THREAT INTELLIGENCE AGGREGATOR AUTOMATION TOOLKIT

(Detection Only)

Project Report submitted in partial fulfillment of the requirements for the completion of

UNIFIED INTERNSHIP PROGRAM

(Cyber Security / Ethical Hacking)

Submitted By

Name : Aquib Ahmad Khan

Intern ID : UMID27112571911

Domain : Cyber Security

Submitted To

Unified Internship Program

Operating System Used

Microsoft Windows 11

Project Duration

January 2026 – February 2026

1. Introduction

Threat Intelligence Aggregation plays a critical role in modern cyber defense mechanisms. This project focuses on the automated collection, parsing, and aggregation of Indicators of Compromise (IOCs) such as malicious IP addresses and domain names from trusted open-source feeds. The system is strictly designed for detection-only and defensive monitoring purposes.

2. Objectives

- Automate threat intelligence collection from multiple sources.
- Parse and normalize IP addresses and domain indicators.
- Generate defensive blocklists for security monitoring.
- Produce structured intelligence reports.

3. Tools & Technologies

- Python 3.14.2
- Requests Library
- Microsoft Windows 11
- Open Source Threat Intelligence Feeds
- Windows PowerShell

4. Project Architecture

The project is organized using a modular directory structure including feeds, output, and reports. The aggregator script fetches threat data from open sources, validates indicators, and stores the processed data into structured output files for defensive usage.

5. Methodology

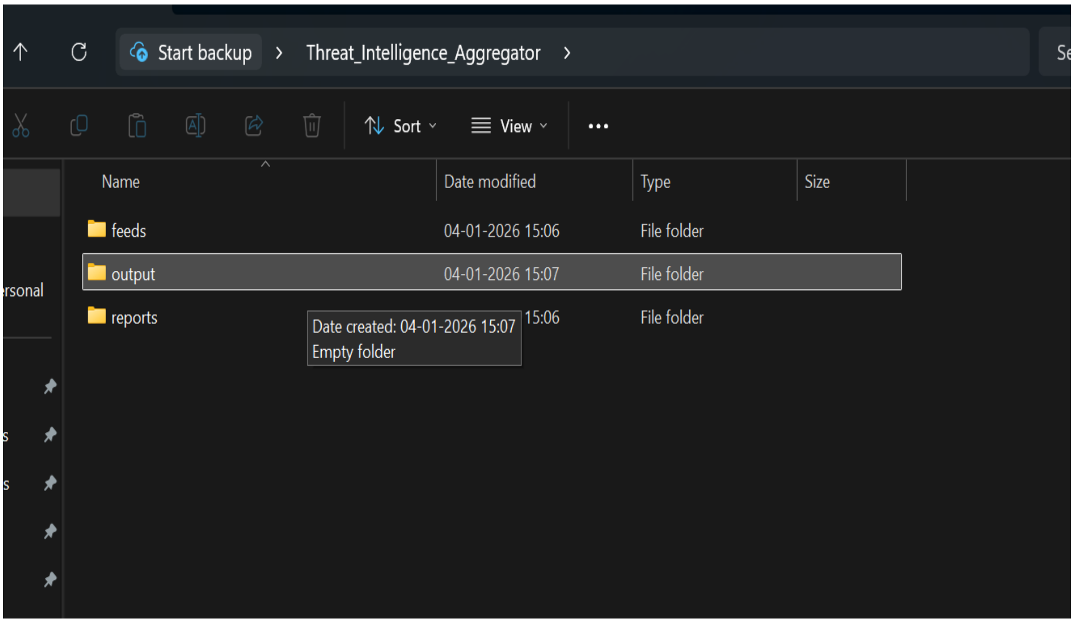
1. Fetch threat intelligence feeds from trusted sources.
2. Extract malicious IP addresses and domains.
3. Validate and normalize indicators.
4. Generate blocklist files.
5. Produce final threat intelligence report.

