LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 20D

RE: UTILYZING VIRUSTOTAL IN DETECTING, ANALYZING AND CONTAINING MALICIOUS DATA

**TASK OBJECTIVES**

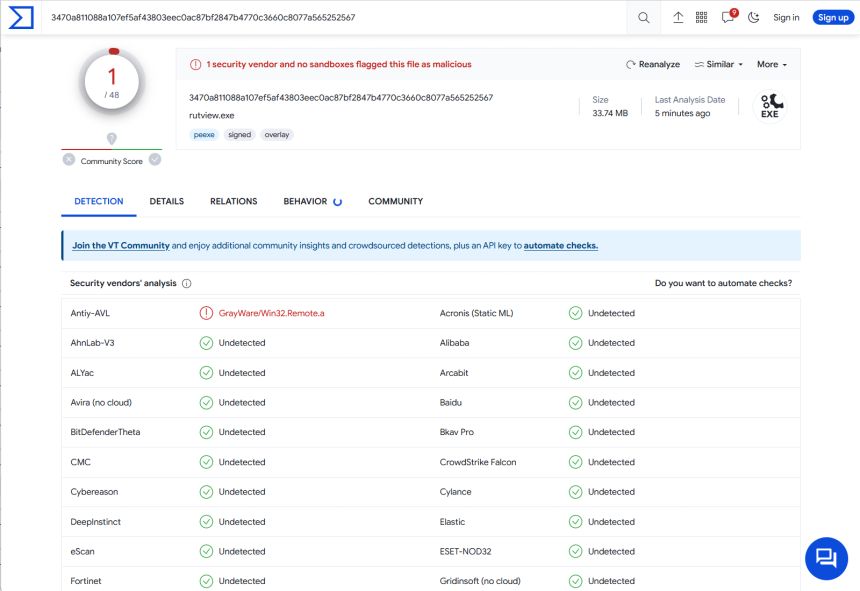
* **Perform a comprehensive technical analysis** of the following domains using **VirusTotal**:

1. 17ebook.com
2. aladel.net
3. clicnews.com

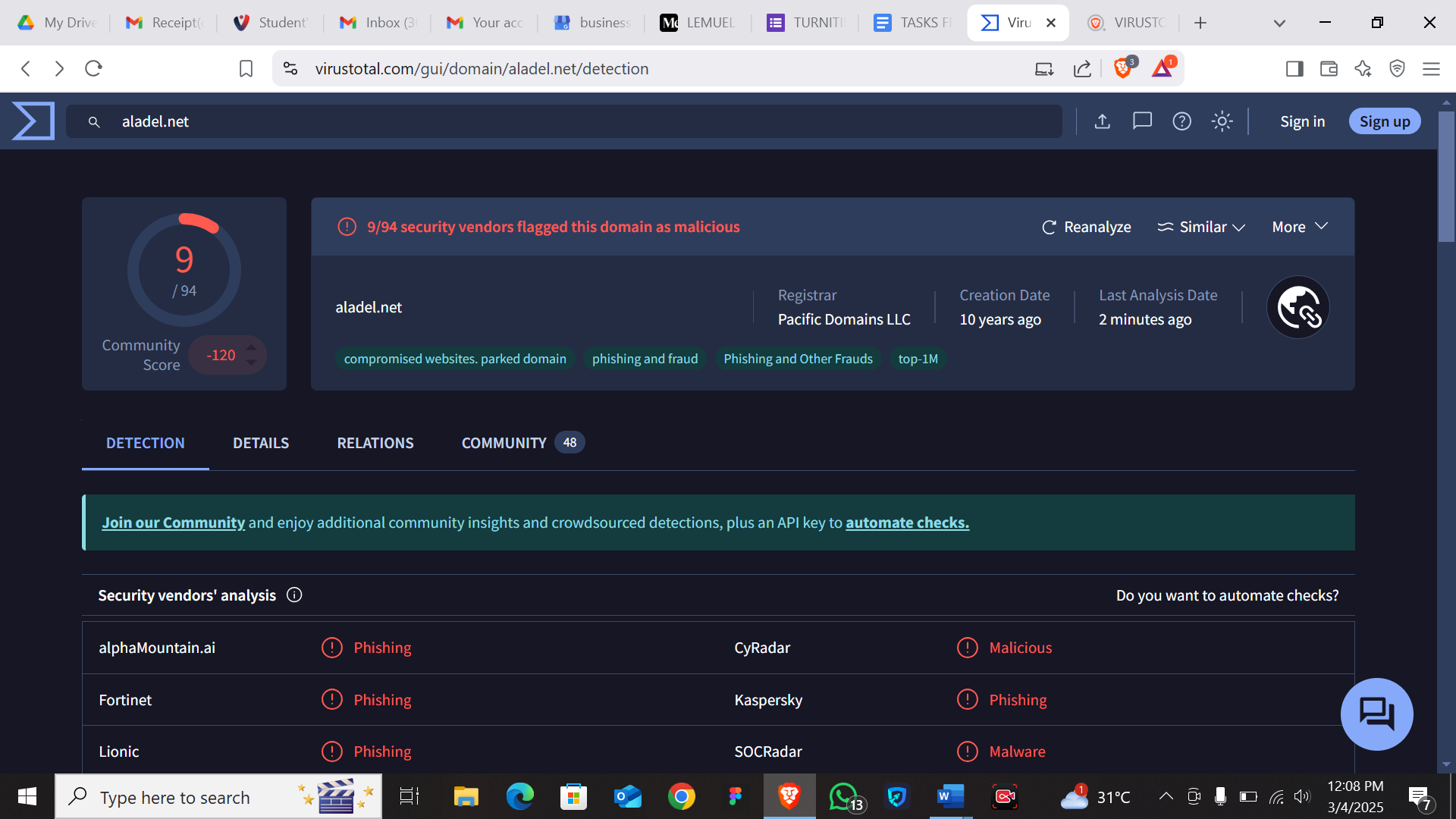
* **Utilize VirusTotal's capabilities**, including:

