Vibe Check.... idk about this

Why students may shy away from cyber in a surveillance state

Mika Devonshire

Mika Devonshire

GCFA, CISSP, MSc Digital Forensics

Incident response and investigations by day

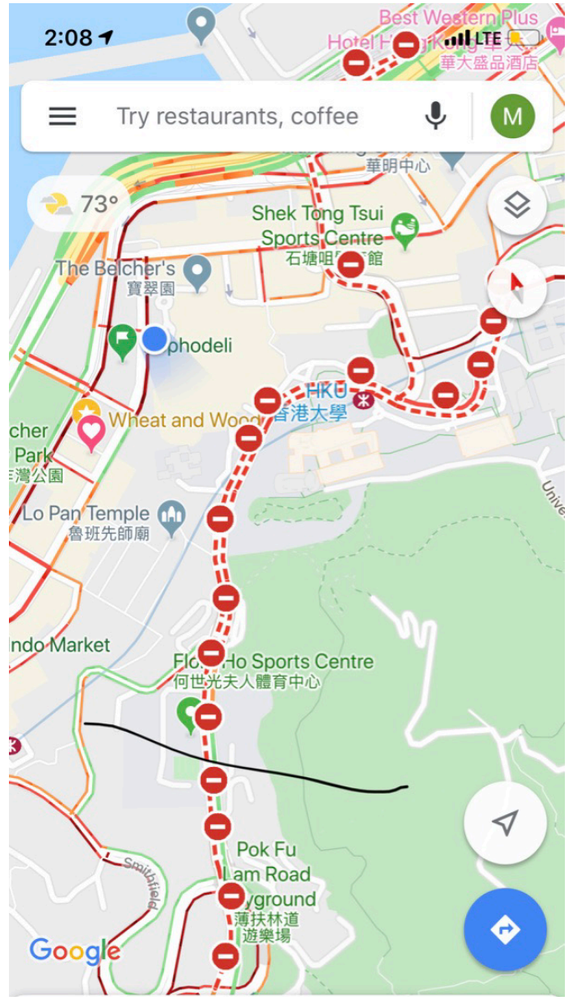
Assistant professor of malware analysis by night

linkedin.com\mikadevonshire

@cybermeeks

Hong Kong University

Fall 2019



Purpose

We all need to hire

There aren't enough talented cybersecurity trainees (2.4 Million short in Asia, 4M world wide)

Newcomers are opting for "safe" careers

Why is that…

"There's simply not enough interest for us to pursue cyber security professionally"

- Graduate Student, Hong Kong University

Reason number one….

Fear

Reason number two….

Lack of Interest

Reason number three….

