controlplane

I'LL LET MYSELF IN

IAIN SMART & ANDREW MARTIN, CONTROLPLANE

INTRODUCTIONS

Iain Smart

@Smarticu5

Andy Martin

@Sublimino

controlplane

AGENDA

Define Offsec

Talk about common findings

Demos

Post-compromise activities

More Demos

THE PROBLEM

Kubernetes is Complicated

NO, BUT REALLY

Moving parts

Rapid changes

Differing operational requirements

Security

controlplane

OFFENSIVE SECURITY

PENETRATION TESTING

You think you're secure. Let's validate that assumption.

THEN WHAT?

controlplane

PURPLE TEAMING

Collaborative engagement

Evaluate monitoring team's responses

Test detection coverage

controlplane

ASSUMED BREACH

Users have been compromised. What can you do?

controlplane

COMMON FINDINGS

Things we see regularly, that you should check for

controlplane

🦶 🔫

footgun (noun): Any feature whose addition to a product results in the user shooting themselves in the foot.

KUBERNETES RBAC

People still make mistakes assigning roles

Administrators make assumptions; leads to escalations

COMMON RBAC ISSUES

Secrets `get` & `list`

Pod Creation

Pipeline Service Account

Permissions

RBAC `Escalate` or `*`

https://kubernetes.io/docs/concepts/security/rbac-good-practices/

controlplane

DEMO - CI/CD BREAKOUT

controlplane

POST-COMPROMISE ACTIVITIES

controlplane

HIDING YOUR TRACKS

Are you auditing everything you need to?

ATTACKER EVICTION

Can you really get rid of an attacker once they're in?

KUBERNETES

Minted user certs
Direct etcd Access
Craft SAT
Create custom RBAC

Create workload
Static node manifests
Malicious admission
controller/operator

LINUX

Cronjobs on nodes

SSH Keys on nodes

Modify container runtime

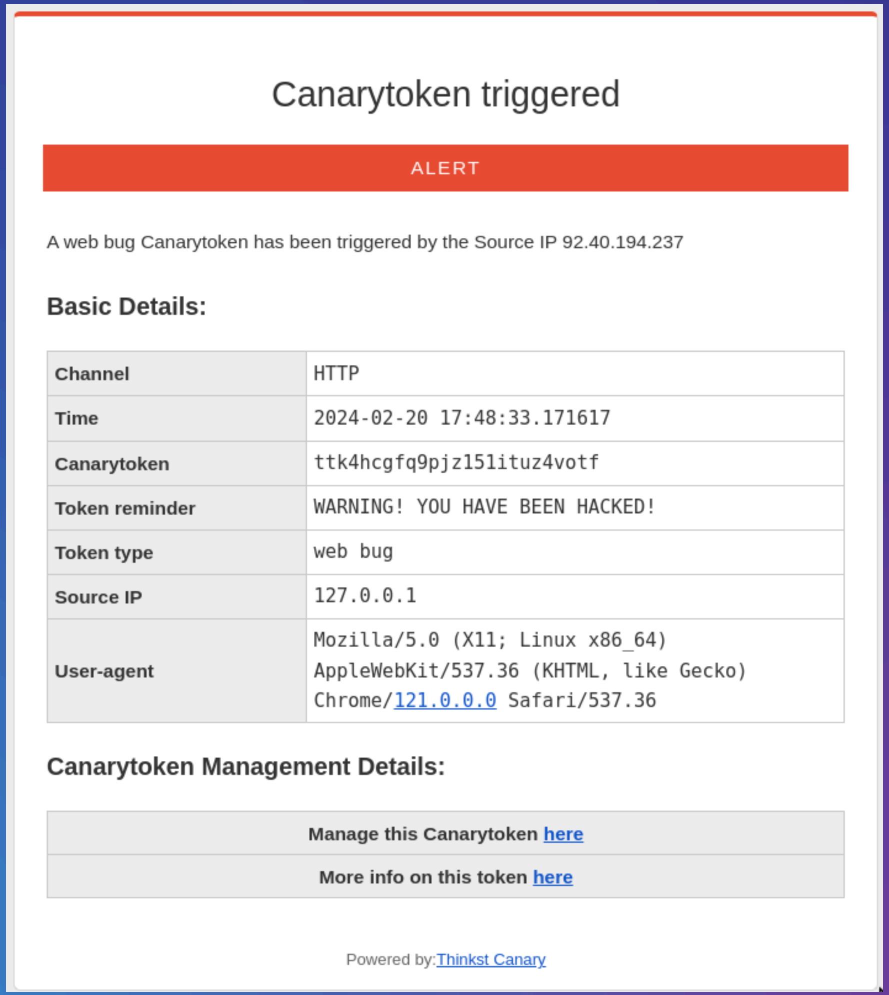
Implant on attached cloud storage

https://attack.mitre.org/tactics/TA0003/

DEMO - PERSISTENCE

controlplane

WHAT WOULD YOU DO?



Canarytoken triggered

ALERT

A web bug Canarytoken has been triggered by the Source IP 92.40.194.237

Basic Details:

Channel	HTTP
Time	2024-02-20 17:48:33.171617
Canarytoken	ttk4hcgfq9pjz15lituz4votf
Token reminder	WARNING! YOU HAVE BEEN HACKED!
Token type	web bug
Source IP	127.0.0.1
User-agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

Powered by:Thinkst Canary

controlplane

CAPTURE THE FLAG

If you've enjoyed this talk, come and practice some of what you've learned.

Pavilion 7 | Level 7.3 | W08

Or find us at Booth G31