



MUSANZE COLLEGE

DEPARTMENT: ICT
PROGRAM: INFORMATION TECHNOLOGY

RQF LEVEL: 8

MODULE: CYBERSECURITY

Academic: 2024-2025

ASSIGNMENT 1

Date: 16/03/2025

Name: NIYOMUHOZA Chantal

Reg No: 24RP14252

Q1. Which best practices used to detect and identify malwares?

ANSWER:

1. Signature-based Detection

Signature-based detection involves using a database of known malicious file signatures or hash values to identify malware. The best practice here is to regularly update antivirus or endpoint protection software with the latest malware signature definitions. This ensures the system can detect known threats effectively.

2. Heuristic Analysis

Heuristic analysis identifies malware by examining its behavior or attributes rather than relying on known signatures. The best practice is to use heuristic scanning to detect previously unknown malware based on patterns like suspicious file behaviors, unusual system calls, or abnormal activity.

3. Behavioral-based Detection

Behavioral-based detection focuses on monitoring a program's actions in real-time to identify suspicious or harmful behaviors, such as unauthorized file access or system changes. To implement this best practice, organizations can use endpoint monitoring tools that track file modifications, network traffic, and resource usage.

4. Sandboxing and Static Analysis

Sandboxing involves running malware in a controlled environment to observe its behavior without impacting the rest of the system. The best practice is to use sandbox tools to analyze suspicious files in a virtualized environment, providing insight into how malware behaves before it can cause harm. However, sophisticated malware may be able to detect sandbox environments and alter its behavior to evade detection, making it a less reliable method on its own.

5. Network Traffic Analysis

Network traffic analysis involves examining the flow of data within a network to detect unusual activity, such as connections to known malicious IPs or domains. The best practice is to implement Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to monitor inbound and outbound traffic for malware-related behavior, such as command-and-control communications. This method has limitations, especially when malware uses encryption or tunneling protocols to hide its communications.

6. File Integrity Monitoring

File integrity monitoring tracks changes to files, especially critical system files, to detect unauthorized alterations, a common indicator of malware activity. The best practice is to use file integrity monitoring tools to watch for unauthorized file changes or system configurations, which often point to malware presence.

7. Machine Learning & AI-based Detection

Machine learning and AI-based detection uses algorithms to analyze large datasets for patterns indicative of malicious behavior. The best practice is to leverage AI-based tools that learn and adapt over time, helping to detect new and evolving malware strains. This approach, however, requires large volumes of labeled data and continuous model training, which can be resource-intensive and may not be immediately effective without proper tuning.

8. Threat Intelligence Feeds

Threat intelligence feeds provide up-to-date information on emerging threats and Indicators of Compromise (IOCs). The best practice is to integrate threat intelligence feeds into your security tools and processes to stay informed about new malware variants and attack strategies.

9. Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) tools monitor endpoints (like computers, servers, and mobile devices) for suspicious activity and help respond to threats quickly. The best practice is to deploy EDR solutions that offer visibility into endpoint activities, enabling early detection and automated response.

10. Regular Security Audits and Penetration Testing

Regular security audits and penetration testing involve reviewing systems for vulnerabilities and simulating cyberattacks to identify weaknesses. The best practice is to conduct frequent audits and tests to find and address vulnerabilities that could be exploited by malware.

11. User Education and Awareness

User education and awareness programs are essential for teaching individuals how to recognize phishing attacks, suspicious downloads, and other malware delivery methods. The best practice is to conduct regular training sessions to help employees understand the importance of security and to encourage cautious behavior when interacting with emails and websites.

12. Regular System and Software Updates

Keeping systems and software up to date is crucial for mitigating vulnerabilities that malware can exploit. The best practice is to implement automated patch management systems to ensure all systems are updated with the latest security patches.

