Sep 21 2023

NETMANAGEIT

Intelligence Report

npm packages caught exfiltrating Kubernetes config, SSH keys

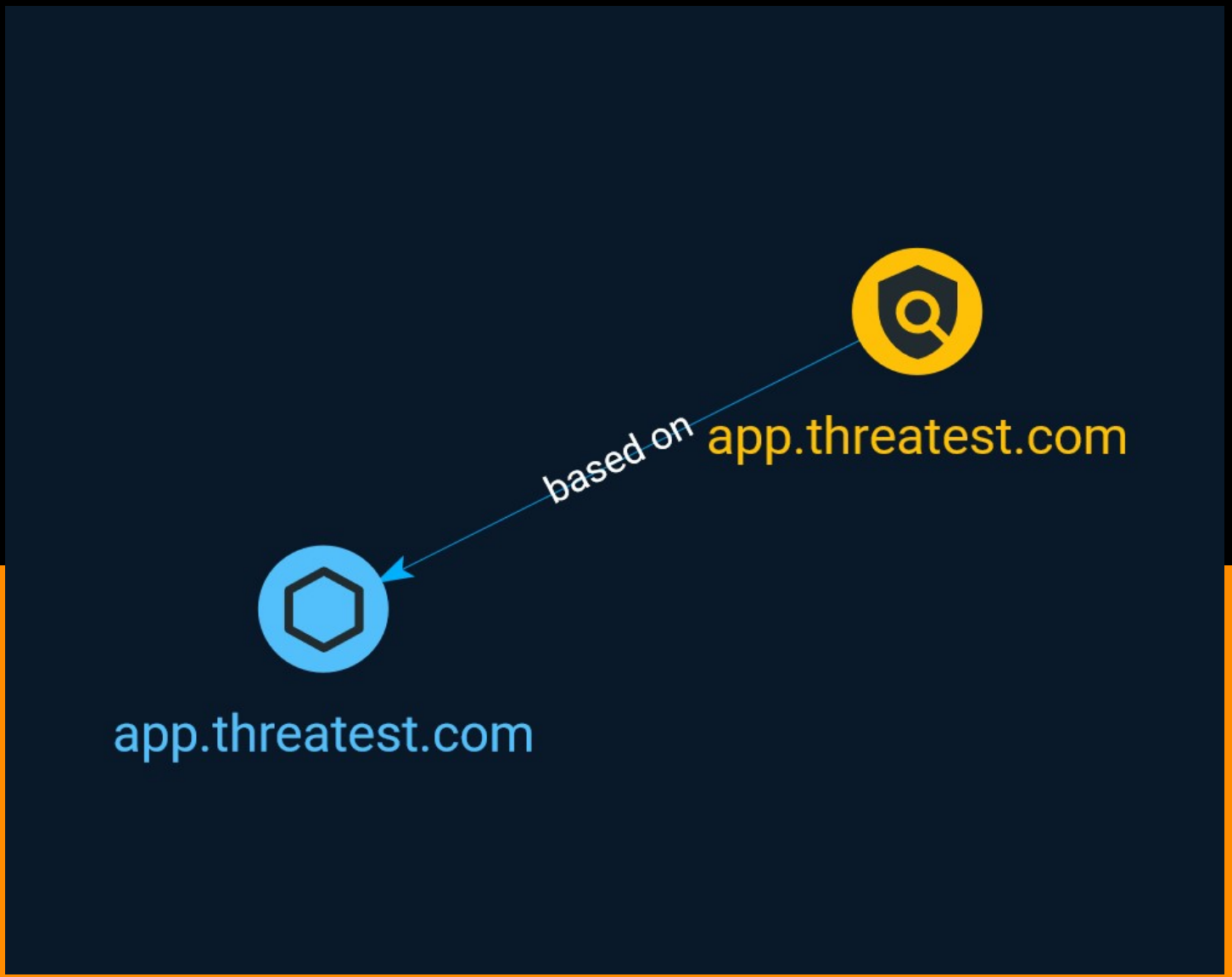

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Sonatype tracks an ongoing campaign that uses npm packages to retrieve and exfiltrate Kubernetes configuration and SSH keys to an external server

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name
app.threatest.com
Pattern Type
stix
Pattern
[hostname:value = 'app.threatest.com']

Hostname

Value
app.threatest.com

External References

- https://otx.alienvault.com/pulse/650b0077aac192d5839053ee
- https://blog.sonatype.com/npm-packages-caught-exfiltrating-kubernetes-config-ssh-keys