

## Report of Analysis

**Name:** - Vishal Dixit

**University Roll No:-** 201500792

### **1> Malware Analysis :-**

File name - 16.pdf

Sha 256 - [83e7219942b1b4dc5ccba2aa29480add7cf5e126bf6edc7facab593b0e209842](#)

This report has 10 indicators that were mapped to 7 attack techniques and 5 tactics.

### **Brief about sandbox analysis (One para) :-**

Sandboxing is widely employed in software development and testing environments. Software developers use sandboxes to isolate and evaluate the behavior of new or untrusted code, ensuring that it does not adversely impact the overall system. By providing a safe and controlled testing environment, developers can identify bugs, vulnerabilities, and compatibility issues without risking damage to the production environment. Sandboxing also facilitates the creation of safe, reproducible, and standardized testing scenarios, allowing developers to validate their code in various conditions before deployment. This practice promotes more robust and secure software development, leading to higher-quality products that are less prone to crashes or security breaches. Overall, sandboxing offers an indispensable toolset for both cybersecurity professionals and software developers to enhance the safety, stability, and reliability of their systems and applications.

### **2> URL Analysis :-**

**1. URL** - http://totalpad.com

**2. Is it malicious** - Yes

**3. URL categories** -

Forcepoint ThreatSeeker      search engines and portals

Xcitium Verdict Cloud              media sharing

alphaMountain.ai              Malicious, News (alphaMountain.ai)

BitDefender              news

**4. First Submission** -      2012-03-26 12:26:42 UTC

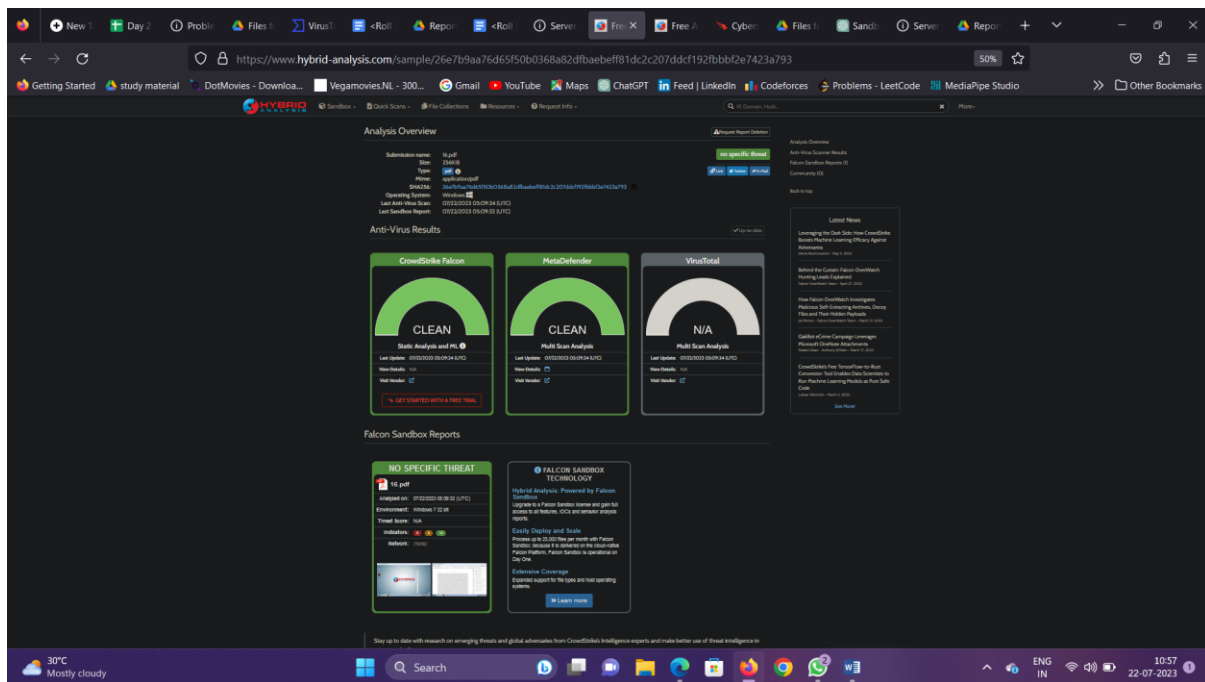
**5. Last Submission** -      2023-06-16 09:36:18 UTC

