Макровирус

https://habr.com/company/dsec/blog/353800/

Информационная безопасность,
Блог компании «Digital Security»

Безопасность Microsoft Office: макросы VBA

- В 2016 году исследователи отметили всплеск активности, практически второе рождение, еще недавно казавшейся безнадежно устаревшей техники распространения нежелательного ПО — несущих злонамененную нагрузку макросов в документах Microsoft Office, т.н. «**макровирусов**».

  Самый знаменитый **макровирус, Melissa**, появился в марте 1999 года. Вирус поразил по крайней мере сто тысяч компьютеров по всему миру, парализовал работу сотен компаний, ущерб экономике составил 80 миллионов долларов в одних только США.

Макровирусы «сегодня»

Судя по отчетам компаний, связанных с информационной безопасностью, на сегодняшний день макровирусы все еще занимают **верхние строчки в рейтингах по распространенности**.

Что такое «макрос»

Так называемые «макросы» Microsoft Office представляют собой небольшие программы для интерпретируемого языка Visual Basic for Applications (VBA), поддержка которого встроена в линейку продуктов Microsoft Office.

Макросы в силу своих возможностей могут быть использованы для практически любой задачи автоматизации офисной работы.

Какие программы поддерживают макросы VBA

- VBA охватывает все версии Microsoft Office для Windows, начиная с 1997г. и включая еще не вышедший 2019, а также некоторые другие приложения Microsoft, такие как MapPoint и Visio, и ПО других производителей: AutoCAD, CorelDraw, LibreOffice, Reflection, WordPerfect.

  Реализована поддержка VBA и в Office for Mac OS X, за исключением 2008.

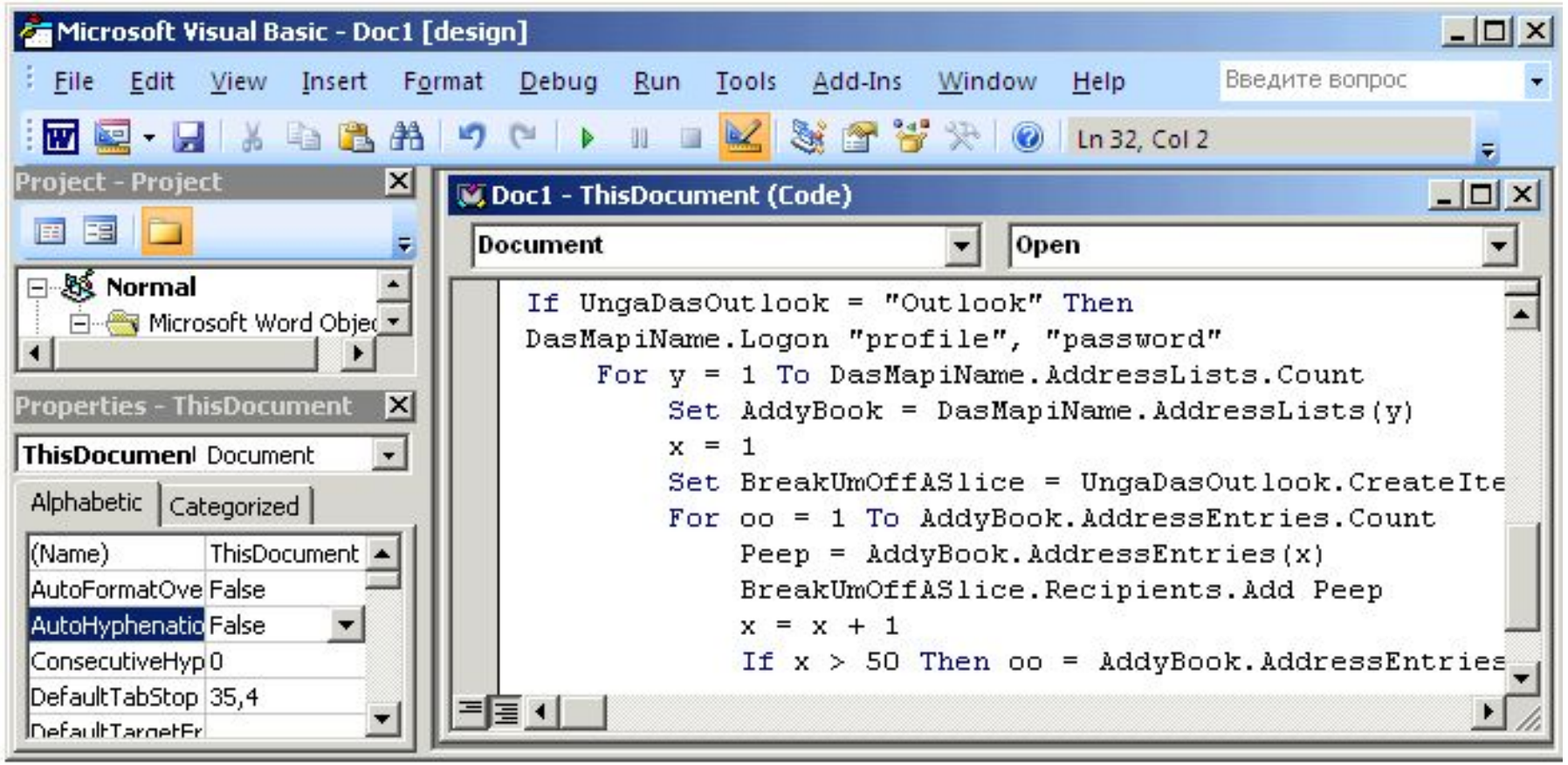
  При выборочной установке Microsoft Office можно отказаться от поддержки VBA, но по умолчанию эта подсистема входит в набор устанавливаемых программ.

