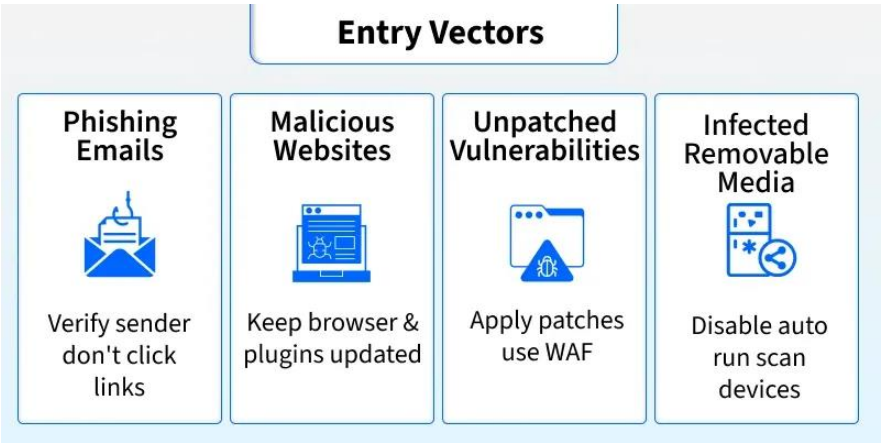
CYBER SECURITY INTERNSHIP

Task 4

MALWARE TYPES & BEHAVIOR ANALYSIS (BASIC)

JASHMI KS

Malware is software that infects systems without user consent to steal sensitive data (bank details, passwords, personal emails), disrupt operations, or alter core system behavior. It can exfiltrate confidential information, corrupt or delete files, and impair system availability or integrity. Examples include ransomware (encrypts files for ransom) and spyware (monitors activity); mitigate risks with up-to-date antivirus and caution when opening links or attachments. Malware commonly spreads through the following vectors:



Types of Malware

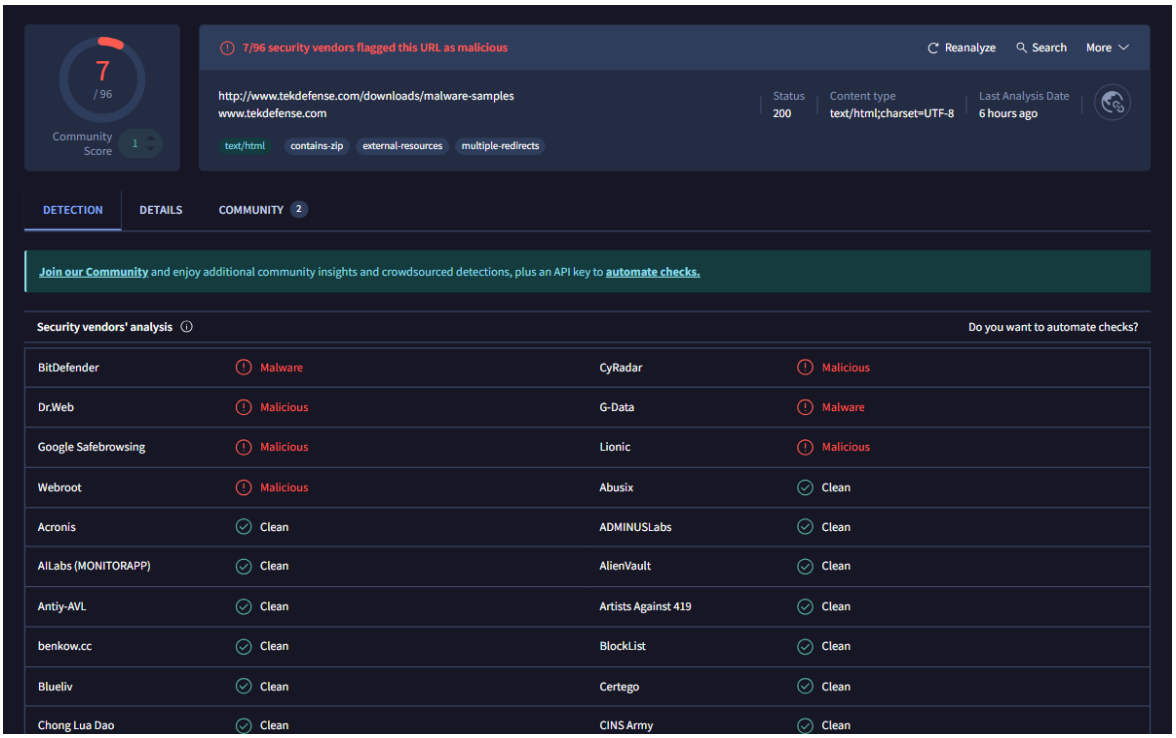
- **Viruses -** A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.
- **Worms -** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
- **Trojan horse -** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.
- **Ransomware** - Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.
- **Adware** - It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.
- **Spyware** - Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

