Phishing Email Investigation Methodology

1. Tools & Setup

- **Notepad++**
  - Open the email header in Notepad++.
  - For better formatting and readability:
    - Go to **Languages → YAML** → headers and fields will be highlighted.
  - This makes it easier to analyze fields during phishing investigations.
- **OSINT Tools**
  - VirusTotal
  - DomainTools
  - WHOIS lookups
  - Other open-source intelligence platforms

2. Methodology: *"What to Look For"*

When investigating phishing emails, focus on these **key fields**:

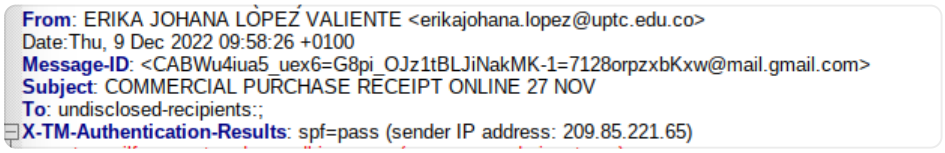
- **From**: Sender's display name and email address
- **To**: Recipient (sometimes "undisclosed-recipients")
- **Subject**: Subject line of the email
- **Message-ID**: Unique identifier; the domain shows the mail service used
- **Date**: Timestamp of when the email was sent
- **Received**: Mail servers that processed the message (infrastructure clues)
- **Authentication-Results**: SPF, DKIM, DMARC results
- **Return-Path**: Often used to spot spoofing attempts

> **Note:** With more investigations, you'll refine and build your own methodology.

3. Step-by-Step Analysis (Case Example)

Header Analysis

- **From:** `ERIKA JOHANNA LOPEZ <erikajohana.lopez@upt.edu.co>`



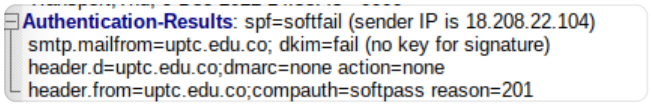
- **To:** `undisclosed-recipients` (recipient hidden)
- **Subject:** `COMMERCIAL PURCHASE RECEIPT ONLINE 27 NOV`
- **Message-ID:** Ends with `@mail.gmail.com` → indicates Gmail delivery system
- **Date:** `Thu, 9 Dec 2022 09:58:26 +0100`

Received Field

- First receiving mail server domain: `@fsfb.org.co`
- OSINT can be used here to learn about attacker infrastructure.

Authentication-Results

- SPF → **Fail**
- DKIM → **Fail**
- DMARC → **Fail**
- Suggests spoofing or poor configuration.



Return-Path

- `erikajohana.lopez@uptc.edu.co` (slightly different domain than From)
- Common tactic in phishing → mismatched Return-Path vs From.

4. Body Analysis

- Text: "COMMERCIAL PURCHASE RECEIPT" with reference to **625,000 pesos**.
- Hyperlink present:

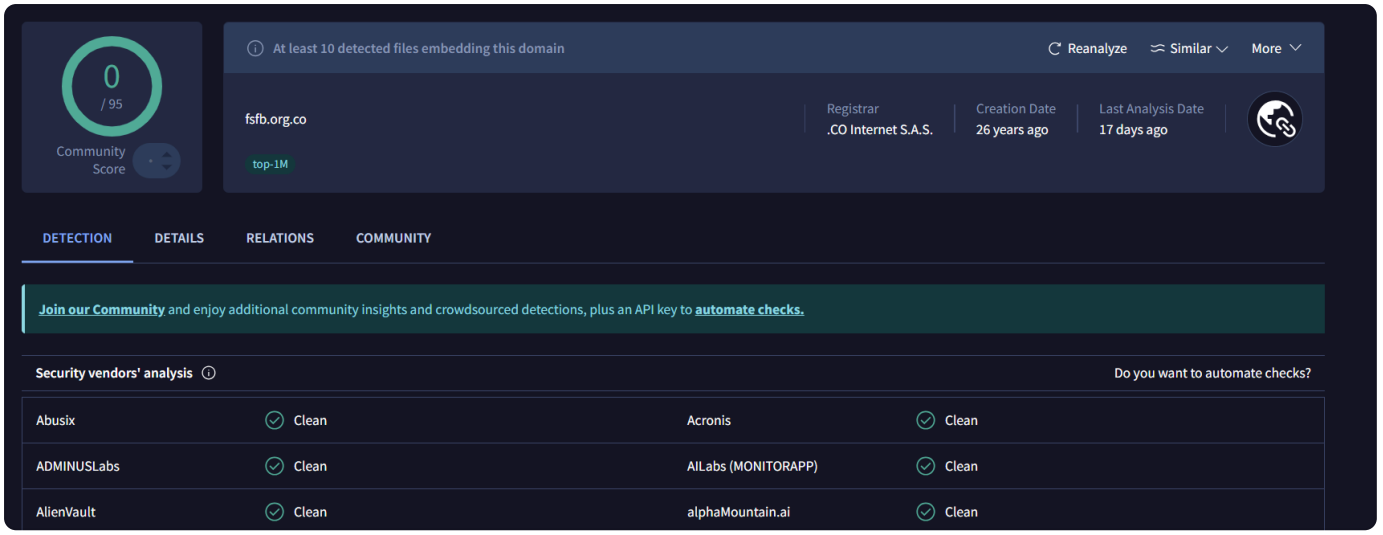
```
http://107.175.247.199/loader/install.exe
```

