

Download utilizando MalwareBazaar API

Para interagir com a API do MalwareBazaar, você precisa obter uma Auth-Key. Se ainda não tiver uma, você pode obtê-la gratuitamente aqui:

<https://auth.abuse.ch/>

Profile Settings

Required

Screen Name

Nome

✓

username is available

Display Name

Nome display

✓

Email

email@gmail

you'll need to confirm you email address if you change it

X not Connected

This account doesn't have an X user associated with it. If you've used the abuse.ch sites with your X or Twitter login before, you can **connect your old contributions to this account** by connecting your X account below. You can disconnect the login method later if you want.

Don't show this message again

Optional

Pushover Token

Malpedia API key

Auth Key

generated

Generate Key

Avatar

change

delete

Hide Profile

☐

Save Profile

Reset

Preencha com Nome e Email

Gere sua chave de autenticação e salve em um local seguro, e salve o perfil.

Vamos fazer o download através do SHA-256, existem duas formas de fazer isso:

Acesse site do Malware bazaar: <https://bazaar.abuse.ch/browse/>

SHA256 hash	Type	Signature
1ea3b0dde89c84697818...	sh	Mirai
e48926cb822fe5fd29a81...	exe	
d38e82d4afd8416c456b...	elf	Mirai
e235aca768ae0905c9e13...	elf	Mirai
bf4ee47d0df1870104f4fa...	exe	Bancos

Identifique o tipo exemplo: .exe e a signature exemplo Bancos

Ao clicar em uma determinada Signature você verá a lista de todas amostra adicionadas:

The table below shows all malware samples that have been identified by MalwareBazaar as **Bancos** (max 1000).

Show 50 entries

Firstseen (UTC)	SHA256 hash	Tags
2025-04-10 13:15:25	bf4ee47d0df1870104f4fa...	Bancos, genome, exe, signed
2025-02-25 12:20:56	04525932d4faea070cd04...	Bancos, EngineGame, exe, signed
2024-12-28 21:18:14	9f3b062a0f8caf16be80ac...	AdesStealer, Bancos, BlackGuard, exe, NitroSte...
2024-10-13 21:26:18	07c1abb57c4498748c4f1...	Bancos, exe, signed
2023-05-19 09:16:00	1c74dd43b3f3f5411711b...	Bancos, exe
2023-05-12 16:40:21	4c5bfc6a3ba65d8330eb...	Bancos, exe, signed
2020-11-14 18:09:05	b162273f01fd92f7afa5ae...	Bancos
2020-11-10 11:40:25	72b057c5a0c95d7352fbd...	Bancos
2020-11-08 14:06:35	a753480228263d54de37...	Bancos

Copie os SHA256

Entretanto, o número de amostra máxima que o site permite visualizar é de 1000, e algumas signature tem uma quantidade superior. Uma alternativa é baixar uma planilha onde terá os lotes de todas as amostras a partir do ano 2020.

Acesse site o link: <https://bazaar.abuse.ch/export/>

CSV files

The following data exports exists in CSV format:

- Recent additions (8) [download](#)
- Full data dump (5) [download - zip compressed](#)

Escolha a opção Full data dump

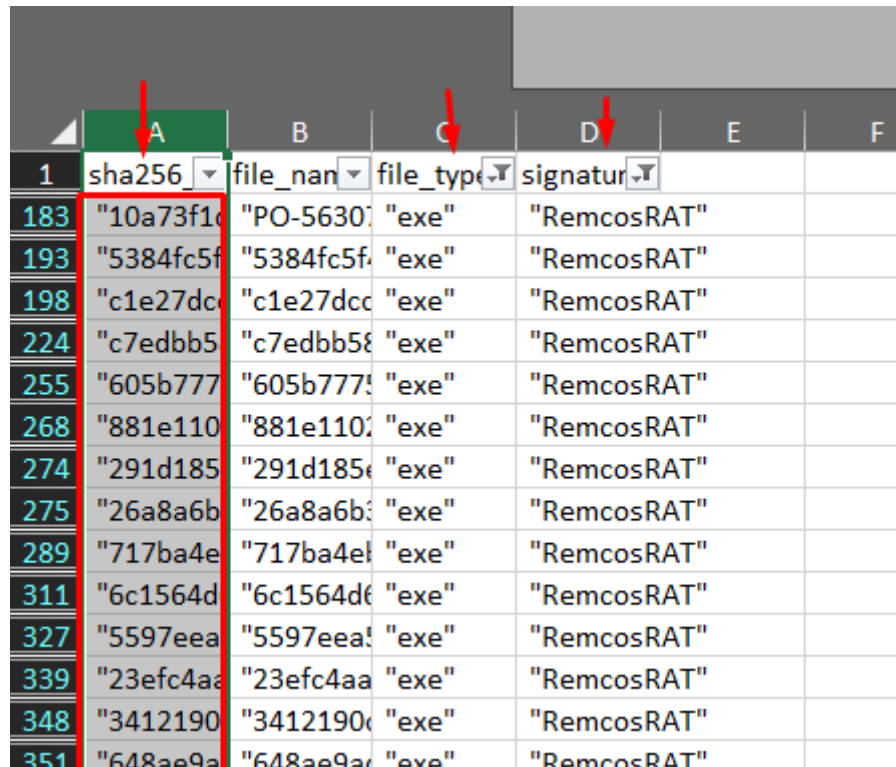
```
# MalwareBazaar full malware samples dump (CSV)
# Last updated: 2025-04-10 12:28:22 UTC
#
# Terms Of Use: https://bazaar.abuse.ch/faq/#tos
# For questions please contact bazaar [at] abuse.ch
#
# "first_seen_utc","sha256_hash","md5_hash","sha1_hash","reporter","file_name","file_type_guess","mime_type","signature","clamav","vipercent","imphash","ssdeep","t
2025-04-10 12:28:22","46e0837be5b484800e694540bbc219e4211e443034c07974f6f50d5def53f1b","6f59b1b8f73966f90be5f99776e052e9","176489884db0f43fcb1a1ea83ae9a31:
2025-04-10 12:26:54","af8598d97a4dd7c2d53a74272a8bb3f9616e189bd9910e0da7eb005a53b58","609fee63801a8892afcdf2e1e16cd146","cf3fa0f758e649725292617b560afe8
2025-04-10 12:26:20","9a8ba2203cf45bb5fe142cb4cee82fe397af4504d51e7fc8c7db19a8ef1c71e4","a3ab6acece6ac4b9d00d6bb6c1ec2a","9c2926c227b1d00ac0b2e8bed9641d1
2025-04-10 12:04:02","aca960aff7773c0de1f1bd6a4760b06f98475b8e23251c3905ed8619216ad956","14153af1a6bf3908ee65c711bd02968c","d50be87eff8c4c83b6f6d0dcb1795c69
2025-04-10 12:03:30","2ae6d996c2ad9e5d2bf6905d8c5c9c16f7a189f91187a6fb79512e7ed99ea50","70173d1e9501797cae7dae9e501aef2b","e2d403cbb64ba0c9acebf5ea0f8c05
2025-04-10 12:03:29","f5d99474cd78ecbfdb5409a54d721c8aca7a0004b09d2d093f31e4785ee3","c37c8e2e2dd67cdd5bb22e8dffc705","94a1a8f9c3e3073df92a9e0f6ebd4c
```

