх більш захищеними, але менш універсальними, бо користувачі не зможуть змінити мову субтитрів, або відключити їх взагалі.

Подібною є ситуація і з сурдоперекладом, особливо в режимі "картинка в картинці". Так як переважна більшість людей без вад слуху не знає мови жестів, підміна відео із сурдоперекладом може бути дуже вдалою, прицільною атакою на користувачів нашого відеохостингу, у яких є вади слуху.

Допоміжні функції

За аналогією із веб-ресурсами, що займаються конвертацією форматів файлів, наш відеохостинг теж може бути використаний іншим ресурсом для подібних цілей. Наприклад, у нас може бути функція конвертування відео з одного формату в інший, або стиснення відео з погіршенням якості, або генерацією автоматичних субтитрів, або перевіркою на наявність захищених авторським правом матеріалів (зазвичай це стосується музики у відео). Порушник може завантажити довільне відео на наш відеохостинг, до якого було додано аудіо, щоб побачити, чиї саме авторські права він "порушив". Фактично порушник може використовувати наш відеохостинг як громіздкий і складний music identifier.

Аудіо в форматі відеофайлу

Порушенням може бути і завантаження відеофайлу із чорним екраном або статичною картинкою і наявним аудіо. Чи будуть вважатися такі музикальні відео допустимим контентом на нашому відеохостингу, залежить від рішення керівництва. Якщо подібне не допускається, необхідно вводити механізми, що відслідковують подібні файли. Розпізнати файл з одним кадром в якості фону не складно, але порушник може додати якусь просту анімацію до відео, щоб кадри відрізнялися і тоді виявлення аудіофайлів без фактичного відео стає більш складною задачею, що потребуватиме залучення людини-модератора або нейронних мереж.

Передача файлів

Ще одним способом використання відеохостингу не за призначенням є його використання для передачі файлів, коли один порушник завантажує файл на відеохостинг, другий його тут же скачує, і після цього файл видаляється. Так як файл існує лише декілька хвилин (необхідний час для його скачування другим порушником), то його практично ніхто не встигне переглянути, а якщо нема переглядів, то нема і прибутку від вбудованої реклами, і для розробки профілю користувача та рекомендацій йому цікавого контенту такий файл теж не вийде застосувати. Для захисту від цієї атаки можна встановити обмеження за часом, що заборонить скачувати файли протягом перших декількох годин або днів від моменту їх завантаження на сервер. Звичайно в цьому випадку все ще залишається варіант завантаження файлу методом запису з екрану, але цим ми обмежимо хоча б частину порушників. Також можна встановити обмеження на мінімальний час існування файлу, щоб його власник не міг його видалити протягом декількох годин чи днів з моменту завантаження. Якщо звичайні користувачі мають можливість завантажувати деякий обсяг контенту безкоштовно, цим ми обмежимо їх бажання використовувати наш відеохостинг для передачі файлів.

Окремим варіантом даної атаки є password sharing, коли замість передачі самого файлу з одного акаунта на інший, два (або більше) порушників використовують один акаунт. В цьому сценарії перший порушник завантажує файл на сервер, а потім передає своєму спільнику свої логін та пароль, щоб той міг зайти з цього ж акаунту, і завантажити відео на свій пристрій. З точки зору відеохостингу користувач просто передає цей файл сам собі, можливо з одного пристрою на інший, і така поведінка не є цілком аномальною, так як багато користувачів мають крім персонального комп'ютера інші пристрої (смартфони, планшети, ноутбуки та ін.)

Соціальна мережа

Порушник може провести атаку з метою впливу на механізм рекомендацій відео для деякого користувача. В такій ситуації порушнику не потрібно додавати нові відео, або видаляти вже існуючі. Йому достатньо додати посилання на вже існуюче відео до списку рекомендованих. З одного боку це може призвести до репутаційних втрат для нашого відеохостингу, так як користувачі можуть бути незадоволені рекомендованими відео. Навіть якщо відео не порушує

жодних правил, користувач може вважати його неприйнятним. Одним із варіантів нав'язування відео є включення його до списків відтворення. Наприклад до збірки відео з деякого каналу новин може бути додано відео з випуском новин від їх конкурентів, де ті самі події подають з іншої точки зору. Подібну атаку можуть використати навіть для політичної пропаганди.

