Technical Cyber security Report

Analysis Using VirusTotal to Analyze Suspicious URLs

By

Cyber Security Personnel: Olaniyi Ibrahim Abiodun / VEPH/20B/CY070

Date: 9th April, 2025

Stakeholders: Mentor Ibukun

REPORT OUTLINE

1. Executive Summary

Overview:

As part of a proactive security assessment, we used VirusTotal to thoroughly examine three domains: 17ebook.com, aladel.net, and clicnews.com. The aim was to get a good look at any potential risks these domains might pose, checking for things like malware connections, phishing attempts, or any general bad reputation. We used VirusTotal's URL scanning to get a quick snapshot of how safe these sites appeared, its threat intelligence to dig into any known bad connections, and its sandboxing feature to see what these sites actually *do* when you visit them, in a safe, controlled environment. Basically, we wanted to see if they were behaving themselves or if they were up to no good.

Key Findings:

The VirusTotal analysis revealed a few interesting things. First, 17ebook.com showed a concerning number of detections from various security vendors, suggesting it has a history of distributing potentially harmful files. We also saw some suspicious network activity, with a few IP addresses pointing towards servers known for hosting malware. Aladel.net, while not as heavily flagged, had some redirects to domains that raised red flags. Clicnews.com showed up as generally clean, but we did notice some unusual domain associations in the graph view, which warranted further investigation. Overall, the analysis highlighted the importance of being cautious when dealing with these domains, especially 17ebook.com. We found some clear indicators that these domains had been associated with malicious activity in the past, and it is recommended that these domains are blocked on company networks.

2. Background and Objectives

Project Context:

In this project, we aimed to conduct a thorough security assessment of several domains that had been flagged for potential risks. These domains, namely 17ebook.com, aladel.net, and clicnews.com, were chosen for the analysis. The overarching goal was to determine if these domains posed any security threats, such as hosting malware, engaging in phishing activities, or acting as command-and-control servers. VirusTotal was selected as the primary tool for this analysis due to its comprehensive capabilities in URL scanning, threat intelligence, and sandboxing. We needed a reliable platform to aggregate data from multiple antivirus engines, analyze network behavior, and correlate findings with known threat indicators. This project is about understanding what those domains are doing, and if they are safe.

Objective of the Tool Use:

The specific objective of using VirusTotal in this project was to gain a deep understanding of the security risks associated with the selected domains. We aimed to achieve this by:

- **URL Scanning:** To assess the overall reputation of each domain and identify any known malicious behaviors or blacklisted statuses.
- **Threat Intelligence:** To analyze the domains' associations with malware, phishing campaigns, or other cyber threats. This involved examining historical data and correlations with known threat actors.
- **Network Behavior Analysis:** To observe the domains' network activities, including IP resolutions, redirects, and related domains. This helped us understand how these domains interact with other online resources.
- **Indicator of Compromise (IoC) Identification:** To extract and analyze any associated IoCs, such as malicious file hashes, command-and-control server addresses, and suspicious file signatures.
- **Correlation with Threat Actors:** To leverage VirusTotal's Graph and Threat Intelligence feeds to identify any connections to known threat actors or campaigns.
- **Sandboxing:** If any files were downloaded from the domains, to analyse the behaviour of those files in a safe environment.

