

## Lab# 02: Threat Intelligence Feeds & Portals









**Objective #1** Learn about Threat Intelligence feeds for security analysis.

### 1. ThreatView

**Link:** <https://threatview.io/>

This portal generates threat feeds every day at 11 pm UTC with 'high confidence' → less false positives. Threat feeds are in machine readable format and can be ingested readily in security appliances like firewalls, SIEM, Ad Blockers, PiHole etc.

This information can be used for Threat Hunts and blocking traffic or files coming from these sources that can potentially perform some malicious activities. E.g. Malicious Hash feeds can be ingested in Forensic tools readily by creating a hash set and then can be used for finding malicious files matching ingested hash values.

 <b>OSINT Threat Feed</b> Malicious indicators of compromise gathered from OSINT Source - Twitter and Pastebin	 <b>C2 Hunt Feed</b> Infrastructure hosting Command & Control Servers found during Proactive Hunt by Threatview.io	 <b>IP Blocklist</b> Malicious IP Blocklist for known Bad IP addresses	 <b>Domain Blocklist</b> Malicious Domains identified for phishing/ serving malware/ command and control
 <b>MD5 Hash Blocklist</b> MD5 hashes of malicious files or associated with - malware, ransomware, hack tools, bots etc.	 <b>URL Blocklist</b> Malicious URL's serving malware, phishing, botnets and C2	 <b>Bitcoin Address Intel</b> Bitcoin addresses identified to be linked with malicious activity	 <b>SHA File Hash Blocklist</b> SHA hashes of files known or linked with malware execution

### 2. ThreatMiner

**Link:** <https://www.threatminer.org>

Threat intelligence and intrusion analysts who regularly perform research into malware and network infrastructure often find the need to rely on multiple websites that individually holds a small piece of the larger puzzle. It is often the case for pivoting directly from an open-source research report is unavailable and that it is sometimes difficult to remember if an indicator has already been reported and/or attributed. All these small but frustrating obstacles distract an analyst from what they do best: **analyse**.

This is why ThreatMiner was created. ThreatMiner is a threat intelligence portal designed to enable analysts to research under a single interface.

Step 1: Check domains for phishing attacks.



Full Featured Tools  
SOC Tools

allindiachat.com

Search

Step 2: Check for Denial of Service Resilience



Full Featured Tools  
SOC Tools

upes.ac.in

Search

Step 3: Use the email analyzer option to validate email headers and check malicious email samples.

**Objective #2:** Learn about Threat Intelligence portal and security analysis.

## 1. VirusTotal

**Link:** <https://www.virustotal.com/gui/>

VirusTotal is a free online service that analyzes suspicious files and URLs for potential malware. It acts as a central hub, leveraging the power of multiple antivirus engines and threat intelligence sources to provide a comprehensive report on the submitted item. VirusTotal can reveal information about the script's functionality and potential infection attempts.

- **Multi-engine Analysis:** VirusTotal scans files and URLs with dozens of antivirus engines, giving a broader perspective on potential threats.
- **Community Reporting:** The platform allows users to share information about identified malware, providing valuable insights for IOC analysis.
- **Historical Data:** VirusTotal maintains a vast database of analyzed files and URLs. You can search for existing information on known IOCs.
- **Hash Lookups:** Quickly determine if a file hash is associated with previously identified malware.

VirusTotal can inspect files, URLs, Hashes for potential malware infections with over 70 antivirus scanners and URL/domain blocklisting services. Users can select a file from a computer via the browser and send it to VirusTotal. Submissions may be scripted in any programming language using the HTTP-based public API.

When users submit files or URLs to VirusTotal, it undergoes analysis by multiple antivirus engines, including popular products such as McAfee, Symantec, Kaspersky, and many others. These engines scan the submitted item and generate reports indicating whether they detect any malicious elements. VirusTotal then compiles these reports into a comprehensive analysis, providing insights into the potential threats associated with the submitted item.

