Viruses Part 2:
The Making of a Virus

S-38.153 Security of Communication Protocols, Spring 2003
Jaakko Kotimäki

Writing viruses – the hard way

- Assembler language
  - MS-DOS, Windows
- Visual Basic Scripts
  - Windows
- Other languages (C, Java, scripting)
  - Unix/Linux and other

Writing viruses – the easy way

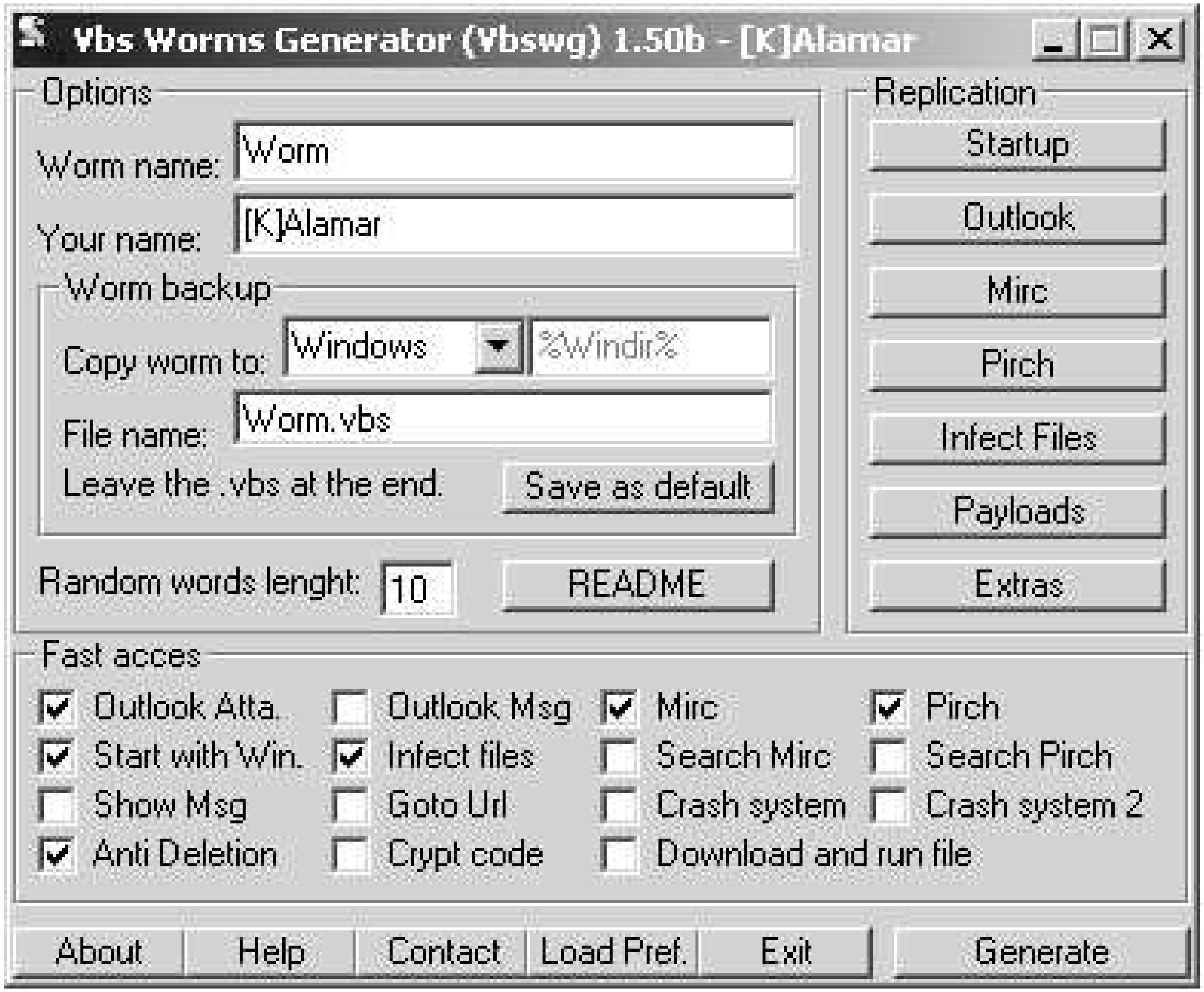
Virus generators

- Virus Script Generators
- Polymorphic Virus Generators

Virus Script Generators

- Most common type of virus generation kit
- No expertise in programming needed, just point and click
- A lot of variants, easily found from the web
- Generated viruses are easily detected with virus scanners

Virus Script Generators



Vbs Worms Generator (Vbswg) 1.50b - [K]Alamar

Options

Worm name: Worm

Your name: [K]Alamar

Worm backup

Copy worm to: Windows %Windir%

File name: Worm.vbs

Leave the .vbs at the end.

Random words lenght: 10

Fast acces

☑ Outlook Atta.
☑ Start with Win.
☐ Show Msg
☑ Anti Deletion
☐ Outlook Msg
☑ Infect files
☐ Goto Url
☐ Crypt code
☑ Mirc
☐ Search Mirc
☐ Crash system
☐ Download and run file
☑ Pirch
☐ Search Pirch
☐ Crash system 2

Polymorphic Virus Generators

- A way to boost a virus attack effiency
- Modifies an existing virus’s signature to avoid detection
- Easy GUI generators or modules attached to the actual virus

Case examples of viruses

- A DOS file virus
- The Internet Worm ‘Love Letter’
- An Unix Trojan

DOS file virus

- Written in assembly language
- Infect COM, EXE and SYS files
- Overwriting and non-overwriting viruses

DOS file virus
Example of the simplest structure

- Find a file to infect
- Open the file
- Write the virus to the file
- Close the file and exit

The DOS file virus source code

Internet Worm “Love Letter”

- Hit millions users within days of its existence
- Spread through email and IRC as an attachment
- A Visual Basic script which exploited vulnerabilities of Windows and naivety of users

Love Letter disassembled

- Once executed, the virus copies itself Windows system -directory and modifies the Registry to execute them on startup
- Downloads and installs a trojan which runs hidden in Windows and sends passwords to a email box
- Sends the virus via email as an attachment to every adress in Outlook address book.
- Infects all potential files on all hard drives

The Love Letter source code

An Unix Trojan

- Source code virus – malicious code hidden in a configure script of an application
- Works only if run as root
- Creates a backdoor to the system

The Unix Trojan source code

Future of virus making

- Spreading to new platforms
  - mobile phones and other embedded systems
- Platform independent viruses
  - Java viruses
- The still growing Internet
  - more worms