1. **Malware Analysis**

File name – 1.pdf
Sha 256 - 0b4e30c8a8ead0bae21046b628cdfc46e6c472e3159784deb80cf22315639e05

Brief about sandbox analysis : Sandbox analysis is a cybersecurity technique used to detect and analyze potential threats, such as malware and suspicious files, in a safe and isolated environment.

no specific threat
AV Detection: Marked as clean

Cryptographic Related
Sample file has high entropy (likely encrypted/compressed content)

Network Analysis

DNS Request

No relevant DNS requests were made.

Contacted Hosts

No relevant hosts were contacted.

HTTP Traffic

No relevant HTTP requests were made.

2. **URL Analysis**

URL - http://subtitleseeker.com/
Is it malicious - NO
URL categories - BitDefender : Education
First Submission - 2011-12-01 09:51:42 UTC
Last Submission - 2023-07-19 20:08:34 UTC
Last Analysis - 2023-07-19 20:08:34 UTC

Brief about the URL

Final URL

http://ww1.subtitleseeker.com/

Serving IP Address

69.16.230.228

Meta Tags

Description:
subtitleseeker.com is your first and best source for all of the information you're looking for. From general topics to more of what you would expect to find here, subtitleseeker.com has it all. We hope you find what you are searching for!

3. **Email Header Analysis**

Checking header is compliant or not

Headers Found

Header Name	Header Value
Delivered-To	anikateag7316@gmail.com
X-Google-Smtp-Source	APBJJlHikP9tthw6bo9CnJN8DxxG8yp9bL36vQZi3VvPpzHxDPXEU1u3FSPftEmMvyo9YJTf0y87
X-Received	by 2002:a05:620a:130e:b0:767:f845:74e with SMTP id o14-20020a05620a130e00b00767f845074emr771976qkj.62.168996
ARC-Seal	i=1; a=rsa-sha256; t=1689963580; cv=none; d=google.com; s=arc-20160816; b=zip2c6jkrTg9fXD34NMAO4QyEpvEz4Nr32 zKNAtuXlp6jvpRNDYXHg+UnYf+ OmV513btRk96e605UzdX9nalim3j5TCBz8TlIJJdFMtw6p7dWIccjsTLRFf1w77FBkRJ Gp 3vMGeHZR0bM61H2rMBfFfa91b+nBy6+cKHnpgh72Kq6ykRhdZlS67lJ8Ao 5D1Q==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=feedback-id:message-id:mime-version:subject:re ncorWTzCvVEf4bi/1n1uKxnuql=; fh=hlQerW2X4CiusVXxKio30pV+CN1HftMVMKjl6GoxT8k=; b=FRkJFlfYEx9j+YK3V55bR NcQkR+8SZwkpfHz6nhXz3er+spK9JF+mc6 ZT+F+WEHmmVit9WiODU9y+3gr9JVqmuUT8VgSwP3wvLNQwSTuCwJFkxo HRI4WnB uqlk23d3i3QJsJdJBfex6uXAWO9xu2lC99i3XRYAOvYFV7SR37HH1HfdM9zyvUc9DzRk bcMg==

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

DKIM Authentication: DKIM (DomainKeys Identified Mail) is an email authentication method that adds a digital signature to the email header. It verifies the email's integrity and authenticity by using a private key associated with the sending domain and a public key in the domain's DNS records.
DKIM Alignment: DKIM alignment checks if the domain in the "From" field of an email matches the domain used in the DKIM signature. When they match, it indicates that the sender's identity is valid, increasing email trustworthiness.
SPF Alignment: SPF (Sender Policy Framework) alignment verifies if the domain in the "Return-Path" or "Mail From" field aligns with the domain specified in the SPF record. Alignment confirms that the email's return path is authorized by the domain's owner.
SPF Authentication: SPF is an email authentication protocol that specifies authorized mail servers for a domain. SPF authentication involves checking if the sender's IP address is listed as an allowed sender in the domain's SPF record. A pass result indicates a legitimate sender, while a fail result suggests potential email spoofing.

4. **Suggested security controls and how will you implement them.**

- Add a firewall to the network to prevent and block untrusted sites and packets.
- Use EDR in the end devices for detection and recovery in case of attacks.
- Enable proper patch management to keep security updated.
- Add IPS to monitor the incoming data.
- Create awareness about cybersecurity and proper ways to handle incidents of breach.
- Create a crisis recovery plan to quickly handle breach.
- Use SIEM for monitoring.
- Implement proper encryption of data and use of strong passwords.
- Enable proper and minimal Access controls.
- Do vulnerability analysis and penetration testing.