Списки відтворення відрізняються від облікових записів тим, що замість самих відеофайлів містять посилання на них. Список відтворення може містити посилання на файли з різних облікових записів. На один файл може бути декілька посилань в різних списках відтворення і це не буде порушенням правил. Видалення посилання із списку відтворення ніяк не впливає на файл. Файл не видаляється навіть якщо на нього немає посилань в жодному списку відтворення. Видалення файлу не видаляє посилання на нього. За посиланням все ще можна перейти і побачити, що файл вже недоступний. Списки відтворення можуть містити посилання також на заблоковані відеофайли. Списки відтворення не мають таких жорстких обмежень за обсягом. Вони можуть містити тисячі відеофайлів і їх можна редагувати довільним чином. Посилання на будь-який файл можна додати до списку відтворення, але заблоковані та видалені файли не можна буде переглянути.

Персональні дані

Ще однією можливою атакою є збір даних профілю користувача, щоб визначити його коло інтересів. Будь-яка особиста інформація може бути використана пізніше для атак із застосуванням соціальної інженерії. Для запобігання подібним атакам, або для зниження їх впливу, в нашому відеохостингу повинен існувати анонімний режим, при якому переглянуті відео не враховуються при визначенні кола інтересів та рекомендацій всіх наступних відео для даного користувача.

Коментарі до відео

Секція коментарів під відео теж може використовуватися для розміщення посилань на інші ресурси, що можуть бути заборонені, або для розміщення закликів до насильства. Поле для вводу коментарів повинне бути захищене від XSS-атак.

Біометричні дані

Якщо для введення пошукових запитів на відеохостингу реалізовано не лише поле для вводу тексту, а і голосові команди, порушник може отримати зразок голосу жертви, навіть якщо він зберігається в системі лише декілька секунд. Це може бути використано для атак на системи з біометричною автентифікацією користувачів. Також записані зразки голосу можуть бути використані для шахрайства. Також для отримання біометричних даних може використовуватися безпосередньо саме відео, коли порушник просто отримує зразок голосу людини з відео.

"Цифрове кладовище"

Трагічним, хоча і закономірним наслідком існування будь-якої соціальної мережі, в тому числі і сервісів, які включають функції соціальних мереж є так зване "цифрове кладовище". Даний термін використовують для опису акаунтів, власники яких вже не будуть їх використовувати. Видалення таких акаунтів і прив'язаного до них контенту не лише дозволяє "розвантажити" відеохостинг, а і запобігти зловживанню, так як за відсутності власника, такий акаунт може бути захоплений порушником і використовуватися для сумнівних цілей протягом тривалого часу без будь-яких скарг від реального власника.

Thumbnail

Обираючи наступне відео для перегляду, користувач зверне увагу на його мініатюру (thumbnail). Мініатюрою може бути перший кадр відео або випадковий кадр відео, або ж зображення, що було завантажено як частина метаданих. В цьому випадку мініатюра може відрізнятися від будь-якого кадру в відео і містити інформацію, якої немає в самому відео. Мініатюра має суттєвий вплив на кількість переглядів, а перший кадр відео часто може бути "чорним екраном" або просто невдалим кадром через те, що при обробці відео, його невдало обрізали. Вибір випадкового кадру із відео теж може призвести до незадовільних результатів. Вплив на мініатюру є досить небезпечним, тому цю інформацію треба захищати обов'язково. Так як мініатюра не завжди є кадром із відео, автоматизувати перевірку мініатюри на відповідність відео в загальному випадку ми не можемо. Особливо небезпечною підміна мініатюри є в файлах, що включені в списки відтворення. Порушник може підмінити один із файлів, зберігши назву та мініатюру. В цьому випадку підміну можна буде виявити лише після того, як даний відеофайл почне відтворюватися при перегляді. Заборона змінювати мініатюру відеофайлу не є універсальним рішенням, так як порушник може одразу завантажити на сервер відео із "правильною" мініатюрою, подібною до інших в списку відтворення.

