**Evaluation-1**

**Agenda:**

1. Problem Statement
2. Aim of the Project
3. Introduction to Malware

* Definition
* Types of Malwares
* How malware penetrates into the system?
* How to detect a malware?
* Web Attacks

1. Algorithm
2. Flow Chart
3. How an Anti-Virus software works?

* Definition
* Working Concept

1. Our Approach

* Malware Analysis
* Concept of Signatures
* Malware Attacking Techniques (Static and Dynamic)
* General Rules for analyzing a malware

1. The Malware Analyzer- (The Tool)

* Introduction to the Tool
* Description
* How tool works? (Algorithm)
* Capabilities of the tool
* Installation process
* GitHub Link

9.References

1. **Problem Statement:**

Over the past two decades, the Internet has evolved from something of a novelty to a tool most of us heavily rely upon every single day. The Internet has completely changed the way we do things, from how we work to how we communicate, socialize, shop and learn. When we think about how much we depend on the Internet in our daily lives, it's hard to imagine life without it There are an abundance of Trojan horses, bots, adware, ransomware, macro viruses, ransomware, spyware, worms and phishing attacks that target Internet users every day.

If a user got attacked then listed below are some techniques so that he can get rid off from the malware.

* **Disconnect**

If you're a victim of a crimeware attack you should disconnect from the Internet immediately. If you're connected via Wi-Fi, phone or Ethernet cable, you need to disable the connection as soon as possible to prevent data being transmitted to the criminal.

* **Scan your Device**

It's good practice to have antivirus software, such as Norton™ Anti-Virus or Norton™ Internet Security, installed and up-to-date in case this kind of incident occurs

* **Create a backup**

It's good practice to create regular backups of your files and folders. While the aim of crimeware is largely to steal information or data, there's a good chance that files may be lost or destroyed during the recovery process.

* **Reinstall your operating system**

Depending on the severity of the attack, it might be necessary to reinstall the operating system of your computer. Some threats are very sophisticated and can hide deep in the system using rootkit techniques, meaning they'll go unnoticed by antivirus software.

So eventually the problem is that how to get rid off from malware.

1. **Aim of the project:**

* We are going to make a Malware Analyzer.
* It will work on Python Programing.
* It will analyze the file using signatures based technique and prepare a PE file.

1. **Introduction to Malware**

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

**3.1 Where does malware come from?**

Some of the most common sources of malware are email attachments, malicious websites, torrents, and shared networks.

1. **Phishing** – Emails can be disguised to be coming from a fraudulent company for the sole purpose of getting you to reveal personal information
2. **Malicious Websites** – Some websites may attempt to install malware onto your computer, usually through popups or malicious links

**3.2 Types of Malwares**

1. **Virus:**

Possibly the most common type of malware, viruses attach their malicious code to clean code and wait for an unsuspecting user or an automated process to execute them. Like a biological virus, they can spread quickly and widely, causing damage to the core functionality of systems.

1. **Worm:**

Worms get their name from the way they infect systems. Starting from one infected machine, they weave their way through the network, connecting to consecutive machines in order to continue the spread of infection.

1. **Trojans**:

A Trojan (or Trojan Horse) disguises itself as legitimate software with the purpose of tricking you into executing malicious software on your computer.

### **Spyware**:

Spyware invades your computer and attempts to steal your personal information such as credit card or banking information, web browsing data, and passwords to various accounts.

### **V) Adware**:

Adware is unwanted software that displays advertisements on your screen. Adware collects personal information from you to serve you with more personalized ads.

**VI) Rootkits**:

Rootkits enable unauthorized users to gain access to your computer without being detected.

