SIGPwny @ UIUC
Intro to Opsec

Spring 2017

Announcements

- Manticore focus group
- Thotcon & Defcon
  - May 4 & 5
- Cyphercon
- UIUCTF Challenge Idea Submissions
  - https://goo.gl/forms/fmp7eWsl6MEDqGyq1

News of the week

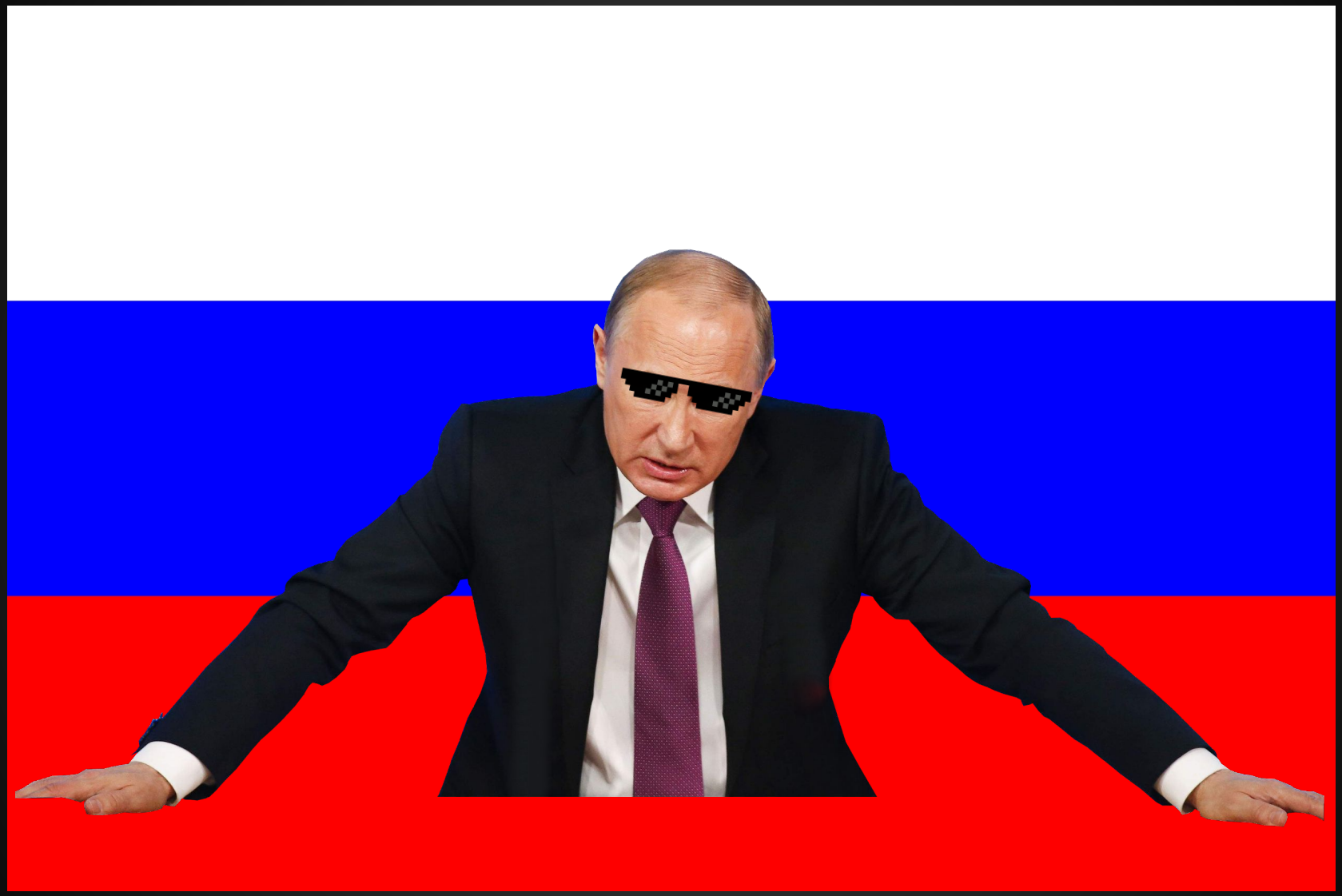
- Google Publishes Windows Vuln (Again)
- Kim Dotcom Getting Extradited
- IDF Targeted with Android Malware
- SHA1 Collision Found
- Double Free in Linux Kernel
- Pentesting cheat sheet

Disclaimers

- Most of these slides are stolen from @thegrugq
- I am not a lawyer
- I’m not going to jail for you

What is Opsec?