**6. Last Analysis** -      2023-06-16 09:36:18 UTC






### **Brief about the URL (One para)**

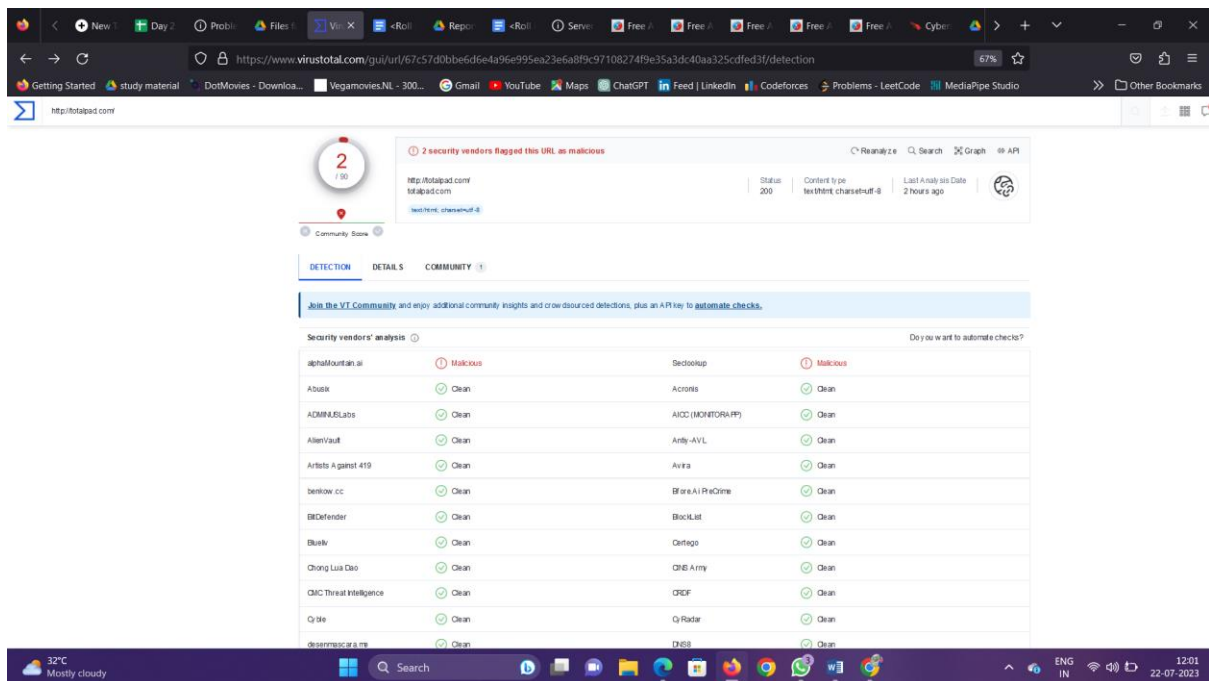
URL stands for Uniform Resource Locator, and it is a fundamental concept in web technology used to address and locate resources on the internet. A URL is a string of characters that

provides a web browser with the information necessary to retrieve a specific resource, such as a web page, an image, a video, or a file, from a web server. It typically consists of several components, including the protocol (e.g., "http" or "https"), the domain name (e.g., "[www.example.com](http://www.example.com)"), an optional path to a specific resource, and additional parameters or queries. URLs enable users to access and share web content easily, acting as the foundation of the internet's interconnectedness, and form the basis for navigating the vast network of web pages and online resources available worldwide.



## Email Header Analysis :-

-  [DMARC Compliant](#)
  -  [SPF Alignment](#)
  -  [SPF Authenticated](#)
  -  [DKIM Alignment](#)
  -  [DKIM Authenticated](#)



Security controls are countermeasures or safeguards used to reduce the chances that a threat will exploit a vulnerability.

## **1> Malware Analysis Security Controls:**

Anti-Malware Solutions: Deploy robust anti-malware solutions across all endpoints and network gateways to scan and detect malicious files and activities. These solutions should have regular updates to stay current with the latest malware threats.

## **2> Email Header Analysis Security Controls:**

### **SPF, DKIM, and DMARC:**

Implement Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to verify the authenticity of email headers and prevent email spoofing.

### **Email Gateway Security:**

Use advanced email security gateways that inspect email headers and content for anomalies, suspicious domains, and phishing indicators. These gateways can filter out potentially harmful emails before they reach the users' inboxes.

In implementing these security controls, organisations should take a layered approach to cybersecurity. Combine preventive measures like firewalls and access controls with detective measures such as intrusion detection systems (IDS) and security information and event management (SIEM) solutions. Regular security audits and updates to security policies are essential to stay ahead of evolving threats and ensure a robust security posture. Additionally, collaboration with threat intelligence sharing communities and staying informed about the latest security developments can further enhance an organisation's ability to defend against Cyber Attacks effectively.