Kasm Workspaces REMnux Streaming App Powers Cloud-Hosted Malware Analysis Lab

REMnux Linux Workspace used for Secure Malware Analysis in Incident Response Investigations.

Kasm Technologies

TechRaj

MCLEAN, VA, USA, February 10, 2023 /EINPresswire.com/ -- Kasm Technologies, today announced that Kasm Workspaces was featured on the Tech Raj YouTube channel as the technology powering Cloud-Hosted Malware Analysis Lab using REMnux: https://youtu.be/_80fpeY-_AI

The lab is also covered in detail in the Tech Raj Blog: https://www.blog.techraj156.com/post/cloud-hosted-malware-analysis-lab-using-remnux

"Let me tell you why a cloud hosted lab for performing malware analysis is better than a lab running on your local machine - It is safer and there is less risk of your personal machine getting infected with all the malware you will be dissecting." said Teja Swaroop, Owner of Tech Raj. "There's no doubt that you are going to execute different kinds of malicious binaries on your lab to analyze them - but what if the malicious binary you are executing has some kind of functionality that enables it to escape your sandbox and do damage outside of it? This is where a Cloud hosted lab has the advantage, since it is running on the cloud it can't affect your personal computer, and your digital footprint is also not compromised."

> Performing malware analysis in a cloud hosted container is safer and there is less risk of your personal machine getting infected with all the malware you will be dissecting."
>
> *Teja Swaroop, Owner of Tech Raj*

In this video Teja provides a comprehensive overview of a cloud-based malware analysis:

- Kasm Workspaces Community Edition deployment to AWS
- Collecting the malware sample using ELF-Malware-Analysis-101 from intezer on GitHub:

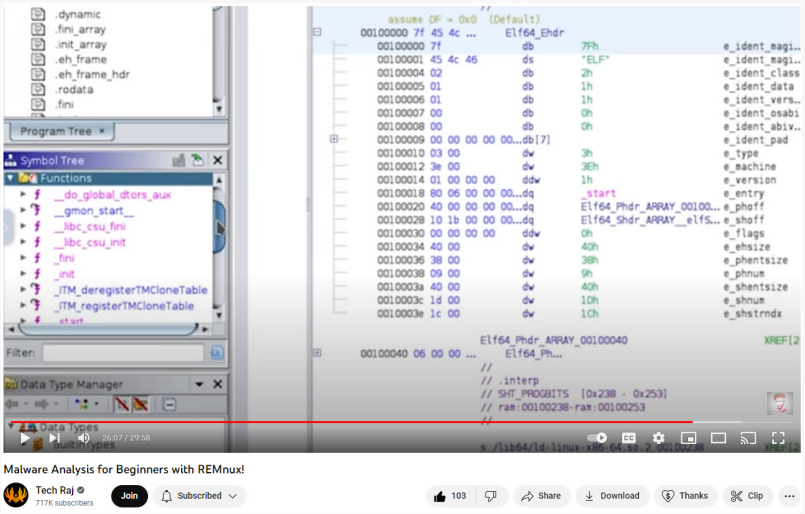
https://github.com/intezer/ELF-Malware-Analysis-101/tree/master/Part-2-Initial-Analysis/Article-samples

- Using Detect It Easy v3.05
- Malware hashing with MD5sum and searching on virus total
- Readelf analysis
- Reading of the program headers and explanation of packers
- Analyzing beaconing via strings command
- Reading ASCI text
- Decoding strings
- Ghidra for decompiling binary files

“Kasm Technology appreciates Tech Raj demonstrating malware analysis on REMnux utilizing a Kasm Workspaces cloud-hosted platform.” Said Kasm Technologies Chief Technology Officer – Matt McClaskey. “This video demonstrates an easily accessible Malware Analysis Lab that is hosted in the cloud.”

For more information on our community edition see: https://www.kasmweb.com/community-edition

REMnux Lab



REMnux Console

ABOUT KASM WORKSPACES

Kasm Workspaces is a container streaming platform for delivering browser, desktop, and application workloads to the web browser. Kasm is changing the way that businesses deliver digital workspaces using our open-source web-native container streaming technology to establish a modern devops delivery of Desktop as a Service (DaaS), application streaming, and browser isolation. Kasm is not just a service, it is a highly configurable platform, with a robust developer API that can be customized for your use-case, at any scale. Workspaces is truly wherever the work is. It can be deployed in the cloud (Public or Private), on-premise (Including Air-Gapped Networks), or in a hybrid configuration.

ABOUT KASM TECHNOLOGIES

Kasm Technologies is a privately held small business led by a team of cybersecurity engineers

experienced in developing web-native remote work platforms for Federal/State Government, Fortune 500 companies, Startups, and Small/Medium sized businesses. Our team's experience in offensive/defensive cyber operations, rapid prototyping, and cutting-edge technology provides us with a unique perspective on how to provide reliable, private, and secure communications.

Matt
McClaskey
+1 571-444-5276
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube
Other
