Who Goes There? Actively Detecting Intruders With Cyber Deception Tools

RVASEC
RICHMOND.VA

The Omni Richmond: June 13-14, 2023

@mcdwayne

Hi, I’m Dwayne

Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of The Security Repo Podcast
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

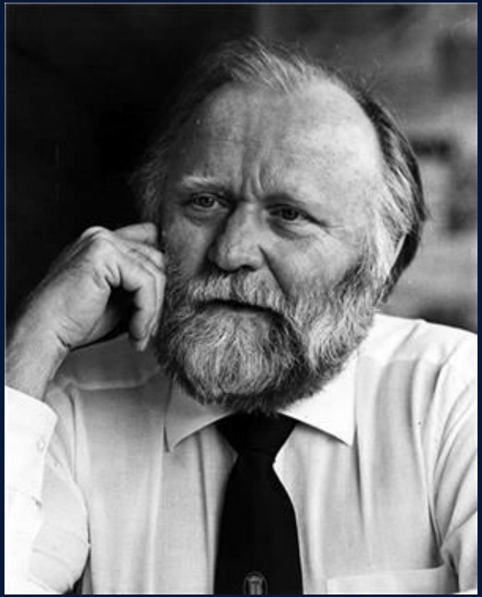
About GitGuardian

GitGuardian is the code security platform for the DevOps generation.

We help enterprises answer the issue of "Where are my hardcoded secrets and have they been leaked?"

Code Leaks Are A Problem

“I must not fear. Fear is the mind-killer. Fear is the little-death that brings total obliteration. I will face my fear. I will permit it to pass over me and through me. And when it has gone past I will turn the inner eye to see its path. Where the fear has gone there will be nothing. Only I will remain.”

