FEDERAL UNIVERSITY OYE-EKITI, EKITI-STATE.

FACULTY

ENGINEERING

DEPARTMENT

COMPUTER ENGINEERING

COURSE CODE

CPE 413

COURSE TITLE

COMPUTER SECURITY TECHNIQUES

ASSIGNMENT

A GROUP PRESENTATON ON MALWARE PRESENTED BY GROUP 2

LECTURER IN CHARGE

DR.(ENGR.) BOLAJI OMODUNBI

NAME	MATRIC NUMBER
ADEYEMI SUNDAY OLUWASEYI	CPE/2018/1019
ADEYEYE ADEDOTUN EMMANUEL	CPE/2018/1020
ADIGUN AL MUBARAK	CPE/2018/1021
AFOLABI AYOMIDE SOLOMON	CPE/2018/1022
AJAYI AYOMIDE TIMOTHY	CPE/2018/1023
AJIBADE AYOMIDE ISREAL	CPE/2018/1024
AKINBOBOYE JOSHUA TOLULOPE	CPE/2018/1025
AKINDELE OLUWATOYIN OLUWAFIFUNMI	CPE/2018/1026
AKINLALU IYANUOLWA ROTIMI	CPE/2018/1027
AKINLOYE PELUMI MICHEAL	CPE/2018/ 1028
AKINLOYE PELUMI EMMANUEL	CPE/2018/1029
AKINMERESE AKINWALE MIRACLE	CPE/2018/1030
AKINYEMI TIMILEHIN DAVID	CPE/2018/1031
AKOMOLAFE AYOMIDE JOSHUA	CPE/2018/1032
AKOMOLAFE OLAOLUWA DAVID	CPE/2018/1033
AKUBOR SAMUEL TOLUWANI	CPE/2018/1034
ALADE TUNDE ADEWUNMI	CPE/2018/1035
ALADELOYE JOSHUA ADEYANJU	CPE/2018/1036

Table of contents

- **Introduction to malware**
- **Different types of malware and how each one of them spread**
- **More recent examples of malware**
- **Differences between Viruses, Worms and Trojan horse**
- **Preventive measure for avoiding malware**
- **Handling and cure for malware**

Introduction To Malware

Malware, short for “malicious software,” includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.

Malware carries out many of the cyberattacks on the Internet, including nation-state cyber-war, cybercrime, fraud and scams. For example, Trojans can introduce a backdoor access to a government network to allow nation-state attackers to steal classified information. Ran-somware can encrypt data on a user’s computer and thus making it unaccessible to the user,and only decrypt the data after the user pays a sum of money. Botnet malware is responsible for many of the Distributed Denial-of-Service (DDoS) attacks as well as spam and phishing activities. We need to study the techniques behind malware development and deployment innorder to better understand cyberattacks and develop the appropriate countermeasures. As the political and financial stakes become higher, the sophistication and robustness of both the cyber defence mechanisms and the malware technologies and operation models have also increased. For example, attackers now use various obfuscation techniques such as packing and polymorphism as well as metamorphism to evade malware detection systems, and they set up adaptive network infrastructures on the Internet to support malware updates, command-and-control, and other logistics such as transits of stolen data. In short, it is becoming more important but also more challenging to study malware.

Different Types Of Malware And How Each One Of Them Spread

1) **Adware**

   Adware — commonly called "spam" — serves unwanted or malicious advertising. While relatively harmless, it can be irritating as adware can hamper your computer's performance. In addition, these ads may lead users to download more harmful types of malware inadvertently. To defend against adware, make sure you keep your operating system, web browser, and email clients updated so they can block known adware attacks before they are able to download and install.

How Does Adware Spreads

Adware usually spreads in one of the two ways:

- **Users could download a free program online that they don't know contains adware.**
- **Users go to websites infected with adware that takes advantage of vulnerabilities within browsers, downloading adware in files.**

2) **Viruses**

   A computer virus is a type of malware that attaches to another program (like a document), which can replicate and spread after a person first runs it on their system. For instance, you could receive an email with a malicious attachment, open the file unknowingly, and then the computer virus runs on your computer. Viruses are harmful and can destroy data, slow down system resources, and log keystrokes.

