CWL
CyberWarFare Labs

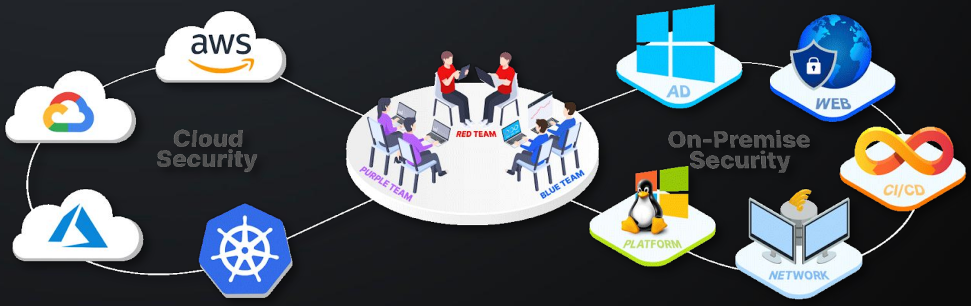
Unmasking The Trap
A Study of Canary Tokens

CWL
CyberWarFare Labs

About CyberWarFare Labs

CW Labs is a renowned Infosec company specializing in cybersecurity practical learning. They provide on-demand educational services. The company has 3 primary divisions :

1. Learning Management System (LMS) Platform
2. CWL CyberSecurity Playground (CCSP) Platform
3. Infinity Learning Platform



INFINITE LEARNING EXPERIENCE

About Speaker

Abhijeet Kumar (Security Researcher)

His research areas include Red Team Operations, Network Security, Cloud Infrastructure, and Linux Systems. Apart from this, he enjoys researching Adversarial TTPs and experimenting in his homelab.

"All warfare is based on deception. There is no place where espionage is not used. Offer the enemy bait to lure them."

- Sun Tzu

The garlic in your soup waiting for you to confuse it for a piece of potato

DECEPTION ENGINEERING

★ The process of identifying adversary activities by implementing deceptive measures

DECEPTION ENGINEERING

- ★ The process of identifying adversary activities by implementing deceptive measures
- ★ Defenders gets alerts whenever a trap is triggered, helping them track the adversary behaviour.

DECEPTION ENGINEERING

- ★ The process of identifying adversary activities by implementing deceptive measures
- ★ Defenders gets alerts whenever a trap is triggered, helping them track the adversary behaviour
- ★ Some products include:-
  - ○ Zscaler Deception
  - ○ Thinkst Canaries

CANARY TOKENS

- ★ Also known as Honey Tokens

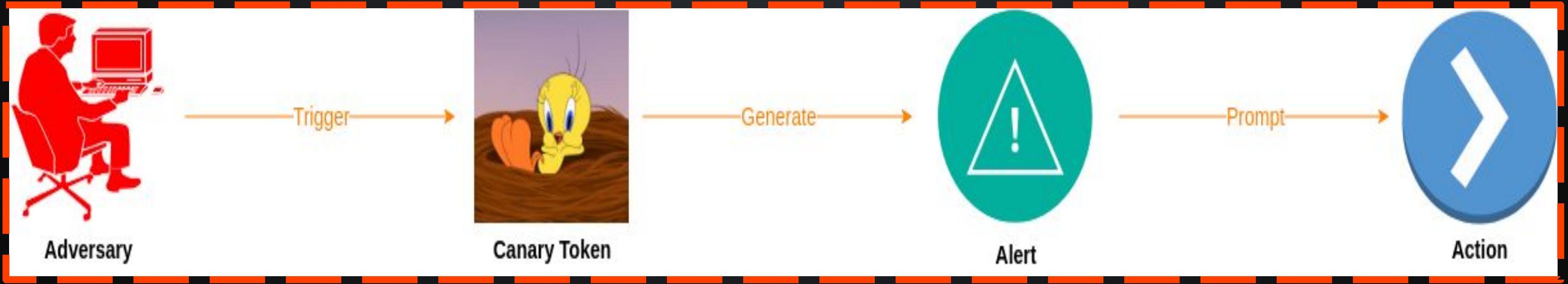
CANARY TOKENS

- ★ Also known as Honey Tokens
- ★ Serves as a *tripwire* mechanism

CANARY TOKENS

- Also known as Honey Tokens
- Serves as a *tripwire* mechanism
- Some common locations include:-
    - Applications
    - Credentials
    - Files
    - URLs

