2. Конвенція про заборону розробки, виробництва та накопичення запасів бактеріологічної (біологічної) і токсинної зброї та про їх знищення. Електронний ресурс [Режим доступу]: http://zakon.rada.gov.ua/laws/show/995_054

3. Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення. Електронний ресурс [Режим доступу]: http://zakon.rada.gov.ua/laws/show/995_182

Томайли Д.О.

аспірант,

Національний авіаційний університет

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ ВЕБ ДОДАТКАХ

Сучасний світ корпоративних додатків все більше змінює фокус з класичних додатків в бік веб додатків. Цьому факту може свідчити бурхливий розвиток різноманітних технологій розробки веб додатків та зростання кількості вакансій веб розробників на ринку праці [1]. Зростання кількості та складності веб додатків збільшує кількість різноманітних векторів атак та їх численність [2]. Нажаль не існує комплексних рішень щодо захисту веб додатків, які дозволяють перешкоджати зловмиснику аналізувати клієнтську частину веб додатку або змінювати поведінку клієнтської частини додатку.

Враховуючи вживаність електронного листування в корпоративному світі та достовірно відомі успішні крадіжки приватної інформації з корпоративних електронних листів [3] було проведене дослідження Microsoft Outlook Office 365, одного з найбільш вживаних та напрямлених на корпоративний сегмент веб додатку електронного листування [4; 5].

Під час дослідження використовувався найбільш розповсюджений браузер Google Chrome [6] та звичайний текстовий редактор. Інші додатки та більш складні техніки аналізу або атаки не використовували навмисно.

Дослідження було націлене на реалізацію додатку або декількох додатків, які дозволять, без відома користувача, здійснювати постійний виток приватної інформації та не потребують особливих знань для впровадження. Також для цілей дослідження використовувалися найбільш жорсткі з наявних, з точки зору правил безпеки, обмеження веб додатку, які включали в себе двофакторну автентифікацію, заборону перегляду та\або завантаження файлів з електронного листа.

Під час дослідження було виявлено, що є можливість перехоплювати всі повідомлення, які надсилає веб додаток до серверу. Використовуючи цю вразливість вдалось розробити додаток, який перехоплює всі дані та пересилає всі листи до тестового сховища. Також було виявлено, що під час завантаження електронних листів клієнтська частина веб додатку завантажує листи повністю, тобто немає необхідності робити допоміжні запити або очікувати коли

користувач відкриє листа. Таким чином вдалося, непомітним для користувача чином, перехоплювати будь-які електроні листи та дані про користувачів.

Outlook Office 365 дозволяє переглядати без завантаження деякі типи файлів, які прикріплені до електронних листів. Веб додаток обробляє їх особливим чином, тому виток таких файлів потребує додаткового дослідження. Під час додаткового дослідження було з'ясовано, що не зважаючи на встановлену заборону перегляду та\або завантаження є можливість отримати деякі файли, які було прикріплено до листа. Outlook Office 365 на початку завантаження даних з сервера отримує просту конфігурацію, яка керує здатністю додатку надавати користувачу можливість перегляду файлів, які, в свою чергу, прикріплені до електронного листа. Перехопивши та змінивши цю просту конфігурацію вдалось отримати доступ до більшості типів файлів. Складність в реалізації несанкціонованого доступу до всіх типів файлів полягає в додаткових дослідженнях інших продуктів корпорації Microsoft, які входять до пакету Office 365 та використовуються для обробки тих типів файлів, до яких не вдалось отримати доступу. Перелік типів файлів, до яких вдалось отримати доступ, включає в себе найбільш вживані типи файлів в корпоративному документообороті: зображення, текстові, PDF, Excel, Word та Power Point файли.

Під час дослідження також розглядалось питання щодо впровадження додатку. Було виявлено, що найбільш простим шляхом встановити додаток буде використання магазину розширень Google Chrome Web Store, де шкідлива частина може бути прихована в іншому додатку, який за допомогою фішингу може бути доданий до браузеру на корпоративній робочій станції.

