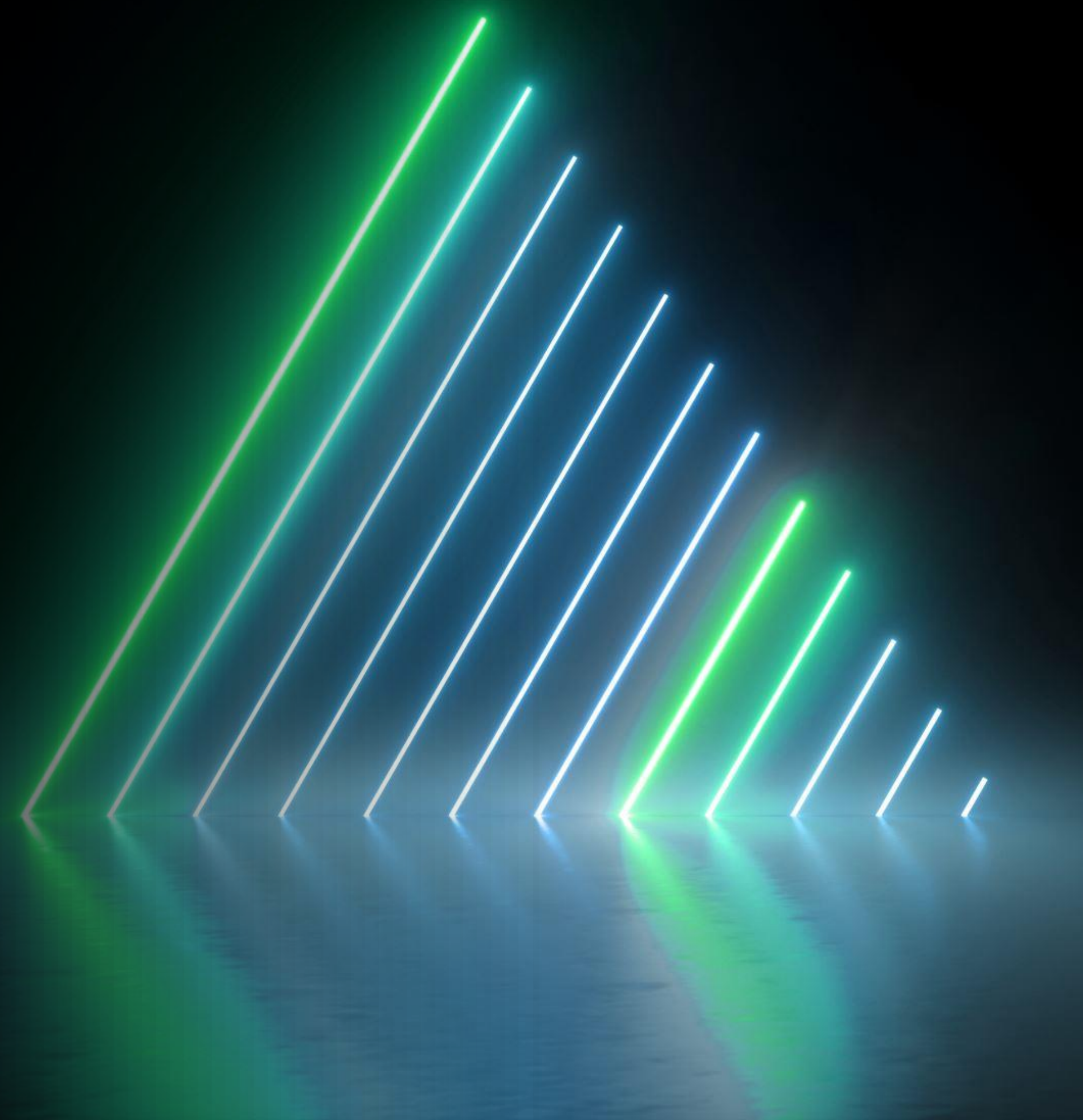
Docker Vulnerabilities

Network and Security Project

