

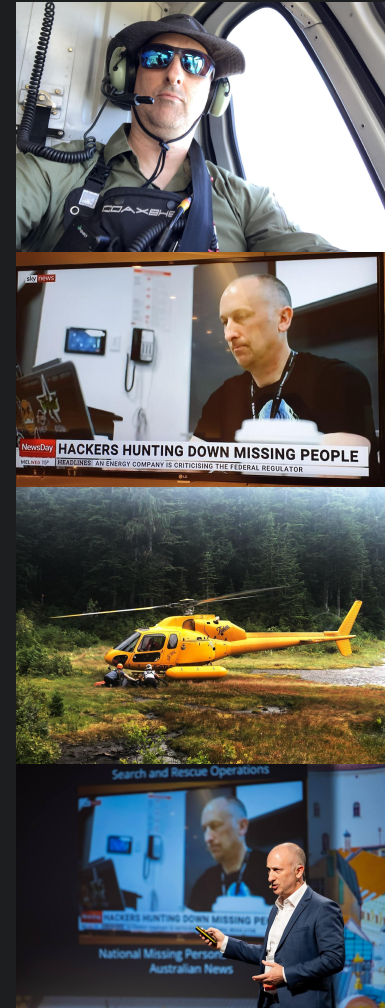
# OPSEC

## The Discipline of the Grey Man

Presented by: Robert Sell  
[robert.sell@tracelabs.org](mailto:robert.sell@tracelabs.org)

# Introductions

- Founder/President of Trace Labs
  - **OpSec:** Non theoretical OSINT CTFs: human trafficking
- Search Rescue
  - Team Leader, Marine Rescue Technician, Tracker
  - **OpSec:** Closed coms, Need to know, chain of command, specific OpSec training
- Information Technology/Security – Corporate Day Job
  - CISSP & CISM certified, daily Global Operations
  - 3rd place in SE Village CTF at Defcon Vegas (twice)
  - **OpSec:** Extremely closed coms, coded projects, global exposure to great variety of organizations.



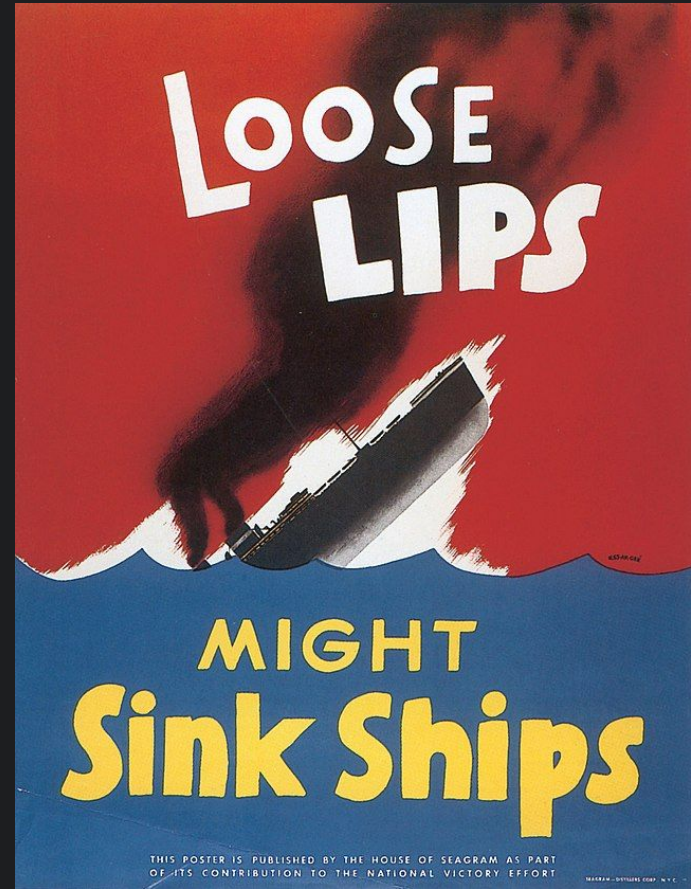
# Disclaimer

- None of the opinions or details presented here are in any way representative of any employers (or any other entity I might participate in) from my past, present or future.
- All details presented here are for lawful use only.
  - Not advocating anyone violate any community standards re sock puppets
- All information presented here is categorized as Public – TLP: White
- Rapidly changing state (ie sock puppets) - What works today, may not work tomorrow
- OpSec from a Trace Labs perspective - Not a detailed OpSec for Red Teams talk

