OPSEC

Ryan Cunningham
The Grugq

- Security researcher famous for researching this topic
- His work inspired this lecture
- All credit to The Grugq
OPSEC

- Originally a military term
- Operations Security
  - Protecting information
  - Preventing data leaks
- Related ideas:
  - Counterintelligence – defense against espionage
  - Tradecraft – espionage techniques
  - COMSEC – communication security
OPSEC for Criminal Hackers

- “So You Want to Break the CFAA? Good Luck With That.”
- “How to Break the Law and Not Go to Jail (for a while)”
- “How to (not really) Avoid the FBI and NSA”
- “Why Cyber Criminals Get Caught”
THE ADVERSARY
Who is the adversary?

- Law enforcement and intelligence communities
- Corporate security employees
- Private investigators
- Digital forensics experts
- Other criminal enterprises
- All of your victims
- Vigilante white/grey hats
UNIFIED DIGITAL FORENSICS PLATFORM

Explore Cellebrite’s new and innovative Analytics platform and transform the way your agency uses mobile evidence

READ MORE
Encase

From beginning to endpoint.

Request Demo »
IBM i2 Analyst's Notebook

IBM i2 Analyst's Notebook arms analysts with multidimensional visual analysis capabilities so they can quickly uncover hidden connections and patterns in data.

Starting at $4,120.00 USD per user

Buy
Launch interactive demo
Link Analysis

- Analyze and integrate surveillance data to discover relationships:
  - People (social graph)
  - Organizations
  - Transactions (money, credit cards)
  - Geolocation (space)
  - Communications (people, devices, accounts, IPs)
Pattern-of-Life Analysis

- Analyze and integrate surveillance data to discover habits and routines:
  - When you wake up
  - When you leave for work/class
  - What routes you use
“See, the thing is, you only got to fuck up once. Be a little slow, be a little late, just once. And how you ain't gonna never be slow? Never be late? You can't plan through no shit like this, man. It's life.” – Avon Barksdale (The Wire)
OPSEC is a lifestyle

- A mindset
- A set of habits
- A way of thinking
- A way of living
OPSEC is proactive

- “Paranoia does not work retroactively.” – The Grugq
- Practice before you need it
- Boring and tedious work must be done up front
- Must be maintained
- “The more you sweat in peace the less you bleed in war.”
The Zeroth Rule of OPSEC

- Eventually, you will fail
- Be prepared to face the consequences
The First Rule of OPSEC
The First Rule of OPSEC

- You do not talk about criminal activities
- Don’t brag
- Don’t demonstrate skills or knowledge or interest
- Don’t get blackmailed
- Only tell people what they need to know
- Keep your methods secret
One Law at a Time

- Only break one law at a time:
  - No drugs
  - No stealing
  - No fighting
  - No DUls
  - No illegal firearms
  - No speeding
  - PAY YOUR TAXES!
Be Clean

- Know all relevant forensic artifacts
- Know what forensic data potentially implicates you
- Destroy forensic artifacts
- Wipe computers used in criminal activity
- Disable logging, browser history
- Encrypt any data you keep
- Encrypt all communications
- Shut down computers
Be Very, Very Clean

- Turn off phones
- Both device and SIM ID numbers are logged
- Assume all communications are monitored
- Store incriminating scripts and data on a remotely hacked machine
- One trace can ruin you (e.g. the background of a photo, a chance meeting, unexpected device metadata, an surprise ATM camera)
Be Vague

- Never be explicit about criminal activities
  - Obscures monitored communications
  - Assists in defense if you are caught
- Use code words for targets and operations
- Use cryptonyms like the intel community
  - Random, not cute or clever
- Law enforcement will figure out code words
- Change code words
Be Professional

- Methodically plan criminal activities
- Maintain discipline
- Criminal activity cannot be recreational
- If you do it for fun, you will get careless.
Be Nobody

- Keep a low profile
- Limit social media use
- Keep irregular hours
- Use US ASCII keyboards, common devices
- Avoid meetings, conferences, mailing lists, and groups
- Blend in and be boring
- “You can be famous, and you can be a hacker, but you can’t be a famous hacker.” – The Grugq
Be Someone Else

- Invent new personas (fake identity)
- Give persona a history
- Supporting evidence (e.g. social media profile)
- Create sub-aliases (cover within cover)
  - Hacker pseudonyms
- Have additional personas ready in case you are compromised
- Phase out persona if it is successful
Be One Person at a Time