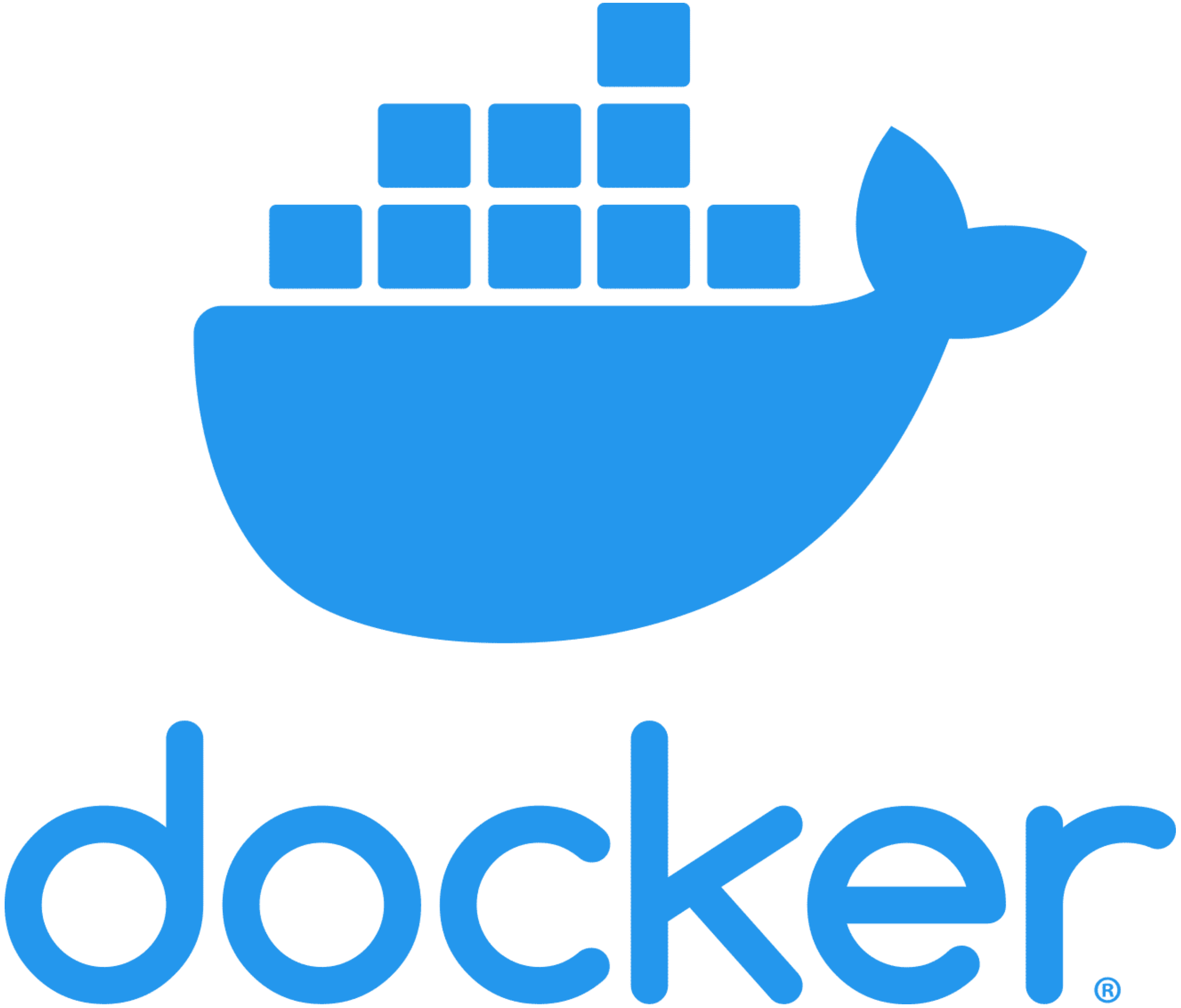
Crudo Giovambattista



What is Docker?