1. **URL scanning** to detect potential malicious behavior and reputation scores.
2. **Threat intelligence** to analyze domain associations with malware, phishing, or other cyber threats.
3. **Sandboxing** to observe dynamic execution and behavioral indicators.

* **Compile a detailed technical report**, including:
* **Detected threats** such as malware, phishing indicators, or blacklisted status.
* **Network behavior** analysis, including IP resolutions, redirects, and related domains.
* **Associated Indicators of Compromise (IoCs)** like malicious hashes, C2 servers, and file signatures.
* **Correlations with known threat actors or campaigns**, leveraging VirusTotal’s **Graph and Threat Intelligence feeds**.
* **Screenshots and structured data** from VirusTotal to support finding

[](https://www.remoteutilities.com/blog/is-virustotal-the-right-tool/)

VirusTotal is an online service that analyzes files and URLs to detect viruses, worms, trojans, and other malicious content using antivirus engines and website scanners. It is a free service with numerous useful features such as, storing all the analyses it performs, allowing users to search for file hashes. By sending the hash to the VirusTotal engine, searchers can know if VirusTotal has already scanned that specific file, and can analyze its report. Also, it provides an API that allows access to the information generated by VirusTotal without needing to utilize the HTML website interface. This API is subject to its Terms of Service, which we briefly discuss in the following section.



