

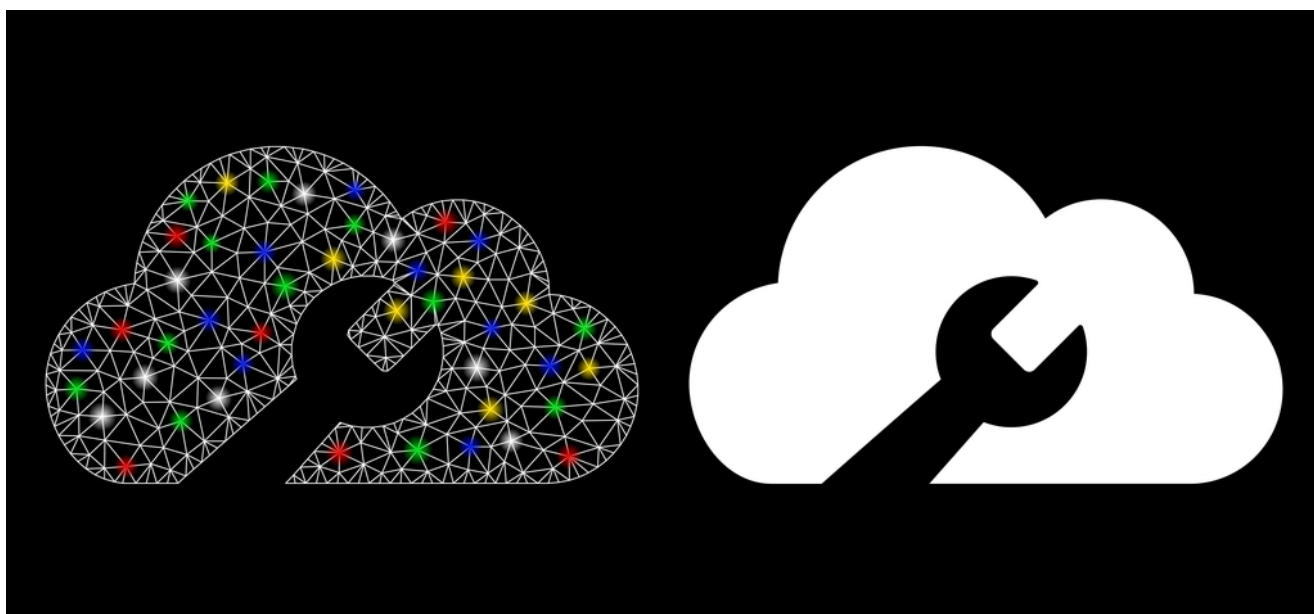
Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks

[intezer.com/blog/cloud-workload-protection/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/](https://www.intezer.com/blog/cloud-workload-protection/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/)

September 8, 2020



Written by Nicole Fishbein - 8 September 2020



[Get Free Account](#)

[Join Now](#)

Introduction

TeamTNT is a cybercrime group that targets cloud environments including Docker and Kubernetes instances. The group has been [previously documented](#) using several tools including crypto-miners and Amazon Web Services (AWS) credential stealing worms.

TeamTNT has also been spotted using a malicious Docker image which can be found on Docker Hub to infect its victims' servers. Now the group is evolving. In a recent attack observed by Intezer, TeamTNT uses a new technique by abusing [Weave Scope](#), a trusted tool which gives the user full access to their cloud environment and is integrated with Docker, Kubernetes, the Distributed Cloud Operating System (DC/OS), and AWS Elastic Compute Cloud (ECS). The attackers install this tool in order to map the cloud environment of their victim and execute system commands without deploying malicious code on the server.

To our knowledge, this is the first time attackers have been caught using legitimate third party software to target cloud infrastructure. When abused, Weave Scope gives the attacker full visibility and control over all assets in the victim's cloud environment, essentially functioning as a backdoor.

