|  |
| --- |
| [Nom de la société] |
| Threat Intelligence Sources |
| [Sous-titre du document] |

|  |
| --- |
| Abdallah Chbaro  09/04/2023 |

Table des matières

[The Hacker News 2](#_Toc132029329)

[Abuse.ch 3](#_Toc132029330)

[Urlhaus.abuse.ch 4](#_Toc132029331)

[Bazaar.abuse.ch 4](#_Toc132029332)

[VirusTotal 5](#_Toc132029333)

[AnyRun 7](#_Toc132029334)

[GitHub 10](#_Toc132029335)

[Twitter 10](#_Toc132029336)

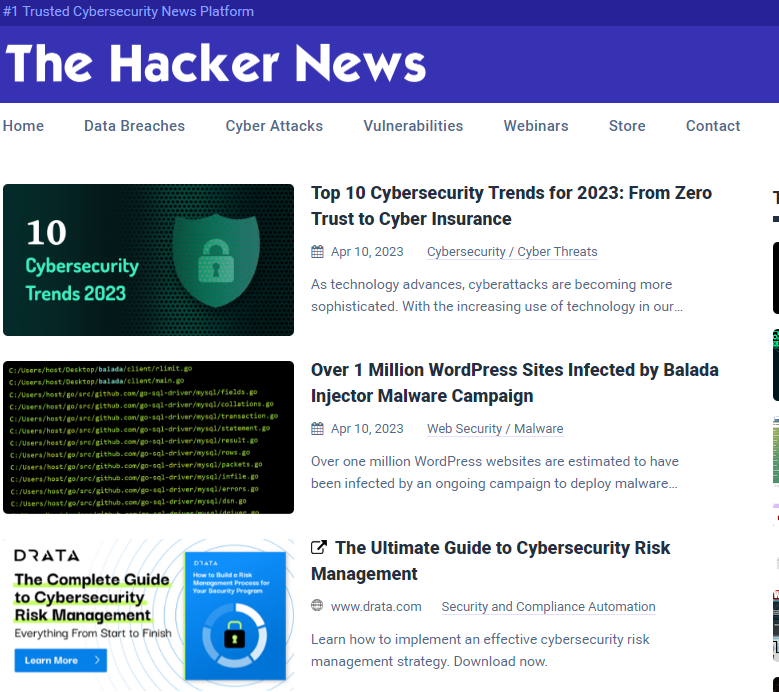
[RSS Feeds 11](#_Toc132029337)

[Articles 12](#_Toc132029338)

[YouTube 13](#_Toc132029339)

# The Hacker News

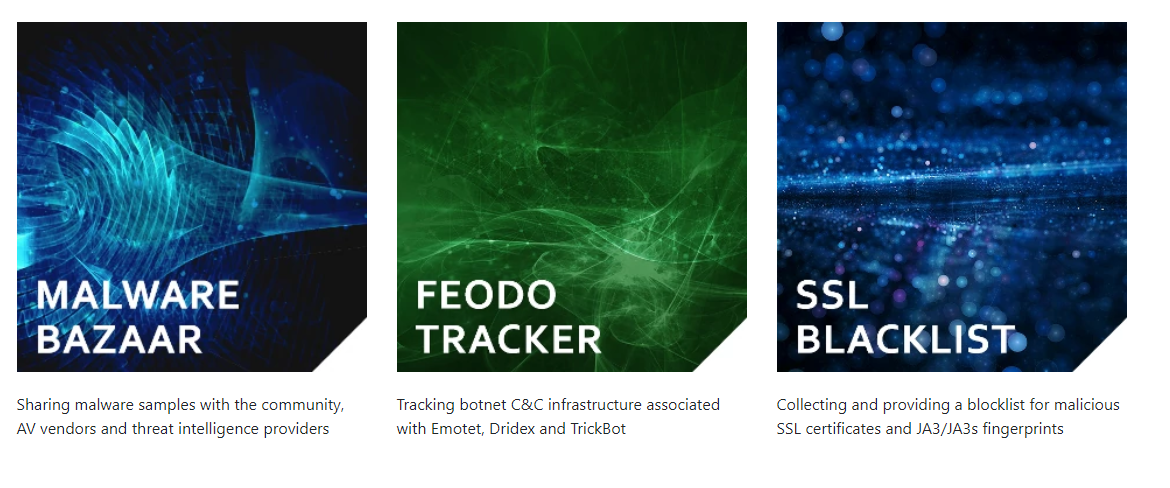
The Hacker News is a telemetry service providing real time needs and updates about security content, especially about active malwares and vulnerabilities.