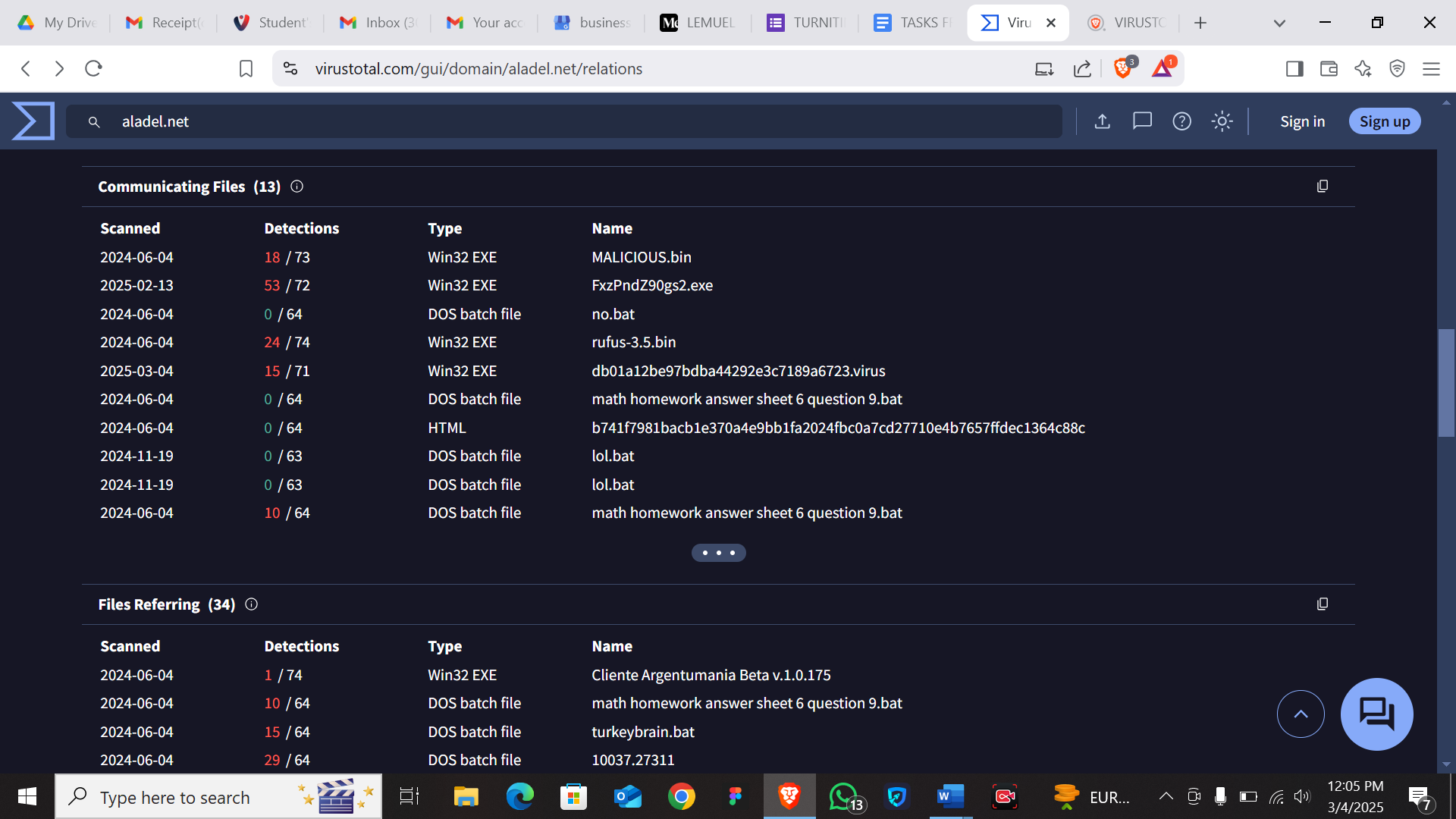
**File name:** aladel.net

**Observation:** Dangerous phishing malware that steals IP