Honeypot Boo Boo

Better Breach Detection With Deception Inception

Justin Varner
Security Philosopher
justin@radzen.io
@JustinTVarner

BSides Munich
October 15, 2023

BSIDES MUNICH

THINKST CANARY
AUTHORISED PARTNER

My Honeytrap Brings All The Bums To The Jar

A **honeytrap** (honeypot or honeytoken) is a security mechanism designed to entice adversaries to make mistakes and announce their presence.

It is a component of a larger discipline known as **deception technology** where trickery is the name of the game.

Honeytraps are designed to provide a **low volume of high fidelity alerts** that only fire when something bad is happening.

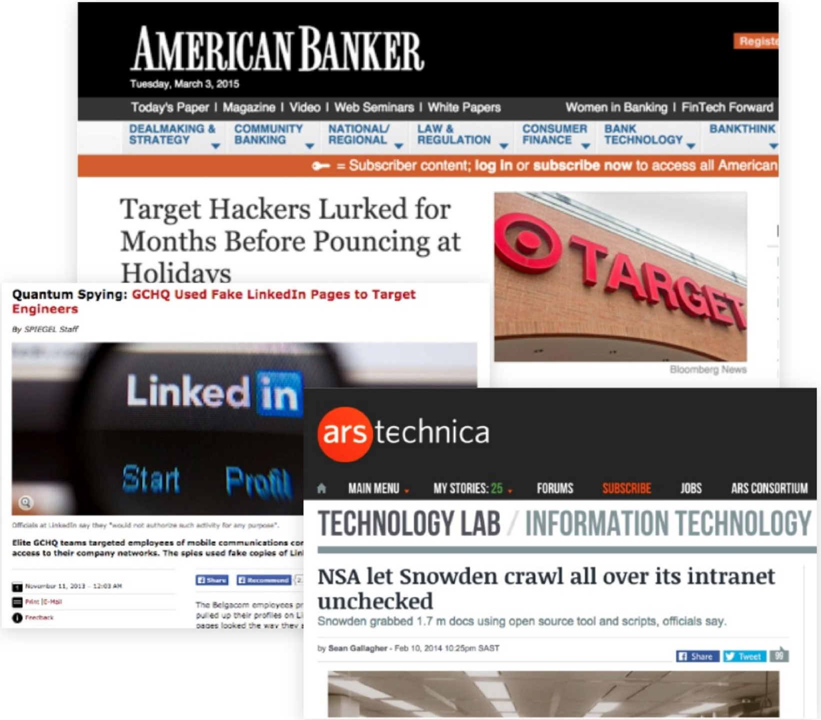
An approach like this is necessary to reduce the **mean time to detect (MTTD),** mitigate the **blast radius of a breach,** and prevent **massive burnout** of security professionals.

The Pyramid Of Pain And Working Until You Go Insane

DON'T GO TO BED, THEY SAID
TRIAGE TICKETS ALL NIGHT INSTEAD SO YOU CAN GET AHEAD AND THEN YOU'LL BE DEAD, THEY SAID

Why Deception Technology?

Because millions of ignored alerts continue to result in devastating and expensive breaches with no end in sight.



Tuesday, March 3, 2015

Target Hackers Lurked for Months Before Pouncing at Holidays

Bloomberg News

Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers

By SPIEGEL Staff

Officials at LinkedIn say they "would not authorize such activity for any purpose".

Elite GCHQ teams targeted employees of mobile communications cor
access to their company networks. The spies used fake copies of Lin

November 11, 2013 – 12:03 AM

The Belgacom employees pr
pulled up their profiles on Li
pages looked the way they

TECHNOLOGY LAB / INFORMATION TECHNOLOGY

NSA let Snowden crawl all over its intranet unchecked

Snowden grabbed 1.7 m docs using open source tool and scripts, officials say.

by Sean Gallagher - Feb 10, 2014 10:25pm SAST

Hackers conduct one of the largest supply chain cyberattacks to date

A breach at Kaseya has affected over 200 companies.

Hackers Breached Colonial Pipeline Using Compromised Password

U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise

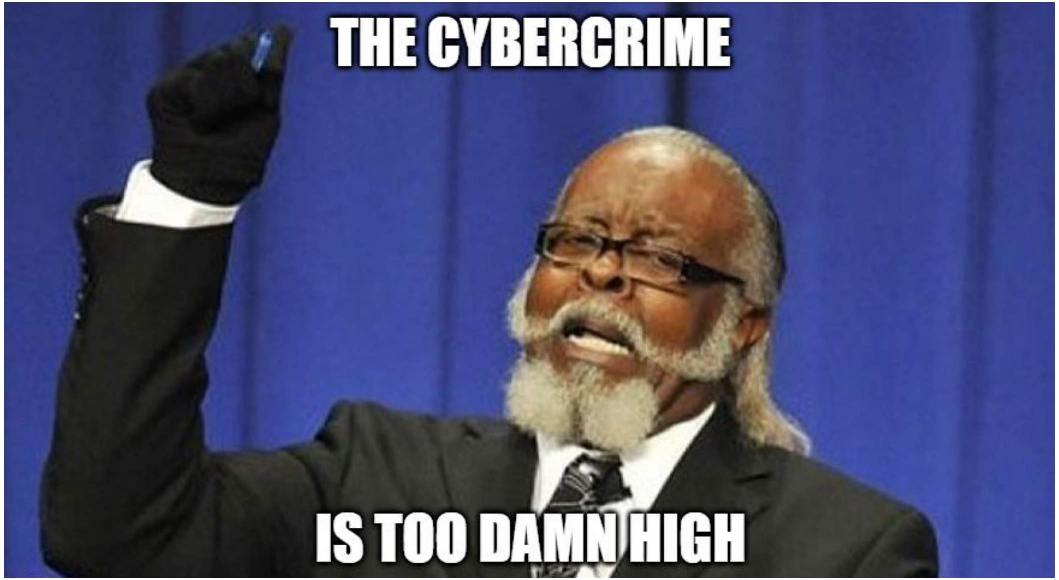
Codecov hack aftermath: hundreds breached, many more to follow

Attackers who breached Codecov for over 2 months also reportedly hacked into hundreds of networks. The full extent of this incident is yet to unfold in the upcoming weeks.

Twitter hack probe leads to call for cybersecurity rules for social media giants

Breach at Equifax May Impact 143M Americans

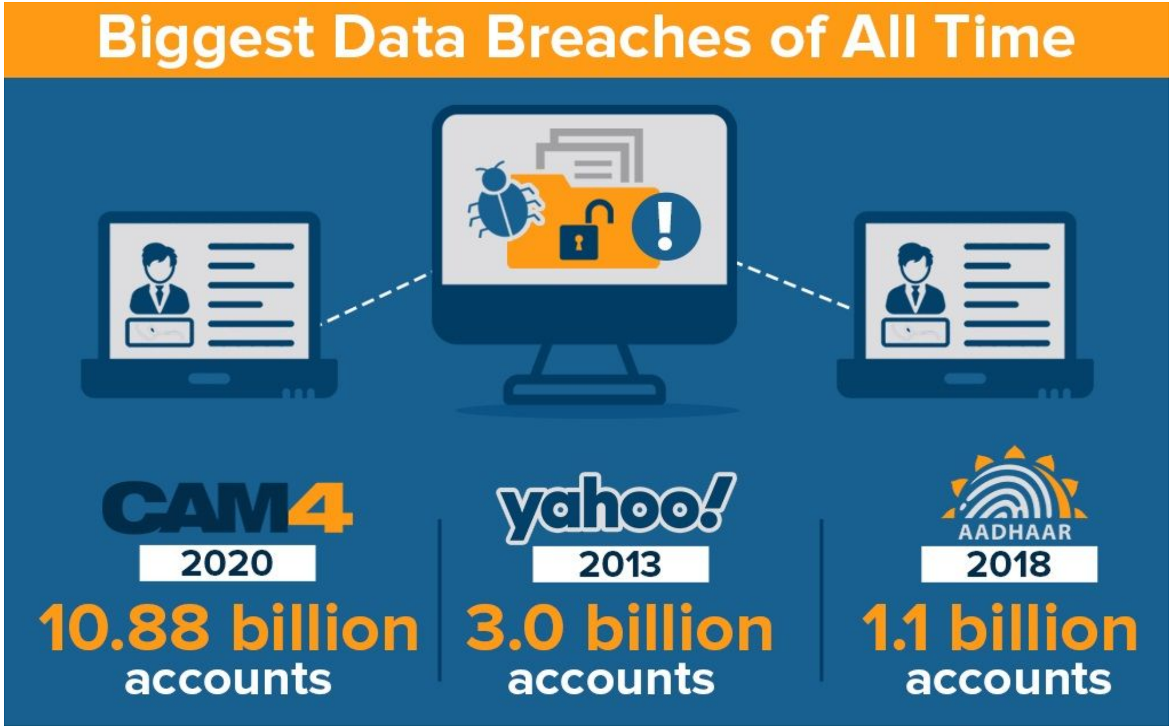
The Price of Rent Isn't The Only Problem Anymore



Global cost of cybercrime topped $6 trillion in 2021: defence firm

- Cybercrime is predicted to cost the world **$10.5 trillion** in 2025
- Every **39 seconds** a business is breached
- **847,376** FBI cyber complaints filed in 2021
- Zero hope of a solution (until now)

212 Days Before Anyone Had A Clue



Biggest Data Breaches of All Time

CAM4
2020
10.88 billion
accounts

yahoo!
2013
3.0 billion
accounts

AADHAAR
2018
1.1 billion
accounts

Canary In The Code Mine

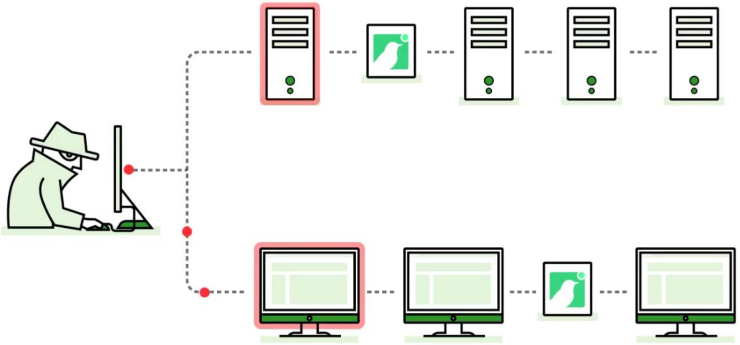
Though it's no longer **coal** to use actual canaries, it is cool to use them in code.

Canaries come in the form of **birds** (honeypots) and **Canarytokens** (honeytokens).

Birds are devices that run legitimate services to appear real and attractive. They can take on the personality of everything from a smart fridge to a dumb terminal.

Canarytokens are digital tripwires that manifest as documents, spreadsheets, API Keys, QR codes, and anything else you can imagine.

We can use Canaries as our early-warning breach detection system.



The Bird Is The Word

THINKST
CANARY

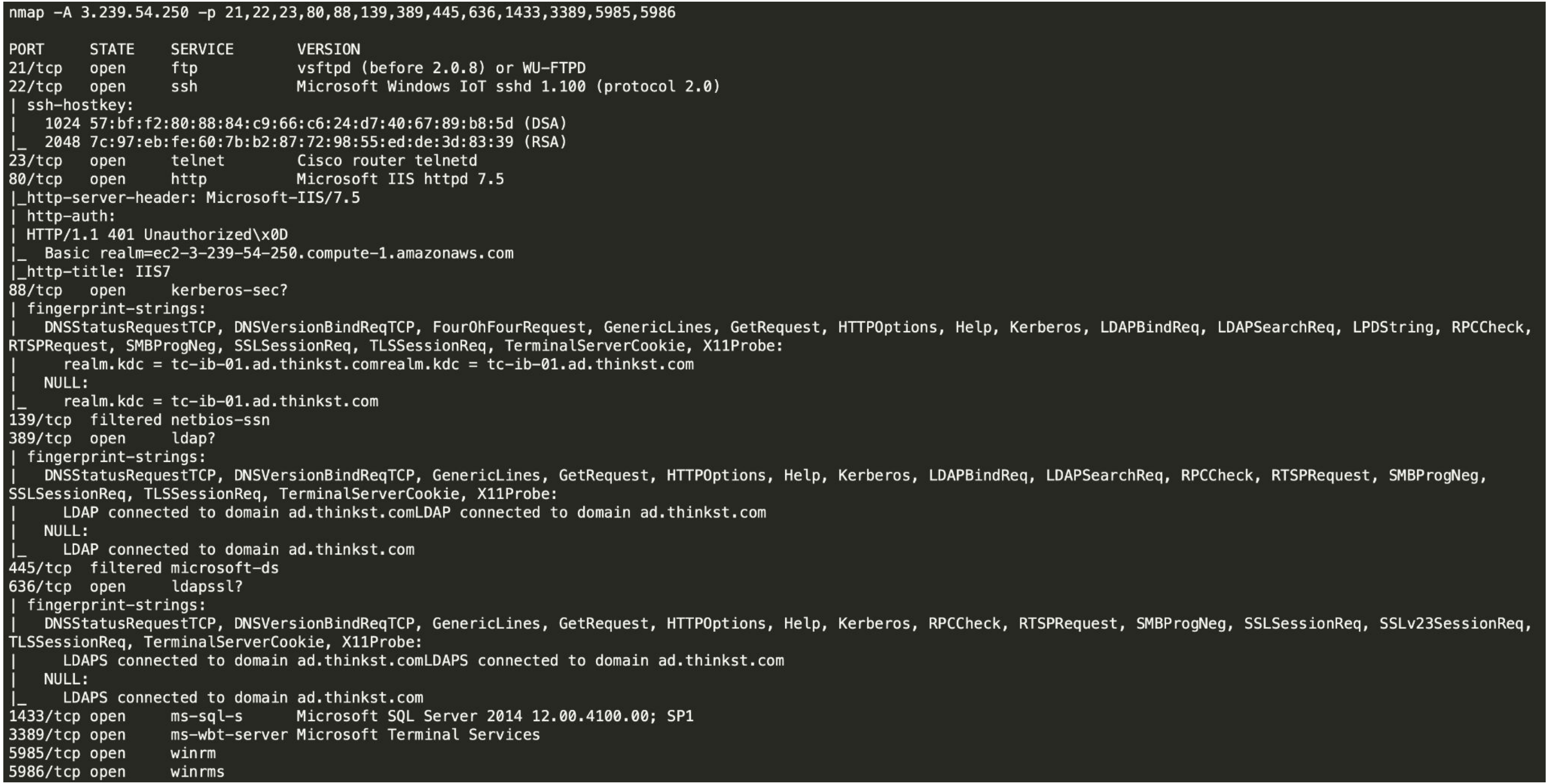
From The Window To The Lulz

Many organizations rely on Microsoft's **Active Directory (AD)** served by a collection of Windows **Domain Controllers (DC)** to centrally manage users, machines, passwords, and files.

