K. J. Somaiya College of Engineering, Mumbai-77

(Autonomous College Affiliated to University of Mumbai)

Batch: B1 **Roll No.: 1711072**

Experiment / assignment / tutorial No. 8

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of the Staff In-charge with date

Title: Study of Malware creation, Scanning System for Malware, Removal of Malware.

AIM: To study and understand Malware creation, Scanning System for Malware, Removal of Malware.

Expected OUTCOME of Experiment:

CO 3: To learn servicing, maintenance and security of computer system

---

Books/ Journals/ Websites referred:

1. IBM- PC BY Govindrajalu, THM

Pre Lab/ Prior Concepts:

Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.Malware is defined by its malicious intent, acting against the requirements of the computer user — and so does not include software that causes unintentional harm due to some deficiency.

Malware creation:

1. Determine OS to be attacked

The most common target is Microsoft Windows, especially older versions. Many old Windows users do not update their operating system, leaving them vulnerable to security holes that may be fixed in newer versions.

2. Decide malware functionality

Executable file (.EXE, .BAT, .COM etc.) - This program needs to be run by the user, and is often disguised as something else, Macro (Microsoft Office) - Macros are programs that are embedded into a document or email. They target Word, Outlook, and other macro-enabled products. The most common method of delivery is via email with an infected document attached. Effects can range from nothing, to displaying a message, to deleting files, and much worse. Be aware that creating and spreading a malicious virus is a serious crime in most countries.

3. Start writing the malware script

Experiment as much as possible, and research ways to replicate your code depending on the language you are using. Research polymorphic code. This will alter the code of your virus every time it replicates, making it difficult to track with antivirus programs. Polymorphic code is fairly advanced, and is implemented differently in every language.

4. Research ways to hide your code.

Besides polymorphic coding, there are other ways to hide your virus. Encryption is a very common tool used by virus developers. It takes a lot of practice and reading, but it can go a long way in increasing the lifespan of the virus.

5. Test and release the malware script.

Once you have a prototype up and running, test it out on as many different machines and setups as possible. This will be easiest if you are able to set up virtual machines in different configurations. Make sure that you keep your tests contained so that you don't accidentally release your virus before you are ready. Put the test machines on an isolated network and see the effects of the virus spreading and finally the virus can be released.

Here, we have created a simple malware bat file (for Windows), which when executed, infinitely opens up Chrome Browser (which uses up GPU extensively) eventually crashing the entire system.

-> *window.bat*

```
@echo off

:here
        SET BROWSER=chrome.exe
        SET WAIT_TIME=0.5
        START %BROWSER% -new-window "website"
goto here
```

Scanning System for Malware:

These are general steps to scan and remove malware from your PC

1. Download and run the Microsoft Windows Malicious Software Removal Tool. This free, Microsoft provided malware removal tool won't find everything, but it will check for specific, "prevalent malware".

2. Update your antivirus/ anti-malware software installed on your computer. These regular updates tell your antivirus software how to find and remove the latest viruses from your PC. Definition updates usually happen automatically but not always.

3. Run a complete virus scan on your entire computer.
   If you happen to have another non-persistent (not always running) antimalware tool installed, like Malwarebytes, run that too when this is done. Don't simply run the default, quick system scan which may not include many important parts of your PC. Check that you're scanning every part of every single hard drive and other connected storage device on your computer. Specifically, make sure any virus scan includes the master boot record, boot sector, and any applications currently running in memory.

Removal of Malware:

1. Enter Safe mode.
   In this mode, only the minimum required programs and services are loaded. If any malware is set to load automatically when Windows starts, entering in this mode may prevent it from doing so. This is important because it can make removing the nefarious files easier since they’re not actually running or active.
2. Delete temporary files.
3. Download malware scanners.

They simply check for corrupted files or the file systems and for any unusual activity.

4. Run a malwarebyte scan script.
   This is basically an antivirus which scans for stray batch or bash files, checks for their ownership depending upon their date of creation and eventually classifies them as a malware script or not.

Conclusion: In this way, we have successfully created a malware along with finding a solution to remove this malware.

Post Lab Questions:

Explain spyware, rootkit, keyloggers, rogue security software, browser hijackers and backdoors.

Ans.

Spyware: It is software that "spies" on your computer. Nobody likes to be spied on, and your computer doesn't like it either. Spyware can capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information. If left unchecked, the software can transmit this data to another person's computer over the Internet.

Rootkit: A rootkit is a software program designed to provide a user with administrator access to a computer without being detected. Rootkits are are considered one of the most serious types of malware since they may be used to gain unauthorized access to remote systems and perform malicious operations. The name "rootkit" includes the word "root," because the goal of a rootkit is to gain root access to a computer. By logging in as the root user of a system, a hacker can perform nearly any operation he or she wishes. This includes installing software and deleting files. The word "kit" refers to the software files that make up the rootkit. These may include utilities, scripts, libraries, and other files.

Keyloggers: A keylogger is a program that records the keystrokes on a computer. It does this by monitoring a user's input and keeping a log of all keys that are pressed. The log may be saved to a file or even sent to another machine over a network or the Internet. Keylogger programs are often deemed spyware because they usually run without the user knowing it. They can be maliciously installed by hackers to spy on what a user is typing. By examining the keylog data, it may be possible to find private information

such as a username and password combination. Therefore, keyloggers can be a significant security risk if they are unknowingly installed on a computer.

Rogue security software: Rogue security software is malware that poses as anti-malware software, often in an attempt to install additional malware or solicit money for its fake services. The most common scam is for the software to alert the user to malware that doesn't exist, then charge them for a malware removal tool.

Browser hijackers: A browser hijacker is defined as a "form of unwanted software that modifies a web browser's settings without the user's permission." The result is the placement of unwanted advertising into the browser, and possibly the replacement of an existing home page or search page with the hijacker page. The idea is to make users visit certain websites whether they want to or not so the hijacker enjoys higher advertising revenue. Browser hijackers may also contain spyware to obtain banking information and other sensitive data.

Backdoors: A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device, or its embodiment, e.g. as part of a cryptosystem, an algorithm, a chipset, or a "homunculus computer" —a tiny computer-within-a-computer.

Date: 08/03/2019 **Signature of faculty in-charge**