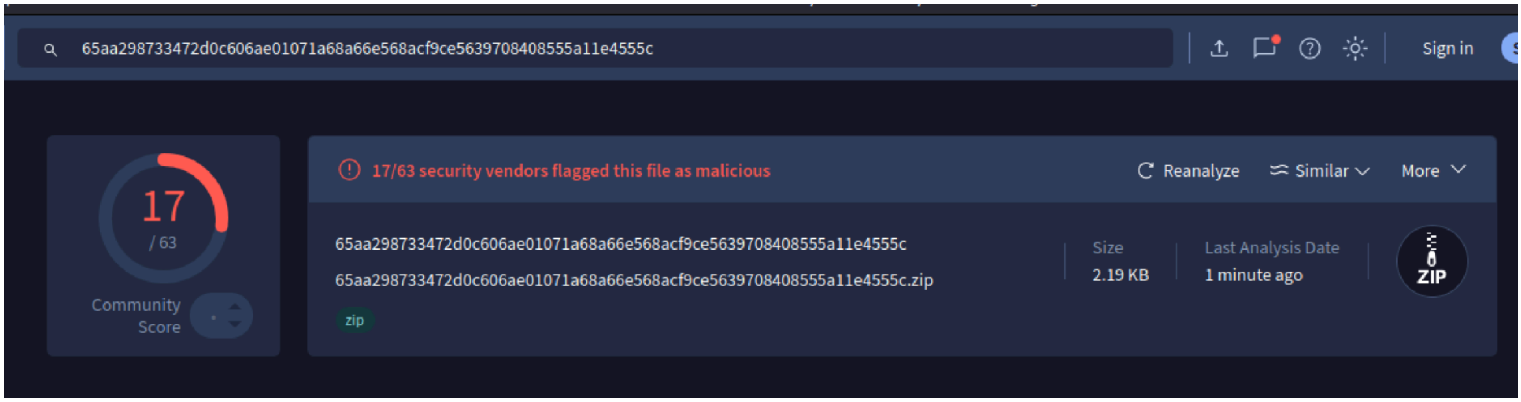
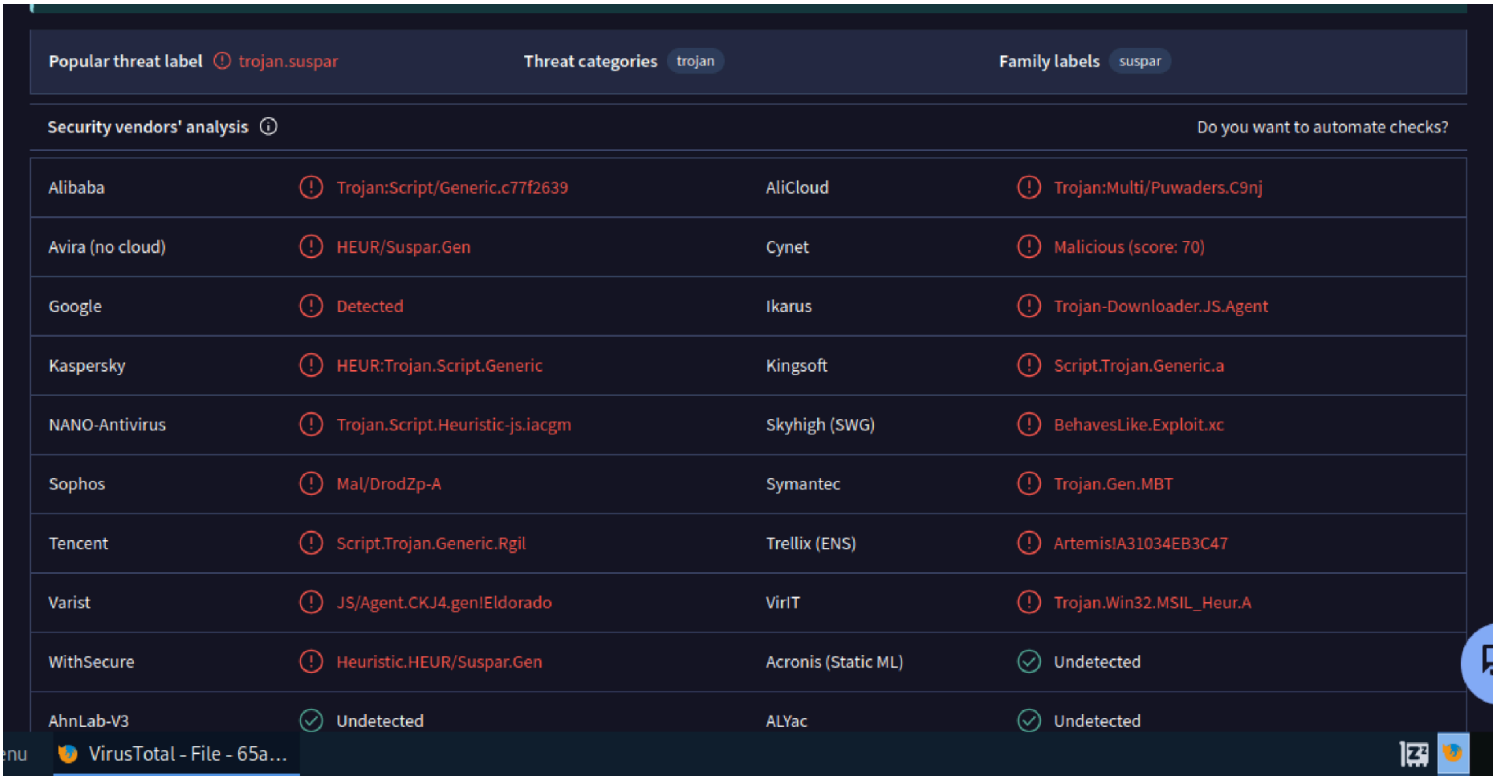
- **Identify and Analyze Cyber Threats**