Розроблений під час дослідження додаток можна встановити за декілька секунд (це потребує всього двох кліків). Також можна підкреслити, що цей додаток не потребує особливих дозволів та автоматично буде працювати тільки в моменти, коли веб додаток відкрито.

В наш час, коли витоки інформації можуть спричинити не тільки втрату довіри або коштів компанії, але й більш катастрофічні наслідки для компанії необхідно переглянути не тільки підходи до розробки веб додатків, але й необхідність у додаткових можливостях, які надаються користувачу сучасними браузерами. Необхідно враховувати, що корпорації повинні бути захищені не тільки від ненавмисного витоку інформації, який був спричинений халатністю співробітників, але й від цілеспрямованого витоку інформації інсайдером. Як показує проведене дослідження для витоку інформації зловмиснику достатньо мати доступ до стандартних додатків на будь-якій робочій станції.

Список використаних джерел:

1. 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

2. Positive Technologies «WEB APPLICATION ATTACK STATISTICS 2017», 2018 р.

3. The Guardian «Deloitte hit by cyber-attack revealing clients' secret emails» [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails, дата візиту: 28.10.2018.

4. Litmus «The 2017 Email Client Market Share» [Електронний ресурс]. – Режим доступу: https://litmus.com/blog/the-2017-email-client-market-share-infographic, дата візиту: 28.10.2018.

5. Zapier «The 8 Best Email Hosting Services for Business» [Електронний ресурс]. – Режим доступу: https://zapier.com/blog/best-email-hosting-services, дата візиту: 28.10.2018.

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

Томайли Д.О.
аспірант,
Національний авіаційний університет

ПРОБЛЕМИ ЗАХИСТУ АВТОРСЬКОГО ПРАВА ТА КОНТЕНТУ В СУЧАСНИХ ВЕБ ДОДАТКАХ

Сучасний світ дозволяє будь-кому, як створювати свій контент, так і споживати загально доступний контент, який був створений іншими авторами. В наш час існує багато різноманітних майданчиків монетизації свого контенту. Також існують різноманітні шляхи монетизації починаючи від класичного продажу та закінчуючи більш сучасною монетизацією через показ реклами. Однією з проблем монетизації через показ реклами є те, що контент (зазвичай відео або аудіо матеріали) розміщені у вільному доступі і будь-хто може спожити цей контент. Однак споживач контенту не завжди розуміє, що порушує авторські права коли намагається використовувати контент не звичайним чином. Привести приклад можна за допомогою найбільш популярного майданчика для розповсюдження відео – YouTube від ALPHABET [1]. Але в наш час такі майданчики використовуються вже не тільки для кінцевих користувачів, але й корпораціями та існує цілий сегмент корпоративного ринку, бізнес якого напряму побудований на YouTube [2; 3; 4; 5]. Тому вкрай необхідно захистити авторські права не тільки від випадкового порушення, але й від цілеспрямованої крадіжки контенту або піратства.

Під час дослідження використовувався найбільш розповсюджений браузер Google Chrome [6] та звичайний текстовий редактор. Інші додатки та більш складні техніки аналізу або атаки не використовували навмисно.

Було проведено аналіз можливості завантаження авторського контенту з майданчика YouTube та можливість автоматизації цього процесу. Проаналізувавши яким чином працює YouTube виявилось, що запросивши з сервера YouTube напряму JavaScript файл з частиною коду для роботи веб додатку він буде в собі містити автоматично згенерований прихований ключ. Використовуючи цей ключ під час запиту інформації про відео по унікальному ідентифікатору сервер видає повну інформацію про дане відео. Таку як назва, зображення відео та прямі посилання на відео. Завдяки прямим посиланням на відео легко напряму як завантажити відео, так і переглядати його, навіть у тому випадку, якщо автор цього відео заборонив розповсюдження або скрив його.