- → Suspicious file download (likely malware).

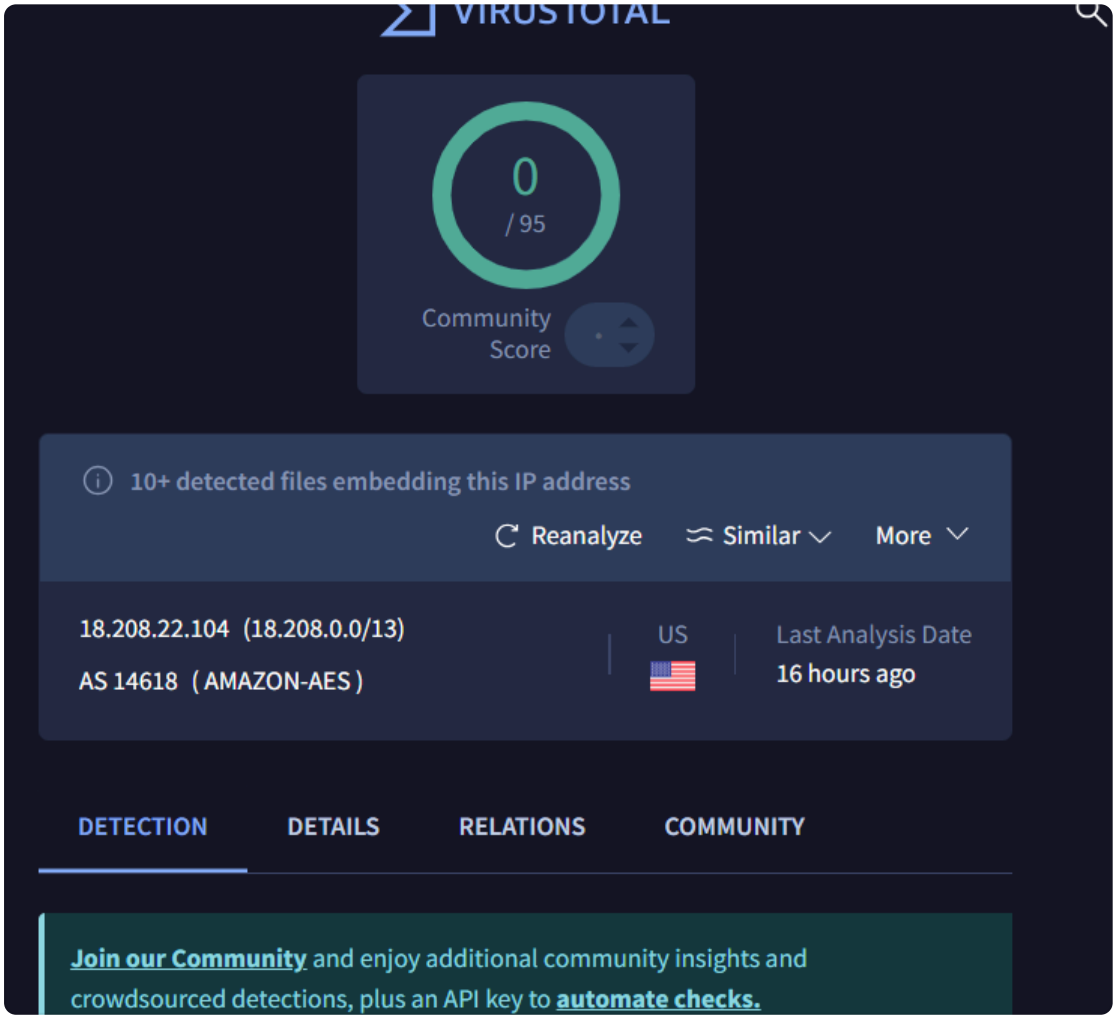
5. Next Steps (OSINT & Threat Hunting)

