

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 8.5
import requests
import time

API_KEY = "58aba74fd99838851le75e88ea86650ebdef738ed07c76ec53781ec34eaef870"

hashes = ["9f2b2d7e8a3f1c5b9d2e0fa47c3b6ed1f2a5c9bd07e3f6a2c4b8e9d1f51c6", "3d8c9a2bde7d1fca5c3b9e8d7f6a2c9b4e3df5a7c6e0b9d2f4a3c1e0b7d62f5", "156335b95ba216456f1ac0894b7b9d6ad9540ac7d7f447941f21646ca0090673", "6d7e8a3f1c5b9d2e0fa7c"]

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"\n⚠️ {file_hash} is flagged as malicious by:")
            for detection in detected_by:
                print(f" - {detection}")
        else:
            print(f"\n✅ {file_hash} appears clean.")

    else:
        print(f"\n✗ 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)

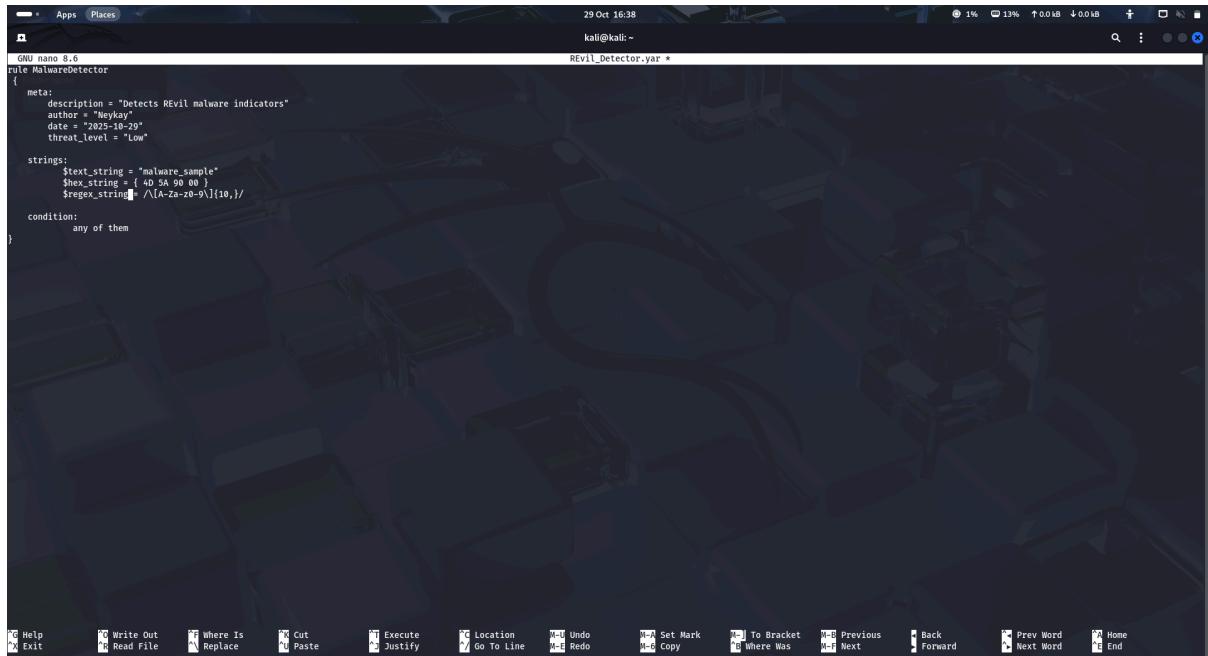
Didnt find the tool?

