Agree & Join LinkedIn

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

Sign in to view more content

Create your free account or sign in to continue your search

Sign in

Welcome back

Email or phone

Password   Show

Forgot password? Sign in

or

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

New to LinkedIn? Join now

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.

- Articles
- People
- Learning
- Jobs
- Games
- Get the app

Join now Sign in

Outlook-Backdoor using VBA

- Report this article

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

[Like](#)
[Comment](#)

- Copy
- LinkedIn
- Facebook
- Twitter

Share
☐ [16](#)

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

More articles by this author

No more previous content

- [Preventing Privileges Escalation via real-time monitoring of Common Bad Habits P1/2](#)

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

  Jun 20, 2018

- Credentials Phishing using the annoying Outlook Password Dialog Popup

  Credentials Phishing using the annoying Outlook Password Dialog Popup

  Feb 21, 2018

- Mimikatz detection using Windows Security Event Logs

  Mimikatz detection using Windows Security Event Logs

  Jan 25, 2017

- Detect and monitor threats to your executive mailboxes

  Detect and monitor threats to your executive mailboxes

  Aug 12, 2016

- Windows Events vs Malware

  Windows Events vs Malware

  Sep 12, 2015

- File Extensions That Are Potentially Dangerous on Windows

  File Extensions That Are Potentially Dangerous on Windows

  Aug 26, 2015

No more next content

See all

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

-

  ## Microsoft VBA

  Ragini Trivedi 2y

-

  ## VBA Basics - Sub Procedures Vs Functions

  Jonathan Reyes 6y

-

  ## Making VBA Development Version Independent Part 1

  Kamal Bharakhda 6y

-

  ## 001: Introduction to Visual Basic for Applications (VBA)

  Craig Parry 5y

-

  ## VBA

  Rijika Roy 1y

-

  ## You do NOT know yet how to use Excel VBA

Julien Ribon 7y

- **Dynamic dependent Excel drop-downs using VBA**

  Sachdeep Sivakumar 4y

- **VBA**

  Dipti Goyal 2y

- **VBA: The Gateway Code**

  Jeremiah Vanderlaan 9y

Show more   Show less

Explore topics

- Sales
- Marketing
- IT Services
- Business Administration
- HR Management
- Engineering
- Soft Skills
- See All

- Ελληνικά (Greek)
- **English (English)**
- Español (Spanish)
- فارسی (Persian)
- Suomi (Finnish)
- Français (French)
- हिंदी (Hindi)
- Magyar (Hungarian)
- Bahasa Indonesia (Indonesian)
- Italiano (Italian)
- עברית (Hebrew)
- 日本語 (Japanese)
- 한국어 (Korean)
- मराठी (Marathi)
- Bahasa Malaysia (Malay)
- Nederlands (Dutch)
- Norsk (Norwegian)
- ਪੰਜਾਬੀ (Punjabi)
- Polski (Polish)
- Português (Portuguese)
- Română (Romanian)
- Русский (Russian)
- 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