Technical Cyber security Report

Analysis Using VirusTotal for a given Domain

By

Cyber Security Personnel : Victor Shedrack

Date : 10th April, 2025

Stakeholders : Lucy O. Raymond, PGD (Dublin), MSc (England), CDSA

Devrichard@vephlauni.com

Mentor Ibukun M. CompTIA Security+, CC ISC, CISSP.

REPORT OUTLINE

1. **Executive Summary**
2. **Background and Objectives**
3. **Methodology**
    - **3.1 Tool Configuration**
    - **3.2 Execution Process**
    - **3.3 Monitoring and Analysis**
4. **Findings and Analysis**
    - **4.1 Indicators of Compromise (IOCs)**
    - **4.2 Behavioral Analysis**
    - **4.3 Risk and Impact Assessment**
5. **Recommendations**
    - **5.1 Immediate Remediation Actions**
    - **5.2 Long-Term Mitigation**
6. **Conclusion**

Appendix: Additional Data

1. Executive Summary

- **Overview:** to use the threat intelligence and multi-engine detection features of VirusTotal to evaluate a URL or domain's reputation, behavior, and threat level.

  Key Findings:

  - 17ebook.com was flagged by 12 out of 96 vendors, with six identifying it as malicious and five associating it with phishing.
  - aladel.net was flagged by nine vendors and linked to phishing, malware delivery, and suspicious redirections.
  - clicnews.com showed minimal detection (1/96) but was still flagged as suspicious and potentially linked to compromised sites.

---

2. Background and Objectives

- **Project Context:**
  This analysis was conducted as part of a threat intelligence initiative aiming to proactively identify domains used in phishing, malware distribution, or other malicious activities. VirusTotal was selected for its reputation among threat analysts, its wide coverage of vendor feedback, and its ability to correlate domains with related files and network indicators.

- **Objective of the Tool Use:**

  VirusTotal: A free web service that compiles findings from more than 90 antivirus providers, community reports, website scanners, and sandbox settings.
  VirusTotal was used to:

  - Evaluate domain reputations.
  - Analyze URL behaviors and redirection patterns.
  - Identify IoCs such as file hashes, IP addresses, and associated subdomains.
  - Determine possible threat categories (e.g., phishing, malware hosting)

---

3. Methodology

3.1 Tool Configuration

- **VirusTotal Configuration:**
  - **Step 1: Go to https://www.virustotal.com to access VirusTotal** - Signing in is not required, but it is advised in order to access history and advanced features.
  - **Step 2: Provide the website**
    1. Click on the “URL” tab.
    2. Type the dubious URL into the search bar, such as http://aladel.net/.
    3. Press "Search" or "Enter."
  - **Step 3: Examine the Outcomes**
    - **a. The tab for detection**
      - Examine the detection rate (e.g., 9/96).
      - Determine the kinds of risks that have been flagged, such as malicious, phishing, and malware.
      - Make a note of the security providers that disclosed findings.
    - **b. Detail Tab**
      - Review the HTTP response, content type, redirection behavior and IP address
      - Check for signs of suspicious behavior
    - **c. Community Tab**
      - Examine comments and votes from the cybersecurity community
      - Pay attention to tags like phishing, C2 or ransomware
  - **Step 4: Contextualize the Threat**
    1. Compare flagged detections to: Vendor consensus (multiple vendors = more reliable)
    2. Community Score (strong negative score = high risk)
    3. Cross-reference with internal logs or other threat intelligence platforms.
  - **Step 5: Document and Report**
    1. Type of threat
    2. Technical indicators (URLs, IPs, behavior)
    3. Recommendations.

3.2 Execution Process

- **File Execution in Sandbox:**

Setup for URL Scanning:

- I input each domain into VirusTotal's URL scanner (17ebook.com, aladel.net, and clicnews.com).
- Output detection from the many URL reputation services and antivirus engines that were incorporated into VirusTotal.
- For details on IP resolves, redirects, and associated domains, we looked at the "Details" page.