Source | Package | Command | List all tools
```

```
Automate Scanning for Malicious Hashes  
python3 check_hashes.py
```

```
23 Oct 18:07  
kali㉿kali:~  
  
# No data available for 156335b95ba216456flac0894b7b9d6ad9540ac7df47948f21640ca0090873  
# 1% 32% ↑ 0.4 kB ↓ 0.5 kB  
#  
# The following file was flagged as malicious by:  
# - Bkav: M32_ATDetectMalware  
# - Lionic: Trojan.Win32.Sodinokibi!c  
# - MicroWorld-eScan: Trojan.Ransom.Sodinokibi.P  
# - ClamAV: Win.Dropper.Revil-9875493-0  
# - Cuckoo: 156335b95ba216456flac0894b7b9d6ad9540ac7df47948f21640ca0090873  
# - Skyhigh: Dropper-7YD1561CF8BA87  
# - ALYac: Trojan.Ransom.Sodinokibi  
# - Cylance: Unsafe  
# - VIPRE: Trojan.Ransom.Sodinokibi.P  
# - K7AntiVirus: Trojan ( 00570000 )  
# - ESET-NOD32: Win32.Trojan.Ransom.Sodinokibi.P  
# - K7GW: Trojan ( 0057ee151 )  
# - CrowdStrike: win.alicious_confidence_100% (w)  
# - Arcabit: Trojan.Ransom.Sodinokibi.P  
# - VirusShare: Win32.Gen.KRP  
# - ESET: Malicious (confidence)  
# - ESET-NOD32: Win32.FileCoder.Sodinokibi.N  
# - Zoner: Trojan.Win32.118614  
# - TremorMicro-MouseCall: Trojan.Win32.SODININSTALL.YABGC  
# - Paloalto: generic_ml  
# - McAfee: Malicious (confidence: 50)  
# - Kaspersky: HEUR:Trojan-Ransom.Win32.Gen.gen  
# - Alibaba: Ransom.Win32.Sodinokibi.68a201e;  
# - Tencent: Win32.Trojan.Sodinokibi.Bhx  
# - Sophos: Troj/Ransom-GIS  
# - F-Secure: Trojan-Dropper-W32/Revil.A  
# - Drweb: 156335b95ba216456flac0894b7b9d6ad9540ac7df47948f21640ca0090873  
# - Zillya: Trojan.FileCoder.Win32.15841  
# - TremorMicro: Trojan.Win32.SODININSTALL.YABGC  
# - McAfee: t1055F93C94C  
# - SentinelOne: Static AI - Malicious PE  
CTX: exe.Trojan.Sodinokibi  
ESET: Malicious (Confidence: A (A))  
IKarus: Trojan-Ransom.Sodinokibi  
Jiangmin: Trojan.Gen.bln  
Google: Detected  
Avira: TRAD/Sodinokibi-Gen  
Avast: Win32.Trojan-Sodinokibi  
Gridinsoft: Ransom.Win32.Gen.oais1  
Xcitium: Malwaregen12g9uewggle  
Microsoft: Ransom.Win32.Sodinokibi  
ViRobot: Trojan.Win32.S.Ransom.912264  
ZoneAlarm: Win32.Trojan-Sodinokibi  
GData: Win32.Trojan-Sodinokibi.Sokinokibi.LW26W  
Varist: W32.Sodinokibi.C.genEldorado  
AhnLab-V3: Ransomware/Win.Sodinokibi.C4540962  
VBA2Z: TrojanRansom.Gen  
TACHYON: Ransom/W32.Sodinokibi.912264  
DeepSight: Win32.Sodinokibi  
Malwarebytes: Rillyif.Virus.FileInfecter.bns
```

Created a simple YARA rule



```
29 Oct 16:38                               kali㉿kali:~
```

```
GNU nano 8.0                                REvil_Detector.yar *
```

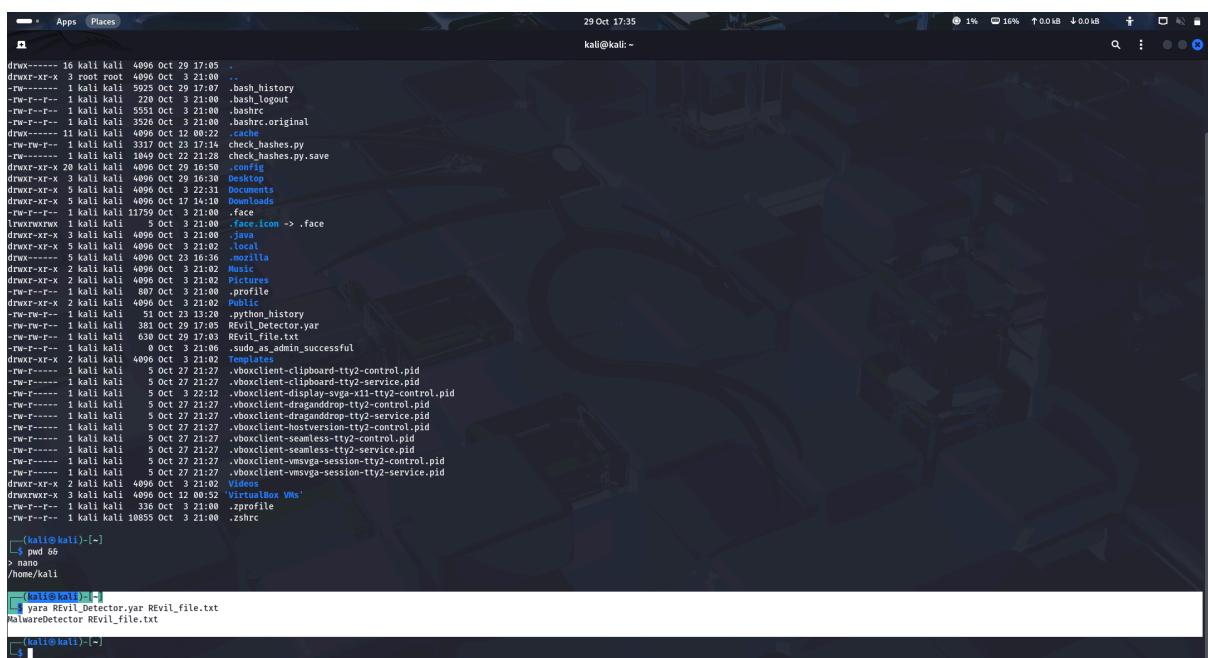
```
rule MalwareDetector
{
    meta:
        description = "Detects REvil malware indicators"
        author = "Neykay"
        date = "2025-10-29"
        threat_level = "Low"

