Tor: DarkNet OpSec by a Veteran DarkNet Vendor & the Hacker Mentality





Hello!

I am Sam Bent

aka DoingFedTime

aka 12189-082

aka 2happytimes2

aka Killab

My Day Job, My night job

Day Job @ a Software Company that integrates with Student Information Systems

My employer condones nothing in this talk, and has nothing to do with it.

I am the Technical Communications Operations Liaison aka the guy who writes the "man" pages.

Night Job @ DoingFedTime

I bash the BOP, federal government, and LE's low hanging fruit arrests that they get so proud of.

I write books, and do a lot of social marketing while learning about SEO, and helping people deal with federal indictments and loved ones who's families are in federal prison, or headed there.

More info about me at https://www.doingfedtime.com/about or on twitter @doingfedtime, most active on facebook, as DoingFedTime.

Feel free to email me at ksllc27@gmail.com for business inquiries, or reservesteel9@gmail.com for other inquiries.

I have worked for a few DNMs - as staff dong disputes and/or PR.



Title	Username	UR
PGP Market, mOD Liberta…	LibertasModerator	
AeroModeratorPGP	AeroModerator	
mail.com	hghghkgearwa	mai
mail.com	decorman	
OlympusModerator -pgp	OlympusModerator	
onion email	2happytimes@tt3j…	tt3j
PGP	2happytimes@tt3j…	
PGP	adam@none.com	
PGP for BlueBios	BlueBios	
PGP libertas	LibertasOfficial	
protonmail.com	2happytimes2	http
rebus PGP key	Rebus admin	
torbox	Tracer	http:
torbox - for cashout - gold	fanofgold	http:



acctstolenwtf123	sourcery
aero forums	AeroVendor9000
aero forums	AeroVendor9000
aero market vendor	AeroVendor9000
coinb.in tutorial	AeroVendor9000…
dread	2happytimes2
hansa	2happytimes
libertas	2happytimes2
mail.com	kirk223@mail.com
pgp key for AeroVendor9000	
protonmail	2happytimes2
Sample Entry	User Name
Sample Entry #2	Michael321
traderoute	TechnicalSupportT…



Title	Username
admin Reddit Libertas	LibertasDNM
aero	2happytimes2
aero mod	AeroModerator
agora reloaded	2happytimes2
coinb.in	2happytimes@tt3j…
coinbin	Sexygurl24@tt3j2…
new coinb.in	2happytimes2@no…
nov 19 DD account	asdf@dfergewgSD…
reddit	TradeRouteModer…
reddit	QEywvcB9utqScJN6
reddit AeroMod PGP	AeroMarketMod - …
reddit AeroPR	AeroMarketMod
reddit olympus	OlympusPR
rsclub	2happytimes2
TR MOD FORUM	BlueBios
traderoute	sexygurl24
traderoute	2happytimes2
traderoute forum	2happytimes2
traderoutestaff	bluebios

My Objective

- Show a different perspective on the Darknet, that goes beyond academic.
- Show Darknet subculture through the eyes of a hacker.
- Show a real world example of the hacker mindset applied to real world scenarios that are less common in the scene.
- Have an open discussion about the Darknet, and move past the propaganda, and idiocy that we see in abundance on sites like youtube.
- Show the adaptability of a hacker in different hostile environments both virtually and IRL.
- Show the trajectory that the mindset can take when applied, for the wrong reasons.



1. Hacking Subculture => DarkNet Subculture

Subculture cousins.

Background

Distinct Similarities include:

- Both are paranoid for a reason.
- Both prioritize anonymity, secrecy, intellectual dominance, have high levels adaptability, and typically prefer tech over social interactions.
- Both have a learning curve – DarkNet subculture though has been around for less time, and has less documentation on it.

Paths of learning: Hacker vs DNV

Hacker

- Starting off, you have no adversaries.
- Learn everything contained in the Penetration Testing Standards, and how to do it.
- Forums, man pages, vuln hub, phrack, packetstomsecurity, books, all hacking cons, irc, etc.

DNV

- Starting off, your adversaries are: pissed off customers, every federal agency foreign and domestic, all LE
- Know about Infosec and IT, as well as a hacker does (or hire someone who does, and trust them).
- Forums, recent exploit announcements, packetstomsecurity, Darknet News live, dark.fail, and dread, etc.



2. Recon / Information Gathering

First Steps. A lurker is born.

“Time spent in reconnaissance is seldom wasted.”

- John Marsden

Know thy enemy…

- In “Ghost in the wires” Kevin Mitnick uses SE to get into the NCIC.
- This approach of understanding and using the enemies resources can be applied to becoming a DNV when discussing things like logistics:
- The United States Postal Inspector – top cop for the Post office.
- He/she too has a manual.
- Locating and reading this let’s you know how they operate.

Government of the District of Columbia

Public Safety Bulletin

Homeland Security and Emergency Management Agency

GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

SUSPICIOUS PACKAGE INDICATORS



WHAT TO DO

1. Leave the package where you found it
2. Clear the immediate area
3. Call 911 & follow your building's security procedures
4. Anyone who handled the package should wash their hands with soap and water
5. Isolate those exposed to the package
6. Shut down equipment and HVAC systems
7. Direct yourself and others from the area
8. If possible, document the package's location and any written details for first responders

You might be suspect if:

- You use to much tape on your package
- You hand write the label
- You don't use the official USPS box
- You use a fake recipient address or name
- You use a fake return address or name.
- You do not live in that town/or the employees don't know you.
- ALL of these can be avoided or set up in a way that they are not issues.
- FOR EXAMPLE…