   Examples of computer virus include; boot sector virus, web scripting virus, resident virus, browser hijacker, direct action virus, macro virus.

How Does Viruses Spread

Viruses may spread as different form such as images, programs, .exe file, word documents, and other file types. Below are the most common ways through which computer viruses spread on your computer:

- **Through downloading of free software**
- **Through downloading of suspicious E-Mail attachments**
- **Clicking on phishing emails**
- **Use of external devices**
- **Clicking on online advertisements**
- **Clicking on malicious file**
- **Visiting Infected Website**
- **Copying data from infected computer**
- **Unsolicited e-Mail**
- **Social Media scam links**

3) Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue.

Examples of computer worms include; email worms, file sharing worms, crypto worms, instant messaging worms, internet worms

How Does Worms Spread

Computer worms spread via replication

The computer worms spread by replicating themselves and making them a somewhat unstoppable computer virus. By replicating, it can do more damage in a short space of time and result in multiple infected computers.

4) Trojans

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.

Example of Trojans include : Remote Access Trojans (RATs), Backdoor Trojans(backdoors), IRC Trojans (IRCbots), Keylogging Trojans.

How Does Trojans Spread

Before a Trojan horse program can attack, it must first find a way to entice the victim to copy, download, and run it. Since few people knowingly run a malicious program, Trojan horses must disguise themselves as other programs that the victim believes to be harmless (such as games, utilities, or popular applications).

Besides disguising themselves as harmless programs, Trojan horses can also disguise themselves inside a legitimate program, such as Adobe Photoshop or Microsoft Excel. To do this, malicious hackers have created special wrapper or binder programs with names like Saran Wrap, Silk Rope, or The Joiner, which can package any Trojan horse inside another program, thereby reducing the likelihood that someone will discover it. Since most users won't suspect that a program from a large, well-known publisher would contain a Trojan horse, the victim is likely to run the linked program containing the Trojan horse.

Once someone has written a Trojan horse, the next step is to spread it by copying it onto a victim's computer, posting it on a website for others to download, sending it as a file attachment via email, distributing it through IRC and online service chat rooms, or sending it through ICQ and other instant messaging services.

5) Spyware

Spyware is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission. Spyware is a kind of malware that secretly gathers

information about a person or organization and relays this data to other parties

Once spyware infiltrates the computer, it can carry out a host of actions, including:

- **Running an application that generates numerous pop-up ads, which can negatively effect the usability of your browser**
- **Re-directing your Internet searches as it sees fit, effectively rendering your search engines useless**
- **Recording your actions such as clicks, searches, and in particularly malicious situations, your account logins and credit card information**
- **Changing your firewall settings to allow more malicious software in**
- **Recognizing and blocking attempts to remove it**

Examples of spyware include : keyloggers, adware, infostealer.

How Does Spyware Spread

Spyware can spread into the computer in a variety of ways through

- **hiding within malicious pop-ups,**
- **software downloads,**
- **email attachments,**
- **pirated movies/music.**

6) Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
Examples of phishing attacks includes: Spear phishing, whaling, vishing, email Phishing

How does Phishing spread

Phishing generally spreads through E-mails.

7) Ransomware

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. Examples of ransormware includes: CryptoLocker, CryptoWall, Locky, and TeslaCrypt

How does ransomware spread

- **Email attachments**
- **Malicious URLs.**
- **Remote desktop protocol**
- **Pirated software**
- **Removeable devices**

More Recent Examples Of Malware

1) Clop ransomware

An especially damaging new threat, clop ransomware can disable Windows' built-in security safeguards, including Windows Defender and Microsoft

Security Essentials, along with over 600 other processes that might serve to stop it. Cybercriminals can deploy this malware to infect individuals or entire networks, making it exceedingly dangerous if a company network is infiltrated. Like other types of ransomware, clop encrypts all files on a computer and demands a fee to have it decrypted.

2) Ransomware as a Service (RaaS)

Service-based ransomware has made dangerous and sophisticated malware publicly available for anyone to use. With RaaS, anyone who wants to attack someone else can hire a team of professional hackers to do it for them.