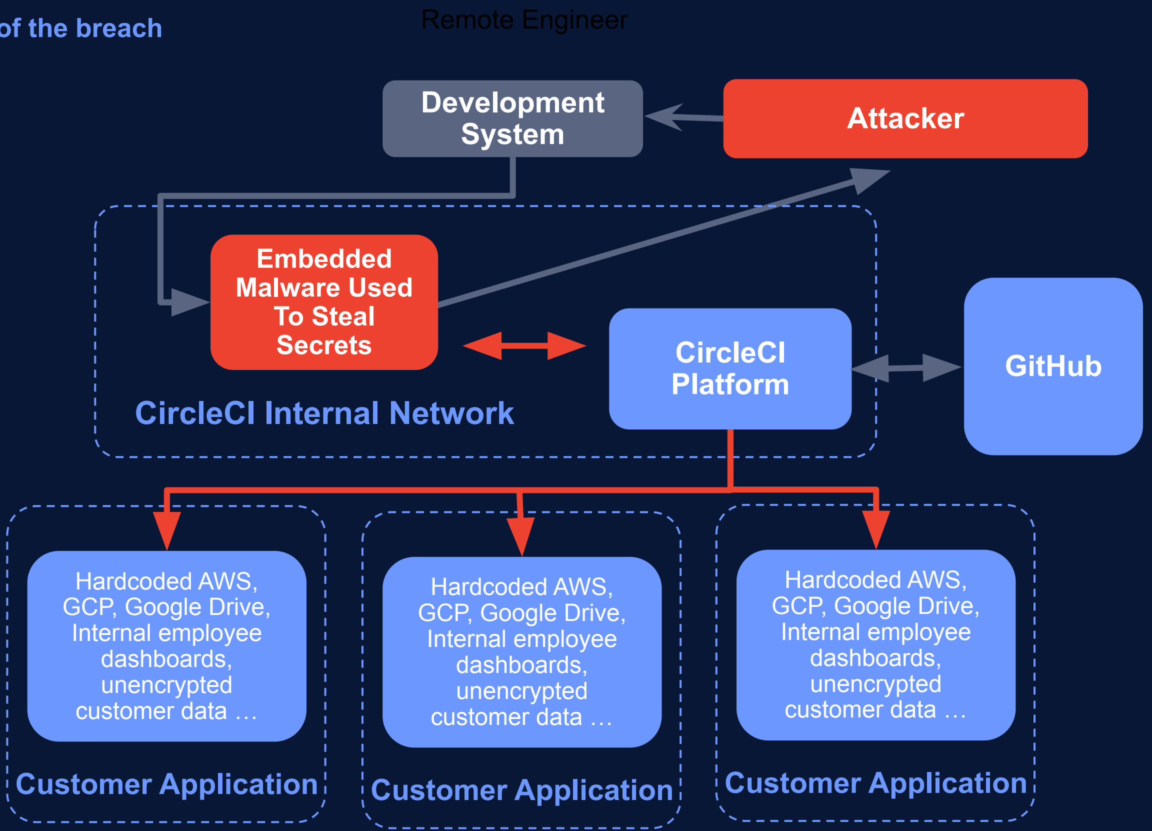


— Frank Herbert, Dune
Bene Gesserit Litany Against Fear

CircleCI – January 2023

Use of a honeytoken alerted the security team of the breach

Customer secrets stolen, unauthorised access to GitHub repos and third-party systems


Remote Engineer
Development System
Attacker
Embedded Malware Used To Steal Secrets
CircleCI Platform
GitHub
CircleCI Internal Network
Hardcoded AWS, GCP, Google Drive, Internal employee dashboards, unencrypted customer data …
Customer Application
Hardcoded AWS, GCP, Google Drive, Internal employee dashboards, unencrypted customer data …
Customer Application
Hardcoded AWS, GCP, Google Drive, Internal employee dashboards, unencrypted customer data …
Customer Application

@mcdwayne

@mcdwayne

A Few Incidents

Uber

- Reported: 15 Sept, 2022
- Teenager from the Lapsus$ hacking group phished login info from a super admin
- Immediately discovered access credentials hardcoded in PowerShell scripts
- The attacker used those credentials to gain access to every other system

@mcdwayne

A Few Incidents

Toyota

- Reported: 7 October, 2022
- A subcontractor hired to work on the Toyota T-Connect source code pushed a private codebase into a public GitHub repo.
- The repo contained access credentials for a data server, which exposed the emails of 296,019 customers
- The repo was public from December 2017 to September 2022 - **5 years!**

A Few Incidents

AstraZeneca

- Reported: 3 November 2022
- Developer hardcoded credentials and pushed to GitHub in 2021, giving access to test environments
- "User error" caused an undisclosed amount of patient data to be available in a test environment
- Credentials were exposed for over a year

@mcdwayne

What Attackers Want

1. Access To Data
2. Machine Resources
3. Anything That Leads To 1 or 2

In the 2023 edition of The State of Secrets Sprawl

10M secrets found exposed
in 2022 in public GitHub repositories

—

More than 67% increase compared to 6 Million in 2021

—

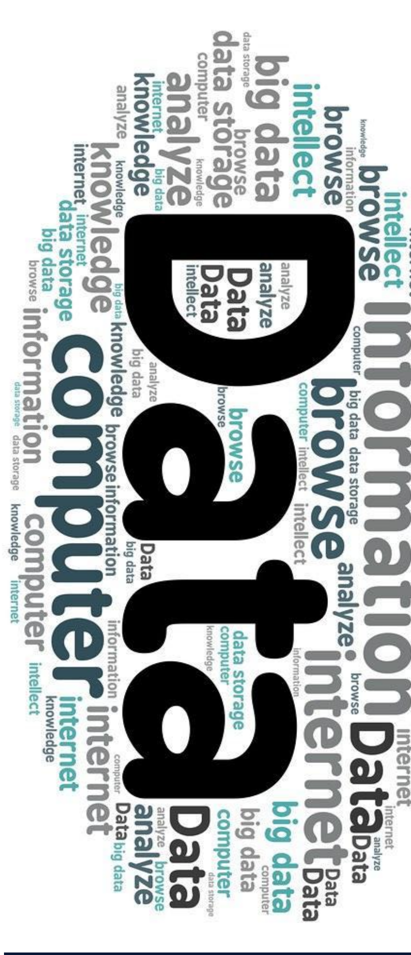
On average, 5.5 commits out of 1,000 exposed at least one secret **+50% compared to 2021**