6. Implementation (Python Script)

```
#!/usr/bin/env python3
import requests
import ipaddress

feeds = {
    "ips": "https://raw.githubusercontent.com/stamparm/ipsum/master/ipsum.txt",
    "domains": "https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts"
}

ips = set()
domains = set()

print("[*] Loading threat intelligence feeds...")

ip_response = requests.get(feeds["ips"])
if ip_response.status_code == 200:
    for line in ip_response.text.splitlines():
        if line.startswith("#") or not line.strip():
            continue
        ip = line.split(",")[0]
        try:
            ipaddress.ip_address(ip)
            ips.add(ip)
        except:
            pass

print(f"[+] Loaded malicious IPs: {len(ips)}")

domain_response = requests.get(feeds["domains"])
if domain_response.status_code == 200:
    for line in domain_response.text.splitlines():
        if line.startswith("0.0.0.0"):
            domains.add(line.split()[1])

print(f"[+] Loaded malicious domains: {len(domains)}")

with open("output/ip_blocklist.txt", "w") as f:
    for ip in sorted(ips):
        f.write(ip + "\n")

with open("output/domain_blocklist.txt", "w") as f:
    for domain in sorted(domains):
        f.write(domain + "\n")

with open("reports/ti_report.txt", "w") as r:
    r.write("Threat Intelligence Aggregator Report\n")
    r.write(f"Total IPs: {len(ips)}\n")
    r.write(f"Total Domains: {len(domains)}\n")

print("[+] Blocklists and report generated successfully")
```

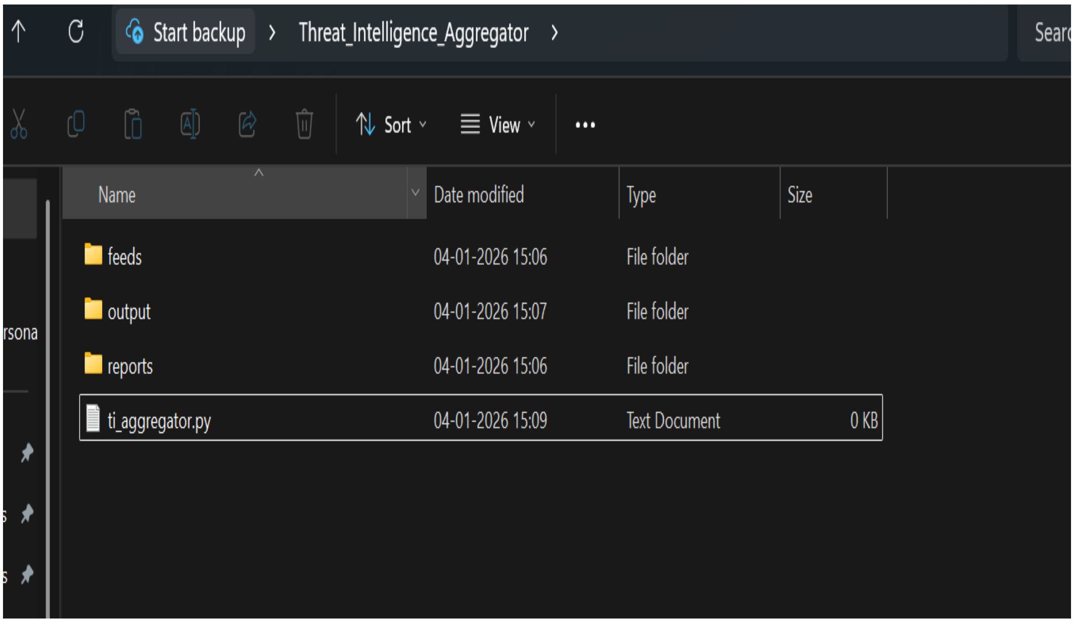
7. Output & Screenshots

The following screenshots demonstrate successful execution, blocklist generation, and report creation.