A DC is an irresistible target because if you can compromise AD you can often **take over the entire company.**

Let's lure them in with a bird that looks, acts, and chirps like a DC.

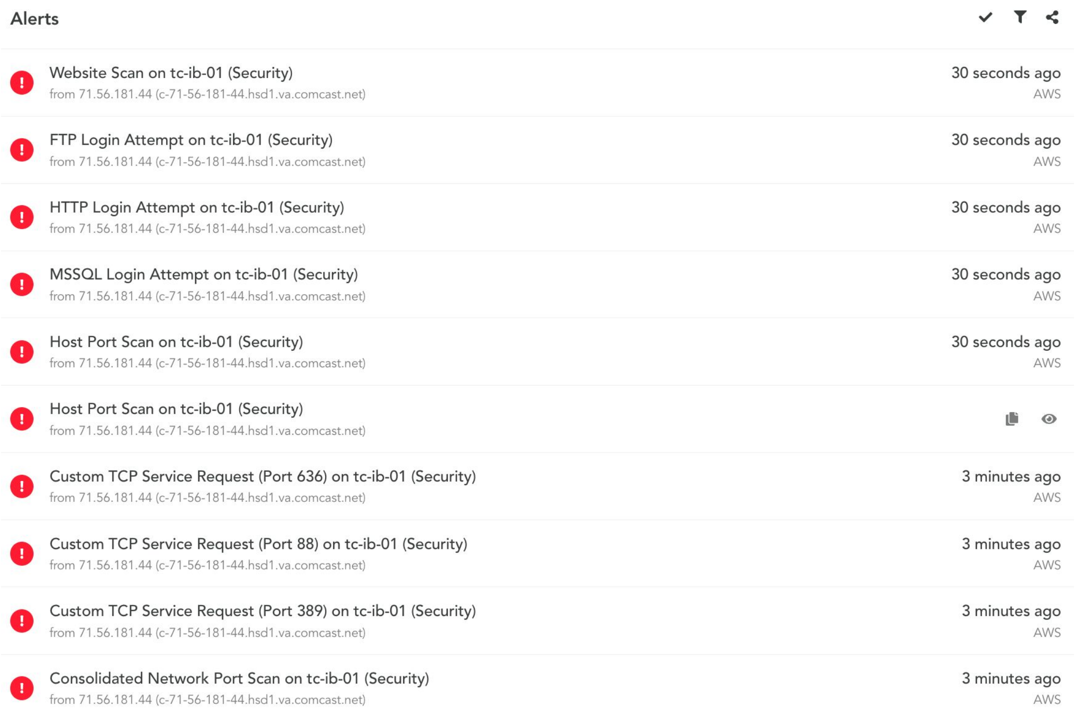
This Is When Keeping It Real Goes Right



```
nmap -A 3.239.54.250 -p 21,22,23,80,88,139,389,445,636,1433,3389,5985,5986

PORT     STATE    SERVICE       VERSION
21/tcp   open     ftp           vsftpd (before 2.0.8) or WU-FTPD
22/tcp   open     ssh           Microsoft Windows IoT sshd 1.100 (protocol 2.0)
| ssh-hostkey:
|   1024 57:bf:f2:80:88:84:c9:66:c6:24:d7:40:67:89:b8:5d (DSA)
|_  2048 7c:97:eb:fe:60:7b:b2:87:72:98:55:ed:de:3d:83:39 (RSA)
23/tcp   open     telnet        Cisco router telnetd
80/tcp   open     http          Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=ec2-3-239-54-250.compute-1.amazonaws.com
|_http-title: IIS7
88/tcp   open     kerberos-sec?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, RPCCheck,
RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|     realm.kdc = tc-ib-01.ad.thinkst.comrealm.kdc = tc-ib-01.ad.thinkst.com
|   NULL:
|_    realm.kdc = tc-ib-01.ad.thinkst.com
139/tcp  filtered netbios-ssn
389/tcp  open     ldap?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LDAPBindReq, LDAPSearchReq, RPCCheck, RTSPRequest, SMBProgNeg,
SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|     LDAP connected to domain ad.thinkst.comLDAP connected to domain ad.thinkst.com
|   NULL:
|_    LDAP connected to domain ad.thinkst.com
445/tcp  filtered microsoft-ds
636/tcp  open     ldapssl?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, RPCCheck, RTSPRequest, SMBProgNeg, SSLSessionReq, SSLv23SessionReq,
TLSSessionReq, TerminalServerCookie, X11Probe:
|     LDAPS connected to domain ad.thinkst.comLDAPS connected to domain ad.thinkst.com
|   NULL:
|_    LDAPS connected to domain ad.thinkst.com
1433/tcp open     ms-sql-s      Microsoft SQL Server 2014 12.00.4100.00; SP1
3389/tcp open     ms-wbt-server Microsoft Terminal Services
5985/tcp open     winrm
5986/tcp open     winrms
```

No Need To Light Up Your Own Christmas Tree



Alerts

Website Scan on tc-ib-01 (Security) — 30 seconds ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

FTP Login Attempt on tc-ib-01 (Security) — 30 seconds ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

HTTP Login Attempt on tc-ib-01 (Security) — 30 seconds ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

MSSQL Login Attempt on tc-ib-01 (Security) — 30 seconds ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

Host Port Scan on tc-ib-01 (Security) — 30 seconds ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

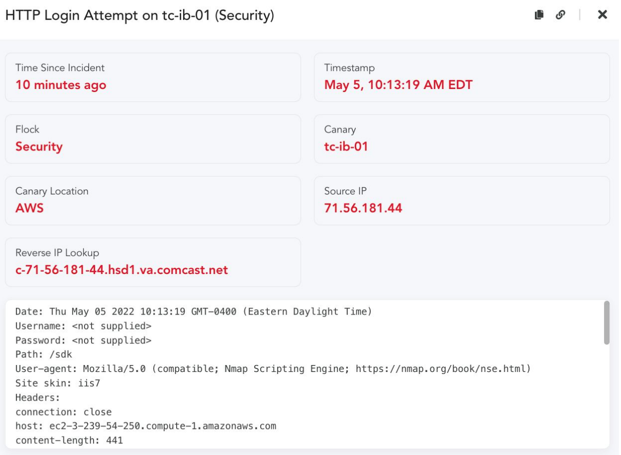
Host Port Scan on tc-ib-01 (Security)
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net)

Custom TCP Service Request (Port 636) on tc-ib-01 (Security) — 3 minutes ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

Custom TCP Service Request (Port 88) on tc-ib-01 (Security) — 3 minutes ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

Custom TCP Service Request (Port 389) on tc-ib-01 (Security) — 3 minutes ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS

Consolidated Network Port Scan on tc-ib-01 (Security) — 3 minutes ago
from 71.56.181.44 (c-71-56-181-44.hsd1.va.comcast.net) — AWS



HTTP Login Attempt on tc-ib-01 (Security)

Time Since Incident: 10 minutes ago

Timestamp: May 5, 10:13:19 AM EDT

Flock: Security

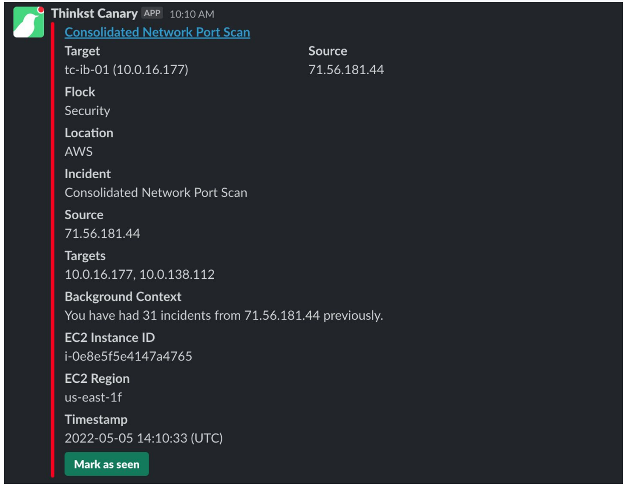
Canary: tc-ib-01

Canary Location: AWS

Source IP: 71.56.181.44

Reverse IP Lookup: c-71-56-181-44.hsd1.va.comcast.net

```
Date: Thu May 05 2022 10:13:19 GMT-0400 (Eastern Daylight Time)
Username: <not supplied>
Password: <not supplied>
Path: /sdk
User-agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
Site skin: iis7
Headers:
connection: close
host: ec2-3-239-54-250.compute-1.amazonaws.com
content-length: 441
```



Thinkst Canary APP 10:10 AM

Consolidated Network Port Scan

Target
tc-ib-01 (10.0.16.177)

Source
71.56.181.44

Flock
Security

Location
AWS

Incident
Consolidated Network Port Scan

Source
71.56.181.44

Targets
10.0.16.177, 10.0.138.112

Background Context
You have had 31 incidents from 71.56.181.44 previously.

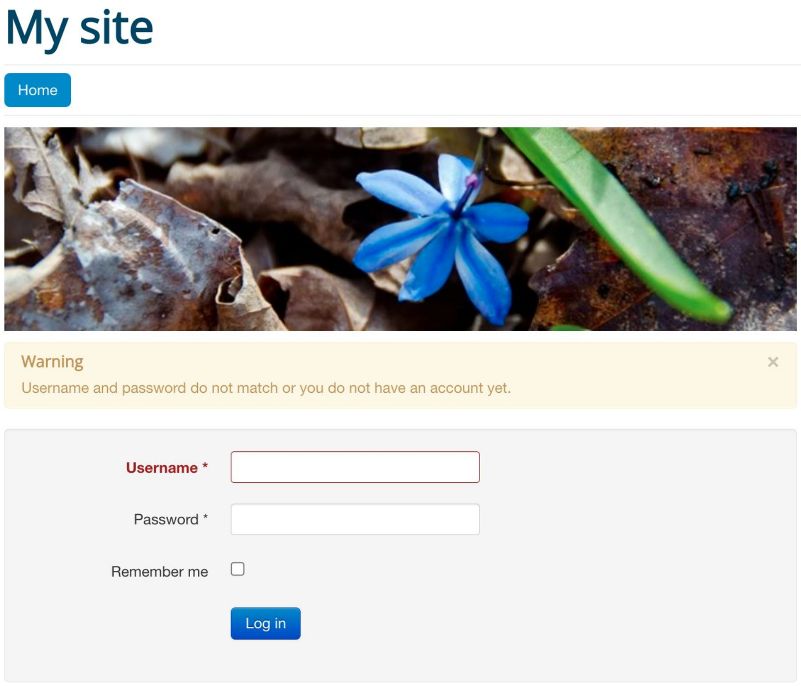
EC2 Instance ID
i-0e8e5f5e4147a4765

EC2 Region
us-east-1f

Timestamp
2022-05-05 14:10:33 (UTC)

What A Tangled Web We Weave When We Deceive

Canaries can be customized to mimic the personality of everything from a database to a Joomla CMS.
Let your birds blend into the rest of your environment and adversaries will inevitably poke at them.



My site

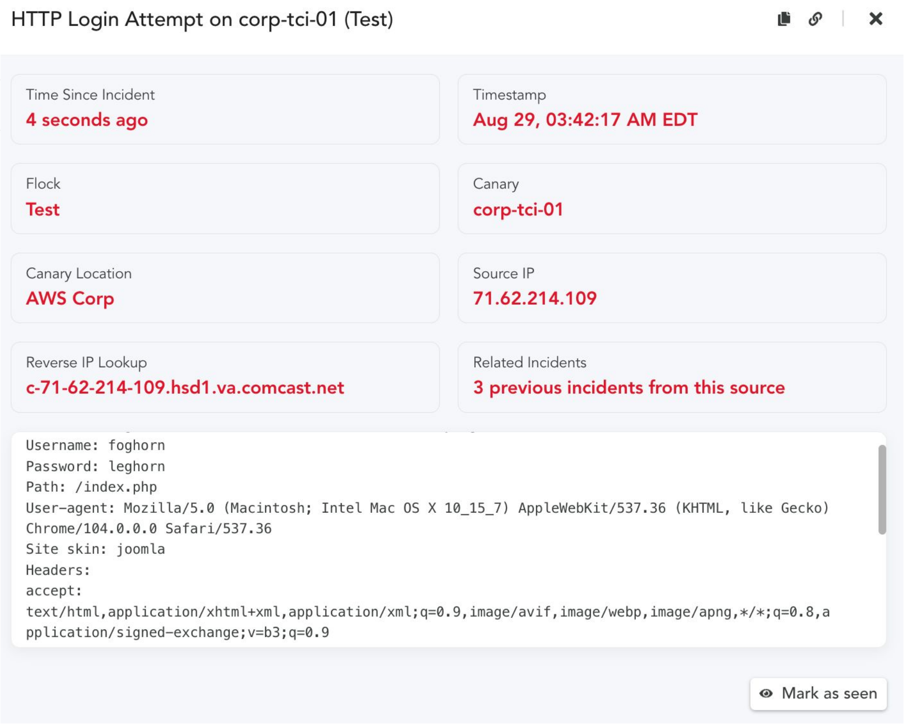
Warning

Username and password do not match or you do not have an account yet.