Step 1: Open VirusTotal from <https://virustotal.com>

Step 2: Analyze malicious Document Hash which could be a Word document containing malicious macros. Search VirusTotal for the hash to see historical scan reports from various antivirus engines. Download malware sample from <https://github.com/LJ9859/Malware-Database>. The password for all zip files is "1337" without the quotation marks.

Step 3: Analyze hashes / signatures of files which could be a JavaScript being used to steal data or redirect users. Copy hashes from [https://github.com/bitdefender/malware-ioc/blob/master/metamorfo\\_malware/samples.hash](https://github.com/bitdefender/malware-ioc/blob/master/metamorfo_malware/samples.hash)

Step 4: Phishing URLs are analyzed and identified for suspicious elements like website age, content similarity to known phishing sites, and reports from other users. Copy URLs from <https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset>.

Step 5: Command and Control Server (C&C / C2): VirusTotal can help identify the server's purpose and potential malware families it communicates with. Download the C2 Server list from [https://github.com/duggytuxy/malicious\\_ip\\_addresses/blob/main/botnets\\_zombies\\_scanner\\_spam\\_ips.txt](https://github.com/duggytuxy/malicious_ip_addresses/blob/main/botnets_zombies_scanner_spam_ips.txt)

In addition to antivirus engines, VirusTotal also incorporates other security tools and services. It uses behavioural analysis, sandboxing, and Machine Learning techniques to detect and analyse malware that may evade traditional signature-based detection. This multi-layered approach enhances the accuracy and effectiveness of the analysis, helping users identify previously unknown or zero-day threats.

## 2. AlienVault

**Link:** [AlienVault Open Threat Exchange \(OTX\)](#)

AlienVault OTX or AT&T Alien Labs Open Threat Exchange [OTX]) is a free, open threat intelligence community for sharing indicators and details about malware and threat actors. OTX has over 100,000 participants, and over 19 million threat indicators are contributed daily.

It provides a wide range of security and threat detection capabilities, including intrusion detection, vulnerability assessment, security information and event management (SIEM), and threat intelligence. AlienVault is designed to help organizations of all sizes improve their security posture and effectively respond to threats.

You can subscribe to pulses which are threat summaries, detailing the reference (external report or blog post), adversary (threat actor), affected industries, malware family, associated ATT&CK techniques, IoCs, and related pulses. You can also follow contributors to monitor their OTX contributions.

### AlienVault Open Threat Exchange (OTX)

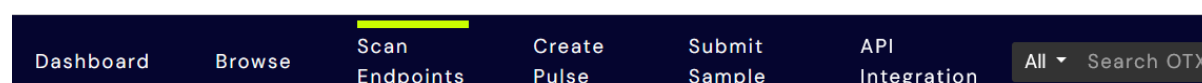


Figure 2: Alien Vault Options

- Dashboard → View a graph of malware clusters reported within a timeframe. Clicking a malware cluster shows features of the malware, and associated pulses.
- Browse → searches for Pulses, users, groups, indicators, malware families, industries, and adversaries, with ability to filter and sort.
- Scan Endpoints is a free threat scanning service that scans endpoints for IoCs in OTX to identify malware and other threats.
- Create Pulse: Create a new pulse by having OTX extract IoCs from a source that you provide (website, blog post, PDF report, email, PCAP, STIX, OpenIOC, CSV, or text file), or by manually adding IoCs.
- Submit Sample: Submit a URL or file for analysis. OTX will scan the content at submitted URLs and will perform static (and possibly dynamic) analysis on submitted files.
- API Integration: Provides info on using the OTX DirectConnect API to integrate OTX with Bro-IDS, STIX/TAXII, Suricata, and other third-party tools.
- Search: Search within all OTX, or narrow search to indicators, malware families, adversaries, etc.