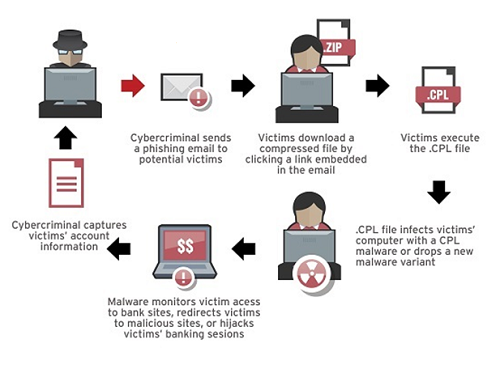
### **3.3 How Malware attacks?**

### **Examples of Malware Attacks**

Here are just a few of the many types of malware cyber attackers use to target sensitive data:

* [**Pony malware**](https://www.cyberark.com/threat-research-blog/a-pony-hidden-in-your-secret-garden/) is the most commonly used malware for stealing passwords and credentials. It is sometimes referred to as Pony Stealer, Pony Loader or fare IT. Pony malware targets Windows machines and collects information about the system and the users connected to it. It can be used to download other malware or to steal credentials and send them to the command and control the server.
* [**Loki**](https://www.cyberark.com/threat-research-blog/loki-number-seven-loki-malware-keeps-stealing-your-credentials/), or Loki-Bot, is an information-stealing malware that targets credentials and passwords across approximately 80 programs, including all known browsers, email clients, remote control programs and file sharing programs. It has been used by cyber attackers since 2016 and continues to be a popular method for stealing credentials and accessing personal data.
* [**Krypton Stealer**](https://www.cyberark.com/threat-research-blog/krypton-stealer-kryptonite-for-credentials/) first appeared in early 2019 and is sold on foreign forums as malware-as-a-service (MAAS) for just $100 in cryptocurrency. It targets Windows machines running version 7 and above and steals credentials without the need for admin permissions. The malware also targets credit card numbers and other sensitive data stored in browsers, such as browsing history, auto-completion, download lists, cookies and search history.
* [Triton malware](https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/) crippled operations at a critical infrastructure facility in the Middle East in 2017 in one of the first recorded malware attacks of its kind. These systems are used to shut down operations in nuclear facilities, oil and gas plants in the event of a problem, such as equipment failure, explosions or fire. The Triton malware is designed to disable these failsafe mechanisms, which could lead to physical attacks on critical infrastructure and potential human harm.

## 3.4 Basic idea of how malware attacks the system



## How do you detect malware?

## Popup ads start popping up everywhere.

## Your browser keeps getting redirected.

## An unknown app sends scary warnings.

## Mysterious posts appear on your social media.

## You get ransom demands.

## Your system tools are disabled.

## 3.5) STAGES OF WEB ATTACKS

1. **ENTRY**:

The first part of an attack involves a drive-by download from an entry point, either a hijacked website or an email that contains a malicious link. Drive-by downloads A drive-by download is the process of inadvertently downloading malicious web code simply by visiting a web page. A drive-by download happens automatically and without the user knowing.

* 1. How trusted websites get hijacked

Web servers like Apache and IIS, as well as their content management systems, have vulnerabilities. Hackers uses website exploit tools can attack these vulnerabilities to inject malicious code into web pages. Some campaigns, such as Dark-leech for example, have been active for several years. As the exploit kit landscape changes, the underlying traffic redirection tools simply change as necessary.

1. **TRAFFIC DISTRIBUTION:**

Once a drive-by download has reached the browser, the unsuspecting user is redirected to an exploit kit. However, rather than sending users to known exploit kit hosting sites, elaborate traffic distribution systems (TDS) create multiple redirections that are nearly impossible to track and therefore black-list.

1. **EXPLOITATION:**

The next phase of a modern web attack is the downloading of an exploit pack from the malware hosting site. These kits execute a large number of exploits against vulnerabilities in web browsers and associated plugins such as Flash, Silverlight, and Java. Once a user’s browser has landed on a site hosting the Angler exploit kit, it will load files that target vulnerabilities relevant to the victim’s computer based on information readily available from the browser. Once a user’s browser has landed on a site hosting the Blackhole exploit kit, it will load files that target vulnerabilities relevant to the victim’s computer based on information readily available from the browser.