CANARY TOKEN FLOW



CREDENTIAL-BASED CANARY TOKENS

★ Consists of Keys, Credential pairs, or Certificates

CREDENTIAL-BASED CANARY TOKENS

- ★ Consists of Keys, Credential pairs, or Certificates
- ★ Triggers an alert via the configured detection mechanism

CREDENTIAL-BASED CANARY TOKENS

- ★ Consists of Keys, Credential pairs, or Certificates
- ★ Triggers an alert via the configured detection mechanism
- ★ Usually implements cloud-native services for detection

CANARY TOKEN DETECTION

- Use local decoding
  - For e.g: Decode AWS Account ID from Access_Key

CANARY TOKEN DETECTION

- ★ Use local decoding
  - ○ For e.g: Decode AWS Account ID from Access_Key
- ★ Use Provider/3rd Party APIs
  - ○ For e.g: Microsoft Graph APIs
  - ○ For e.g: AADInternals Azure Function for Tenant Info

CANARY TOKEN DETECTION

- Use local decoding
  - For e.g: Decode AWS Account ID from Access_Key
- Use Provider/3rd Party APIs
  - For e.g: Microsoft Graph APIs
  - For e.g: AADInternals Azure Function for Tenant Info
- Gather data from Public IOCs/Community/Vendor itself

ARTIFACT-BASED CANARY TOKENS

- ★ Consists of Documents, Executables, or Configuration files

ARTIFACT-BASED CANARY TOKENS

- ★ Consists of Documents, Executables, or Configuration files
- ★ Embeds the callback URL in the artifact itself

ARTIFACT-BASED CANARY TOKENS

- ★ Consists of Documents, Executables, or Configuration files
- ★ Embeds the callback URL in the artifact itself
- ★ Usually implements cloud-native services along with for detection

CANARY TOKEN DETECTION

- ★ Analyse the metadata
  - ○ Look for suspicious fields
  - ○ Check signatures

CANARY TOKEN DETECTION

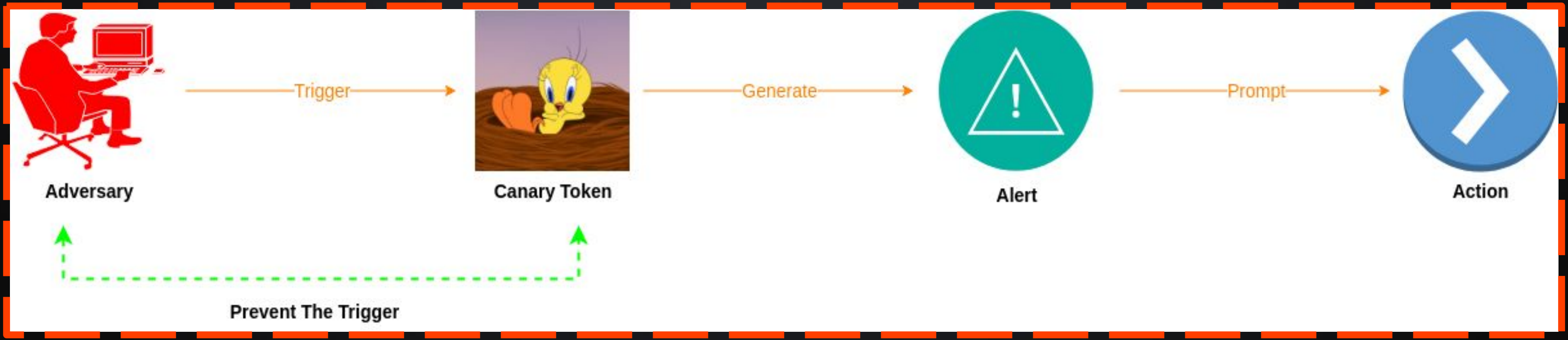
- Analyse the metadata
  - Look for suspicious fields
  - Check signatures
- Dissect the artifact locally without opening
  - Extract URLs from document