—

https://www.gitguardian.com/state-of-secrets-sprawl-report-2023

@mcdwayne

HACK


Data
information
computer
internet
browse
big data
analyze
knowledge
intellect
data storage

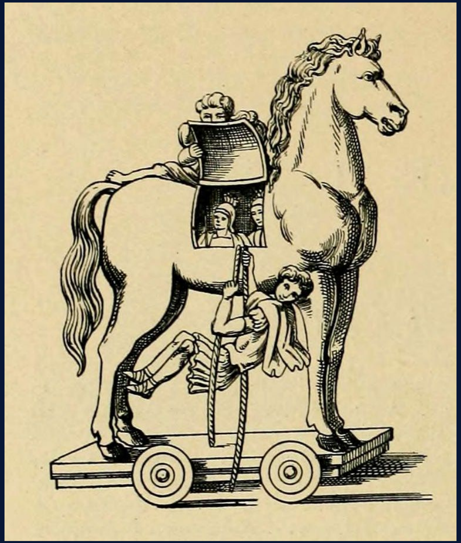
A Brief History Of Cyber Deception

Brief History of Deception

Trojan Horse
~ 1200 BCE

"*I thought I was getting a gift horse from the Achaeans , what I got was defeat*"

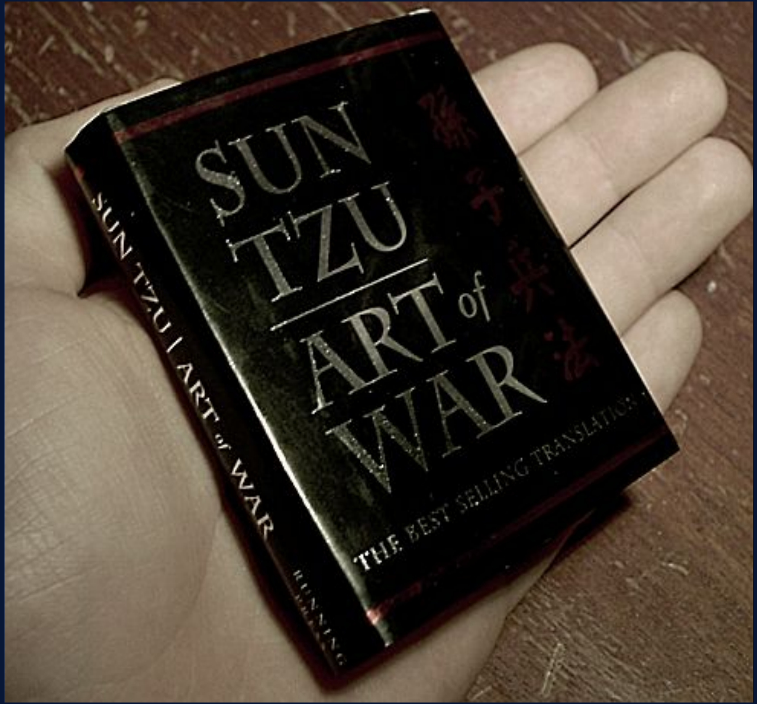
- Trojan security officer



Brief History of Deception

Art of War
~ 400 BCE

"*Appear weak when you are strong, and strong when you are weak*"
- Sun Tzu



Brief History of Deception

Ghost Army
1942

"The first mobile, multimedia, tactical deception unit in U.S. Army history"

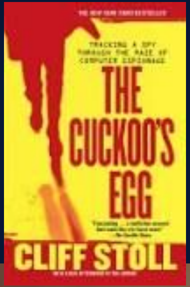
- James Linn - Curator National WWII Museum

Brief History of Deception

The First Honeypot
1985

"Hi, is this the FBI? At my girlfriend's suggestion, I used fake documents to trick someone working with the KGB into keeping their connection to a Lawrence Berkeley National Laboratory computer open long enough to trace their exact location."