Інші атаки

Деякі відеохостинги крім розміщення відео також надають можливість його прямої трансляції (стрімінг). Якщо дана функція реалізована, з нею теж буде пов'язано декілька кібератак. Очевидно, що порушник може спробувати перервати пряму трансляцію для приховування інформації (наприклад трансляція новин), ідеологічного (перервати трансляцію військового параду) або економічного впливу (той, хто веде трансляцію, не зможе отримати прибуток від реклами або пожертвувань від глядачів). Другою атакою, що пов'язана із прямою трансляцією є її підміна, коли замість одного відео, буде транслюватися інше. Дана атака є більш загрозливою, ніж проста атака на відмову в обслуговуванні, тому що при підміні відео порушник може розмістити будь-який контент, який порушуватиме правила нашого відеохостингу. Підміна може відбуватися як в явному вигляді (коли глядачам очевидно, що дане відео транслюється не оригінальним автором, а порушником), так і в прихованому вигляді (коли глядачі не знають, що автором контенту є порушник і дане відео може містити дезінформацію). Прихована підміна є більш загрозливою, так як в цьому випадку частина користувачів нашого сервісу "повірить" у надану їм версію відео, а цього може бути достатньо для спричинення хвилювань, або навіть паніки серед населення.

За своєю природою, стрімінгові сервіси дуже подібні до радіоефіру. Просто у випадку із радіо пере-

дається лише аудіо контент, а при стрімінгу передається аудіо та відео. Це також означає, що при наявності функції стрімінгу, наш ресурс може бути використаний як радіостанція. Ніщо (технічно) не заважає користувачу передавати лише звук. Використання стрімінгової функції для радіотрансляції все ж може порушувати правила нашого відеохостингу.

Як і у випадку із збереженням звичайних відео, стрім можна записувати. Це означає, що у порушника є ще одна можлива атака, що спрямована на порушення функції запису прямої трансляції. Тобто саме відео не зазнає змін, користувачі можуть його дивитися при прямій трансляції, але в повторі його не буде існувати.

Цікавим варіантом атаки є підміна стріму на завчасно записане відео, коли користувачі думають, що відео, яке вони переглядають, є прямою трансляцією, коли насправді це не відповідає дійсності. Можливість завчасно записати відео, яке буде використано для підміни дає порушнику достатньо часу та можливостей зробити подібне відео досить правдоподібним. І тим серйознішим буде результат (більша кількість користувачів повірить в те, що дивилися пряму трансляцію)

Ще одним напрямком атаки є дії, що порушують приватність. Порушник може розмістити на хостингу відео, що було відзняте без згоди особи, що потрапила на відео, якщо така згода була необхідною (запис відео в публічних місцях не потребує подібної згоди). Для ідентифікації особи на відео може використовуватися не лише її зовнішність, а і голос. Розголошення приватної інформації можливе і в секції з коментарями.

Використання програмного забезпечення, що блокує рекламу, теж можна вважати загрозою для нашого відеохостингу. Значно більшою загрозою з реальними фінансовими втратами є перенаправлення реклами (Legitimate advertising delivered to fraudulent end points). Суть подібної загрози полягає в тому, що реклама може бути показана нецільовій аудиторії, або взагалі аудиторії, що не містить людей. Якщо із нашим відеохостингом взаємодіє ботнет, то все відео, разом із рекламою буде показано ботам. Тобто аудиторія де-факто відсутня, а гроші за розміщення реклами були сплачені. Якщо ця проблема стане проявлятися регулярно, рекламодавці можуть припинити співпрацю.

Із рекламою також пов'язана атака, при які порушник замінює рекламу в відео на іншу інформацію. Це може бути як реклама іншого продукту (недобросовісна конкуренція), або реклама заборонених товарів та послуг, або відео, що взагалі не є рекламним (напр. пропаганда). Якщо переключення з основного відео на рекламу відбувається досить плавно, то порушник може також замінити рекламу до відео на матеріал, який виглядатиме як частина оригінального відео. В такому випадку користувачі можуть навіть не здогадуватися, що основне відео переривалося на "рекламу". Для запобігання подібній атаці потрібно реалізувати вбудовування реклами у відео таким чином, щоб його не можна було сплутати з основним матеріалом. Наприклад можна рандомізувати момент показу реклами, або додавати до відео watermark, або навіть змінювати інтерфейс на стороні клієнта (наприклад в Youtube змінюється вигляд полоси прокрутки відео під час показу реклами). При цьому бажано, щоб рекламу можна було розпізнати і на слух.

