ІНФОРМАЦІЙНА БЕЗПЕКА В МЕДІА КОНТЕЙНЕРІ

Маркітаненко І. В., ст. (гр. КВ-83мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: В даній роботі розглядаються різні види інформаційних небезпек у медіа контейнері з використанням скорочених посилань. Приведені способи захисту від зламу особистих даних користувача, наприклад, перевірка посилання спеціальним сервісом перевірок скорочень URL (CheckShortURL, GetLinkInfo).

Ключові слова: медіа контейнер, короткі посилання, URL, акаунт, вкладення.

Abstract: In this workwe consider various types of information hazards in a media container using short links. The following are ways to protect against personal data fragmentation, such as checking the link by a special URL-checking service (CheckShortURL, GetLinkInfo).

Keywords: media container, short links, URL, account, contribution.

Мікроблоги, як сучасні засоби передачі думок в письмовій формі у вигляді розмови, відкривають широкий спектр для невербального спілкування між Інтернет-користувачами. Без популярних соціальних мереж сучасній молоді нині й годі уявити життя.

Новомодні месенджери диктують свої правила, наприклад ліміт символів у повідомленнях. Користувачі Twitter часто замислюються про те, як вмістити всі думки в один твіт з обмеженням в 140 символів. І такі випадки непоодинокі. Особливих труднощів завдає момент, коли у своєму повідомленні необхідно переслати довжелезне посилання. І тут приходять на допомогу короткі посилання.

З одного боку, завдяки коротким посиланнямURLнабуває акуратного вигляду, не перевищує допустиму встановлену соціальними мережами кількість знаків та значно полегшує користування Інтернетом. Але, як і будь-яка технологія чи нововведення, скорочення посилань мають свої загрози та недоліки [1].

Короткі посилання стали досить ефективним допоміжним інструментом для зловмисників. Щохвилини, навіть щосекунди по Інтернету поширюється безліч посилань з веб-сайтів, блогів, соціальних мереж. Саме таким способом зловмисники розповсюджують небезпечні файли. Натискаючи на копку «Перейти», користувачу складно передбачити можливі загрози, що можуть скриватись за цим посиланням.

Для спрощення процесу створення коротких посилань створено чимало сервісів. Прикладами є платформа для скорочення довгих посилань (URL) bit.LY, доповнення до браузерів Un shorten.it (Mozilla Firefox) та Long URL (Google Chrome) [2].

Основна задача зломщиків: замаскувати небезпечні посилання, щоб вони залишились непоміченими. Варіантів існує безліч – від підробки URL, яка перенаправляє на іншу сторінку, до злому облікових записів користувача і

відправки посилання його контактам. Зручність коротких посилань в плані злому це те, що вони дозволяють зловмиснику приховати, куди насправді здійснюється перехід.

Нещодавно компанія Check Point провела дослідження, в ході якого було встановлено, що акаунти в Telegram та What sapp можна зламати та заразити вірусом з допомогою всього лише однієї присланої картинки. Вся справа у змісті, який криється за нею, а точніше за спеціальних кодом, який міститься в ній. Коли отримувач відкриває зображення, код розповсюджується як вірус. Вірус працює за принципом отримання доступу до списку контактів користувача і самочинно розсилає заражену інформацію всім, хто знаходиться в цьому списку.

Також стало можливим існування загрози персональній інформації, що зберігається в хмарних сховищах, таких як One Drive, Google Drive, Google Maps. У це складно повірити, адже загальновідомо, щоGoogle гарантує безпеку. Один з можливих сценаріїв: користувачеві на пошту надходить лист, в якому міститься файл, розташований в Google Drive [3].

Це може бути що завгодно, проте важливо лиш те, що замість вкладених текстових файлів, PDFчи таблиць це є нічим іншим як картинкою, імітованою таблицею чи будь-яким іншим електронним документом. Після натиснення на них користувач попадає на фейкову сторінку авторизації Google, єдина відмінність якої від справжньої полягає в адресі.

Після введення користувачем паролю й логіну від пошти зловмиснику безперешкодно вдається здійснити злам. Якими ж мають бути способи убезпечення від зламу? Щоб не стати черговою жертвою, досить пам’ятати декілька простих правил:

1. Будь-які вкладення є потенційно небезпечними, навіть ті, які такими донедавна не вважались.

2. Бути пильним при вводі пароля, адреса сторінки авторизації має значення, вона обов’язково має починатись на *https://*.

3. Використання двоетапної авторизації, необхідно обирати якийсь спосіб підтвердження: сповіщення на телефон, SMS, електронний ключ та інше.

Існують також спеціальні веб-сервіси для перевірок скорочених посилань. Check Short URL містить більшість сервісів скорочень URL. На відміну від нього, Get Link Info дає змогу користувачеві простежити етапи переадресації. Для оцінки безпеки Get Link Info використовує технологію безпечного перегляду Google.

Висновок. Отже, ми знаємо, що скорочення посилань може нести в собі окрім користі ще й шкоду, тому необхідне перестрахування. У наш час розвитку кіберзлочинності давати нові шляхи для хакерів не є найбільш слушною думкою, тому для скорочення треба користуватись лише перевіреними порталами та сайтами по скороченню, що працюють вже багато років та зарекомендували себе з найкращої сторони. Наприклад: top-link.com.ua, ls.gd, To.click, goo.gl, тощо.

Ці сервіси, як і будь-які інші, ніколи не дадуть стовідсоткової впевненості у тому, що ваш персональний комп’ютер буде у безпеці, але ризик понижується до мінімуму, так як у всіх компаніях таких масштабів система безпеки працює злагоджено і перевірено.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Небезпека коротких посилань: вразливість персональної інформації [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.securitylab.ru/blog/company/PandaSecurityRus/294672.php
2. Чим небезпечні короткі посилання і як від цього уберегтися [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.maketecheasier.com/dangers-of-shortened-links-and-stay-safe/
3. Хакери придумали новий спосіб злому акантів Google [Електронний ресурс]/Дмитро Горчаков. – 2017. – Режим доступу до ресурсу:https://lifehacker.ru/novyj-sposob-vzloma-akkauntov-google/