# What is OpSec?

## Industry Definitions:

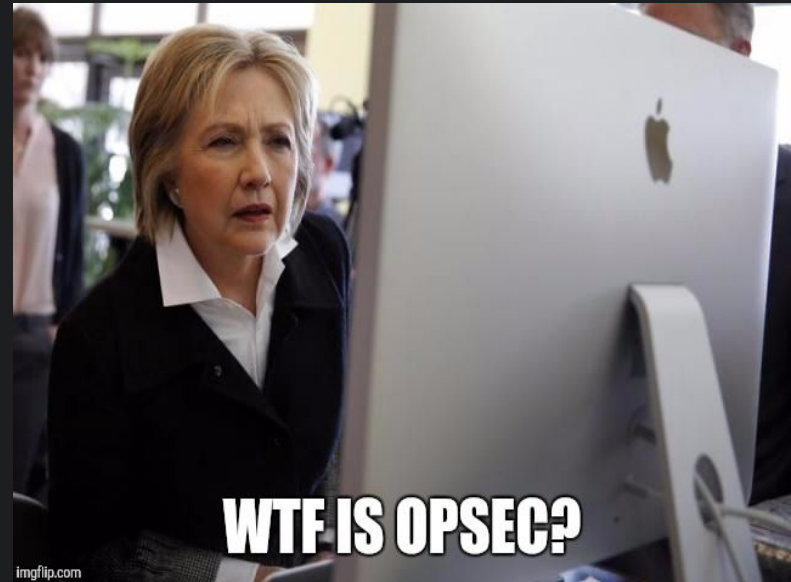
1. "The process or doctrine of *denying an adversary information* that could compromise the secrecy and/or the completion of a mission."
2. "Operational security (OPSEC) is a security and risk management process that *prevents sensitive information from getting into the wrong hands*. Another OPSEC meaning is a process that *identifies seemingly innocuous actions* that could inadvertently reveal critical or sensitive data to a cyber criminal."



# What is OpSec?

## My Definition (perhaps better?):

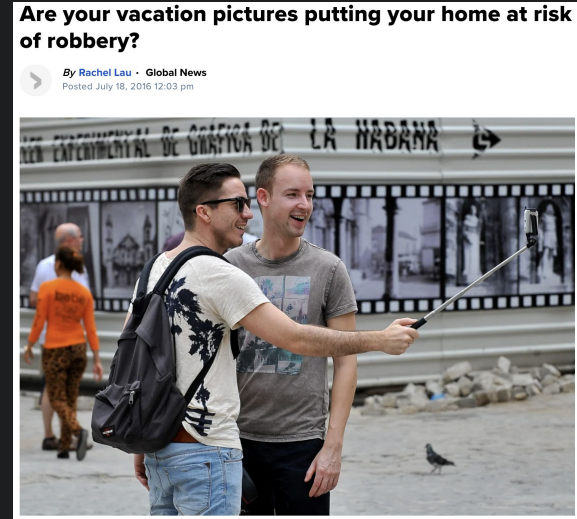
1. Ensuring only specific information is shared with specific audiences.
2. Not only restrict what information is being distributed, but understand what actions will be taken by adversaries after consuming that information.
3. Therefore, not only do we know what information is being acquired, but we also understand how this will modify adversary behaviors.



# Why care about OpSec?

## What can happen from poor OpSec?

- **Burnt:** Target is alerted to your intentions and/or true identity
- **Compromised Operation:** Increased cost, increased risk, wasted time, damaged reputation, etc
- **Liability:** Third party (not necessarily target) acquires your critical data (ie red team infrastructure)
- **Interference:** criminal investigation, other operations
- **Tables Turned:** The hunted now can become the hunter
- **Personal Risk:** employment, home break in, blackmail, jail, injury/death, friends/family



Stratfor had **warned on 28 October** that there could be disastrous results from the plan: "Loss of life will be a certain consequence if Anonymous releases the identities of individuals cooperating with cartels. The validity of the information Anonymous has threatened to reveal is uncertain, as it might not have been vetted. This could pose an indiscriminate danger to individuals mentioned in whatever Anonymous decides to

# Hacker Group Backs Away From Threat To Mexican Cartel

November 2, 2011 · 3:55 PM ET

EYDER PERALTA



## Police say Ukrainian MP, OSINT group coordinator Tymchuk could be assassinated (Photo)

15:50, 19.06.19 · 1 min · 31432

The investigation put forward a number of versions: an accident, careless handling of a weapon, as well as versions of a criminal nature.



фото kyiv.npu.gov.ua

Police are considering different versions of the death of Ukrainian MP Dmytro Tymchuk in an assassination.