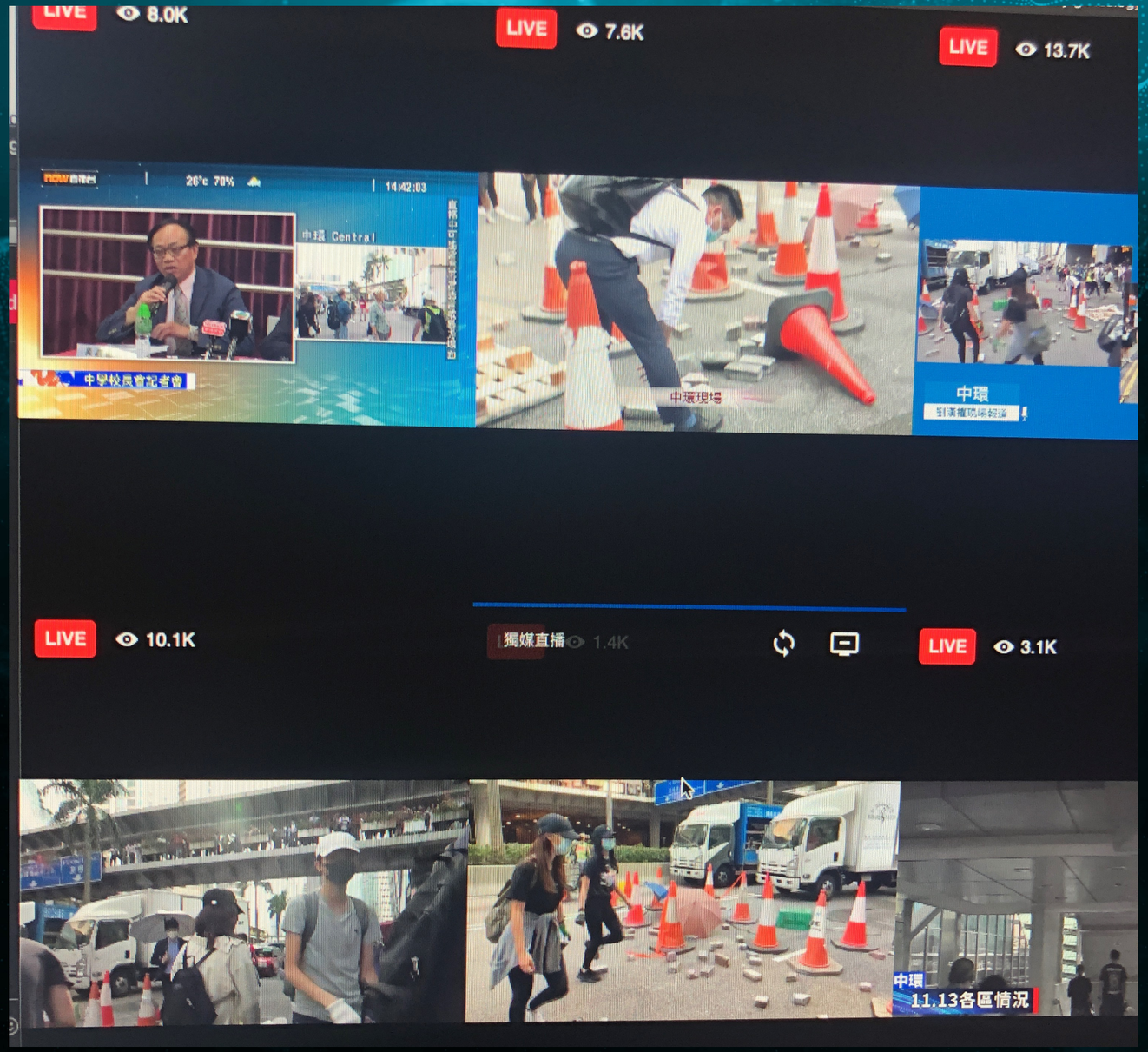
Lack of Prestige

Watch Towers

What is a “surveillance state”?

Governments seek to optimize their security apparatus to reduce crime

- Zero tolerance policies
- CCTV
- Lighting on streets
- Facial recognition
- Firewalls and monitoring



Reason number one....

Fear

- As a student without well legal education, it is very hard to judge which activity is prohited by laws and scared about practicing offensive security techniques

Fear

Know the Rules

Are these activities really prohibited?

SG – Computer Misuse Act

HK - Cap 200 crimes ordinance

US – Computer Fraud and Abuse Act, Information and Technology Act

PH - Cybercrime Prevention Act of 2012

From career prepective,

- There are background checks before onboarding a company.

Fear

Best Practices

What to do and what NOT to do?

DO – learn the laws of your country

DO – always obtain authority and clarify the scope

Do NOT – assume that what you are doing is legal

Do NOT – export or obtain sensitive information

Do NOT – misuse computer resources to negatively impact systems

In a surveillance state, collecting our data are considered legal, as defined by the government. Everyone are so used to having their personal data collected and speeches being monitored that data breach news does not create any ripple. Then, the only legal careers on cyber security would be joining the state, implementing and reinforcing the surveillance.

Reason number two….

Lack of Interest

Case Study:

An Australian researcher noticed a common ID in his bank’s URL on the statement page

He then extracts 500 customer records to prove he could break into a financial services application

He sent those statements to the bank, and expected a huge reward

Best Practices

What to do and what NOT to do?

Do NOT – go beyond the reasonable bounds to obtain proof

Do NOT – publish on impulse, work with the process

Act with integrity, not with pride

Some companies will find ways to avoid paying a researcher

Case Study: HITB Attendee's public declaration of hacking

I recently attended HITB in Singapore, and what interests me more is the hotel's WiFi. I went to three hotels, and WiFi uses a unified authentication system, which is AntLabs' IG3100 device. When connected to WiFi, an authentication page with the address ezxcess.antlabs.com pops up:

Fear

Case Study:

HITB Attendee’s public declaration of hacking

He posted the information he found from the hotel on his public website

Singapore Cyber Security Authority flagged his post and pressed charges, he escaped a prison sentence but was fined 5,000 SGD

Fear

Best Practices

What to do and what NOT to do?

Do NOT – go beyond the reasonable bounds to obtain proof

Do NOT – publish on impulse, work with the process

Act with integrity, not with pride

Some companies will find ways to avoid paying a researcher

“... the company did what every company should not do, become defensive and take legal action against the security researcher."

- Director, Australian Security Firm

Case Study:

A researcher used a fake Gmail account to submit findings that customer data was being exposed on the web

The company flagged the email as extortion

He then expressed his grievances, and the company eventually paid a bounty to avoid having to disclose the breach publicly

Best Practices

What to do and what NOT to do?

DO – use your real information

DO – use appropriate channels

direct disclosure or bug bounty programs

Companies react poorly to bug disclosures

Security researchers may seem threatening

Build trust by showing your good intentions

Reason number two….

Lack of Interest

“To be a Project manager you only need a PMP"

- Graduate Student, Hong Kong University

Identify Talent

What makes a good “hacker”?

