Univerza *v Ljubljani*
Fakulteta *za računalništvo*
in informatiko

Outline of the course

doc. dr. David Modic

21.10.2020

whoami

- dr. David Modic, an economic psychologist.
- Fluidly employed at FRI (waiting for habilitation)
- CEO of Cambridge Red Queen Systems (https://crq.systems).
- Previously:
    - Researcher at the Computer Laboratory, Cambridge University.
    - Deputy Head CamCERT (social engineering).
    - Honorary Graduate Fellow at the University of Exeter.
- In practice, I deal with security incidents, research which mechanisms work well in social engineering, and what kind of people hackers are.
- Web page: https://david.modic.org.uk
- mailto: david.modic@fri.uni-lj.si
- Slack: https://frisecurityteam.slack.com/
- ICQ: 686777259

Why would you want to listen to what I say?

- I started working with computers in the early eighties.
- Finished high school for computer sciences.
- Was employed as a sysadmin in various NGO's.
- Ran a Games Development company - CEO, project lead, storyline lead - http://sinistersystems.com
- Started researching cyberspace in 1999.
- Hold a PhD in psychology of cybercrime.
- Worked in the oldest computer laboratory in the world for five years.
- Lectured and consulted all over the world (Japan, Brasil, the US, the UK, Estonia, Luxembourg etc).

- But enough about me, let's talk about the course.

The AIM of the course

- The aim of the course is to familiarize yourselves with INFOSEC, understand what is involved, and what the buzzwords (like INFOSEC) mean.
- We will do lots of practical examples.
- You will not get a PEN TESTER certificate in the end.
- You will not learn how to write 0-day exploits or malware.
- But you will learn threat modelling and how to discover attack vectors. You will also learn the steps of the process and what they involve.

The course

- We will meet eight times.
- Final presentation **in mid January 2021**
- There will sometimes be homework (like today ☺).
- Mostly, I will present, but sometimes you will.
- I will mark your homework and presentations. They will constitute 50% of your final grade.
- Because of the small class, this will be less about lectures and more about mentoring.
- The schedule is on the next slide.

Important dates

- **21.10.** Outline of the course and cyber ethics.
- **28.10.** The PENTESTING process and breach databases.
- **04.11.** Open Source Intelligence (OSINT) gathering and reporting.
- 11.11. NO LECTURE
- **18.11** Shodan hacking (you present). + **18.11** Metasploit (you present).
- **25.11** Human attack vectors.
- **02.12** Team assignment and rules of engagement.
- **13.01** Final Presentation.

More general info on the course

- Final presentation will be a team effort. You will receive a target, write a plan and execute it.
- For the presentations, you will get pointers and starting literature. Practically all hackers are autodidacts.
- You will then present to your fellow students and to me (and possibly the stakeholders).
- At the end of today, I will ask for volunteers to take on the assignments. Please do volunteer.

Operational aspects

- Feel free to use Slack (https://frisecurityteam.slack.com/) for communications. In fact, I'd prefer it.
- You will get access to a fully functioning KALI Linux installation containing the latest breach database. Instructions on how to access it and your login credentials will be available by the time we meet next.
- **At no point in time are you allowed to do active attacks unless expressly permitted by me. Ignoring this leads to flunking the course and potentially going to jail! If you don't know what active attacks are, they will be explained on the 28th.**
- *Once you get access to the breach database, please do not download it. Trust me, I will notice you doing it. Do not be fancy, steal someone else's credentials and then attempt to download it as if you are them. Use this creative energy to do your assignments.*

Operational aspects II.

- With great power comes great responsibility.
- There is an obvious temptation to monetize the breach data.
- **You will retain access to the breach database until the end of term.**
- We will define the scope and rules of engagement for our targets. Do not overstep, please.

Any questions?