- **Check the domain & IP** on **VirusTotal**
- Look for related phishing/malware campaigns
- Verify sender domains with WHOIS/DomainTools
- Map infrastructure (IP, domain, hosting provider)
- Document findings for reporting and defense

Using **VirusTotal** to scan the **domain** from the **Received** field, we can see that this domain was created **26 years ago**. While an **old domain** is generally less suspicious than a newly registered one, it does not automatically mean the email is legitimate, because attackers can compromise older domains for phishing campaigns. If the domain were **newly created**, it would be a strong indicator of potential phishing, prompting a deeper investigation. Additional checks are necessary to confirm the email's legitimacy.

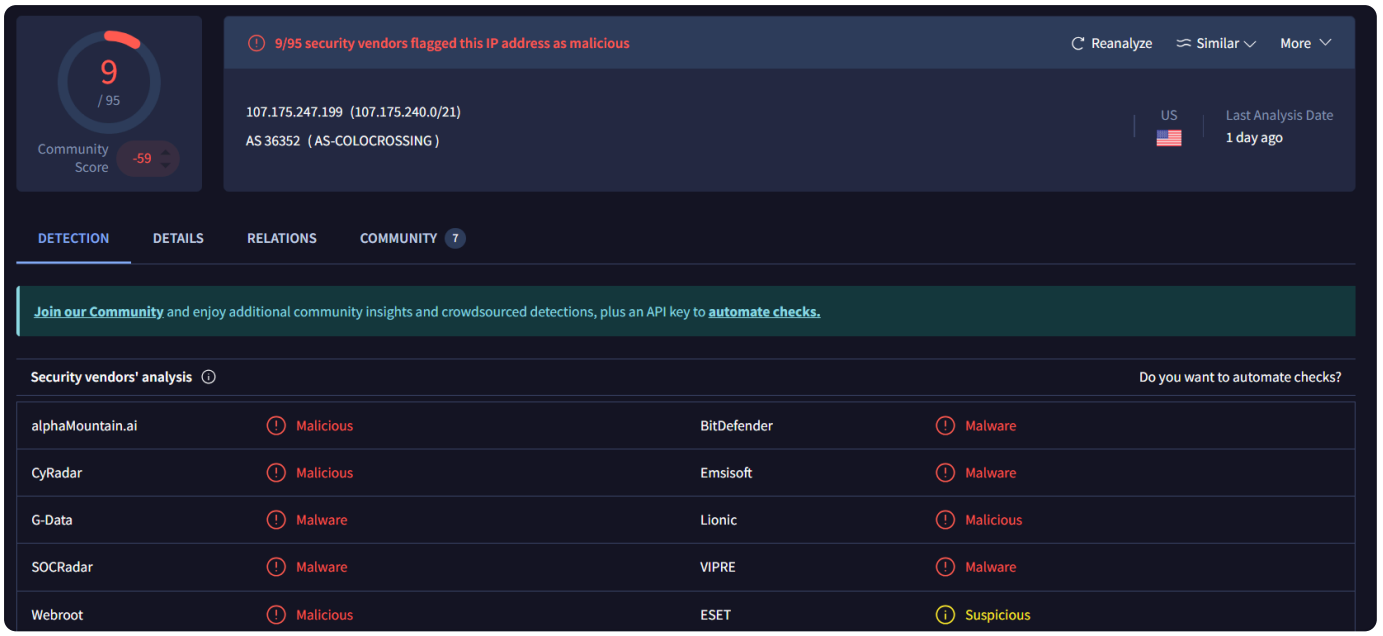


Further analysis of the **Authentication-Results** shows that the sender's **IP address** is **18.208.22.104**. VirusTotal indicates that this IP belongs to **Amazon AWS**, which is commonly used for hosting and email delivery. While the IP itself is not inherently malicious, attackers sometimes abuse cloud services like AWS to send phishing emails. Therefore, we should **not block the IP outright**, as it could disrupt legitimate traffic. Instead, this information serves as a **pivot point for investigation**, helping analysts identify potential abuse without affecting overall availability.