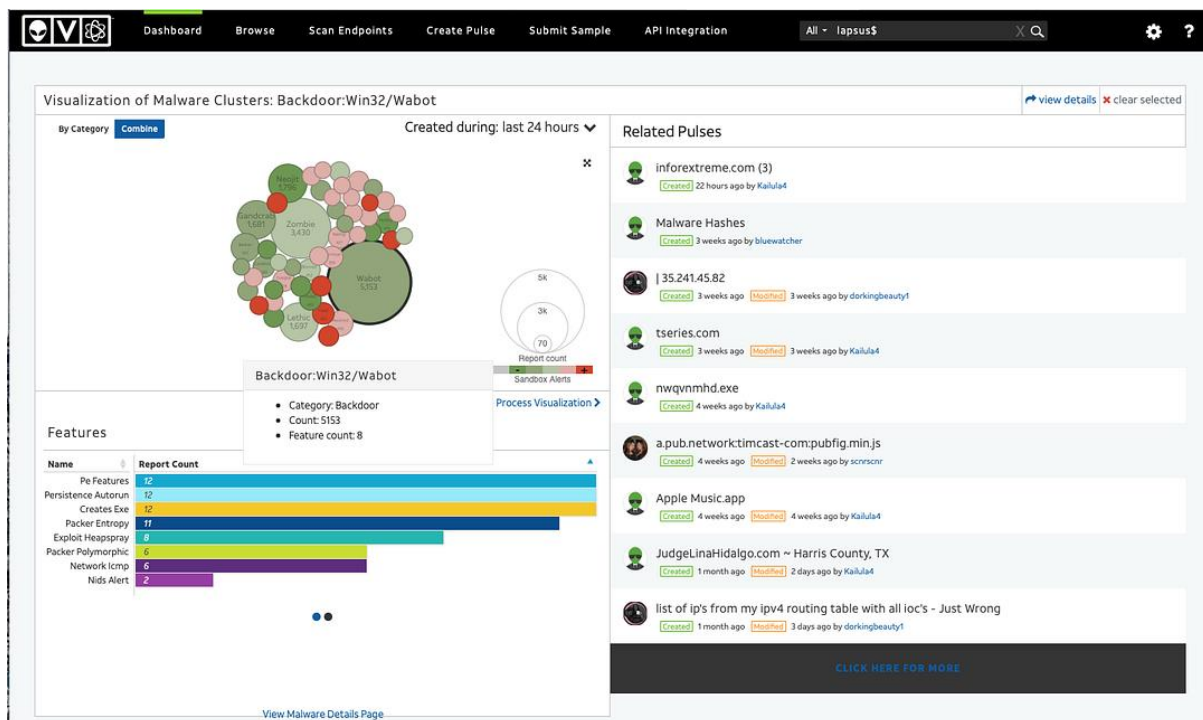


Figure 1: AlienVault OTX dashboard

### 3. Anti Scan Me

Step 1: Login with Key to <https://antiscan.me/>

Step 2: Upload and analyse your sample.

#### Lab activities:

- Perform the above-mentioned steps and present your lab report in WORD file with screenshots snipped with relevant details.
- Do NOT copy from others, else your submission will be graded ZERO.

1. Study the ThreatView portal and research about the various threat intel feeds.
2. Use ThreatMiner to research and find details about the artifacts in the threat feeds.
3. Upload malware samples from Gitub link (Lab #01) into VirusTotal to find potential malware infections from at least one IP address, Blacklisted Domain, Malware File and Hash.
4. Within OTX AlienVault find the most active malware in the last 7 days and write your findings from related pulses and reports.
5. Submit your report on malware samples for:
  - a. Files from <https://github.com/ThatSINEWAVE/Malware-Samples/tree/main/Samples>
  - b. URLs from <https://github.com/rodanmaharjan/ThreatIntelligence>
6. Perform Threat Hunt for your endpoint systems using OTX free malware scanning services.
7. Download and install OTX Endpoint agent running the PowerShell command. Prefer to use a virtual machine for this work.