**Decalage Malware Search**

**Malicious File Analysis | 23.09.2023**

# Executive Summary

Decalage is a free online tool that allows users to search for malware samples containing specific strings, filenames, hashes, or other indicators of compromise (IOCs). Decalage indexes data from several malware analysis websites, including malwr.com, hybrid-analysis.com, virustotal.com, and virusshare.com. This makes it 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 Decalage malware search 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. Decalage is a free online tool that can help malware analysts search for malware samples containing specific strings, filenames, hashes, or other IOCs. This can be useful for identifying malware samples that are related to a particular attack or campaign, or for finding malware samples that are similar to known malware samples.

Decalage indexes data from several malware analysis websites, including malwr.com, hybrid-analysis.com, virustotal.com, and virusshare.com. This makes it a valuable tool for malware analysts, security researchers, and incident responders.

# Tool Details

It is a web based tool.  
http://www.decalage.info/en/mwsearch#gsc.tab=0

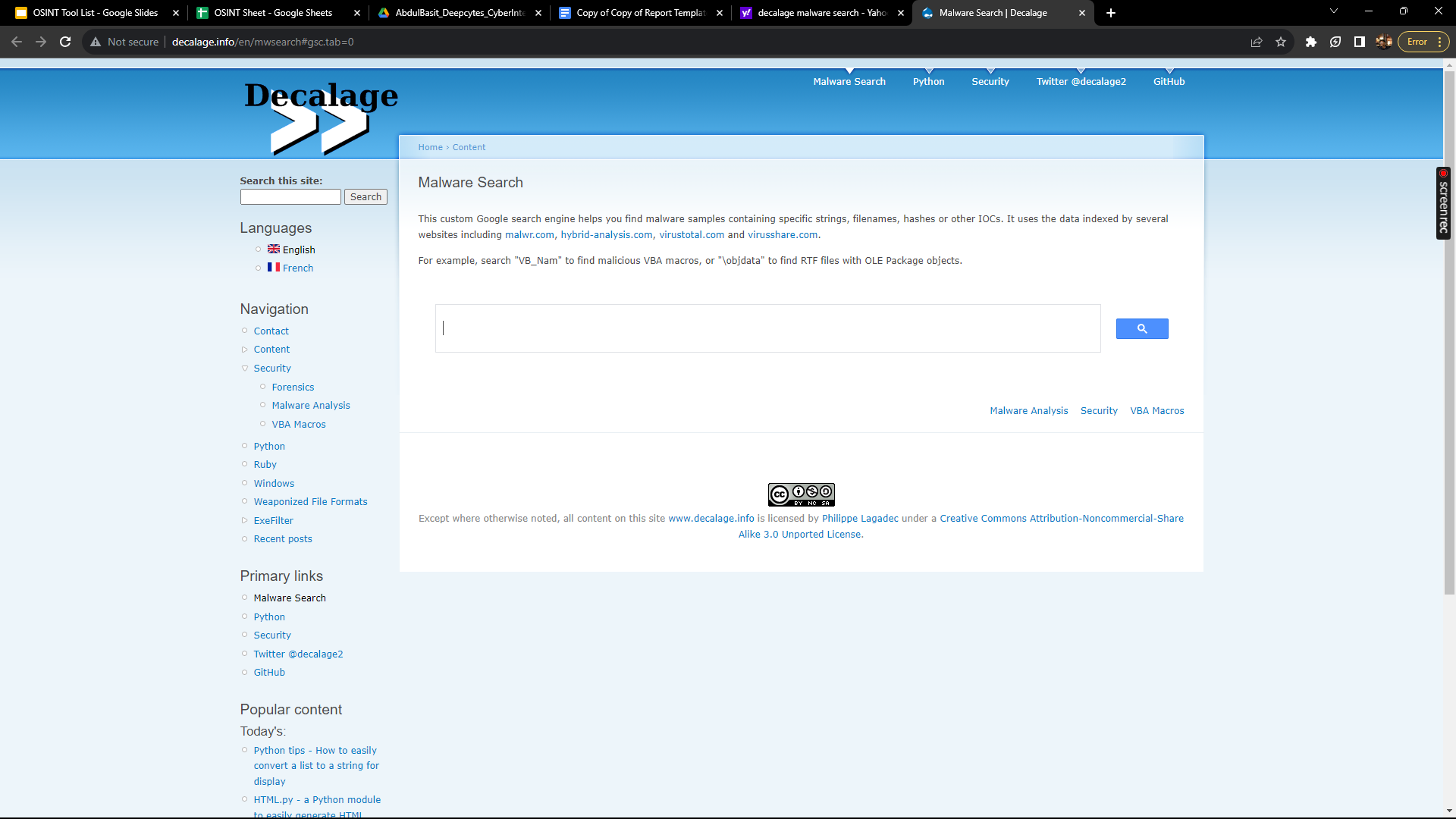
# Installation

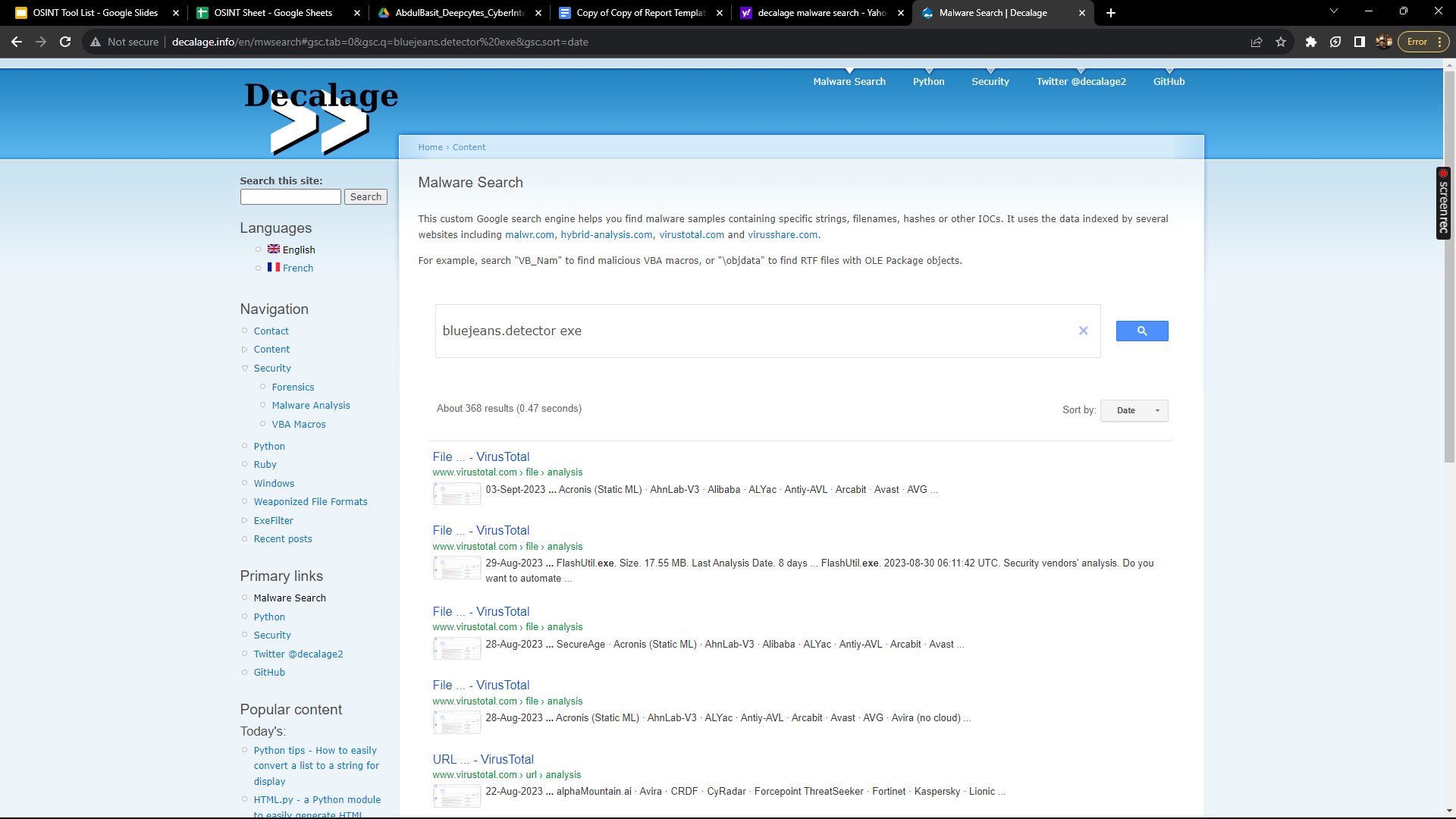
**Decalage is a web-based tool, so there is no need to install any software. To use the tool, simply visit the Decalage website and create an account.**

# Execution

To use the Decalage malware search tool, simply enter the string, filename, hash, or other IOC that you want to search for into the search bar and click "Search." Decalage will then return a list of malware samples that contain the specified IOC.