**3.5.1) Four types of files are often used to exploit vulnerabilities in the user’s system:**

1. **Java**: JAR files with either JavaScript or applet code are usually the most successful at finding an exploit.
2. **HTML/JS/VBS**: Runtime code can be downloaded to target a vulnerability in Microsoft Help and Support Center.
3. **PDF**: PDF files with embedded JavaScript attempt to exploit known vulnerabilities in Adobe Reader.
4. **Flash:** Two types of flash files with specially designed code are often loaded to exploit Adobe Flash Player.
5. **INFECTION:**

Once the attacker exploits an application vulnerability to gain some control over the computer, the next step in the attack is to download a malicious payload to infect the system. The payload is the actual malware or virus that will ultimately steal data or extort money from the user.  
**3.6) Difference between Malware and a virus:**

1. **Malware :**

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user’s permission. Malware includes worms, Trojan horses, ransomware, spyware and other malicious programs.

**2.Virus :**

A virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.

## 4) Algorithm of Malware

**Step 1: Initiation of the Attack**

This first stage is where the attacker sets up the ransomware to infiltrate your system. This can be done in several ways such as sending out phishing email attacks, setting up malicious websites, exploiting weaknesses in RDP connections, or attacking software vulnerabilities directly.

**Step 2: Instantiation**

The second stage occurs once the ransomware has infiltrated your system. The malicious code will set up a communication line back to the attacker. The ransomware attacker may download additional malware using this communication line. At this point, the ransomware may lay hidden and dormant for days, weeks, or months before the attacker chooses to initiate the attack.

**Step 3: Activation**

The third stage is when the attacker activates, or executes, the ransomware attack remotely. This can happen at any time the attacker chooses and catch your organization completely off guard. Once the attack has begun, it can be a race against time for your organization to even identify that the attack is occurring so that mitigation and recovery efforts may go into action.

**Step 4 – Encryption**

Ransomware holds data hostage through encryption (or in some cases a lock screen but encryption is most likely in a corporate attack.) Different ransomware variants use different encryption methods which range from encrypting the master boot record of a file system to encrypting individual files or entire virtual machines. Ransomware that also targets backup systems may delete or encrypt the backups to prevent recovery.

**Step 5 – Ransom Request**

In this stage, you’re officially the victim and the ransomware has encrypted data. You’re presented with information on how to pay a ransom via a cryptocurrency transaction. Depending on what data the ransomware was able to encrypt, not only will data be inaccessible, but applications and entire systems can be disabled by the encryption.

**Stage 6 – Recovery or Ransom**

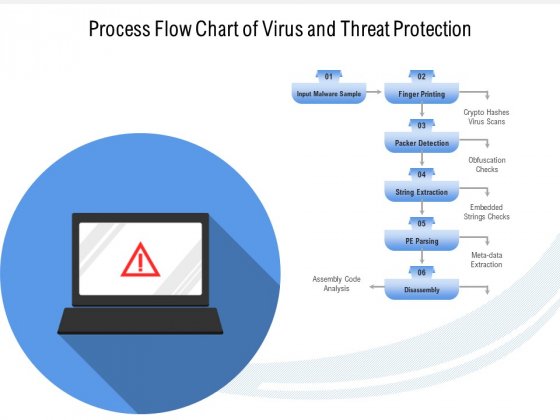
This is the stage where many of the organizations we’ve seen in the news experienced impacts of significant downtime or disruption and many have chosen to pay a ransom as a result. Without an effective recovery method, even if the data can be recovered, at least partially, the cost of doing so may exceed the cost of paying the ransom.

**Stage 7 – Clean Up**

Paying a ransom or even recovering data from a backup or replica does not necessarily eliminate the ransomware on the system. The malicious files and code may still be present and need to be removed. The attack itself will likely reveal the type of ransomware and make it easier to locate and purge from the system. If necessary, systems can be recovered in an isolated network to clean up the malware without risking re-activation.