- Cliff Stoll

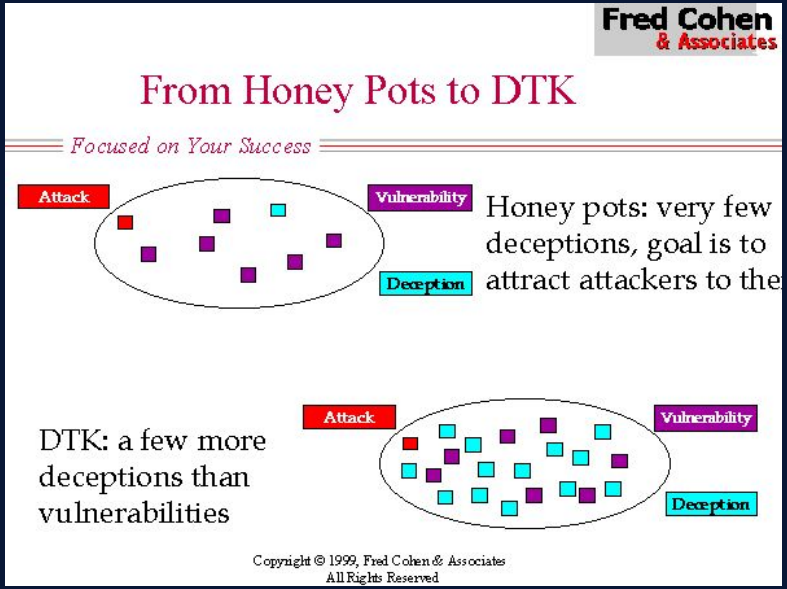


Brief History of Deception

Fred Cohen's Deception Toolkit 1991

"*Under DTK, deceptions are spread among the normal systems in a network in such a way that unused services on those systems are consumed with deceptions. This increases the likelihood of an intelligence probe encountering a deception rather than a vulnerability*"

- Fred Cohen



Fred Cohen & Associates

From Honey Pots to DTK

Focused on Your Success

Honey pots: very few deceptions, goal is to attract attackers to the

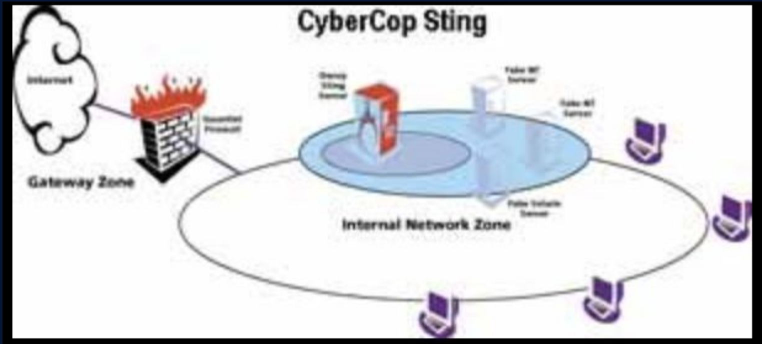
DTK: a few more deceptions than vulnerabilities

Brief History of Deception

First Commercial Honeypots 1998

"These hackers aren't kids on a digital joyride, ... It's clear their motive is financial gain."