Username *

Password *

Remember me □



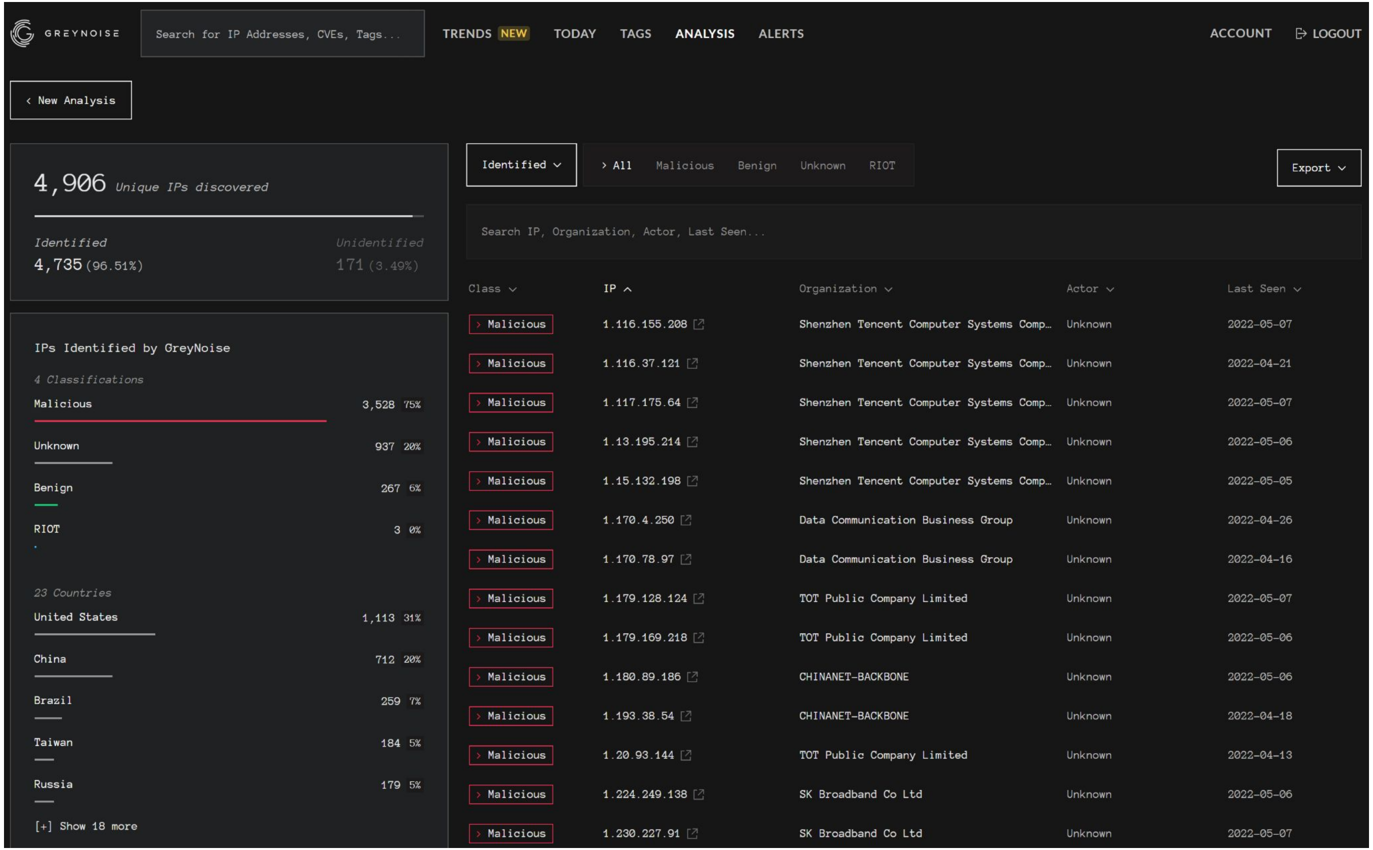
HTTP Login Attempt on corp-tci-01 (Test)

Time Since Incident 4 seconds ago	Timestamp Aug 29, 03:42:17 AM EDT
Flock Test	Canary corp-tci-01
Canary Location AWS Corp	Source IP 71.62.214.109
Reverse IP Lookup c-71-62-214-109.hsd1.va.comcast.net	Related Incidents 3 previous incidents from this source

```
Username: foghorn
Password: leghorn
Path: /index.php
User-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.0.0 Safari/537.36
Site skin: joomla
Headers:
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.9
```

The Internet Is Not A Big Truck…It's Mostly (Grey)Noise

Curious minds can deploy an **outside bird** to collect malicious IPs from the Internet and then automate contextual analysis with the natively-integrated meta-threat intel service **GreyNoise** to quickly identify who is actively targeting you in the wild.



4,906 *Unique IPs discovered*

Identified 4,735 (96.51%)

Unidentified 171 (3.49%)

IPs Identified by GreyNoise

4 Classifications

Malicious	3,528	75%
Unknown	937	20%
Benign	267	6%
RIOT	3	0%

23 Countries

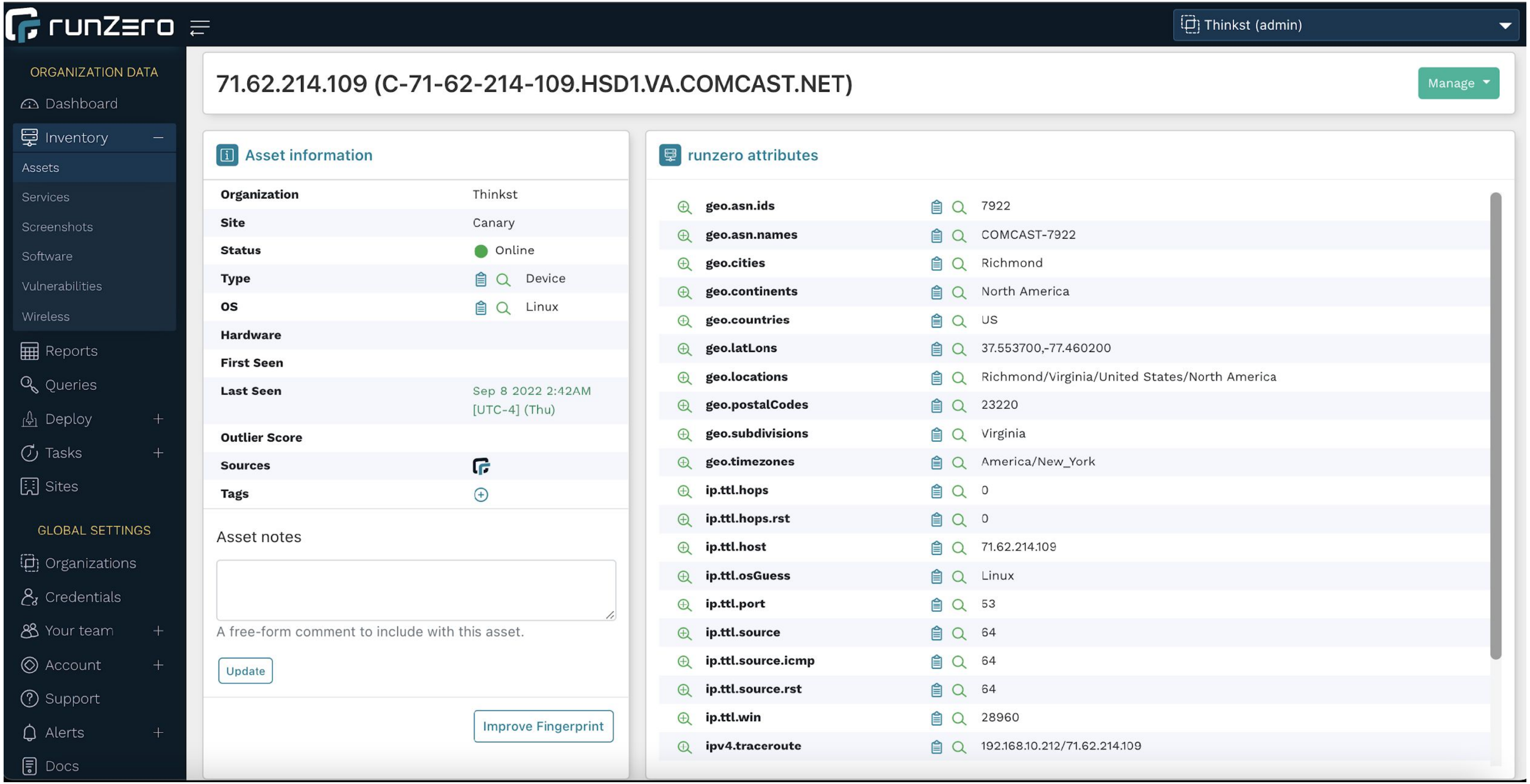
United States	1,113	31%
China	712	20%
Brazil	259	7%
Taiwan	184	5%
Russia	179	5%

[+] Show 18 more

Class ⌄	IP ^	Organization ⌄	Actor ⌄	Last Seen ⌄
› Malicious	1.116.155.208	Shenzhen Tencent Computer Systems Comp…	Unknown	2022-05-07
› Malicious	1.116.37.121	Shenzhen Tencent Computer Systems Comp…	Unknown	2022-04-21
› Malicious	1.117.175.64	Shenzhen Tencent Computer Systems Comp…	Unknown	2022-05-07
› Malicious	1.13.195.214	Shenzhen Tencent Computer Systems Comp…	Unknown	2022-05-06
› Malicious	1.15.132.198	Shenzhen Tencent Computer Systems Comp…	Unknown	2022-05-05
› Malicious	1.170.4.250	Data Communication Business Group	Unknown	2022-04-26
› Malicious	1.170.78.97	Data Communication Business Group	Unknown	2022-04-16
› Malicious	1.179.128.124	TOT Public Company Limited	Unknown	2022-05-07
› Malicious	1.179.169.218	TOT Public Company Limited	Unknown	2022-05-06
› Malicious	1.180.89.186	CHINANET-BACKBONE	Unknown	2022-05-06
› Malicious	1.193.38.54	CHINANET-BACKBONE	Unknown	2022-04-18
› Malicious	1.20.93.144	TOT Public Company Limited	Unknown	2022-04-13
› Malicious	1.224.249.138	SK Broadband Co Ltd	Unknown	2022-05-06
› Malicious	1.230.227.91	SK Broadband Co Ltd	Unknown	2022-05-07

RunZero Is The Hero We Deserve And The One We Need

Canary and runZero go together like **Pretzels and Beer Cheese**.
Source IPs from Canary alerts automatically create runZero assets for enrichment and context.



71.62.214.109 (C-71-62-214-109.HSD1.VA.COMCAST.NET)

Asset information

Organization	Thinkst
Site	Canary
Status	● Online
Type	Device
OS	Linux
Hardware	
First Seen	
Last Seen	Sep 8 2022 2:42AM [UTC-4] (Thu)
Outlier Score	
Sources	
Tags	⊕

Asset notes

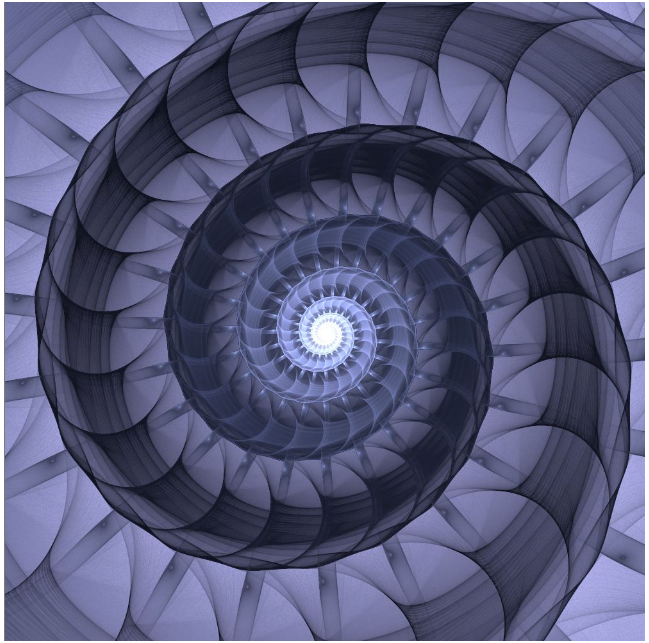
A free-form comment to include with this asset.

runzero attributes

geo.asn.ids	7922
geo.asn.names	COMCAST-7922
geo.cities	Richmond
geo.continents	North America
geo.countries	US
geo.latLons	37.553700,-77.460200
geo.locations	Richmond/Virginia/United States/North America
geo.postalCodes	23220
geo.subdivisions	Virginia
geo.timezones	America/New_York
ip.ttl.hops	0
ip.ttl.hops.rst	0
ip.ttl.host	71.62.214.109
ip.ttl.osGuess	Linux
ip.ttl.port	53
ip.ttl.source	64
ip.ttl.source.icmp	64
ip.ttl.source.rst	64
ip.ttl.win	28960
ipv4.traceroute	192.168.10.212/71.62.214.109

Now That's Tasty

It’s Tokens All The Way Down

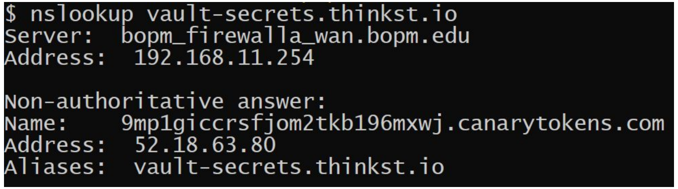


Recon? Damn Near Killed Him!

Deceive Nosy Strangers (DNS)

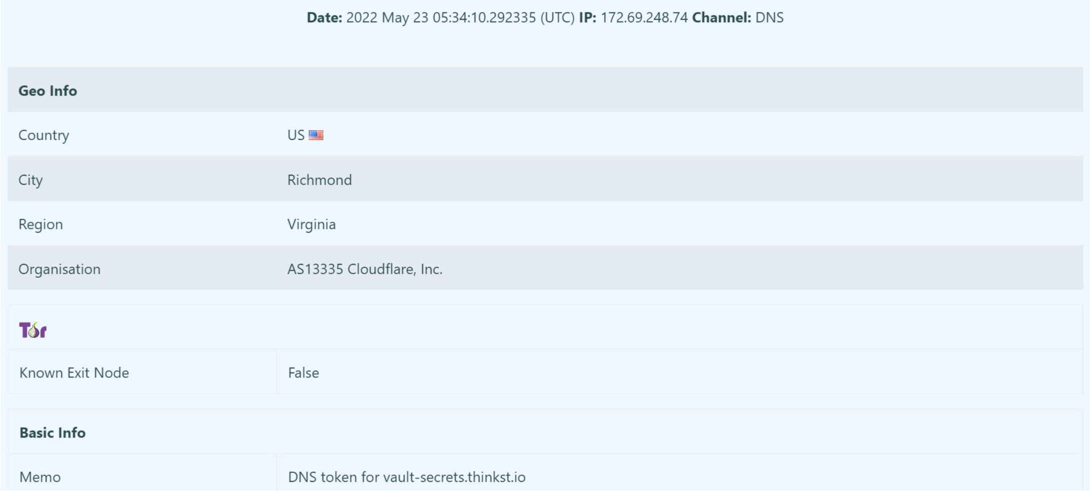
The **Domain Name System (DNS)** is a comprehensive directory of human-readable names mapped to IP addresses that was built because most people don’t enjoy memorizing numbers.