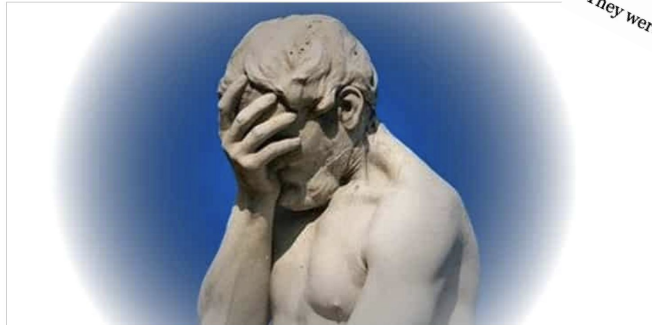
## This Murder Has Exposed the Dark Side of Mexico's Hacking Community

Raúl Robles, a prominent Mexican hacker and cybersecurity expert, was shot while eating breakfast with his father the day after his murder was announced in an anonymous online forum.

### OPSEC fail! "Super-hacker" accidentally outs himself through careless clues left on social media

D'oh!

Graham Cluley · @gcluley  
2:26 pm, May 29, 2020

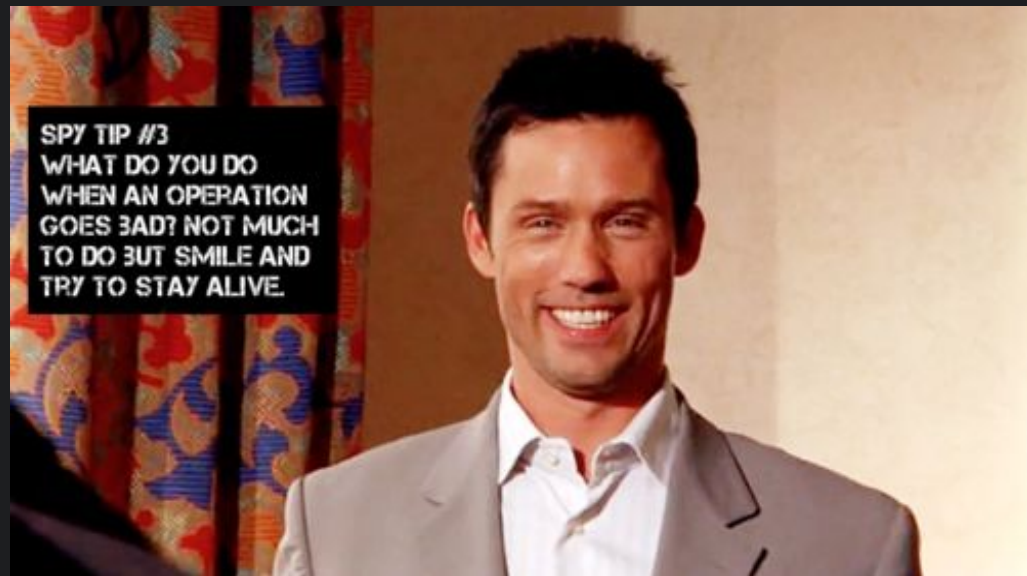


"He took a selfie of him being bored," Lt. Gen. Lori Reynolds told Pentagon reporters in a story first reported by [Military.com](https://www.military.com). "It showed in that selfie it was an artillery unit. You could go geo-locate him, and you could see what unit it was." And once his unit's position was known? "They were like, 'OK, you guys are dead.'"

"This #OpCartel is extremely risky, so we advise new anons to stop only if you have enough experience," a Twitter user known as @ [unclear] yesterday. Earlier today, he also **tweeted** that stopping the #Op [unclear] mean aligning yourself with the Zetas.

# You can't go back & fix it

- Failure to prepare adequate OpSec prior to starting operations can cause serious problems.
- Trying to fix poor OpSec after the risk is detected is virtually impossible.
- It's like building a house and forgetting the foundation.





# The Classic OpSec Process

## Step 1: Identification of Critical Information:

- Capabilities, Activities, Limitations and Intentions (CALI).
- Your true identity, employer, budget, schedule, other priorities and mission (intent).
- Personally this could include:
  - Location
  - Assets
  - Knowledge
  - Weaknesses



# The Classic OpSec Process

## Step 2: Analysis of External Threats:

- Who is your primary adversary?
- Secondary adversaries?
- What is their intent and capabilities?
- Higher intent and capability, the greater the threat.
  - ie Cartel or Street Criminal?