addresses

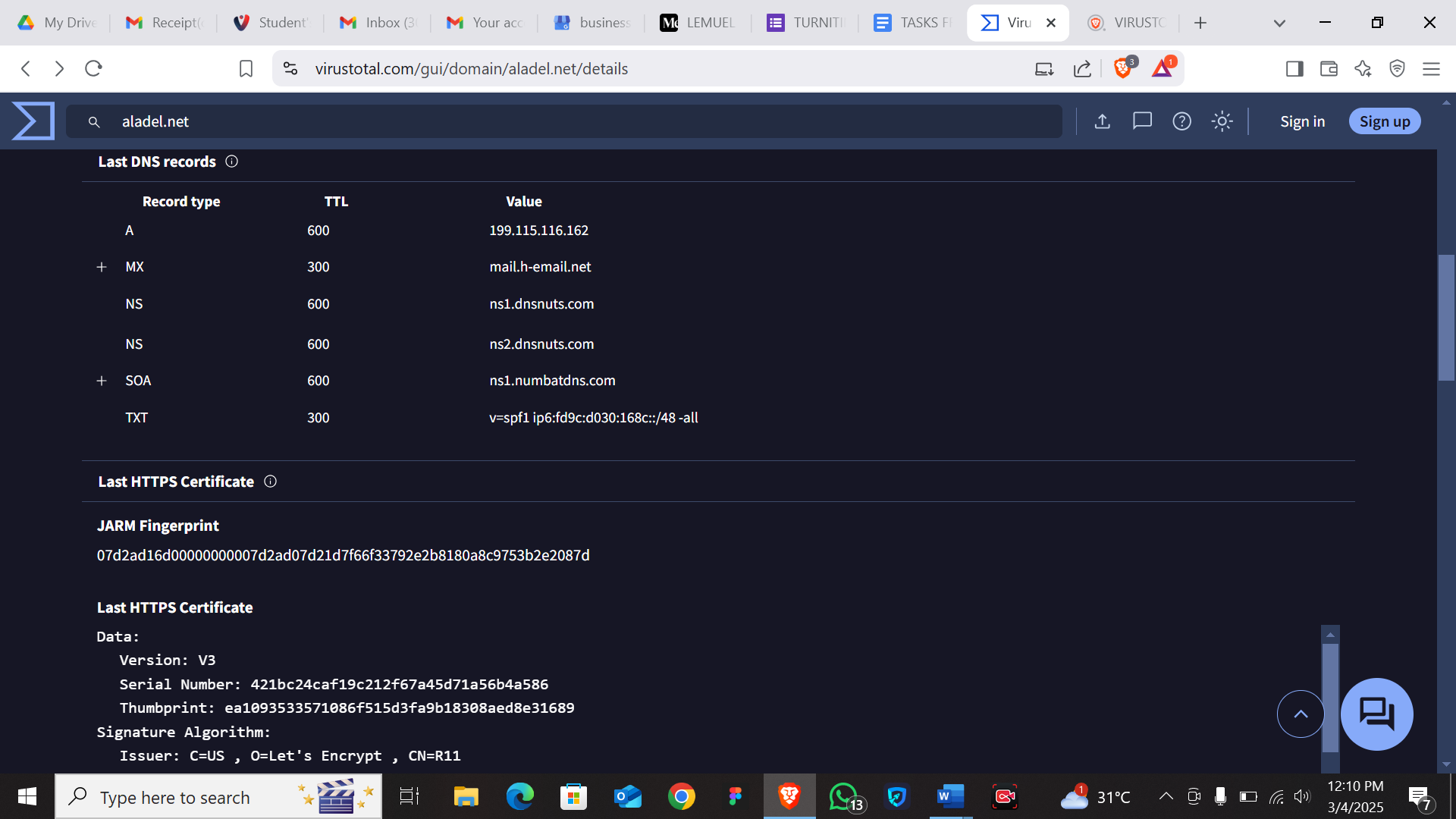
**Description**: compromised website/domain laced with phishing and fraud