We can use **DNS tokens** to map fictitious domain names to unused (dark) network addresses that alert us when **Snoop Dogg** is in the building.



```
$ nslookup vault-secrets.thinkst.io
Server:   bopm_firewalla_wan.bopm.edu
Address:  192.168.11.254

Non-authoritative answer:
Name:    9mp1giccrsfjom2tkb196mxwj.canarytokens.com
Address:  52.18.63.80
Aliases:  vault-secrets.thinkst.io
```



Date: 2022 May 23 05:34:10.292335 (UTC) **IP:** 172.69.248.74 **Channel:** DNS

Geo Info	
Country	US 🇺🇸
City	Richmond
Region	Virginia
Organisation	AS13335 Cloudflare, Inc.

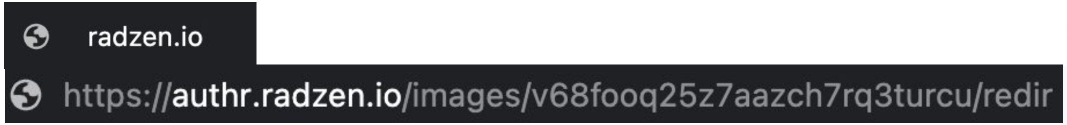
Tor	
Known Exit Node	False

Basic Info	
Memo	DNS token for vault-secrets.thinkst.io

Focus On The Journey And Not The Destination

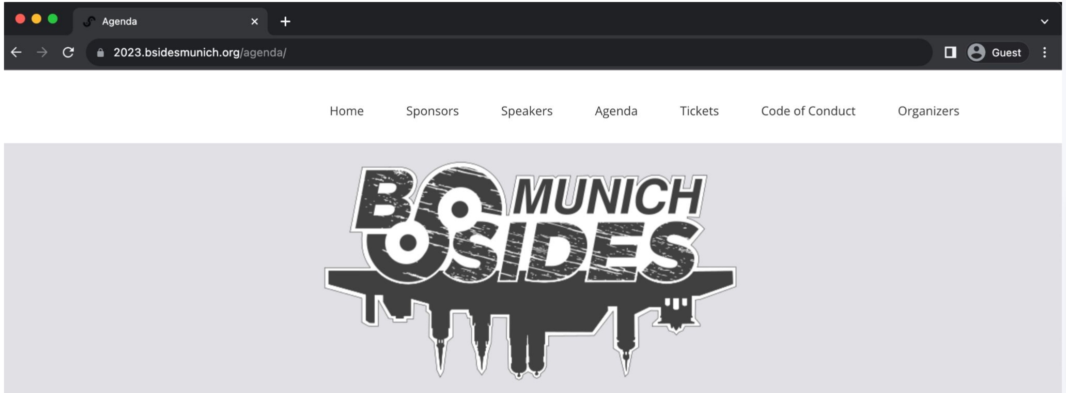
Continuing along the path of DNS, many curious minds will visit interesting subdomains to see what lives there.

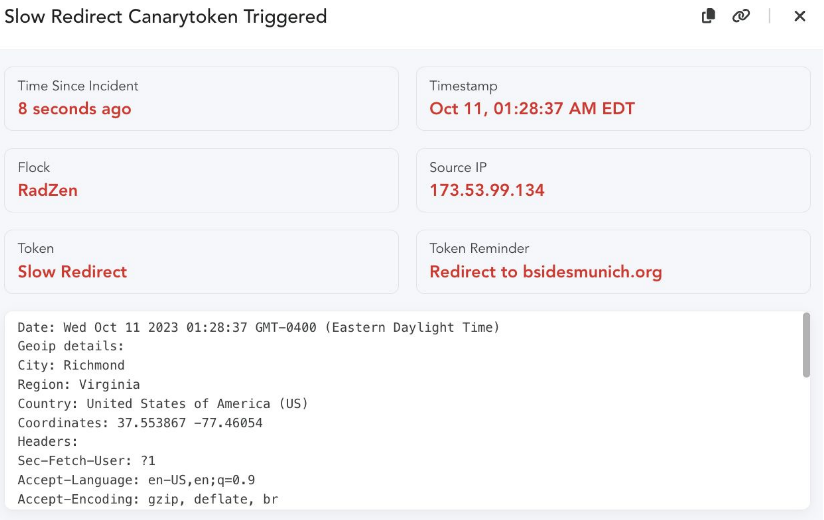
Web redirect tokens are ideal for grabbing tons of useful information from **Nosie O'Donnell's** browser and then sending them to a warm, fuzzy place like **bsidesmunich.org** with their feelings of consternation left intact.



radzen.io

https://authr.radzen.io/images/v68fooq25z7aazch7rq3turcu/redir





Slow Redirect Canarytoken Triggered

Time Since Incident
8 seconds ago

Timestamp
Oct 11, 01:28:37 AM EDT

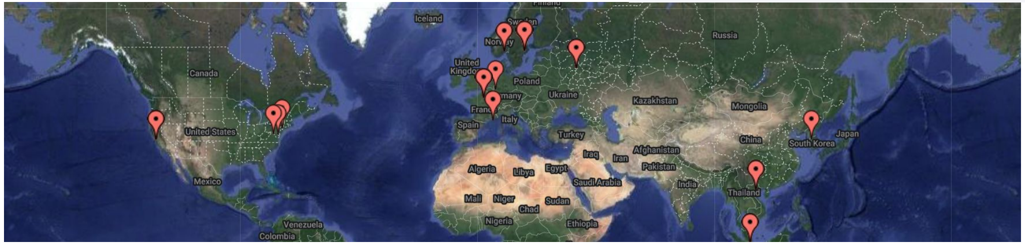
Flock
RadZen

Source IP
173.53.99.134

Token
Slow Redirect

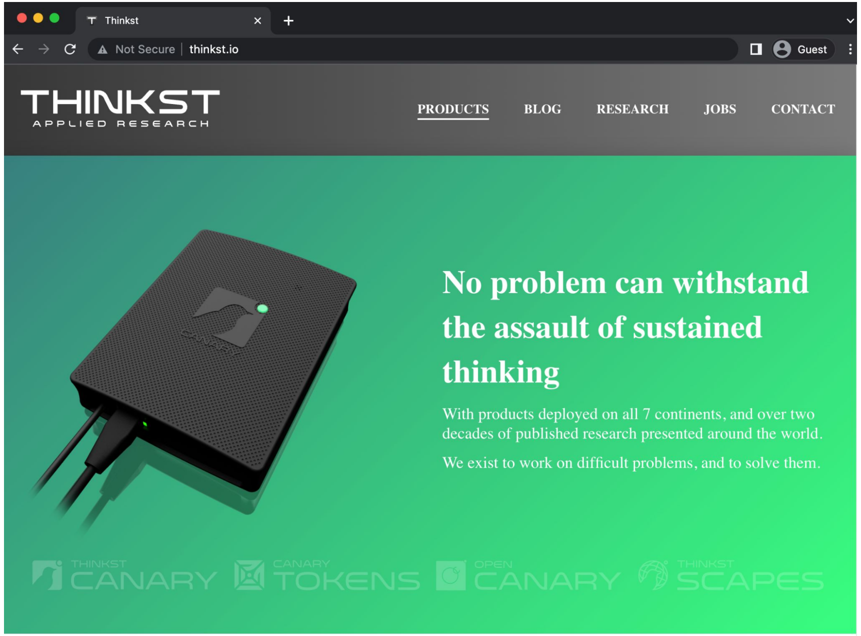
Token Reminder
Redirect to bsidesmunich.org

```
Date: Wed Oct 11 2023 01:28:37 GMT-0400 (Eastern Daylight Time)
Geoip details:
City: Richmond
Region: Virginia
Country: United States of America (US)
Coordinates: 37.553867 -77.46054
Headers:
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate, br
```



Dodge, Duck, Dip, Dive, And Desist

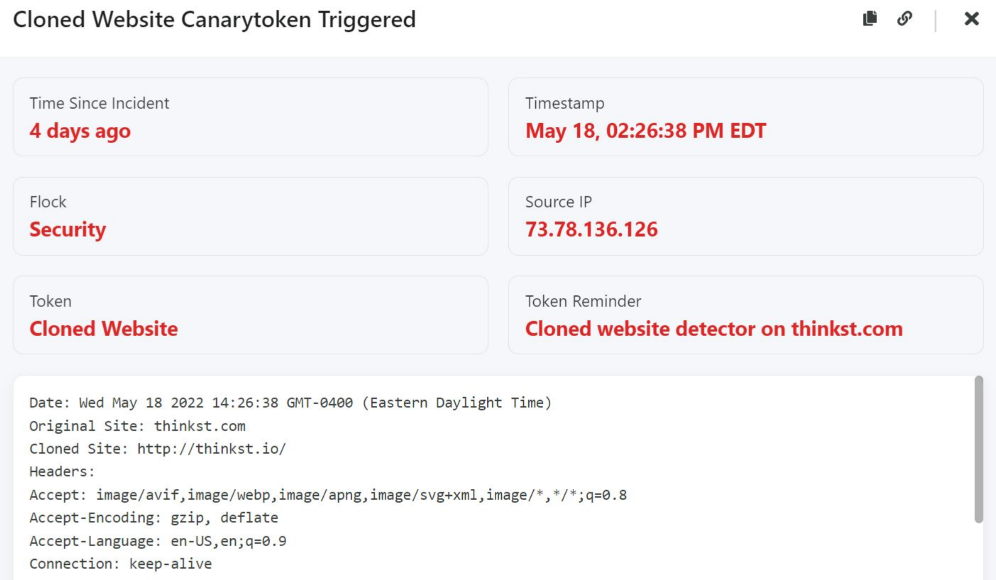
They say imitation is the sincerest form of flattery but if your website is cloned and deployed on a doppelganger domain, there’s a good chance a **phishing campaign is underway.**



No problem can withstand the assault of sustained thinking

With products deployed on all 7 continents, and over two decades of published research presented around the world.

We exist to work on difficult problems, and to solve them.



