Overview

1. **File Information**:
    - The file scanned is a compressed .zip archive, likely containing malicious content.
    - File size: 2.19 KB.
    - Popular threat label: **trojan.suspar**.
    - Threat category: **Trojan**.
2. **Detection Rate**:
    - **18 out of 63 security vendors** flagged this file as malicious.
    - While not all vendors detected the file as harmful, the significant detection rate and the identification by well-known antivirus engines strongly suggest malicious intent.

Detailed Breakdown

Key Vendors Flagging the File:

- **Alibaba: Classified as Trojan:Script/Generic.**
- **Avira: Flagged as HEUR/Suspar.Gen.**
- **Google: Detected as malicious (generic).**
- **Kaspersky: Marked as HEUR:Trojan.Script.Generic.**
- **Microsoft: Identified as Trojan:Script/Wacatac.B!ml.**
- **Sophos: Labeled as BehavesLike.Exploit.xc.**

File Behavior:

- **Common Indicators:**
    - **Multiple vendors indicate the presence of a Trojan Downloader or Trojan Generic activity, suggesting it may download further malicious payloads.**
    - **Heuristic detections like HEUR/Suspar.Gen indicate suspicious behavioral patterns rather than known malware signatures.**

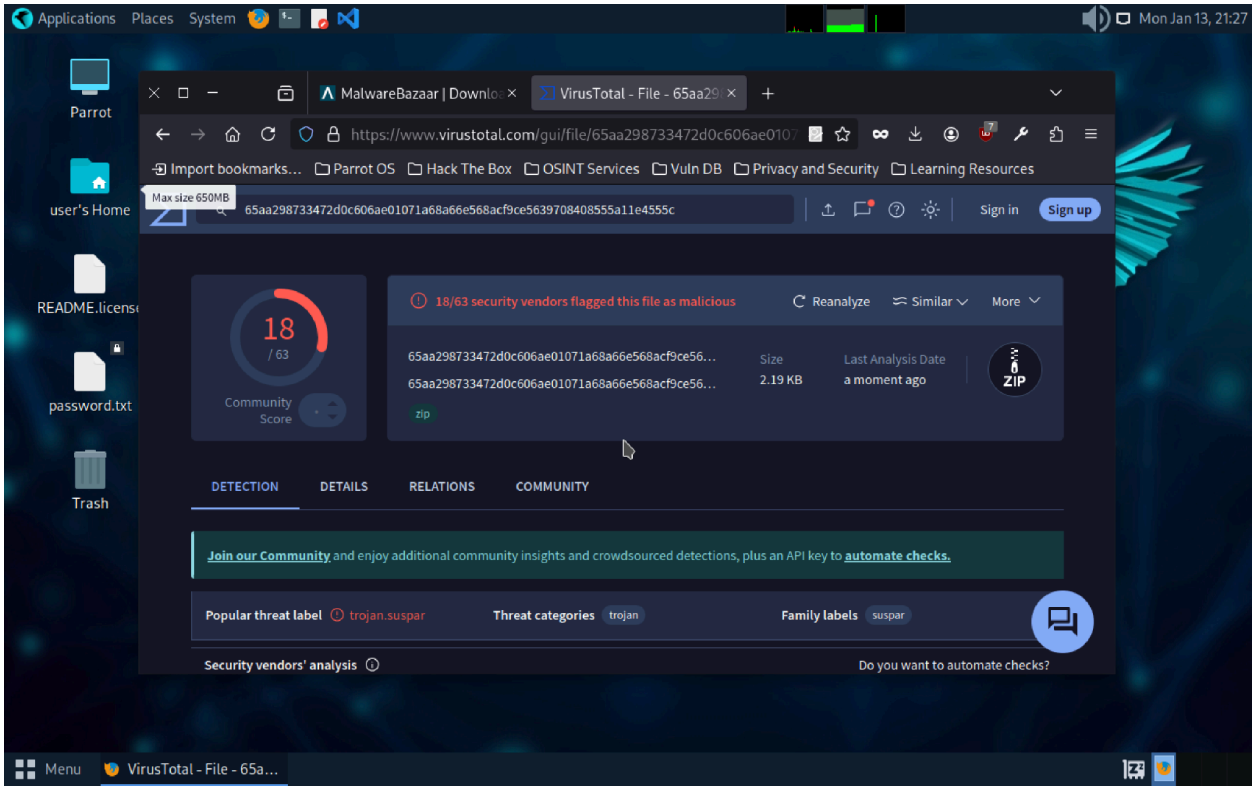
Vendors Not Detecting Malicious Activity:

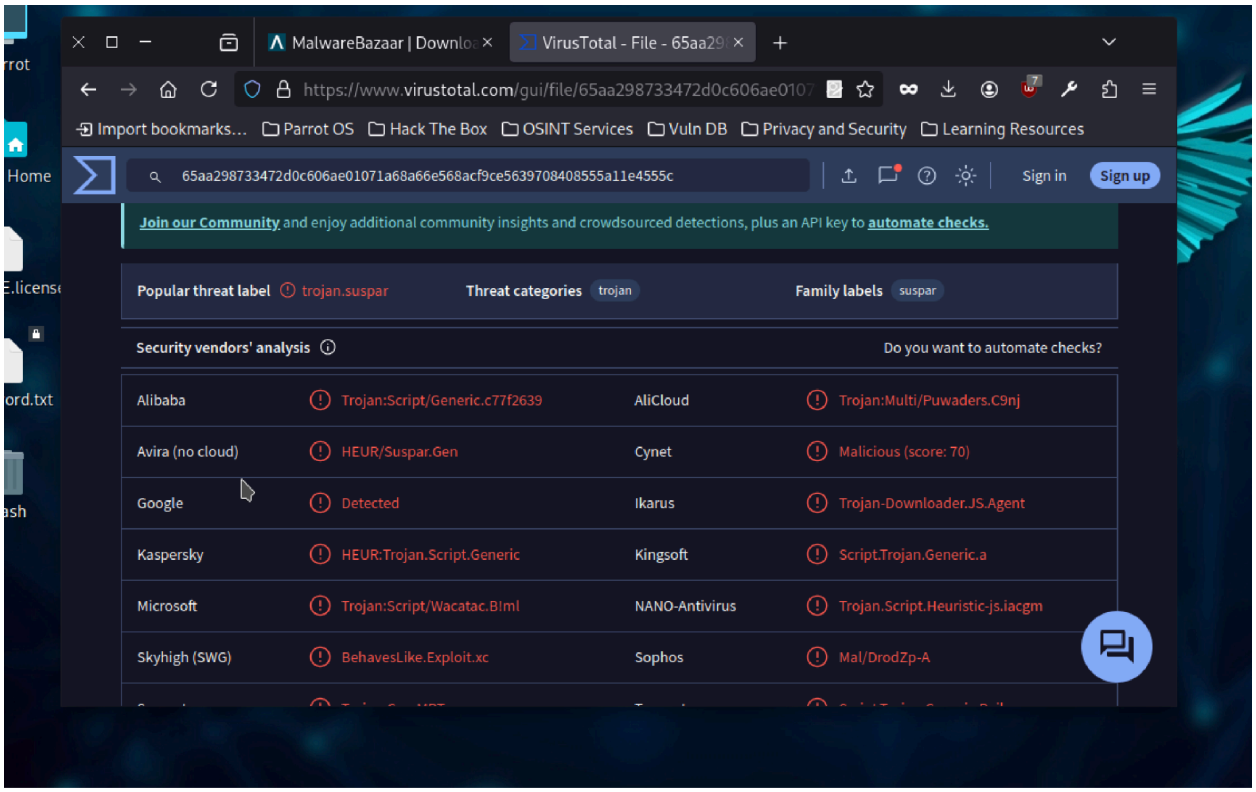
- **A significant number of antivirus tools (e.g., Avast, Bitdefender, Malwarebytes, etc.) reported the file as "undetected." This could mean:**
    - **The malicious behavior is obfuscated or not included in their detection database.**
    - **The file may evade detection due to specific encoding or encryption techniques.**