**Threat**: 9/94

**Analysis**: 3 min ago

**Behavior**: 

IOCs:



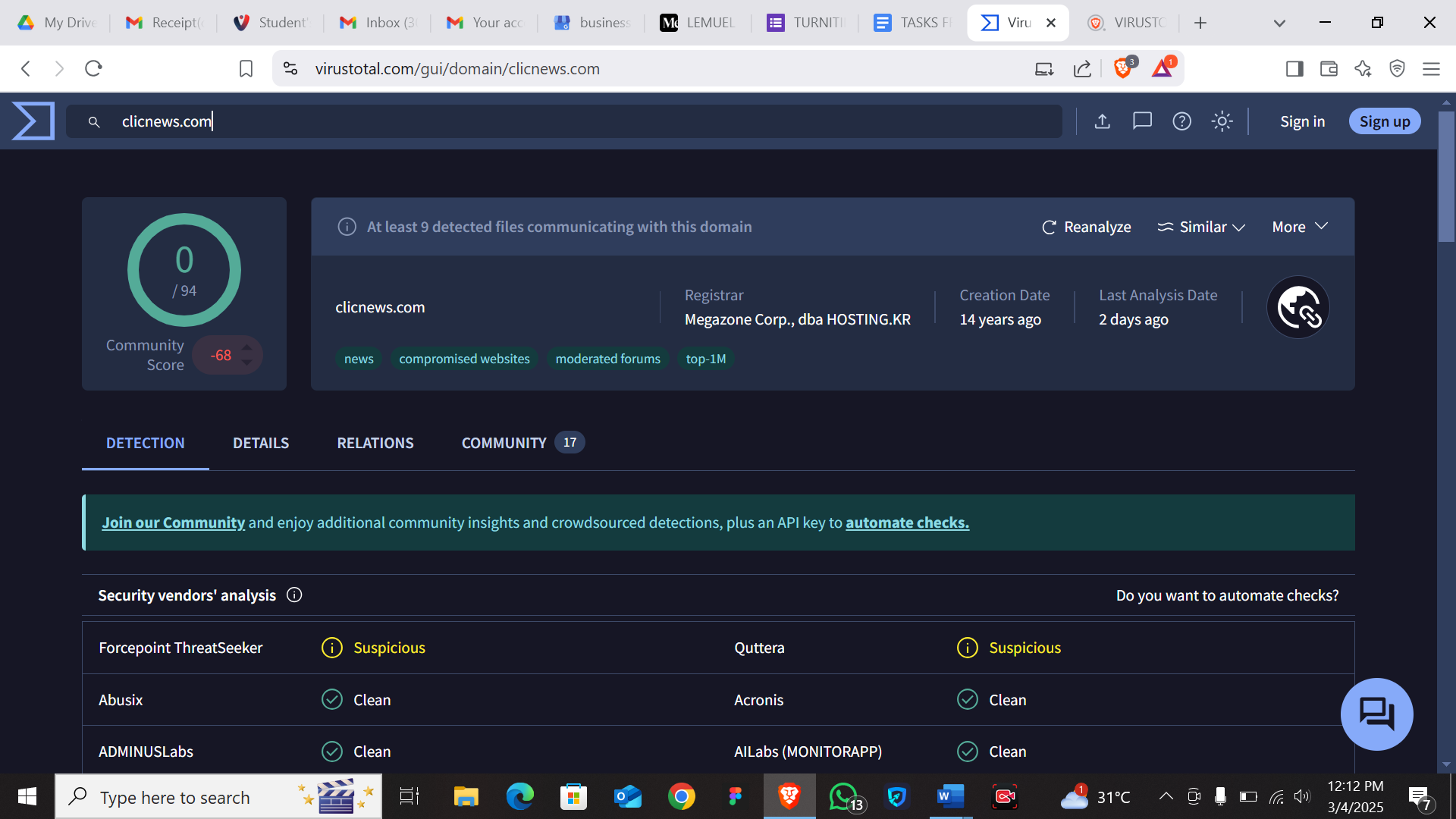
**File name**: clicnews.com

**Observation:** compromised malicious website with the threat level minimal. Once the website