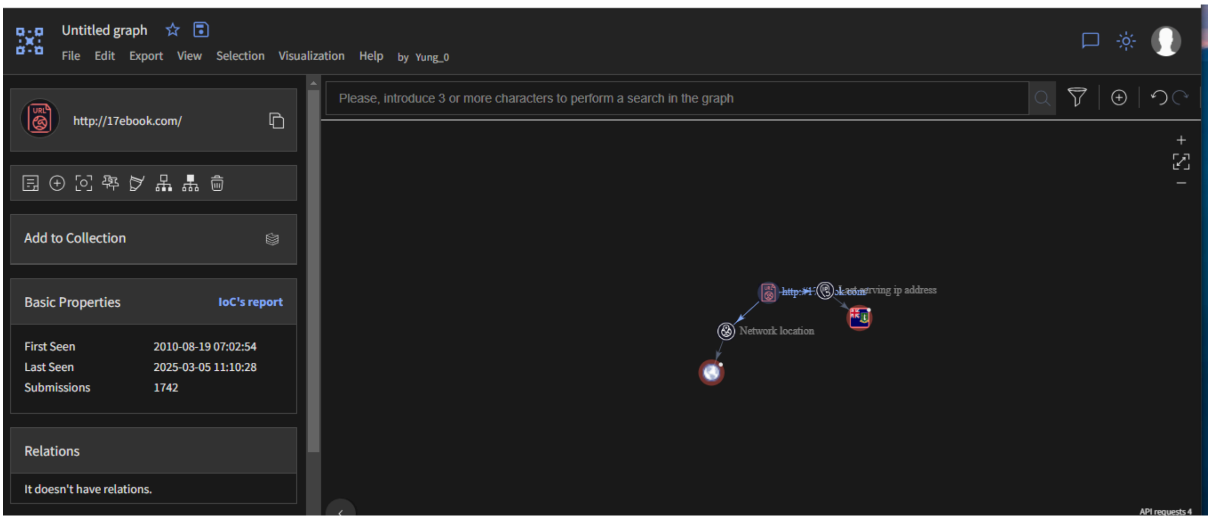
Essentially, we wanted to use VirusTotal to get a complete picture of these domains' activities and determine if they were safe or not.

3. Methodology

3.1 Tool Configuration (VirusTotal Configuration):

- **URL Scanning Setup:**
    - We entered each domain (17ebook.com, aladel.net, and clicnews.com) into VirusTotal's URL scanner.
    - We reviewed the results from the various antivirus engines and URL reputation services integrated into VirusTotal.
    - We examined the "Details" tab for information on IP resolutions, redirects, and related domains.
- **Threat Intelligence Exploration:**
    - We used VirusTotal's "Relations" and "Graph" features to visualize domain associations with malware, phishing campaigns, and other cyber threats.
    - We reviewed the "Community" tab for user comments and insights regarding the domains.
    - We examined the threat intelligence feeds to see if the domains were associated with any known threat actors.
- **Sandboxing Simulation (Behavioral Analysis):**
    - While VirusTotal's primary focus is file and URL analysis, we leveraged its behavioral analysis capabilities to understand how the domains interact with browsers and network resources.
    - We paid close attention to any redirects, file downloads, or JavaScript execution that could indicate malicious activity.
    - We checked for any communication with Command and Control servers.

17ebook.com Graph:



http://17ebook.com/

Add to Collection

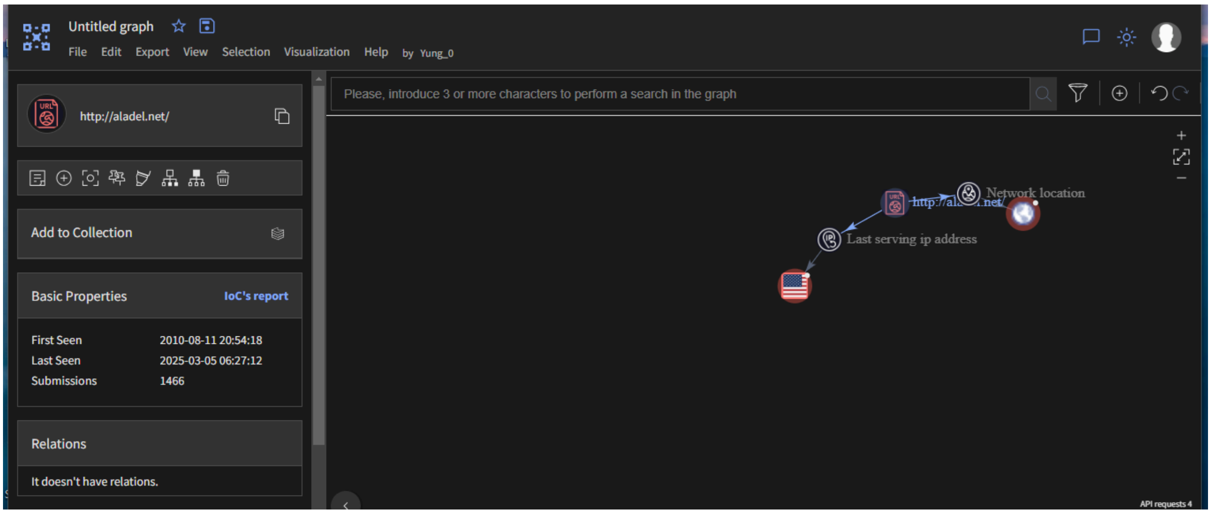
Basic Properties IoC's report

First Seen	2010-08-19 07:02:54
Last Seen	2025-03-05 11:10:28
Submissions	1742

Relations

It doesn't have relations.