CWL
CyberWarFare Labs

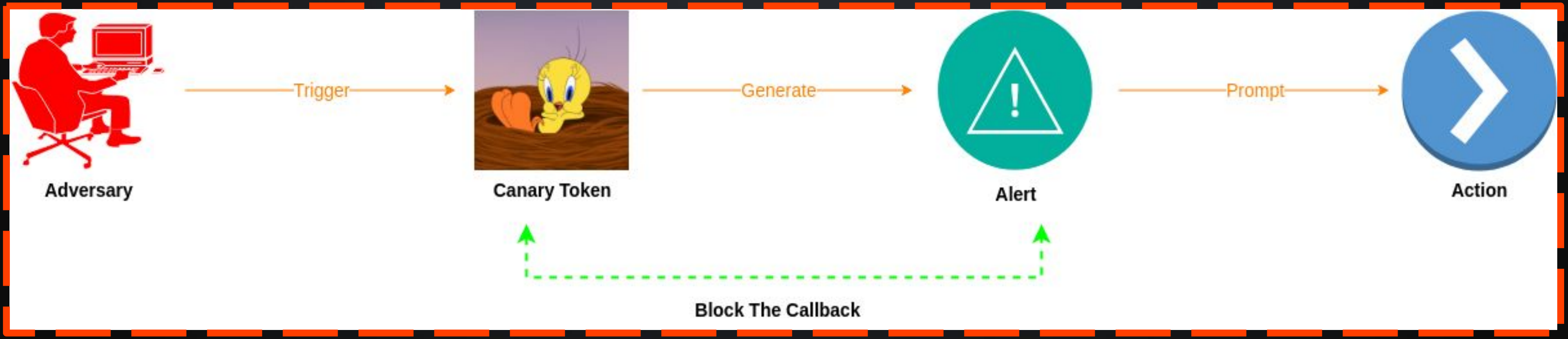
CANARY TOKEN DETECTION

- Analyse the metadata
  - Look for suspicious fields
  - Check signatures
- Dissect the artifact locally without opening
  - Extract URLs from document
- Open in sandbox (*without internet access*) and analyse network traffic

DEFEATING CANARYTOKENS 01



DEFEATING CANARYTOKENS 02



WAIT A MINUTE
ARE YOU TELLING ME THAT IT ACTUALLY WORKS?
quickmeme.com

SHUT UP AND
SHOW ME A DEMO
memegenerator.es

OPSEC CONSIDERATIONS

- ★ Use own infrastructure for configuring Canary Tokens whenever possible
  - ○ Don’t reuse the infrastructure

OPSEC CONSIDERATIONS

- ★ Use own infrastructure for configuring Canary Tokens whenever possible
  - ○ Don’t reuse the infrastructure
- ★ Hide endpoint URLs behind CDNs/proxy
  - ○ For e.g: CloudFront, Azure CDN

CWL
CyberWarFare Labs

OPSEC CONSIDERATIONS

- Use own infrastructure for configuring Canary Tokens whenever possible
  - Don’t reuse the infrastructure
- Hide endpoint URLs behind CDNs/proxy
  - For e.g: CloudFront, Azure CDN
- Rotate Canary Tokens once triggered

RESOURCES

- ★ Zachary's Talk: https://youtu.be/1WLxvq_130U
- ★ Original Repo: https://github.com/CatchingCanaries/CanaryEnumeration
- ★ My Fork: https://github.com/wand3rlust/CanaryEnumeration

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team, Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live