Cloned Website Canarytoken Triggered

Time Since Incident
4 days ago

Timestamp
May 18, 02:26:38 PM EDT

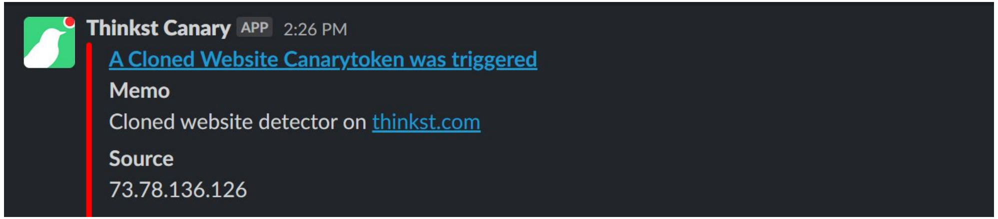
Flock
Security

Source IP
73.78.136.126

Token
Cloned Website

Token Reminder
Cloned website detector on thinkst.com

```
Date: Wed May 18 2022 14:26:38 GMT-0400 (Eastern Daylight Time)
Original Site: thinkst.com
Cloned Site: http://thinkst.io/
Headers:
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```



Thinkst Canary APP 2:26 PM

A Cloned Website Canarytoken was triggered

Memo

Cloned website detector on thinkst.com

Source

73.78.136.126

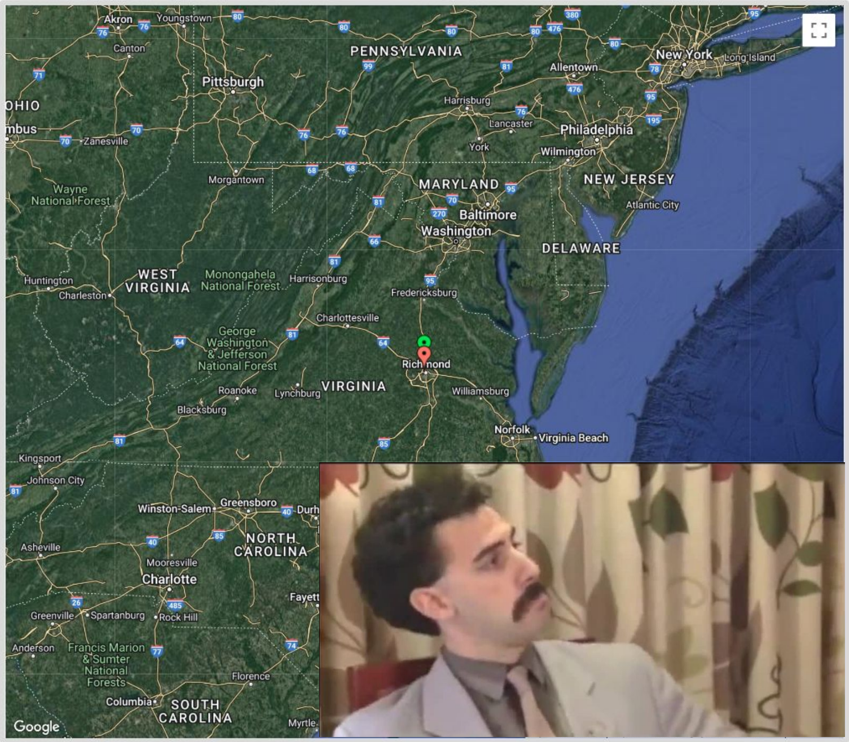
THINKST CANARY

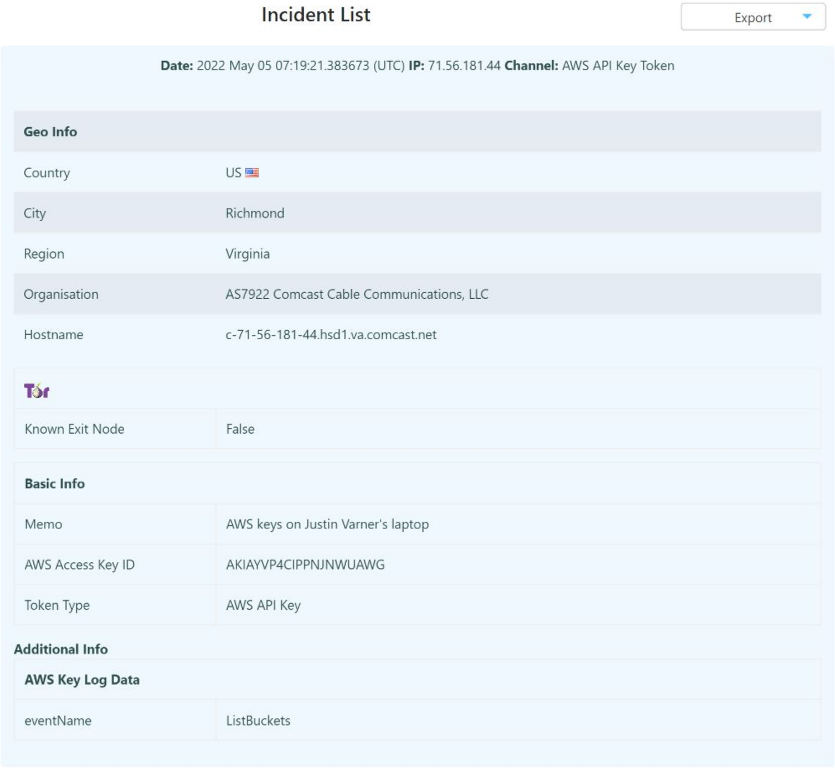
API = Alert. Protect. Investigate.

King Of The Cloud Wa Wa Wee Wa

Amazon Web Services (AWS) keys are an attractive target because in the cloud-native world these are the proverbial **keys to the kingdom**. You can drop these tokens on every company machine and know exactly when a bad actor is up to no good.

Incident Map




Incident List

Export

Date: 2022 May 05 07:19:21.383673 (UTC) **IP:** 71.56.181.44 **Channel:** AWS API Key Token

Geo Info	
Country	US 🇺🇸
City	Richmond
Region	Virginia
Organisation	AS7922 Comcast Cable Communications, LLC
Hostname	c-71-56-181-44.hsd1.va.comcast.net

Tor	
Known Exit Node	False

Basic Info	
Memo	AWS keys on Justin Varner's laptop
AWS Access Key ID	AKIAYVP4CIPPNJNWUAWG
Token Type	AWS API Key

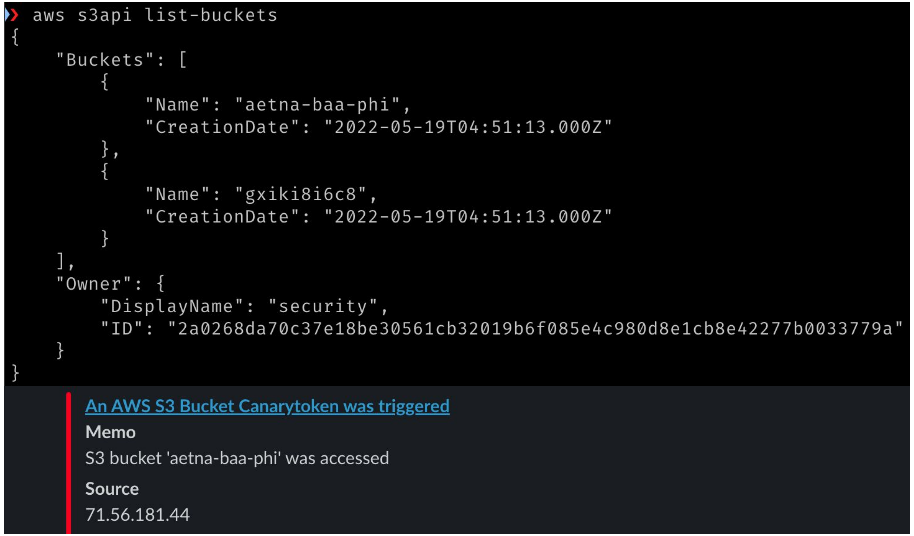
Additional Info

AWS Key Log Data	
eventName	ListBuckets

More Bang For The Bucket

It’s not a matter of **if** an organization will get breached but rather **when** (and how badly).
This means that although **prevention is futile**, we can ensure **detection is fruitful**.

A highly effective detection mechanism is a tokened **AWS Simple Storage Service (S3) bucket**.
Merely listing the buckets will fire an alert so you’ll know when someone is banging on your trash cans.



```
❯ aws s3api list-buckets
{
    "Buckets": [
        {
            "Name": "aetna-baa-phi",
            "CreationDate": "2022-05-19T04:51:13.000Z"
        },
        {
            "Name": "gxiki8i6c8",
            "CreationDate": "2022-05-19T04:51:13.000Z"
        }
    ],
    "Owner": {
        "DisplayName": "security",
        "ID": "2a0268da70c37e18be30561cb32019b6f085e4c980d8e1cb8e42277b0033779a"
    }
}
```

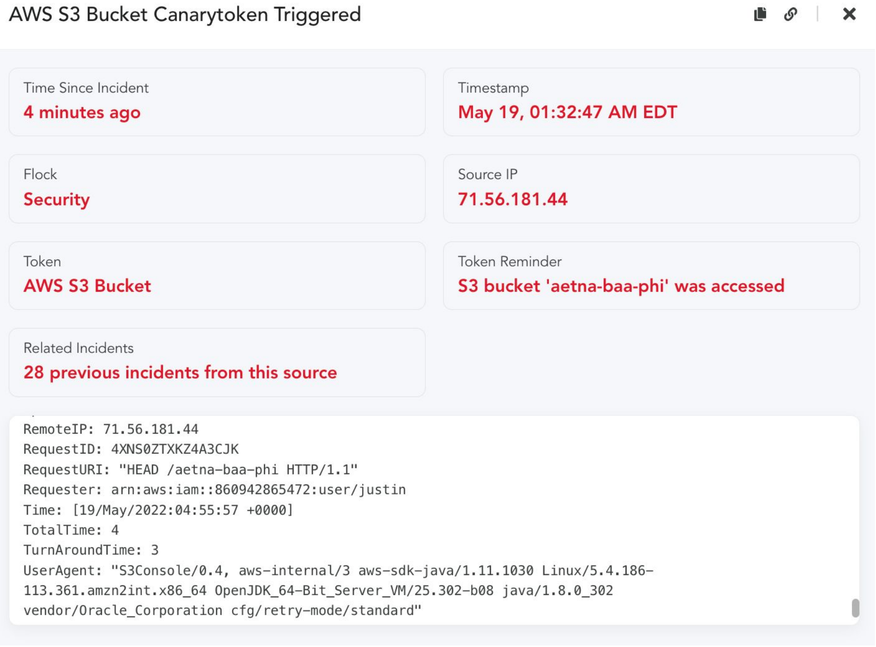
An AWS S3 Bucket Canarytoken was triggered

Memo

S3 bucket 'aetna-baa-phi' was accessed

Source

71.56.181.44



AWS S3 Bucket Canarytoken Triggered

Time Since Incident
4 minutes ago

Timestamp
May 19, 01:32:47 AM EDT

Flock
Security

Source IP
71.56.181.44

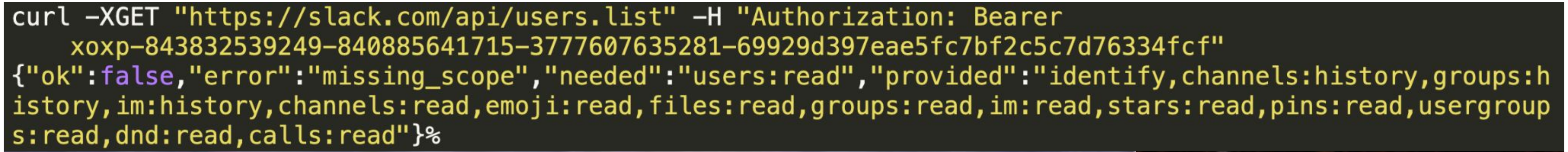
Token
AWS S3 Bucket

Token Reminder
S3 bucket 'aetna-baa-phi' was accessed

Related Incidents
28 previous incidents from this source

```
RemoteIP: 71.56.181.44
RequestID: 4XNS0ZTXKZ4A3CJK
RequestURI: "HEAD /aetna-baa-phi HTTP/1.1"
Requester: arn:aws:iam::860942865472:user/justin
Time: [19/May/2022:04:55:57 +0000]
TotalTime: 4
TurnAroundTime: 3
UserAgent: "S3Console/0.4, aws-internal/3 aws-sdk-java/1.11.1030 Linux/5.4.186-
113.361.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.302-b08 java/1.8.0_302
vendor/Oracle_Corporation cfg/retry-mode/standard"
```

Heavy Meta Slack

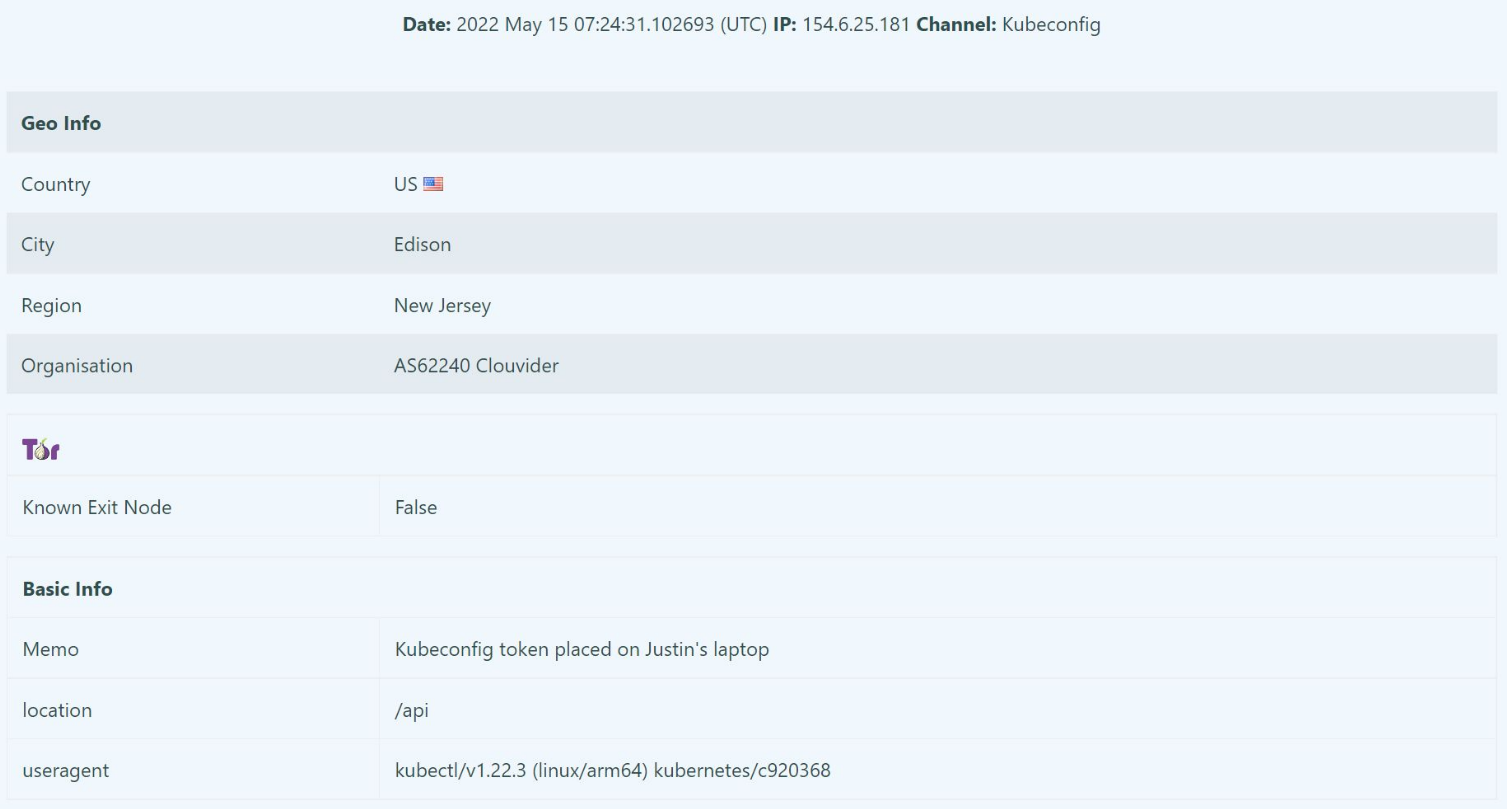