# The Classic OpSec Process

## Step 3: Analysis of Internal Vulnerabilities:

- What is the likelihood of critical information leakage?
- What are the known adversary capabilities to capitalize on that leakage?
  - What about other adversaries?
- What is the impact of leakage?

## **BLOOD SERVICE APOLOGISES FOR DONOR DATA LEAK**

FRIDAY 28TH OCT 2016

The Australian Red Cross Blood Service is apologising to donors for an error which allowed a back-up copy of an online enquiry database to be accessed by an unauthorised person.

Blood Service Chief Executive Shelly Park said today that on 26 October the Blood Service became aware that a file containing donor information was placed in an insecure environment by a third party that develops and maintains the Blood Service's website.

This file contained registration information of 550,000 donors made between 2010 and 2016. The file was part of an online application to give blood and information such as names, addresses, dates of birth and some personal details are included in the questionnaire.

# The Classic OpSec Process

## Step 4: Assessment of Risks:

- Based on Step 2 and 3, we evaluate the expected risk levels.
- External threats + Internal Vulnerabilities = Risk Level

### A False Sense of Security

High	High	Serious	Medium
High	High	Serious	Medium
High	Serious	Medium	Low
Serious	Medium	Medium	Low
Medium	Medium	Medium	Low

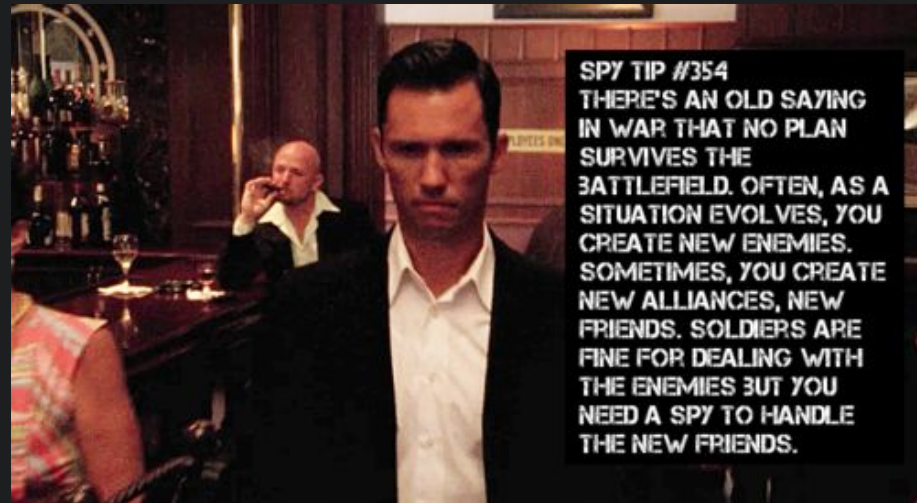
# The Classic OpSec Process

## Step 5: Application of Appropriate Measures:

- Based on step 4, we apply “appropriate” OpSec measures and countermeasures

### Issues with this model:

- “Appropriate” changes fast
- Inappropriate can’t be fixed after the fact
- Expert adversaries will make you assume the risk is low
- Extremely difficult to recover from starting with inappropriate OpSec.



**SPY TIP #354**  
THERE'S AN OLD SAYING IN WAR THAT NO PLAN SURVIVES THE BATTLEFIELD. OFTEN, AS A SITUATION EVOLVES, YOU CREATE NEW ENEMIES. SOMETIMES, YOU CREATE NEW ALLIANCES, NEW FRIENDS. SOLDIERS ARE FINE FOR DEALING WITH THE ENEMIES BUT YOU NEED A SPY TO HANDLE THE NEW FRIENDS.

# Typical Adversaries

Who are we defending against with OpSec?

- Red teaming / Corporate
- Corporate espionage / Ransomware
- Scam artists / Criminals
- Organized crime
- Nation state teams
- Specific adversaries (individuals or groups)



# OpSec Usage

## Individual OpSec:

- Are you aware what you (the real you) are sharing and the risk associated with that?
- Very direct exposure

## Corporate OpSec:

- Are you aware what your company is sharing?
- Initial reconnaissance stage of attack often dictates adversaries investment in target

## Team OpSec:

- Used by teams to secure what information is being shared (red/blue)

## Special Operations OpSec:

- Task focused with specific objective.