Lastly, we can analyze the **link in the body of the email** using **VirusTotal**. It is often helpful to first examine the **IP address** associated with the link before pasting the full URL. From the IP check, we can see that **9 out of 95 vendors** reported it as **malicious malware**, which already raises a red flag about the link's safety.

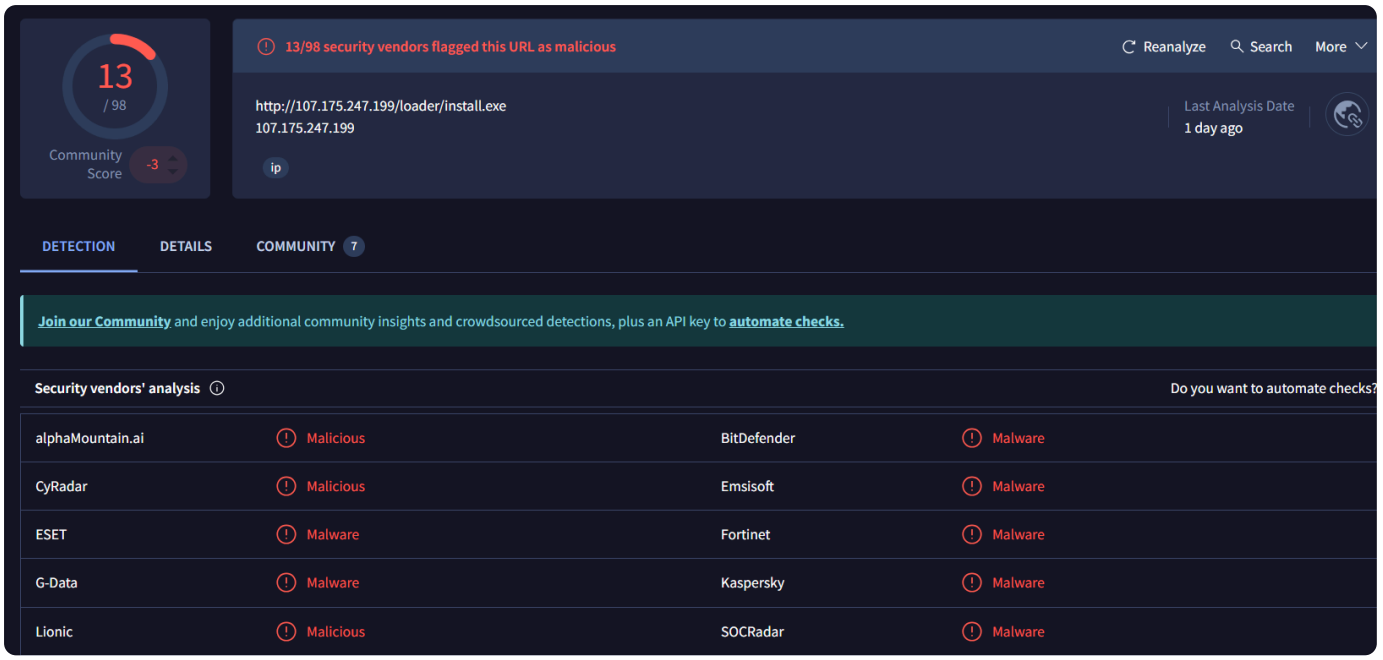
If you click on relations, you will get more information on the IP. There you will see the files communicating with that IP address under communicaing file whicgh resulted in 6 binaries.



