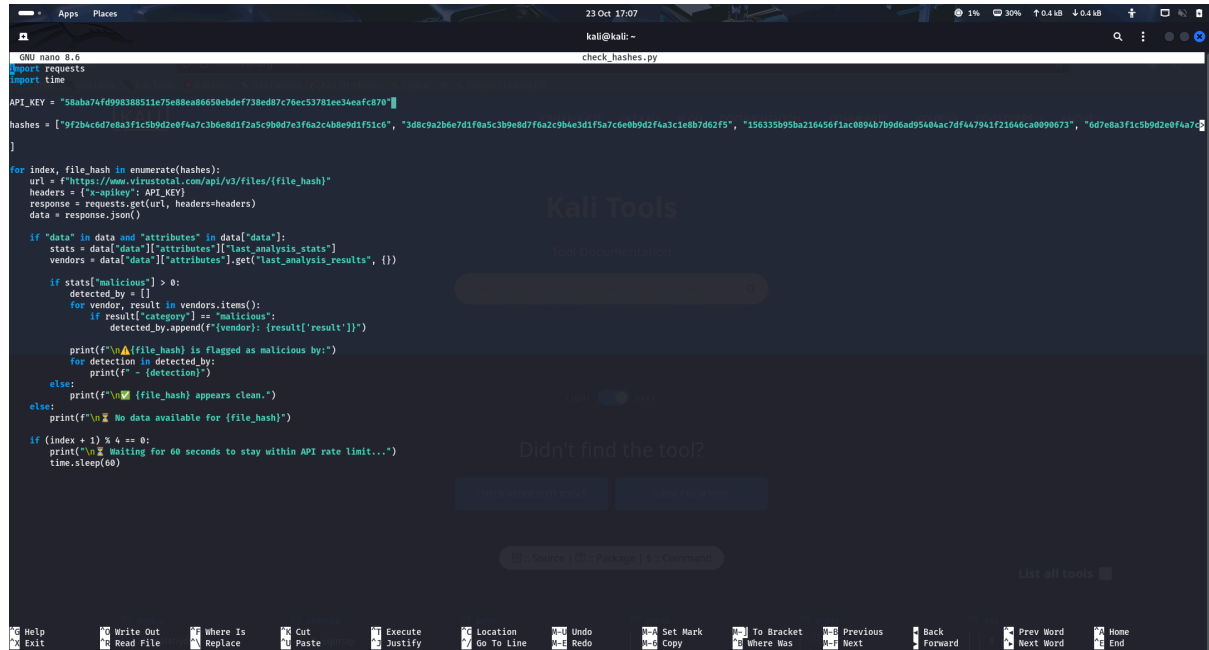


Identifying Malicious Hashes Using VirusTotal

- * Generated Virus Total API key
- * open a file to write a python script for automation
 >nano check_hashes.py"



```
GNU nano 2.8.6
check_hashes.py

import requests
import time

API_KEY = "58aba74fd998388511e75e88ea8650ebdef738ed87c76ec53781ee34eafc870"

hashes = ["9f2b4cd07ba3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b0e9d1f31c0", "3d8c9a2b6e7d1f8a5c3b0e8d7f6a2c9b4e3d1f5a7c6e0b9d2f4a3c1e8b7d62f5", "156335b95ba216456f1ac0894b7b9d6ad9540ac7df447941f21646ca0890673", "6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b0e9d1f31c0"]

for index, file_hash in enumerate(hashes):
    url = f"https://www.virustotal.com/api/v3/files/{file_hash}"
    headers = {'x-apikey': API_KEY}
    response = requests.get(url, headers=headers)
    data = response.json()