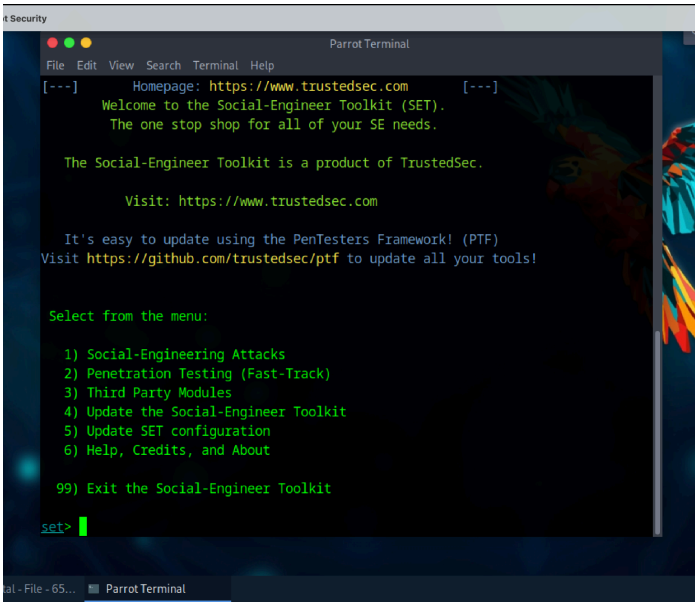


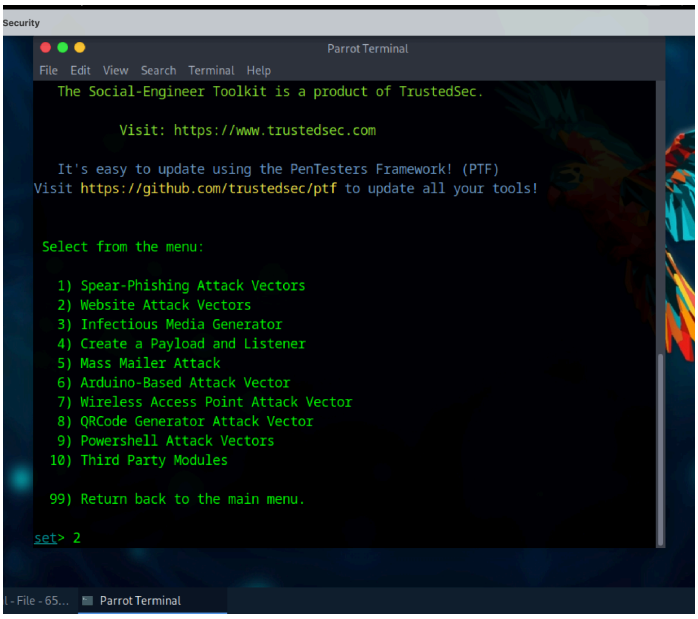


- File Details
  - The file analyzed is a .zip file with a size of 2.91 KB.
  - The file has been flagged as potentially malicious by 17/63 antivirus engines.
- Threat Label
  - The threat label found is the popular Trojan.Suspar (Trojan malware family).
    - Trojan malicious software disguises as legitimate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

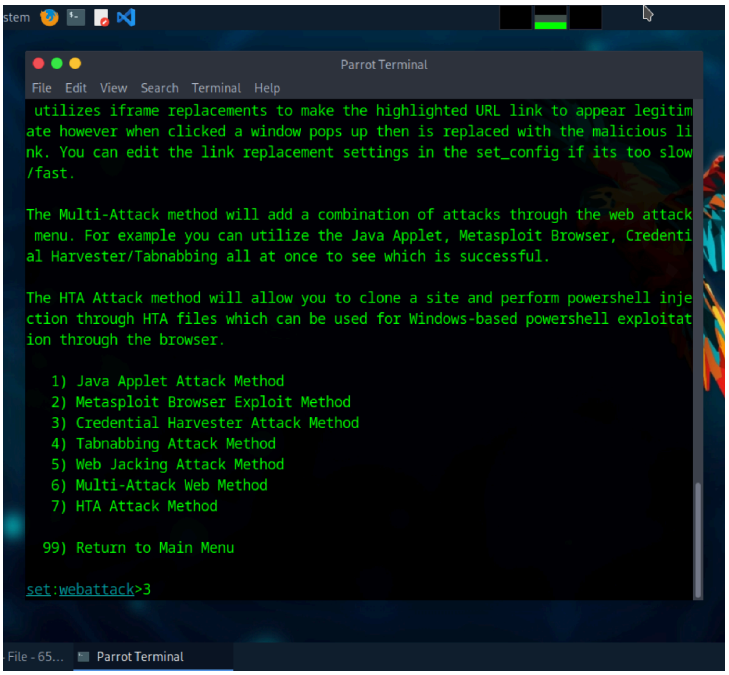
- Community Score:
    - A community score of 17/63 indicates that 17 engines detected malicious traits in the file, while the others found no issues or were unable to classify it as harmful.
- Detection Overview
    - Vendors Alibaba, Avira, Kaspersky, Tencent, and others flagged this file as:
        - "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.

