



# VIRUSTOTAL

Louise Altvater

RCTS CERT



<https://www.virustotal.com/>



[Intelligence](#) [Hunting](#) [Graph](#) [API](#)

 [Sign in](#) [Sign up](#)



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

[FILE](#) [URL](#) [SEARCH](#)



Choose file

# VTAPI - HTTPS://DEVELOPERS.VIRUSTOTAL.COM/V2.0/



VTAPI

API Reference

JUMP TO CTRL-J

BASICS

- Getting started with v2
- Public vs Premium API
- API responses

FILES

- /file/report** GET
- /file/scan POST
- /file/scan/upload\_url GET
- /file/rescan POST
- /file/download GET
- /file/behaviour GET
- /file/network-traffic GET
- /file/feed GET
- /file/clusters GET
- /file/search GET

URLS

- /url/report GET
- /url/scan POST
- /url/feed GET

DOMAINS & IPS

- /domain/report GET
- /ip-address/report GET

COMMENTS

- /comments/get GET
- /comments/put POST

## /file/report

GET https://www.virustotal.com/vtapi/v2/file/report

Retrieve file scan reports

YOUR REQUEST HISTORY

| TIME                | STATUS | PATH | USER AGENT   |
|---------------------|--------|------|--------------|
| 10/18/2022 02:56 PM | 200    |      | API Explorer |

The `resource` argument can be the MD5, SHA-1 or SHA-256 of a file for which you want to retrieve the most recent antivirus report. You may also specify a `scan_id` returned by the [/file/scan](#) endpoint.

If the `allInfo` argument is set to `true` additional information other than the antivirus results is returned. This additional information includes:

- the output of several third party tools acting on the file (PDFID, ExifTool, sigcheck, TrID, etc).
- the output of other in-house technologies.
- metadata regarding VirusTotal submissions:
  - number of unique sources that have sent the file in the past
    - `first_seen` first seen date
    - `submission_names` a list of file names it was submitted as
- `behaviour-v1` output of behavioral sandboxes if there was successful execution in the sandbox.
  - File operations (read, write, open, etc)
  - Network operations
  - Mutex/registry operations

**sandbox data**

The [file/behaviour](#) has the raw sandbox data, and requires additional parsing on the client side. [file/report](#) with `allInfo | behaviour-v1` contains a good summary

**Private API**

The `allInfo` argument is available in the [Private API](#) only.

Example response

LANGUAGE

- Shell
- Python
- PHP

```
DEFAULT
REQUEST
1 import requests
2
3 url = 'https://www.virustotal.com/vtapi/v2/file/report'
4
5 params = {'apikey': '<apikey>', 'resource': '<resource>'}
6
7 response = requests.get(url, params=params)
8
9 print(response.json())
Replay Request

RESPONSE 200
1- {
2-   "scans": {
3-     "Bkav": {
4-       "detected": true,
5-       "version": "1.3.0.9899",
6-       "result": "W32.AIDetect.malware1",
7-       "update": "20220710"
8-     },
9-     "Lionic": {
10-      "detected": true,
11-      "version": "7.5",
12-      "result": "Trojan.Win32.Nanna.toNI",
13-      "update": "20220710"
14-    },
15-     "Elastic": {
16-      "detected": true,
17-      "version": "4.0.40",
18-      "result": "malicious (high confidence)",
19-      "update": "20220623"
20-    },
21-     "DrWeb": {
22-      "detected": true,
23-      "version": "7.0.56.4040",
24-      "result": "Trojan.Encoder.10718",
25-      "update": "20220710"
26-    },
27-     "Cynet": {
28-      "detected": true,
29-      "version": "4.0.0.27",
30-      "result": "Malicious (score: 100)",
31-      "update": "20220710"
32-    },
33-     "FireEye": {
34-      "detected": true,
```

[HTTPS://WWW.VIRUSTOTAL.COM/](https://www.virustotal.com/)



Este e-mail não está sendo exibido corretamente? [Veja no seu navegador.](#)

Quer ainda mais **segurança e comodidade** para todos os seus momentos?

Querido cliente do BB

**Mantenha o seu cadastro sempre atualizado!**

Mudou de telefone, endereço ou tem um novo e-mail? Avise o BB! Com o seu cadastro atualizado, evite de ter sua conta bloqueada!

Aplicativo Banco do Brasil para celular. Fácil, seguro e completo. Baixe agora.

Atualize agora no App

<http://www.atualizarconta.com/>

The advertisement features a woman with long dark hair looking at her smartphone. The background is a mix of yellow and blue geometric shapes. The text is in white and blue, with key phrases in bold. A hand cursor icon points to the 'Atualize agora no App' button, which is linked to the URL 'http://www.atualizarconta.com/'.

# ANÁLISE DE URLS - HTTP://WWW.ATUALIZARCONTA.COM



- **Ao pesquisar pelo URL através do VirusTotal, podemos confirmar que nosso colega está certo em achar que o email seja suspeito?**
  - ❖ Sim
- **Qual foi a classificação que o site recebeu dos diferentes vendors?**
  - ❖ Phishing e Malicious
- **Quando é que este URL foi submetido para análise pela primeira vez?**
  - ❖ 2017-08-19 18:31:17 UTC

# ANÁLISE DE URLS



Qual destes dois URLs parece suspeito:

- <http://sandk8s30.dlc.zzbm.360es.cn>
- <https://www.peterclarkllc.com>

# ANÁLISE DE BINÁRIOS



ChromeSetup.exe



ChromeSetup.exe

# ANÁLISE DE BINÁRIOS



**LINUX:**

**ssh sebastiao@193.136.2.x**

**Password: ...**

**PUTTY:**

No campo Host Name (or IP address)

**sebastiao@193.136.2.x**



# ANÁLISE DE BINÁRIOS



Qual é o hash sum SHA256 de cada um dos ficheiros? (sha256sum NomedoFicheiro)

1. `1e7c91dbce7e273ce973bd366df311e3ce5fe47621b2bc13ae0e1e5922811e03`
2. `cf8533849ee5e82023ad7adbdbd6543cb6db596c53048b1a0c00b3643a72db30`

Qual é o nome dos ficheiros sugeridos pelo VirusTotal e o tamanho de cada ficheiro?

1. `GoogleUpdateSetup.exe` - 1.36 MB
2. `EternalRocks.exe` – 5.03 MB



**Quais são as táticas de Defense Evasion usadas por este malware?**

- ❖ Masquerading (T1036), Virtualization/Sandbox Evasion (T1497) e Disable or Modify Tools (T1562.001)

**Quantos Contacted IP Addresses estão associados com este ficheiro?**

- ❖ 5

# ANÁLISE DE BINÁRIOS



**Alguma sandbox detetou o ficheiro como malicioso?**

❖ Não

**O ficheiro possui algum tipo de assinatura?**

❖ Sim, Copyright 2018 Google LLC

**Quem são os Signers?**

❖ Google LLC e DigiCert



Obrigada!