Outlook-Backdoor using VBA

Samir B. Samir B.

Samir B.

Published May 31, 2018
+ Follow

In this post I will share with you how to create a simple yet effective method to obtain persistence, code execution and leak emails of interest from a victim using outlook and with limited user privileges.

What is VBA for Outlook?

Visual Basic for Applications (**VBA**) is one of two programming languages available for writing code in **Outlook**. Useful for automating repetitive tasks like clean-up of multiple contacts, saving automatically certain e-mail attachments in a specific folder or database, creating automatically calendar items etc.

How to enable unrestricted VBA execution in Outlook?

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
2. Check for the existence of a specific kind of e-mail within Inbox or Junk e-mail folders with **$$startcmd** and **$$endcmd** and execute code in between
3. Save the attachment on emails with **$$startcmd** keyword on the message body, can be coupled with previous feature to deploy extra payloads
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 Studio Tab.
3. Place this code in the "**ThisOutlookSession**" class module, after it's saved outlook will generate a compiled VBA file named "**VbaProject.OTM**" in **c:\users <redacted>\AppData\Roaming\Microsoft\Outlook\VbaProject.OTM**. You can copy this file in the victim computer on the equivalent same location:


4. Replace the hard coded e-mail address for forwarding-to-e-mails of interest to your owned address. For the command execution function it's not need (independent from the sender address)

Some screenshots:

Don't forget to change the text color of $$startcmd and $$endcmd to "white"


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

شكرا للقراءة

More articles by Samir B.

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

  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

- Credentials Phishing using the annoying Outlook Password Dialog Popup

Feb 21, 2018

Credentials Phishing using the annoying Outlook Password Dialog Popup

No need to introduce to Outlook users the daily occurrence of the Outlook Password Popup (OPP)! Some users close it and…

39
1 Comment

- Mimikatz detection using Windows Security Event Logs

Jan 25, 2017

Mimikatz detection using Windows Security Event Logs

How-To: > Audit Policy Configuration: Enable Object Access Audit (Audit Handle Manipulation + Audit Kernel Object)…

73
10 Comments

- Detect and monitor threats to your executive mailboxes

Aug 12, 2016

Detect and monitor threats to your executive mailboxes

Monitoring access to your company executives mailboxes is very important (Some of the Risks listed below), especially…

6

- Windows Events vs Malware

Sep 12, 2015

Windows Events vs Malware

Below some Microsoft windows events that can help to identify malware presence, at the end of the post a summary of the…

12
1 Comment

- File Extensions That Are Potentially Dangerous on Windows

Aug 26, 2015

File Extensions That Are Potentially Dangerous on Windows

Most people know that .exe files are potentially dangerous, but that isn't the only file extension to beware of on…

20
9 Comments

Show more
See all articles

Insights from the community

- Business Analysis
  What are the steps to using VBA macros in Excel for data analysis?
- Statistical Programming
  How do you test and validate the results of your SAS programs?
- Statistical Programming
  What are the best practices for writing and testing SAS macros?
- Geographic Information Systems (GIS)
  How do you troubleshoot a GIS application with high memory usage?
- Computer Literacy
  What are the easiest ways to automate Excel functions?
- Analysis Services
  How do you automate SSAS testing with Visual Studio and SSIS?
- Programming
  How do you choose the right data types for generic programming?
- Analysis Services
  What are the common causes and solutions for SSAS deployment timeout errors?
- Linear Programming
  How do you use Excel Solver for linear optimization in different fields and applications?
- Programming
  How can you use HTML5 File API to read and write files?

Show more Show less

Others also viewed

- **Excel for ENGINEERS**

  Rahul Harale 1y
- **Excel - SWITCH Function**

  Excel BI 3y

- ### AI Apps on your Phone? Visual Basic points the way

  Dave Holmes-Kinsella 4mo

- ### 🌟 Exciting News from the Excel World! 🚀

  Andrew Chan, IFRI Certified 10mo

- ### VBA

  NISHI KUMARI 2y

- ### How to Remove VBA Password from XLSM File in Simple Steps?

  Leena Taylor Paul 2mo

- ### Is VBA on the Verge of Extinction? Exploring the Decline in Popularity of Visual Basic for Applications

  Sanjay T S 1y

- ### Some hat tricks on Excel VBA

  Alex Ooi 5y

- ### Best Practices for Excel VBA Code

  Olusola Oguntuberu 5y

Show more Show less

Explore topics

- Sales
- Marketing
- IT Services
- Business Administration

- HR Management
- Engineering
- Soft Skills
- See All

- Svenska (Swedish)
- తెలుగు (Telugu)
- ภาษาไทย (Thai)
- Tagalog (Tagalog)
- Türkçe (Turkish)
- Українська (Ukrainian)
- Tiếng Việt (Vietnamese)
- 简体中文 (Chinese (Simplified))
- 正體中文 (Chinese (Traditional))

Language