Threat Intelligence Exploration:

- I visualized domain relationships with malware, phishing campaigns, and other cyberthreats using VirusTotal's "Relations" and "Graph" capabilities.
- looked over user feedback and thoughts about the domains on the "Community" tab.
- To determine whether the domains were connected to any known threat actors, I looked at the threat intelligence feeds.

Although VirusTotal's main focus is on file and URL analysis, it also uses behavioral analysis capabilities to understand how the domains interact with browsers and network resources. Communication with Command and Control servers was examined, and any redirects, file downloads, or JavaScript execution that might point to malicious activity were properly noted.

3.3 Monitoring and Analysis:

- **System Monitoring:**
  - The IP resolutions, redirects, and linked domains of the domains were detected and recorded by VirusTotal.
  - Data analysis was done to find any suspicious trends or links to known malicious infrastructure.
  - Careful consideration of any downloaded materials.

- **Network Monitoring:**
  - VirusTotal offered information about the network activity of the domains, including outgoing connections and efforts to get in touch with known malicious IP addresses or domains.
  - Information about connected domains and IP addresses was analyzed on the "Details" tab.
  - Correspondence between the examined domains and any additional domains was recorded.

4. Findings and Analysis

4.1 Indicators of Compromise (IOCs):

- **Detected IOCs:**
  - **For 17ebook.com :** Malicious- 6, Malware- 1, Phishing- 5, Clean- 46, Unrated- 26
  - **IOCs Report**

Categories	
alphaMountain.ai	Phishing (alphaMountain.ai)
BitDefender	education
Dr.Web	known infection source
Sophos	phishing and fraud
Webroot	Malware Sites
Forcepoint ThreatSeeker	parked domain

  - **For aladel.net :** Malicious- 2, Malware- 4, Phishing- 3, Suspicious- 1, Clean- 60, Unrated- 26
  - **IoC's REPORT**

Categories	
alphaMountain.ai	Phishing (alphaMountain.ai)
Xcitium Verdict Cloud	moderated forums
Sophos	phishing and fraud
Webroot	Phishing and Other Frauds
Forcepoint ThreatSeeker	compromised websites. parked domain

History	
First Submission	2010-08-11 20:54:18 UTC
Last Submission	2025-03-06 09:22:43 UTC
Last Analysis	2025-03-06 09:22:43 UTC

  - **For clicnews.com: Malicious- 1, Suspicious- 2, Clean- 60, Unrated- 16**
  - **IoC's REPORT**

Categories	
BitDefender	news
Forcepoint ThreatSeeker	compromised websites
Xcitium Verdict Cloud	moderated forums
alphaMountain.ai	News (alphaMountain.ai)

Popularity ranks		
Rank	**Position**	**Ingestion Time**
Statvoo	196158	2023-01-29 16:58:05 UTC
Alexa	196158	2023-01-29 16:58:03 UTC

4.2 Behavioral Analysis:

- **Malware Actions:** Since we're analyzing domains, we're not dealing with direct malware execution in the same way as a file. However, we can look at the potential behavior these domains could exhibit if they were used maliciously.
    - 17ebook.com, if used maliciously, could act as a distribution point for malware downloads. The flagged IPs suggest it might be involved in hosting malicious content.
    - aladel.net, with its redirects, could be used in phishing attacks, where users are redirected to fake login pages to steal credentials.
    - clicnews.com, with the mixed engine detections, and poor reputation of associated domains, could lead to drive-by downloads, or the hosting of malicious advertisements.

4.3 Risk and Impact Assessment:

- **Potential Impact:**
  Domains such as 17ebook.com and aladel.net present a moderate-to-high risk, given their associations with phishing and malware hosting. While clicnews.com showed limited direct threat, its history of compromise makes it a candidate for further monitoring.
        - Risk level: High
        - Threat Type: Phishing/Malware
        - Likelihood of User Compromise: Elevated
        - Potential Impact: Credential theft, Malware infection, C2 communication, User/device profiling.

