Malware Sandboxing

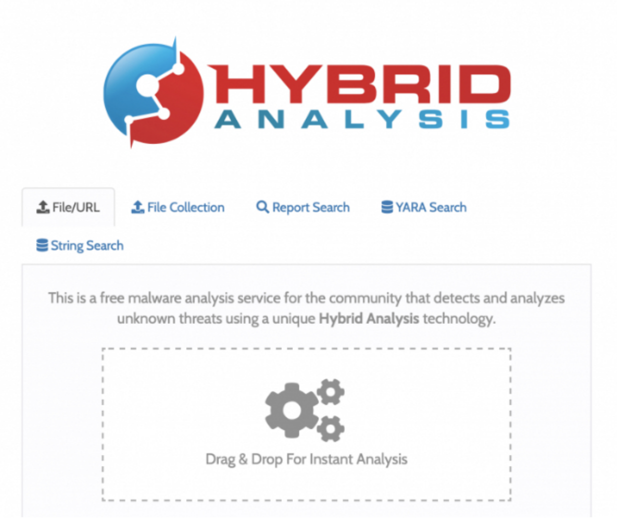
Blue Team Level 1 Certification (Standard) > PA5) Analysing URLs, Attachments, and Artifacts > M... COMPLETE

Sandboxing is the process of detonating (running/executing) a piece of malware in a contained environment, and closely monitoring exactly what the software does, allowing security teams to collect indicators of compromise. Examples include monitoring the network traffic to see if the malware tries to communicate with a command-and-control (C2) server on the internet to receive commands or download additional modules, giving the malware more capability. By understanding how the malware operates, it becomes easier to create defenses that can detect and alert on similar activity.

Security teams will have access to dedicated enterprise-grade sandboxing and malware analysis tools. Replicating this is out of scope for this course, but we can teach you about sandboxing and malware analysis and have you learn to use the online platform Hybrid Analysis.

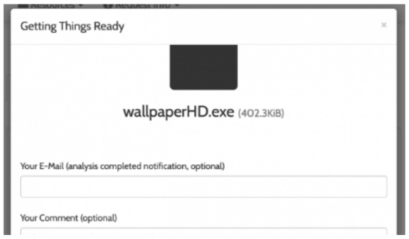
HYBRID ANALYSIS

Hybrid Analysis is an online malware analysis platform that lets you upload malware for instant cloud-based analysis, providing you with a detailed report about the observed activity.



This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

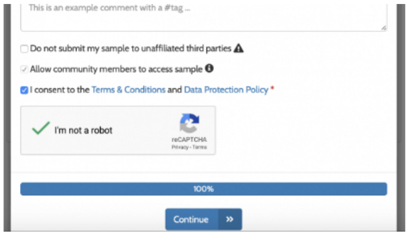
First, navigate to the Hybrid Analysis website. Here you can drag-and-drop, or browse for the file you want to upload.



wallpaperHD.exe (402.3KiB)

Your E-Mail (analysis completed notification, optional)

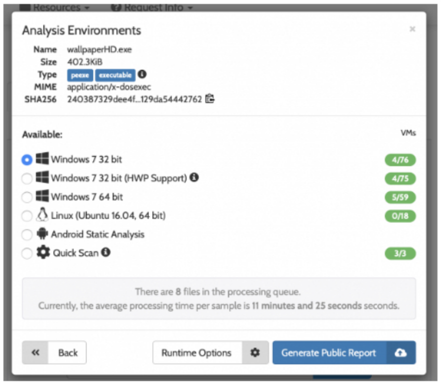
Your Comment (optional)



This is an example comment with a #tag ...

□ Do not submit my sample to unaffiliated third parties ⚠
☑ Allow community members to access sample ℹ
☑ I consent to the Terms & Conditions and Data Protection Policy *

Next, you can choose the operating system that you want to detonate the malware on – this is perfect for malware that only targets specific operating systems. For this activity, we'll just use the default Windows virtual machine.



Analysis Environments

Name wallpaperHD.exe
Size 402.3KiB
Type peexe executable
MIME application/x-dosexec
SHA256 240387329dee4f...129da54442762

Available: VMs

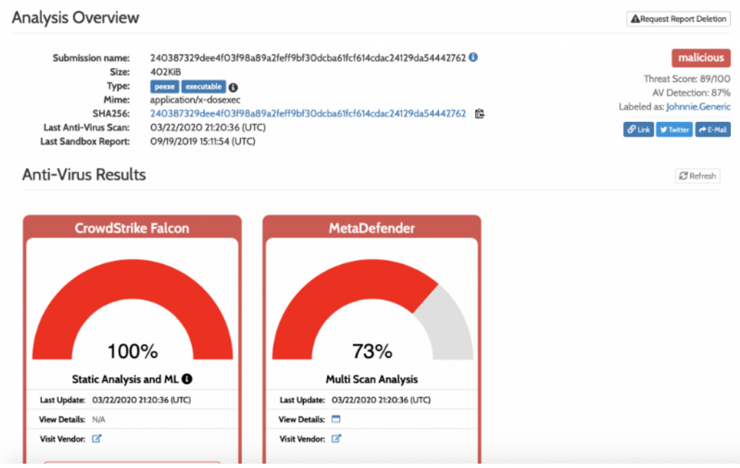
● Windows 7 32 bit 4/76
○ Windows 7 32 bit (HWP Support) 4/75
○ Windows 7 64 bit 5/59
○ Linux (Ubuntu 16.04, 64 bit) 0/18
○ Android Static Analysis
○ Quick Scan 3/3

There are 8 files in the processing queue.
Currently, the average processing time per sample is 11 minutes and 25 seconds seconds.

Once you've clicked "Generate Public Report" you will be directed to the report page once the analysis has completed. You can see this below.

ANALYSIS RESULTS

Below is a screenshot of the results provided by Hybrid Analysis after we uploaded the piece of known malware. You can also view the report yourself here – https://www.hybrid-analysis.com/sample/240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762.



Analysis Overview

Submission name: 240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762
Size: 402KiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: 240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762
Last Anti-Virus Scan: 03/22/2020 21:20:36 (UTC)
Last Sandbox Report: 09/19/2019 15:11:54 (UTC)

malicious
Threat Score: 89/100
AV Detection: 87%
Labeled as: Johnnie.Generic

Anti-Virus Results

CrowdStrike Falcon
100%
Static Analysis and ML
Last Update: 03/22/2020 21:20:36 (UTC)
View Details: N/A
Visit Vendor:

MetaDefender
73%
Multi Scan Analysis
Last Update: 03/22/2020 21:20:36 (UTC)
View Details:
Visit Vendor:

CONCLUSION

Hybrid Analysis is a great free platform to submit suspicious attachments to see if they are malicious. While security teams will have their enterprise-grade tools, this is the perfect tool for security researchers and provides detailed analysis and reputation checks.

‹ Previous Topic

Back to Lesson

Next Topic ›