The ILOVEYOU Worm

Matt Bishop
Dept. of Computer Science
University of California, Davis

Outline

- Overview of Worm
- The Five Parts (in detail)
- The Analysis
  - Putting it all together
  - System requirements
  - Effects of execution
  - Countermeasures
- Conclusion

Overview

- Questions this talk answers:
  - The worm targeted Windows system running Visual Basic. Would it work against other systems?
  - Is it architecturally tailored to Windows? How hard would it be to modify it to run on UNIX-based or Macintosh systems?
  - What can we do to minimize this danger?

Overview of Worm

- Visual Basic, processed by Wscript
- Four separate components, all invoked by *main* routine
- Notation:
  - *rootfolder*: folder at root of file hierarchy
  - *systemfolder*: folder containing Windows OS
  - *tempfolder*: folder for temporary files

main

- Copy worm script into:
  - *rootfolder*\MSKernel32.vbs
  - *rootfolder*\LOVE-LETTER-FOR-YOU.TXT.vbs
  - *systemfolder*\Win32DLL.vbs
- Invoke other routines:
  - *regrun*
  - *spreadtoemail*
  - *html*
  - *listadriv*

regruns Component

- Set reboot registry keys to the first and third names
- Set up *tempfolder*\WIN-BUGSFIX.exe
  - Set the Internet home page for Internet Explorer to one of 4 randomly-chosen values for the WIN-BUGSFIX.exe program
  - If *tempfolder*\WIN-BUGSFIX.exe present, set it to run at boot time and reset IE Internet home page to blank

html Component

- Creates a web page to be forwarded through IRC
  - Contains Java script to create window, pass control to Visual Basic script that recreates and executes worm
  - Considerable care in code to include chars meaningful to VB and HTML such as \, /, ‘, and “

spreadtoemail Component

- Go through Outlook address book (list)
  - Create Registry key for list
  - Create Registry key for each entry in list
  - If latter key doesn't exist yet, send addressee a letter with subject ILOVEYOU and containing the LOVE-LETTER-FOR-YOU.TXT.vbs as attachment

listadriv Component

- It modified files
  - VB files were overwritten with the worm
  - Some interpreter files deleted, VB file with same name but with “vbs” extension containing the worm created
  - JPEG files deleted, VB file with same name but with “vbs” extension appended to jpg extension containing the worm created
  - MPEG files hidden, VB file like JPEG

listadriv Component

- Send web page over mIRC
  - Check for mIRC files in each folder
  - If found, create script.ini that will send the LOVE-LETTER-FOR-YOU.HTM to any channels joined

Putting It All Together

- *main* makes copies of the worm for future use, and makes sure the worm survives across system boots.
- *regruns* arranges that the next invocation of Internet Explorer will download a program. On the next run of the worm, this program is added to the startup program set.

Putting It All Together

- *html* creates a web page that will go out over IRC later.
- *spreadtoemail* gathers the addresses in the Outlook address books, and forwards a copy of the worm to each (once per address).

Putting It All Together

- *listadriv* recursively scans the drives and replaces VB, ActiveX, Java, and JPEG files with the worm. It hides MPEG files and creates unhidden files that contain the worm. It then prepares an mIRC initialization script that forwards the worm whenever an IRC channel is joined

Worm Bugs and Bogosities

- The address in an address book with exactly 1 address is skipped
- A routine (*folderexists*) to check that a folder exists is not called anywhere, and would not work right even if it were called.

Effects on Other Systems

- Macintosh: no Registry
  - If you use Outlook, worm is sent to all folks every time worm is run
  - Download for WIN-BUGSFIX fails
  - Files neither deleted nor overwritten
  - *mIRC* doesn't run

Effects on Other Systems

- UNIX-based, Linux
  - None; no VB interpreter available

Worms In General

- Any system with a "little language" can fall victim to something like the ILOVEYOU worm
  - Macintosh: Applescript, PERL
  - UNIX-based Systems: *sh*, *csh*, *awk*, *sed*, PERL, …
- Function of power of macro language and facility

Countermeasures

- Locating and deleting the worm
  - Look for files mentioned earlier and delete them
  - Delete Registry keys
  - Reset IE's home page
  - Search for the .vbs files and delete them

General Protection

- Analysis
  - Malicious logic
  - Discretionary Trojan Horse
  - Worm
  - Virus?
- What are some defenses against these?

Strong Typing

- Types: data, instructions
- Data arrives via email
- Converting it to instructions requires a *trusted* user to act

Sandboxing

- Limit the protection domain in which programs run
- Problems:
  - May impose unacceptable constraints
  - Need to define the constraints carefully, on a per-program basis

Karger's Subsystem

- Intercept every resource access
- Check that it is allowed
  - If not known, ask user or follow predefined action (should be deny access)
- If allowed, complete the access

Signatures

- Usual approach to malicious logic detection
- Tied to particular characteristic(s) of malicious logic
  - ILOVEYOU
  - Funny joke
  - Mother's Day

Anomaly Detection

- Variant: know what expected behavior is, and look for unusual behavior
- Problems: define “unusual behavior”; what do you do when you see it?

Conclusion

- It's pretty bad
- It's not going to get better
- Take steps to protect yourself
- Understand what happens, and you will be better prepared to handle the next one