Moral dilemma for a drug trafficker

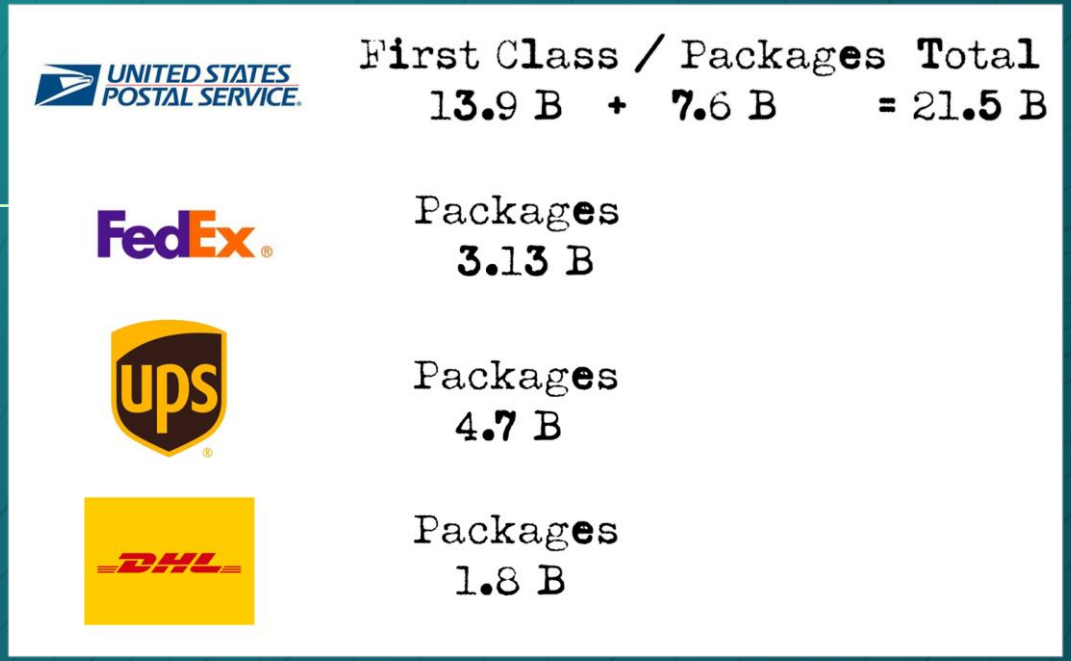
- I needed a real return address.
- Did not want to get the “average” working person in trouble.
- Address needs to have a real person, and a real address to not attract the USPI.
- Needed a database of people that I did not care about, who in my opinion deserved to get screwed up OR it did not matter to me that they did catch a case.
- How would you locate this info?


THE UNITED STATES DEPARTMENT of JUSTICE
SMART Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking
DRU SJODIN
NATIONAL SEX OFFENDER PUBLIC WEBSITE
HOME
SEARCH
SAFETY AND EDUCATION
ABOUT NSOPW
FAQS
ABOUT DRU
ESPAÑOL
SEARCH NSOPW
Search sex offender registries for all 50 states, The District of Columbia, U.S. Territories, and Indian Country.
Advanced Search
SEARCH BY NAME
First Name *
Last Name *
Name Search
SEARCH BY LOCATION
Address *
City/Town *
Alabama
1 Mile
Location Search



- Other services like DHL, UPS, etc can open a package at any time, for any reason.
- A warrant is required to open a USPS box/letter.

- Tons of locations near you, tor to door service in 3 days or less!
- Run by the federal government - not a private corporation.
- Turing the federal government into your personal drug mule is ironically safer than using the other services.



- Even if USPS COULD open any package, what are the odds they open mine?
- USPS ships more packages in general than any other carrier.
- Drug sniffing dogs are irrelevant as they cannot work 8 hour shifts.

- Typically your worst case scenario is a “Love Letter” from USPS.
- This letter says that “your package” is available come to our location to get it. This is what the feds use as “proof” that you ordered the pack.
- Solution: Throw your love letter away, consider the addy burnt.



"Controlled delivery" shall mean the technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons ...

- Controlled Deliveries suck.
- Countermeasures:
- NEVER sign for a package.
- Don't answer your door, you have no obligation to do so for Jehovah witnesses, police or mail men. Be wary of "deliveries" that do not come from USPS.
- If your worried, wait a day to open the package. If a device is in: this may cause the battery to die.
- Open it off site - may kill local transmission abilities.
- If your not sure walk away/deny it's yours.

When you have done well in your OpSec efforts: This is what it should look like.

DEPARTMENT OF HOMELAND SECURITY

HOMELAND SECURITY INVESTIGATIONS

REPORT OF INVESTIGATION

OFFICIAL USE ONLY | LAW ENFORCEMENT SENSITIVE

When asked about Sam BENT, the employees said that they had never seen him. They said BENT had called the East Burke Post Office last Christmas looking for a package that he thought was being detained in Miami, Florida. BENT told the employee that the package contained a computer part. The postal employees believe that BENT works with computer networks.

DISPOSITION: Pending further investigation.

Current Case Title	ROI Number	Date Approved
Investigation of "2Happytimes2"	NT13LR18NT0001-002	5/14/2018

This document is loaned to you for official use only and remains the property of the Department of Homeland Security. Any further request for disclosure of this document or information contained herein should be referred to HSI Headquarters together with a copy of the document.

Cultivating a Persona/Brand

- 2happytimes2 was born on Hansa.
- Contributed 5,000 posts on the forums in 1 month.
- Built a following prior to listing anything.
- Established Rapid Rapport and Trust, in a anonymous, hostile environment in 30 days.
- Advice on OpSec
- Explain and ask questions
- Call out scammers
- Offer genuine support
- Customer service can be > savings/pricing

Recon/Intelligence Gathering

Evasion of a multibillion dollar adversary - various federal agencies/governmental entities

History

- LE announcements on busted DNV – how they did it.
- Know thy enemy – investigating the investigators: Pacer
- Mandatory reading includes Kevin Mitnick books
- Attempt to locate things like USPS Inspector's manual.
- My OpSec Goal: Learn from the past.

Present

- Stay up-to-date with the latest news regarding exploits, vulnerabilities, and other aspects of technical security.
- Review current stories of LE busts to learn technical adaptations they have made, daily.
- Review bluetooth/wifi, and other local devices regularly.
- My OpSec goal: make the feds break the law.

Future

- Planning expansions
- Get postal supplies securely.
- Review changing landscape of crypto with no KYC options and built in tor by default like bisq.
- Review technological trends
- My OpSec Goal: Predict adversary's attacks.