Обход методов противодействия макровирусам

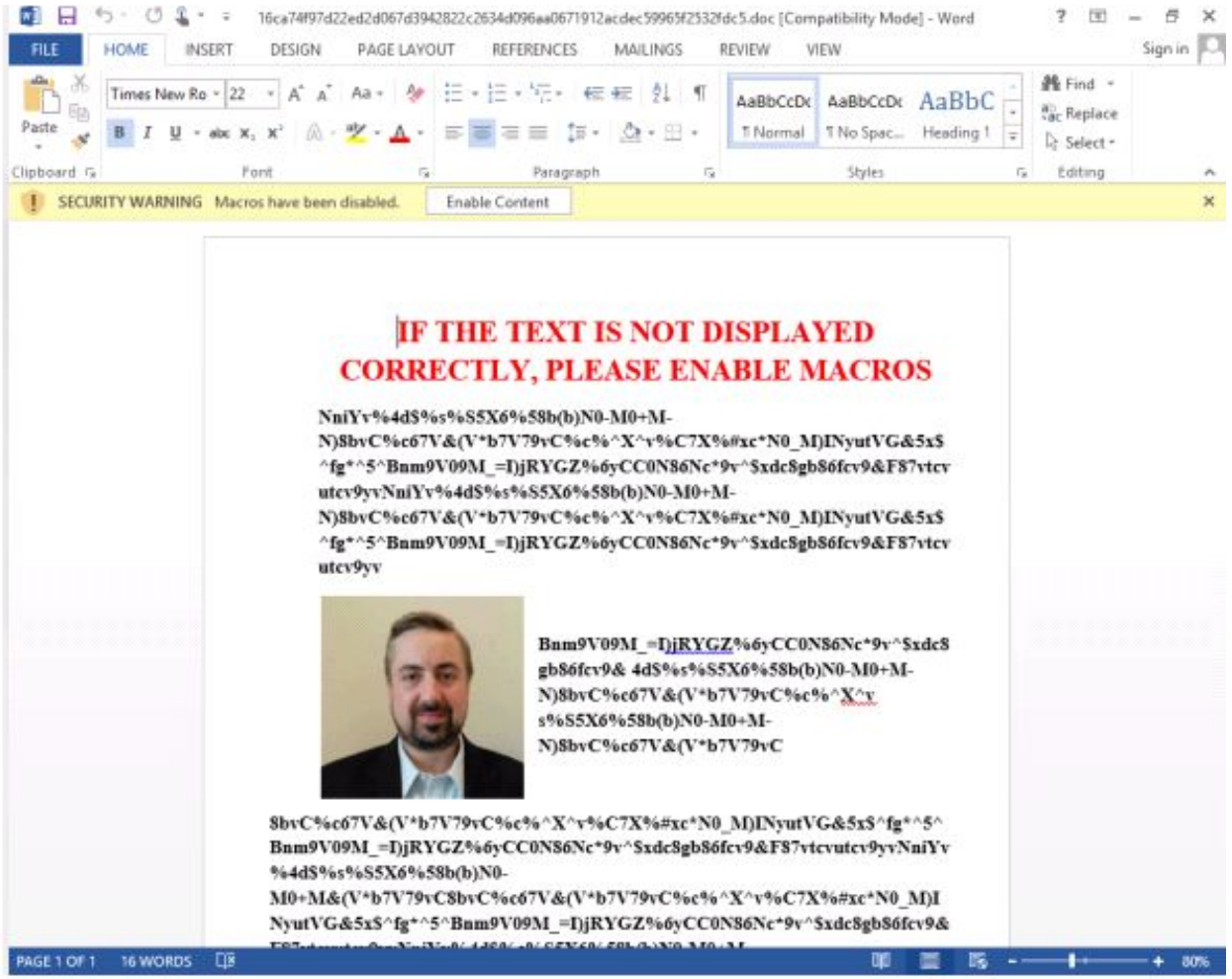
- Большинство методов обхода механизмов безопасности строятся на **социальной инженерии**. Пользователи не воспринимают файлы Microsoft Office с макросами как исполняемые, поэтому легко вводятся в заблуждение демонстрацией ненормального открытия документа и приглашением пользователя включить макросы, чтобы устранить проблемы. Злоумышленники предоставляют подробные инструкции, на случай, если пользователи сами не могут догадаться как это сделать, и весомо выглядящее обоснование необходимости их включения.