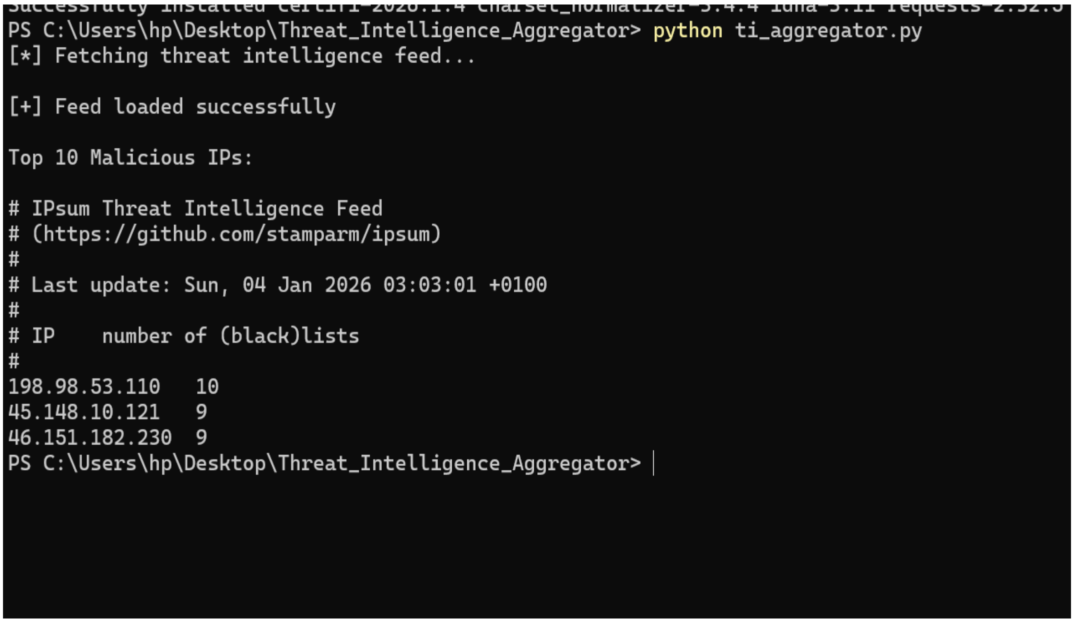


Name	Date modified	Type	Size
feeds	04-01-2026 15:06	File folder	
output	04-01-2026 15:07	File folder	
reports	15:06	File folder	

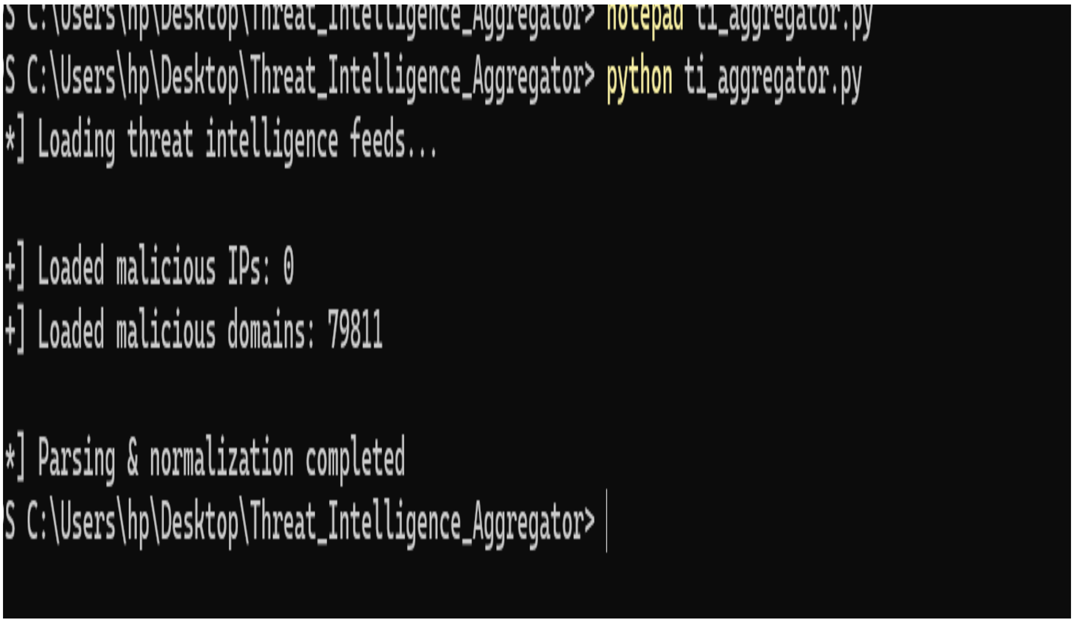
Date created: 04-01-2026 15:07
Empty folder