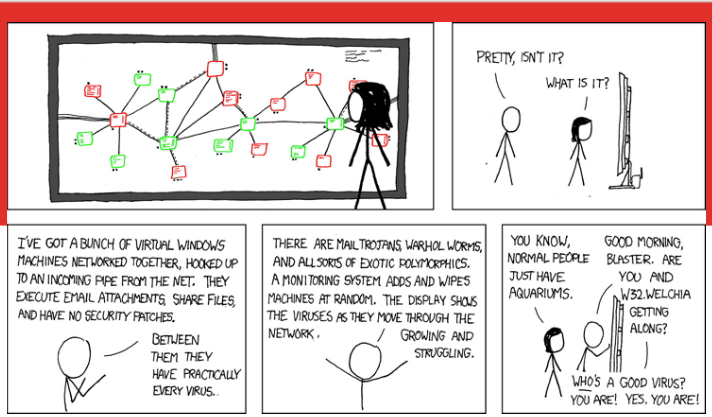
- Go ahead, ask. Please do not worry about your English. No one is judging you. If they do, that means they are even more insecure than you.
- …
- Let’s do a short break of say 10 minutes? And go on to the next phase.

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Ethics in cybersecurity

doc. dr. David Modic

21.10.2020


PRETTY, ISN'T IT?
WHAT IS IT?
I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS..
THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK,
GROWING AND STRUGGLING.
YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!

What is this talk about?

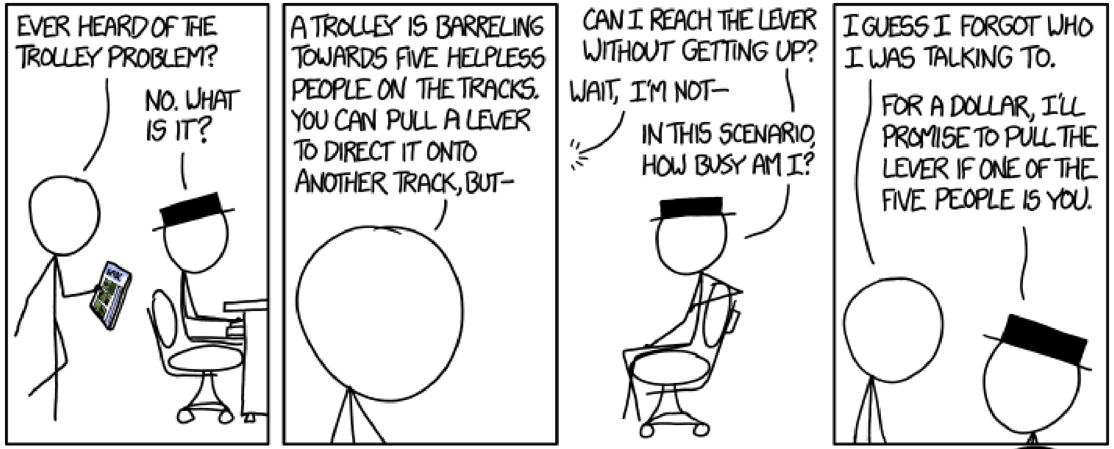
- We'll talk about Ethics in Informational Security (INFOSEC).
  - Origins of ethics
  - Distinction between laws and ethics
  - How do ethics apply to hacking?
  - Game theory and hacking
- Case studies.
- Practical advice.

Why would we want to talk about Ethics in INFOSEC?

- The blackhat anecdote.
- Most of the talk will be about *why*, not *what* ☺.
- This is not a talk about Ethics in general. There are other modules about that at FRI. Anže attended one. I know, I was there.

