Варганова Д. О., ст. викладач кафедри комп'ютерних технологій у медицині та телекомунікаціях
Окунькова О. О., ст. викладач кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»

ЗАХИСТ ДАНИХ В ДОДАТКАХ MICROSOFT OFFICE

В сучасному світі досить складно уявити людину, яка була б позбавлена доступу до інформативних ресурсів, адже інформатизація проникла абсолютно у всі сфери суспільного життя, є одним із чинників ефективного соціально-економічного, культурного та духовного розвитку кожного в майбутньому. Тому питання інформаційної безпеки є актуальним для всіх користувачів комп'ютерної техніки.

Компанія Microsoft починаючи з квітня 2022 року ввела нові правила для офісного пакету, які полягають в автоматичному блокуванні виконання макрокоманд мовою VBA. У компанії вважають, що це допоможе знизити кількість випадків зараження шкідливим програмним забезпеченням через фішингові повідомлення. Саме таким шляхом у 25% випадків програми-шкідники потрапляють на комп'ютери користувачів. Блокування за замовчуванням буде застосовуватися до завантажених з Інтернету файлів, що містять макроси і призначені для додатків Word, Access, Excel, PowerPoint і Visio. Цей захід, на думку розробників, дозволить ускладнити життя кіберзлочинцям, які практикують фішингові атаки.

Поведінка додатків зміниться для Office 2021, Office 2019, Office 2016 та Office 2013 для Windows. Після встановлення оновлення користувач не зможе єдиним натисканням кнопки дозволити запуск вбудованого в документ Office макросу, як це працювало раніше. Важливо зазначити, що заплановане нововведення не позбавить користувача можливості запускати макроси всередині документів Office, а лише трохи ускладнить процедуру.

Вимкнути захист можна буде, знайшовши завантажений файл на диску і знявши відповідну галочку в його властивостях. Microsoft сама пояснює в деталях, як це робиться, на спеціальній сторінці, потрапити на яку можна натиснувши при відкритті документа кнопку Learn more, що приходить на зміну кнопці Enable Content.

Крім того, організації, які використовують макроси Office, зможуть вимкнути новий захід безпеки за допомогою групових політик. Адміністратори також зможуть встановити так звані надійні розташування (Trusted Locations), тобто папки, диски та мережеві ресурси, що містять файли, які за правилами організації можна відкривати без додаткових пересторог.

Ще один не зовсім очевидний нюанс полягає в тому, що захист від шкідливих документів Office працює тільки якщо ті завантажені з інтернету на накопичувач з файловою системою NTFS. Тільки вона зберігає метадані (альтернативні потоки даних, ADS) про походження файлу, які розуміють Windows і Office.

Файлова система FAT32, яка все ще періодично зустрічається на USB-накопичувачах невеликої ємності (флешках), на відміну від NTFS не підтримує ADS і, зокрема, потік Zone.Identifier, який при необхідності автоматично генерується в момент створення файлу у файловій системі та містить відомості про зону його розміщення.

Запропонований метод не є панацеєю і викликає нарікання з боку користувачів. Втім, і в самій Microsoft погоджуються з такою думкою. За словами представника компанії Трістана Девіса, сенс нововведення полягає в тому, щоб зловмисникам стало важче змусити користувачів обманом запустити шкідливий код. Розробники планують і надалі вносити правки в роботу макросів на платформі Office.

Маркус Хатчинс, дослідник безпеки, який свого часу зупинив поширення WannaCry, у своєму Twitter привітав рішення Microsoft, проте дорікнув, що компанія обмежилася мінімумом змін.

Техніка приховування шкідливого VBA-скрипту в документах Office та примусу користувачів до його запуску фішинговими методами широко застосовується сучасними кіберзлочинцями. Як пише Bleeping Computer, таким чином, зокрема, поширюються відомі Emotet, Trickbot, Qbot і Dridex.

Що стосується особистих документів то існує дві основні причини, за яких варто вжити заходів безпеки: захист конфіденційних даних та захист даних від редагування. Розробники офісного пакету Microsoft Office передбачили ряд функцій, для вирішення таких завдань. Щоб скористатися такими функціями необхідно виконати Файл→Відомості→Захист документа. В результаті користувачу будуть доступні функції: (1) Позначити як остаточний. Документ стане заблокованим для редагування; (2) Зашифрувати паролем. Пропонується ввести пароль, за допомогою якого буде зашифрований документ; (3) Обмежити редагування. Буде встановлено обмеження на форматування або редагування документа; (4) Додати цифровий підпис. Захистити файл за допомогою цифрового підпису. Такий метод захисту дозволяє упевнитися в достовірності і цілісності документа.