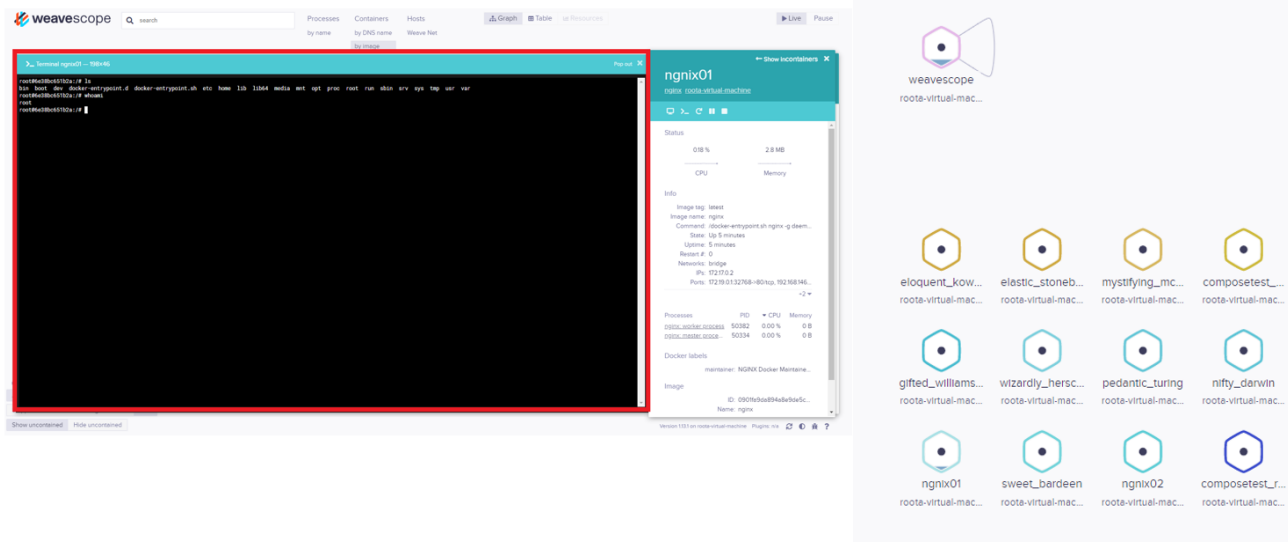
Below we will describe the attack flow and the use of Weave Scope by the attacker.

Attack Flow

TeamTNT's attacks typically involve the use of malicious Docker images from the Docker Hub in addition to crypto-miners and malicious scripts. The uniqueness of the recent attack observed by Intezer is the group abuses a legitimate open source tool called Weave Scope to gain full control over the victim's cloud infrastructure.

Weave Scope is an open source tool from [Weave Works](#), a company that offers automation tools for working with containerized applications. It provides monitoring, visualization, and control over Docker and Kubernetes. Using a dashboard accessible from the browser the user gains full control over the infrastructure including all information and metadata about containers, processes, and hosts.

Weave Scope is a powerful utility, giving the attackers access to all information about the victim's server environment with the ability to control them including: installed applications, connection between the cloud workloads, use of the memory and CPU, and a list of existing containers with the ability to start, stop, and open interactive shells in any of these containers. By installing a legitimate tool such as Weave Scope the attackers reap all the benefits as if they had installed a backdoor on the server, with significantly less effort and without needing to use malware.



The image above is a Weave Scope visualization of a Linux server. On the left is the open terminal of a Nginx-based container. On the right is a view of all the containers on the server.

To install Weave Scope on the server the attackers use an exposed Docker API port and create a new privileged container with a clean Ubuntu image. The container is configured to mount the file system of the container to the filesystem of the victim server, thus gaining the attackers access to all files on the server. The initial command given to the container is to download and execute several cryptominers.

The attackers then attempt to gain root access to the server by setting up a local privileged user named 'hilde' on the host server and use it in order to connect back via SSH.

Next the attackers download and install Weave Scope. As described in the installation guide in [Weave Scope's git](#), it takes only a few commands to complete installation of the tool.

```
sudo curl -L git.io/scope -o /usr/local/bin/scope
sudo chmod a+x /usr/local/bin/scope
scope launch
```

Once installed, the attackers can connect to the Weave Scope dashboard via HTTP on port 4040 and gain full visibility and control over the victim's infrastructure.

From the dashboard the attackers can see a visual map of the Docker runtime cloud environment and give shell commands without needing to deploy any malicious backdoor component. Not only is this scenario incredibly rare, to our knowledge this is the first time an attacker has downloaded legitimate software to use as an admin tool on the Linux operating system.

Mitigation Recommendations

Precise and correct configuration of cloud workloads and services can prevent many attacks which is why it's important to take the time and effort to check them. To protect yourself from this attack we recommend to:

- **Close exposed Docker API ports:** This attack takes advantage of a common misconfiguration of the Docker API which gives the attacker full control over the Docker service. Therefore, Docker API ports should be closed or contain restricted access policies in the firewall.
- **Block incoming connections to port 4040:** Weave Scope uses default port 4040 to make the dashboard accessible and anyone with access to the network can view the dashboard. Similar to the Docker API port, this port should be closed or restricted by the firewall.
- Block the IOCs provided below.
- Check out our article [Best Practice for Securing a Docker Runtime environment](#).
- Take advantage of the free Intezer Protect [community edition](#) to protect your Linux cloud servers and containers in runtime against unauthorized code.