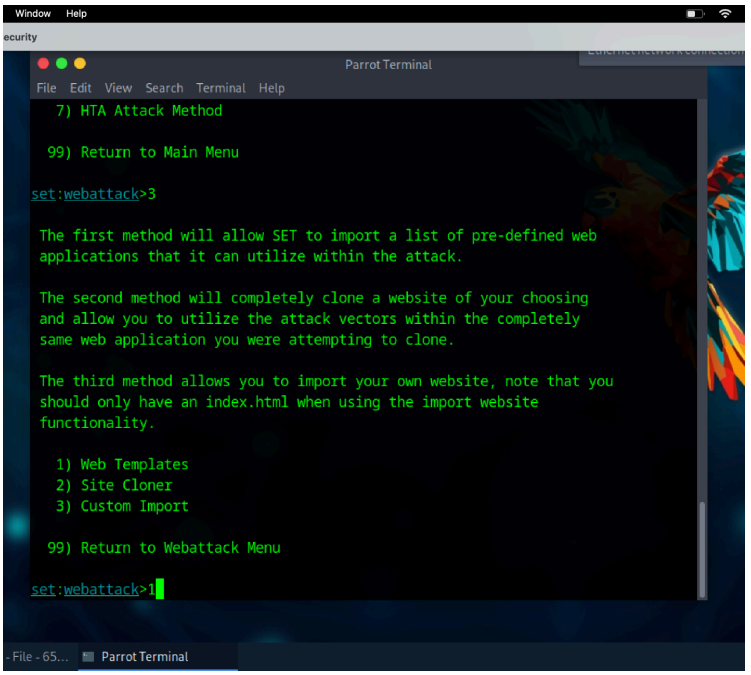
• Setoolkit



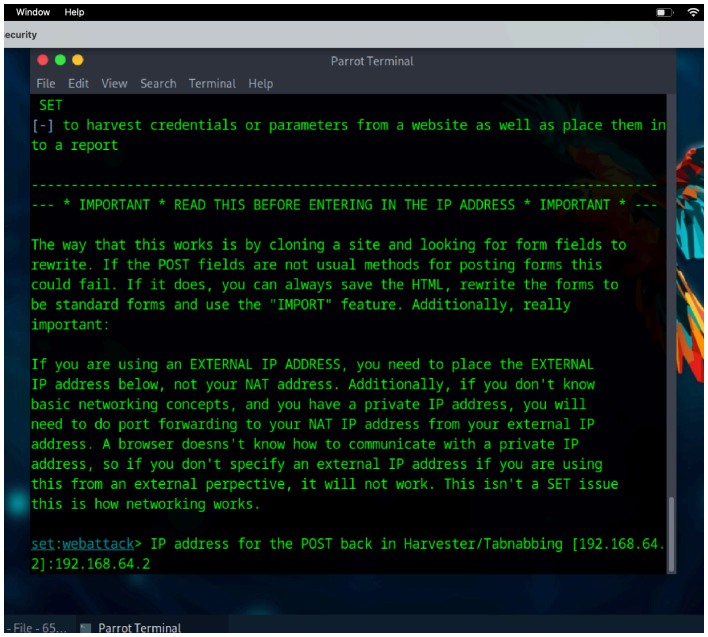


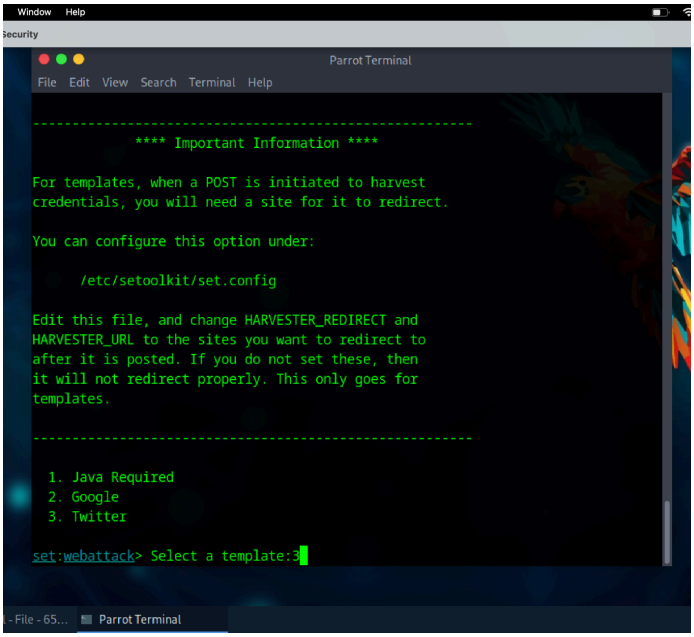
- Launching the Social Engineering Toolkit.
    - The SET offers multiple options for performing social engineering attacks.
    - The option two, Website Attack Vectors is a feature for creating fake websites to capture user credentials.