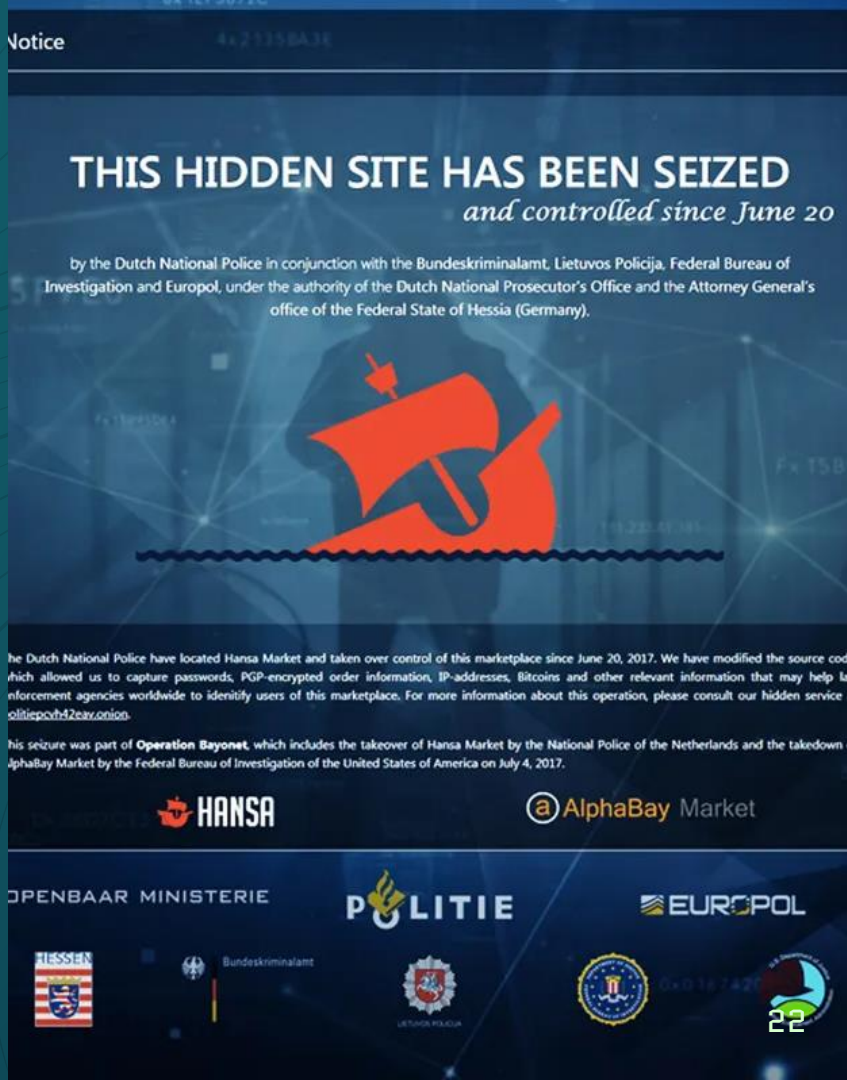
A picture is worth a thousand words, none good.

DNM's come and go.

Typically on their own.

Every once in a while, an admin screws up though and gives LE a fighting chance by fucking off proper opsec because they become complacent.

The rest of the time LE just does DDoS attacks.

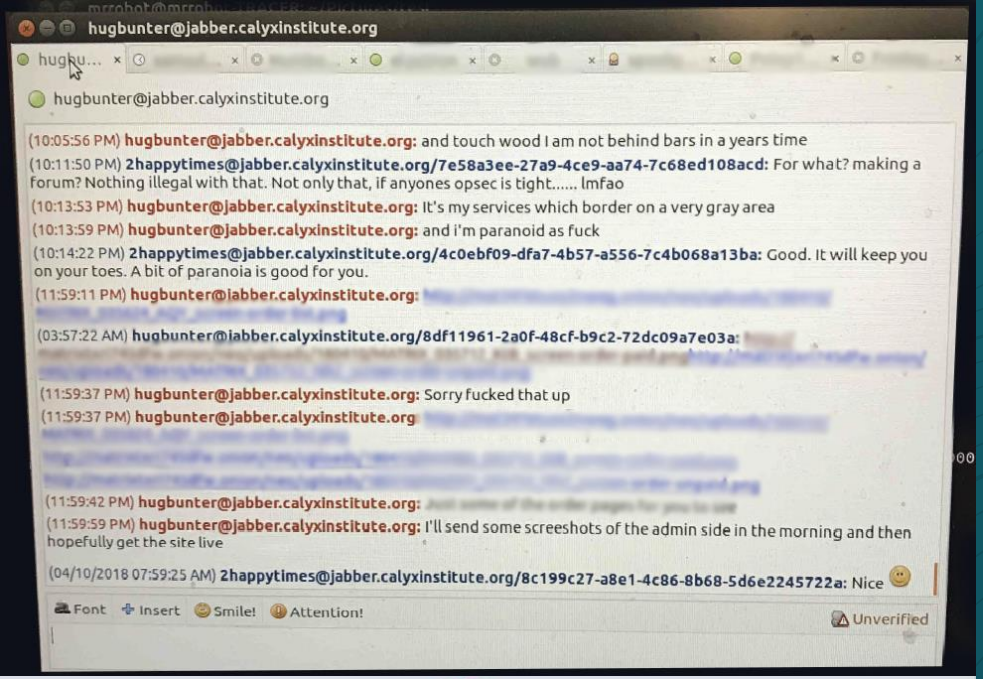


I have worked for a few DNMs - as staff dong disputes and/or PR.