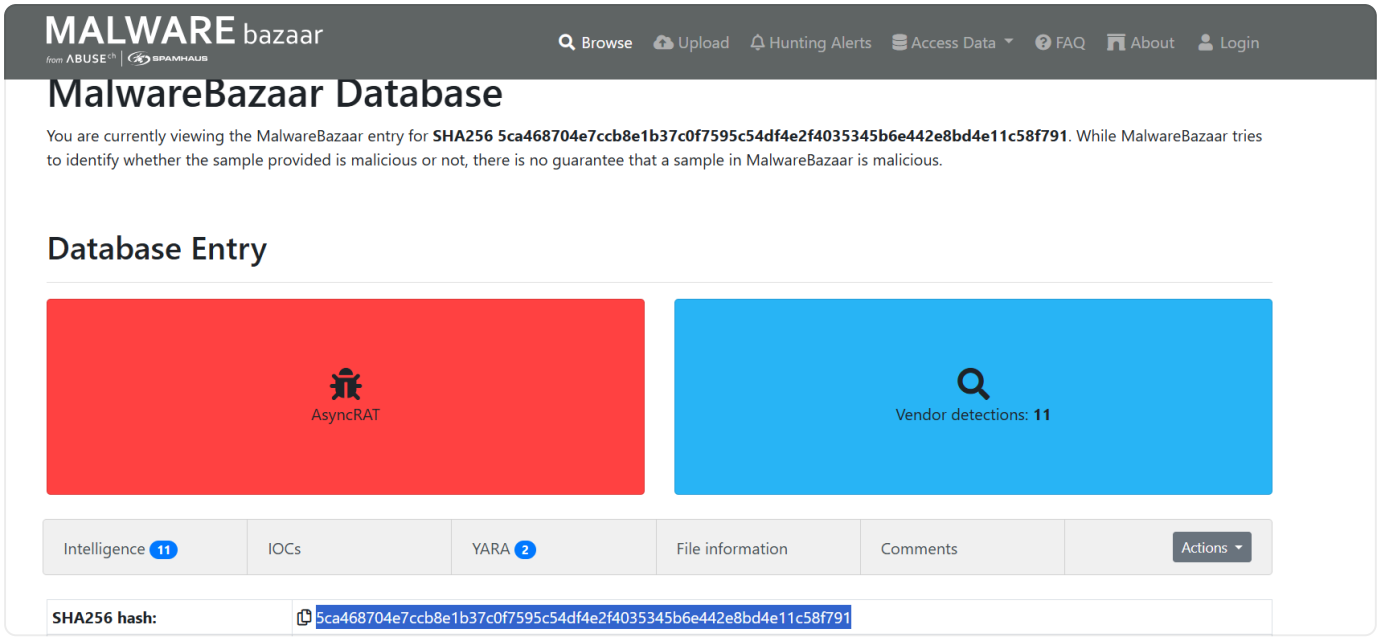
Checking the Details, you will see more information on that. Looking at Abuse.ch, it is quite interesting , more informations can be gotten from taht . click on teh URI of the Abuse.ch to get further analysis on taht .

Next, by pasting the **complete URL** `http://107.175.247.199/loader/install.exe` into VirusTotal, we find that **13 out of 98 vendors** flagged it as **malicious malware**. This confirms that the link is indeed dangerous and likely part of a phishing or

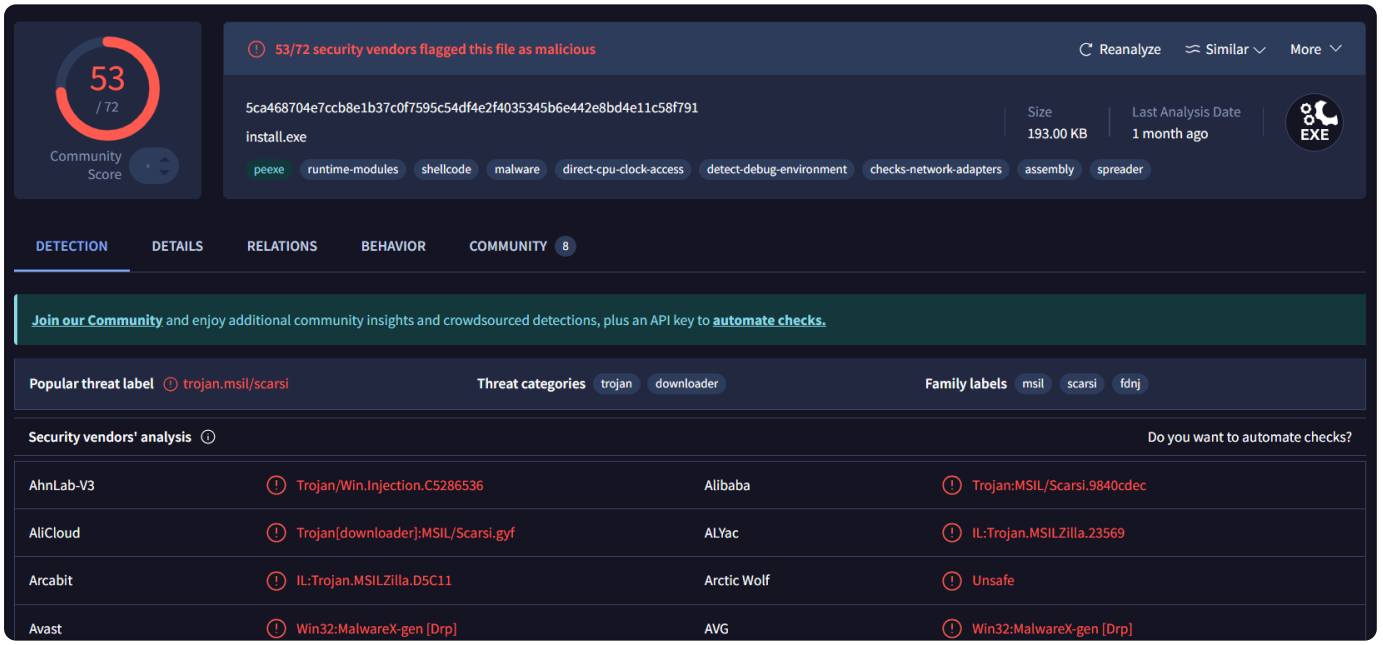
malware campaign, reinforcing the need for caution and further investigation before interacting with any content from this email.