- **Logic Bombs -** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.
- **Rootkits -** A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
- **Backdoors -** A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.
- **Keyloggers -** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Detection Report:

- Detection ratio: 7/96 vendors flagged the URL as malicious
- Vendors detecting as malicious: BitDefender, Dr.Web, Google Safebrowsing, Webroot, CyRadar, G-Data, and Lionic
- Vendors detecting as clean: Most vendors, e.g., Acronis, ADMINUSLabs, AlienVault, BlockList, ESET, etc.
- Content type: text/html, multiple redirects, contains zip/external resources
- Community score: 1 (indicating some user reports of risk)

Analysis: Even though only 7 vendors flagged the URL, the detections by major vendors such as BitDefender, Dr.Web, and Google Safebrowsing confirm that the URL is potentially malicious.



Observe Behavior Indicators

- URL contains external resources (likely malware downloads or trojan payloads)
- Multiple redirects suggest it may lead to phishing sites or malware distribution
- Some antivirus engines marked it as Malware, others as Malicious, indicating potential trojan/ransomware delivery
- Presence of zip content may indicate a compressed malware file for download

Malware Lifecycle

From URL analysis, the lifecycle can be inferred:

1. **Creation:** Malicious actor creates a website hosting malware
2. **Distribution:** URL shared via email, social media, or advertisements
3. **Execution:** Victim clicks the link and the malicious payload attempts to download
4. **Infection:** Malware (e.g., trojan, ransomware) executes on the victim system
5. **Payload Action:** Steals data, encrypts files, or creates a backdoor
6. **Persistence:** Malware may remain on the system for future attacks

Categories

Dr.Web	known infection source
Webroot	Malware Sites
Forcepoint ThreatSeeker	computer security

History

First Submission	2015-10-12 18:57:32 UTC
Last Submission	2026-01-22 06:29:46 UTC
Last Analysis	2026-01-22 06:29:46 UTC

HTTP Response

Final URL
http://www.tekdefense.com/downloads/malware-samples

Serving IP Address
198.185.159.160

Status Code
200

Body Length
44.84 KB

Body SHA-256
c2c796d560b0cd3758f1d57dc81a19771e3c3df251ca651db94a8817021ec031

Headers

Accept-Ranges	bytes
Age	0
Content-Type	text/html;charset=UTF-8
Date	Thu, 22 Jan 2026 06:29:48 GMT
Server	Squarespace
Set-Cookie	JSESSIONID=FBD36DB52236C6C5F0A55A0198765BEE.v5-web004; Path=/; HttpOnly
X-Contextid	bquUe8QS/GBDGvLx6
Transfer-Encoding	chunked

- **Phishing emails** containing malicious links
- **Malvertising** (malicious online advertisements)
- **Fake websites** pretending to be trusted sources
- **Social media or messaging apps** distributing malicious links
- Drive-by downloads from compromised websites

From analysis and general best practices:

- Avoid clicking unknown or suspicious URLs
- Verify URLs using **VirusTotal or similar services**
- Keep antivirus software up-to-date
- Enable browser security features like **safe browsing and URL filtering**
- Educate users to recognize phishing or suspicious sites
- Regular system and browser updates to patch vulnerabilities

Summary

- The URL http://www.tekdefense.com/downloads/malware-samples is flagged by 7/96 vendors, confirming potential risk
- Malware could be delivered via zip files or redirects
- Behavior indicators include suspicious downloads and multiple redirects
- The malware lifecycle shows potential for infection, payload execution, and persistence
- Malware spreads primarily via phishing emails, fake websites, and social engineering
- Prevention involves safe browsing, antivirus software, URL verification, and user education