Docker is an open-source platform created to speed up the deployment and the maintenance of software applications.

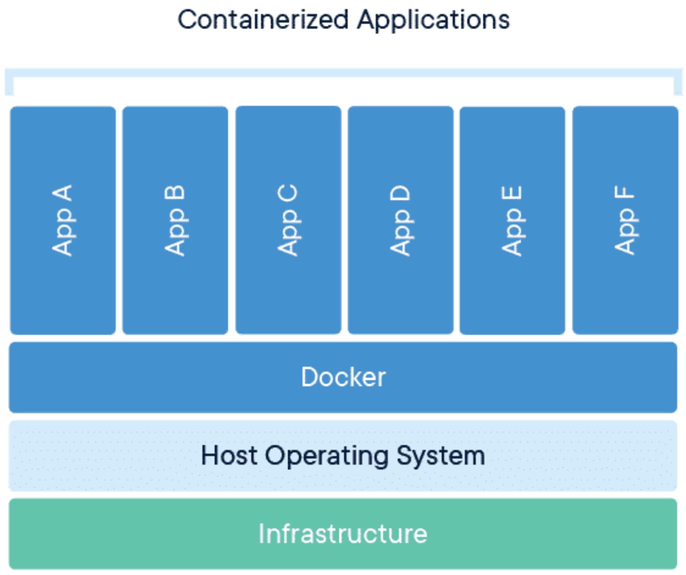
Is based on the concept of “Containers” which are minimal, generic-purpose and isolated environments.

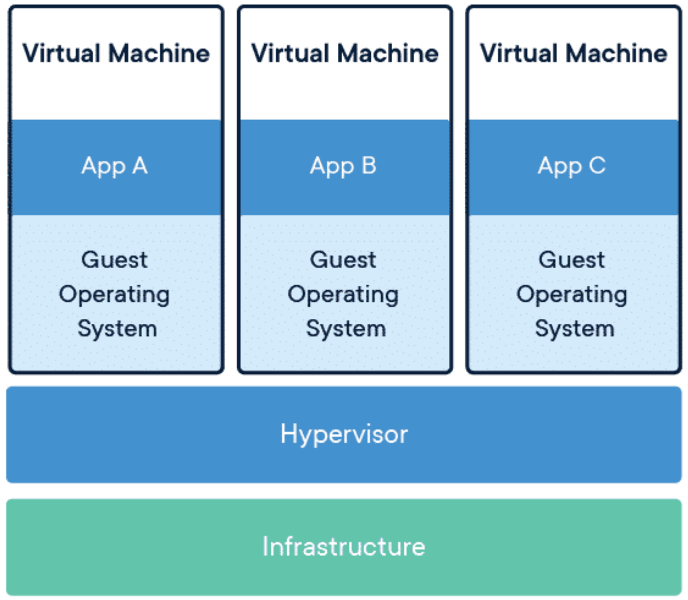


Containers vs Virtual Machines

Containers are isolated units that include code and all the dependencies, so the application runs quickly and reliable from one environment to another.

Differently from Virtual Machines which are packed with a guest operating system, the containers shares the hardware of system that is running them.





Why Docker is vulnerable

The problem lays in the fact that since Docker has a lot of moving parts, it may be difficult to make it secure and because of this an attack can come from everywhere.

In the following slides are explained some of the most high-rated vulnerabilities discovered in the years.

CVE-2018-8115: JACK IN THE BOX

Rated with a Severity Code of 8.6/10, this vulnerability affects Docker for windows.

It allows attackers to insert malicious code into special container images.

This code is executed by Windows Host Computer Service Shim Library(hcsshim) thus allowing hackers to remotely execute code in the host's filesystem.

CVE-2020-13401: IPV6 INPUT VALIDATION

Rated with a Severity Code of 6.0/10, allows attackers to perform a main-in-the-middle attack against another container on the host's network.