```
curl -XGET "https://slack.com/api/users.list" -H "Authorization: Bearer
    xoxp-843832539249-840885641715-3777607635281-69929d397eae5fc7bf2c5c7d76334fcf"
{"ok":false,"error":"missing_scope","needed":"users:read","provided":"identify,channels:history,groups:h
istory,im:history,channels:read,emoji:read,files:read,groups:read,im:read,stars:read,pins:read,usergroup
s:read,dnd:read,calls:read"}%
```

YO DAWG I HEARD YOU LIKE SLACK
SO I DROPPED SOME SLACK TOKENS IN YOUR SLACK
SPACE SO YOU CAN TAKE YOUR STUNNED FACE BACK TO MYSPACE

If You Need Great Bait Just Cast Some K8s

Kubernetes (K + 8 letters + S) is a platform for easily managing tons of containerized applications. You better believe K8s will bring all the bums to the jar.



Date: 2022 May 15 07:24:31.102693 (UTC) **IP:** 154.6.25.181 **Channel:** Kubeconfig

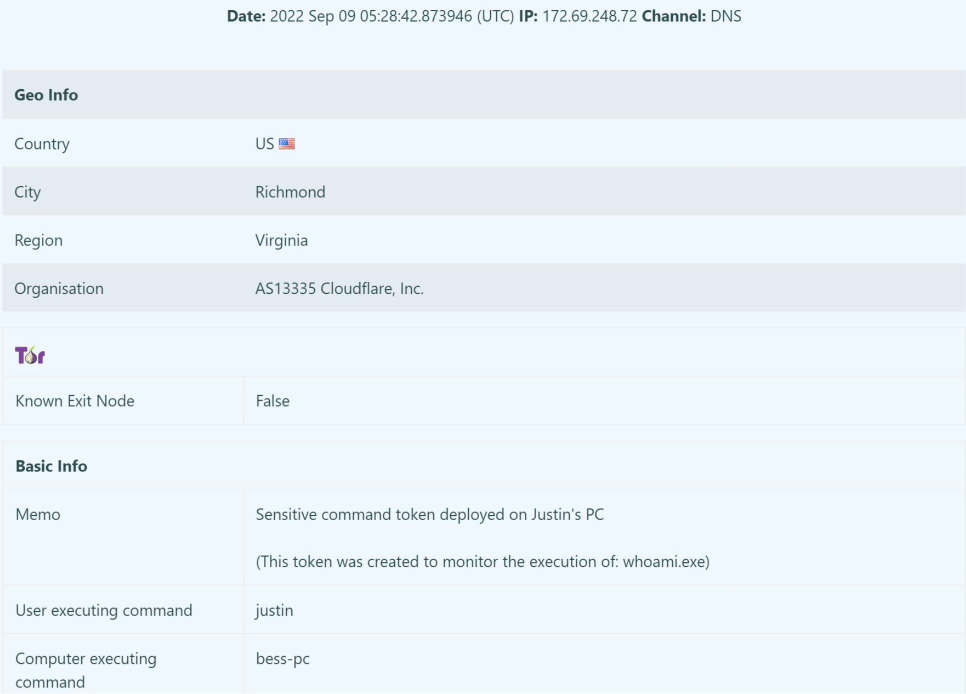
Geo Info	
Country	US 🇺🇸
City	Edison
Region	New Jersey
Organisation	AS62240 Clouvider

Tor	
Known Exit Node	False

Basic Info	
Memo	Kubeconfig token placed on Justin's laptop
location	/api
useragent	kubectl/v1.22.3 (linux/arm64) kubernetes/c920368

I Accidentally A Tripwired Executable…Is This Dangerous?

The newest canarytoken monitors for Windows commands that you wouldn't expect to see executed on a healthy host.
If **Jim Lahey** from facilities starts running **whoami** then he likely let the liquor do the thinking before he started cruising online.


Date: 2022 Sep 09 05:28:42.873946 (UTC) **IP:** 172.69.248.72 **Channel:** DNS

Geo Info	
Country	US 🇺🇸
City	Richmond
Region	Virginia
Organisation	AS13335 Cloudflare, Inc.

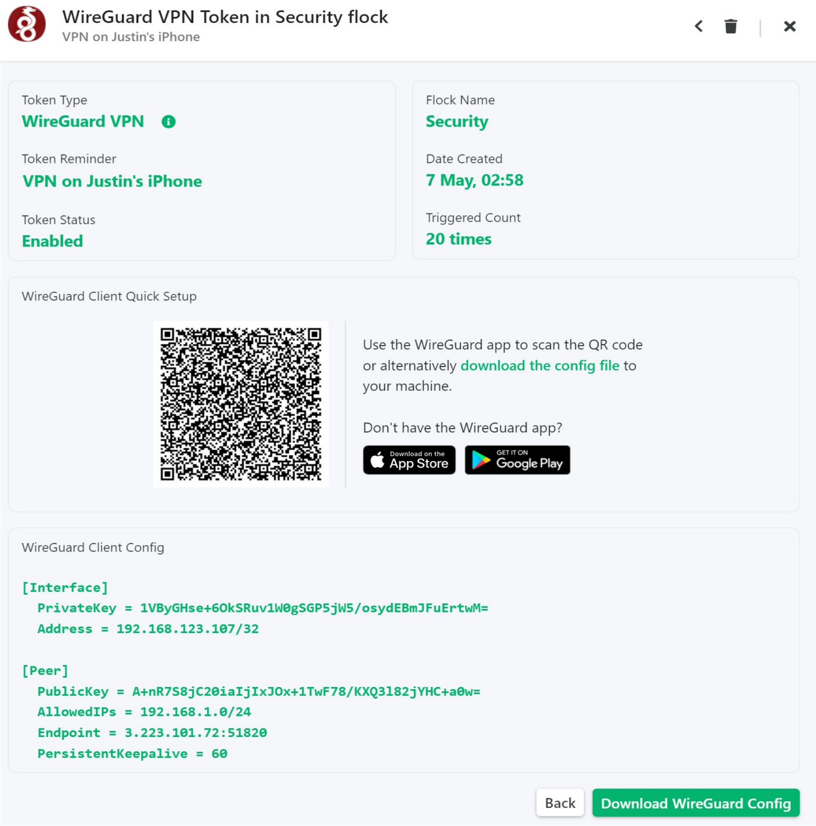
Tor	
Known Exit Node	False

Basic Info	
Memo	Sensitive command token deployed on Justin's PC (This token was created to monitor the execution of: whoami.exe)
User executing command	justin
Computer executing command	bess-pc

You’re Not Gonna Breach My Telephone

How Would I Know If My iPhone Got iPwned?

A **Wireguard VPN** token is ideal for alerting us if our mobile device has been surreptitiously compromised by nasty spyware. Install the app, scan the QR code, give the profile an intriguing name, and then go get a Walkie Talkie if this phone gets owned.



WireGuard VPN Token in Security flock

VPN on Justin's iPhone

Token Type
WireGuard VPN

Token Reminder
VPN on Justin's iPhone

Token Status
Enabled

Flock Name
Security

Date Created
7 May, 02:58

Triggered Count
20 times

WireGuard Client Quick Setup

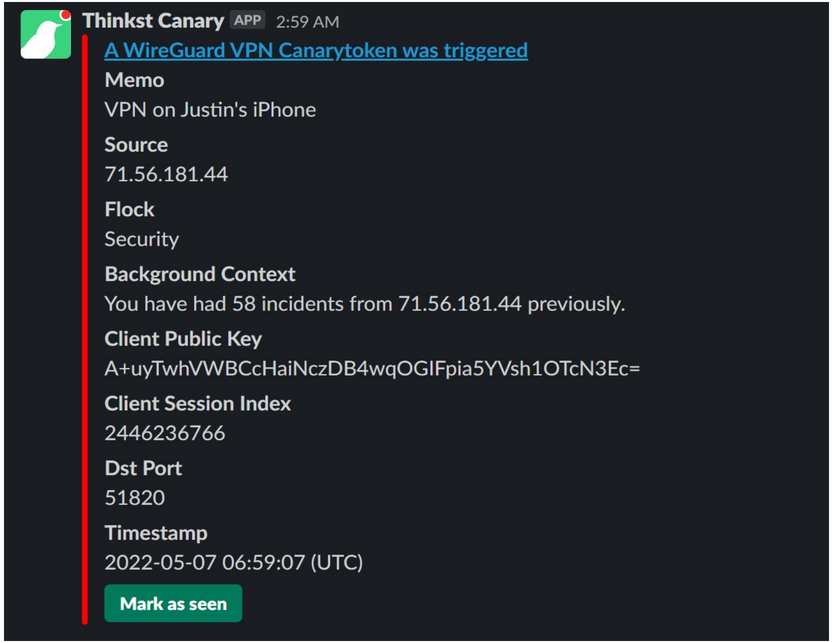
Use the WireGuard app to scan the QR code or alternatively download the config file to your machine.

Don't have the WireGuard app?

WireGuard Client Config

```
[Interface]
  PrivateKey = 1VByGHse+6OkSRuv1W0gSGP5jW5/osydEBmJFuErtwM=
  Address = 192.168.123.107/32

[Peer]
  PublicKey = A+nR7S8jC20iaIjIxJOx+1TwF78/KXQ3l82jYHC+a0w=
  AllowedIPs = 192.168.1.0/24
  Endpoint = 3.223.101.72:51820
  PersistentKeepalive = 60
```



Thinkst Canary APP 2:59 AM

A WireGuard VPN Canarytoken was triggered

Memo
VPN on Justin's iPhone

Source
71.56.181.44

Flock
Security

Background Context
You have had 58 incidents from 71.56.181.44 previously.

Client Public Key
A+uyTwhVWBCcHaiNczDB4wqOGIFpia5YVsh1OTcN3Ec=

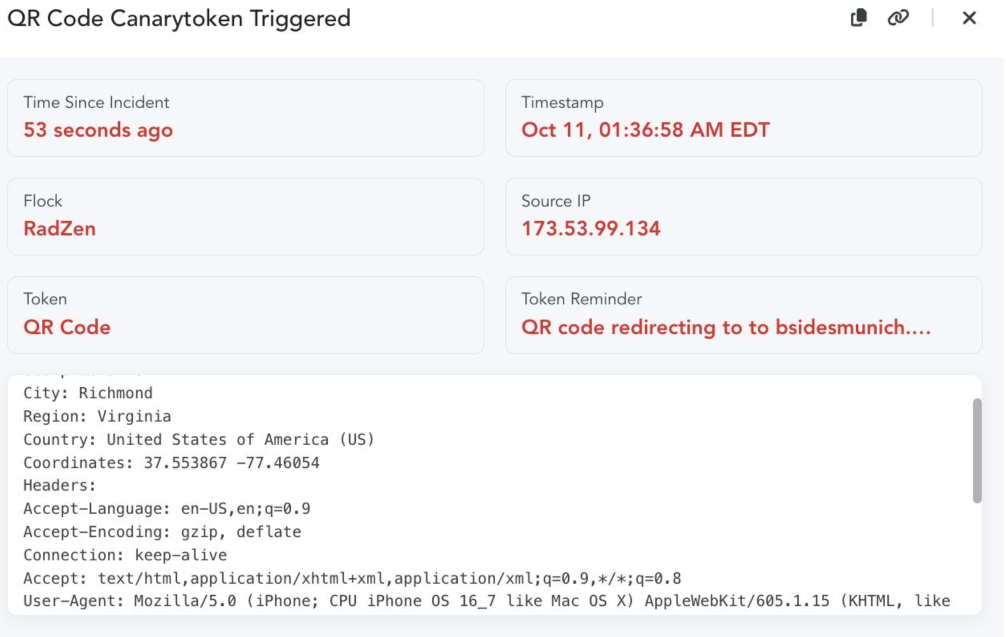
Client Session Index
2446236766

Dst Port
51820

Timestamp
2022-05-07 06:59:07 (UTC)

Bad Guys Hate It When You Use This One Weird Trick

1) Open the camera on your phone
2) Point it at the QR code below
3) Click the box to launch the URL
4) ???
5) Deception



QR Code Canarytoken Triggered

Time Since Incident
53 seconds ago

Timestamp
Oct 11, 01:36:58 AM EDT

Flock
RadZen

Source IP
173.53.99.134

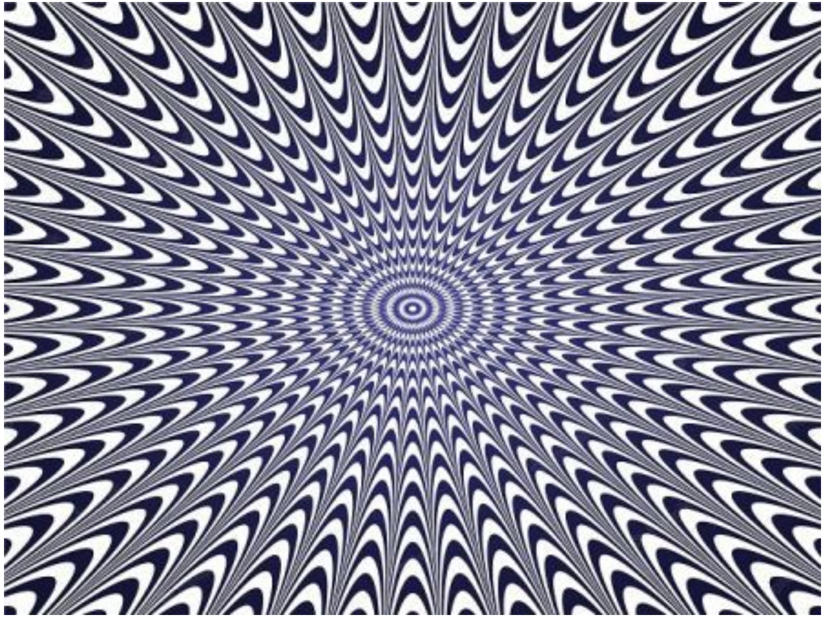
Token
QR Code

Token Reminder
QR code redirecting to to bsidesmunich....

```
City: Richmond
Region: Virginia
Country: United States of America (US)
Coordinates: 37.553867 -77.46054
Headers:
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
```

Drop an unread message in your mailbox with the subject line "MFA Device Enrollment Code"

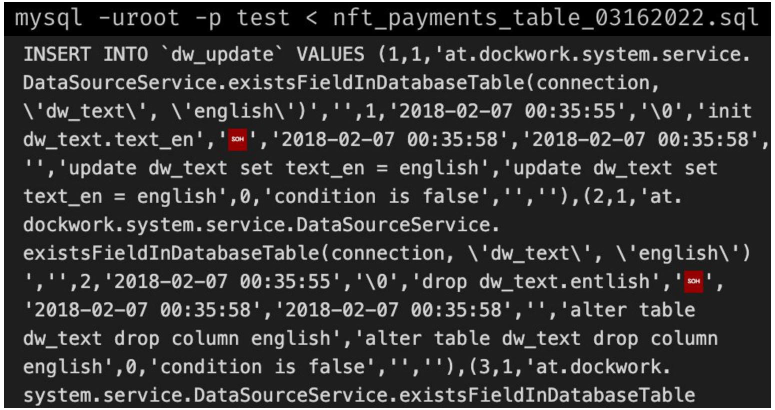
Mind Games



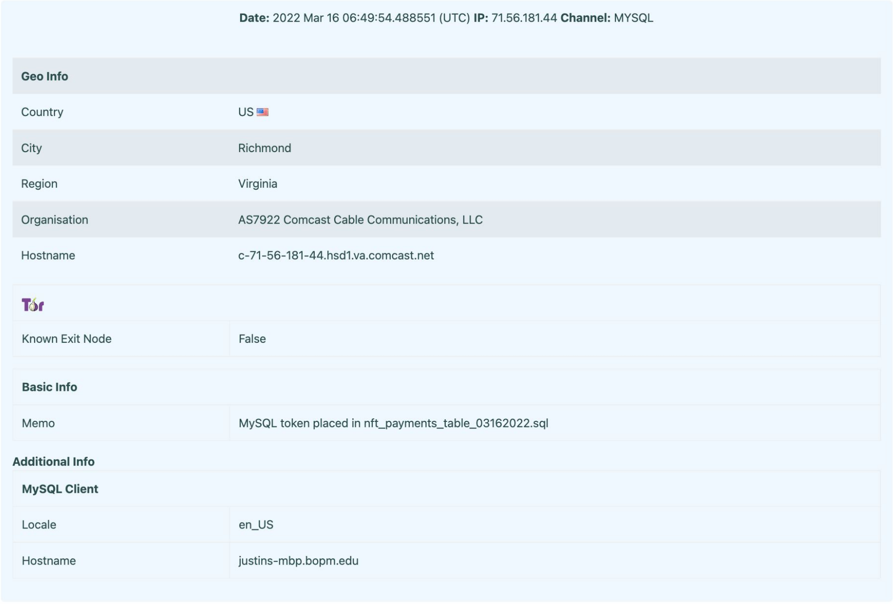
This Data Basically Is Asking To Be Dumped

They say data is digital gold and a juicy database may be filled with **valuable nuggets** like credit cards, social security numbers, and detailed financial history that could **ruin an organization if exposed**.

Let’s go ahead and ruin their day instead by serving up an ostensibly genuine goldmine with a useless pile of nothing.