is opened, it redirects you to alphamountain.ai

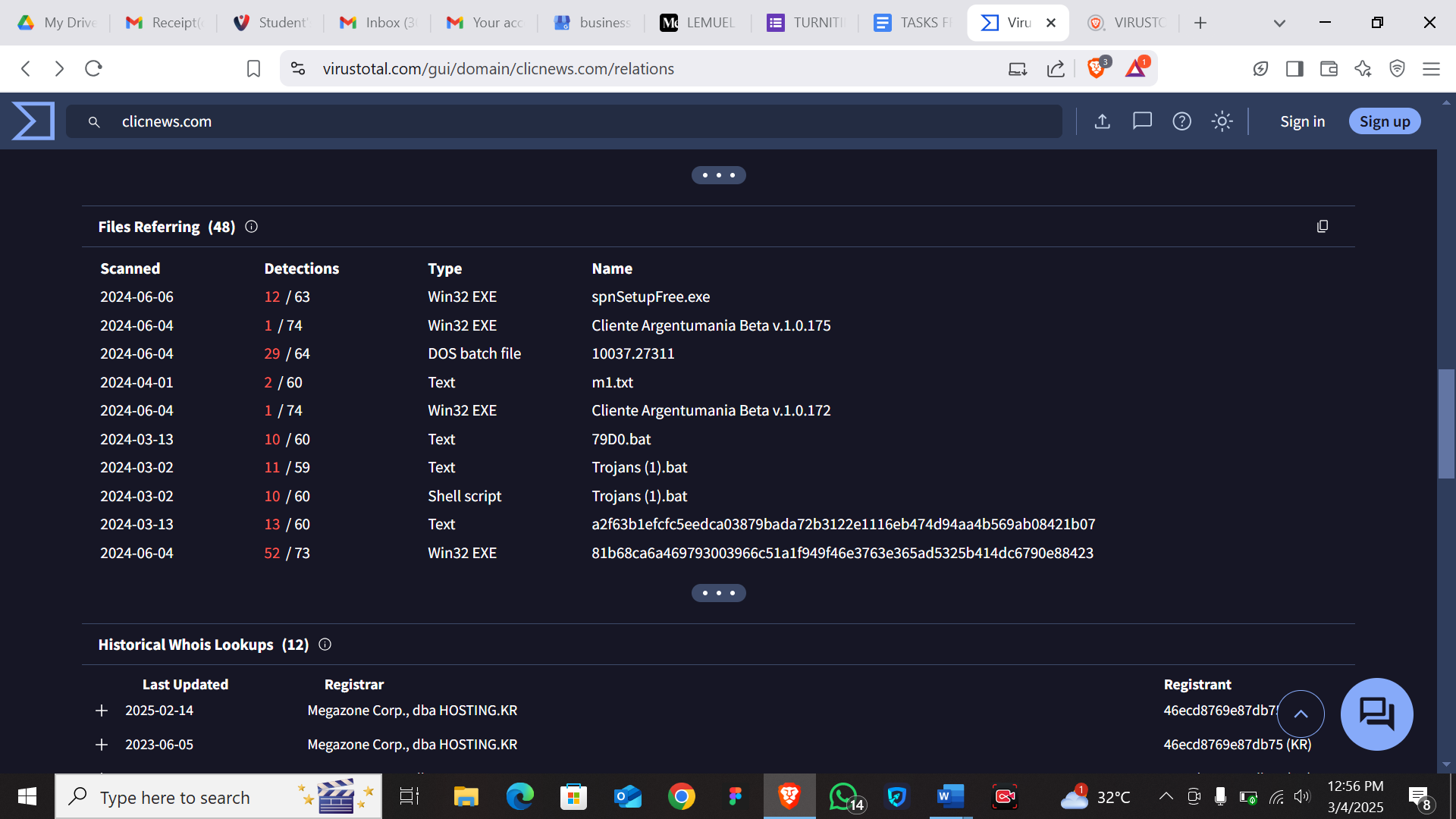
**Description**: it is a news website that was affected through a malicious mail which almost ruined its credibility but was later resolved.