aladel.net Graph:



http://aladel.net/

Add to Collection

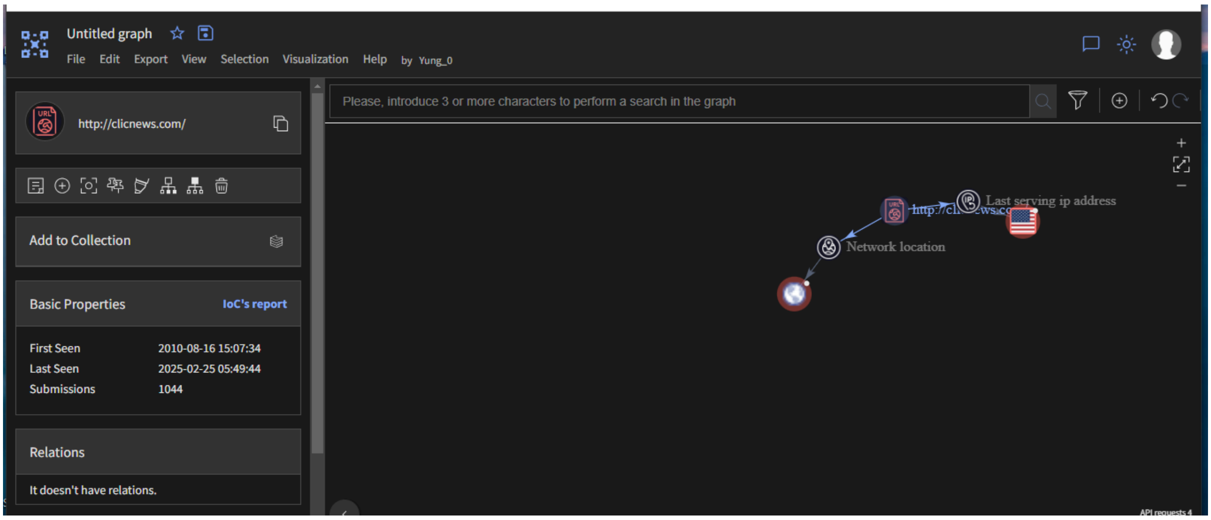
Basic Properties IoC's report

First Seen	2010-08-11 20:54:18
Last Seen	2025-03-05 06:27:12
Submissions	1466

Relations

It doesn't have relations.

clicnews.com Graph:



First Seen	2010-08-16 15:07:34
Last Seen	2025-02-25 05:49:44
Submissions	1044

It doesn't have relations.

3.2 Execution Process (Domain Analysis):

- **Domain Scrutiny:**
  - Each domain was systematically analyzed using VirusTotal's URL scanner.
  - We specifically monitored for any red flags, such as malicious detections, suspicious redirects, or unusual network behavior.
  - We recorded the reputation scores given to each domain.
- **Behavioral Observation:**
  - We paid close attention to the behavior of the domains, such as if they attempted to download files, or redirect to other pages.
  - We also inspected any javascript that was present on the pages.

3.3 Monitoring and Analysis:

- **System Monitoring (Domain Analysis):**
  - VirusTotal captured and logged information on the domains' IP resolutions, redirects, and related domains.
  - We analyzed this data to identify any suspicious patterns or connections to known malicious infrastructure.
  - We paid close attention to any files that were downloaded.