- Alfred Huger, Creator of CyberCop Sting

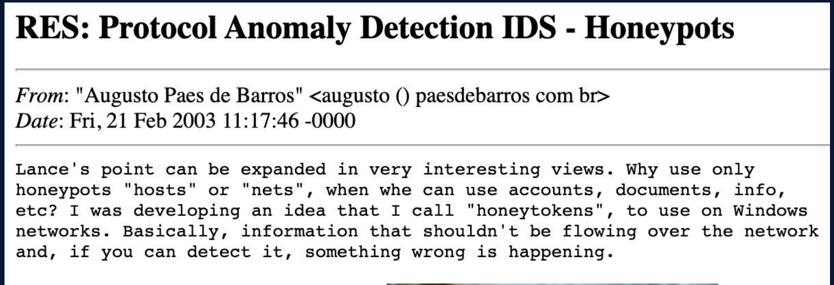


Brief History of Deception

"Honeytokens" is coined 2003

"I was developing an idea that I call 'honeytokens'... *Basically, information that shouldn't be flowing over the network and, if you can detect it, something wrong is happening.*"

- Augusto Paes de Barros



RES: Protocol Anomaly Detection IDS - Honeypots

From: "Augusto Paes de Barros" <augusto () paesdebarros com br>
Date: Fri, 21 Feb 2003 11:17:46 -0000

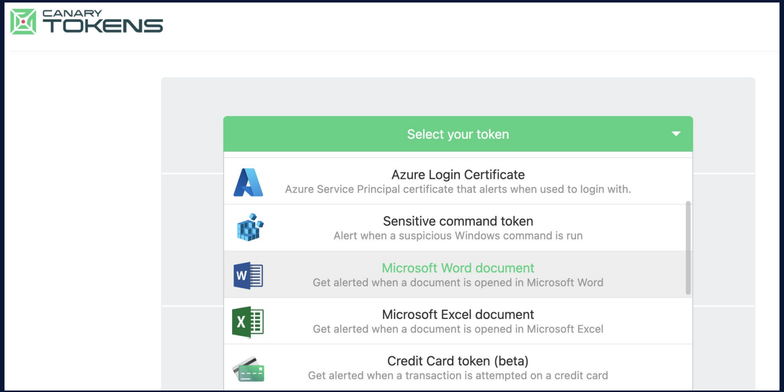
```
Lance's point can be expanded in very interesting views. Why use only
honeypots "hosts" or "nets", when whe can use accounts, documents, info,
etc? I was developing an idea that I call "honeytokens", to use on Windows
networks. Basically, information that shouldn't be flowing over the network
and, if you can detect it, something wrong is happening.

--
Augusto Paes de Barros, CISSP
http://www.paesdebarros.com.br
augusto () paesdebarros com br
```

Brief History of Deception

Canarytokens
2015

"*Added aws token*
Added svn + smtp tokens to generate"

- nickrohrbs, Thinkst developer in a git commit message upon adding aws tokens to the code in 2016.



Select your token

Azure Login Certificate
Azure Service Principal certificate that alerts when used to login with.

Sensitive command token
Alert when a suspicious Windows command is run

Microsoft Word document
Get alerted when a document is opened in Microsoft Word

Microsoft Excel document
Get alerted when a document is opened in Microsoft Excel

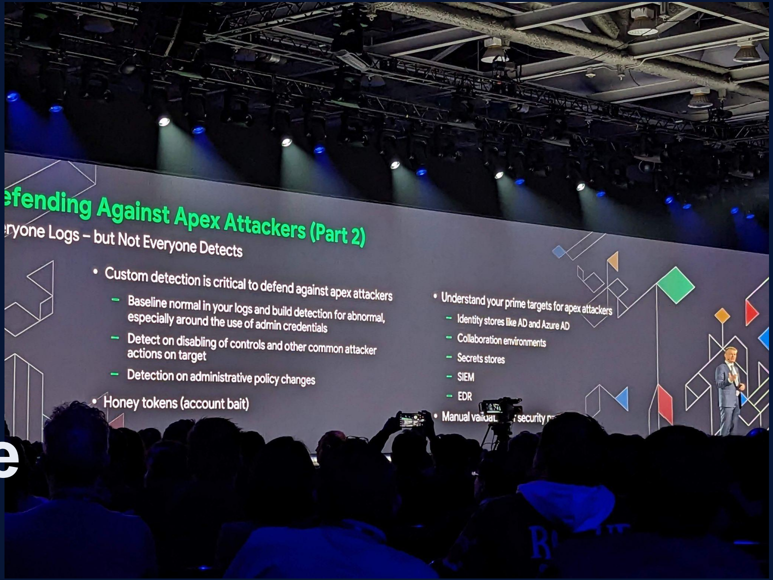
Credit Card token (beta)
Get alerted when a transaction is attempted on a credit card