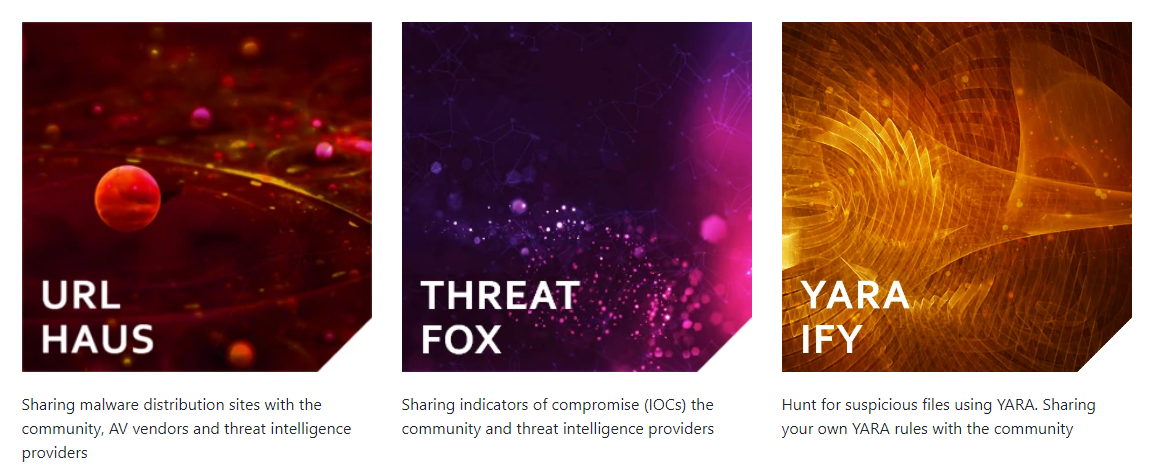


# Abuse.ch

abuse.ch is providing community driven threat intelligence on cyber threats. It is the home of a couple of projects that are helping internet service providers and network operators protecting their infrastructure from malware. IT-Security researchers, vendors and law enforcement agencies rely on data from abuse.ch, trying to make the internet a safer place.

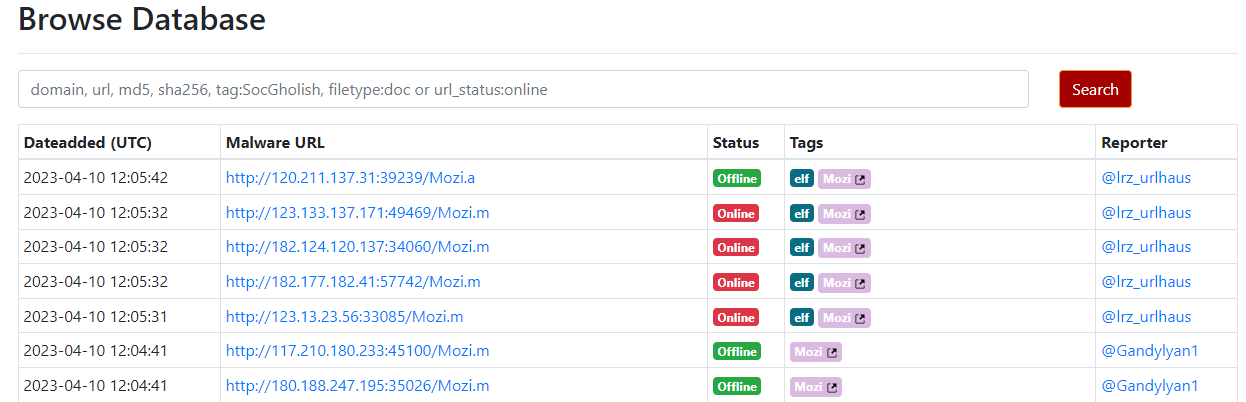
Abuse.ch contains different platforms, listed in the below screenshot:





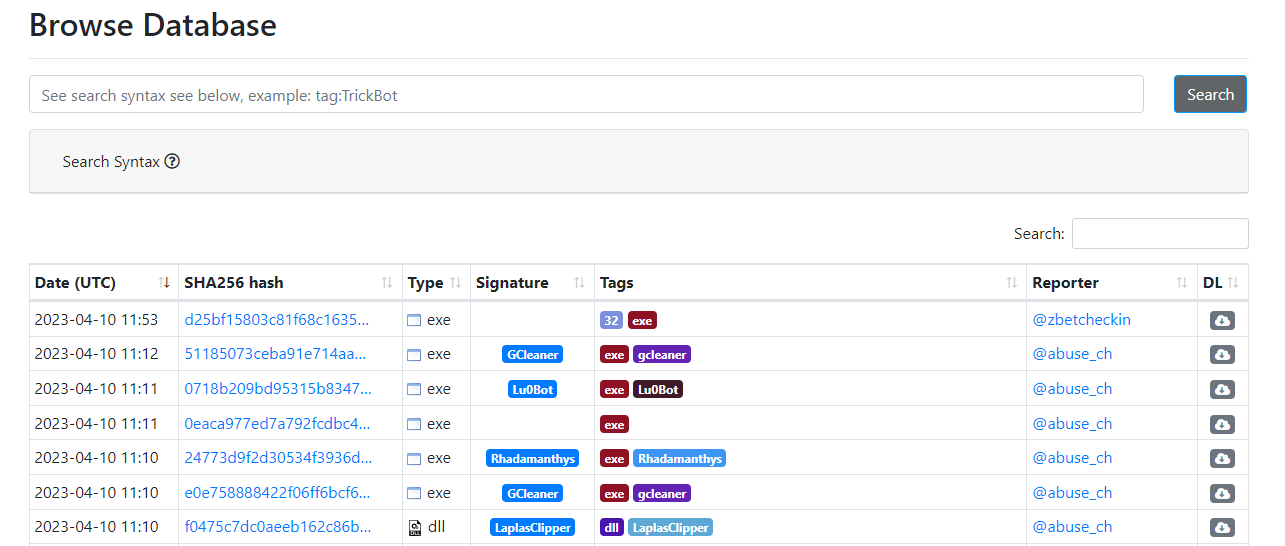
# Urlhaus.abuse.ch

URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution. It can be used to collect IOCs, such as: domains, URLs and Hashes.



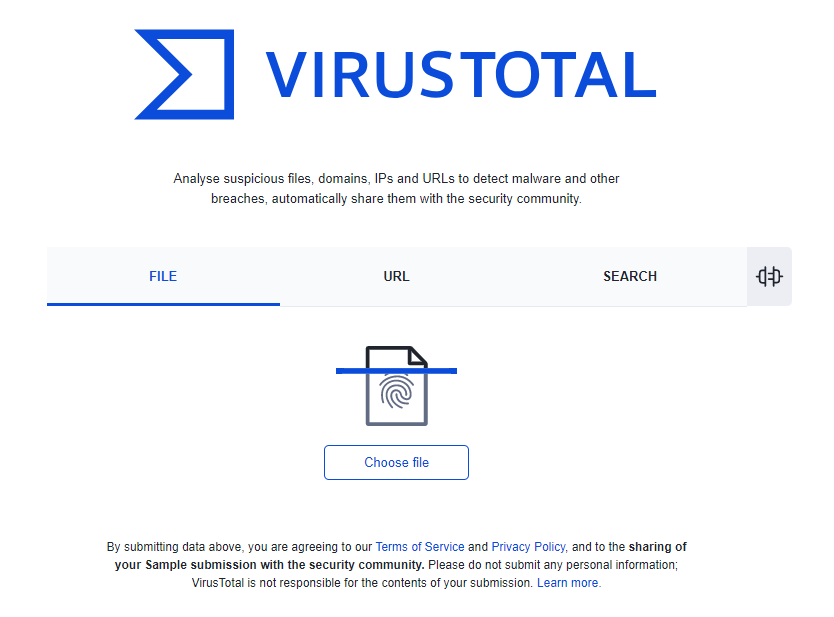
# Bazaar.abuse.ch

MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers.