# Benefits of OpSec

Beyond operational success, OpSec can improve your life:

- Avoiding general criminal risk during holidays and travel
- Reducing the risk of online scams and blackmail
- Improves your business mindedness (preserves competitive advantage)
- Allows you to better detect deception
- Makes you a better listener





# What is Gray Man?

- Gray Man is the spy craft term for being there but not being remembered. Being a ghost.
- Physical aspect of OpSec where covert is the desired outcome
- Gray Man understands the local culture, mannerisms and dress code
- Avoids highlights and typically blurs the image
- The Gray Man avoids detection or at least identification



# Gray Man and OpSec

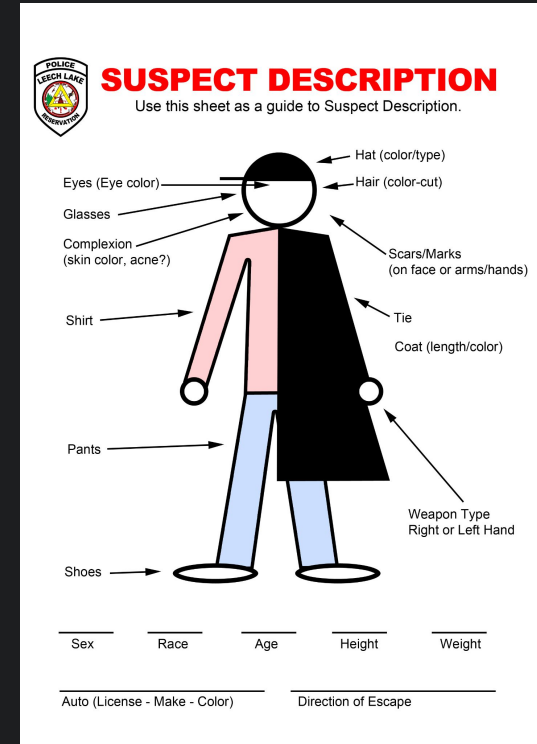
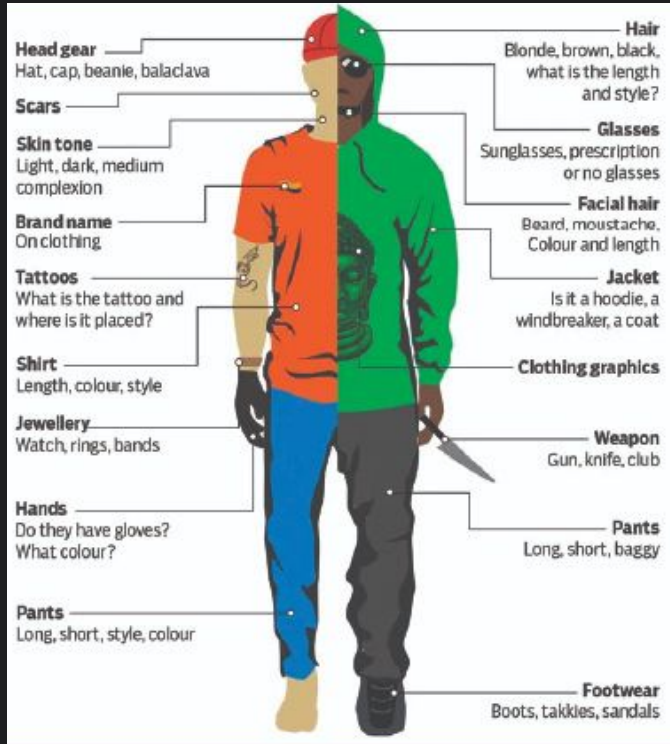
- Grey man principles are the physical representation of virtual OpSec requirements
- Many of the same (OpSec) principles are applied (specific information to specific audience)
- Formalized spy craft that understands the environment and adversaries
- Not only avoids detection & identification but may also leave false trails/fake data
- Starts strong and stays strong through formalization and mature process

# Identification Techniques

Physical identification is built on descriptive attributes:

- **Basic Attributes:** Height, weight, build, sex, age, hair
- **Unique identifiers:** Hair, scars, tattoos, jewelry
- **Clothing:** Brands, graphics, patterns, color, layers, non standard items
- **Behaviours:** Purpose, calm/nervous, injured, intoxicated, evasion techniques
- **Interactions:** Intent, language, accent, familiarity, duration
- **Movement:** Direction of travel, speed, precision, timing, gait, balance

# Identification Techniques



# Physical vs Virtual

Physical appearance vs virtual (sock puppet)

- Detection of fake persona
- Identification of real identity
- What information is provided and what impact will that have?

Instead of clothing brands/colors, language and gait, we are now concerned with:

- Computer/Browser settings for language and our accurate use of translation services.
- Computer/Browser settings for time zone and our operational periods (matching local time)
- Appearance of location. Are we using VPN to adequately mask our true location?