---

5. Recommendations

5.1 Immediate Remediation Actions:

- Block the domain/IP on firewalls, proxy servers, and email gateways.
- Alert relevant teams if indicators appear in your environment.
- Monitor for further related indicators of compromise (IOCs)

- **Network Isolation:**
  Implement firewall rules to block all outbound traffic to malicious-domain.com.

5.2 Long-Term Mitigation:

- **Security Measures:**
  - Do not upload confidential/internal files to virusTotal (unless using the Private Enterprise instance)
  - Hash before uploading to check if it already exists in the database.
  - Regularly rotate the API key if there be any misuse detected or suspected.

---

6. Conclusion

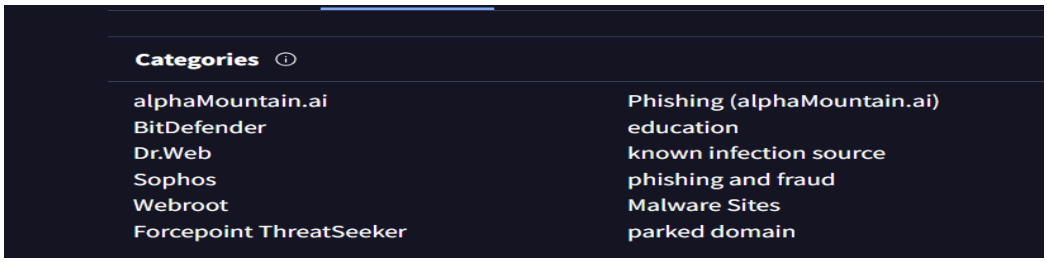
- **Summary of Findings:**
  The domain has a high likelihood of being part of a malicious campaign based on their detection across multiple vendors and their negative community score. Immediate preventive actions should be taken to mitigate risk and monitor for indicators of compromise related to the given domain.

- **Next Steps:**
  - Block URL at all perimeter and endpoint defence systems (firewall, proxies, DNS filters)
  - Blacklist the domain in web security gateways and SIEMs.
  - Alert security teams to investigate potential exposure or compromise.
  - Educate users about phishing domains and how to report suspicious links.

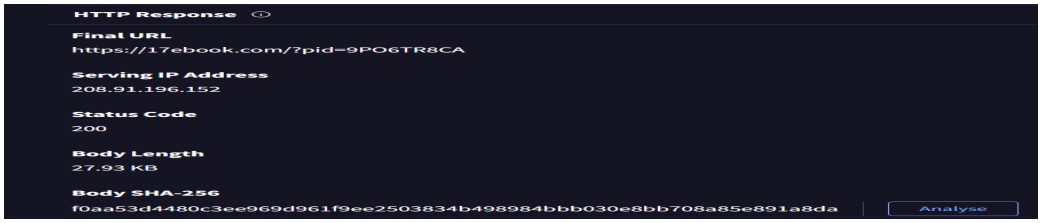
Appendix: Additional Data:

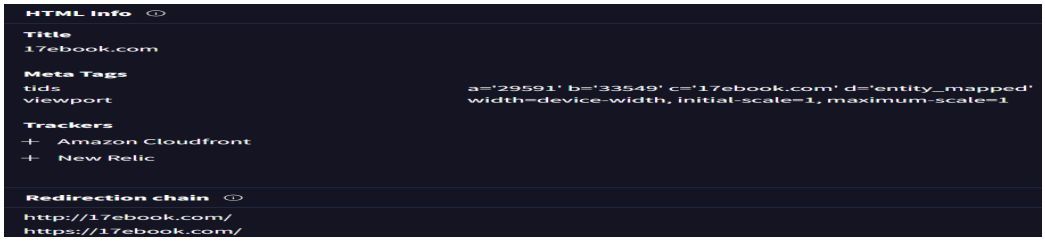
Step1: Access the VirusTotal website
Step2: Navigate to URL and type in the domain to be analyzed (17ebook.com)