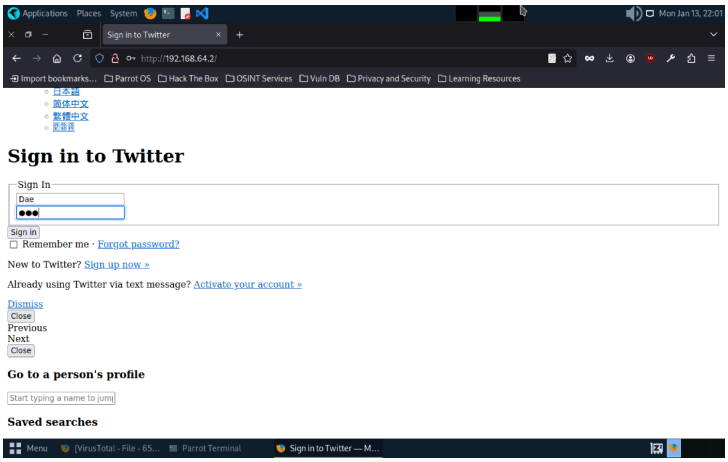


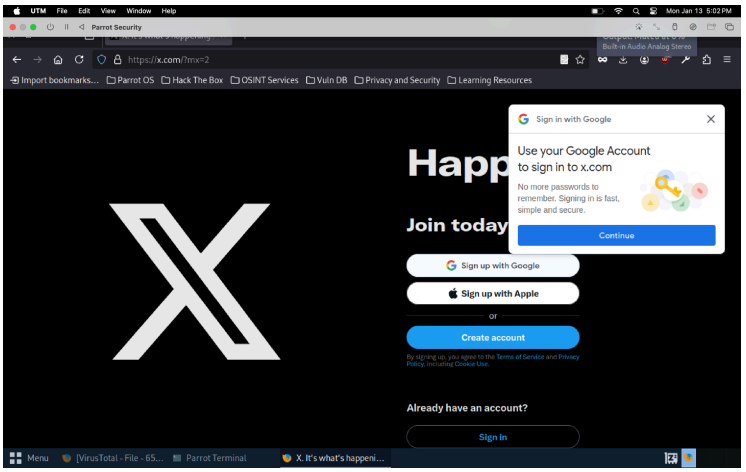
- Credential Harvester Attack Method
  - Option 3, the Credential Harvester Attack, designs a fake website to mimic a legitimate one.
  - This allows it to gather data from unsuspecting users such as usernames and passwords.
- Cloning a Website
  - Option 2, Site Cloner, creates designs a near replica 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.



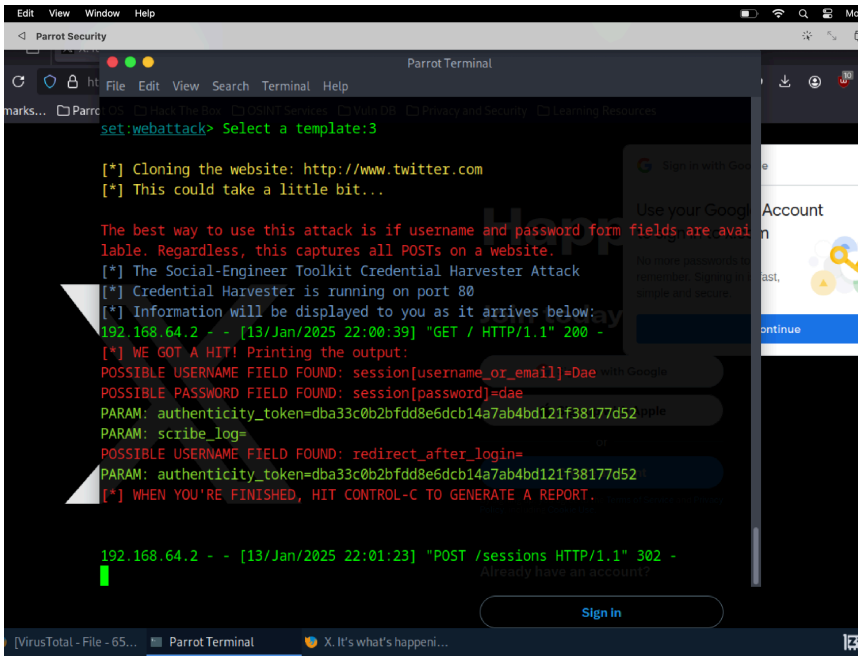


- Template Selection:
  - A template resembling a popular website (Twitter in this case) is selected.
  - The cloned site is hosted locally, and credentials entered into this fake page are captured by SET.





- 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.



- 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.