Title	Username
admin Reddit Libertas	LibertasDNM
aero	2happytimes2
aero mod	AeroModerator
agora reloaded	2happytimes2
coinb.in	2happytimes@tt3j...
coinbin	Sexygurl24@tt3j2...
new coinb.in	2happytimes2@no...
nov 19 DD account	asdf@dfergewgSD...
reddit	TradeRouteModer...
reddit	QEywvcB9utqScJN6
reddit AeroMod PGP	AeroMarketMod - ...
reddit AeroPR	AeroMarketMod
reddit olympus	OlympusPR
rsclub	2happytimes2
TR MOD FORUM	BlueBios
traderoute	sexygurl24
traderoute	2happytimes2
traderoute forum	2happytimes2
traderoutestaff	bluebios

Title	Username	UR
PGP Market, mOD Liberta...	LibertasModerator	
AeroModeratorPGP	AeroModerator	
mail.com	hghghkgearwa	mai
mail.com	decorman	
OlympusModerator -pgp	OlympusModerator	
onion email	2happytimes@tt3j...	tt3j
PGP	2happytimes@tt3j...	
PGP	adam@none.com	
PGP for BlueBios	BlueBios	
PGP libertas	LibertasOfficial	
protonmail.com	2happytimes2	http
rebus PGP key	Rebus admin	
torbox	Tracer	http:
torbox - for cashout - gold	fanofgold	http:

acctstolenwtf123	sourcery
aero forums	AeroVendor9000
aero forums	AeroVendor9000
aero market vendor	AeroVendor9000
coinb.in tutorial	AeroVendor9000...
dread	2happytimes2
hansa	2happytimes
libertas	2happytimes2
mail.com	kirk223@mail.com
pgp key for AeroVendor9000	
protonmail	2happytimes2
Sample Entry	User Name
Sample Entry #2	Michael321
traderoute	TechnicalSupportT...





Finding a new home

- Working as PR for random DNM's you tend to meet interesting people, this was how I met, and started working with Hugbunter.
- He created Dread, my job was to manage it as an admin/global moderator.
- It exploded, as it became the new home for r/darknetmarkets.
- Today Dread is one of the largest forums on the Darknet, and one of the largest unofficial repos of information about the Darknet.



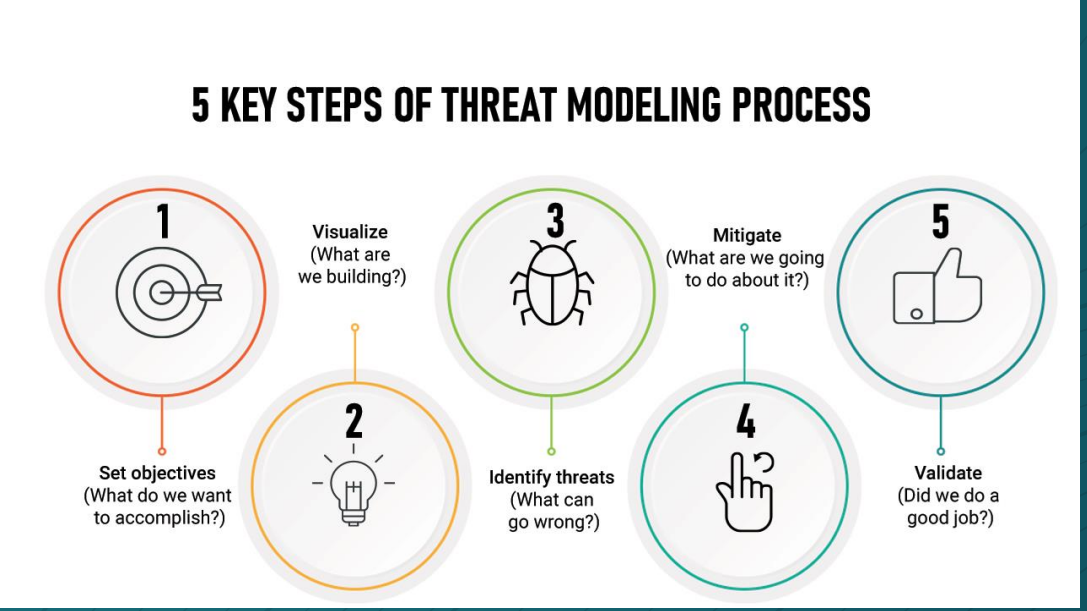
“To know your enemy, you must become your enemy.”

- Sun Tzu



3. Threat Modeling

The best laid schemes of mice and men...



1. Not get arrested.
2. A secure persona.
3. We can get arrested, if any mistakes are made.
4. Take all precautions including virtual and physical.
5. If we are not in federal custody, then yes.

- Attempt to map and set up responses to various situations that may occur.
- Plan for physical security, including a clean room to prevent traces of DNA.
- Know what your shipper considers a “suspicious package”, do the opposite.
- If an issue comes up, how will you deal with it?

Threat Modeling

Layout of specific potential threats

Physical

- DNA Evidence
- Nosy Neighbors
- Sloppy packaging
- Weak packaging
- Bluetooth/Wifi MITM attacks
- Trash
- Physical failsafes

Electronic

- Highest Sec. Settings in Tor, if using browser
- Whonix / qubes / Tails
- Strong encryption
- Digital failsafes
- Best practices
- Solid incident response plan
- Advanced Persistent Threat safeguards

Social

- Loose lips (sink ships)
- Linguistic analysis – “Yall” or “wicked”
- Secure communications platforms
- Lack of communication = communication

My Internet service – nonexistent.

- Don’t use your own internet service.
- I bought a Yagi, and used an internet connection a mile away, that I could see.
- I monitored the house with a telescope, watching for black vehicles, it was my “perimeter fence”.
- I drew my inspiration from Kevin Mitnick.