Step3: Click enter to analyze

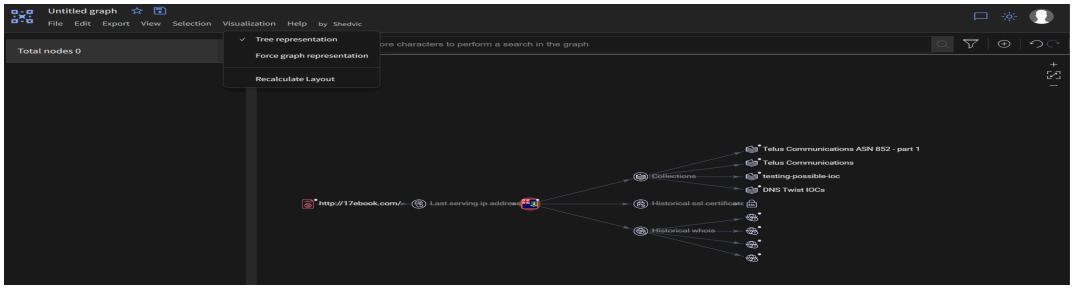


Below is the Network behavior showing serving IP address, URL and SHA



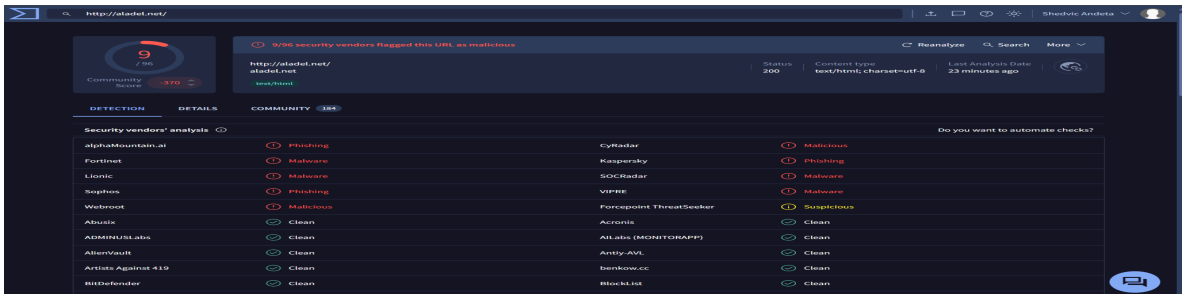


Step4: Navigating to the VirusTotal Graph, click on virtualization to display the Tree representation and Forced graph representation of the analysis.



Tree Representation

ANALYSIS ON (aladel.net) USING VIRUSTOTAL



OBSERVATIONS

The above analyzed interface shows that the URL Link: http://aladel.net/ has a Reputation Score of 9/96, it means about 9/96 security vendors who flagged this link as Malicious with a community score of – 370

IoC's REPORT

Categories

alphaMountain.ai	Phishing (alphaMountain.ai)
Xcitium Verdict Cloud	moderated forums
Sophos	phishing and fraud
Webroot	Phishing and Other Frauds
Forcepoint ThreatSeeker	compromised websites. parked domain

History

First Submission	2010-08-11 20:54:18 UTC
Last Submission	2025-03-06 09:22:43 UTC
Last Analysis	2025-03-06 09:22:43 UTC

HTTP Response

Final URL
http://survey-smiles.com/

Serving IP Address
185.107.56.57

Status Code
200

Body Length
1.07 KB

Body SHA-256
504819d0b32c3ccb7105e1c664f4655c7b4b7a0549cf91e8777ee257b8cab2cb

Headers

date	Thu, 06 Mar 2025 09:22:44 GMT
content-type	text/html; charset=utf-8
content-length	1094
x-request-id	46906e9a-cf50-4af2-a723-79ed92a336ab
cache-control	no-store, max-age=0
accept-ch	sec-ch-prefers-color-scheme
critical-ch	sec-ch-prefers-color-scheme
vary	sec-ch-prefers-color-scheme
x-adblock-key	MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_QxUn…
set-cookie	parking_session=46906e9a-cf50-4af2-a723-79ed92a336ab; expires=Thu, 06 Mar 2025 09:37:45 GMT; path=/