Висновки. Класичні атаки із використанням шкідливого ПЗ становлять загрозу для будь-якого ресурсу. Незалежно від типу діяльності, наша система може бути захоплена для використання її ресурсів в злочинних цілях (ботнет) або стати ціллю атаки на відмову в обслуговуванні (яку б функцію вона не виконувала, це приносить прибуток і власник/користувачі системи не хочуть, щоб виконання даної функції припинялося).

При цьому існує набір специфічних саме для відеохостингу атак, що можуть бути спрямовані як на його основні функції, так і на допоміжні функції або користувачів системи. Деяка дія може бути атакою для одного відеохостингу і дозволеною діяльністю для іншого (наприклад скачування відео для перегляду його на клієнті в режимі офлайн). Механізми виявлення атак, що реагують на аномальну поведінку, можуть захистити від видалення списки відтворення відео, але не окремі відеофайли. А захист кожного відео окремим паролем є досить громіздким та складним для користувачів.

Список літератури

[1]. Arendt F. Suicide on Instagram – Content Analysis of a German Suicide-Related Hashtag. Crisis. 2019 Jan;40(1): 36-41. doi: 10.1027/0227-5910/a000529. Epub 2018 Jun 21. PMID: 29932019.

[2]. Chin-Yung Lin, "Watermarking and digital signature techniques form ultimedia authentication and copyright protection", PhDThesis, Columbia University, 2001.

[3]. Nandakishore Ramaswamy and K. R. Rao. 2006. Video authentication for H.264/AVC using digital signature standard and secure hash algorithm. In Proceedings of the 2006 international workshop on Network and operating systems support for digital audio and video (NOSSDAV '06). Association for Computing Machinery, New York, NY, USA, Article 21, 1-6. https://doi. org/ 10.1145/1378191.1378218.

[4]. Bor-Chun Chen, Pallabi Ghosh, Vlad I. Mora riu, Detection of Metadata Tampering Through Discrepancy Between Image Contentand Metadata Using Multi-Task Deep Learning in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, July, 2017.

[5]. P. Kakarand N. Sudha. Verifying temporal data in geotagged images viasunazimut hestimation. IEEE Transactions on Information Forensics and Security, 7(3): 1029–1039, 2012.

[6]. Sadek, M.M., Khalifa, A.S. &Mostafa, M.G.M. Video steganography: a comprehensive review. Multimed ToolsAppl74, 7063–7094 (2015). https://doi.org/ 10.1007 /s11042-014-1952-z.

[7]. E. I. Lin, A. M. Eskicioglu, R. L. Lagendijkand E. J. Delp, "Advances in Digital Video Content Protection," in Proceedings of the IEEE, vol. 93, no. 1, pp. 171-183, Jan. 2005, doi: 10.1109/JPROC.2004.839623.

[8]. Treimer, M; Simonson, M. Journal ofSocialPsychology; Worcester, ass. Том 128, Изд. 4, (Aug 1, 1988): 563-565.

УДК 004

Kireienko O.V. Attack scenarios on videohosting

Abstract. *The development of both the violator model and threat model is required for protection of information system from potential harmful influence. Harmful influence can be caused by accident (by its legit users) or intentionally (by violators). Each model is an abstraction and the level of detail of this abstraction is determined by a few factors. One such factor is the object of protection. The most detailed models can be designed for specific systems, more generalized models – for the system type, even more generalized – for the systems of the certain field and the most generalized models are developed without specifying the system at all. In any case attacks, that will be included into the model, are selected from a certain set. The specifics of functioning of videohosting imply processing of large videofiles and substantial amount of misuse of its functions by legit users whereas the availability of given service means that attacks will be present in a form of a sequence of actions that are only prohibited at organizational level and are not blocked by the system itself.*

Keywords: *videohosting, streaming, steganography, playlists, thumbnail, password sharing, subtitles.*

Кіреєнко Олександр Володимирович, асистент спеціальності «Кібербезпека» Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Oleksandr Kireienko, assistant of the "CyberSecurity" specialty of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".

Отримано *9 березня 2024 року*, затверджено редколегією *1 квітня 2024 року*