# Fingerprinting

- Both you and the target can be fingerprinted based on correlation and attributes.
- This might be achieved through various means, such as:
  - Browser/IP fingerprinting
  - Time zone/online
  - Language, accent, choice of syntax/semantics, memes, abbreviations, etc
  - Behaviours
- Audit yourself:
  - <https://whoer.net/>
  - <https://www.deviceinfo.me/>



# Fingerprinting

## Date & Time:

## System (Live):

Sun, Jun 05, 2022, 17:03:12 (UTC-07:00 PDT) (DST: Yes)

## Local (Live):

Sun, Jun 05, 2022, 17:03:12 (UTC-07:00 PDT) (DST: Yes)

Local Time Zone: America/Vancouver

ISP: Shaw Communications

## Nameservers:

(IPv4) /

(IPv4) /

(IPv4) /

## Location:

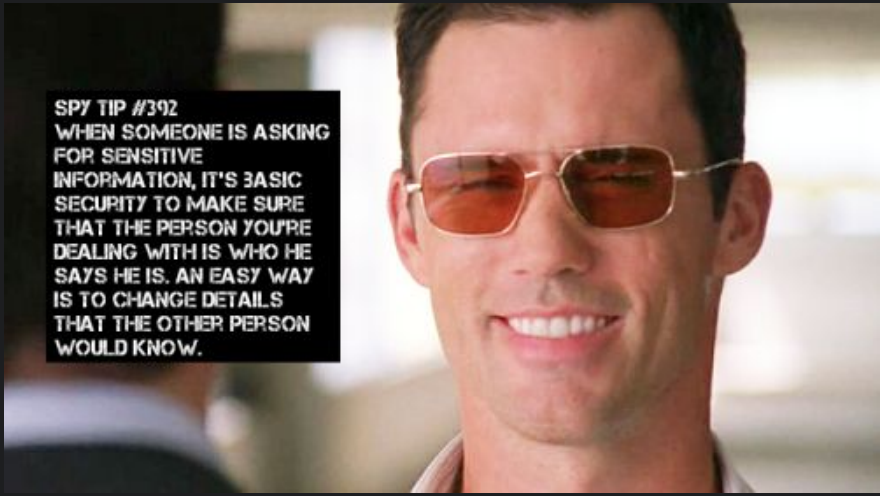
Country: Canada (CA)

Region: British Columbia (BC)

City: Coquitlam

# OpSec Common Mistakes

- **Reuse:** Username reuse, picture reuse, email reuse, jargon/acronym/signature reuse
- **Inconsistency:** Persona errors
  - Time zone errors, naming patterns, story conflicts and/or picture conflicts
- **Innocent Small Talk:** Tricked into talking about the weather
  - Even the simplest most benign topics can accumulate to identify and locate you.
- **Forgetting the Game:**
  - Becoming actual friends with the target
  - Disclosing personal information
- **Pollution:**
  - polluting your personas or system

A close-up photograph of a man with short dark hair, wearing gold-rimmed aviator sunglasses and a light-colored collared shirt. He is smiling slightly. A black rectangular text box is overlaid on the left side of his face.

SPY TIP #392  
WHEN SOMEONE IS ASKING  
FOR SENSITIVE  
INFORMATION, IT'S BASIC  
SECURITY TO MAKE SURE  
THAT THE PERSON YOU'RE  
DEALING WITH IS WHO HE  
SAYS HE IS. AN EASY WAY  
IS TO CHANGE DETAILS  
THAT THE OTHER PERSON  
WOULD KNOW.



# OpSec Common Mistakes

Even when the primary target is hard, secondary targets are often soft. Friends, family, suppliers, etc.



# OpSec Common Mistakes – Examples

## Silk Road (username/email reuse)

- Username with the handle "altoid" posted on a bitcoin forum about a new hidden service that would be an "anonymous amazon.com," linking to a site at silkroad420.wordpress.com. Months later, the same user posted looking to hire an "IT pro in the bitcoin community," and urged candidates to write to rossulbricht@gmail.com. **That Gmail address was in turn connected to a Google+ account** that posted content about Austrian economic theory, a set of libertarian ideas that was also the subject of posts on Silk Road from the Dread Pirate Roberts.

## AlphaBay (email reuse)

- Law enforcement officials noted that emails AlphaBay users received when they signed up or reset their password contained the email address Pimp\_Alex\_91@hotmail.com in their headers. **That email was connected to some 2008 posts** on an online tech forum from a user with the handle Alpha02 (also the username of the AlphaBay administrator).