```
mysql -uroot -p test < nft_payments_table_03162022.sql
 INSERT INTO `dw_update` VALUES (1,1,'at.dockwork.system.service.
 DataSourceService.existsFieldInDatabaseTable(connection,
 \'dw_text\', \'english\')','',1,'2018-02-07 00:35:55','\0','init
 dw_text.text_en','SOH','2018-02-07 00:35:58','2018-02-07 00:35:58',
 '','update dw_text set text_en = english','update dw_text set
 text_en = english',0,'condition is false','',''),(2,1,'at.
 dockwork.system.service.DataSourceService.
 existsFieldInDatabaseTable(connection, \'dw_text\', \'english\')
 ','',2,'2018-02-07 00:35:55','\0','drop dw_text.entlish','SOH',
 '2018-02-07 00:35:58','2018-02-07 00:35:58','','alter table
 dw_text drop column english','alter table dw_text drop column
 english',0,'condition is false','',''),(3,1,'at.dockwork.
 system.service.DataSourceService.existsFieldInDatabaseTable
```



Date: 2022 Mar 16 06:49:54.488551 (UTC) **IP:** 71.56.181.44 **Channel:** MYSQL

Geo Info	
Country	US
City	Richmond
Region	Virginia
Organisation	AS7922 Comcast Cable Communications, LLC
Hostname	c-71-56-181-44.hsd1.va.comcast.net

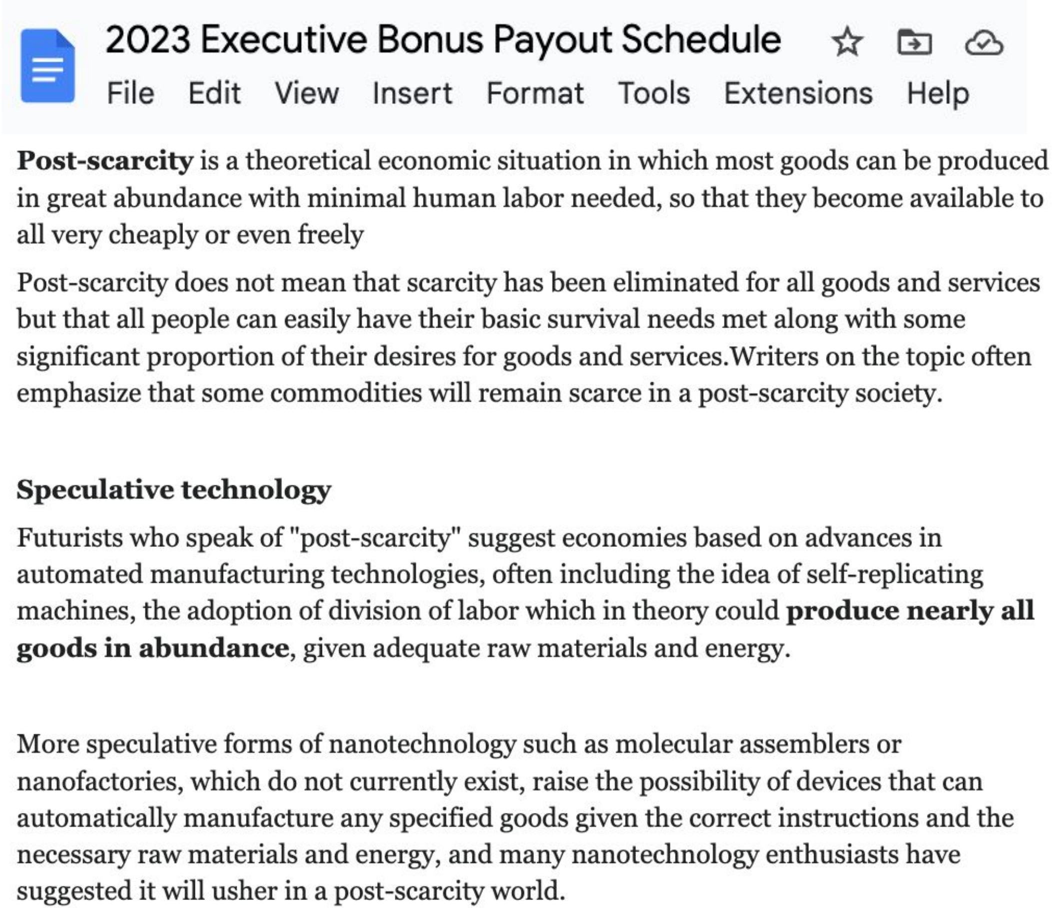
Tor	
Known Exit Node	False

Basic Info	
Memo	MySQL token placed in nft_payments_table_03162022.sql

Additional Info

MySQL Client	
Locale	en_US
Hostname	justins-mbp.bopm.edu

What If...Conspiracy Theories Are Conspiracy Realities



2023 Executive Bonus Payout Schedule

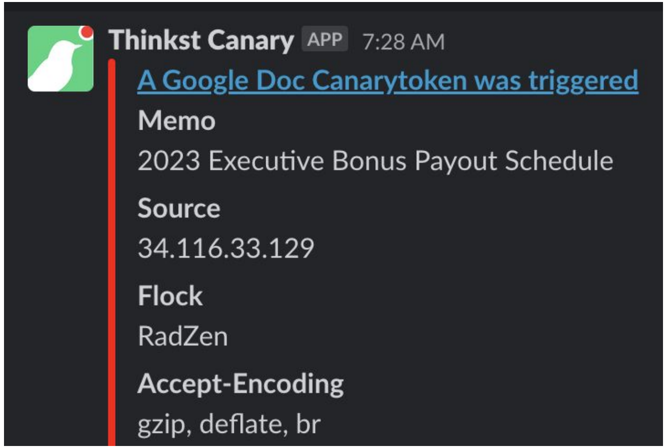
Post-scarcity is a theoretical economic situation in which most goods can be produced in great abundance with minimal human labor needed, so that they become available to all very cheaply or even freely

Post-scarcity does not mean that scarcity has been eliminated for all goods and services but that all people can easily have their basic survival needs met along with some significant proportion of their desires for goods and services.Writers on the topic often emphasize that some commodities will remain scarce in a post-scarcity society.

Speculative technology

Futurists who speak of "post-scarcity" suggest economies based on advances in automated manufacturing technologies, often including the idea of self-replicating machines, the adoption of division of labor which in theory could **produce nearly all goods in abundance**, given adequate raw materials and energy.

More speculative forms of nanotechnology such as molecular assemblers or nanofactories, which do not currently exist, raise the possibility of devices that can automatically manufacture any specified goods given the correct instructions and the necessary raw materials and energy, and many nanotechnology enthusiasts have suggested it will usher in a post-scarcity world.



Thinkst Canary APP 7:28 AM

A Google Doc Canarytoken was triggered

Memo
2023 Executive Bonus Payout Schedule

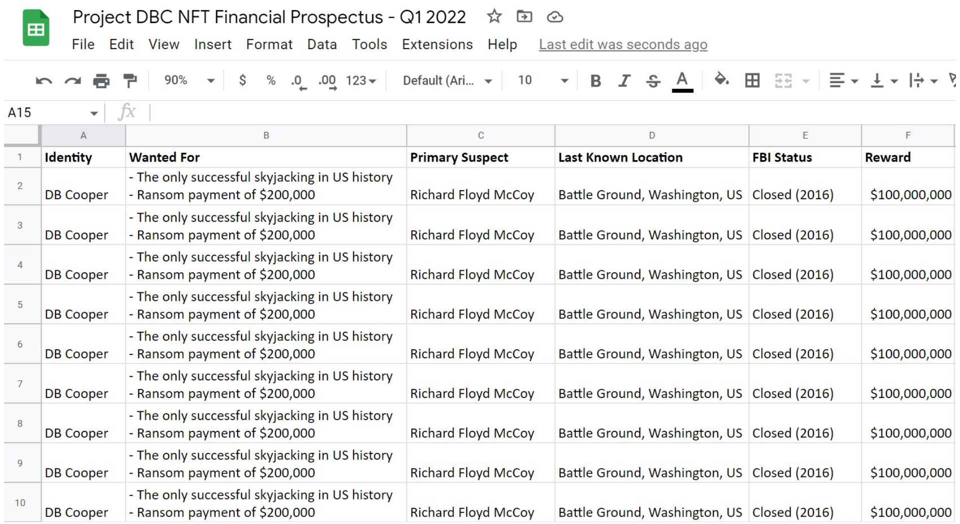
Source
34.116.33.129

Flock
RadZen

Accept-Encoding
gzip, deflate, br

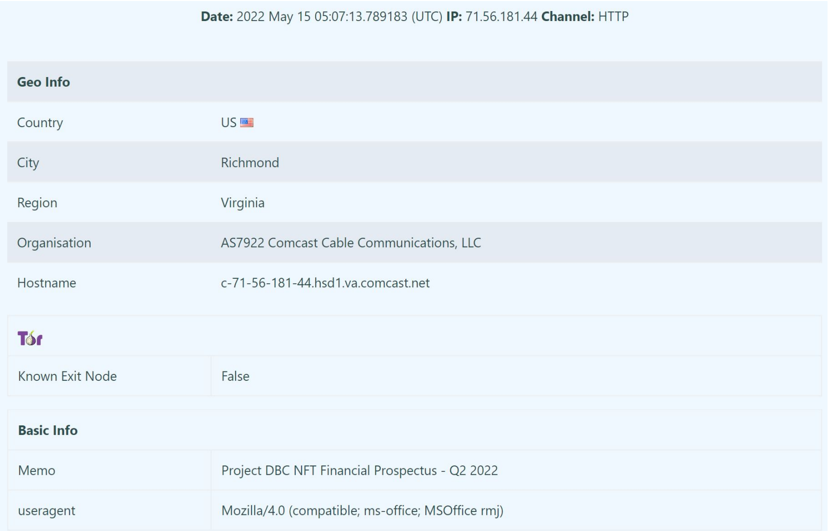
Spread Some Bullish Sheets

It’s hard to resist the urge to look at a company’s financials and it’s hard to resist the urge to drive nefarious people insane.



Project DBC NFT Financial Prospectus - Q1 2022

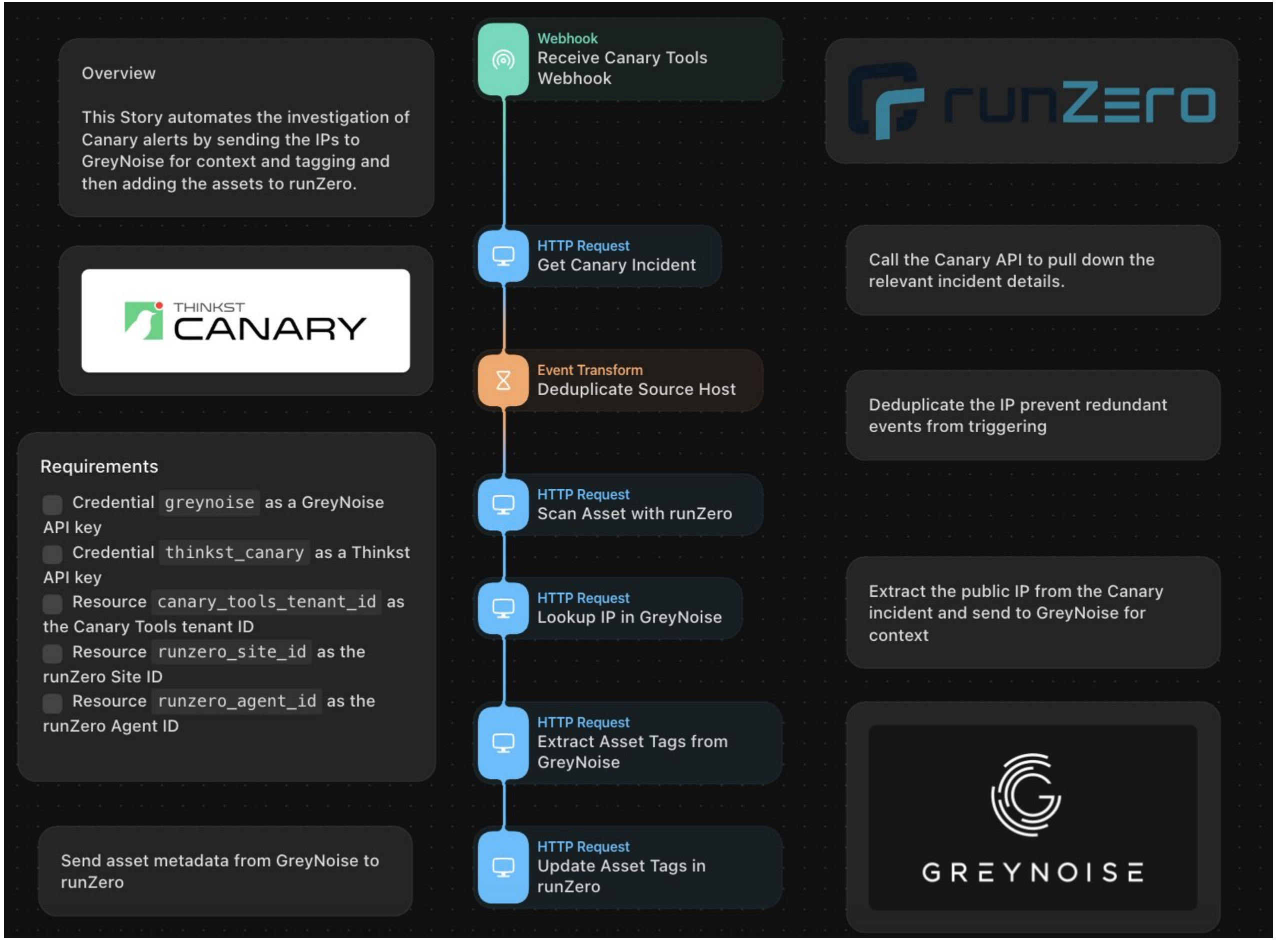
Identity	Wanted For	Primary Suspect	Last Known Location	FBI Status	Reward
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000
DB Cooper	- The only successful skyjacking in US history - Ransom payment of $200,000	Richard Floyd McCoy	Battle Ground, Washington, US	Closed (2016)	$100,000,000



Date: 2022 May 15 05:07:13.789183 (UTC) **IP:** 71.56.181.44 **Channel:** HTTP

Geo Info	
Country	US
City	Richmond
Region	Virginia
Organisation	AS7922 Comcast Cable Communications, LLC
Hostname	c-71-56-181-44.hsd1.va.comcast.net
Tor	
Known Exit Node	False
Basic Info	
Memo	Project DBC NFT Financial Prospectus - Q2 2022
useragent	Mozilla/4.0 (compatible; ms-office; MSOffice rmj)

It's Tines To Put It All Together



Overview

This Story automates the investigation of Canary alerts by sending the IPs to GreyNoise for context and tagging and then adding the assets to runZero.

Requirements

- □ Credential `greynoise` as a GreyNoise API key
- □ Credential `thinkst_canary` as a Thinkst API key
- □ Resource `canary_tools_tenant_id` as the Canary Tools tenant ID
- □ Resource `runzero_site_id` as the runZero Site ID
- □ Resource `runzero_agent_id` as the runZero Agent ID

Send asset metadata from GreyNoise to runZero

Webhook
Receive Canary Tools Webhook

HTTP Request
Get Canary Incident

Event Transform
Deduplicate Source Host

HTTP Request
Scan Asset with runZero

HTTP Request
Lookup IP in GreyNoise

HTTP Request
Extract Asset Tags from GreyNoise

HTTP Request
Update Asset Tags in runZero

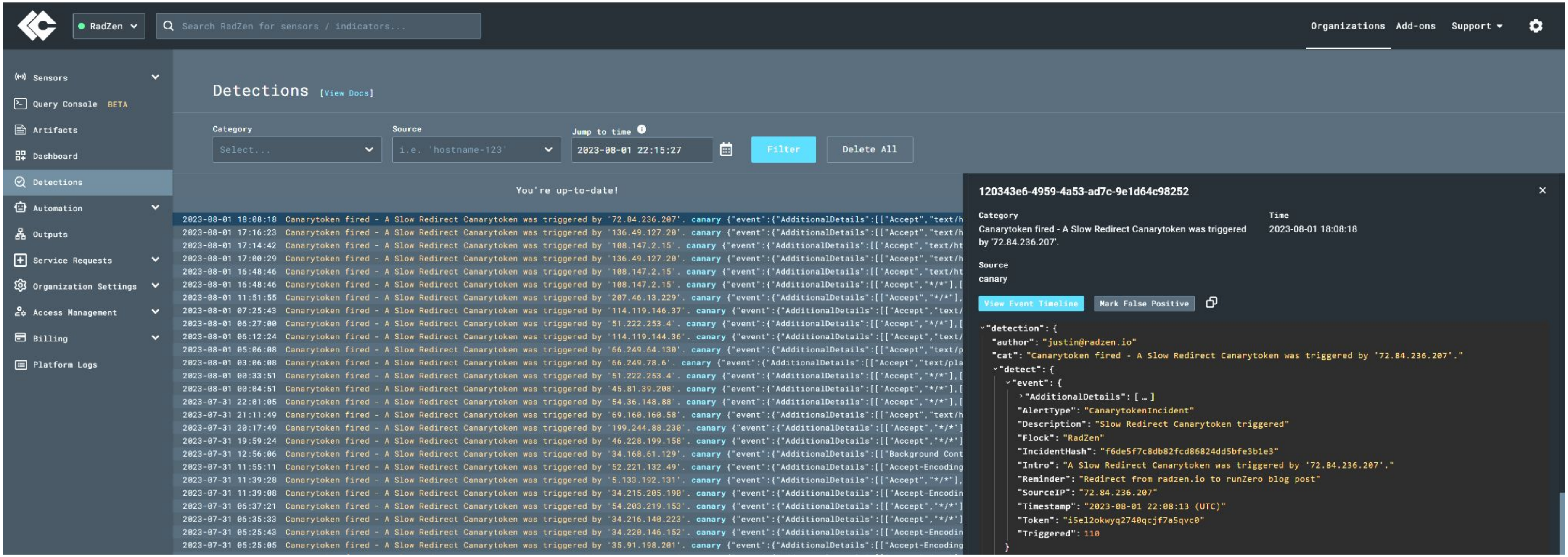
Call the Canary API to pull down the relevant incident details.

Deduplicate the IP prevent redundant events from triggering

Extract the public IP from the Canary incident and send to GreyNoise for context

Adversary Is Here, Loud and Clear

LimaCharlie is a comprehensive security operations platform that can ingest Canary events and build a detailed detection timeline for forensics, correlation, and context. You need only look here to understand just how screwed our adversary is.



Detections

Category: Select...
Source: i.e. 'hostname-123'
Jump to time: 2023-08-01 22:15:27

You're up-to-date!