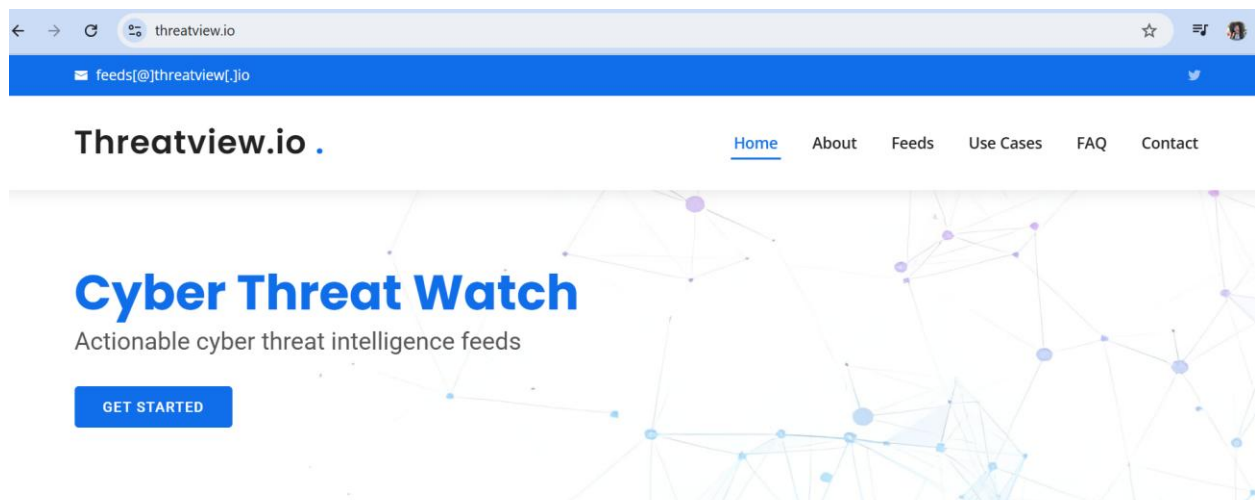
13. Multi-layered Security Approach

A multi-layered security approach involves using a combination of different security measures to protect against malware at various stages of an attack. The best practice is to integrate tools like firewalls, antivirus software, EDR, network monitoring, and user education to create a defense-in-depth strategy.

Q2. From one practice, screenshot how to identify a malware

ANSWER: Use this “Threat Intelligence Feeds”

Step1: browsing “threatview”



Step2: after start

← → threatview.io

Threatview.io . Home About Feeds Use Cases FAQ Contact

Find Out More About Us

- Public Blocklists
- Honeypot Sensors
- Malware Repositories / Sandboxes
- OSINT Crawling
- Darkweb Crawling

- IP Blocklist
- Domain Blocklist
- Bitcoin Intel
- File Hash Blocklist
- OSINT Feeds

Overview of our Feed generation cycle - Threatview.io

Cyber Threat Intelligence is a process of collection, processing and analyzing the indicators of compromise for understanding attackers behavior and other TTP's.

With the increase in cyber-attacks and new tactics, it is becoming increasingly difficult to identify malicious activities carried out by the attackers. Cyber Threat Watch is a Cyber Threat Intelligence Project (currently in beta) created for researching about cyber threat actors, campaigns and for supporting InfoSec community professionals to efficiently protect, identify and hunt malicious actors in IT environments. In order to simplify the process and provide actionable intelligence for rapid breach detection indicators of compromise in the form of IP, Domain, File Hash, MD5/SHA1 blocklists have been created from Threat

Step 3: use threatminer

← → threatminer.org/index.php

ThreatMiner
Data Mining for Threat Intelligence

Indicators Reports

Search for domains, IPs, MD5(SHA1)SHA256, email address or APTnotes(aptnotes:), ssl(ssl:), user-agent(ua:), AV family(av:), filename (filename:), URI (uri:), registry (reg:), mutex (mutex:)... Q

25636651

Files

50372511

Domains

48887726

Hosts

978

APTNotes Reports

Recent domains

Recent hosts

Recent files


Step 4: search dns server like 8.8.8.8


Indicators


Reports


8.8.8.8


Q


 25636651
Files


 50372511
Domains

 48887726
Hosts

 978
APTNotes Reports

 Recent domains

 Recent hosts

 Recent files

Step5: select pulsefret.com

Passive DNS

Historical DNS resolutions associated with 8.8.8.8.

Copy Excel CSV PDF

Search: pul

Domain	First seen	Last seen	Sources
pulsefret.com	1552348800000	1559606400000	SecurityTrails

Showing 1 to 1 of 1 entries (filtered from 3,478 total entries)

Previous

1

Next

Step6: <https://www.threatminer.org/domain.php?q=pulsefret.com>

Passive DNS

Historical DNS resolutions associated with pulsefret.com.

IP	BGP Prefix	Country code	Last seen	Sources
104.27.149.241	N/A	US	1561099350000	VirusTotal SecurityTrails
104.27.148.241	N/A	US	1561099350000	VirusTotal SecurityTrails
216.170.122.25	N/A	US	1561075200000	SecurityTrails
112.213.89.135	N/A	VN	1561075200000	SecurityTrails
51.83.68.185	N/A	FR	1561075200000	SecurityTrails
192.185.16.30	192.185.0.0/18	US	1561075200000	SecurityTrails
87.98.179.183	87.98.128.0/17	FR	1561075200000	SecurityTrails
183.129.169.22	N/A	CN	1561075200000	SecurityTrails
72.15.255.229	72.15.252.0/22	US	1561075200000	SecurityTrails
47.254.95.228	N/A	HK	1561075200000	SecurityTrails Back to the top