Brief History of Deception

Honeytokens Becomes Default 2nd Line Defence at Google 2023

"*Honeytokens are your early warning signs*"

- Kevin Mandia from Mandiant /Google Cloud - The state of Cybersecurity - Year in Review talk at RSA 2023



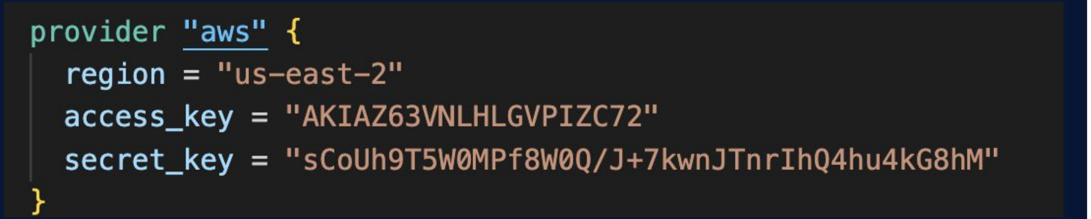
efending Against Apex Attackers (Part 2)

ryone Logs – but Not Everyone Detects

- Custom detection is critical to defend against apex attackers
  - Baseline normal in your logs and build detection for abnormal, especially around the use of admin credentials
  - Detect on disabling of controls and other common attacker actions on target
  - Detection on administrative policy changes
- Honey tokens (account bait)

- Understand your prime targets for apex attackers
  - Identity stores like AD and Azure AD
  - Collaboration environments
  - Secrets stores
  - SIEM
  - EDR
- Manual valida security n

What Is A Honeytoken?