```
2023-08-01 18:08:18  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '72.84.236.207'. canary {"event":{"AdditionalDetails":[["Accept","text/h
2023-08-01 17:16:23  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '136.49.127.20'. canary {"event":{"AdditionalDetails":[["Accept","text/h
2023-08-01 17:14:42  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '108.147.2.15'. canary {"event":{"AdditionalDetails":[["Accept","text/ht
2023-08-01 17:00:29  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '136.49.127.20'. canary {"event":{"AdditionalDetails":[["Accept","text/h
2023-08-01 16:48:46  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '108.147.2.15'. canary {"event":{"AdditionalDetails":[["Accept","text/ht
2023-08-01 16:48:46  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '108.147.2.15'. canary {"event":{"AdditionalDetails":[["Accept","*/*"],[
2023-08-01 11:51:55  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '207.46.13.229'. canary {"event":{"AdditionalDetails":[["Accept","*/*"],
2023-08-01 07:25:43  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '114.119.146.37'. canary {"event":{"AdditionalDetails":[["Accept","text/
2023-08-01 06:27:00  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '51.222.253.4'. canary {"event":{"AdditionalDetails":[["Accept","*/*"],[
2023-08-01 06:12:24  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '114.119.144.36'. canary {"event":{"AdditionalDetails":[["Accept","text/
2023-08-01 05:06:08  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '66.249.64.130'. canary {"event":{"AdditionalDetails":[["Accept","text/p
2023-08-01 03:06:08  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '66.249.78.6'. canary {"event":{"AdditionalDetails":[["Accept","text/pla
2023-08-01 00:33:51  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '51.222.253.4'. canary {"event":{"AdditionalDetails":[["Accept","*/*"],[
2023-08-01 00:04:51  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '45.81.39.208'. canary {"event":{"AdditionalDetails":[["Accept","*/*"],[
2023-07-31 22:01:05  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '54.36.148.88'. canary {"event":{"AdditionalDetails":[["Accept","*/*"],[
2023-07-31 21:11:49  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '69.160.160.58'. canary {"event":{"AdditionalDetails":[["Accept","text/h
2023-07-31 20:17:49  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '199.244.88.230'. canary {"event":{"AdditionalDetails":[["Accept","*/*"]
2023-07-31 19:59:24  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '46.228.199.158'. canary {"event":{"AdditionalDetails":[["Accept","*/*"]
2023-07-31 12:56:06  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '34.168.61.129'. canary {"event":{"AdditionalDetails":[["Background Cont
2023-07-31 11:55:11  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '52.221.132.49'. canary {"event":{"AdditionalDetails":[["Accept-Encoding
2023-07-31 11:39:28  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '5.133.192.131'. canary {"event":{"AdditionalDetails":[["Accept","*/*"],
2023-07-31 11:39:08  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '34.215.205.190'. canary {"event":{"AdditionalDetails":[["Accept-Encodin
2023-07-31 06:37:21  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '54.203.219.153'. canary {"event":{"AdditionalDetails":[["Accept","*/*"]
2023-07-31 06:35:33  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '34.216.140.223'. canary {"event":{"AdditionalDetails":[["Accept","*/*"]
2023-07-31 05:25:43  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '34.220.146.152'. canary {"event":{"AdditionalDetails":[["Accept-Encodin
2023-07-31 05:25:05  Canarytoken fired - A Slow Redirect Canarytoken was triggered by '35.91.198.201'. canary {"event":{"AdditionalDetails":[["Accept-Encoding
```

120343e6-4959-4a53-ad7c-9e1d64c98252

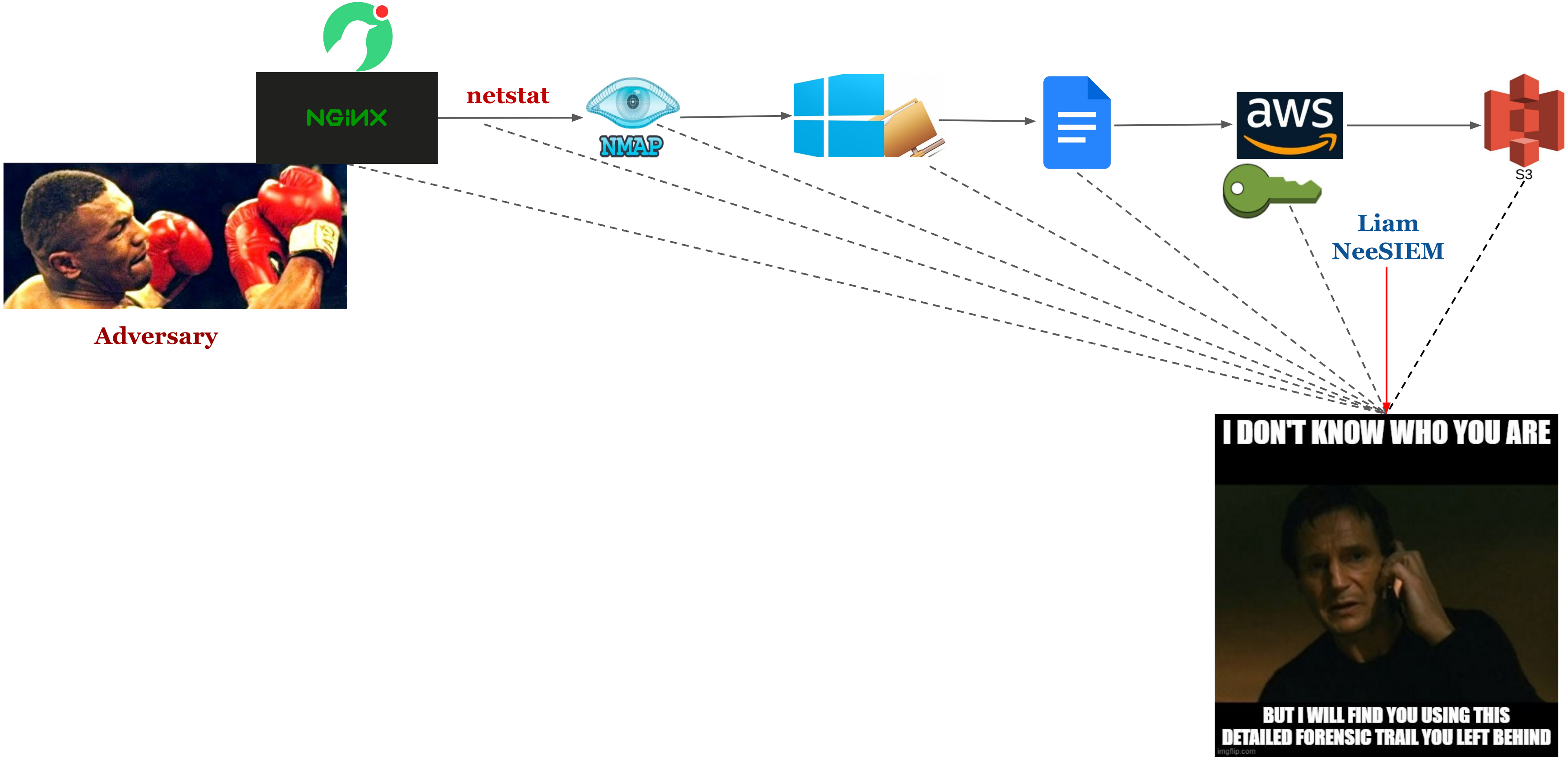
Category: Canarytoken fired - A Slow Redirect Canarytoken was triggered by '72.84.236.207'.

Time: 2023-08-01 18:08:18

Source: canary

```
"detection": {
  "author": "justin@radzen.io"
  "cat": "Canarytoken fired - A Slow Redirect Canarytoken was triggered by '72.84.236.207'."
  "detect": {
    "event": {
      "AdditionalDetails": [ … ]
      "AlertType": "CanarytokenIncident"
      "Description": "Slow Redirect Canarytoken triggered"
      "Flock": "RadZen"
      "IncidentHash": "f6de5f7c8db82fcd86824dd5bfe3b1e3"
      "Intro": "A Slow Redirect Canarytoken was triggered by '72.84.236.207'."
      "Reminder": "Redirect from radzen.io to runZero blog post"
      "SourceIP": "72.84.236.207"
      "Timestamp": "2023-08-01 22:08:13 (UTC)"
      "Token": "i5el2okwyq2740qcjf7a5qvc0"
      "Triggered": 110
    }
```

Better Breach Detection With Deception Inception



netstat

Adversary

Liam NeeSIEM

NGINX
NMAP
aws
S3
I DON'T KNOW WHO YOU ARE
BUT I WILL FIND YOU USING THIS DETAILED FORENSIC TRAIL YOU LEFT BEHIND
imgflip.com

And That's A Wrap!

Thinkst Canary: https://canary.tools/

Free Canarytokens: https://canarytokens.org/

GreyNoise: https://www.greynoise.io

RunZero: https://www.runzero.com

Security Saves Money (And Drives Business!): https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Big and Bad: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

2023 IBM Breach Report: https://www.ibm.com/security/data-breach

Half Man Half Myth: https://www.fbi.gov/history/famous-cases/db-cooper-hijacking

Free Your Mind:
https://www.npr.org/2019/09/09/758989641/the-cias-secret-quest-for-mind-control-torture-lsd-and-a-poisoner-in-chief

Tines: https://www.tines.com/story-library/1117240/check-thinkst-canary-alerts-in-greynoise-and-record-in-runzero

Lima Charlie: https://limacharlie.io/