- Keeps information safe
- Stops plans from going awry
- Keeps you out of jail



Part One: Comsec

- In order to operate, you need to communicate.
- Communication is a great way to map out your organization for Vladimir.

Tenets

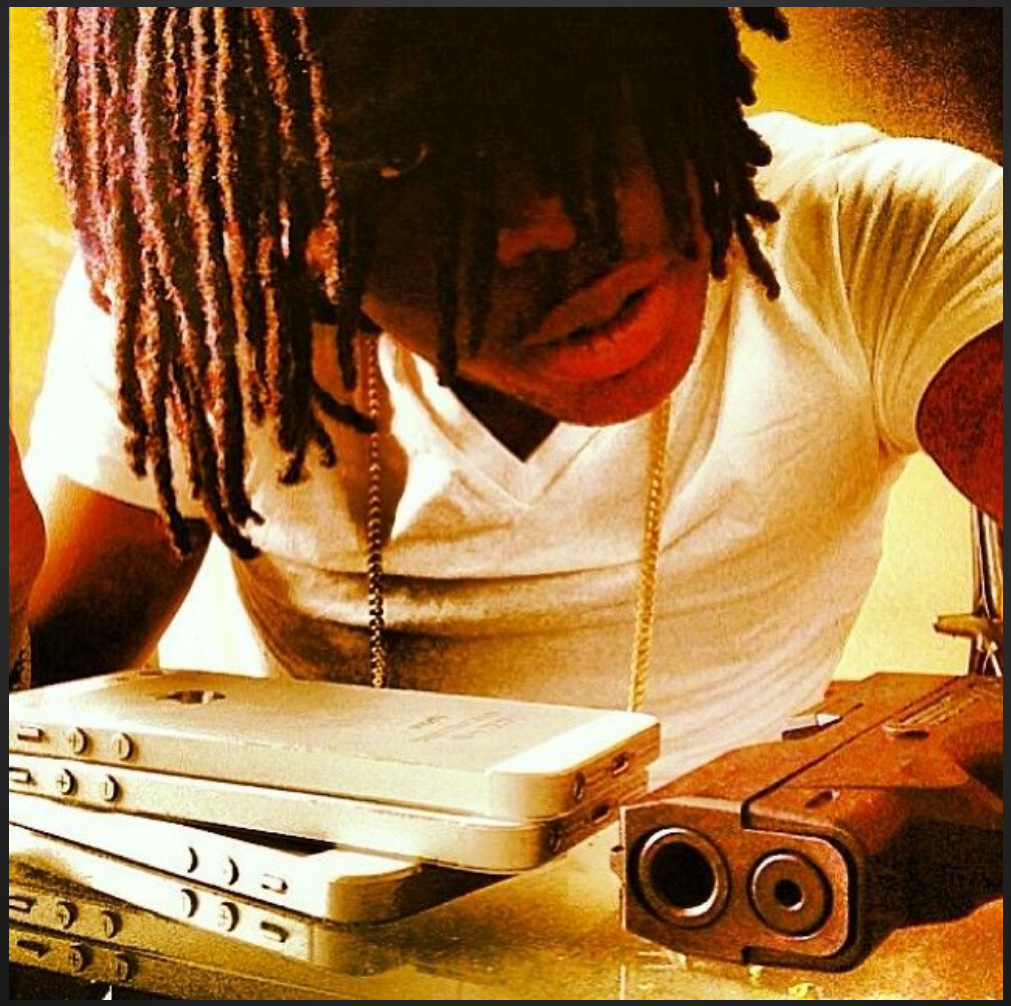
- Confidentiality
  - No one can read your messages
- Integrity
  - No one can modify your messages
- Availability
  - Messages are hard to block (P25)
- Cover
  - Helps avoid closer scrutiny
- Concealment
  - If it looks like a duck, it's probably not a spy plane
- Compartmentalization
  - Limited sensitive information in any one place
  - PFS

Real Gs move in silence, like lasagna

Concealment

- TOR traffic looks like TOR traffic
  - Even if you can’t tell where it’s going, it’s suspicious
- PRC can identify VPN traffic easily
- Use Signal for everything, with everyone
- If it looks like HTTPS, no one will bat an eye
- Steganography - not just for lazy CTF authors

I got two phones, one for the plug and one for the load



Compartmentalization

- Information
  - Tell people only what they need to know to do their job.
  - You're better off not knowing.
- Communications
  - Cycle keys often.
- Devices
  - Absolutely nothing traceable to you ever touches your throwaway devices. Ever.
- Identity
  - Have an alternate persona strong enough to use when you need it.
  - Set this up well in advance.

