

Definition

A Trojan horse is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality

Origin of term: The ancient greeks laying siege to Troy...

Goals of Trojans

Duping user/syadmin into installing the Trojan

Blending in with “normal” programs running on a machine.

File naming tricks

Goal – hide true nature of a program

Hiding true filetype extension after spaces

- `textfile.txt -> textfile.txt` `.exe`
- Just as companion viruses

Many kinds of files can contain malware:

- `.api, .bat, .bpl, .chm, .com, .cpl, .dll, .dpl, .drv, .exe, .hta, .js, .ocx, .pif, .pl, .scr, .shs, .sys, .vbe, .vbs, .vxd, .wma, .wsf, .wsh`

Mimicking other processes

Goal – pretend to be another task

- Rename executable, so in a process listing, it will look like other nice processes

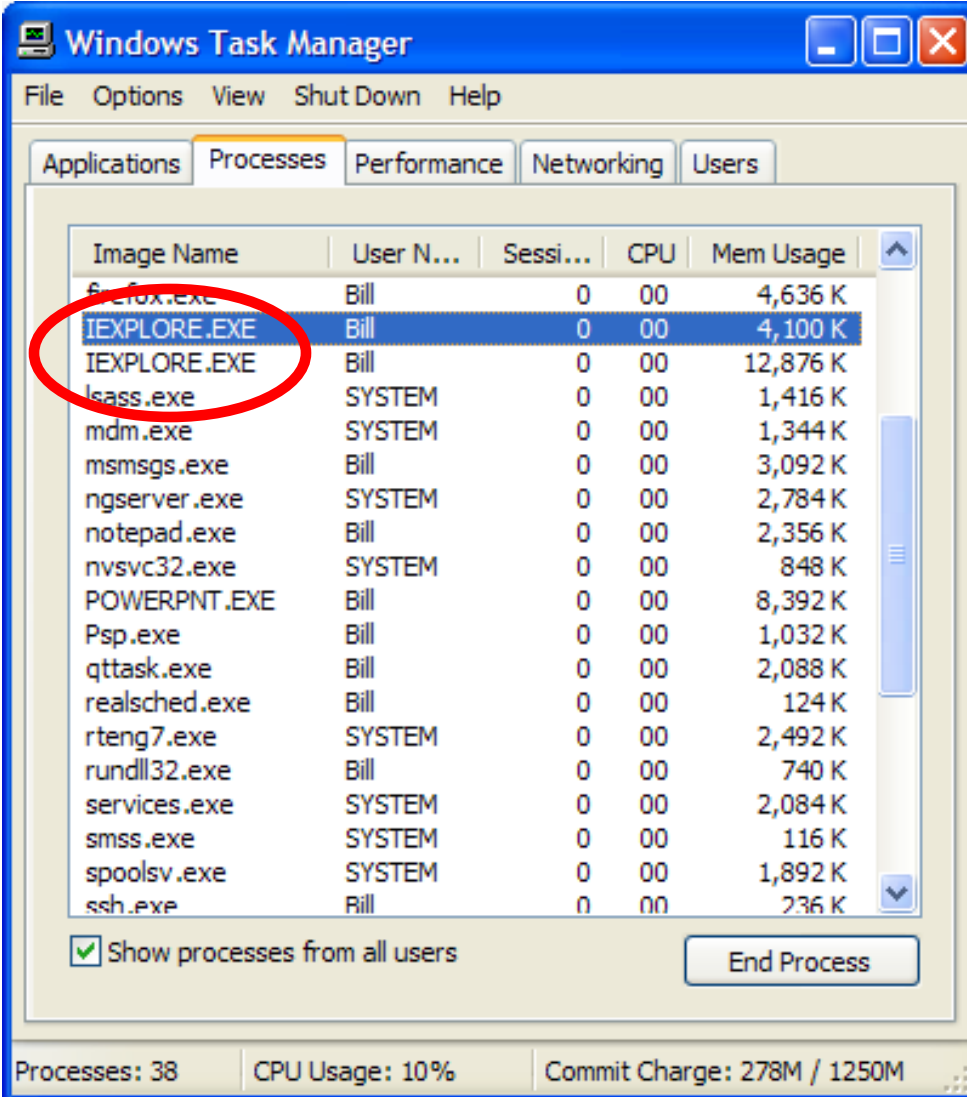
UNIX Examples:

- httpd, sshd, crond, syslogd

Windows Examples:

- explorer.exe, notepad.exe, iexplorer.exe

Windows Example



The screenshot shows the Windows Task Manager window with the 'Processes' tab selected. The window title is 'Windows Task Manager' and the menu bar includes 'File', 'Options', 'View', 'Shut Down', and 'Help'. The 'Processes' tab is active, showing a list of running processes. The 'IEXPLORE.EXE' process is highlighted with a red circle. The status bar at the bottom shows 'Processes: 38', 'CPU Usage: 10%', and 'Commit Charge: 278M / 1250M'.

Image Name	User N...	Sessi...	CPU	Mem Usage
firefox.exe	Bill	0	00	4,636 K
IEXPLORE.EXE	Bill	0	00	4,100 K
IEXPLORE.EXE	Bill	0	00	12,876 K
lsass.exe	SYSTEM	0	00	1,416 K
mdm.exe	SYSTEM	0	00	1,344 K
msmsgs.exe	Bill	0	00	3,092 K
ngserver.exe	SYSTEM	0	00	2,784 K
notepad.exe	Bill	0	00	2,356 K
nvsvc32.exe	SYSTEM	0	00	848 K
POWERPNT.EXE	Bill	0	00	8,392 K
Psp.exe	Bill	0	00	1,032 K
qtask.exe	Bill	0	00	2,088 K
realsched.exe	Bill	0	00	124 K
rteng7.exe	SYSTEM	0	00	2,492 K
rundll32.exe	Bill	0	00	740 K
services.exe	SYSTEM	0	00	2,084 K
smss.exe	SYSTEM	0	00	116 K
spoolsv.exe	SYSTEM	0	00	1,892 K
ssh.exe	Bill	0	00	236 K