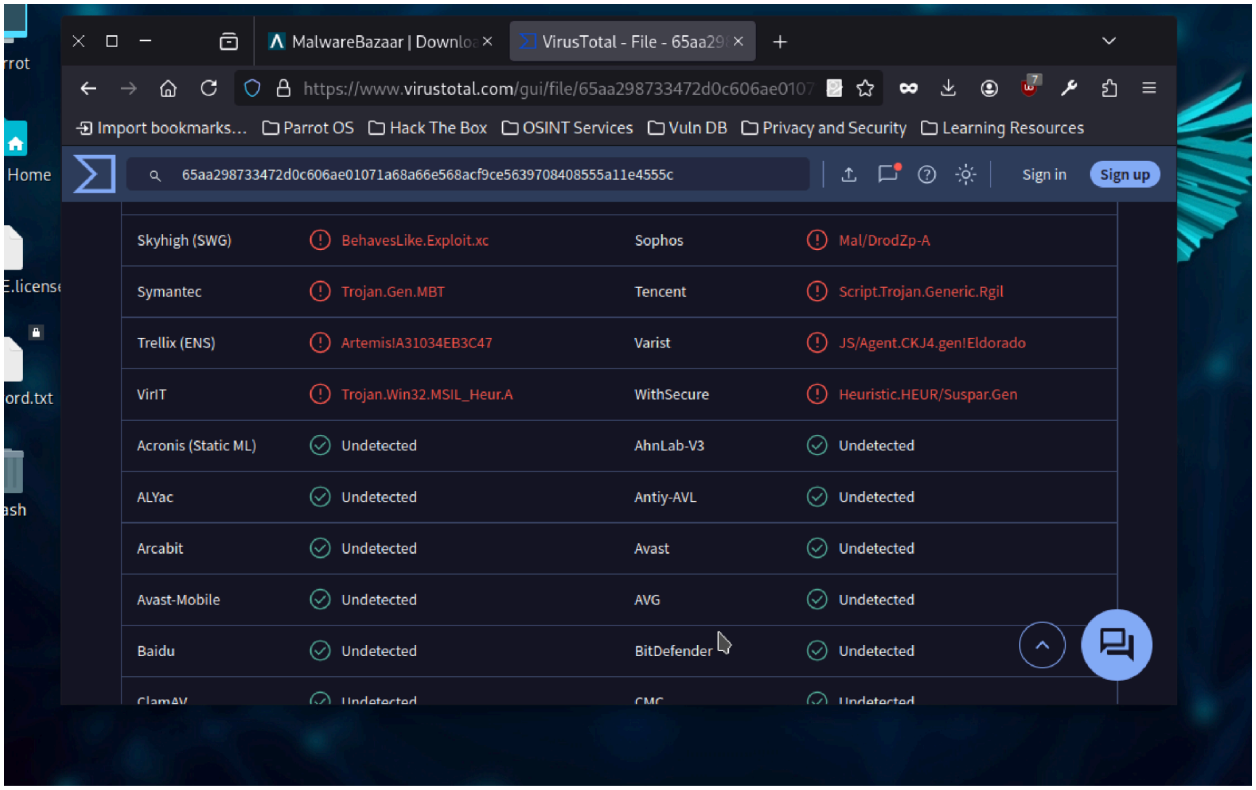
Recommendations

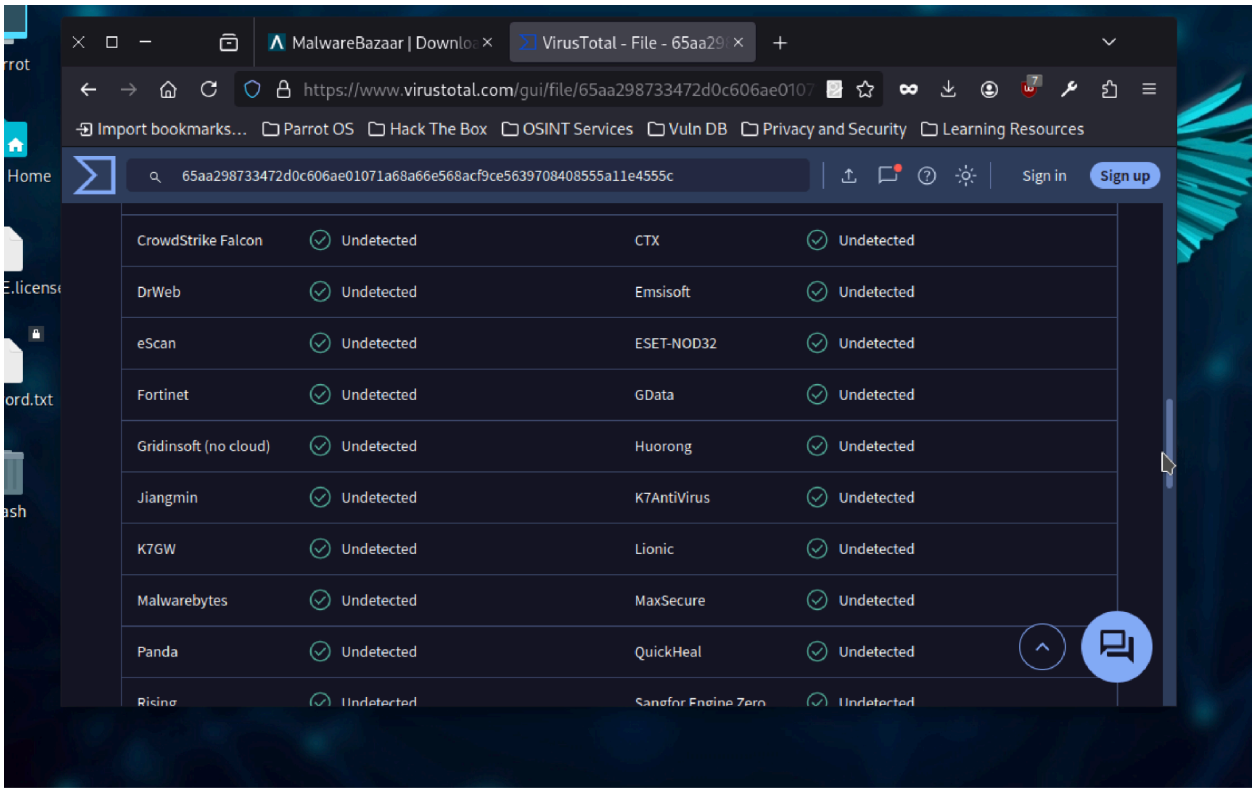
1. **Do Not Open or Execute:**
    - **Avoid unzipping or running the contents of the file.**
    - **The risk of infection, data theft, or further downloads of malicious payloads is high.**
2. **Isolate the File:**
    - **If downloaded on a physical machine, remove it immediately or quarantine it in antivirus software.**
3. **Further Investigation:**
    - **Run the file in a sandbox environment for analysis, if necessary.**
    - **Cross-reference with additional tools like hybrid-analysis or ANY.RUN for dynamic analysis.**
4. **Preventive Measures:**
    - **Update antivirus software on your system.**
    - **Avoid downloading files from untrusted sources like MalwareBazaar unless analyzing for research purposes in a secure, isolated environment.**