  На форумах соответствующей тематики можно встретить объявления о создании «индивидуальных дизайнерских решений» для оформления документов, призванных убедить пользователя включить активное содержимое. Стоимость таких решений может быть значительной, а эффективность, по мнению авторов, доходит до 60%.

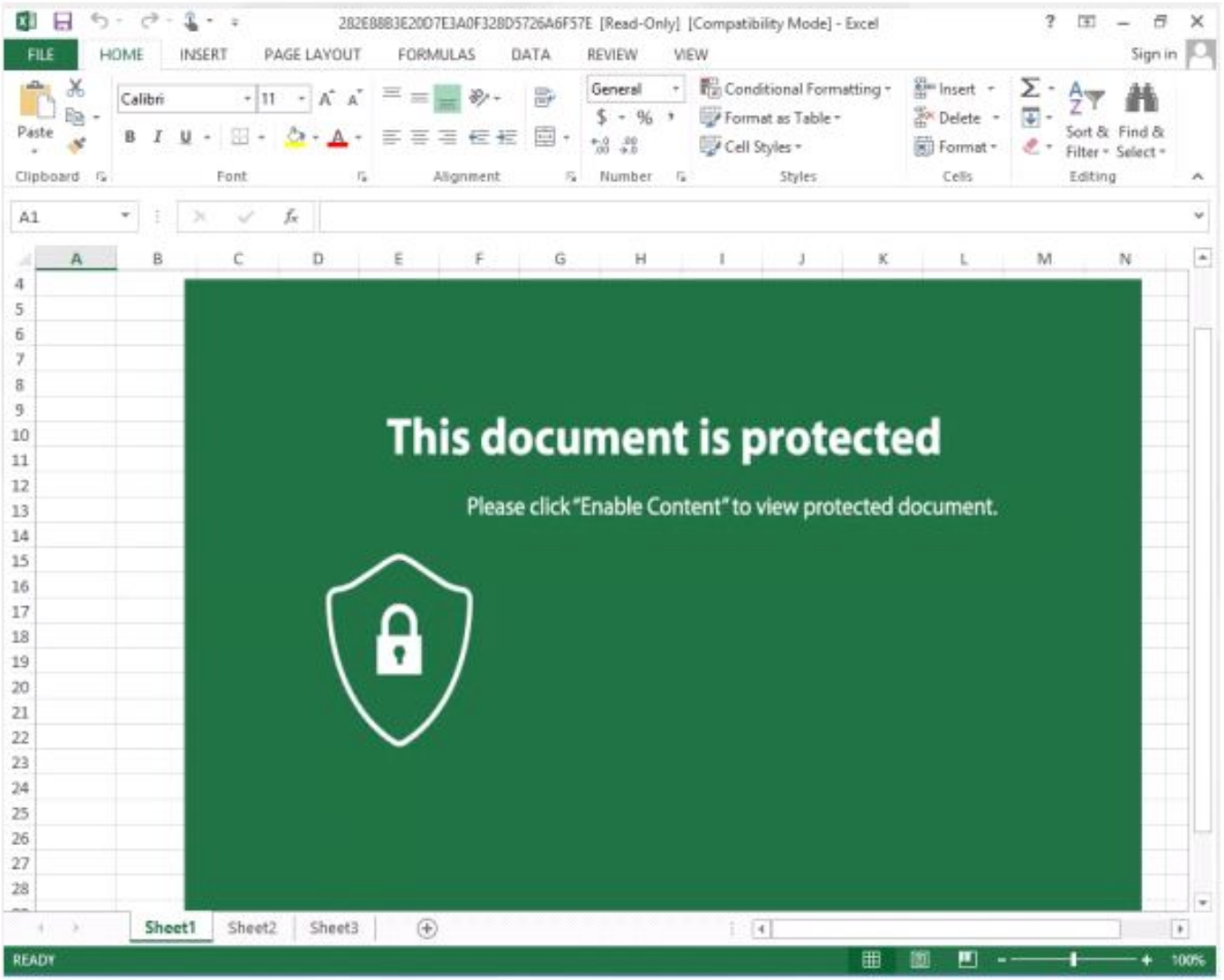
VBA


Microsoft Visual Basic - Doc1 [design]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Введите вопрос
Ln 32, Col 2
Project - Project
Normal
Microsoft Word Objec
Properties - ThisDocument
ThisDocumen Document
Alphabetic Categorized
(Name) ThisDocument
AutoFormatOve False
AutoHyphenatic False
ConsecutiveHyp 0
DefaultTabStop 35,4
Doc1 - ThisDocument (Code)
Document
Open
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
For y = 1 To DasMapiName.AddressLists.Count
Set AddyBook = DasMapiName.AddressLists(y)
x = 1
Set BreakUmOffASlice = UngaDasOutlook.CreateIte
For oo = 1 To AddyBook.AddressEntries.Count
Peep = AddyBook.AddressEntries(x)
BreakUmOffASlice.Recipients.Add Peep
x = x + 1
If x > 50 Then oo = AddyBook.AddressEntries

