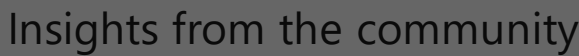




 16



## What are the steps to using VBA macros in Excel for data analysis?

## What are the best practices for writing and testing SAS macros?

How do you test and validate the results of your SAS programs?

What are the easiest ways to automate excel functions?

## How do you automate SSAS testing with Visual Studio and SSIS?

## What are the common causes and solutions for SSAS deployment timeout errors?

explore topics

## Soft Skills



## Open the app

Published May 31, 2018

## What is VBA for Outlook?

Visual Basic for Applications (**VBA**) is a programming language for writing code in **Outlook**. Useful for automating tasks such as adding contacts, saving automatically certain items, and creating automatically calendar items.

## How to enable unrestricted VBA execution

Disable Outlook's security policies via modifying the following registry (by default it's value is set to **0**, disabled) key to enable the macro to run without prompting any warning to the user/victim:

```
REG ADD "HKEY_CURRENT_USER\Software\Microsoft\Office\  
<redacted_version_number>\Outlook\Security" /v "Level" /f /t REG_DWORD /d 1
```


## How to enable persistence ?

Modify the following Outlook registry setting (by default it's value is set to 0 meaning disabled) to enable automatic loading of any configured VBA project/module:

```
REG ADD "HKEY_CURRENT_USER\Software\Microsoft\Office\  
<redacted_version_number>\Outlook" /v "LoadMacroProviderOnBoot" /f /t REG_DWORD  
/d 1
```

## Backdoor functionalities ?

- ## 1. Monitor the Inbox, Junk and Sent Items



LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your [settings](#).

4. Forward emails sent or received containing list of keywords (i.e. Confidential, Secret, Payroll, Payment, Password, Credential etc.) in the email body or subject

5. Delete all left traces from the Sent, Inbox, Junk and Deleted email folders

### Meat, Viande, لحم ?

VBA code can be downloaded from [here](#), to test it follow those steps (after modifying the above mentioned Outlook registry settings):

1. Add the Developer tab in Outlook: Step 1: Click the File tab and Options button in Outlook 2010 / 2013. Step 2: In the Outlook Options dialog box, click the Customize Ribbon on the left bar. Step 3: In the right section, select the Main Tabs in the Customize the Ribbon box. Step 5: Check the Developer item.

2. Open Visual Basic Menu: Step 1: Click On the Developer tab in Outlook. Step 2: Click on the Visual Basic Menu button. Step 3: Click on the Visual Basic Editor button. Step 4: Click on the Visual Basic Studio Tab.

3. Place this code in the "ThisOutlookSession" module of a new VBA project. Save the compiled VBA file named "**VbaProject**" in the path: **<redacted>\AppData\Roaming\Microsoft\Outlook\** the victim computer on the equivalent path on the attacker computer.

4. Replace the hard coded e-mail address with the attacker's e-mail address (i.e. owned address. For the command execution, replace the e-mail address with the sender address)

### Some screenshots:

*Don't forget to check the registry settings*


### Detection ?

Using Sysmon or an EDR solution:

- regmod: Outlook\Security\Level (registry modification)
- regmod: Software\Microsoft\Office\*\Outlook\LoadMacroProviderOnBoot
- (process\_name:cmd.exe or process\_name:powershell.exe) and parent\_name:outlook.exe
- filemod: \*\VbaProject.OTM (First Write Operation)
- filemod: \*\VbaProject.OTM and -process\_name:outlook.exe

Using Email Security Gateway or Exchange Logs:

- High number of emails with subject "FW:\*" to non-domain destination email addresses from same sender within interval of 30 minutes
- High number of emails with destination non company email address from same sender. (useful for Data Leak detection) within interval of 30 minutes




### Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? [Join now](#)


By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

 LINKEDIN

### LinkedIn is better on the app

Don't have the app? Get it in the Microsoft Store.

[Open the app](#)

 LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your [settings](#).

To view or add a comment, [sign in](#)

More articles by Samir B.

Jun 20, 2018

**Preventing Privileges Escalation via real-time monitoring of Common Bad Habits P1/2**

Systems privileges escalation is a critical step for any attacker to achieve his intended objectives. Oftentimes it...

20

Feb 21, 2018

**Cre**

**Pass**

No n

Outl

39

Jan 2

**Min**

How

(Aud

Aug


**Det**

Mon

imp

6

Show more



### Sign in to view more content


Create your free account or sign in to continue your search

or

New to LinkedIn? [Join now](#)

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

© 2024   About   Accessibility   User Agreement   Privacy Policy   Cookie Policy   Copyright Policy   Brand Policy   Guest Controls   Community Guidelines   Language

 LINKEDIN

**LinkedIn is better on the app**  
Don't have the app? Get it in the Microsoft Store.

Open the app

Page 3 of 3