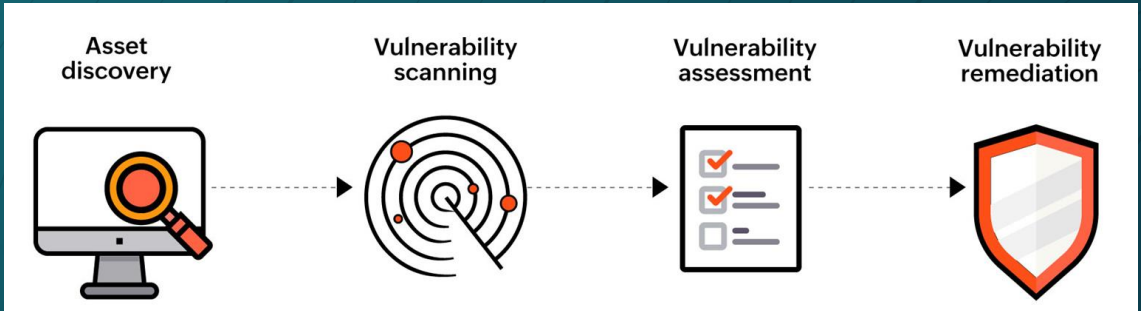


4. Vulnerability Analysis

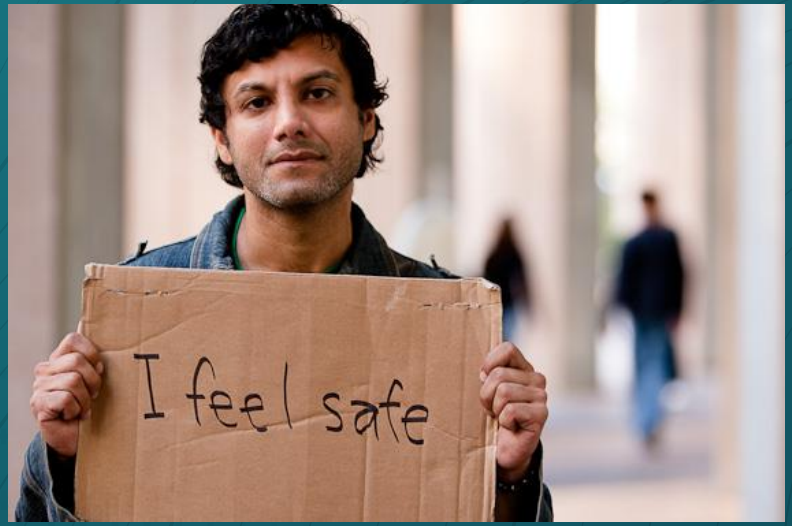
Review; Daily.

Are we on top of our OpSec?

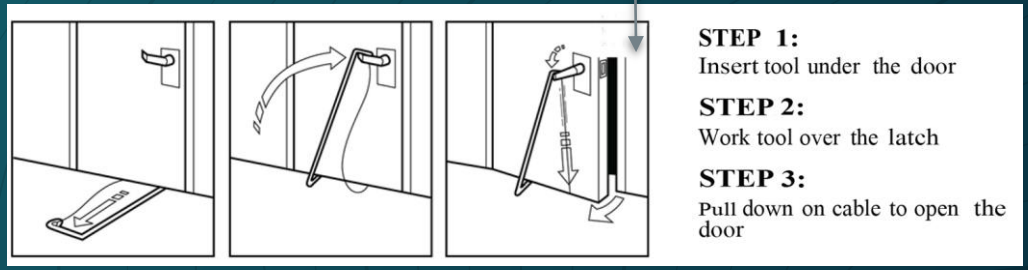
- Create a daily, weekly, monthly and quarterly checklist to keep your OpSec on point.
- List from least complex -> most complex tasks.
- Start simple: EXIF data scrubbing and other stupid things that will land you in prison.
- Test your threat modeling by simulating a real word issue and analyze your outcomes.



We all feel secure, until we evaluate…







Vulnerability Analysis

Where are you weak?

History

- What have DNV's traditionally screwed up? Was it out of stupidity, laziness or complacency?
- What OpSec mistakes have you made in the past?

Present

- Stick to your plan: religiously.
- Shut down shop (or go on vacation) as opposed to making a change you have not fully evaluated.
- Stay away from emotional decisions.
- Constantly reevaluate your position, and OpSec.

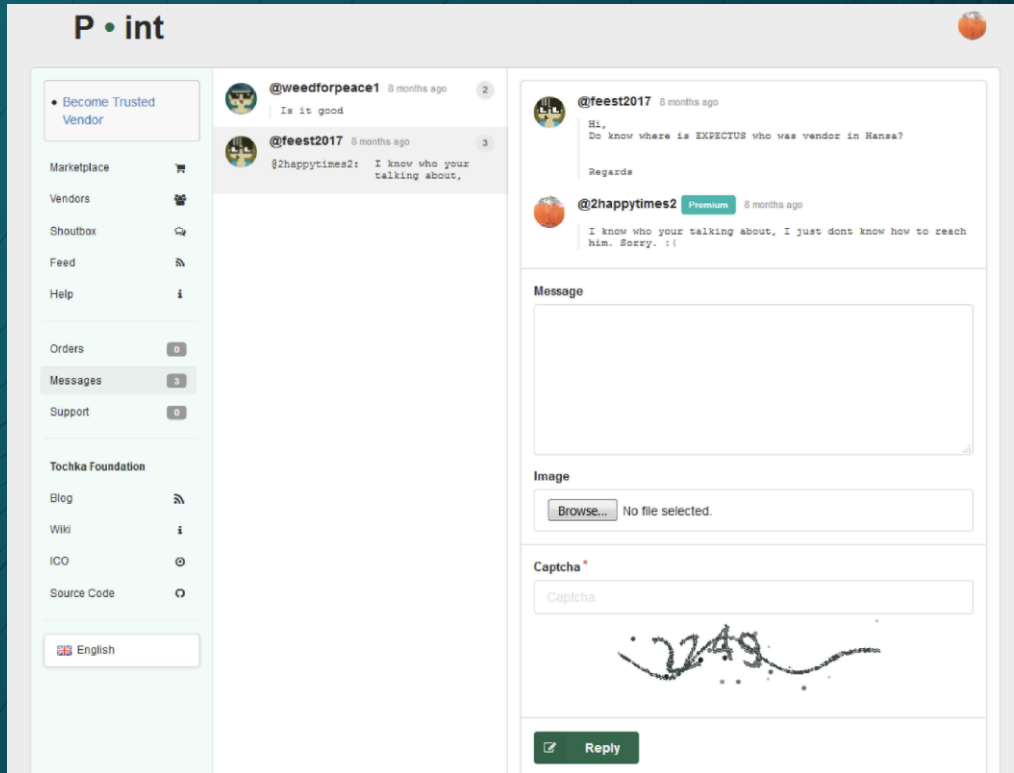
Future

- How long do you plan to do this for, set a cut off date, or an amount of money as a cut off.
- Reinvest into security.
- Avoid being the topic of a Defcon Panel.