I’mma look fresh as hell if the feds watchin’

Threat Modeling

- FSB/Mossad/PRC
  - If it has wires, it's spying on you
- Russian Mafia
  - Well-resourced, technically sophisticated
- Local Law Enforcement
  - Probably bound by the law
- Disgruntled Ex
  - Limited technical expertise and resources, insider information
- Bitter Enemies in the Electronics Hobbyist Community
  - Will destroy your pacemaker with a CB radio and a Pringles can.

“There is no such thing as tiger self-defence. You can’t just ‘train harder!’ and fight tigers one day.”

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don’t click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU’RE STILL GONNA BE MOSSAD’ED UPON

https://www.usenix.org/system/files/1401_08-12_mickens.pdf

Why You Threat Model

- Trying to authenticate messages?
  - PGP proves key-holder wrote a message
- Fighting the FSB?
  - PGP provides a provable ring of conspirators
  - Signing = cryptographic proof you wrote an incriminating message
  - “--- BEGIN PGP SIGNED MESSAGE ---” = “Hey Vladimir, check this out”
- Decide what you need from your tools, then choose tools accordingly. NOT the other way around.

“I don’t have to outrun the bear - I just have to outrun you!”

This is the worst analogy ever.

The Bear is LEO. With care and attention we can beat LEO, and we want to be in the woods (where there are bears), because the woods are full of heroin money… or honey or whatever metaphor thing everyone wants.

1. None of you can outrun the bear. Bears run at 60kph
2. The first person that gets caught by the bear won’t get eaten. They will snitch.
3. Next, the bear runs you all down, one by one, at 60kph, and kills you
4. The snitch will never do jail time, get a million dollars for their life story, and party at VICE.

So the moral, if anything, is “run slowly and learn to speak bear”

tl;dr

In the long run, CCC > CIA

Tools

- Strong password + 2FA (Not SMS)
- Signal
- TOR
- VPN
  - Algo
- VM
  - Qubes
- Windows
- iOS
- Chrome OS

Disposable Hardware

- Raspberry Pi
  - Anything you won't mind melting in thermite
- Cellular Modem
- VPS
  - Somewhere over international lines (preferably unfriendly country)
  - Pay in BTC
    - Tumble your bitcoins!
- iPod Touch
  - No touch login
  - Long passcode
  - Only used for Signal