1. Creativity
2. Patience
3. Humility

“defense is cool... but offense is cooler”

- Someone in this audience

BOUNTY RANKINGS	RESPONSE	HACKERS
Total Bounties Paid **>$9,408,000**	Average First Response **8 HOURS**	Thanked **1,315**
Top Bounty **$70,000**	Average Time to Bounty **13 DAYS**	Reports Resolved **5,928**

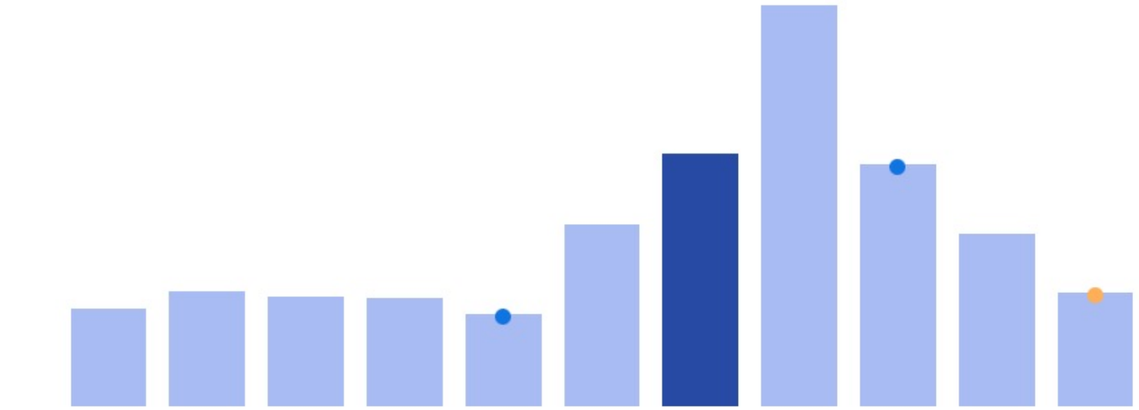
Program launched February 2014

Reason number three….

Lack of Prestige

Ethical Hacker Salary

Yearly Monthly Weekly Hourly Table View



$119,289 /year

Reason number three….

Lack of Prestige

Bright Outcomes

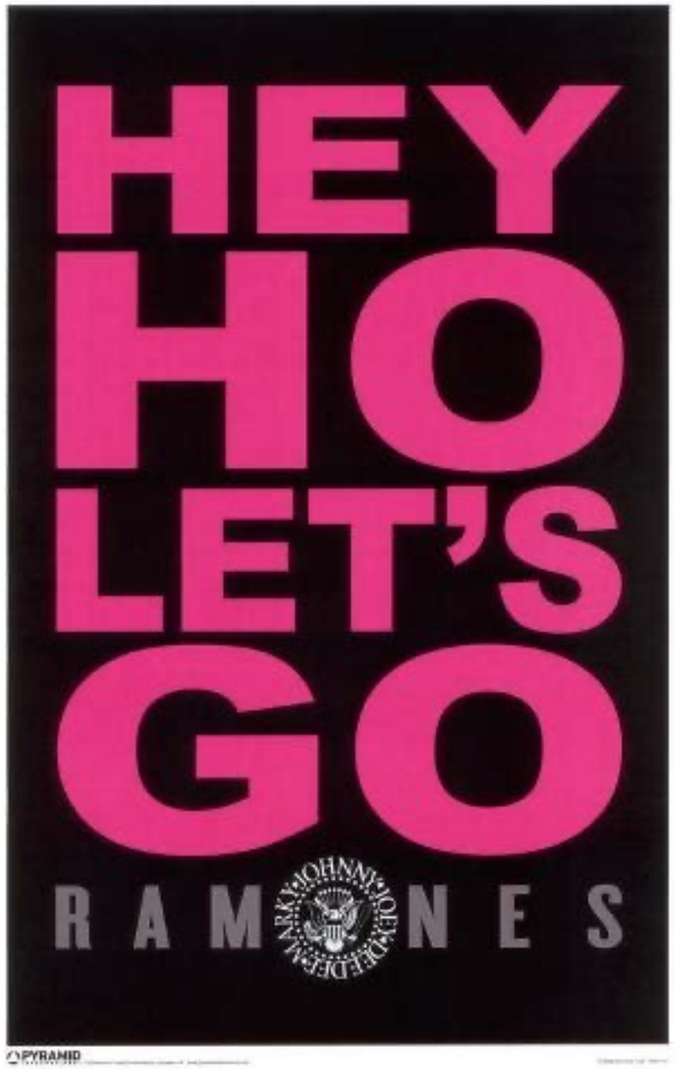
Debunk the myth…..

1. Offensive security engineers can work at hundreds of companies and thrive
2. Ethical hacking is safe when done right
3. Careers are well paid
4. There are many opportunities to pivot – CISO, forensics, compliance, defense, policy, or management

Call to Action

What can I do?

1. Identify mentorship opportunities
2. Request a generous training budget
3. Send your interns to BH Asia next year!



Thank you!!

Please stay in touch

linkedin.com\mika.devonshire

@cybermeeks