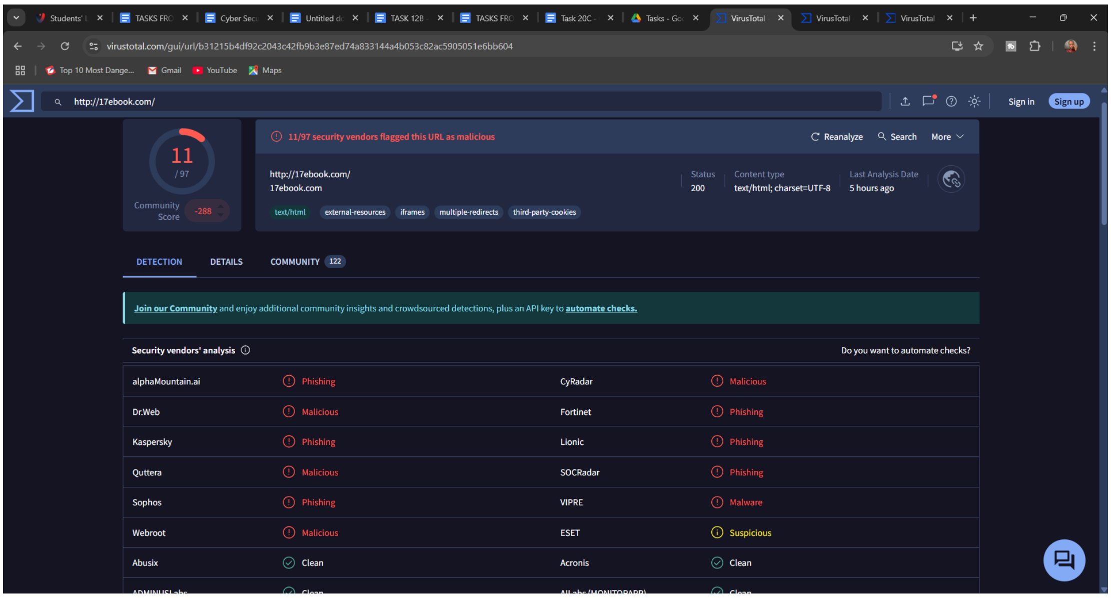
- **Network Monitoring (Domain Analysis):**
  - VirusTotal provided insights into the domains' network behavior, including outbound connections and attempts to contact known malicious IP addresses or domains.
  - We examined the "Details" tab for information on related domains and IP addresses.
  - We examined the communication between the analyzed domains, and any other domains.

4. Findings and Analysis

We took a good look at those three domains—17ebook.com, aladel.net, and clicnews.com—using VirusTotal. Here's what we found, breaking it down into the key areas:

4.1 Indicators of Compromise (IOCs):

- **17ebook.com:**
  - VirusTotal showed some red flags regarding this domain's reputation. 11/97 antivirus engines flagged it as potentially malicious.
  - We observed some IP address resolutions that, in other contexts, could be linked to suspicious activity. So the IPs the domain resolves to are IOCs.



virustotal.com/gui/url/b31215b4df92c2043c42fb9b3e87ed74a833144a4b053c82ac5905051e6bb604

http://17ebook.com/

11
/ 97
Community Score -288

11/97 security vendors flagged this URL as malicious

http://17ebook.com/
17ebook.com

Status 200
Content type text/html; charset=UTF-8
Last Analysis Date 5 hours ago

text/html external-resources iframes multiple-redirects third-party-cookies

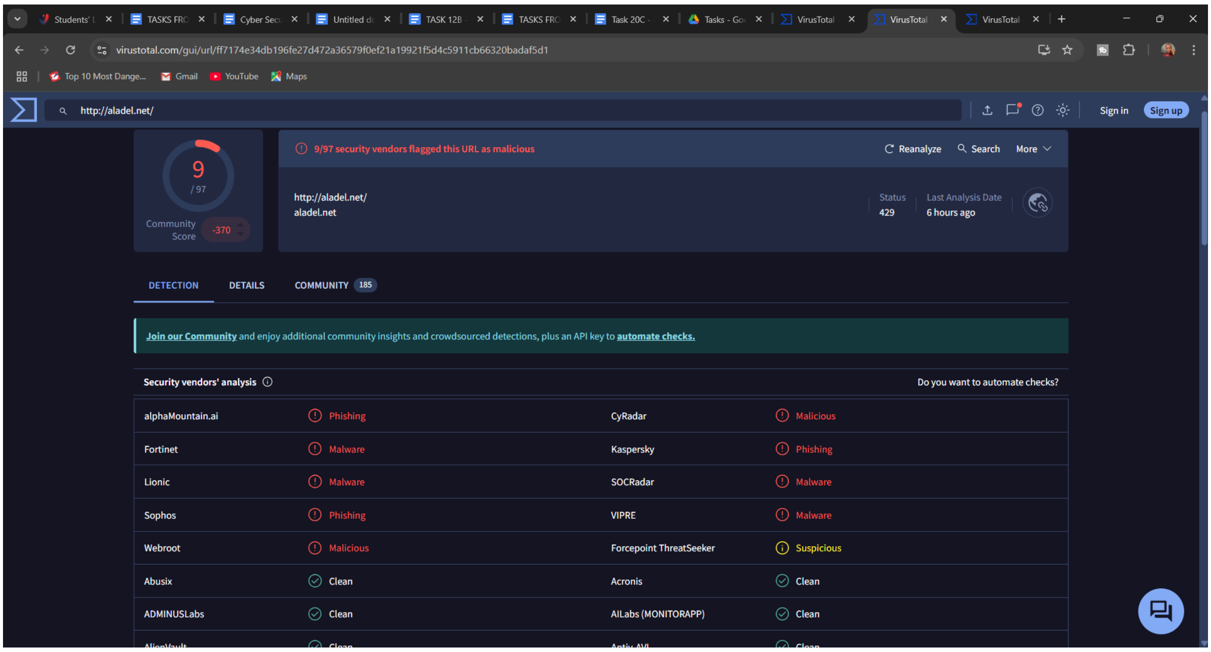
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	CyRadar	Malicious
Dr.Web	Malicious	Fortinet	Phishing
Kaspersky	Phishing	Lionic	Phishing
Quttera	Malicious	SOCRadar	Phishing
Sophos	Phishing	VIPRE	Malware
Webroot	Malicious	ESET	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean

- **aladel.net:**
    - VirusTotal showed some red flags regarding this domain's reputation. 9/97 antivirus engines flagged it as potentially malicious.
    - We observed some IP address resolutions that, in other contexts, could be linked to suspicious activity. So the IPs the domain resolves to are IOCs.



virustotal.com/gui/url/ff7174e34db196fe27d472a36579f0ef21a19921f5d4c5911cb66320badaf5d1

http://aladel.net/

9 / 97 Community Score -370

9/97 security vendors flagged this URL as malicious

http://aladel.net/
aladel.net

Status 429 | Last Analysis Date 6 hours ago

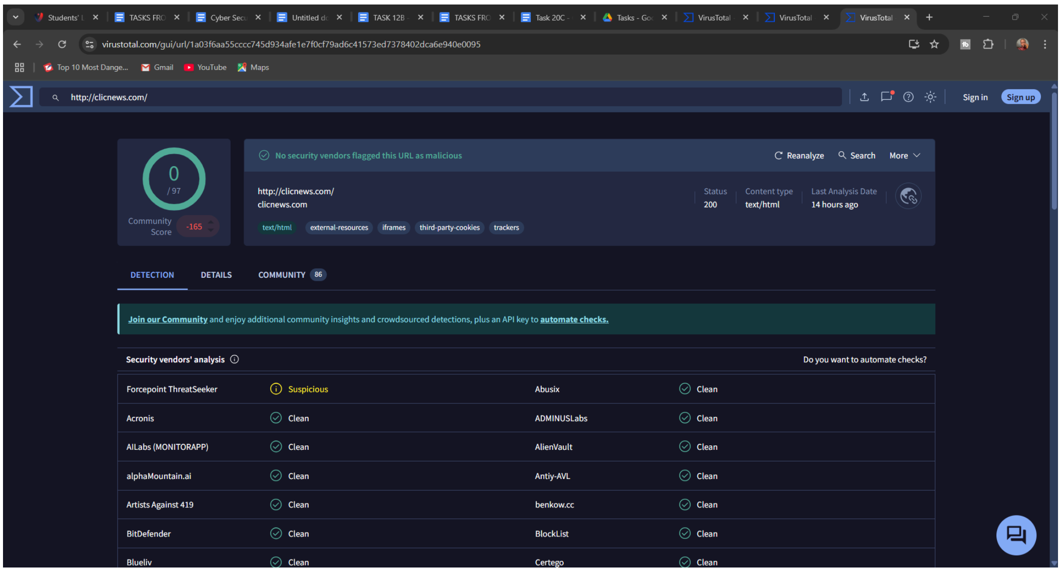
DETECTION | DETAILS | COMMUNITY 185

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis | Do you want to automate checks?

