

• Identify and Analyze Cyber Threats

The screenshot shows the VirusTotal analysis interface for a .zip file. The file has been flagged as malicious by 17 out of 63 security vendors. The file size is 2.19 KB and it was last analyzed a minute ago. The file name is 65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c.zip. A 'ZIP' button is available for download.

The screenshot shows the threat analysis section of the VirusTotal interface. It displays the threat label (trojan.suspar), threat categories (trojan), and family labels (suspar). The table below lists the security vendors' analysis results:

Vendor	Detection	Vendor	Detection
Alibaba	Trojan:Script.Generic.c77f2639	AliCloud	Trojan:Multi/Puwaders.C9nj
Avira (no cloud)	HEUR/Suspar.Gen	Cynet	Malicious (score: 70)
Google	Detected	Ikarus	Trojan-Downloader.JS.Agent
Kaspersky	HEUR:Trojan.Script.Generic	Kingsoft	Script.Trojan.Generic.a
NANO-Antivirus	Trojan.Script.Heuristic-javascript.iacgm	Skyhigh (SWG)	BehavesLike.Exploit.xc
Sophos	Mal/DrodZp-A	Symantec	Trojan.Gen.MBT
Tencent	Script.Trojan.Generic.Rgil	Trellix (ENS)	Artemis/A31034EB3C47
Varist	JS/Agent.CKJ4.gen!Eldorado	VirIT	Trojan.Win32.MSIL_Heur.A
WithSecure	Heuristic.HEUR/Suspar.Gen	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	ALYac	Undetected

- File Details
 - The file analyzed is a .zip file with a size of 2.91 KB.
 - The file has been flagged as potentially malicious by 17/63 antivirus engines.
- Threat Label
 - The threat label found is the popular Trojan.Suspar (Trojan malware family).
 - Trojan malicious software disguises as legitimate files to infiltrate a system and execute harmful actions.

- Community Score:
 - A community score of 17/63 indicates that 17 engines detected malicious traits in the file, while the others found no issues or were unable to classify it as harmful.
- Detection Overview
 - Vendors Alibaba, Avira, Kaspersky, Tencent, and others flagged this file as:
 - "Trojan.Script.Generic"
 - "HEUR:Trojan.Script.Generic"
 - "Mal/DrodZp-A"
 - "JS.Agent.CKJ4.gen!Eldorado"
 - These indicate the presence of suspicious or harmful scripts (potentially JavaScript or other executables).
- Undetected Results:
 - Some vendors, such as AhnLab-V3 and ALYac, reported the file as "undetected," meaning they found no malicious activity or patterns.

● Setoolkit

```

Security
Parrot Terminal
File Edit View Search Terminal Help
[--] Homepage: https://www.trustedsec.com [--]
Welcome to the Social-Engineer Toolkit (SET).
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!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 

```

```

Security
Parrot Terminal
File Edit View Search Terminal Help
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!

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

```

- Launching the Social Engineering Toolkit.
 - The SET offers multiple options for performing social engineering attacks.
 - The option two, Website Attack Vectors is a feature for creating fake websites to capture user credentials.

```

Parrot Terminal
File Edit View Search Terminal Help
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 settings 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 powershell 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

```

```

Parrot Terminal
File Edit View Search Terminal Help
7) HTA Attack Method
99) Return to Main Menu

set:webattack>3

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>3

```

- Credential Harvester Attack Method
 - Option 3, the Credential Harvester Attack, designs a fake website to mimic a legitimate one.
 - This allows it to gather data from unsuspecting users such as usernames and passwords.
- Cloning a Website
 - Option 2, Site Cloner, creates designs a near replica of a legitimate site (eg. Google)
 - An IP address is specified for hosting the cloned site, allowing the attacker to capture and redirect form submissions to their setup.

```

Parrot Terminal
File Edit View Search Terminal Help
SET
[ ] to harvest credentials or parameters from a website as well as place them in to a report

----- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * 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.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.64.2]192.168.64.2