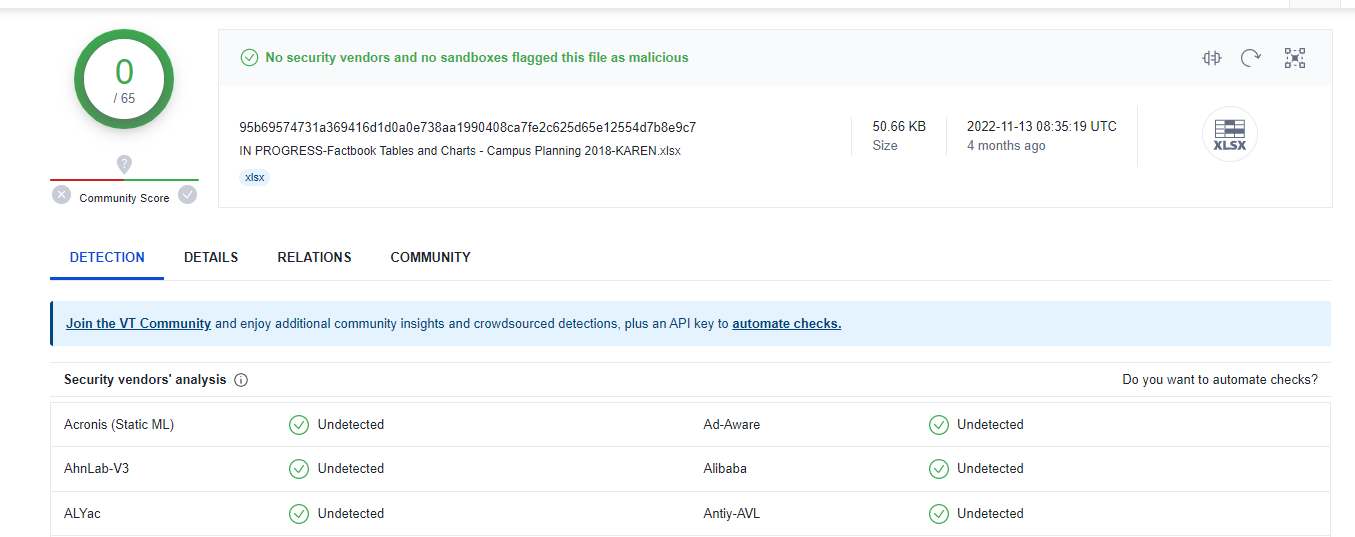


# VirusTotal

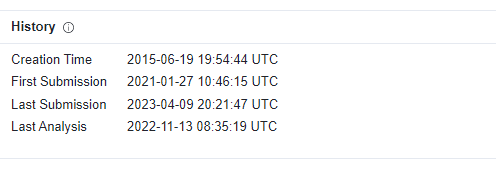
VirusTotal can be used to submit feeds, such as hashes, URLs and file to test against known detection engines.



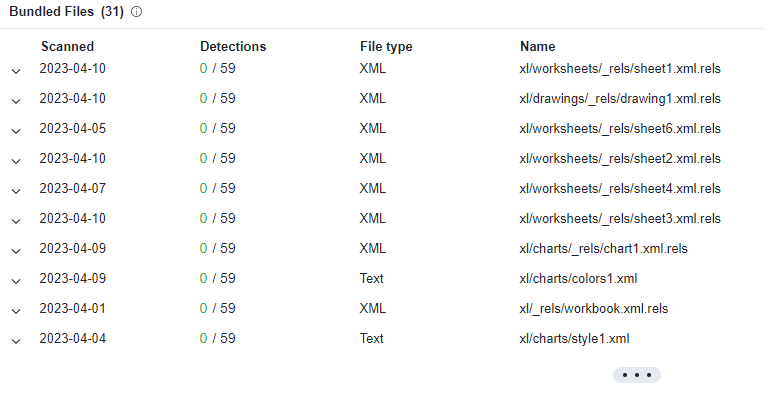
Once a feed is submitted, the result will be as follows:



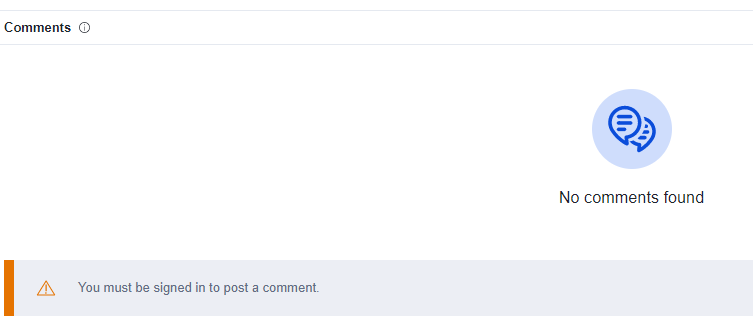
We can collect more information in the details section, such as the creation time and the last submission time, to check if the malware is still active:



Moreover, we can check relationships with other IOCs:

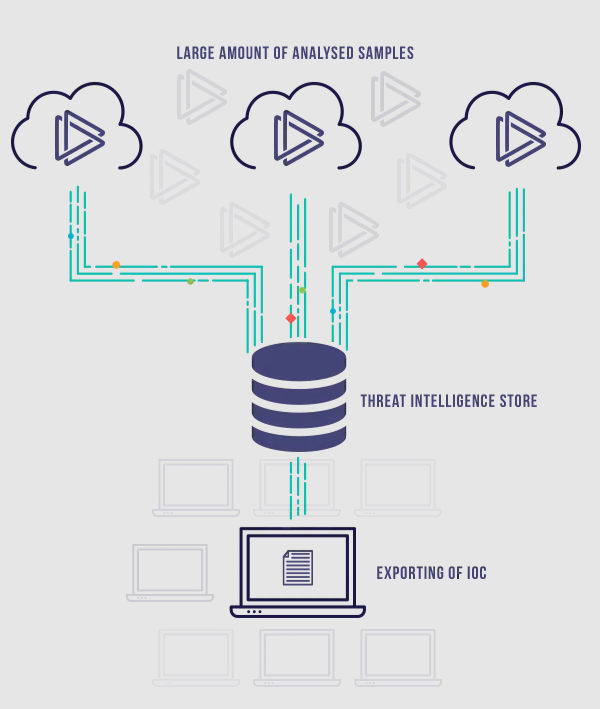


Finally, we can check the community section, to see what other wrote about the feed:

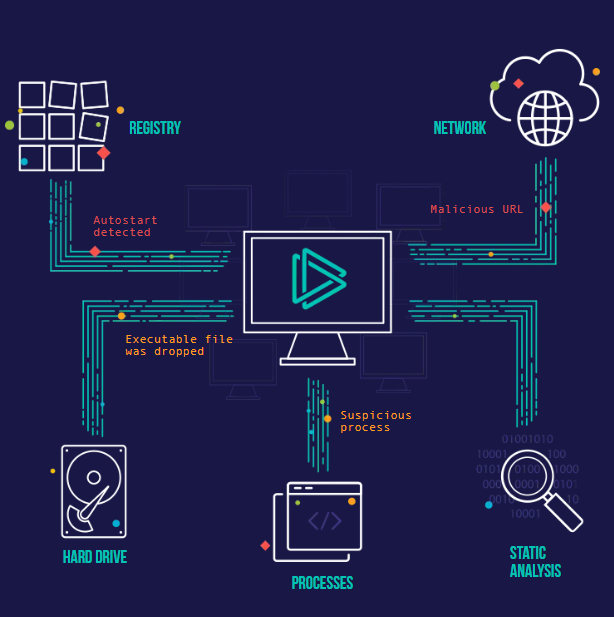


# AnyRun

AnyRun is primarly used as an online sandbox. However, it contains a threat intelligence platform. A community consisting of a large number of researchers from different countries contributes to our threat intelligence platform, allowing to collect and analyze attacks at the moment of their appearance, revealing the IOC at the initial stage. The malware reports can be accessed through public submissions and downloaded in specialized formats.



Once a feed is submitted, it will test all its behavior, as shown below:



At the end, AnyRun will generate a detailed report about the behavior and will qualify it as malicious or not.

# GitHub

GitHub is enriched by community members that shares everything we need about a specific malware. For example, we can find detailed description and IOCs.

# Twitter

A lot of security vendors, researchers and community post their findings on twitter. For example, we can have a look at the following accounts:

* Sophos
* Cisco Talos Intelligence
* Secjuice
* KitPloit
* Hipotermia
* Brad
* Abel
* German Fernandez
* Ankit Anubhav
* Execute Malware
* ProxyLife
* Cryptolaemus
* Huskyhacks
* And a lot more …

# RSS Feeds

Imagine being able to log into one dashboard and getting the latest news and events from all of your favorite websites, blogs, or podcasts? With RSS feeds, it’s possible!

Checking each site one by one will take forever. Signing up for their newsletters could ensure you keep up with the latest updates and information, but it’s also easy to mistake the emails as spam or to ignore them altogether in your crowded inbox. Then again, relying solely on the site’s social media updates might mean you miss something important you wanted to know about.

In an RSS feed, these updates and notifications are gathered, organized, and updated in real-time into one convenient dashboard. Awesome right?

Hence, RSS feeds are used to receive information, updates and IOCs, instead of going out to search through the internet. Most of security vendors provide RSS feeds, such as:

* Sophos News
* ReversingsLabs Blog
* The Hacker News
* Red Canary Blog
* The DFIR Report

# Articles

Report and Google articles can also be analyzed. For example, the following share updated articles and reports:

* Fortinet
* MalwareBytes
* Red Canary
* ZScaler
* SentionelOne
* Kaspersky
* TrendMicro
* NordVPN

# YouTube

My favorite YouTube channel for malware analysis and security content is ‘John Hammound’. He analyzes updated malwares and gets in deep.