Vulnerability Analysis

Avoid specific questions

- Answering general questions in regards to best practices of OpSec is fine.
- Answering what you know, or where someone else is should be considered carefully prior to the submission of an answer or avoided all together.
- Pay special attention to different ways of talking, look for abrupt changes in personality or mannerisms.
- Avoid the question all together, by asking your own question.



“Invincibility depends on one’s self; the enemy’s vulnerability on him.”

- Sun Tzu



5. Exploitation

Going Live.

It begins.

1. Dealing with customers and their questions.
2. Building OpSec into your T&C.
3. Don't fold on tracking numbers.
4. No one likes you, except for the people that do.
5. Remember, you live in a different world now, act accordingly.
6. Don't drink and type, it's more dangerous than operating a car.

- Change your PGP key as often as needed.
- When will do, change your vendor name, it will suck starting from scratch, but hitting the reboot button, is not a bad thing and good for security.

Exploitation

Making Money, and getting it.

Ingress

- Remember it's a job, and the biggest part of it is security.
- Have a plan for egress, prior to ingress.
- Good customer service is not a option, it's a mandate.

Egress

- Be smart about how you cash out.
- Cashing out with narcotics.
- Go hard, then quit.
- Keep good karma, don't exit scam, or selective scam.
- Remember, you are in this to make money, not friends.

Regress

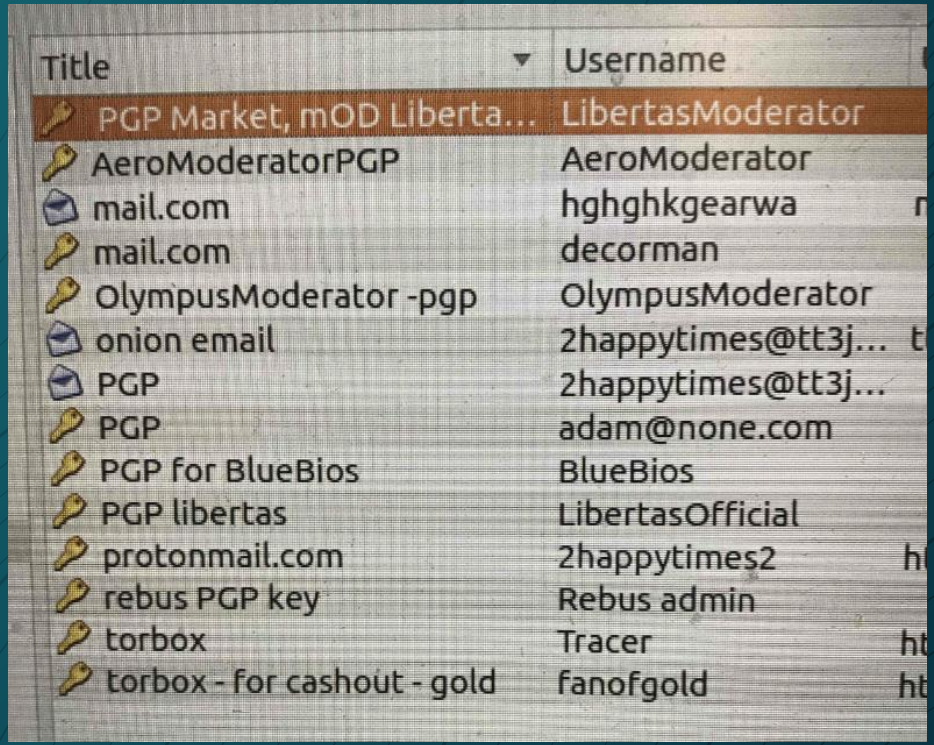
- Switch up your persona. It will cost, but is worth it.
- When refreshing your persona, make no references to prior personas, use a different PGP key.
- Tell no one even if you have dealt with them in the past.

Exploitation

Using one account to make another.

Once you start.

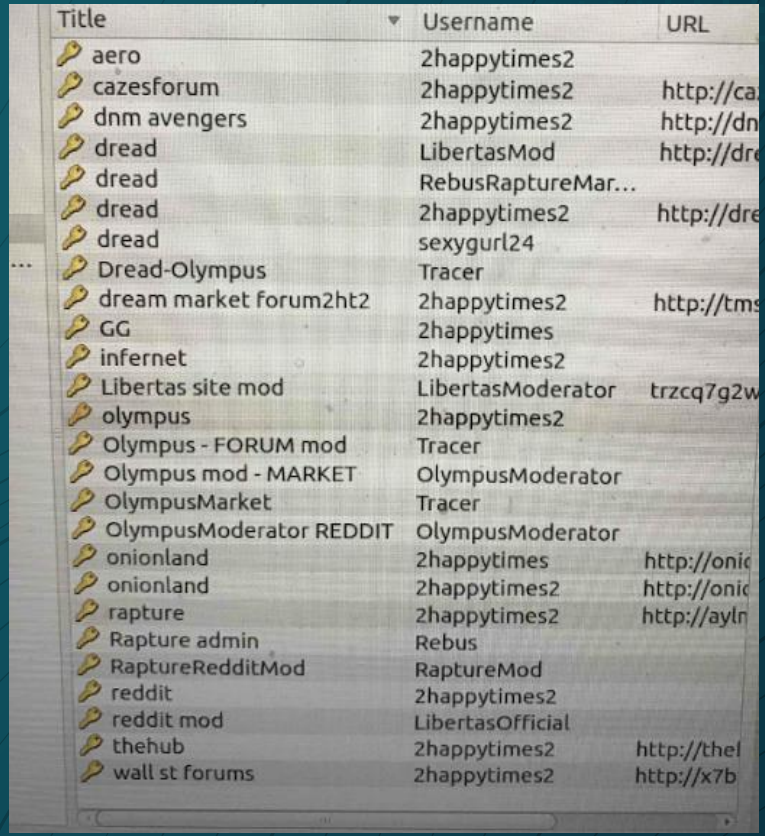
- The lack of reputable people, means opportunity.
- Getting a job working from a DNM is like getting a 9-5, it's mostly about references.
- Once, you have been a mod/admin on one site, and have a working knowledge of social engineering, getting second, and third jobs get significantly easier.



