**Hybrid Analysis**

**Malicious File Analysis | 23.09.2023**

# Executive Summary

Hybrid Analysis is a free online tool that provides a comprehensive analysis of malware samples. The tool uses a variety of techniques, including static analysis, dynamic analysis, and behavioral analysis, to identify the capabilities and behavior of malware samples. Hybrid Analysis is a valuable tool for malware analysts, security researchers, and incident responders.

This tool report provides a comprehensive overview of the installation, execution, scope, and limitations of the Hybrid Analysis tool. The report also includes recommendations for how to use the tool effectively.

# Index

[**Executive Summary 2**](#_heading=h.gjdgxs)

[**Index 2**](#_heading=h.30j0zll)

[**1. Introduction 2**](#_heading=h.1fob9te)

[**2. Tool Details 2**](#_heading=h.3znysh7)

[**3. Installation 3**](#_heading=h.2et92p0)

[**4. Execution 3**](#_heading=h.tyjcwt)

[**5. Scope and Limitations 3**](#_heading=h.3dy6vkm)

[**6. Conclusion 3**](#_heading=h.1t3h5sf)

[**7. References (if any) 4**](#_heading=h.4d34og8)

# Introduction

Malware analysis is the process of examining malware to understand its capabilities, behavior, and how to mitigate it. Hybrid Analysis is a free online tool that can help malware analysts perform a comprehensive analysis of malware samples.

Hybrid Analysis uses a variety of techniques to analyze malware samples, including:

* Static analysis: Static analysis involves examining the code of a malware sample to identify its capabilities.
* Dynamic analysis: Dynamic analysis involves executing a malware sample in a controlled environment to observe its behavior.
* Behavioral analysis: Behavioral analysis involves monitoring the behavior of a malware sample to identify its interactions with the operating system and other software.

Hybrid Analysis also uses machine learning techniques to identify malware samples that are similar to known malware samples. This can be useful for identifying new malware samples or malware samples that have been modified to evade detection.

# Tool Details

It is a web based tool.

<https://www.hybrid-analysis.com/>

# Installation

**Hybrid Analysis is a web-based tool, so there is no need to install any software. To use the tool, simply visit the Hybrid Analysis website and create an account.**

# Execution

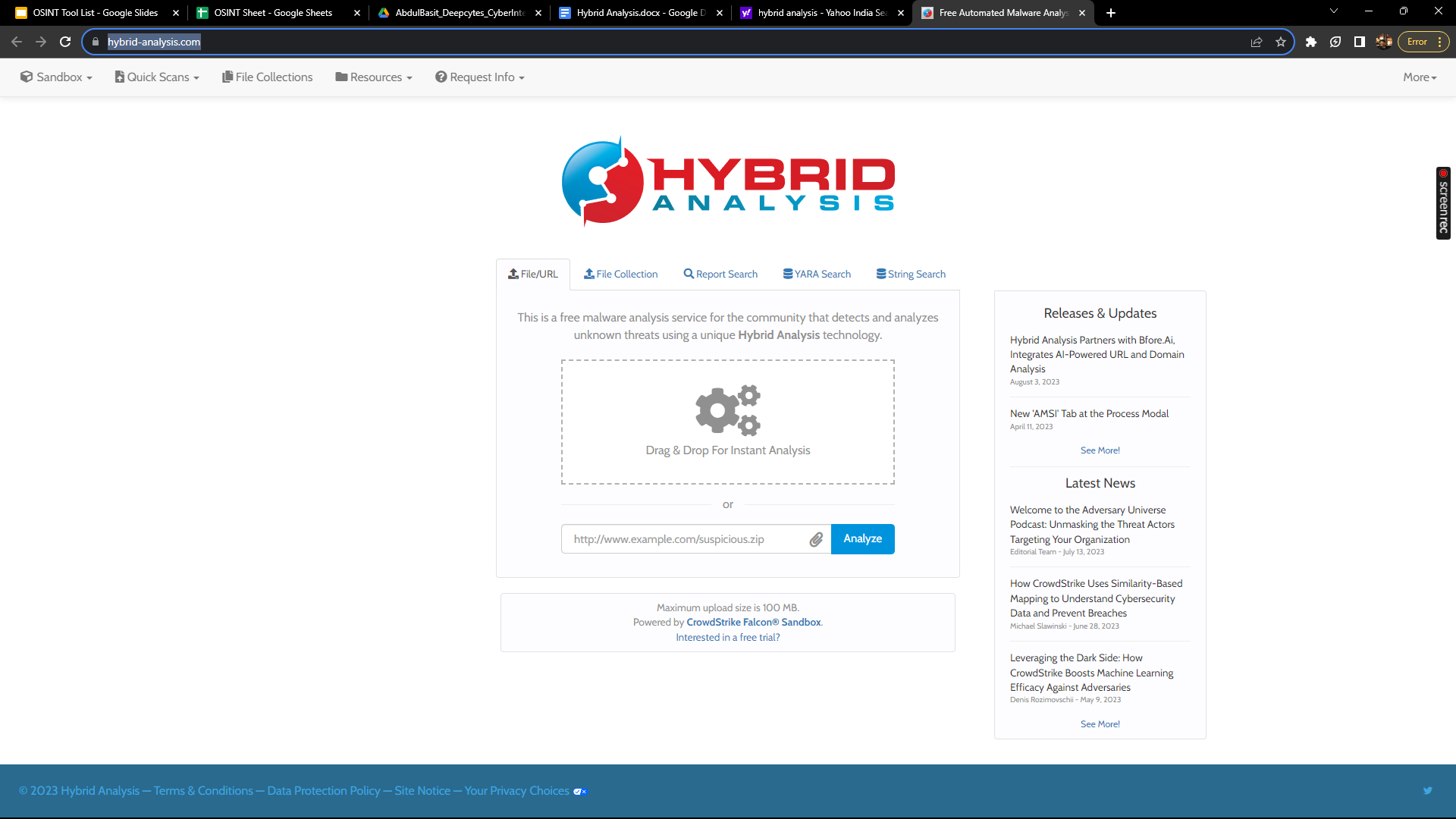
To analyze a malware sample with Hybrid Analysis, simply upload the sample to the website and click "Analyze." Hybrid Analysis will then begin analyzing the sample using the techniques described above.

