UNIVERSITY OF MINES AND TECHNOLOGY
TARKWA

FACULTY OF COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

REPORT ON FALSE WARNING ABOUT COMPUTER MALWARE

BY

GROUP 9
LECTURER: Dr. ERIC AFFUM

Declaration

We declare that this work has not been presented for any examination or degree in any other University.

NAME	SIGNATURES
Erzoah Gaius Junior	
Avornyoh Samuel Obeng	
Okyere Victor	
Biri Ebenezer	
Nana Amankwah Boateng	
Rexford Acquah	
Ankorah Jonas K.M.B	
Asante Bernice Antwiwaa	
Wireko Eugget Nyarko	
Quayson Cornelius	

..... day of ..... (year) .....

Abstract

This practical experience aimed to equip third-year BSc. Computer Science and Engineering students with the skills to identify threats and safeguard their computers against viruses and malware infections. The project work took place from July 1st to July 8th, 2024, providing students with valuable insights into various technologies for threat detection and protection using Antivirus softwares such as Avira.

Acknowledgment

We want to extend our heartfelt gratitude to the Almighty for His unwavering protection and guidance throughout this practical process. We would also like to express our sincere appreciation to Dr. ERIC AFFUM, for the invaluable tutorials and insights provided prior to the practical work. Special thanks are due to the members of Group 9 for their collaborative ideas and unwavering support during the installation of application and testing.

Contents

List of Figures

Task 1

1. **Virus**
   A type of malicious software program (malware) that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Viruses can cause various types of damage, such as corrupting or deleting data, spreading to other systems, and more.

2. **Worm**
   A standalone malware computer program that replicates itself in order to spread into other computers. Unlike a computer virus, it does not need to attach itself to an existing program. Worms often use network connections to spread and can cause harm by consuming bandwidth, overloading systems, or delivering additional payloads, such as viruses or other malware.

3. **Trojan Horse**
   A type of malware that is disguised as legitimate software. Users are typically tricked into loading and executing it on their systems. Once activated, Trojans can perform a variety of malicious actions, such as stealing data, damaging systems, or creating backdoors for other malware to enter.

4. **Spyware**
   A type of malware that secretly observes the user's activities without permission and sends the collected information to a third party. Spyware can monitor and collect various types of data, such as keystrokes, screen captures, and login credentials, often leading to privacy breaches and identity theft.

Task 2

ANTIVIRUS SOFTWARE INSTALLATION

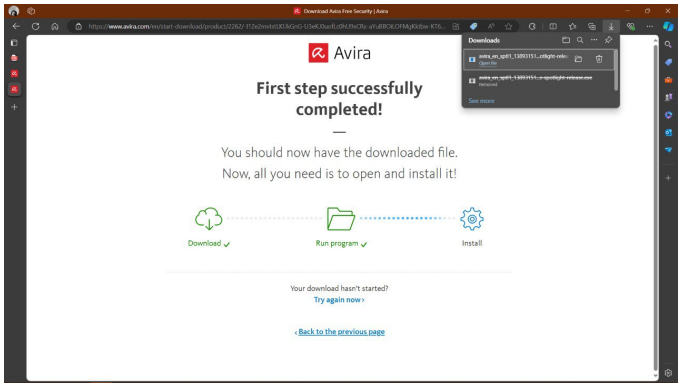
1. Open your web browser and go to the official website of Avira antivirus software to download `https://www.avira.com`

Figure 1: Avira Homepage

2. Before installing Avira Antivirus ensure your operating system is up to date by checking for updates via the "Settings" menu.Uninstalled previous antivirus software to prevent any conflicts during installation.

3. Download and run the (avastfreeantivirussetuponline.exe) installer using the download link provided.

4. Launch and accept the End User License Agreement (EULA) after reading through it.Choose the "Default Installation" option to keep things simple



and let Avira install to the default location on your C: drive.The installation process will take a few minutes as Avira Antivirus copies files and configured settings.

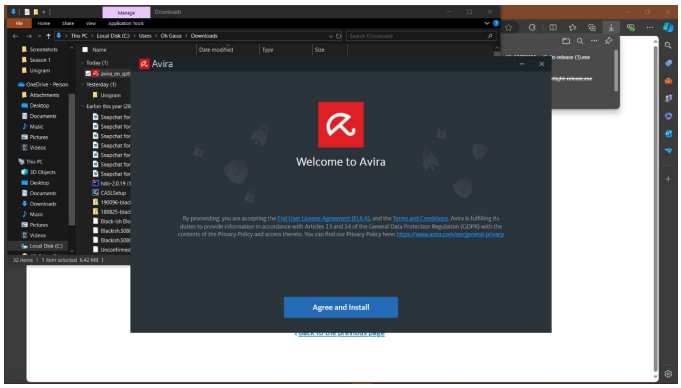


Figure 2: Avira Installation

5. Avira Antivirus automatically checks for updates whiles installing to ensure it has the latest virus definitions in the application.The update process is quick and takes only a couple of minutes to complete.