Cash rules everything around me

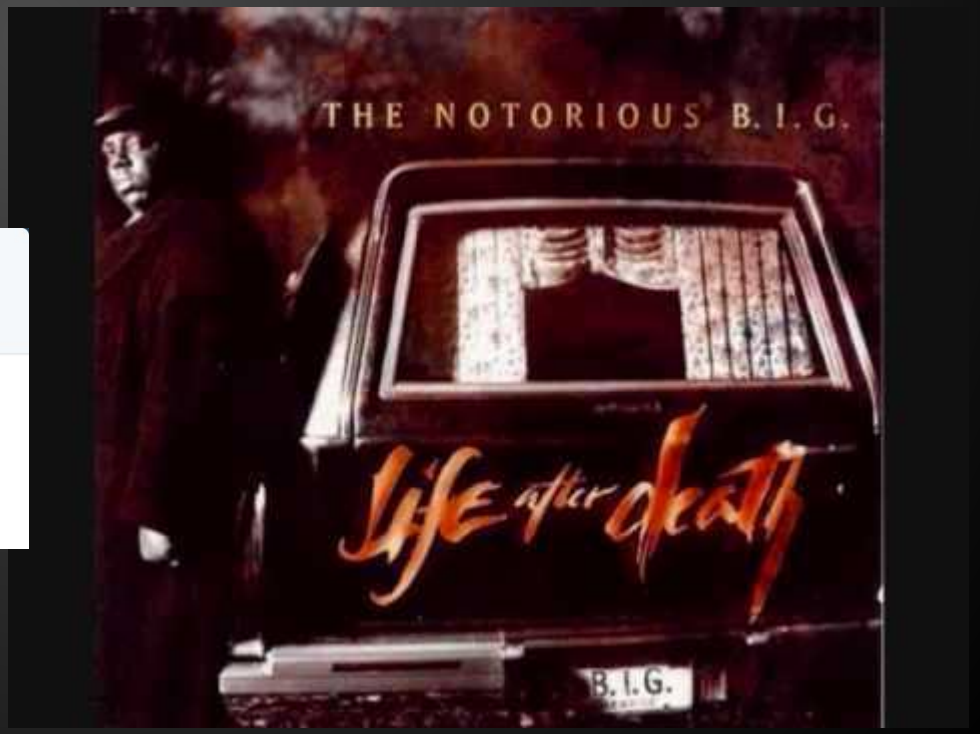
Random Talking Points

- End-to-End or GTFO
- TOR → VPN, because VPN → TOR gets you arrested
- Snitches get reduced sentences
- STFU

Part two: Opsec rules

Required Reading

- The Moscow Rules
- How to Master Secret Work
- Everything @thegrugq has ever written (2)
- Lulzsec casefiles
- This?



Have a Believable Legend

- Do research, seem normal
  - Travel brochures are a gold mine
- Don’t make things up on the spot
- Carry proper documentation
  - “Pocket Litter” - small details that make your persona more believable

If the devil's in the details, then I'm satanic

Compartmentalize Harder

- Never reveal underground activities to anyone
- Maintain pseudonymous relationship with co-conspirators
  - Anonymity is probably overkill
- 7: This rule is so underrated \ Keep your family and business completely separated \ Money and Blood don’t mix.
- Don’t mix recreation with clandestine operations
  - Number four: know you heard this before \ never get high on your own supply.

Mo’ People, Mo’ Problems

- Cap your organization at five people
- Risk of compromise increases exponentially with every person you add
- If you’re running a large-scale intelligence agency, design your hierarchy so cell size is small

Breakin' the law with no codefendant
Go to jail, I get a lesser sentence

Go with the Flow

- Blend in
- Lull adversaries into a false sense of complacency
- You are what you appear to be
  - Project confidence
  - Camouflage

STFU

- Loose lips kill
- Rule nombre uno: never let no one know \ how much dough you hold.
- Number two: never let ‘em know your next move \ don’t you know bad boys move in silence or violence?
- Retroactive paranoia doesn’t work
- Protecting your tweets doesn’t count
- There’s no such thing as a famous hacker

Trust No One

- Number three: never trust nobody \ your mom’ll set that ass up.
- Assume everyone is under opposition control.
  - Adversaries will try to trap you

Be Disciplined

- Lateness is a good indicator of compromise.
  - Never wait more than ten minutes for a meeting.
- Never contaminate compartments. Your life depends on it.
- It only takes one screw-up to land yourself in the Gulag.

Prepare Chaos

- Plan your moves well in advance.
  - Opportunity should be used sparingly.
- Don’t follow a routine. Vary your patterns as much as you can while still blending in.
  - Machine Learning
- Have an escape plan

Need to Know

- Never reveal more information than absolutely necessary to a co-conspirator
- This applies to you too
  - If you don't need to know it, then you're better off not knowing.

Know which Channels are Open

- Avoid use of flagged keywords in public
- Use innocuous code phrases
- Stick to pre-existing secure channels whenever possible

Leave no Trace

- Wipe fingerprints
- Delete logs
- Securely wipe hard drives
- Melt equipment in thermite
- Know which purchases can be tracked
  - Printers are evil
  - Pay for things in cash (or bitcoin)
- Avoid possible means of tracking
  - RFID Infrastructure
  - Wireless Transmitters
- Destroy evidence proactively

Hide Compromising Material

- Memorization > Encrypted storage
- Store things in locations that fit your cover
- Number five: never sell no crack where you rest at
  - Applies both to storage and operations. Nothing happens at home. *Nothing*.
- Number eight: never keep no weight on you.

Coast Guard come, a hundred going overboard

Know the Landscape

- Know how to get around your area of operations without technological aids
- Do more research than you need to
- Monitor your adversaries
  - Google Ads

Don’t Snitch

- Number nine shoulda been number 1 for me: \ if you ain’t gettin’ bagged stay the f*ck from police
- You’re getting gulag’ed either way.

Assume Snitches

- If any member is compromised, assume they've told Vlad everything they know.
- Immediately take precautions. Overkill doesn't hurt.

https://www.youtube.com/watch?v=avsqkevmCIM

Challenge

- http://bit.ly/2mq0RcO
  - When was this photo taken, and where?
- What's Eric's password?
- What's Eric's home address?