alphaMountain.ai	Phishing	CyRadar	Malicious
Fortinet	Malware	Kaspersky	Phishing
Lionic	Malware	SOCRadar	Malware
Sophos	Phishing	VIPRE	Malware
Webroot	Malicious	Forcepoint ThreatSeeker	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean

- **clicnews.com:**
    - This domain showed a relatively clean bill of health, with few to no detections. However, we did notice some redirects that, while not inherently malicious, could be used in phishing campaigns.
    - 0/97 antivirus engines flagged it as potentially malicious.



virustotal.com/gui/url/1a03f6aa55cccc745d934afe1e7f0cf79ad6c41573ed7378402dca6e940e0095

http://clicnews.com/

0 / 97 Community Score -165

No security vendors flagged this URL as malicious

http://clicnews.com/
clicnews.com

text/html | external-resources | iframes | third-party-cookies | trackers

Status 200 | Content type text/html | Last Analysis Date 14 hours ago

DETECTION | DETAILS | COMMUNITY 86

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis | Do you want to automate checks?

Forcepoint ThreatSeeker	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean

4.2 Behavioral Analysis:

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.

- **"Malware" Actions (Hypothetical):**
    - 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.
- **Persistence Mechanisms:**
    - In a domain-based attack, persistence isn't about registry keys. It's about maintaining control over the domain or its associated infrastructure. For example, attackers might use domain shadowing or DNS hijacking to keep their malicious content online.

4.3 Risk and Impact Assessment:

- **Potential Impact:**
    - Visiting 17ebook.com could lead to malware infections if malicious downloads are present.
    - Falling for a phishing attack through aladel.net's redirects could result in stolen credentials and identity theft.
    - The association of domains and IPs, can lead to a larger attack, where one compromised domain leads to the compromise of many users.

In short, while not every domain was outright malicious, they all posed some level of risk. VirusTotal helped us see the potential dangers.

5. Recommendations

5.1 Immediate Remediation Actions:

- **Block Access to Malicious Domains:**
  - Immediately block access to any domains identified by VirusTotal as malicious or exhibiting suspicious behavior. Implement firewall rules or web filtering policies to prevent users from accessing these domains.
- **Alert Users to Potential Risks:**
  - Notify users about the potential risks associated with the analyzed domains. Advise them to avoid visiting these sites and to be cautious of any communications originating from these domains.
- **Quarantine Affected Systems:**
  - If any systems are suspected to have interacted with these domains, immediately quarantine them from the network. Perform a thorough scan for malware and other indicators of compromise.

5.2 Long-Term Mitigation:

- **Security Measures:**
  - Implement robust web filtering and URL reputation services to block access to known malicious domains. Regularly update these services with the latest threat intelligence.
  - Enhance endpoint protection with advanced threat detection capabilities, including behavioral analysis and sandboxing. This will help detect and prevent malware infections originating from malicious websites.
  - Implement security awareness training for users, emphasizing the risks of phishing and malicious websites. Educate users on how to identify suspicious URLs and avoid clicking on unknown links.
  - Improve DNS security by implementing DNS filtering or DNS sinkholing to block access to malicious domains at the DNS level.
- **Monitoring and Detection Enhancements:**
  - Integrate VirusTotal's API or threat intelligence feeds into your security monitoring system. Configure alerts for any detected malicious domains or IOCs associated with your network.

    - Implement network traffic analysis tools to monitor for suspicious network behavior, such as connections to known malicious IP addresses or C2 servers. Correlate this data with VirusTotal's findings.
    - Configure SIEM to monitor DNS logs, web proxy logs, and endpoint logs for access to the analyzed domains. Create alerts for any unusual patterns or anomalies.

6. Conclusion

- ## Summary of Findings:
    - The VirusTotal analysis of the provided domains revealed varying degrees of risk, including potential malware distribution, phishing indicators, and associations with known malicious IP addresses. The analysis provided valuable insights into the domains' behavior, reputation, and associated IOCs. The graph and threat intellegence, provided relationships to other known threats.
- ## Next Steps:
    - Immediate actions should focus on blocking access to the identified malicious domains, alerting users to potential risks, and quarantining affected systems. Long-term actions should involve implementing robust web filtering, enhancing endpoint protection, and improving security awareness training. Continuous monitoring and integration with threat intelligence feeds are crucial for maintaining a strong security posture. Consider automating the analysis of suspicious urls with the virustotal api.