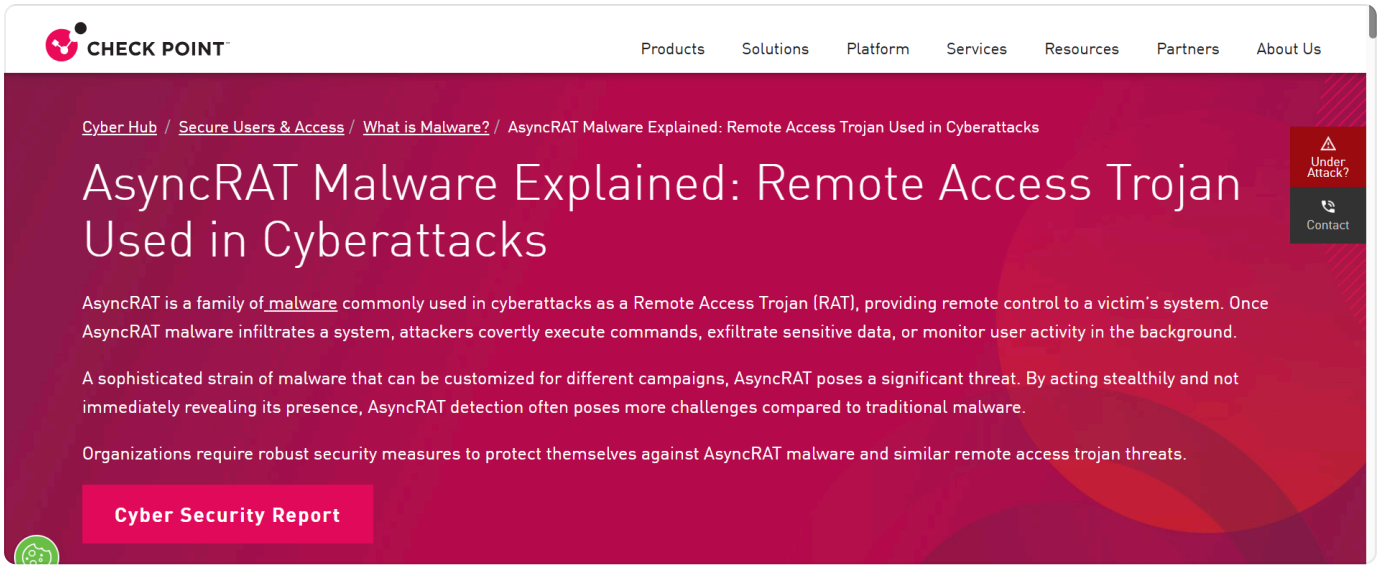
When analyzing the file in **VirusTotal**, clicking on the **Community** and **Details** sections provides additional insights. Under the **Details** tab, the **Google Results** indicate that the file is classified as **malware**. By following the link to **Abuse.ch**, we can confirm that this malware is tagged as **AsyncRAT** and **RAT**. Further research shows that **AsyncRAT** is a **Remote Access Trojan (RAT)** commonly used in cyberattacks to gain unauthorized control of compromised systems.