```

```

Parrot Terminal
File Edit View Search Terminal Help
-----
**** Important Information ****

For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.

You can configure this option under:
/etc/setoolkit/set.config

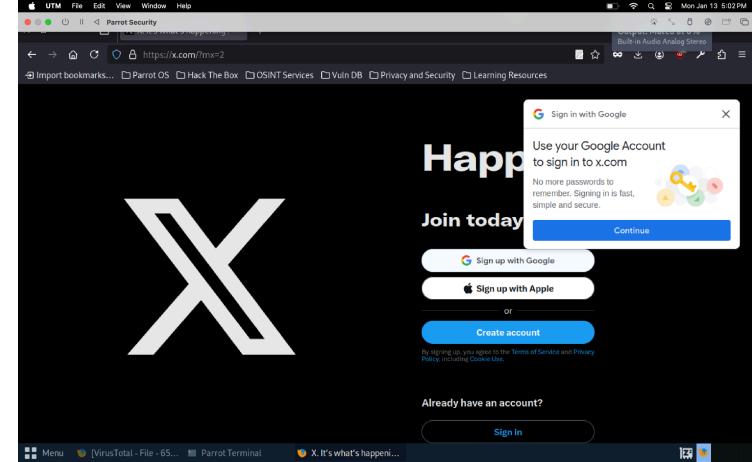
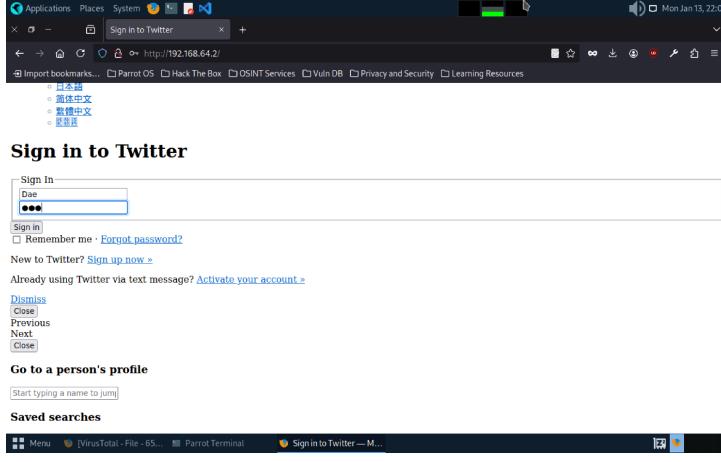
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.

-----
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:3

```

- Template Selection:
 - A template resembling a popular website (Twitter in this case) is selected.
 - The cloned site is hosted locally, and credentials entered into this fake page are captured by SET.



- Testing the Fake Login Page:
 - A fake Twitter login page loaded in a browser, hosted locally at 192.168.64.2.
 - Credentials (username and password) are entered into the form.

```

Edit View Window Help
Parrot Security
File Edit View Search Terminal Help
Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
set:webattack> Select a template:3
[*] Cloning the website: http://www.twitter.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:
192.168.64.2 - - [13/Jan/2025 22:00:39] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=Dae
POSSIBLE PASSWORD FIELD FOUND: session[password]=dae
PARAM: authenticity_token=dba33c0b2bffd8e6dcbb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bffd8e6dcbb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.64.2 - - [13/Jan/2025 22:01:23] "POST /sessions HTTP/1.1" 302 -
Already have an account?

```

- Captured Data Displayed in SET:
 - The terminal logs show that the entered credentials were successfully harvested, including the username (Dae) and password (dae).

● LAPSUS\$

- Overview of Lapsus\$
 - Description: LAPSUS\$ is a cybercriminal group active since mid-2021. They specialize in large-scale social engineering and extortion attacks, typically without deploying ransomware.
 - Targets: The group has attacked organization globally, including sectors like government, education, healthcare, technology, and media.
 - Associated Groups: DEV-0537, Strawberry Tempest.
 - Key Contributors: Includes researchers and security organizations
- Techniques used by Lapsus\$
 - T1531 (Account Access Removal): Disables global admin accounts to lock organizations out of their systems.
 - T1087.002 (Account Discovery): Uses tools like AD Explorer to enumerate accounts.
 - T1098.003 (Account Manipulation): Grants global admin roles to unauthorized accounts in cloud systems.
 - T1583.003 (Acquire Infrastructure): Uses VPS providers for setting up infrastructure.
 - T1586.002 (Compromise Accounts): Bribes employees or suppliers to gain credentials.
 - T1555.003 (Credentials from Web Browsers): Uses tools like Redline Stealer for passwords.
 - T1555.005 (Credentials from Password Managers): Accesses password databases.
 - T1485 (Data Destruction): Deletes resources in on-premises/cloud environments.
 - T1213 (Data from Repositories): Searches collaboration tools like Confluence or GitHub for sensitive information.
 - T1005 (Data from Local Systems): Extracts sensitive files for extortion or public release.
 - T1114.003 (Email Forwarding Rules): Sets forwarding rules to intercept communication.
 - T1068 (Privilege Escalation): Exploits server vulnerabilities like JIRA or Confluence.
 - T1133 (External Remote Services): Gains access to systems like VPNs and RD protocols.
 - T1589 (Gather Identity Info): Collects credentials and email addresses to improve phishing.
 - T1656 (Impersonation): Calls help desks pretending to be employees to access privileged accounts.
 - T1111 (MFA Interception): Exploits multi-factor authentication weaknesses.
 - T1588 (Malware & Tools): Uses tools like RVTools or malware like Redline Password Stealer.

- T1552.008 (Chat Messages): Extracts credentials from collaboration tools like Slack.
- T1078 (Valid Accounts): Uses stolen session tokens for access.
- Software Used: Tools like Mimikatz for credential theft and manipulation.