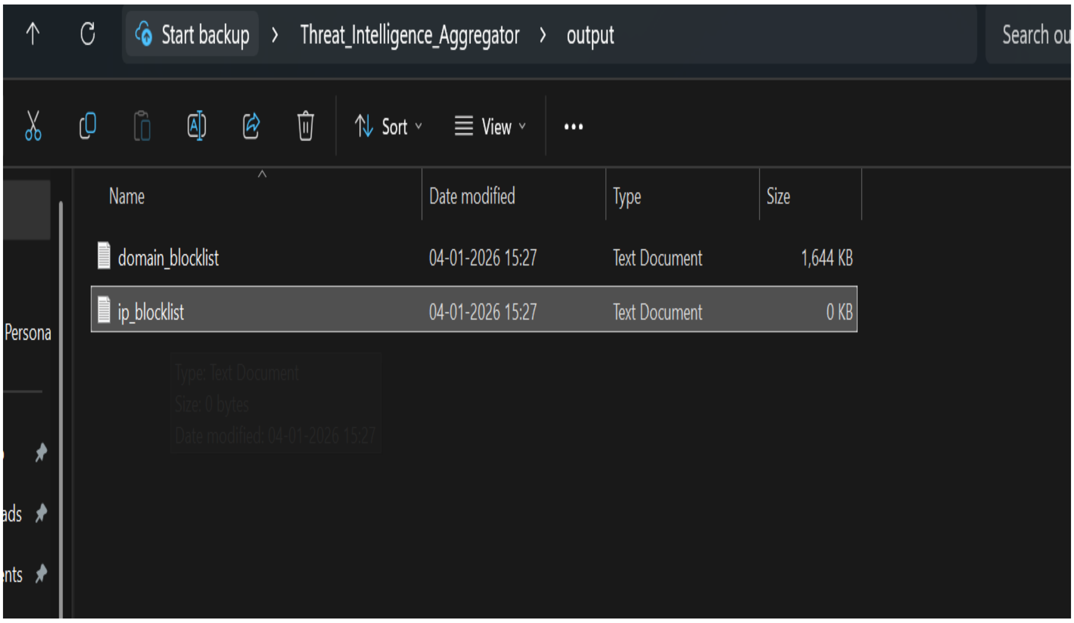
Name	Date modified	Type	Size
feeds	04-01-2026 15:06	File folder	
output	04-01-2026 15:07	File folder	
reports	04-01-2026 15:06	File folder	
ti_aggregator.py	04-01-2026 15:09	Text Document	0 KB



```
Successfully installed certifi-2026.1.4 charset_normalizer-3.4.4 idna-3.11 requests-2.32.5
PS C:\Users\hp\Desktop\Threat_Intelligence_Aggregator> python ti_aggregator.py
[*] Fetching threat intelligence feed...

[+] Feed loaded successfully

Top 10 Malicious IPs:

# IPsum Threat Intelligence Feed
# (https://github.com/stamparm/ipsum)
#
# Last update: Sun, 04 Jan 2026 03:03:01 +0100
#
# IP    number of (black)lists
#
198.98.53.110   10
45.148.10.121   9
46.151.182.230  9
PS C:\Users\hp\Desktop\Threat_Intelligence_Aggregator>
```

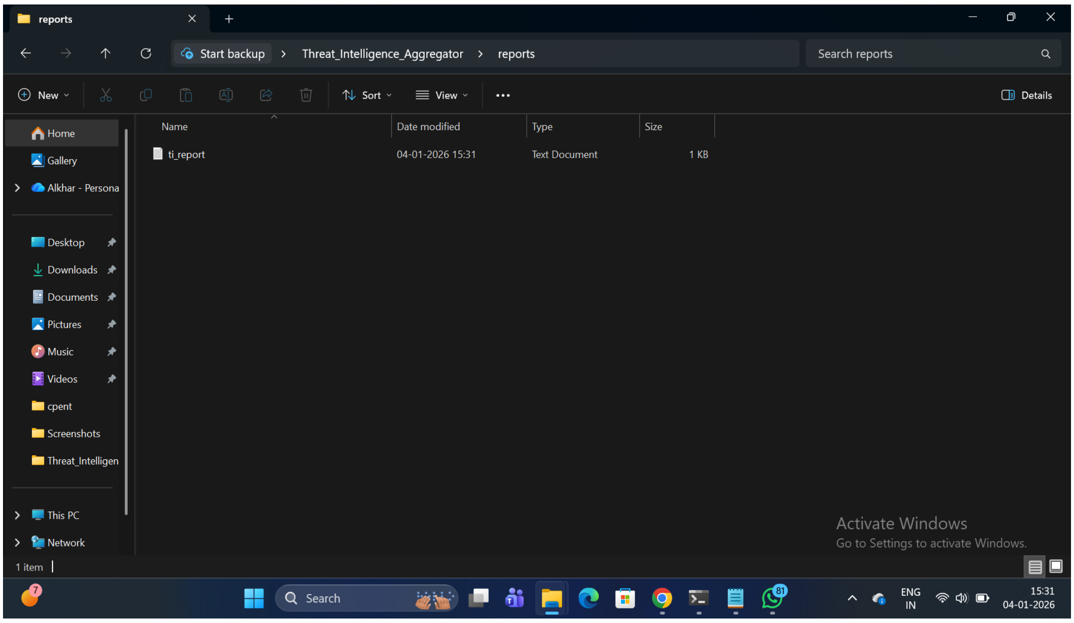


```
S C:\Users\hp\Desktop\Threat_Intelligence_Aggregator> notepad ti_aggregator.py
S C:\Users\hp\Desktop\Threat_Intelligence_Aggregator> python ti_aggregator.py
*] Loading threat intelligence feeds...

+] Loaded malicious IPs: 0
+] Loaded malicious domains: 79811

*] Parsing & normalization completed
S C:\Users\hp\Desktop\Threat_Intelligence_Aggregator>
```



