УДК 004.89

Студ. О.А. Волгина, Ю.В. Горощеня
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СКРЫТАЯ ПЕРЕДАЧА ИНФОРМАЦИИ НА ОСНОВЕ МОДИФИКАЦИИ МАКРОСОВ

Известна проблема, связанная с возможностью сокрытия информации или кода (в том числе – вредоносных) в широко используемых офисных форматах файлов (.doc, .docx и .xml) [1]. Одним из средств для такого сокрытия служат макросы, написанные на языке Visual Basic for Applications (VBA) [2].

Работа фокусируется на использовании документов Microsoft Office, поддерживающих макросы. Формат .docx основан на стандарте Office Open XML (OOXML), представляя собой ZIP-архив с XML-файлами и другими ресурсами [3].

Ключевым компонентом для хранения макросов в таких файлах является бинарный файл vbaProject.bin (обычно расположенный в подкаталогах word/, xl/ и т.п.). Наличие этого файла является индикатором присутствия макросов в документе. Основным контейнером для скрываемой информации в рамках исследуемого метода выступает сам код VBA-макроса, хранящийся внутри vbaProject.bin.

Основная идея метода заключается во внедрении скрываемой информации непосредственно в исходный код VBA-макроса. Это основано на использовании комментариев, модификации имен, внедрение скрываемой информации в строковые литералы/фиктивный код.

Перед внедрением данные кодируются (например, на основе функции StrToBinary для преобразования текста в бинарную строку). Для извлечения необходим обратный процесс: анализ кода макроса (например, функция BinaryToString). В работе исследуется применение средства AutoHotkey (AHK) для автоматизации. AHK – это скриптовый язык для автоматизации задач в Windows.

Алгоритм включает следующие шаги: получение исходного сообщения (из файла, буфера обмена, диалога); кодирование сообщения (встроенными средствами AHK или вызовом внешних скриптов); запуск целевого приложения (например, Excel) и открытие файла-контейнера (.xlsm); использование редактора VBA; выполнение операций стеганографического сокрытия информации.

Для реализации используются ключевые функции AHK: Run, WinWaitActive, SendInput, ControlSend, FileRead, FileCopy и др.

Исследуемый метод имеет существенные ограничения:

1) низкая пропускная способность;

2) высокий риск обнаружения;

3) скрипты, основанные на эмуляции GUI, чувствительны к обновлениям ПО, изменениям интерфейса, разрешению экрана.

Пути повышения устойчивости:

1) шифрование данных;

2) распределение и маскировка: разбиение данных на мелкие фрагменты и их распределение по разным частям кода (комментарии, строки, имена), имитация реального кода;

3) динамическая адаптация: использование автоматизации для выбора разных носителей или модификации структуры макроса для усложнения сигнатурного анализа.

Метод может использоваться как в легитимных (защита коммуникаций в специфических условиях, тестирование безопасности, обучение), так и в деструктивных целях (эксфильтрация данных, управление вредоносным ПО, обход контроля). Это подчеркивает необходимость ответственного подхода к исследованию и применению подобных технологий, соблюдения этических норм и законодательства.

Исследование показало техническую реализуемость скрытой передачи данных через модификацию VBA-макросов, а также эффективность использования AutoHotkey для автоматизации этого процесса. Основным методом сокрытия рассмотрено внедрение данных в комментарии VBA-кода. Выявлены ключевые ограничения метода: низкая пропускная способность и высокий риск обнаружения современными средствами защиты. Предложены пути повышения устойчивости, такие как шифрование и распределение данных. Рассмотрены потенциальные сферы применения и связанные с ними этические и правовые вопросы.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Сидоров И. П. Угрозы информационной безопасности, связанные с использованием макросов в офисных приложениях // Вопросы кибербезопасности. – 2020. – № 4 (38). – С. 21–29.

3. Урбанович П. П., Юрашевич Д. Э. Использование системных свойств и параметров текстовых файлов в стеганографических приложениях// Теоретическая и прикладная криптография: материалы международной научной конференции, Минск, 20–21 октября 2020 г. – Минск: БГУ, 2020. – С. 68–73.