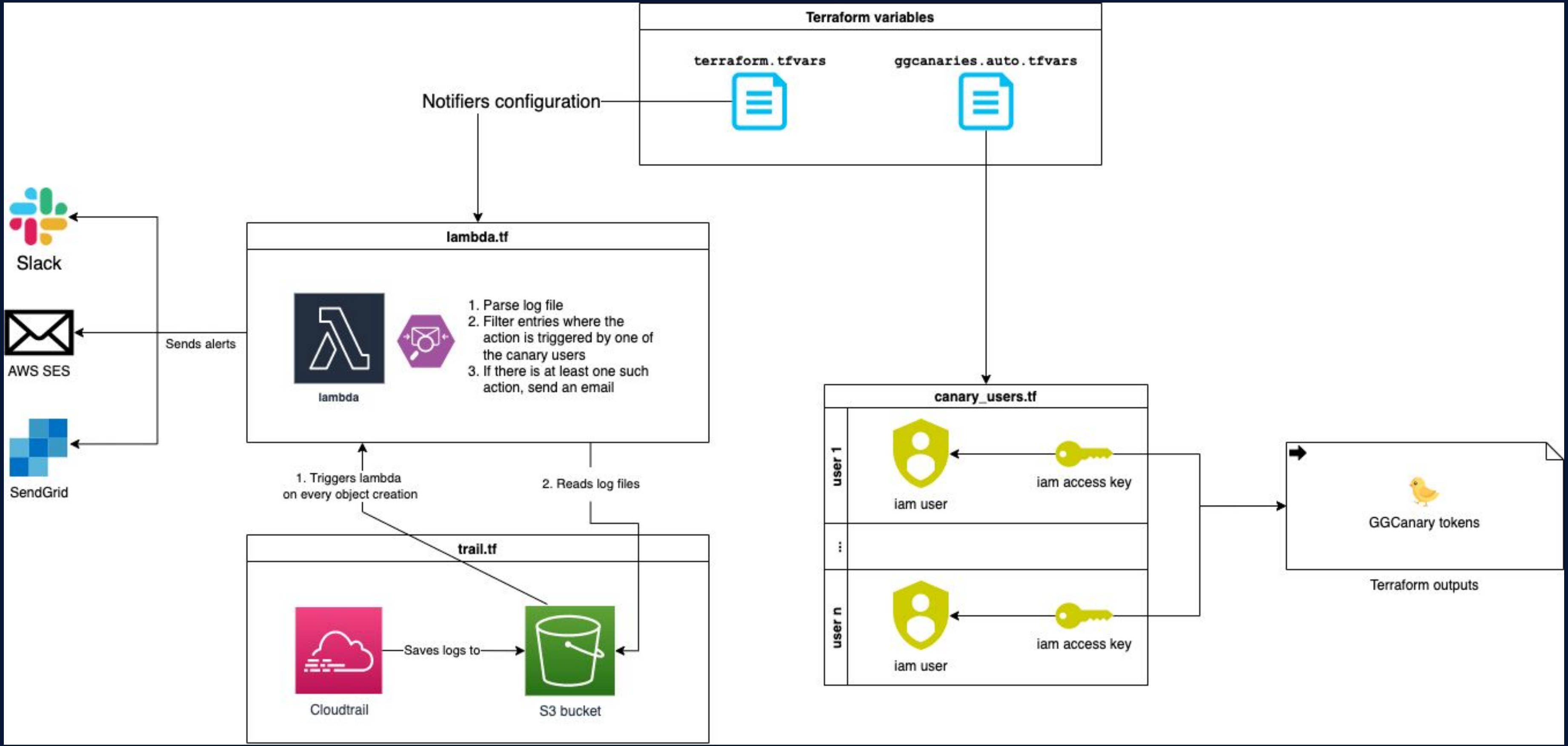


```
provider "aws" {
  region = "us-east-2"
  access_key = "AKIAZ63VNLHLGVPIZC72"
  secret_key = "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"
}
```

Definition

Honeytokens are decoy credentials that do not allow any access to any resources or data. Instead they trigger alerts that reveal the IP address of the user who attempted to use the honeytoken.

Honeytokens look identical to real credentials to an attacker.



https://github.com/GitGuardian/ggcanary

@mcdwayne

Honeytoken Options

vs

@mcdwayne

Open Source - The DIY Route

- Complete DIY - see previous diagram - requires Lambda knowledge and time to tinker with it
- GitGuardian/ggcanary - Requires Terraform and AWS
- spacesiren/spacesiren - Requires AWS how
- thinkst/canarytokens - Requires Docker experience

Commercial Options - Off The Shelf

- Canarytoken.org - free, one off honeytokens
- Thinkst - Canary.tools - The paid version of Canarytoken.org
- GitGuardian Honeytoken Module - Requires GitGuardian account - in Beta
- Microsoft Sentinel - Azure specific
- CrowdStrike - Requires CrowdStrike

Honeytoken Best Practices

Honeytoken Best Practices

Do:

Put honeytokens in your private environments

- Since they don't go to anything, there is no legit reason someone would attempt to use one
  - Code, CI environments, Jira, Slack, Vault

@mcdwayne

Honeytoken Best Practices

Do:

Use a 1:1 ratio of honeytokens to repo/environment

- Keep it simple. When an alarm goes off, make it easy to tell exactly where, and only where, that honeytoken was embedded.

Honeytoken Best Practices

Do:

Use automation to scale deployment

- One off honeytokens have value, but blue teams should be worried about defense at scale
    - Bash or Python scripting should be all you need
    - An example

      https://github.com/mcdwayne/honeytoken-putter

Honeytoken Best Practices

Do:

Think in terms of 'Blue Team'

- Use the IP, UserAgent, and other data points to block access

- The goal is not to track down the individual attacker, it is to guard your stuff

- If you think other credentials are at risk, time to rotate them

Honeytoken Best Practices

Do:

Remember this is a journey, not a one off exercise

- Start with one repo. Worry about scale and automation once you understand and are comfortable with this, or any tech.

