UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00035

TEAMTNT TAKEOVER CLOUD INSTANCES

DATE ISSUED: 14th September 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	LOW	[✓ MEDIUM]	HIGH

OVERVIEW

Legitimate open source cloud-monitoring tool Weave Scope has been utilised by the known group TeamTNT to establish backdoors with no file pointers onto targeted Kubernetes and Docker clusters.

BREAKDOWN

Normally used to provide a top-down view of the user’s application and infrastructure allowing diagnosis of issues within the containerized apps in real time. It is a tool that is trusted and used across many cloud platforms and in this instance is used to give the attacker full visibility and map the victims cloud environment, execute commands, malicious code and functions as a backdoor, leaving no files to trace. The abuser then has full access to make any changes to the environment they wish. TeamTNT specialises in attacking cloud environments and has been mentioned in our previous Cyber Guidance Issue 23 for their activity with Crypto jacking worms.

REMEDIATION STEPS

- Check security configurations in your cloud environment – particularly API, and remote access ports
- Check for superfluous credentials and remove access to those that are not necessary.
- Check passwords are not stored in plaintext on the file system.
- Check access controls for those who require access to the cloud environment and adjust accordingly.

REFERENCES & RESOURCES

Bleeping Computer:	https://www.bleepingcomputer.com/news/security/hackers-use-legit-tool-to-take-over-docker-kubernetes-platforms/
Threatpost:	https://threatpost.com/teamtnt-remote-takeover-cloud-instances/159075/