Show processes from all users End Process

Processes: 38 CPU Usage: 10% Commit Charge: 278M / 1250M

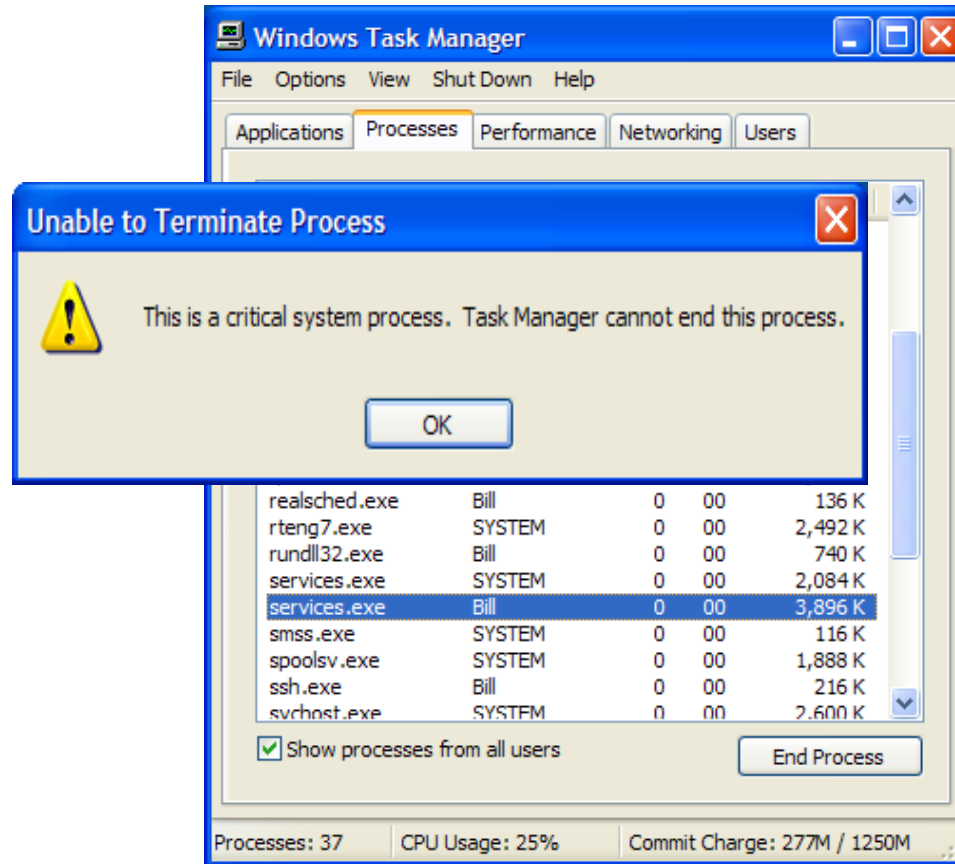
Not just for tricking users

Windows has crucial unkillable tasks

- **csrss.exe** – environment subsystem for 16-bit processes & consols
- **services.exe** – starts/stops services / daemons in background
- **smss.exe** - Session Manager SubSystem, starts programs needed after user logs on
- **winlogon.exe** – authenticates users

Renaming the file tricks the operating system!

Not just for tricking users



Exploiting UNIX paths

Goal: Trick users into running your program instead of system utilities

If user has a bad path, can pick up the wrong executable.

```
victim$ echo $PATH
```

```
./usr/local/bin:/bin:/usr/bin
```

Hiding in hacked binaries

Combine multiple programs together in a single executable

- Program with original, normal non-malicious purpose, and malware
 - e.g. notepad.exe + your back door
- Not just masquerading as other innocuous programs, it is a normal program
- Easy way to add a back door Trojan

Popular wrapper tools

AFX File Lace

- Encrypts exe, adds it to the end of another

Elite Wrap

- Binds together an unlimited # of exe's

Exe2vbs

- Converts an exe into a vbs, sneak it through firewalls

PE Bundle

- Imports all shared libraries (.dll's) into one stand-alone

Saran Wrap

- GUI wrapper for executables

Trojan Man

- Combines exe's, encrypts the result

Trojanning Software Distros

Anyone who installs the software gets your Trojan

Method #1: Old-fashioned method

- Mail the systems administrator your CDs via snail mail
- Make them look authentic so system administrator installs patch
 - “URGENT Security Patch for Solaris mountd service”
- Voila! Instant access

Method #2: Trojanning web distros

- Modify web software distributions.
- Several examples
 - monkey.org: Security/hacker tools 5/02
 - » Dsniff, fragroute, fragrouter IDS
 - openssh.org: July30-Aug1 '02
 - sendmail.org: Sep28-Oct6 '02
 - tcpdump.org Nov11-Nov13 '02

tcpdump/libpcap backdoor

November 11 '02, hackers altered the distribution of tcpdump

Normal software installation on UNIX

- Download the source
- ./configure
- make (compile the package)
- make install (install the package)