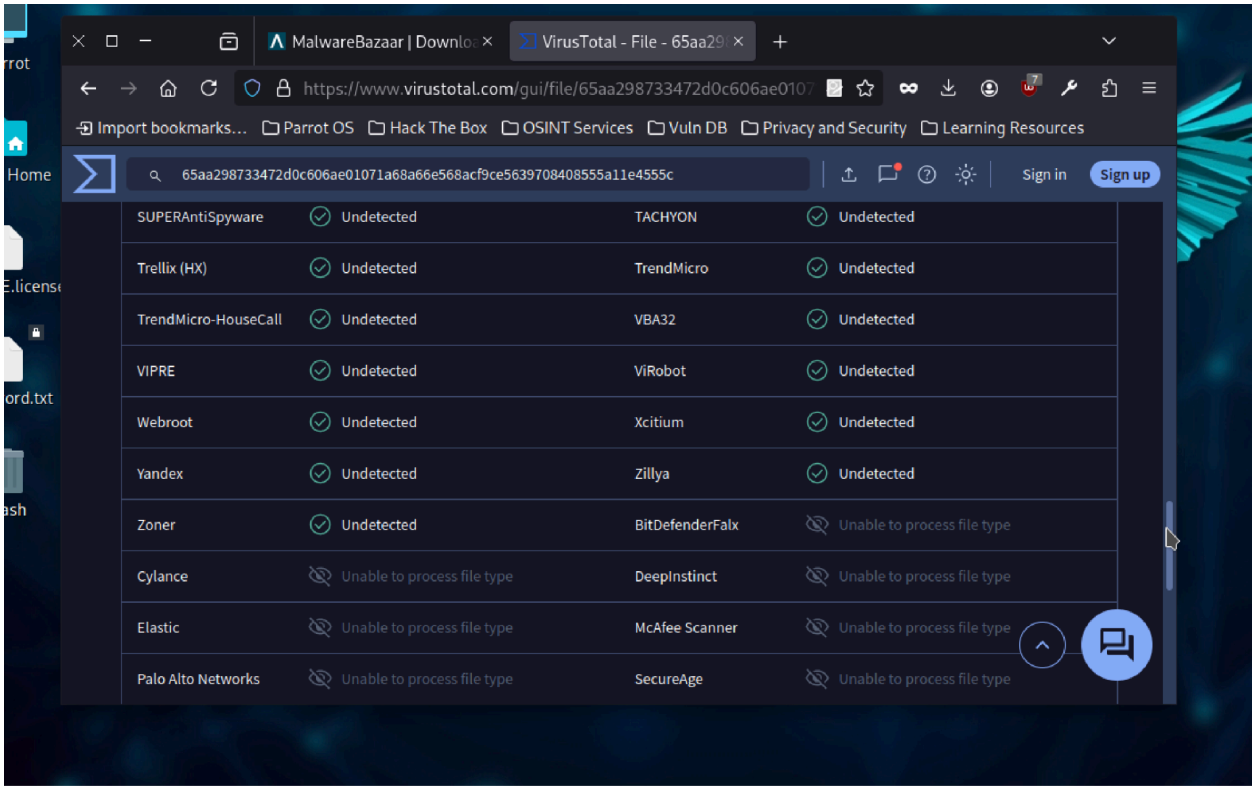
Let me know if you'd like further help with interpreting any specific part of this report or performing additional analysis!