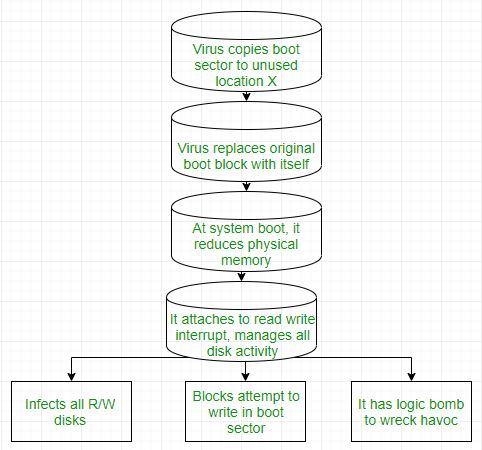
**5) FLOW CHART**

**5.1) Malware Analysis (FLOW CHART)**



## 5.1.1

**5.2.2**



## 6) How antivirus works?

Antivirus software scans a file, program, or an application and compares a specific set of code with information stored in its database. If it finds code that is identical or similar to a piece of known malware in the database, that code is considered malware and is quarantined or removed.Each antivirus functions differently based on the set of features they are developed with. Ideally, the following characters and features are essential to help the users stay ahead of threats.

**6.1.1) There are some techniques on which antivirus algorithm works:**

1. **Signature-based detection** - This is most basic in any traditional antivirus programming that checks each .EXE document and approves it with the known infections of the database and different sorts of malware. Or, on the other hand, it checks if the obscure executable document malfunctions, which denotes signs of infections.
2. **Heuristic-based detection** – The heuristic-based detection generally works better in combination with signature-based detection. Both Heuristic and signature-based detection, when combined, make the antivirus more effective. The Heuristic-based detection has been most used in all the antivirus software. This causes the antivirus programming to recognize new or a variation of an adjusted rendition of malware, even without the most recent infection definitions
3. **Behavioral-based recognition** - This type of recognition is utilized as a part of Intrusion Detection component. This is more biased in recognizing the attributes and traits of the malware during the process of execution. This method functions well to identify malware only when there is malicious performance.
4. **Sandbox recognition** - It works destined to that of behavioral-based identification strategy. It executes any applications in the virtual condition to track the type of activities it performs. Confirming the activities of the application/program when signed in, the antivirus programming can distinguish if the program is malevolent or not.
5. **Data mining strategies** - This is one of the most recent patterns in recognizing a malware. With an arrangement of the traits of a program, Data mining finds if the file or an application is a malware.

**7) Our Approach**

**7.1) Malware Analysis**

Information required to respond to a network intrusion:

* + Exactly what happened?
  + Ensure you’ve located all infected machines and files
  + How to measure and contain the damage
  + Find signatures for intrusion detection systems

**7.2) What are Signatures?**

A virus signature is a continuous sequence of bytes that is common for a certain malware sample. That means it’s contained within the malware or the infected file and not in unaffected files.

**: This is how a Signature look like after analyzation:**

**5.2.1) Types of Signatures**

**7.2.1) Types of Signatures**

**•** **Host-based signatures:**

– Identify files or registry keys on a victim computer that indicate an infection

– Focus on what the malware did to the system, not the malware itself

* **Network signatures**:

– Detect malware by analyzing network traffic

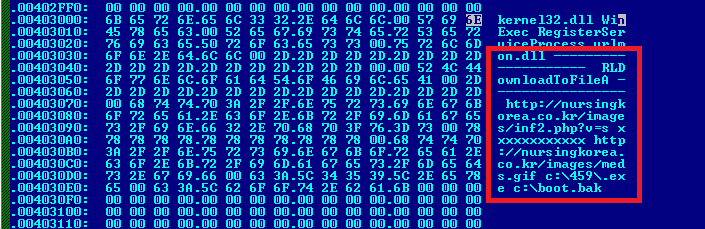
**7.3) Malware Analysis Techniques**

**Basic Analysis:**

* **Static Analysis**:
  + Examines malware without running it
  + Tools: Virus-Total, strings, a disassembler like IDA Pro
* **Dynamic Analysis**:
  + Run the malware and monitor its effect
  + Use a virtual machine and take snapshots
  + Tools: Reg-Shot, Process Monitor, Process Hacker, Capture-BAT

**Advanced Analysis:**

* **Static Analysis:**
  + Reverse Engineering with disassembler
  + Highly complex
* **Dynamic Analysis:**
  + Run code in Debugger
  + Examines internal state of running malicious executable