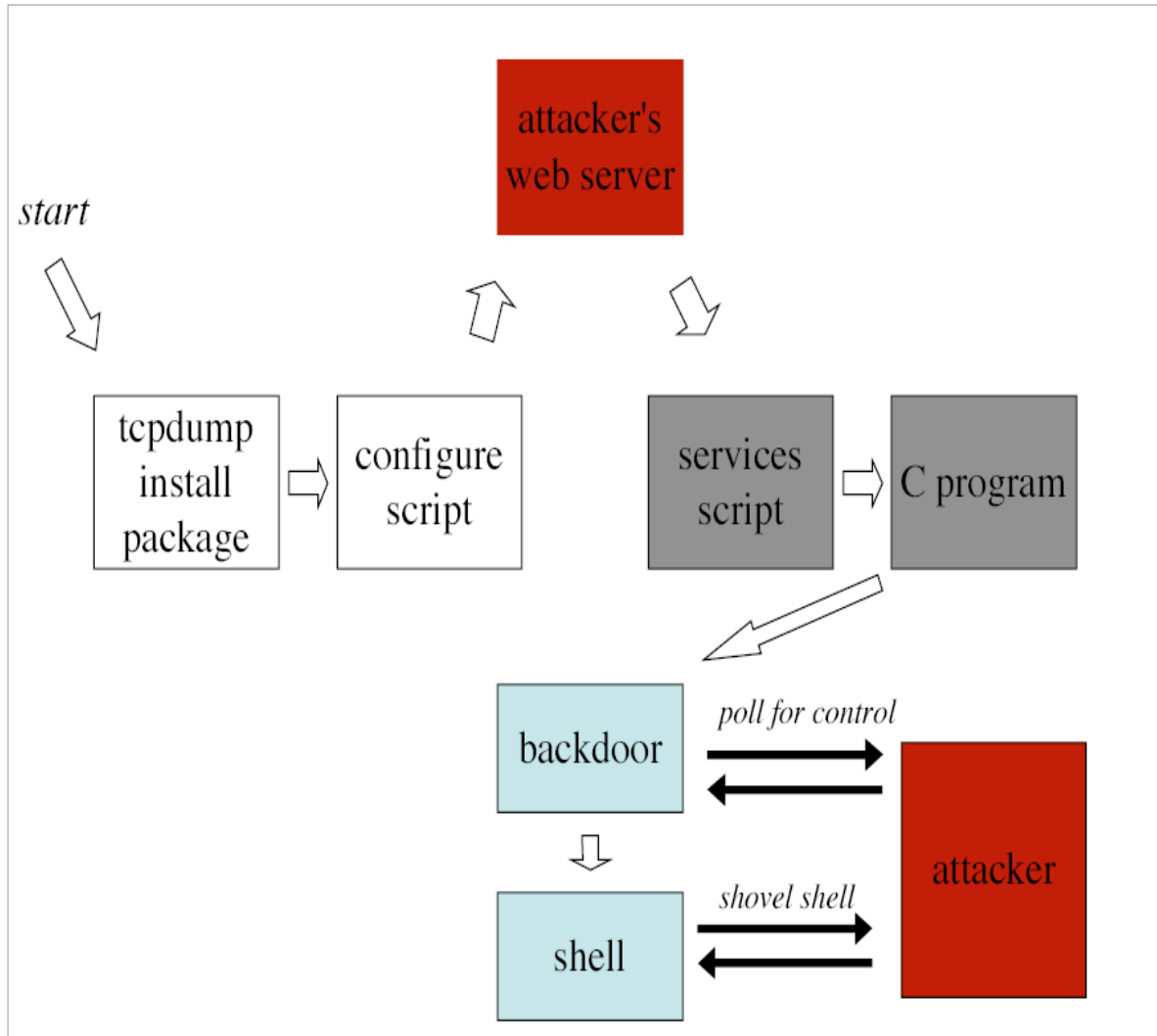
New configure: configure script downloaded software from a webserver and ran it

Execution:

- Polls for requests on TCP port 1993
- Takes one of three 1-character commands
 - 'A' – Turn self off
 - 'D' – Shovel a shell at the sender
 - » (TCPDump is usually installed as administrator)
 - 'M' – Sleep for 1 hour, then resume polling

tcpdump/libpcap backdoor

Execution Diagram



tcpdump/libpcap backdoor

Hiding tracks!

- Modified libpcap doesn't report packets on port 1993
- Packages built on top of libpcap all effected
 - Snort, Bro, Ethereal, tcpdump

Other potential targets

Download.com (C|net)

Fileplanet.com

Tucows.com

Windows Update

Linux distributions

Protecting distros

Create a signature for the package, to make sure the contents are valid. Hard to make a new file with the same signature.

- RPM repository keys, PGP Signed copy, SHA1Sum
- Must make sure you don't get the signature from the same site you download from!
- (Skoudis text recommends MD5 which was broken two years ago)

Other methods

Plant your back door in the original source code somehow. (Possibly through an employee)