    if 'data' in data and 'attributes' in data['data']:
        stats = data['data']['attributes']['last_analysis_stats']
        vendors = data['data']['attributes'].get('last_analysis_results', {})

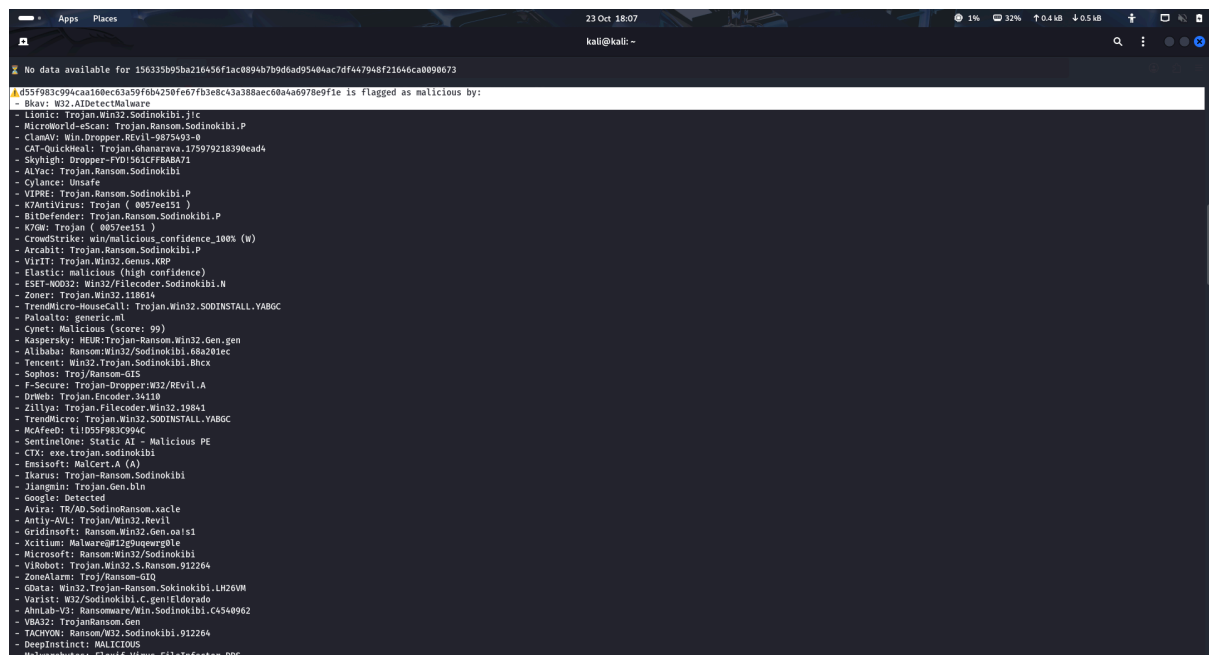
        if stats['malicious'] > 0:
            detected_by = []
            for vendor, result in vendors.items():
                if result['category'] == "malicious":
                    detected_by.append(f"{vendor}: {result['result']}")

            print(f"⚠️ {file_hash} is flagged as malicious by:")
            for detection in detected_by:
                print(f"  - {detection}")
        else:
            print(f"✅ {file_hash} appears clean.")
    else:
        print(f"❌ No data available for {file_hash}")

    if (index + 1) % 4 == 0:
        print("\n⏸️ waiting for 60 seconds to stay within API rate limit...")
        time.sleep(60)
```