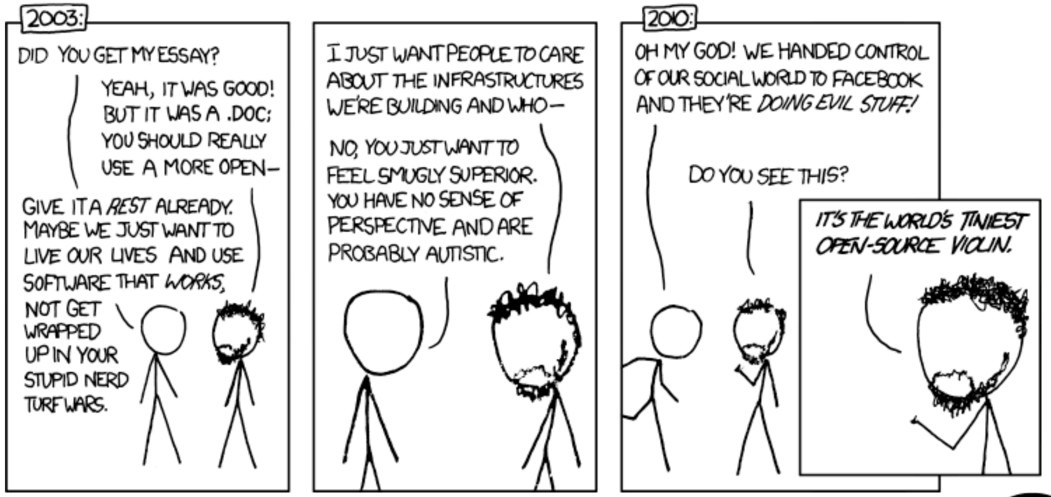
General postulates

- This is emphatically not a lecture on how to be a decent human being. **I will not be moralizing**.
- It is also not a sermon. *Good and Evil* will not feature highly.
- I would like to be direct and up-front about Ethics.


EVER HEARD OF THE TROLLEY PROBLEM?
NO. WHAT IS IT?
A TROLLEY IS BARRELING TOWARDS FIVE HELPLESS PEOPLE ON THE TRACKS. YOU CAN PULL A LEVER TO DIRECT IT ONTO ANOTHER TRACK, BUT–
CAN I REACH THE LEVER WITHOUT GETTING UP?
WAIT, I'M NOT–
IN THIS SCENARIO, HOW BUSY AM I?
I GUESS I FORGOT WHO I WAS TALKING TO.
FOR A DOLLAR, I'LL PROMISE TO PULL THE LEVER IF ONE OF THE FIVE PEOPLE IS YOU.

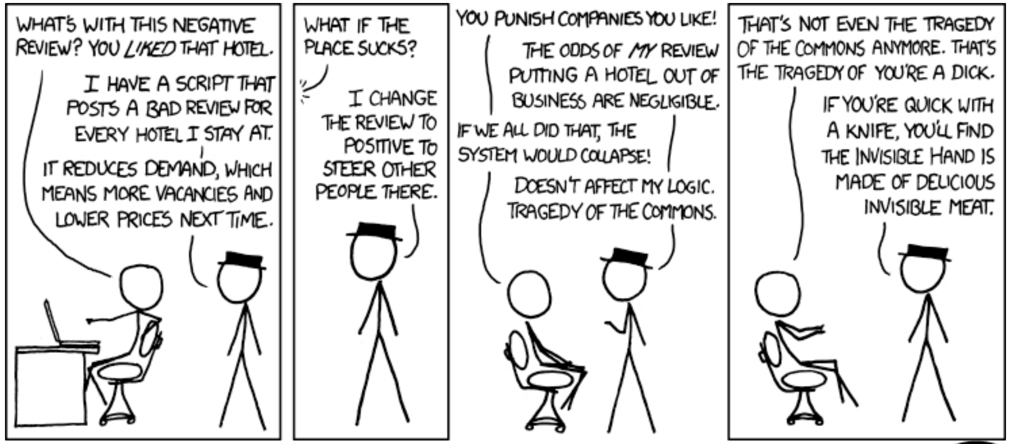
Definitions

- Ethics according to the Oxford English Dictionary: *“Moral principles that govern a person's behaviour or the conducting of an activity.”*
- BUT! *“I said that this will not be about moralizing!“*
- True. So let’s break it down a bit.


2003:
DID YOU GET MY ESSAY?
YEAH, IT WAS GOOD! BUT IT WAS A .DOC; YOU SHOULD REALLY USE A MORE OPEN—
GIVE IT A REST ALREADY. MAYBE WE JUST WANT TO LIVE OUR LIVES AND USE SOFTWARE THAT WORKS, NOT GET WRAPPED UP IN YOUR STUPID NERD TURF WARS.
I JUST WANT PEOPLE TO CARE ABOUT THE INFRASTRUCTURES WE'RE BUILDING AND WHO—
NO, YOU JUST WANT TO FEEL SMUGLY SUPERIOR. YOU HAVE NO SENSE OF PERSPECTIVE AND ARE PROBABLY AUTISTIC.
2010:
OH MY GOD! WE HANDED CONTROL OF OUR SOCIAL WORLD TO FACEBOOK AND THEY'RE DOING EVIL STUFF!
DO YOU SEE THIS?
IT'S THE WORLD'S TINIEST OPEN-SOURCE VIOLIN.

“*Moral principles…*” / So what is morality?