Exploitation

Community Expansion.

- DNM staff references come in the form of screenshots, reddit signed posts, and PGP keys.
- After a particular point, you are so ingrained into the culture and the community that much of the time you need not apply.
- Typical pay rates as a:
  moderator $2,000 - $5,000 per week
  PR (reddit/dread)$2,000 - $10,000 per week
  dispute admin $4,000 - $12,000 per week
  admin %. Most of the time this is automated.



Title	Username	URL
aero	2happytimes2	
cazesforum	2happytimes2	http://ca
dnm avengers	2happytimes2	http://dn
dread	LibertasMod	http://dr
dread	RebusRaptureMar...	
dread	2happytimes2	http://dre
dread	sexygurl24	
Dread-Olympus	Tracer	
dream market forum2ht2	2happytimes2	http://tms
GG	2happytimes	
infernet	2happytimes2	
Libertas site mod	LibertasModerator	trzcq7g2w
olympus	2happytimes2	
Olympus - FORUM mod	Tracer	
Olympus mod - MARKET	OlympusModerator	
OlympusMarket	Tracer	
OlympusModerator REDDIT	OlympusModerator	
onionland	2happytimes	http://onic
onionland	2happytimes2	http://onic
rapture	2happytimes2	http://ayln
Rapture admin	Rebus	
RaptureRedditMod	RaptureMod	
reddit	2happytimes2	
reddit mod	LibertasOfficial	
thehub	2happytimes2	http://thel
wall st forums	2happytimes2	http://x7b



“By means of these seven considerations I can forecast victory of defeat.”

- Sun Tzu



5. Post-Exploitation

When all is said and done.

Getting Out



- Bitcoing Tumblers suck
- Use BTC -> XMR -> BTC instead
- Local cash out methods
- What the feds hate the most about DNVs.
- If your indicted, the feds will lie, and break the law themselves.
- Facing a 200 year sentence, not really…
- The process of “retiring” and why I am glad I was busted.

Post-Exploitation

Retirement

- Switch up your persona. It will cost, but is worth it.
- When refreshing your persona, make no references to prior personas, use a different PGP key.
- Tell no one even if you have dealt with them in the past.
- It's important to know that you have just as much to worry about in retirement as you do while active, your OpSec will need to remain on point.
- There will be no clocking out anytime soon, at least not until the statute of limitations runs out.



Post-Exploitation

Operation Dark Gold

- Buying and selling BTC is legal.
- Used as a red herring for indicting individuals.
- The feds form of post-exploitation – figure out how to find people exchanging BTC for cash, then figure out how to indict them if their OpSec is to tight for them: if needed break their own laws.
- Get someone to rat in order to avoid nullification of their legal violation.



Post-Exploitation

Criminal Feds

- My OpSec was solid enough that the DHS Special agents had to break the law in order to actually catch me.
- I was granted a "franks hearing" because of this.

03/12/2019	39	SECOND REVISED NOTICE OF HEARING as to Sam Bent re: 22 MOTION to Suppress Evidence and MOTION for Franks Hearing. Hearing reset for 3/21/2019 at 1:30 PM in Rutland Courtroom before Chief Judge Geoffrey W. Crawford (time change only). (pjl) (Entered: 03/12/2019)
03/14/2019	40	MOTION to Produce *Subpoena Witnesses* and MOTION For Production of Documents by Sam Bent. (Attachments: # 1 Certificate of Service)(Greenlees, Stephanie). Motion relief added 3/15/2019 (jlh). (Entered: 03/14/2019)
03/18/2019	42	RESPONSE in Opposition to 40 MOTION to Produce *Subpoena Witnesses and*, MOTION for Production of Documents by USA as to Sam Bent. (Attachments: # 1 Exhibit 1)(Drescher, Michael) Text clarified on 3/20/2019 (jlh). (Entered: 03/18/2019)
03/20/2019	45	ORDER re 40 MOTION to Subpoena Witnesses and for Production of Documents as to Sam Bent. The court defers ruling on the motion to subpoena Agent Divigard and Sergeant Loan until after the conclusion of the Franks hearing now set for March 21, 2019. The court understands that Agent West will be available at the hearing. After hearing from counsel and from Agent West, the court will make a decision about whether a further hearing date and the attendance of the two additional witnesses is necessary. (This is a text–only Order.). Signed by Chief Judge Geoffrey W. Crawford on 3/20/2019. (jal) (Entered: 03/20/2019)
03/20/2019	46	PLEA AGREEMENT as to Sam Bent. (pjl) (Entered: 03/20/2019)

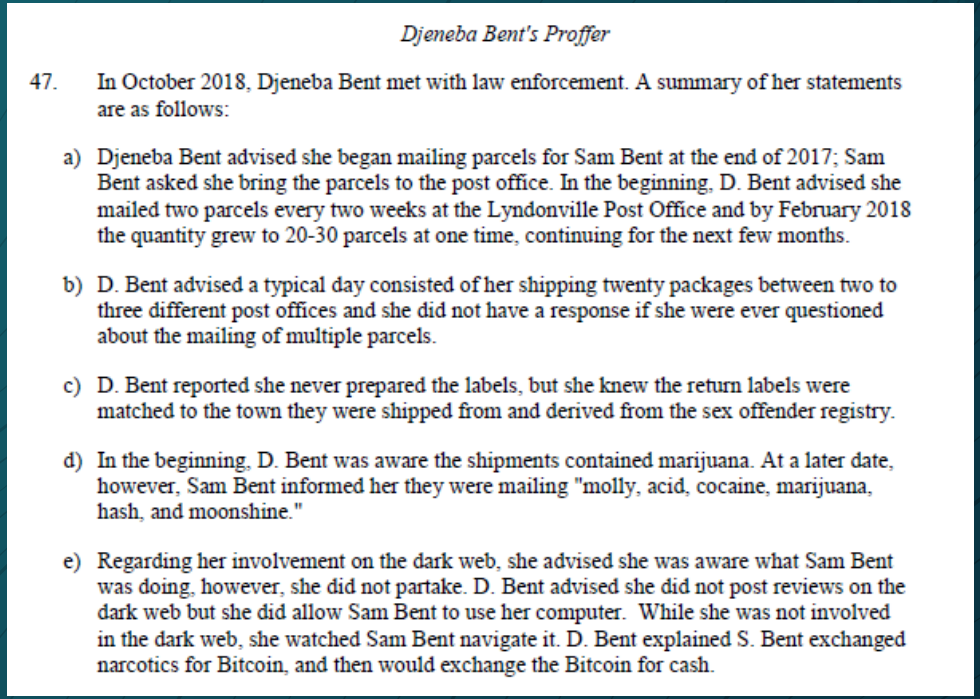
"A **Franks Hearing** is a court proceeding wherein the court is asked to determine if the police officer involved lied in obtaining a search warrant.".