- Do not cross your identity with your cover persona
  - e.g. log in from work IP address to cover persona email
- Do not cross one cover with another
  - e.g. accidentally use the wrong handle in a hacker IRC
- Keep track of “who you are”
- Don’t leak details of personal life
- Don’t talk about the weather, news, or events
Be Patient

- Maintain time and distance between criminal activities
- The more secure the communications, the higher the latency
- Learn as much as possible about your target
- If you suspect compromise, back off
- “You’ll know it works if nothing happens.” - The Grugq
Be Paranoid

- Keep criminal conspiracies small
- Trust no one
- Especially your “partners”
- Work with people who earn your trust
- “They are not your friends, they are criminal co-defendants.” –The Grugq
- If they get caught, they could turn on you
- VPNs, ISPs, cloud providers, and email providers won’t protect you
Compartmentalize (Defense in Depth)

- Hack from public wifi
- Use proxies, VPNs, Tor, Pond
- Use burner phones
  - Purchase with cash
  - Don’t turn them on anywhere near home
  - Never turn them on near personal phone
  - Don’t share SIM cards between devices
- Use burner email accounts
- Use bitcoin (use mixers) or cash
Arrested?

- Don’t assume you are caught
- Don’t talk to the police
- Hire a lawyer
- Trust your lawyer, take the deal
OPSEC FAILS
Lulzsec

- Members: Sabu, Topiary, Kayla, Tflow, Avunit, Pwnsauce, Palladium, Anarchaos, ViraL
- Guardian released transcripts of IRC chats
- Sabu got arrested, flipped on the rest of them
- Anarchaos gave details about marijuana arrests and probation in IRC “it could compromise my identity”
- Member sent website defacement code to another member via a Facebook message
Lulzsec

- Members connected to IRC from one IP address
- Member used real name as IRC login ID
- Sabu: “who is this?” Polonium: “this is palladium”
- Anarchaos: “dumpster diving is all good i’m a freegan goddess” (he really was a freegan)
- Members discussed using Apple products to hack, complained about Tor, mentioned VPN providers
- Sabu asks about an IP address
  Palladium: “ip looks like a wifi I connect from.”
Lulzsec

- After getting arrested, Polonium told IRC channel about getting arrested
- FBI didn’t ask Palladium much about Sabu (the leader)
- Members kept regular life patterns, hacking correlated with their time at home
CabinCr3w

- w0rmer posted a JPEG with EXIF metadata on defaced website
- FBI: intentionally gets SQLi details wrong
- w0rmer: corrects them
- w0mer complains in online about getting arrested
Silk Road

- Ulbricht advertised Silk Road using alias “Altoid” and contact email rossulbricht@gmail.com
- Ulbricht mentioned political views on LinkedIn “creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force”
- Ulbricht mentioned The Von Mises Institute under his real name and DPR pseudonym
- Used same café to access VPN and personal gmail account
- Ulbricht used PGP to encrypt messages, no deniability
Reality Winner

- Complained about new administration on social media
- Searched for keywords to find the relevant document in internal databases
- Printed the document (only document she printed)
- Mailed the document from her home town
- Reporter sent document to contractor and NSA
- Reporter told contractor where the document was mailed from
- Admitted to FBI that she printed the document
Reality Winner

Testo
d

Testo

auf
d

auf
da
Abu Omar Rendition

- Witness noticed Omar being abducted by a van (time of day + location)
- Local CIA assets used burner phones to communicate ONLY with one another and CIA
- Italian LE gathered cell phone metadata, identified cluster of asset phones, produced map of phone locations
- LE analyzed pattern of life to find hotels, which gave passports and credit cards, which gave travel plans
Abu Omar Rendition
Abu Omar Rendition

- SIM cards and phones active and co-located
- One CIA operative used his real name, home address
- Assets used potato chip bags as Faraday cage
- One agent used a friend’s last name as cover identity
- Passports of agents were consecutive
- Only two operatives allowed to contact CIA directly...
- ... but they used dirty and clean SIM cards in the same phone
OPSEC IS DIFFICULT
OR...
... just don’t.

- Don’t break the law.
- Hack for the good guys:
  1. Talk all you want
  2. Trust who you want
  3. Share what you learn
  4. Have fun
  5. Relax and enjoy life
“See, the thing is, you only got to fuck up once. Be a little slow, be a little late, just once. And how you ain't gonna never be slow? Never be late? You can't plan through no shit like this, man. It's life.” – Avon Barksdale (The Wire)