Honeytoken Best Practices

DO NOT:

List honeytokens in public

- AWS, GitHub, GitLab, GitGuardian and many other public scanners are always on the lookout for public keys and will trigger them by scanning them

Honeytoken Best Practices

DO NOT:

Go hunting the attacker…unless you are LEA

- Attacking an attacker feels good but it falls into illegal activity rather quickly as you start monitoring the IP and digging in.

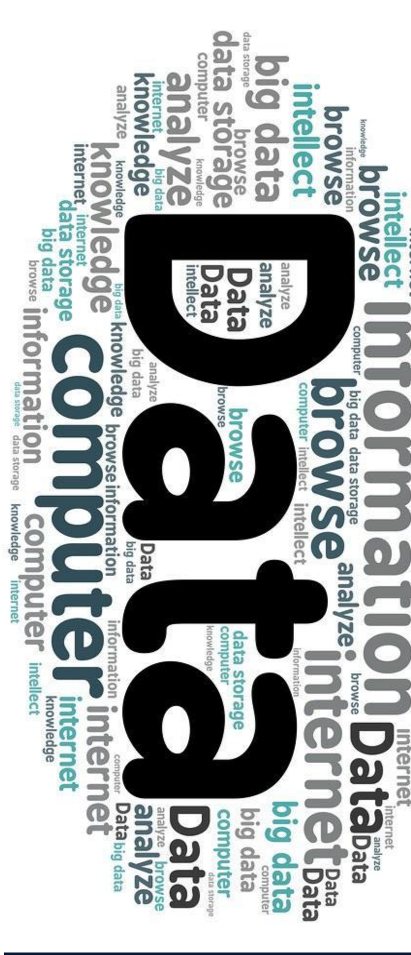
- See earlier slide about Blue Team usage

@mcdwayne

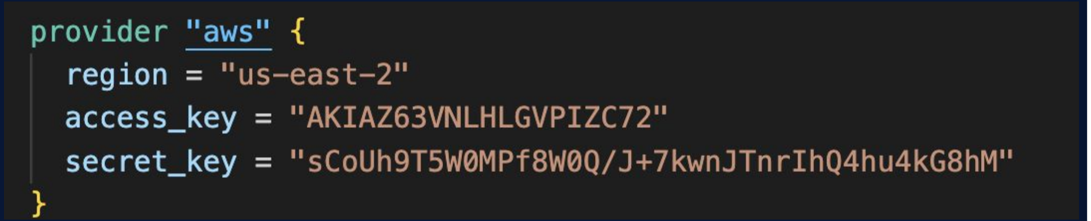
In Conclusion

@mcdwayne

HACK


Data
information
computer
browse
internet
analyze
knowledge
big data
data storage
intellect

@mcdwayne



```
provider "aws" {
  region = "us-east-2"
  access_key = "AKIAZ63VNLHLGVPIZC72"
  secret_key = "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"
}
```

Definition

Honeytokens are decoy credentials that do not allow any access to any resources or data. Instead they trigger alerts that reveal the IP address of the user who attempted to use the honeytoken.

Honeytokens look identical to real credentials to an attacker.

Honeytoken Options

vs

Honeytoken Best Practices

Do:

Think in terms of 'Blue Team'

- Use the IP, UserAgent and other data points to block access
- The goal is not to track down the individual attacker, it is to guard your stuff
- If you think other credentials are at risk, time to rotate them

Hi, I’m Dwayne

Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

Who Goes There? Actively Detecting Intruders With Cyber Deception Tools

RVASEC
RICHMOND.VA

The Omni Richmond: June 13-14, 2023

@mcdwayne