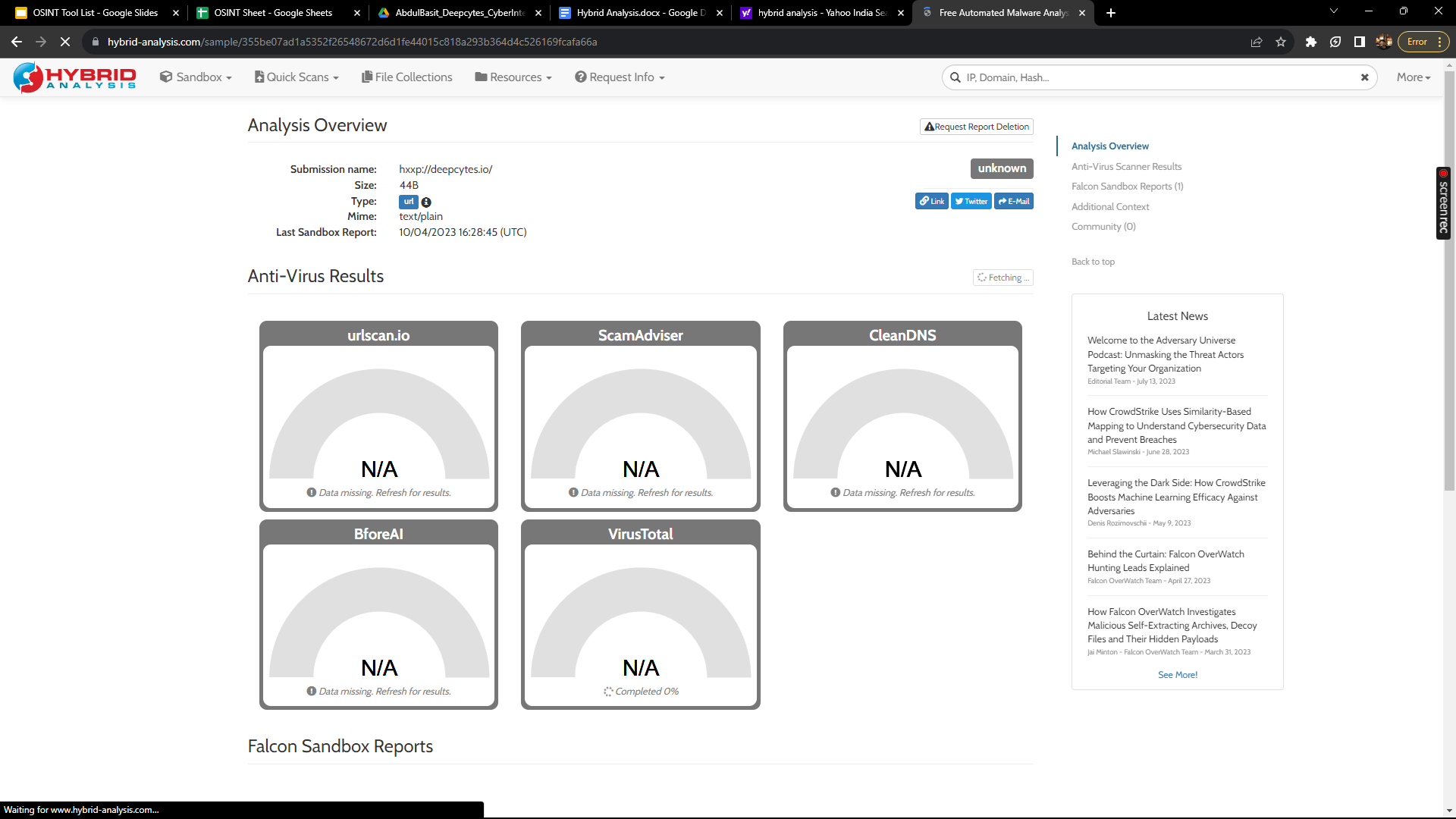
Once the analysis is complete, Hybrid Analysis will provide a report that includes the following information:

* The name of the malware sample
* The file type of the sample
* The size of the sample
* The date that the sample was uploaded
* The results of the malware analysis

The results of the malware analysis can include the following information:

* The capabilities of the malware sample
* The behavior of the malware sample
* The malware families or campaigns that the malware sample is related to
* The tools and techniques that the malware sample uses
* The vulnerabilities that the malware sample exploits





# Scope and Limitations

Hybrid Analysis is a powerful tool for analyzing malware samples. However, it is important to be aware of the limitations of the tool.

Hybrid Analysis can only analyze malware samples that have been uploaded to the website. This means that Hybrid Analysis will not be able to analyze all malware samples in existence.

Additionally, Hybrid Analysis cannot guarantee that the results of the malware analysis are accurate or up-to-date. It is possible that the results of the malware analysis may be incorrect or out of date.

# Conclusion

Hybrid Analysis is a valuable tool for malware analysts, security researchers, and incident responders. The tool is easy to use and provides a variety of useful features. However, it is important to be aware of the limitations of the tool before using it.