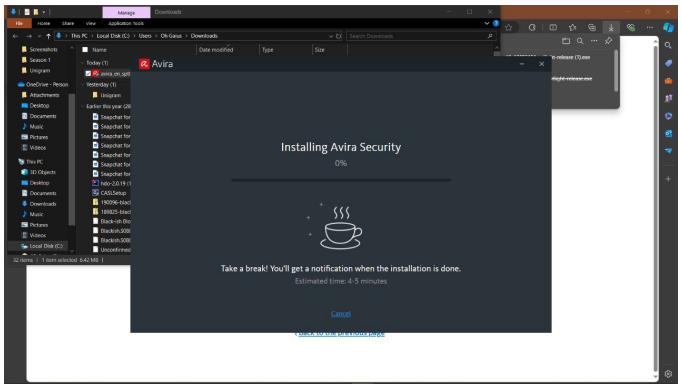


Figure 3: Running Avira Update

6. Run Avira scan to check your pc against malware.

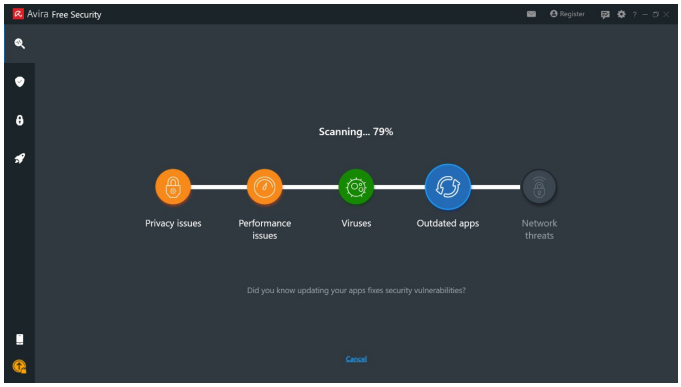


Figure 4: Scanning for malware

Task 3

SPYWARE SOFTWARE INSTALLATION

1. Visit the official Spybot website `https://www.safer-networking.org`.On the homepage, click on Spybot Search and Destroy under the "Products" section.Download the free version of the installer using the link and save file to my "Downloads" folder.

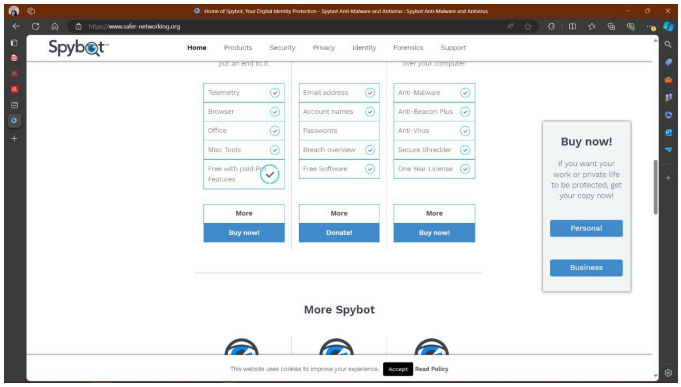


Figure 5: Spybot Homepage

2. Located the downloaded installer file named spybotsd-setup.exe in my "Downloads" folder.To avoid any interruptions, temporarily disable your current antivirus software.

