3. Александр Зайцев, Роман Мещеряков Технические средства и методы защиты информации. - 7 изд. Горячая линия-Телеком, 2012.

УДК 004.056.5

ЗАГРОЗА ЗМІНИ ВМІСТУ БУФЕРУ ОБМІНУ ЗА ДОПОМОГОЮ PASTEJACKING

Бойко К. В., студ. гр КБ-161,
Ткач Ю. М., д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Зазвичай, дія ***копіювати*** і ***вставити*** - це дуже проста дія, яку може виконати будь-який користувач, але час від часу веб браузер може не дозволити користувачеві копіювати і вставляти текст з певних веб-сайтів. Крім того, браузер може навіть не дати вибрати вміст з веб-сторінки, таким чином обмеживши можливість копіювання користувача.

Це може стати досить проблематичним, особливо якщо цільовим користувачеві потрібні великі шматки тексту з сайту для дослідницьких цілей.

Майже всі веб-браузери дозволяють веб-сайтам виконувати JavaScript команди на комп'ютерах користувачів для виконання обчислень інтерфейсу і бізнес логіки веб додатків. Ця функція може дозволити шкідливим веб-сайтам захопити буфер обміну користувача комп’ютера. Тобто, коли ви щось копіюєте і вставляєте його у буфер обміну, веб-сайт може запустити одну або кілька команд за допомогою вашого браузера. Метод може бути використаний для зміни вмісту буфера обміну для виконання атаки в операційній системі користувача.

Веб-сайти виконують команди, коли користувач виконує якусь дію, - наприклад, під час натискання певної клавіші або клацання правою кнопкою миші. Коли ви натискаєте CTRL + C на клавіатурі, він запускає режим командування веб-сайту. Після невеликого очікування, скажімо, 800 мс, він вставляє щось шкідливе у ваш буфер обміну. Очікування користувача такі, що після використання CTRL + V для вставки оригінального тексту, який було скопійовано, але замість нього буде вставлено те, що було потрібно зловмиснику. Деякі веб-сайти можуть відстежувати CTRL + V і використовувати його для запуску команди, яка змінює вміст буфера обміну.

Pastejacking - це метод, який шкідливі веб-сайти використовують для того, щоб взяти під контроль буфер обміну вашого комп'ютера і змінити його вміст на щось "шкідливе" без вашого відома.

Більш того, таким чином ви можете вставити контент прямо в консоль, наприклад в PowerShell або вікно командного рядка, і тоді може виконатися шкідлива команда. Користувачі *Mac* мають деяку безпеку, якщо вони використовують iTerm. Це емуляція, яка дозволяє користувачам Mac замінити консоль за замовчуванням. При використанні iTerm він запитує користувачів, чи дійсно вони хочуть вставити щось, що містить символ «нового рядка». Потім користувачі можуть вибрати «Так» або «Ні» в залежності від того, що вони роблять.

Символ нового рядка це фактично половина клавіші Enter. Клавіша Enter зображена, як правило, стрілкою, яка здається починається від верхньої лінії до нижньої, а потім вліво. Клавіша Enter являє собою комбінацію символу нового рядка (перехід до наступного рядка) і повернення (читається як «повернення каретки в крайнє ліве положення x, 0», як в друкарських машинках). Коли ви натискаєте клавішу Enter, виконується будь-яка команда в цьому рядку консолі. Але це може залежати від консолі, щоб запросити підтвердження.

У більшості випадків, в командному рядку Windows не вимагається підтвердження на виконання команд. Рядок запитує підтвердження тільки в тому випадку, якщо ви

використовуєте команду DEL або FORMAT. Для таких команд, як RENAME і т.д. підтвердження запитуватися не буде.

У будь-якому випадку, якщо веб-сайт розміщує команди в буфері обміну за допомогою клавіші Enter (/ n / r, де / n - це новий рядок, а / r - повернення каретки), консоль або будь-програмований додаток безпосередньо запускає команду(и) . Якщо ці команди шкідливі, вони можуть завдати шкоди вашій машині і мережі.

У такому випадку, як же уникнути "***Pastejacking***"?

Першочерговим захистом, для користувача Windows може бути перевірка, що було поміщено в буфер обміну комп'ютера. Для цього спочатку вставте вміст в блокнот. Він вставляє буфер обміну тільки як текст і дозволяє побачити, що знаходиться в буфері обміну. Якщо ви бачите, що ви скопіювали, ви можете піти далі і вставити його куди завгодно. Це означає додатковий крок, але це краще, ніж виконати шкідливу команду. Пам'ятайте, що використання Word для перевірки буфера обміну може бути небезпечним, оскільки він також програмується за допомогою макросів і т.д.

Ви можете повністю вимкнути Javascript або використовувати надбудову для браузера, як *NoScript*, яка дозволить вам вибирати коли запускати javascript, а коли ні, таким чином це може допомогти в боротьбі з цією проблемою.

HTML - це мова, на якому написані веб-сторінки, але саме CSS (Cascading Style Sheets) визначає, як вони виглядають.

Це той самий CSS, який переставляє сторінки для роботи у всьому, від телефонів до екранів кінотеатру, розміру тексту, додавання колонок, різних кольорів, обведення країв тощо.

Він також може бути використаний для розміщення речей на сторінці або, що більш корисно для Pastejacking, поза сторінки, де ви не можете їх бачити.

Як висновок, задля вашої безпеки, перш за все, ви можете вставити скопійований контент куди завгодно. Так, можливо вам доведеться зробити ще один зайвий крок, але зате ви уникнете Pastejacking'a.

І звичайно, якщо контент який ви копіюєте і вставляєте в будь-який Блокнот, але при цьому ви не бачите формат, шрифт, стиль, це означає, що контент, який ви вставляєте просто в *текстовому форматі*.

У випадку ж *з зображеннями* краще натиснути правою кнопкою миші зображення, яке ви хочете завантажити або скопіювати, і потім вибрати ***Зберегти як***, так буде набагато безпечніше скопіювати команду з неї.

Список використаних джерел

1.Chirgwin R. Pastejack attack turns your clipboard into a threat [Електронний ресурс] / Richard Chirgwin – Режим доступу до ресурсу: https://www.theregister.co.uk/2016/05/25/pastejack_attack_turns_your_clipboard_into_a_vector/

2.Hacker News [Електронний ресурс] – Режим доступу до ресурсу: https://news.ycombinator.com/item?id=21490503

3. Bisson D. Researcher warns of ‘pastejacking’ hack attacks targeting users’ clipboards [Електронний ресурс] / David Bisson – Режим доступу до ресурсу: https://www.grahamcluley.com/researcher-warns-pastejacking-hack-attacks-targeting-users-clipboards/