****

**7.4) General Rules of Malware Analysis**

* Don’t get too caught up in the details. Most malware programs are large and complex, and you can’t possibly understand every detail.
* Focus instead on the key features. When you run into difficult and complex sections, try to get a general overview before you get stuck in the weeds.
* Every situation is different, and the various tools and techniques that you’ll learn will have similar and sometimes overlapping functionality.
* If you’re not having luck with one tool, try another. If you get stuck, don’t spend too long on any one issue; move on to something else.
* Try analyzing the malware from a different angle, or just try a different approach.
* As new malware analysis techniques are developed, malware authors respond with new techniques to thwart analysis.
* To succeed as a malware analyst, you must be able to recognize, understand, & defeat these techniques, and respond to changes in the art of malware analysis.

**8)About the tool (Malware Analyzer)**

**8.1) Brief Introduction:**

* The tool is going to work on the concept of python programming.
* We have used the following built in modules of the python in the source code:
  + Hashlib Module
  + Time Module
  + Operating System Module
  + Struct Module
  + Request Module
  + PE(Portable-Executable) file Module
* The tool is used for Static Analysis of Malware

**8.2) Description**

* This is a portable script written in python used for "Static Analysis" of malwares. Focus on malware PE Headers, Strings, Image Type, MD5 Hash, Virus-Total Analysis. You can skip Virus-Total API Key if do not want to upload your sample on Virus-Total. Supported wherever python is installed (Tested on Linux, Windows). Malware Analyzer will generate 4 output files in the same folder as the script: Strings.txt for the extracted strings, PE Analysis.txt for PE headers, VT Basic Scan.txt and VT Scan.txt for virus total analysis.

**8.3)** **The capabilities of the tool:**

**1.Strings:**

Strings are ASCII and Unicode-printable sequences of characters embedded within a file. Extracting strings can give clues about the program functionality and indicators associated with a suspect binary. For example, if a malware creates a file, the filename is stored as a string in the binary.

**2) Hashes:**

Hashing is simply passing some data through a formula that produces a result, called a hash. That hash is usually a string of characters and the hashes generated by a formula are always the same length, regardless of how much data you feed into it.

**3)Address of Entry point:**

The Address of Entry Point is the relative virtual address of the entry point, not the raw offset in the file. It holds the address of the first instruction that will be executed when the program starts.

**4)Relative Virtual Address:**

RVA (relative virtual address): An RVA is nothing but the offset of some item, relative to where it is memory-mapped; or we can simply say that this is an image file and the address of the item after it is loaded into memory, with the base address of image subtracted from memory

**5)No of sections:**

Roughly, there are 13 sections in an executable – 8 sections due to the PE format and 5 sections due to packing algorithm.

**6)Virtual Address:**

Applications do not directly access physical memory, they only access virtual memory. In other words, the Virtual Addresses (VAs) are the memory addresses that are referenced by an application.

**7)DLL:**

A DLL (Dynamic Link Library) file is an executable file that allows applications to share code to perform one or more predetermined functions. Most DLL files are very useful and aid in the process of running your applications.

**9) References:**

1.<https://antivirus.comodo.com/faq/how-antivirus-works.php>

2.<https://www.slidegeeks.com/business/product/process-flow-chart-of-virus-and-threat-protection-ppt-powerpoint-presentation-file-layout-pdf>

3.<https://www.cisco.com/c/en_in/products/security/advanced-malware-protection/what-is-malware.html>

4.<https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1624&context=etd_projects>

5.<https://www.ijert.org/research/an-emerging-malware-analysis-techniques-and-tools-a-comparative-analysis-IJERTV10IS040071.pdf>

6.<https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/malware-vs-viruses.html>

7.<https://blog.malwarebytes.com/glossary/signature/>

8.<https://www.logixconsulting.com/2020/12/15/what-is-signature-based-malware-detection/>

9.<https://www.malwarebytes.com/mwb-download>

10.<https://www.sciencedirect.com/topics/computer-science/window-firewall>

Our Team Members: Submitted to:

1.Anmol Garg Preeti Kaushik Mam

2.Prakash Chand Thakuri

3.Rohit Kumar

4.Shivam Singh Panwar