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

    condition:
        any of them
}
```

```
File Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location M-U Undo M-E Redo M-A Set Mark M-J To Bracket M-B Previous M-G Copy M-B Where Was M-F Next M-B Back Forward M-B Prev Word M-B Next Word M-B Home M-B End
```

Yara rule scan



```
29 Oct 17:35                               kali㉿kali:~
```

```
drwx----- 16 kali kali 4096 Oct 29 17:05 .
drwxr-xr-x  3 root root 4096 Oct  3 21:00 ..
rwe-----  1 kali kali 9525 Oct 29 17:07 .bash_history
rwe-r--r--  1 kali kali 5501 Oct  3 21:00 .bash_logout
rwe-r--r--  1 kali kali 5501 Oct  3 21:00 .bashrc
rwe-r--r--  1 kali kali 3526 Oct  3 21:00 .bashrc.original
drwx----- 11 kali kali 4096 Oct 12 00:22 .cache
rwe-rw---  1 kali kali 3317 Oct 23 17:14 check_hashes.py
rwe-rw---  1 kali kali 1847 Oct 22 21:20 check_hashes.py.save
drwxr-xr-x  20 kali kali 4096 Oct 29 16:30 .config
drwxr-xr-x  3 kali kali 4096 Oct 29 16:30 .config
drwxr-xr-x  5 kali kali 4096 Oct  3 22:31 .Documents
drwxr-xr-x  5 kali kali 4096 Oct 17 14:18 .Downloads
drwxr-xr-x  1 kali kali 11759 Oct  3 21:00 .face
drwxrwxrwx  1 kali kali 6508 Oct 29 17:07 .face/icon -> .face
drwxr-xr-x  3 kali kali 4096 Oct  3 21:00 .java
drwxr-xr-x  5 kali kali 4096 Oct  3 21:02 .local
drwx-----  5 kali kali 4096 Oct 23 16:36 .mozilla
drwxr-xr-x  2 kali kali 4096 Oct  3 21:02 .Music
drwxr-xr-x  1 kali kali 4096 Oct 29 16:30 .Pictures
drwxr-xr-x  1 kali kali 807 Oct  3 21:00 .profile
drwxr-xr-x  2 kali kali 4096 Oct  3 21:02 .Public
rwe-rw---  1 kali kali 51 Oct 23 13:28 .python_history
rwe-rw---  1 kali kali 381 Oct 29 17:05 REvil_Detector.yar
rwe-rw---  1 kali kali 6508 Oct 29 17:07 .profilefile.txt
rwe-r--r--  1 kali kali 0 Oct  3 21:00 sudo_as_admin_successful
drwxr-xr-x  2 kali kali 4096 Oct  3 21:02 Templates
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-clipboard-tty2-control.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-clipboard-tty2-service.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-display-synergy-tty2-control.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-draganddrop-tty2-service.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-hostversion-tty2-control.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-seamless-tty2-control.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-seamless-tty2-service.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-vmsvga-session-tty2-control.pid
rwe-r----- 1 kali kali 5 Oct 27 21:27 .vboxclient-vmsvga-session-tty2-service.pid
drwxr-xr-x  2 kali kali 4096 Oct  3 21:02 Videos
drwxrwxr-x  3 kali kali 4096 Oct 12 00:52 'VirtualBox VMs'
drwxr-xr-x  1 kali kali 356 Oct  3 21:00 .profile
rwe-r--r--  1 kali kali 10835 Oct  3 21:00 .zshrc
```

```
[kali㉿kali:~]
```

```
-> pwd
/home/kali
```

```
[kali㉿kali:~]
```

```
$ yara REvil_Detector.yar REvil_file.txt
MalwareDetector REvil_file.txt
```

```
[kali㉿kali:~]
```