Extraia o CSV e delete partes desnecessárias no início e final.

Para identificar o tipo e a signature é necessário aplicar filtro na planilha, para isso converta o arquivo em .xlsx. Existem várias formas de fazer isso uma delas é pelo site:

<https://www.datablist.com/pt/csv-editor>

Depois de converter para .xlsx, basta agora aplicar os filtros por type e signature e copiar o Sha256



	A	B	C	D	E	F
1	sha256	file_name	file_type	signature		
183	"10a73f1c"	"PO-5630"	"exe"	"RemcosRAT"		
193	"5384fc5f"	"5384fc5f"	"exe"	"RemcosRAT"		
198	"c1e27dc0"	"c1e27dc0"	"exe"	"RemcosRAT"		
224	"c7edbb58"	"c7edbb58"	"exe"	"RemcosRAT"		
255	"605b7779"	"605b7779"	"exe"	"RemcosRAT"		
268	"881e1107"	"881e1107"	"exe"	"RemcosRAT"		
274	"291d185e"	"291d185e"	"exe"	"RemcosRAT"		
275	"26a8a6b3"	"26a8a6b3"	"exe"	"RemcosRAT"		
289	"717ba4e1"	"717ba4e1"	"exe"	"RemcosRAT"		
311	"6c1564d6"	"6c1564d6"	"exe"	"RemcosRAT"		
327	"5597eea3"	"5597eea3"	"exe"	"RemcosRAT"		
339	"23efc4aa"	"23efc4aa"	"exe"	"RemcosRAT"		
348	"3412190c"	"3412190c"	"exe"	"RemcosRAT"		
351	"648ae9a1"	"648ae9a1"	"exe"	"RemcosRAT"		

No código, coloque o SHA-256, sua chave de autenticação e

adicione a linha: `sys.argv.append('-u')`, Caso queira fazer a extração automática do zip. (exemplo abaixo)

```
parser.add_argument('-s', '--hashes', nargs='+', default=[
    "7de2c1bf58bce09eccc70476747d88a26163c3d6bb1d85235c24a558d1f16754"
], type=check_sha256, help='List of SHA-256 hashes')

parser.add_argument('-u', '--unzip', action='store_true', help='Unzip the downloaded files')
parser.add_argument('-i', '--info', action='store_true', help='Get file information (no download)')
args = parser.parse_args()

if args.unzip and args.info:
    print("[ERROR] Please select either unzip or information display, not both.")
    sys.exit(1)

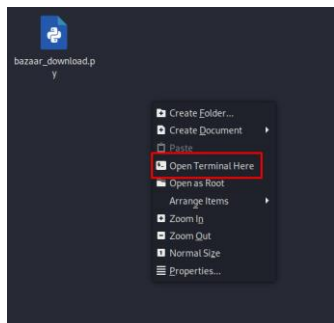
API_KEY = "SUA API AQUI"
headers = {'API-KEY': API_KEY}
ZIP_PASSWORD = b'infected'
```

Colocar um ou mais SHA-256 separados por vírgula

Colocar a chave de autenticação

```
if __name__ == "__main__":
    #sys.argv.append('-u')    #colocar essa linha para extrair automática
    main()
```

Coloque o código dentro da pasta e abra um terminal



Execute o comando: `python bazaar_download.py`

E espere o Download e extração terminar