- In my case ths was the USPI, who violated the law in opening a package he had no warrant for. The used this to raid my house, and eventually flip my cousin, using threats of incarceration.

Post-Exploitation

Which worked.

- Feds are masters at catching people, and lying.
- You can be charged with "ghost weight", even if you never got caught with drugs.
- Anyone can be charged with conspiracy, for any reason, including answering a phone.
- preponderance of the evidence vs beyond a reasonable doubt is very different.



Djeneba Bent's Proffer

47. In October 2018, Djeneba Bent met with law enforcement. A summary of her statements are as follows:

a) Djeneba Bent advised she began mailing parcels for Sam Bent at the end of 2017; Sam Bent asked she bring the parcels to the post office. In the beginning, D. Bent advised she mailed two parcels every two weeks at the Lyndonville Post Office and by February 2018 the quantity grew to 20-30 parcels at one time, continuing for the next few months.

b) D. Bent advised a typical day consisted of her shipping twenty packages between two to three different post offices and she did not have a response if she were ever questioned about the mailing of multiple parcels.

c) D. Bent reported she never prepared the labels, but she knew the return labels were matched to the town they were shipped from and derived from the sex offender registry.

d) In the beginning, D. Bent was aware the shipments contained marijuana. At a later date, however, Sam Bent informed her they were mailing "molly, acid, cocaine, marijuana, hash, and moonshine."

e) Regarding her involvement on the dark web, she advised she was aware what Sam Bent was doing, however, she did not partake. D. Bent advised she did not post reviews on the dark web but she did allow Sam Bent to use her computer. While she was not involved in the dark web, she watched Sam Bent navigate it. D. Bent explained S. Bent exchanged narcotics for Bitcoin, and then would exchange the Bitcoin for cash.

“If you wait by the river long enough, the bodies of your enemies will float by.”

- Sun Tzu



5. Reporting

It’s all documented.

Putting a hacker in federal prison

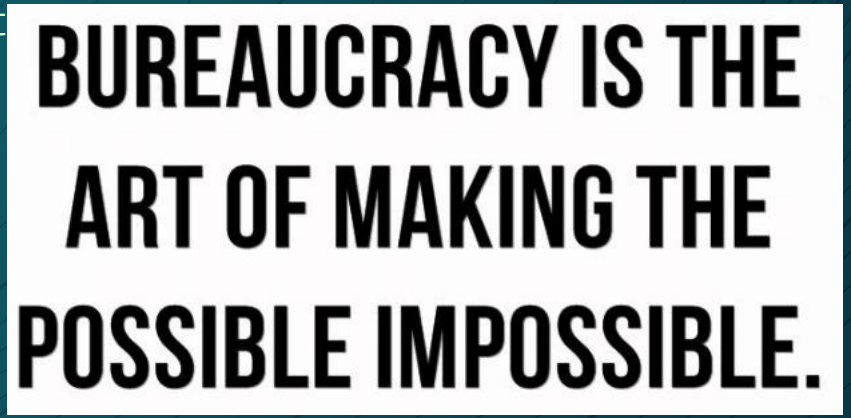


- Yet another hostile environment to conduct metaphorical privilege escalation out of.
- Know the rules both convict's inmates (unwritten), prison systems (BOP Program Statements), and courts (federal law, local court rules, etc).
- "Learn everything" mentality will always equate to power, including the power to get yourself out of prison or do other interesting magic.
- My sentence was 60 months with a max of 108. My judge let me out in 18, because I got myself out, with my own motion after studying federal law.

Reporting

Pen is mightier than the sword

- COVID-19 + federal prison + a hacker + self-taught law education = a vulnerability.
- A motion to the sentencing court + perfecting timing + the systems own failures = a successful exploit.
- BOP or Bureau of Prisons to people incarcerated by them stands for “Backwards on purpose”, because it is. They hate an educated convict or inmate. Your nmap in law is the understanding of it.



- Fighting a 100+ year old bureaucracy requires a ridiculous amount of determination, perseverance, and ruthlessness. For me it was in the form of a 200 page motion my own variation of a bruteforce attack.

Reporting

Hacking – a way of life, as well as a subculture





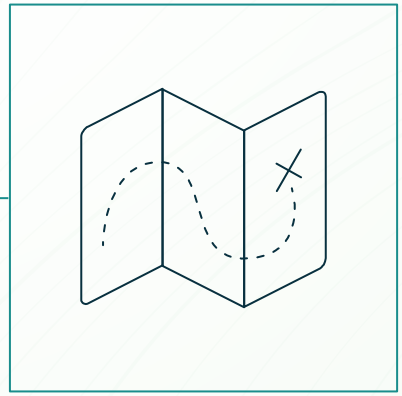


- Defcon's theme this year is "hacker homecoming" and for me that is especially true.
- Being a hacker and having the hacker mentality of never giving up and always learning, motivated me to get myself out of prison.
- In my opinion, one can only truly appreciate the culture of the Darknet, if taken in part with the culture of the hacking community. Both of which are like distant cousins, separate yet the same.

Reporting

cp hacker dnv

- I suggest nobody take this route to make money. It's a bad business model, even if you have perfect OpSec. Anyone watching this is already most likely intelligent enough to do something actually productive, with higher ROI and better longevity.
- Things can go bad, even if you don't fuck up!



Thanks!

Q&A