# OpSec Common Mistakes – Examples

## APT1 (username reuse, pattern correlation, working hours)

- Reused usernames: One APT1 member signed the source code he wrote with the nickname "Ugly Gorilla". This handle was connected to posts on programming that were associated with his real name, Wang Dong. This allowed U.S. researchers to connect Wang to a specific IP address that, it turns out, APT1 used as well.
- Pattern correlation: The group used predictable naming conventions for their users, code, and even passwords.
- Working hours: Most time stamped activity associated with the group took place during business hours in Beijing. That not only pointed security researchers to their location, but also indicated that they were professionals rather than activists or enthusiasts hacking during their free time.

# OpSec Common Mistakes – Examples

## Trace Labs Op Example 1 (username reuse)

- Subject: Teenage girl - Florida, USA – Missing 2 months.
- Username reuse allowed discovery of account on classifieds site.
- Selling her cat to move away from Florida. Account tracked to New York area.
- Posts looking for personal driver “risky work.”
- Hidden social media account owned by subject discovered. Posts 3 weeks after missing.
- Coordinates gathered from photos. Location narrowed to 5 mile radius.

# OpSec Common Mistakes – Examples

## Trace Labs Op Example 2 (username reuse)

- Subject: 21 year old girl - California, USA – Missing 6 months.
- Amazon wish list discovered from username reuse.
- Items on Amazon wish list suggest involvement in adult entertainment industry.
- Username reuse also identifies profiles on adult services websites.
- Advertisements on site are recent and after she went missing.
- The site can offer law enforcement with email, IP address, Internet provider, etc.

# Platform

## Virtualization:

- Base image preconfigured & hardened for fast deploy
- New image for each operation (no leakage)
- Snapshots for point in time restores
- Product Options:
  - Virtual Box (free)
  - VMWare ESXI/VSphere (free)

## Hardware:

- Dedicated laptop
- Physically hardened (ie. webcam/microphone disabled)
- NUC (Next Unit of Computing) for offloading images and running VMs.

\*\*\* No research or personal activity on operational machine. Includes no connecting or linking to personal devices (ie phones) \*\*\*

Home/ Evaluate VMware Products / VMware vSphere Hypervisor 7.0 update 3d

## VMware vSphere Hypervisor 7.0 Update3d Download Center

This download center features technical documentation and installation guides to make your use of vSphere Hypervisor a success.

### Top vSphere Hypervisor Resources

- VMware Hardware Compatibility Guide



# Operating Systems

## Trace Labs Distro:

- Linux distro with OSINT design

## Other Industry Based Recon OSES:

- Kali
- Buscador (Bazzell)

## Whatever you are familiar with:

- Understand how it works and the trail you leave

## Trace Labs OSINT VM

### Crowdsourced OSINT to Find Missing Persons

The Trace Labs team created a specialized OSINT VM specifically to bring together the most effective OSINT tools and customized scripts we saw being used during our Search Party CTF's. Inspired by the infamous Buscador VM, the Trace Labs OSINT VM was built in a similar way, to enable OSINT investigators participating in the Trace Labs Search Party CTF's a quick way to get started and have access to the most popular OSINT tools and scripts all neatly packaged under one roof.

# Communications

## Messaging:

- VoIP numbers often denied in messaging apps
- **SIM card foreign numbers are often accepted (and retain after SIM swap) \*\*\***
- **eSIM is new opportunity \*\*\***

## Email:

- Randomized or themed (part of developed persona) username
- Decentralized communications: Not using Gmail for everything
- Encrypted/Anonymous email may be a red flag. Options include
  - protonmail.com
  - cyberfear.com
  - ctemplar.com
  - tutanota.com
  - sudomail.com



# Browsers



## Whatever you know:

- Understand how it works and the trail you leave

## Librewolf:

- Designed to increase protection against tracking and fingerprinting techniques, while also including a few security improvements. Also aims to remove all the telemetry, data collection and annoyances, as well as disabling anti-freedom features like DRM.

## GNU IceCat:

- Formerly known as GNU IceWeasel. Open source version of the Mozilla Firefox web browser distributed by the GNU Project. It is compatible with Linux, Windows, Android and MacOS.



# Browser Extensions

- **uBlock Origin:** Pattern based filtering on ads. Easy to use.
- **uMatrix:** Allows you to control what you block/allow. More flexible than uBlock Origin.
  - Additional privacy/security (spoofing, clearing blocked cookies, etc)
- **Chameleon:** Spoof your browser profile. Includes a few privacy enhancing options.
- **NoScript:** NoScript is a free software extension for Mozilla-based web browsers and Google Chrome. Caution: <https://iltinkerer.surge.sh/noscript.html>
- **Privacy Badger:** Blocks trackers
- **User-Agent-Switcher:** Chrome ext for spoofing what your browser and OS appear as.