Automate Scanning for Malicious Hashes

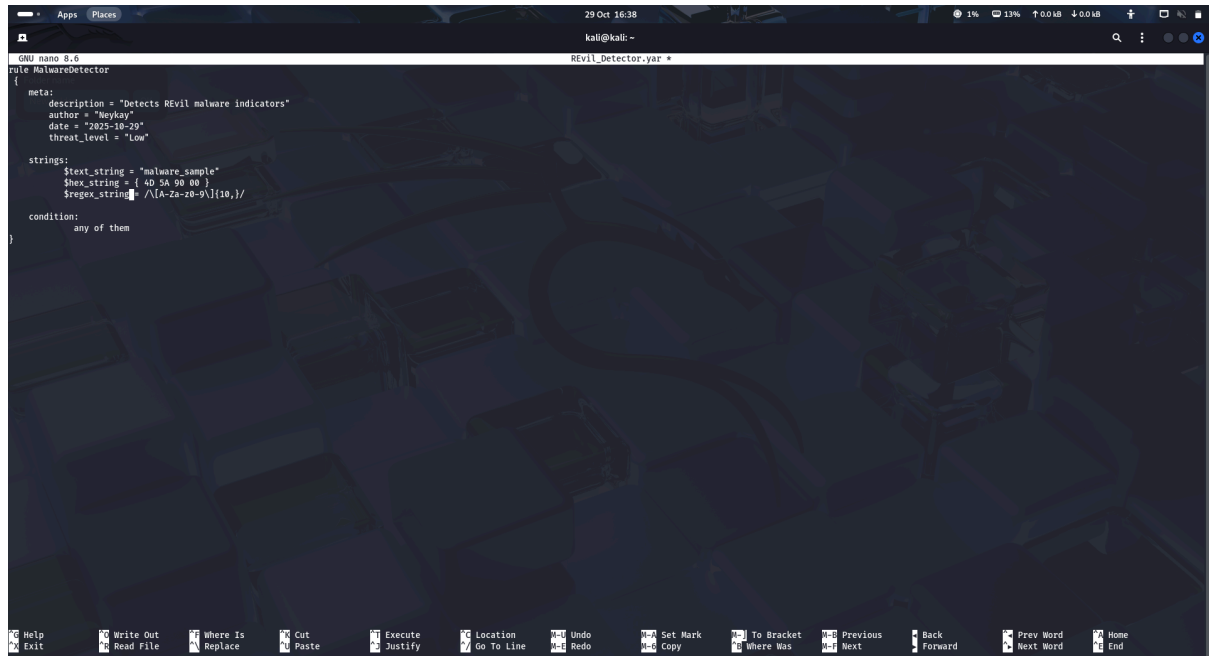
python3 check_hashes.py



```
❌ No data available for 156335b95ba216456f1ac0894b7b9d6ad9540ac7df447941f21646ca0890673

⚠️ 9f2b4cd07ba3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b0e9d1f31c0 is flagged as malicious by:
- Bkav: W32.AIDetectMalware
- Etnice: Trojan.Win32.Sodinokibi.jic
- MicroWorld-eScan: Trojan.Ransom.Sodinokibi.P
- ClamAV: Win.Dropper.REvil-9875493-0
- CAT-QuickHeal: Trojan.Ohmarava.175979218390ead4
- SkyHigh: Dropper-FV016d5cfff8a8a71
- ALYac: Trojan.Ransom.Sodinokibi
- Cylance: Unsafe
- VIPRE: Trojan.Ransom.Sodinokibi.P
- K7AntiVirus: Trojan ( 0057ee151 )
- BitDefender: Trojan.Ransom.Sodinokibi.P
- K7ED: Trojan ( 0027ee151 )
- CrowdStrike: win/malicious_confidence_100% (w)
- Arcabit: Trojan.Ransom.Sodinokibi.P
- VirIT: Trojan.Win32.Genus.KRP
- Elastic: malicious (high confidence)
- ESET-NOD32: Win32/Filecoder.Sodinokibi.W
- Zoner: Trojan.Win32.118614
- TrendMicro-HouseCall: Trojan.Win32.SODINSTALL.YABGC
- Paloalto: generic.ml
- Cynet: Malicious (score: 99)
- Kaspersky: HEUR:Trojan-Ransom.Win32.Gen.gen
- Alibaba: Ransom/Win32/Sodinokibi.68a201ec
- Tencent: Win32.Trojan.Sodinokibi.Bhcx
- Sophos: Troj/Ransom-G15
- F-Secure: Trojan-Dropper.W32/Revil.A
- DrWeb: Trojan.Encoder.34110
- Zillya: Trojan.Filecoder.Win32.19841
- TrendMicro: Trojan.Win32.SODINSTALL.YABGC
- McAfee: t1D55F983C994c
- SentinelOne: Static AI - Malicious PE
- CTR: exe.trojan.sodinokibi
- Emsisoft: Malcert.A (A)
- Ikarus: Trojan-Ransom.Sodinokibi
- Jiangmin: Trojan.Gen.Bln
- Google: Detected
- Avira: TR/AD.SodinoRansom.xacle
- Antiy-AVL: Trojan/Win32.Revil
- Gridinsoft: Ransom.Win32.Gen.oais1
- Xcitium: Malware#129puqewrgole
- Microsof: Ransom/Win32/Sodinokibi
- VirusTotal: Trojan.Win32.S.Ransom.912264
- ZoneAlarm: Troj/Ransom-G10
- GData: Win32.Trojan-Ransom.Sokinokibi.LH26VM
- Varist: W32/Sodinokibi.C.genifdorado
- AhnLab-V3: Ransomeat/Win.Sodinokibi.C4540962
- VBA32: TrojanRansom.Gen
- TACHYON: Ransom/W32.Sodinokibi.912264
- DeepInstinct: MALICIOUS
- Malwarebytes: Floxif.Virus.FileInfector.D05
```