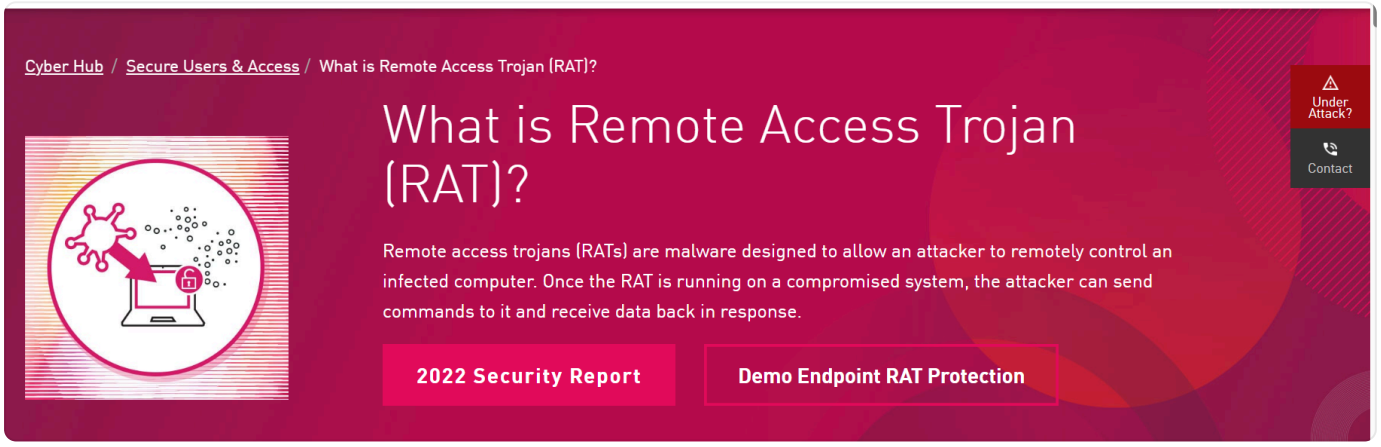


If we take the **file hash** and paste it into VirusTotal, we see that **53 out of 72 vendors** have flagged it as a **Trojan**. Additional open-source searches confirm that **AsyncRAT** is indeed a **remote access tool** used by attackers for persistent access, surveillance, and data exfiltration.



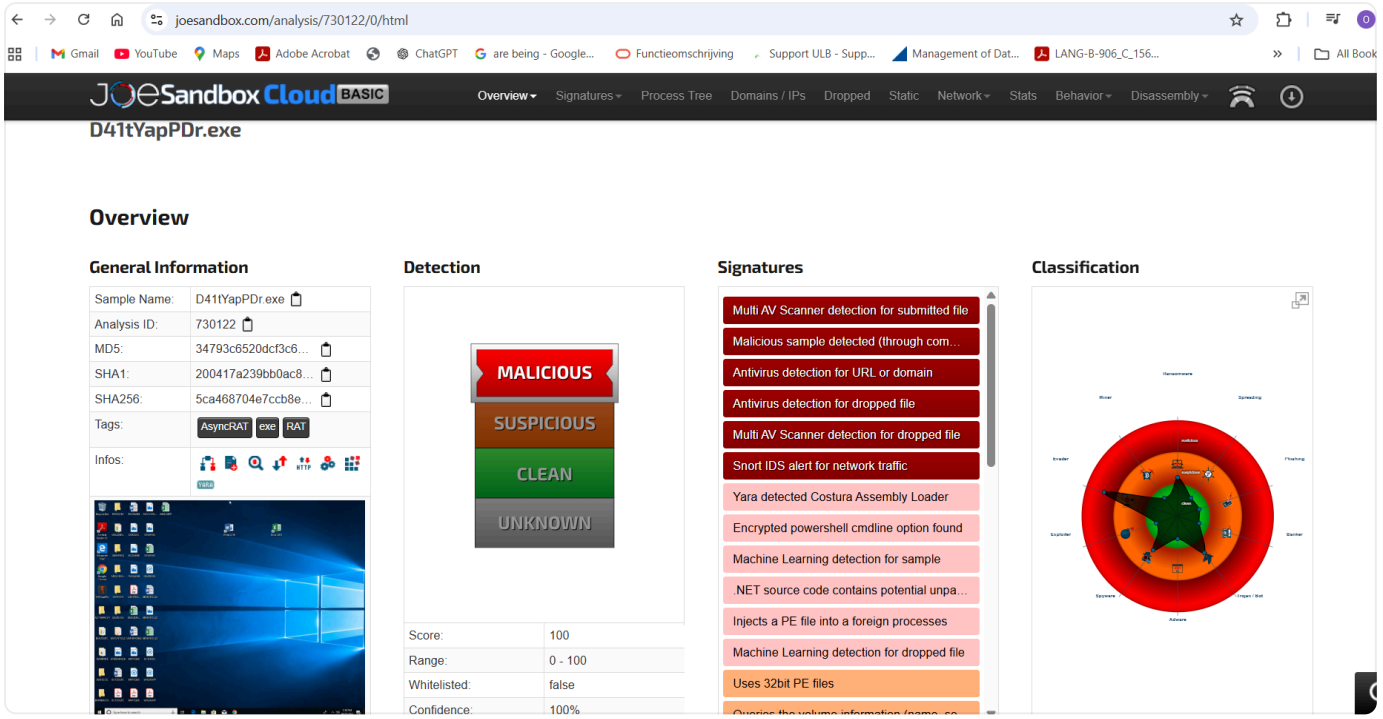
Looking at the **Community section** in VirusTotal, we can also see various comments and shared reports from other analysts. In particular, highlighting the **HTML analysis report** gives us a deeper look into the malware's behavior. For instance, under the **Process Tree**, we find suspicious command-line activity. Decoding the embedded **Base64 command** using **CyberChef** reveals that the malware forces the system to **start, then sleep for 5 seconds**—a technique often used to evade detection.