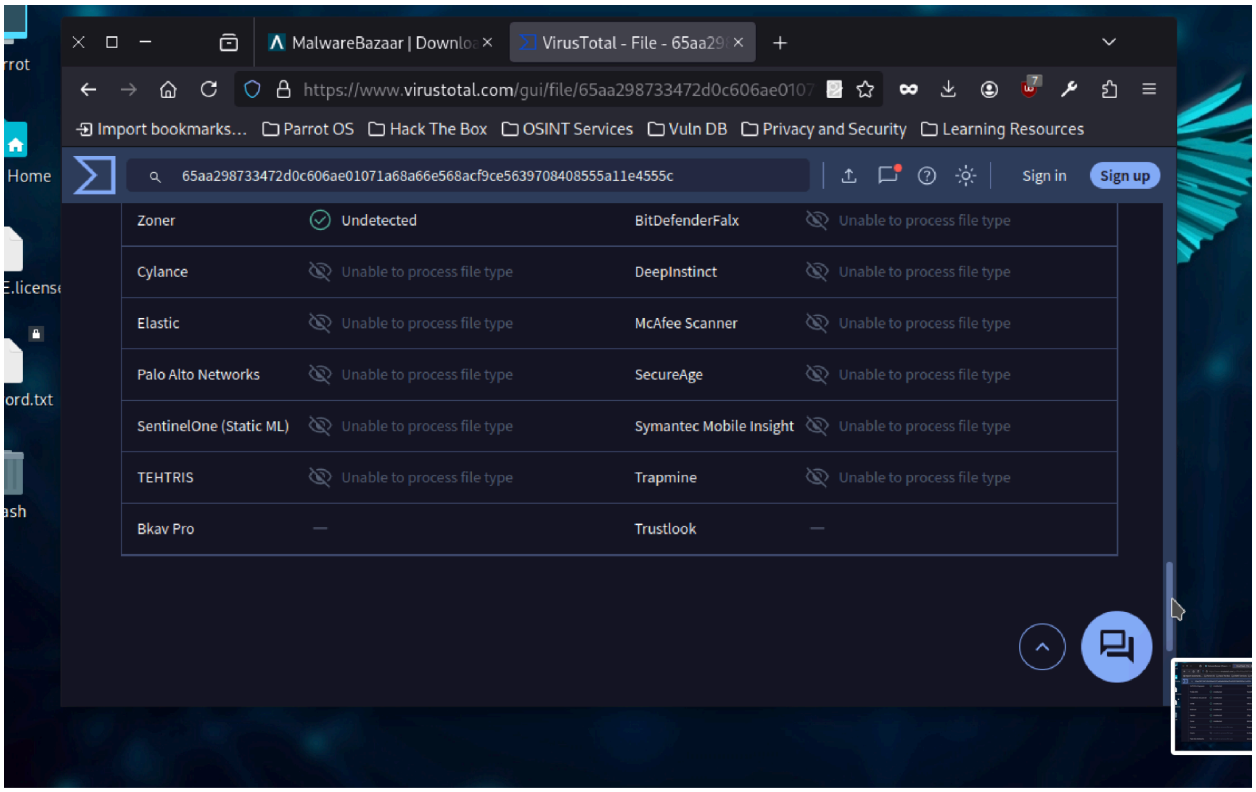

Applications Places System
Mon Jan 13, 21:27
Parrot
user's Home
README.licens
password.txt
Trash
MalwareBazaar | Downlo
VirusTotal - File - 65aa29
https://www.virustotal.com/gui/file/65aa298733472d0c606ae0107
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Max size 650MB
65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c
Sign in
Sign up
18
/ 63
Community Score
18/63 security vendors flagged this file as malicious
Reanalyze
Similar
More
65aa298733472d0c606ae01071a68a66e568acf9ce56...
65aa298733472d0c606ae01071a68a66e568acf9ce56...
zip
Size
2.19 KB
Last Analysis Date
a moment ago
ZIP
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?
Menu
VirusTotal - File - 65a...


MalwareBazaar | Downlo
VirusTotal - File - 65aa29
https://www.virustotal.com/gui/file/65aa298733472d0c606ae0107
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c
Sign in
Sign up
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?
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
Microsoft
Trojan:Script/Wacatac.B!ml
NANO-Antivirus
Trojan.Script.Heuristic-js.iacgm
Skyhigh (SWG)
BehavesLike.Exploit.xc
Sophos
Mal/DrodZp-A


MalwareBazaar | Downlo
VirusTotal - File - 65aa29
https://www.virustotal.com/gui/file/65aa298733472d0c606ae0107
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c
Sign in
Sign up
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
Antiy-AVL Undetected
Arcabit Undetected
Avast Undetected
Avast-Mobile Undetected
AVG Undetected
Baidu Undetected
BitDefender Undetected


MalwareBazaar | Downlo
VirusTotal - File - 65aa29
https://www.virustotal.com/gui/file/65aa298733472d0c606ae0107
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c
Sign in
Sign up
CrowdStrike Falcon Undetected
CTX Undetected
DrWeb Undetected
Emsisoft Undetected
eScan Undetected
ESET-NOD32 Undetected
Fortinet Undetected
GData Undetected
Gridinsoft (no cloud) Undetected
Huorong Undetected
Jiangmin Undetected
K7AntiVirus Undetected
K7GW Undetected
Lionic Undetected
Malwarebytes Undetected
MaxSecure Undetected
Panda Undetected
QuickHeal Undetected





Overview

1. **File Information**:

- The file scanned is a compressed .zip archive, likely containing malicious content.
- File size: 2.19 KB.
- Popular threat label: **trojan.suspar**.
- Threat category: **Trojan**.

2. **Detection Rate**:
   - **18 out of 63 security vendors** flagged this file as malicious.
   - While not all vendors detected the file as harmful, the significant detection rate and the identification by well-known antivirus engines strongly suggest malicious intent.