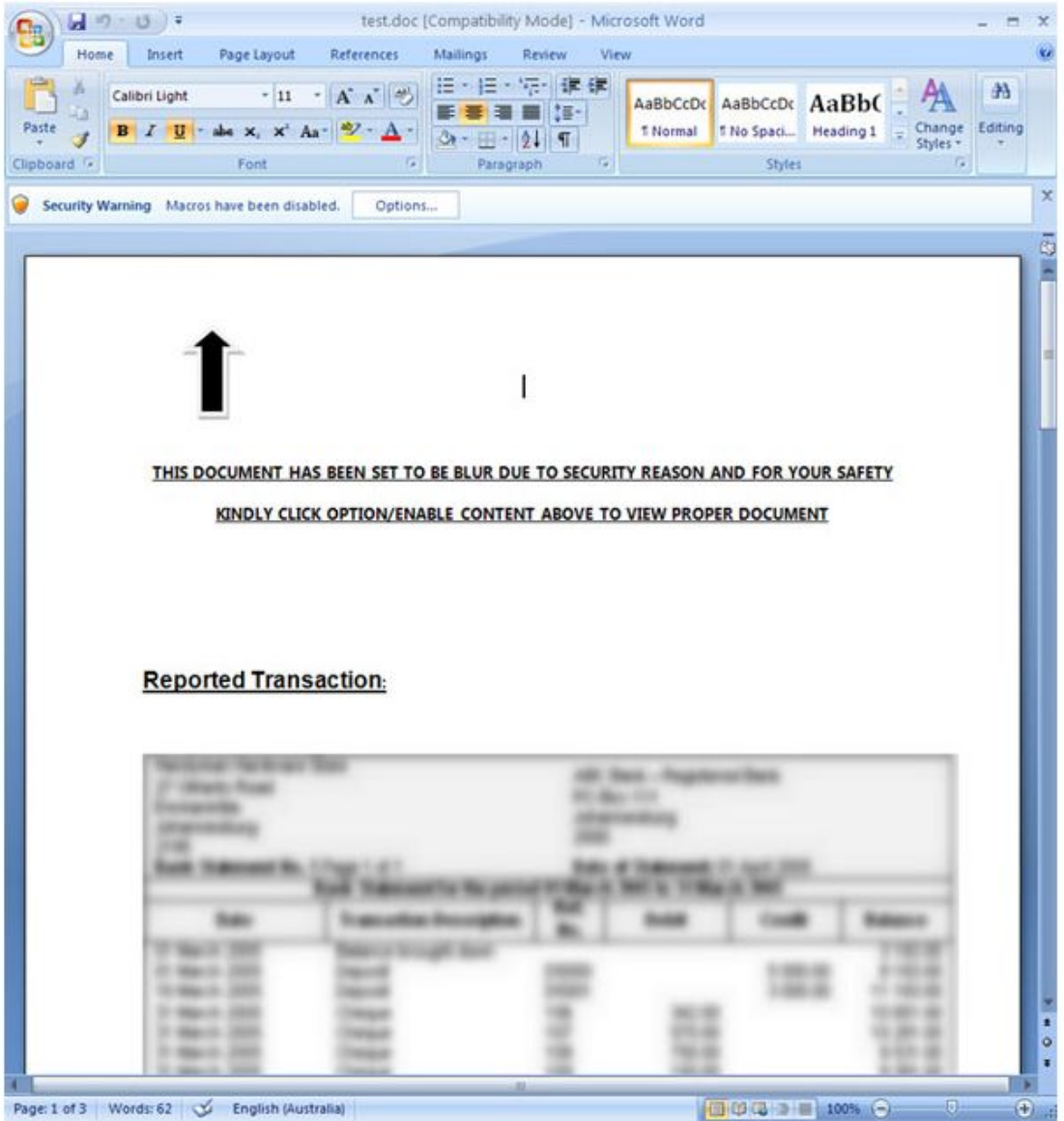
Пример (ENABLE MACROS)



Пример (click “Enable Content”) для просмотра защищенного



Пример (click “Enable Content”) для просмотра свойств документа



Как реализована поддержка VBA

- Код, созданный в редакторе VBA, сохраняется внутри файла документа. Документы современного формата Office Open XML, содержащие макросы, должны иметь специальное расширение (".**docm**",".**dotm**",".**xlm**",".**xltm**", ...), в противном случае приложение откажется их открывать. Внутри zip-архива документа проект VBA хранится в файле-хранилище CFBF.

Встроенные механизмы противодействия макровирусам

- Два механизма безопасности интегрированы непосредственно в приложения Microsoft Office:

  * Защищенный режим просмотра
  * Политики запрета исполнения макросов VBA.

Защищенный режим просмотра

- В Microsoft Office есть защищенный режим, который активируется при просмотре файлов, **загруженных из интернета**, **запрещает запуск любого активного содержимого (в том числе, и макросов)** и создает ряд ограничений для процесса, который открывает этот документ. При открытии документа в таком режиме создается дочерний процесс (в котором и происходит просмотр документа) с пониженным уровнем целостности и ограничением Job на создание дочерних процессов (делается ограничением одного активного процесса в Job).

  Эти ограничения, в первую очередь, направлены на предотвращение эксплуатации обычных бинарных уязвимостей в самом офисном приложении.

  Изоляция процесса, отображающего документ в защищенном режиме, реализована в целом хорошо и заслуживает отдельного упоминания.

Задание

- 1) Изучите методы защиты от макровирусов на сайте https://habr.com/company/dsec/blog/353800
- 2) Какие методы обхода защиты от макровирусов существуют?