3. Run the installer and follow the prompts to install the software successfully.

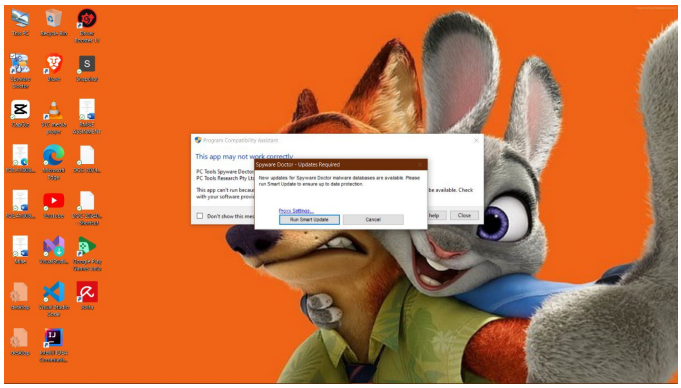


Figure 6: Spybot installation

4. Run spybot after installation.

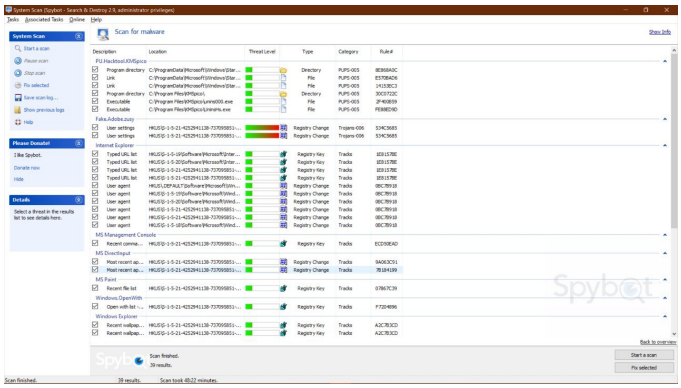


Figure 7: Running Spybot

Task 4

VIRUS AND HOAX EMAIL SERVICES

Message That a Threat is a Hoax

Dear Team,

I hope this message finds you well. It has come to our attention that there is a circulating email warning about a new virus threat. After thorough investigation, we have determined that this email is a hoax.

Here are some tips to help you determine if future messages are real or fake:

1. Verify the Source: Always check the sender's email address and ensure it matches the official domain of the supposed sender.
2. Look for Red Flags: Be wary of urgent language, requests for personal information, or prompts to click on unfamiliar links.
3. Check for Errors: Many hoax emails contain spelling and grammatical errors.
4. Cross-Reference: Search online for keywords from the email along with the word "hoax" to see if others have reported it.
5. Consult IT: If you are unsure about an email, do not hesitate to contact the IT department for verification.

By staying vigilant and following these steps, we can protect ourselves from potential scams and misinformation.

Best regards,
Erzoah Gaius Junior
Executive Manager
(0533876110)

Message That a Threat is a Real

Dear Team,

I hope this message finds you well. My name is Erzoah Gaius Junior and I am your IT Specialist. We have recently been alerted to a serious virus threat

that could potentially compromise our network security. This threat has been confirmed by [Source of Information], and it is crucial that we take immediate action to protect ourselves.
Warning The virus in question is nicknamed "THE END" and it can spread through email attachments and malicious links. It has the capability to steal sensitive information and disrupt our systems.
Steps to Protect Yourself:

1. Do Not Open Suspicious Emails: Be cautious of emails from unknown senders, especially those with attachments or links.

2. Update Your Software: Ensure your antivirus software is up to date. Our IT team has pushed the latest updates, but please verify that your systems are running the latest versions.

3. Report Suspicious Activity: If you receive a suspicious email or notice unusual activity on your device, report it immediately to the IT department.

4. Practice Safe Browsing: Avoid visiting untrusted websites and refrain from downloading software from unreliable sources.

For more detailed information on this threat and how to safeguard your data, please refer to the following resources:
Email of IT Specialist:`jerzo204@gmail.com`
Contact: 0509894360
Your cooperation and vigilance are critical in keeping our organization secure. If you have any questions or need further assistance, please do not hesitate to reach out.
Stay safe,
Erzoah Gaius Junior
IT Specialist
0509884360

Task 5

Practical Implementation

Threats that were found after performing scan

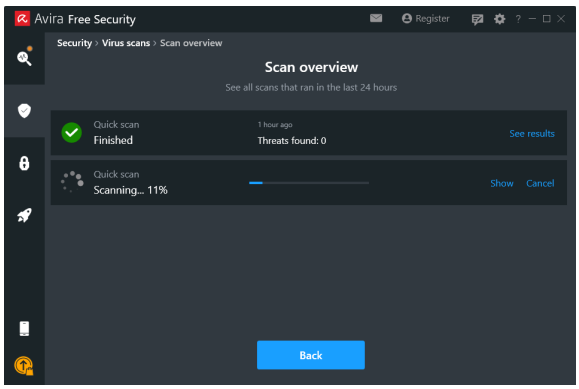


Figure 8: Scanning for Threats

1. Threat Type: Trojan
   Location: `C:\ProgramData\AvastSvcXoF\AvastAuth.dat`
   Severity: High
   Action Taken: Quarantined and deleted by antivirus software.

2. Threat:Available space to free up
   Severity:Medium
   Action:Cleared unused space

IMPORTANCE OF KEEPING ANTIVIRUS AND SPYWARE SOFTWARE UPDATED

The number viruses and spyware are on the rise everyday therefore it is our duty to keep up with it. Our software therefore has to be up to date so as to keep up with the fast pace growth of the viruses. This will help keep our machines safe from the harm viruses and spyware.

SCHEDULE FOR REGULAR SCANS AND UPDATES

1. Scans and updates should be done at least once a week
2. After an external device has been inserted and data or information has been fetched from it
3. After a new software has been installed

EFECTIVENESS OF THE INSTALLED SOFTWARES

The software requires a premium to be more effective. The free versions (which we used) wasn't as effective as would be needed.