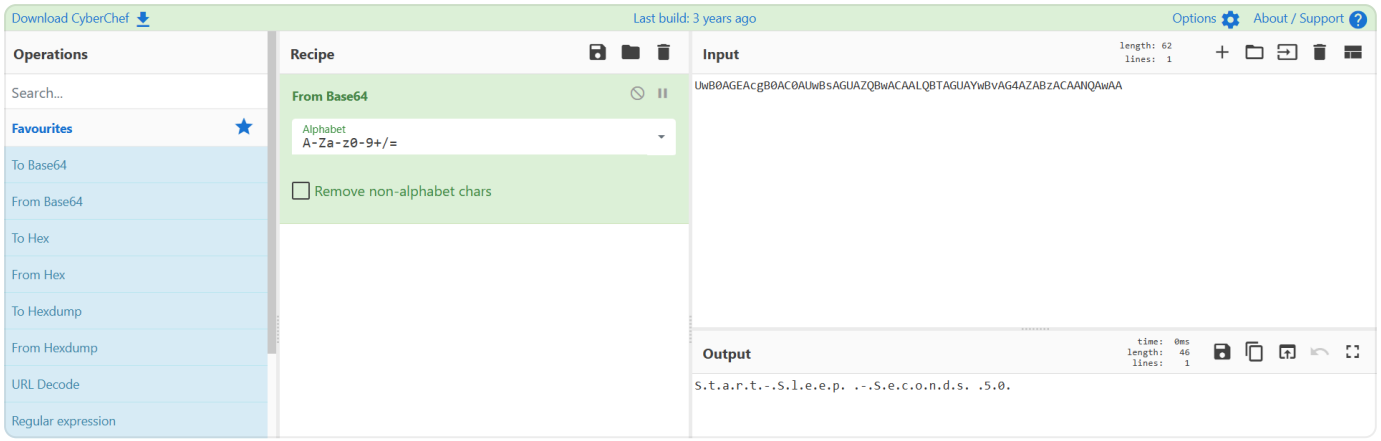
Continuing with the HTML report, we also observe evidence of **persistence and installation behavior**. Specifically, under the **Boot Survival** section, the malware is seen creating a **registry key**, which allows it to survive system reboots and maintain long-term access.

The **HTML report** provides additional details confirming that the file is indeed **malware**. This section of the analysis is especially valuable for understanding the malware's behavior and execution flow.



Analyzing further on the HTML Report, under Process Tree, we can see the following. Copy and paste the base 64 command line on "CyberChef" to see what it does.

Looking deeper into the **Process Tree** within the HTML report, we can identify a suspicious **Base64-encoded command line**. By copying and pasting this into **CyberChef** for decoding, we discover that the command instructs the system to **start and then sleep for 5 seconds**. This type of behavior is a common **evasion technique**, allowing the malware to delay execution and avoid immediate detection by security tools.



Still within the HTML report, we find evidence of the malware's **persistence and installation mechanisms**. Specifically, under the **Boot Survival** section, the report shows that the malware creates a **registry key**, which enables it to survive reboots and maintain a long-term presence on the compromised system. Following the provided link gives even more technical details about these persistence techniques.