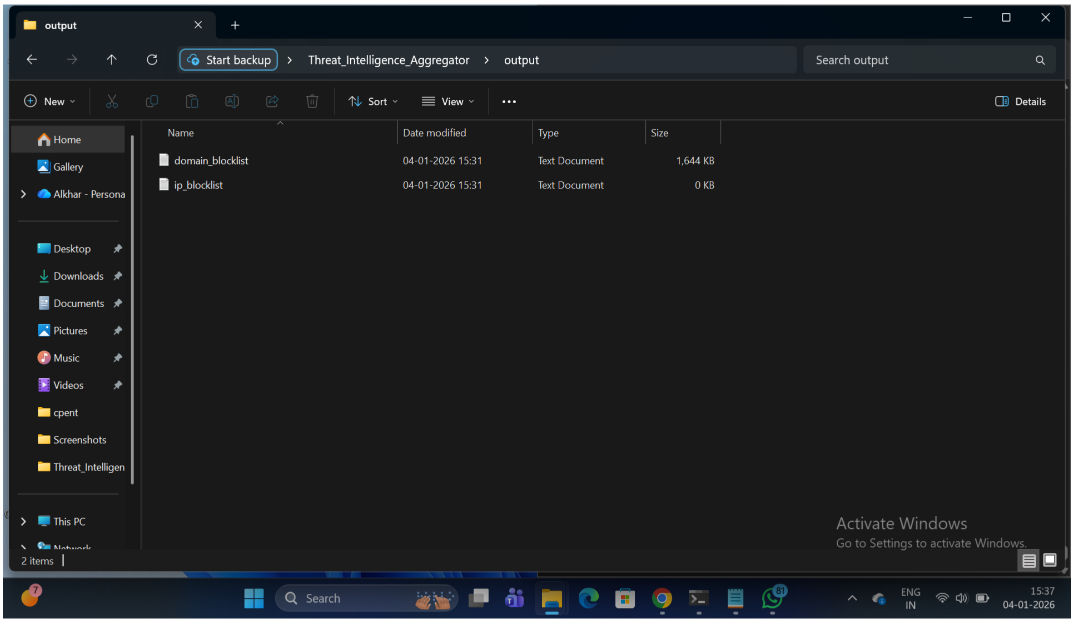
Name	Date modified	Type	Size
domain_blocklist	04-01-2026 15:27	Text Document	1,644 KB
ip_blocklist	04-01-2026 15:27	Text Document	0 KB

Type: Text Document
Size: 0 bytes
Date modified: 04-01-2026 15:27



Name	Date modified	Type	Size
ti_report	04-01-2026 15:31	Text Document	1 KB

Activate Windows
Go to Settings to activate Windows.



Name	Date modified	Type	Size
domain_blocklist	04-01-2026 15:31	Text Document	1,644 KB
ip_blocklist	04-01-2026 15:31	Text Document	0 KB

8. Conclusion

The Threat Intelligence Aggregator successfully demonstrates how automated threat intelligence can be used for proactive cyber defense. This project aligns with industry-standard SOC practices and reinforces the importance of detection-only monitoring.