3) Cryptojacking

A type of malware specific to cryptocurrency, cryptojacking allows someone to mine for cryptocurrencies without the need for common hardware that is

both exceedingly expensive and difficult to maintain, as it requires huge amounts of electricity to function. It can be installed on phones and computers, which are used as tools for cryptocurrency mining. The cryptocurrency is then placed in a cybercriminal's crypto-wallet.

4) Internet of Things (IoT) device attacks

This kind of malware targets devices that typically have little security, such as smart devices, including speakers, doorbells and cameras. After infecting a device, a cybercriminal can gain access to any data that is collected and stored on the device, which might include passwords, home security information and microphone audio.

5) Windows OS update ransomware

This is malware disguised as a Windows update. While not particularly sophisticated, this type of malware spreads via email and requests that the user install a critical Windows update with a provided .exe file. This file opens the door for cybercriminals to install ransomware.

6) Zeus Gameover

An especially dangerous trojan-style virus, Zeus Gameover attempts to steal financial information to drain bank accounts. What makes Zeus Gameover special is the way it operates makes it almost impossible to trace. The malware will bypass centralized servers and create its own independent servers to share its data with cybercriminals, meaning stolen information can't be retrieved or the source of the threat located.

7) News malware

By posing as trending news, this malware encourages users to click its links to learn more. Clicking the link doesn't lead to news, but instead makes the system vulnerable to attack by installing malware. Typically, this malware copies data on the infected computer to steal information.

Differences Between Viruses, Worms, And Trojan Horse

S/N	Viruses	Worms	Trojan Horse
1.	Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
2.	Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
3.	Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility software.
4.	Virus replicates itself	Worms can also replicates itself	But Trojan horse does not replicate itself.
5.	The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.

Preventive Measures For Avoiding Malware

There are no ways to prevent malware attacks but there are reliable ways to detect and block malware attacks, thus protecting your systems from being infected by malicious software.

1. Install anti-virus and anti-spyware software.

Anti-virus and anti-spyware programs scan computer files to identify and remove malware. Be sure to:

- **Keep your security tools updated.**
- **Immediately remove detected malware.**
- **Audit your files for missing data, errors, and unauthorized additions.**

2. Use secure authentication methods.

The following best practices help keep accounts safe:

- **Require strong passwords with at least eight characters, including an uppercase letter, a lowercase letter, a number and a symbol in each password.**
- **Enable multi-factor authentication, such as a PIN or security questions in addition to a password.**
- **Use biometric tools like fingerprints, voiceprints, facial recognition and iris scans.**
- **Never save passwords on a computer or network. Use a secure password manager if needed.**

3. Use administrator accounts only when absolutely necessary.
Malware often has the same privileges as the active user. Non-administrator accounts are usually blocked from accessing the most sensitive parts of a computer or network system. Therefore:

- **Avoid using administrative privileges to browse the web or check email.**
- **Log in as an administrator only to perform administrative tasks, such as to make configuration changes.**
- **Install software using administrator credentials only after you have validated that the software is legitimate and secure.**

4. Keep software updated.

No software package is completely safe against malware. However, software vendors regularly provide patches and updates to close whatever new vulnerabilities show up. As a best practice, validate and install all new software patches:

- **Regularly update your operating systems, software tools, browsers and plug-ins.**
- **Implement routine maintenance to ensure all software is current and check for signs of malware in log reports.**

5. Control access to systems.

There are multiple ways to regulate your networks to protect against data breaches:

- **Install or implement a firewall, intrusion detection system (IDS) and intrusion prevention system (IPS).**
- **Never use unfamiliar remote drives or media that was used on a publicly accessible device.**
- **Close unused ports and disable unused protocols.**
- **Remove inactive user accounts.**
- **Carefully read all licensing agreements before installing software.**

6. Limit application privileges.

A hacker only needs an open door to infiltrate your business. Limit the number of possible entryways by restricting application privileges on your devices. Allow only the application features and functions that are absolutely necessary to get work done.