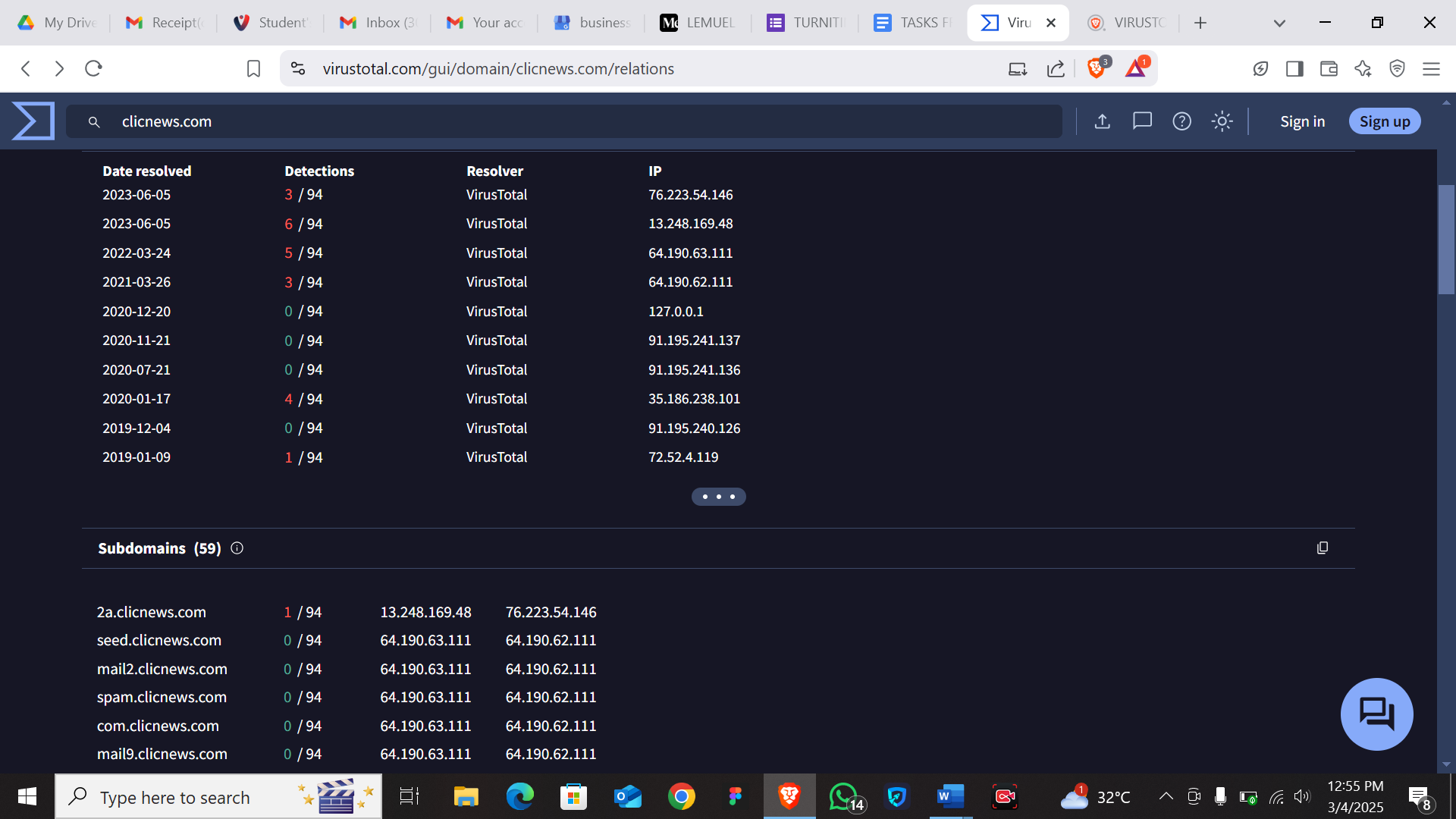
**Threat**: 1/94

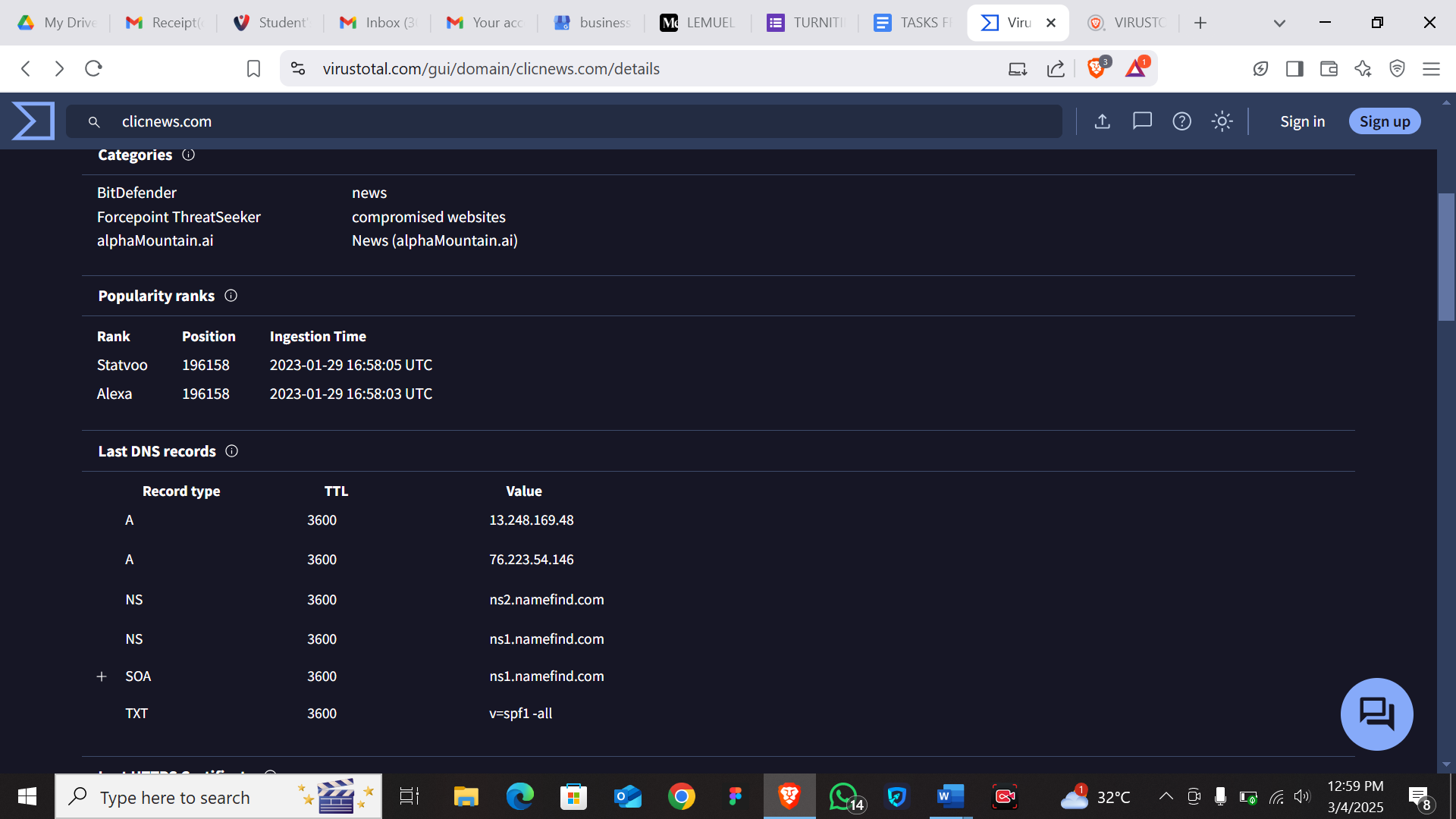
**Analysis:** 1 min ago

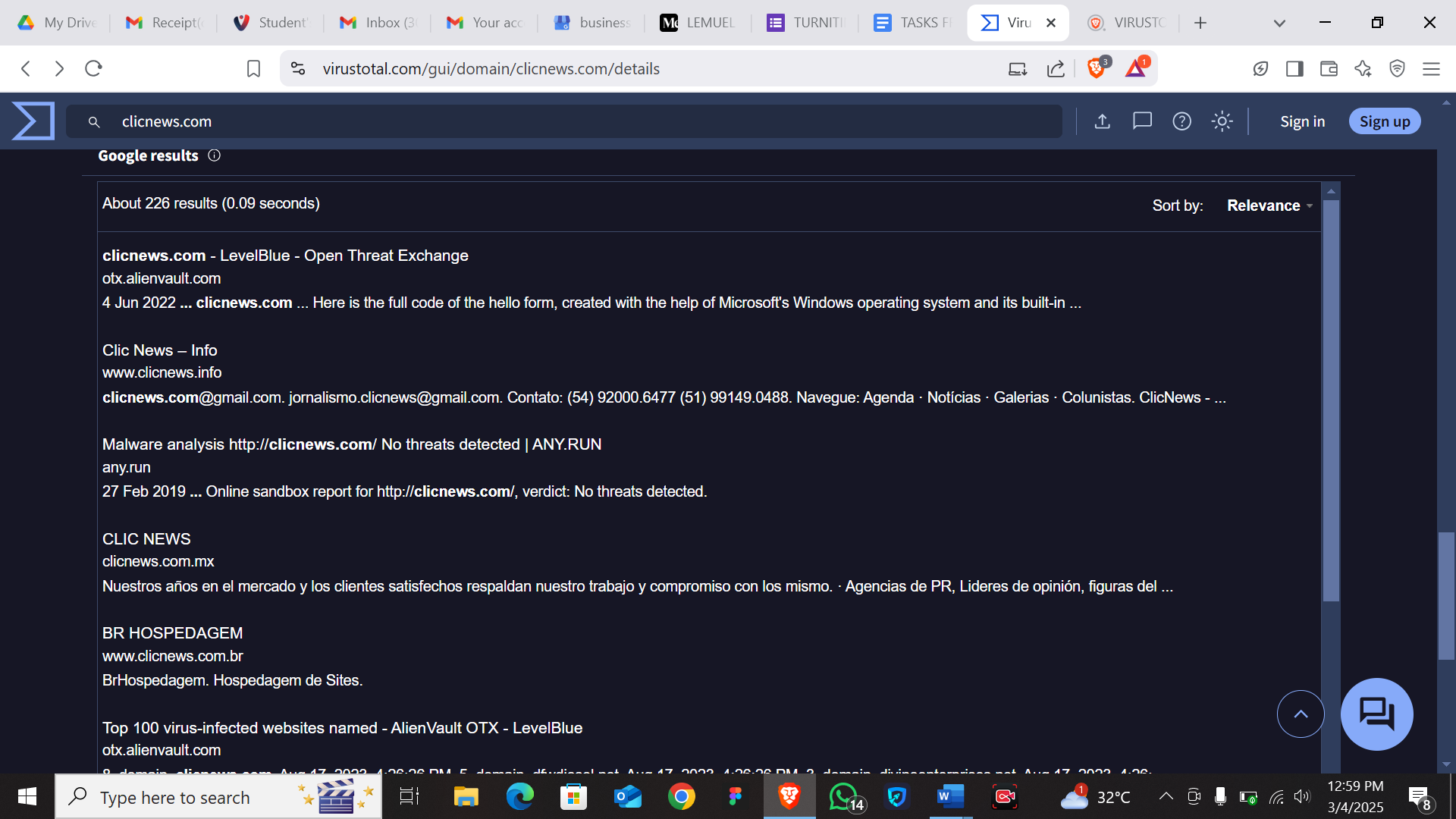


**Behavior**:





**IOCs**: 



[*"New CNMF initiative shares malware samples with cybersecurity industry > U.S. Cyber Command > News"*](https://web.archive.org/web/20200930004308/https:/www.cybercom.mil/Media/News/Article/1681533/new-cnmf-initiative-shares-malware-samples-with-cybersecurity-industry/)*. www.cybercom.mil. Archived from*[*the original*](https://www.cybercom.mil/Media/News/Article/1681533/new-cnmf-initiative-shares-malware-samples-with-cybersecurity-industry/)*on 30 September 2020. Retrieved 22 February 2022.*