# Browser Extensions

- **HTTPS Everywhere:** Enforces encryption where it is dropped to prevent people from eavesdropping on your data in transit.
- **Fake Profile Detector:** Built by V7 Labs. Chrome browser extension.
  - Right click on profile picture and the extension will detect if image contains a GAN generated or real person
- **Sketchfab.com:**
  - Take screenshot of a 3D, AI generated photorealistic human model
  - Use mobile version of platforms to get photo requirements rather than video



V7 Labs has created a new artificial intelligence-based (AI) software that works as a [Google Chrome extension](#) that is capable of detecting artificially generated profile pictures — like the ones above — with a claimed 99.28% accuracy.

# Tools Caution

- **Familiarity:**
  - Do you know what's in the source code? Open source?
  - Is it loud or quiet? Will it set off alarms once active?
  - Do you know exactly what it does?
  - Are you familiar with best configuration?
- **Targeting:**
  - Just doing recon on public sources or targeting an adversary's infrastructure?
- **Basic Tools:**
  - VPN for appearing in certain locations (preferred over browser ext)
  - Blocking software to reduce footprint
  - Updated patch level



# Sock Puppets – Creation

- Generate a personality with a backstory
  - Keep as close to the truth as possible
  - Appear as a prime social media target audience (avoid protonmail etc)
- You want to appear as normal as possible to the provider
  - Public or cellular Internet to initially register
  - VPN to use after registration
  - IP addresses can be a concern
  - Useful to tie sock puppet personas to specific VMs
- Random face generators are becoming less of an option
  - ie thispersodoesnotexist or boredhumans, etc



# Sock Puppets – Creation

- Auto persona generators are fast but low quality
  - <https://www.fakenamegenerator.com/>
- Better to handcraft the persona
  - Use country gov statistics to get popular names for particular years
- Amazing sock puppets have community
  - Friends
  - Family
  - Holidays
  - Hobbies
  - Sports, politics, opinions, etc

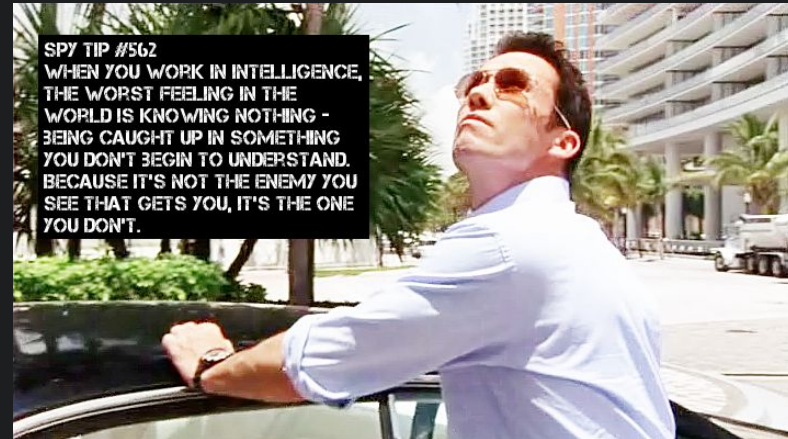


# Sock Puppets – Maintenance

- You must become your alias before you start any other action.
- Avoid cross contamination:
  - When the adversary becomes aware that two of your aliases are both you.
- Appear real:
  - Huge lulls in activity and the activity that is present is often boring and/or operation driven.
  - Real accounts have memes, jokes, teasing, arguments, birthdays and general nonsense.
  - Effective sock puppets require care and attention.

# Interactions

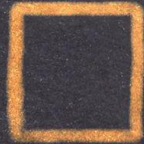
- Direct interactions with your real identity means your burnt
- Always assume the person is not the same as the picture/online identity
- Always assume their motives are masked
- Track the release of info (as your adversary likely is)
- Try not to be the first to answer questions
  - Ie. "Where are you located?"
- A good adversary will build trust before attacking
  - Wait for it, a good attack feels like a favor





# OpSec Review

- Start with zero trust (like the grey man)
- Understand the reaction of released content
- Create a scalable and reusable operating environment
- Examine your footprint - location, language, syntax, etc
- No reuse or cross contamination of personas or environments
- Feed and care for your sock puppets
- Understand not only your objective but also your adversary's objective
- Beware of distractions
- Have a strategy if your persona is burnt



# Questions & Answers