The search results will include the name of the malware sample, the file type, the size of the file, the date that the file was uploaded, and the websites where the file has been analyzed. You can also click on the name of a malware sample to view more information about the sample, such as the results of the malware analysis.





# Scope and Limitations

Decalage is a powerful tool for searching for malware samples. However, it is important to be aware of the limitations of the tool.

Decalage can only search for malware samples that have been uploaded to the malware analysis websites that it indexes. This means that Decalage will not be able to find all malware samples in existence.

Additionally, Decalage cannot guarantee that the information that it returns is accurate or up-to-date. It is possible that the information that Decalage returns may be incorrect or out of date.

# Conclusion

Decalage 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.

Recommendations

To use the Decalage malware search tool effectively, it is important to understand its limitations. For example, Decalage can only search for malware samples that have been uploaded to the malware analysis websites that it indexes. Additionally, Decalage cannot guarantee that the information that it returns is accurate or up-to-date.

It is also important to use Decalage in conjunction with other tools and services. For example, you could use Decalage to search for malware samples containing a specific IOC, and then use a different tool to analyze the malware samples in more detail.

Additionally, it is important to regularly review the search results from Decalage. This will help you to identify any new malware samples that have been uploaded to the malware analysis websites that Decalage indexes.

Overall, the Decalage malware search tool is a valuable resource for malware analysts, security researchers, and incident responders.