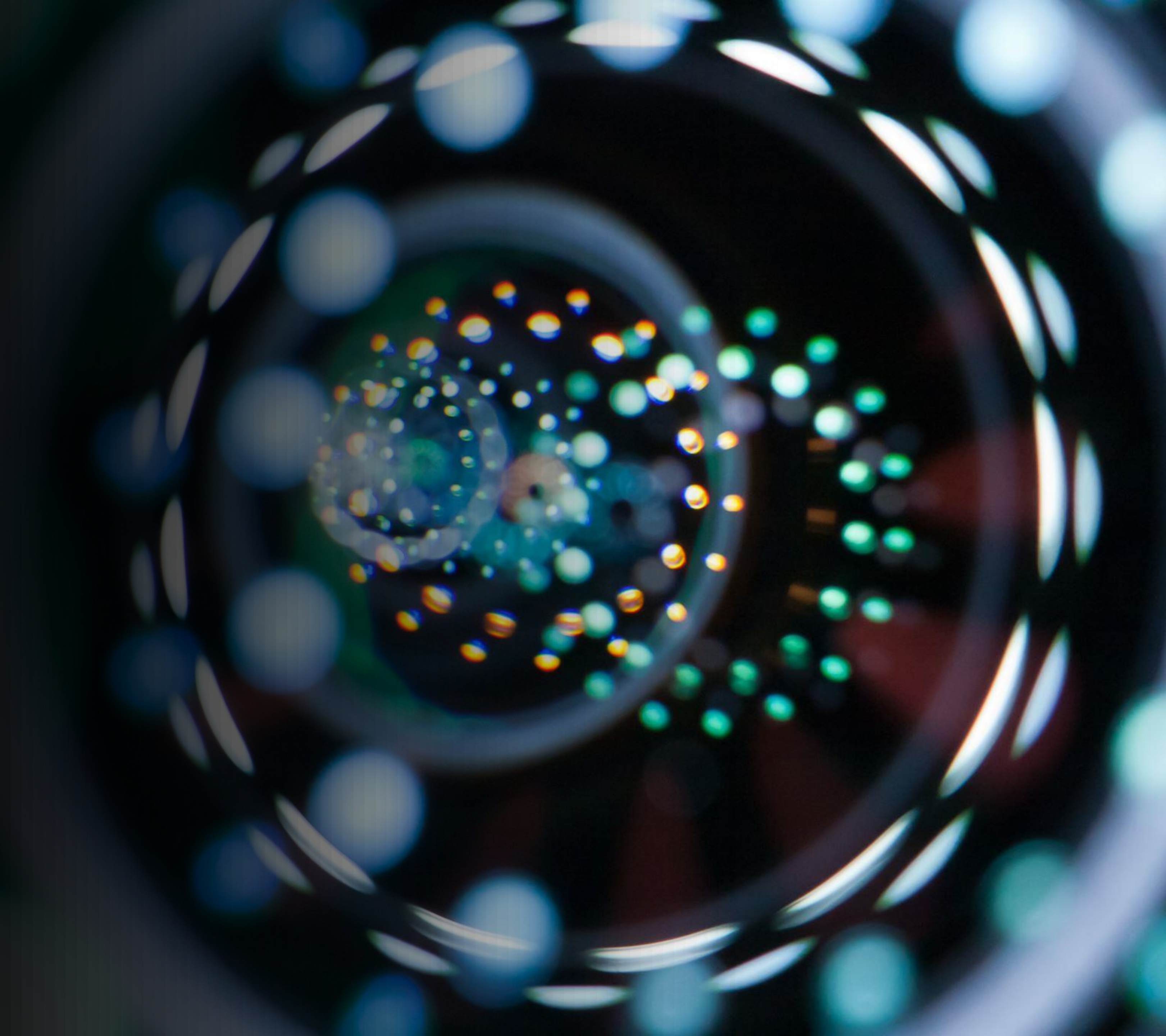
An attacker container with CAP_NET_RAW capability can craft IPv6 router advertisement and spoof external IPv6 hosts, obtain sensitive informations or cause denial of service.

