**LAB 6: Public AV Scanners (VirusTotal, JoeSandbox)**

**Public AV Scanners**

* VirusTotal
* JoeSandbox
* hybrid-analysis.com

**VirusTotal**

* VirusTotalis a subsidiary of Google that analyzes files and URLs. Apart from the free interface, VirusTotalalso has both a private and a public API.
* The results from VirusTotalinclude the detection results of the malware by the supportedantivirusengines. This allows you to better evaluate if you are at risk.
* You can upload different types of files, such as a Windows executable, Android APKs, PDFs, images and JavaScript code.
* The online reports are not individually downloadable, but they are very detailed.
* **Download a sample malware on**
* https://wildfire.paloaltonetworks.com/publicapi/test/pe
* **Upload VirusTotal**

**A screenshot of a computer program

Description automatically generated**

Em tải file malware xuống rồi up lên **VirusTotal**

A screenshot of a computer

Description automatically generated

* **JoeSandbox**

Joe Sandbox Cloud executes files and URLs fully automated in a controlled environment and

monitors the behavior of applications and the operating system for suspicious activities

**Key Features**

* Submit samples and URLs for sandbox analysis
* Search, list, get, download, and delete analyses
* Get, list, and manage server and user info

**Requirements**

* API Key
* Sandbox server (if not using cloud)

**Resources**

* Joe Sandbox API
* Joe Sandbox API wrapper
* Report formats

**Supported Product Versions**

* Joe Sandbox API v2
* A screenshot of a computer

  Description automatically generated

<https://www.joesandbox.com/analysis/1423621/0/html>

A screenshot of a computer

Description automatically generated

* **hybrid-analysis.com**

Download a sample malware on

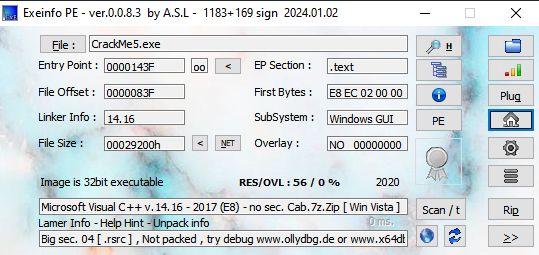
<https://wildfire.paloaltonetworks.com/publicapi/test/pe>

Upload hybrid-analysisA screenshot of a web page

Description automatically generated

**CrackME5**

Em kiểm tra file với tool ExeInfo để xác định thông tin cơ bản của file



Đề bài ở đây là A close up of a message

Description automatically generated

Ở đây em chú ý tới hàm cmp ở dòng thứ 38. Nó sẽ so sánh cái mình nhập vào với outPutString là -3258523. Cái này thì em đã debug ra và biết được  
A screenshot of a computer program

Description automatically generated

Vậy password sẽ là cái **username** + **`-3258523**`

A screenshot of a computer

Description automatically generated