HTML Info

Meta Tags

viewport	width=device-width, initial-scale=1

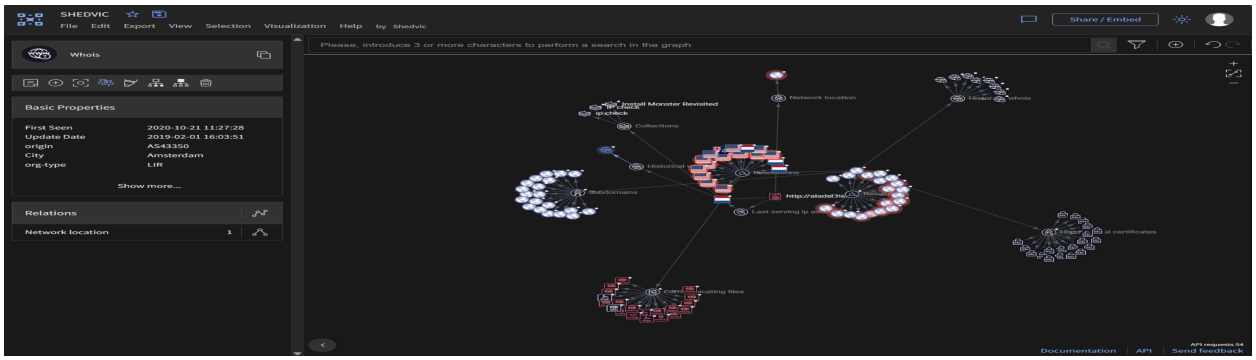
Trackers
New Relic

Cookies

parking_session	46906e9a-cf50-4af2-a723-79ed92a336ab

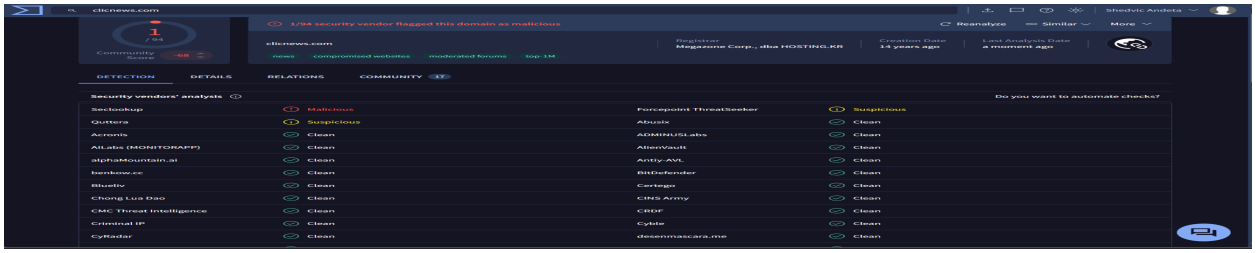
Redirection chain
http://aladel.net/

Navigating to VirusTotal Graph



Forced Graph Representation

ANALYSIS ON (clicnews.com) USING VIRUSTOTAL



OBSERVATIONS

The above analyzed interface shows that the URL Link: http://clicnews.com/ has a Reputation Score of 1/94, it means about 1/94 security vendors flagged this domain as Malicious with a community score of – 68

IoC's REPORT

Categories

BitDefender	news
Forcepoint ThreatSeeker	compromised websites
Xcitium Verdict Cloud	moderated forums
alphaMountain.ai	News (alphaMountain.ai)

Popularity ranks

Rank	Position	Ingestion Time
Statvoo	196158	2023-01-29 16:58:05 UTC
Alexa	196158	2023-01-29 16:58:03 UTC

Last DNS records

Record type	TTL	Value
A	3600	13.248.169.48
A	3600	76.223.54.146
NS	3600	ns1.namefind.com
NS	3600	ns2.namefind.com
SOA	3600	ns1.namefind.com
TXT	3600	v=spf1 -all