Created a simple YARA rule



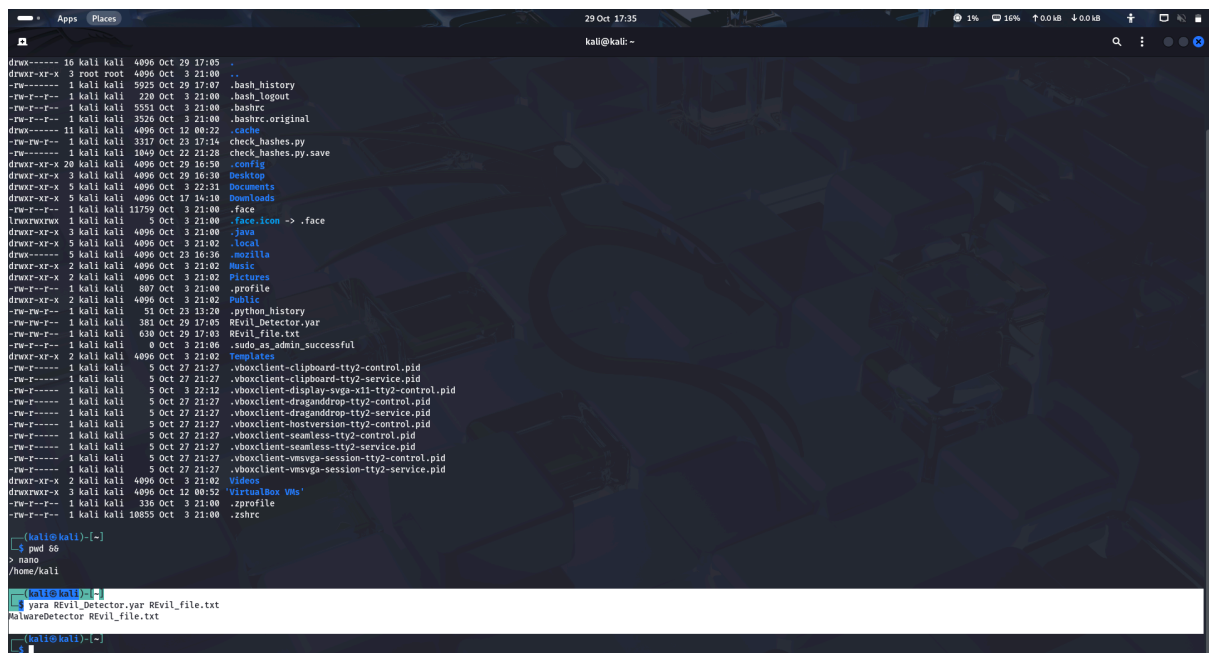
The screenshot shows a terminal window with the GNU nano 2.9.3 editor open. The file being edited is named 'REvil_Detector.yar *'. The YARA rule is defined as follows:

```
rule MalwareDetector
{
  meta:
    description = "Detects REvil malware indicators"
    author = "Neykay"
    date = "2025-10-29"
    threat_level = "Low"

  strings:
    $text_string = "malware_sample"
    $hex_string = { 4D 5A 90 00 }
    $regex_string = /[A-Za-z0-9]{10,}/

  condition:
    any of them
}
```

Yara rule scan



The screenshot shows a terminal window with the command 'yara REvil_Detector.yar /home/kali' being executed. The output of the scan is as follows:

```
MalwareDetector REvil_file.txt
16 kali kali 4096 Oct 29 17:05 .
3 root root 4096 Oct 3 21:00 ..
1 kali kali 5925 Oct 29 17:07 .bash_history
1 kali kali 220 Oct 3 21:00 .bash_logout
1 kali kali 5551 Oct 3 21:00 .bashrc
1 kali kali 3526 Oct 3 21:00 .bashrc.original
1 kali kali 4096 Oct 12 00:22 .cache
1 kali kali 3317 Oct 23 17:14 check_hashes.py
1 kali kali 1049 Oct 22 21:28 check_hashes.py.save
20 kali kali 4096 Oct 29 16:50 .config
3 kali kali 4096 Oct 29 16:10 Desktop
5 kali kali 4096 Oct 3 22:31 Downloads
5 kali kali 4096 Oct 17 14:10 Downloads
1 kali kali 11739 Oct 3 21:00 .face
1 kali kali 5 Oct 3 21:00 .face.icon -> .face
3 kali kali 4096 Oct 3 21:00 .java
5 kali kali 4096 Oct 3 21:02 .local
5 kali kali 4096 Oct 23 16:36 .mozilla
2 kali kali 4096 Oct 3 21:02 .Music
2 kali kali 4096 Oct 3 21:02 .Pictures
1 kali kali 807 Oct 3 21:00 .profile
2 kali kali 4096 Oct 3 21:02 .Public
1 kali kali 51 Oct 23 13:20 .python_history
1 kali kali 381 Oct 29 17:05 REvil_Detector.yar
1 kali kali 630 Oct 29 17:03 REvil_file.txt
1 kali kali 0 Oct 3 21:06 .sudo_as_admin_successful
2 kali kali 4096 Oct 3 21:02 Templates
1 kali kali 5 Oct 27 21:27 .vboxclient-clipboard-tty2-control.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-clipboard-tty2-service.pid
1 kali kali 5 Oct 3 22:12 .vboxclient-display-svga-x11-tty2-control.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-draganddrop-tty2-control.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-draganddrop-tty2-service.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-hostversion-tty2-control.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-seamless-tty2-control.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-seamless-tty2-service.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-vmvga-session-tty2-control.pid
1 kali kali 5 Oct 27 21:27 .vboxclient-vmvga-session-tty2-service.pid
2 kali kali 4096 Oct 3 21:02 Videos
3 kali kali 4096 Oct 12 00:52 'VirtualBox VMs'
1 kali kali 336 Oct 3 21:00 .zprofile
1 kali kali 10835 Oct 3 21:00 .zshrc
```