7. Implement email security and spam protection.

Email is an essential business communication tool, but it's also a common malware channel. To reduce the risk of infection:

- **Scan all incoming email messages, including attachments, for malware.**
- **Set spam filters to reduce unwanted emails.**
- **Limit user access to only company-approved links, messages and email addresses.**

8. Monitor for suspicious activity.

Monitor all user accounts for suspicious activity. This includes:

- **Logging all incoming and outgoing traffic**
- **Baselining normal user activity and proactively looking for aberrations**
- **Investigating unusual actions promptly**

10. Educate your users.

At the end of the day, people are the best line of defense. By continually educating users, you can help reduce the risk that they will be tricked by phishing or other tactics and accidentally introduce malware into your network. In particular:

- **Build awareness of common malware attacks.**
- **Keep users up to date on basic cybersecurity trends and best practices.**
- **Teach users how to recognize credible sites and what to do if they stumble onto a suspicious one.**
- **Encourage users to report unusual system behavior.**
- **Advise users to only join secure networks and to use VPNs when working outside the office.**

Handling And Cure For Malware

Steps In Handling Malware

1. **Detection and Identification**

   Determine fully if a malware outbreak has occurred.

- **The objective of this step is to determine whether a malware outbreak has occurred. Typical indications of a malware outbreak include any or all the following:**
- **Users complain of slow access to the Internet, exhaustion of system resources, slow disk access, or slow system boots.**
- **A number of alerts have been generated by a Host-based Intrusion Detection System (HIDS), or by anti-malware software.**
- **There is significantly increased network usage.**
- **A number of access violation entries have been noticed in perimeter router logs or firewall logs.**

Upon discovery of any of the above symptoms, IT staff should immediately check and validate all suspicious activity to determine if an outbreak has occurred. Once it is confirmed that this is a malware security breach, it is important to collect information about the malware, as this will be essential for the containment and eradication process. Information about the malware can be obtained from anti-malware software vendors' websites if the malware has been around for some time, by reviewing alerts from anti-malware software, by examining firewall and router log files. The following questions can help identify the characteristics of the malware:

- **What kind of malware is it (Network worm, mass-mailing worm, virus, or Trojan Horse etc.)?**
- **How does the malware propagate (By attacking vulnerable network service? By mass mailing?)?**
- **If the malware propagates by attacking vulnerable service, what is the vulnerability being exploited? Has a patch for addressing the vulnerability been released? What are the services or ports that are being attacked?**
- **Does the malware plant backdoors on the infected system?**

- **How can the malware be removed from the affected system? Are there any removal tools available?**

2. **Escalation**

   The second is to notify all appropriate parties and escalate the incident to the appropriate level following a predefined escalation procedure. The information provided during the escalation process should be clear, concise, accurate and factual. Providing inaccurate, misleading or incomplete information may hinder the response process or may even worsen the situation. It is crucial to bear in mind that information about incident should be disclosed only on a need to know basis.

3. Containment

The third step of response to a malware incident is containment. The following are activities that should be carried out in the containment stage:

- **Identify infected systems**
- **Contain the outbreak**
- **Keep records of all actions taken**

4. **Eradication**

   Eradicating a malware outbreak should be designed to remove the malware from all infected systems and media, and rectify the cause of the infection. Prior to carrying out the eradication process, it is advisable to collect all necessary information, including all log files, which may have to be deleted or reset during the clean up process, which will be useful in subsequent investigations. Anti-malware scanning software and removal tools are commonly used as the primary means of eradication.

5. **Recovery**

Clearly, the main purpose of the recovery step is to restore all systems to normal operation. In a malware outbreak, recovering the functionality and data of infected systems may have already been carried as part of the eradication process. Apart from restoring the infected systems, removing any temporary containment measures, such suspended network connections, is another main aspect of the recovery process. Prior to removal of the containment measures, one important step is a pre-production security risk assessment to ensure that no infection is detected, and that the cause of the original infection is rectified.

Cure For Malware

- **Download and install antivirus software**
- **Run a virus scan**
- **Delete or quarantine infected files.**
- **Restart your computer**