Exposed Docker APIs Abused by DDoS, Cryptojacking Botnet Malware

bleepingcomputer.com/news/security/exposed-docker-apis-abused-by-ddos-cryptojacking-botnet-malware/

Sergiu Gatlan

By
Sergiu Gatlan

- June 14, 2019
- 11:48 AM
- 0

Attackers are actively scanning for exposed Docker APIs on port 2375 and use them to deploy a malicious payload which drops a Dofloo Trojan variant, a malware known as a popular tool for building large scale botnets.

The Dofloo (aka AESDDoS) malware was first detected in 2014 [1, 2, 3, 4] and it is known for allowing hackers to quickly assemble vast numbers of compromised machines used to create botnets that can launch DDoS attacks and — in the case of some variants — to load cryptocurrency miners to the infected machines.

Misconfigured Docker services being abused is a known trend given that they have been under constant attack since early-2018 after coinminer campaigns started spreading to the cloud following the drop in activity seen by ransomware operations after the end of 2017.

Attacks, infection, and abuse

In the campaign observed by Trend Micro, misconfigured APIs of the Docker Engine-Community DevOps utility that allow external access to the communication ports are abused by attackers making it possible to infiltrate misconfigured servers.

"Allowing external access — whether intentionally or by misconfiguration — to API ports allows attackers to gain ownership of the host, giving them the ability to poison instances running within it with malware and to gain remote access to users' servers and hardware resources," says Trend Micro.

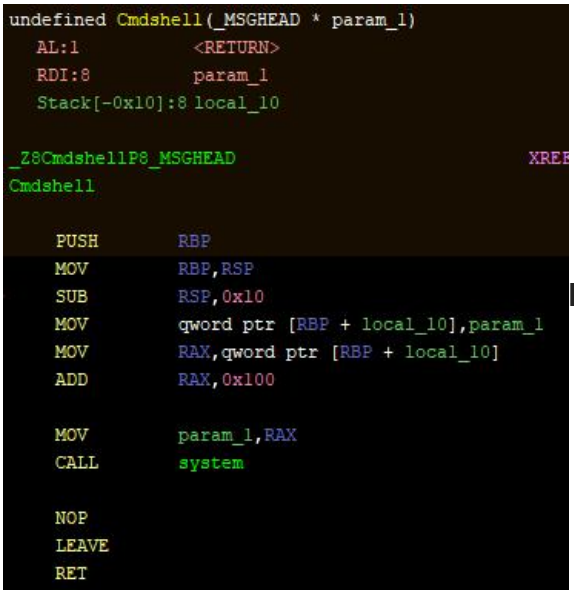
```
GET /containers/json HTTP/1.1
Accept: */*
Referer: http://192.168.0.10:2375/containers/json
Accept-Language: zh-cn
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)
Host: 192.168.0.10:2375
Cache-Control: no-cache
```

Query to list all available containers

The attacks begin with an Internet scan for vulnerable Docker hosts by sending TCP SYN packets to port 2375 — the Docker daemon communication port which allows for unencrypted and unauthenticated communication— using an open source SYN/TCP port scanner, with the bad actors connecting to all live host they found and asking for running containers.

The Dofloo botnet malware is subsequently "deployed using the docker exec command" to all discovered containers says Trend Micro's research, executing the malware that will enable the "attackers to launch several types of DDoS attacks, such as SYN, LSYN, UDP, UDPS, and TCP flood."

System information is also collected by the Trojan after execution, with the data being packed and sent to its command-and-control (C&C) server allowing its masters to decide what the next course of action will be depending on the hardware configuration of the compromised machine.



Dofloo (AESDDoS) malware executing remote shell commands

Trend Micro's research team provides a list of Indicators of Compromise (IOCs) containing hashes of malware samples used during these attacks at the end of the report.

Previous Dofloo and Docker attacks

Dofloo was previously detected while being dropped by a malicious campaign that exploited a critical server-side template injection Atlassian Confluence Server and Data Center vulnerability to compromise Linux and Windows servers in late April.

Exposed Docker APIs were abused by other malicious campaigns, with one being detected in March by Imperva while exploiting the CVE-2019-5736 runc vulnerability disclosed one month earlier allowing attackers to overwrite the host runc binary and gain root-level code execution privileges.

Cryptojacking operations have also actively targeted misconfigured Docker services in November 2018 as unearthed by Juniper Networks researchers, with cybercriminals adding their own containers which executed Monero mining scripts.

Further back, in October 2018 and March 2018, other campaigns have also been observed while scanning the Internet for easy to infiltrate Docker hosts and deploy containers that would download and execute coin miners.

Securing Docker servers

While Docker Engine API abuse is not something new, it keeps being an issue because administrators do not know how to properly secure their systems.

To make sure that their Docker hosts are secured against this types of attacks, admins should be using adequate security controls that allow only trusted sources to access the Docker API as explained in the Securing Docker remote daemon chapter available on the Docker documentation website.

Related Articles:

Docker servers hacked in ongoing cryptomining malware campaign

Microsoft detects massive surge in Linux XorDDoS malware activity

New cryptomining malware builds an army of Windows, Linux bots

Pro-Ukraine hackers use Docker images to DDoS Russian sites

Emotet botnet switches to 64-bit modules, increases activity