CVE-2019-5736: runC CONTAINER ESCAPE

Rated with a Severity Code of 9.3/10, is a docker vulnerability that enables attackers to gain root-level access to a host system by overwriting their runC library.

If this is successful, the attacker gains control of the host's system.

Focus on CVE-2019-5736



Explanation of the vulnerability

Is called «runC container escape» because it allows an attacker to substitute the original runC binary of the host running the container with a modified one, the CVE description reports also the possibility to deploy a new container in the host's network with a custom image, paving the way to other possible attacks.

Why runC?

RunC is a CLI tool used to spawn and run containers on Linux according to the OCI(Open Container Initiative) specifications.

In order to get the job done **we need the runC to create a new process in the container** and since the runC is tasked with running custom binaries defined by the user, **we can exploit it either when running a new container or passing some arguments to the docker exec command** attaching a shell to a running container.

The attack is done in the way Linux handles the symbolic link in the proc filesystem, which is a virtual filesystem that gives informations about processes. **So substituting the runC binary will trick a container to point to a malicious runC bin.**

Starting point of the attack

To exploit the vulnerability we need:

- Docker 18.9.1 or lower
- runC 1.0rc6
- Some malicious containers

POC:
exec exploitation

The first POC is based on the idea of triggering the payload of the malicious container in the moment that a user wants to attach a shell to the container via the docker exec command.

In this first POC we will see a simple substitution of the runC binary of the host running the container. Remember that if the runC binary is modified it will not be possible to create or run new images or containers, also the docker exec command will not work anymore until the runC is replaced with a working one.

POC:
reverse shell

The second POC is similar to the first one but in this case instead of substituting the runC binary with one that contains a simple string we will trick the container to execute a modified runC that open a reverse shell (in our exaple on port 2345) reachable with the command «nc –nvlp 2345» we can achieve a Remote Code Execution on the host running the compromised container.

Post exploitation possibilities

Once we exploit the vulnerability is possible to extend the attack for instance running custom containers, stealing sensitive informations from the host itself, add the host to a botnet, and many other things.

The following slides will report some example of post-attack possibilities

Docker & Kubernetes Kiss-A-Dog

Crowstrike researchers found a new vulnerability **that allows cryptojacking on Docker and Kubernetes infrastructures**. The campaing was named kiss-a-dog because the detected intrusions found on september 2022 were using a domain called "kiss.a-dog[.]top" that was used to inject payload on compromised containers using a python command coded in base 64. **Discovered after the hack of a honeypot** the hackers were moving in the compromised docker network killing all the cloud monitoring processes executed by Kubernetes.

The goal of the campaing was to have a big number of compromised containers running XMRig software to mine cryptocurrencies.

https://www.redhotcyber.com/post/le-applicazioni-docker-e-kubernetes-possono-finalmente-baciare-il-cane/

Frappo PhaaS (Phishing as a Service)

Frappo is a plug and play phishing software discovered by The Resecurity HUNTER that allows attackers to create fake pages and websites of well-made facture, emulating big banks, e-commerce sites, and many others.

Frappo was intended as anonymous cryptowallet and allows an attacker to work with stolen data in anonymous and encrypted way, also the service keeps track of all the stolen credentials via his dashboard.

The leaked credentials will be displayed in the "Registry" section with other details belonging to the victim like IP address, user agent, username, password , etc..

Frappo can be used to gain possess of an account (Account Takeover Attack ATO), to compromise enterprise emails (Business Email Compromise) and to steal payment informations and identity.

https://www.redhotcyber.com/post/frappo-il-kit-di-phishing-as-a-service-completo-di-sito-fake-per-attacchi-professionali/