Apply Zero Trust Execution to Your Workloads

Zero Trust Execution is viewed by market research firms as the best practice for securing cloud workloads for reasons like the nature of this TeamTNT attack. ZTE creates a trusted baseline of your workloads and monitors for any new process or injected code. Any unauthorized code or applications that drift from the pre-approved baseline are blocked from running in your cloud environment, allowing you to retain a trusted state.

In this scenario, although Weave Scope is a legitimate administration tool (it's not malware and therefore doesn't contain malicious code), the application was still flagged by ZTE because it's unauthorized code that deviates from the trusted baseline.

[This article](#) explains how you can adopt a genetic-based ZTE approach to alleviate some of the high overhead caused by traditional implementations.

Learn more about Intezer's support for [runtime Cloud Workload Protection](#).

Update from Weave Works

Weave Works has since provided this [in-depth article](#) on how to prevent malicious attacks using Weave Scope. The article covers both how Scope is used and how you can prevent it being misused by securing it in any Kubernetes installation.

A special thank you to Idan Katz for his contribution to this research.

IOCs

85[.]214.149.236

[https://iplogger\[.\]org/2Xvkv5](https://iplogger[.]org/2Xvkv5)

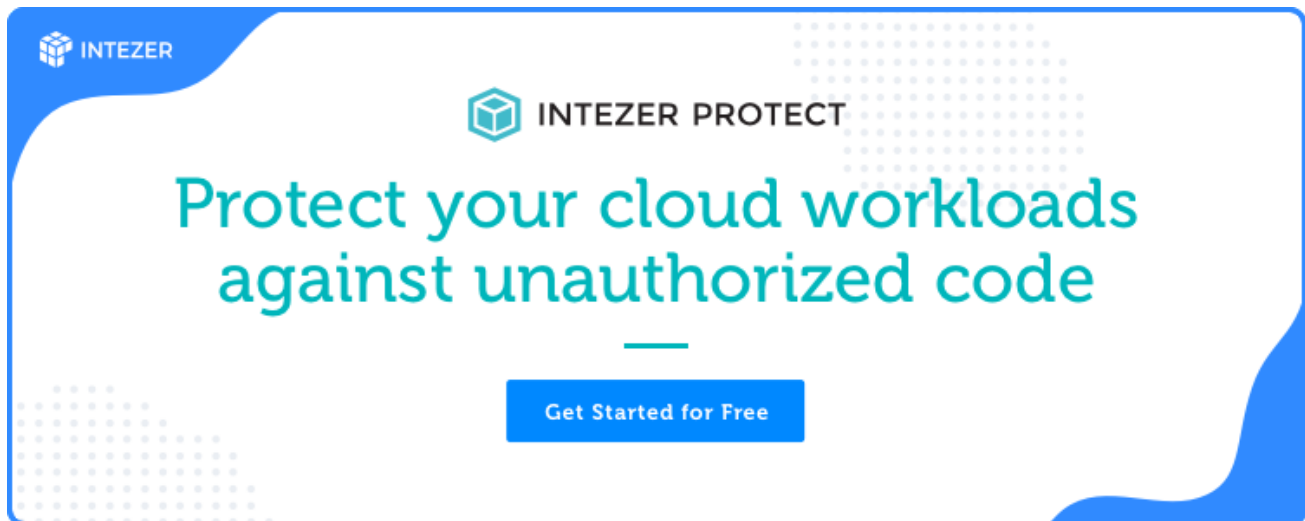
24d7d21c3675d66826da0372369ec3e8

8c6681daba966addd295ad89bf5146af

656eca480e2161e8645f9b29af7e4762

8ffdba0c9708f153237aabb7d386d083

45385f7519c11a58840931ee38fa3c7b

A promotional banner for Intezer Protect. The banner has a blue border and a white background with blue accents. In the top left corner, there is the Intezer logo (a cube icon) and the word "INTEZER". In the center, there is the Intezer Protect logo (a cube icon) and the text "INTEZER PROTECT". Below this, the main headline reads "Protect your cloud workloads against unauthorized code" in a large, teal font. At the bottom center, there is a blue button with the text "Get Started for Free".

Nicole Fishbein

Nicole is a malware analyst and reverse engineer. Prior to Intezer she was an embedded researcher in the Israel Defense Forces (IDF) Intelligence Corps.