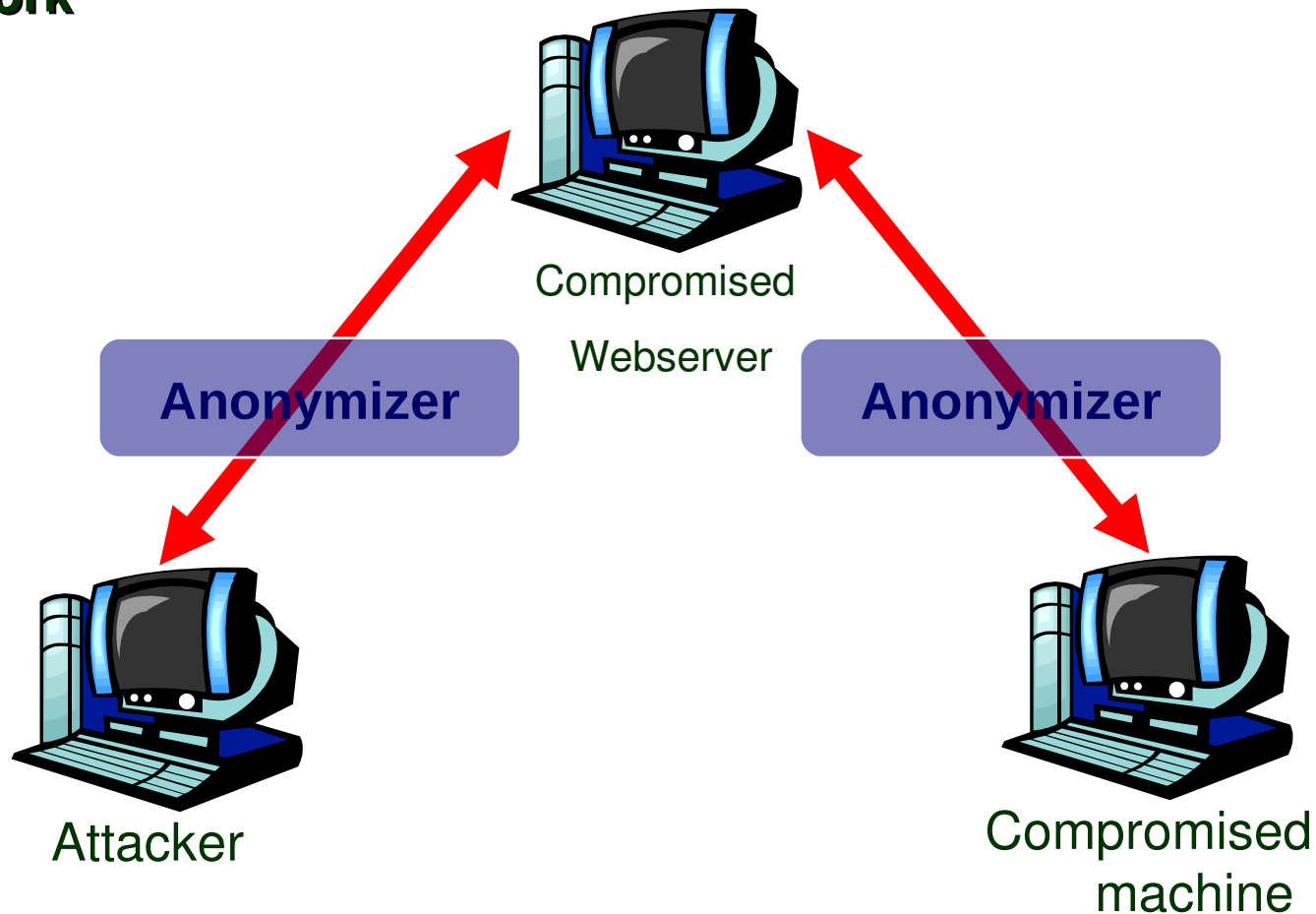
Ken Thomson's GCC hack discussed previously

Introduce an exploitable flaw. (like a buffer overflow!)

- **CMU Study: Programmers introduce between 100-150 defects per 1000 lines of code**
- **Windows XP: 45 Million lines of code**

Setiri

Win32 Trojan Horse Feb 2002 – a new spin on the Trojan principle
Coopts other processes (web browser/server) into doing it's dirty work



Anonymizers

Strip all headers, addresses, cookies, etc. to anonymize access

**Anonymizer.com, idMask, SamAir Resources,
Anonymity 4 Proxy, JAP, Megaproxy, The Cloak**

Used to hide attacker, and compromised victims!

Setiri

Makes a real, valid process do the malicious part (MSIE)

- Uses OLE to communicate with Internet Explorer
- Hard to detect subversion
- Hides communication paths
- Bypasses personal and network firewalls (outgoing port 80)

Communication to compromised web servers with a few new CGI scripts that implement commands

- Upload a file
- Download a file
- Execute a program

Compromised victim machines check for commands on compromised webservers

End of Trojans