- Morality (from Latin: *mōrālis*; proper behavior).
- Morality is a set of rules defining which behaviour is proper and which isn’t.
- Commonly defined: *moral -> good. Immoral -> bad.*
- OK, but who defines *what is moral*?

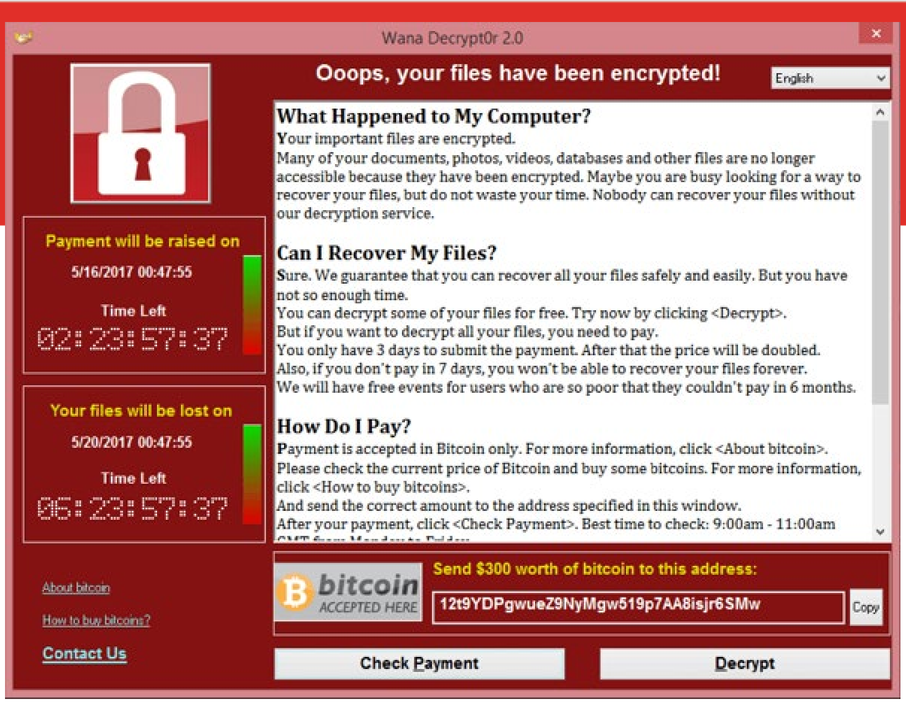

WHAT'S WITH THIS NEGATIVE REVIEW? YOU LIKED THAT HOTEL.
I HAVE A SCRIPT THAT POSTS A BAD REVIEW FOR EVERY HOTEL I STAY AT.
IT REDUCES DEMAND, WHICH MEANS MORE VACANCIES AND LOWER PRICES NEXT TIME.
WHAT IF THE PLACE SUCKS?
I CHANGE THE REVIEW TO POSITIVE TO STEER OTHER PEOPLE THERE.
YOU PUNISH COMPANIES YOU LIKE!
THE ODDS OF MY REVIEW PUTTING A HOTEL OUT OF BUSINESS ARE NEGLIGIBLE.
IF WE ALL DID THAT, THE SYSTEM WOULD COLLAPSE!
DOESN'T AFFECT MY LOGIC. TRAGEDY OF THE COMMONS.
THAT'S NOT EVEN THE TRAGEDY OF THE COMMONS ANYMORE. THAT'S THE TRAGEDY OF YOU'RE A DICK.
IF YOU'RE QUICK WITH A KNIFE, YOU'LL FIND THE INVISIBLE HAND IS MADE OF DELICIOUS INVISIBLE MEAT.

Who defines Morality and, as a consequence, Ethics?

- If someone defines morality, then the definition is dependent on the culture.
- If that is true, then all of this is moral:
  - Female children (15 yo) are forced into marriage with an unknown man (most of the U.S.).
  - Removal of female clitoris before the age of five (FGM).
  - Limb amputation for stealing (e.g. a loaf of bread).
  - Religious environmental noise pollution (Church bells / muezzins).
  - Torture and killing of homosexuals in the Russian federation (e.g. Czechnya 2017).
  - Hacking and destroying Ukrainian infrastructure in order to make it an easy target for Russian invasion (WannaCry and notPetya).
- Let's do a short detour and talk about WannaCry and notPetya.

Univerza *v Ljubljani*
Fakulteta *za računalništvo*
in informatiko

Wannacry



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

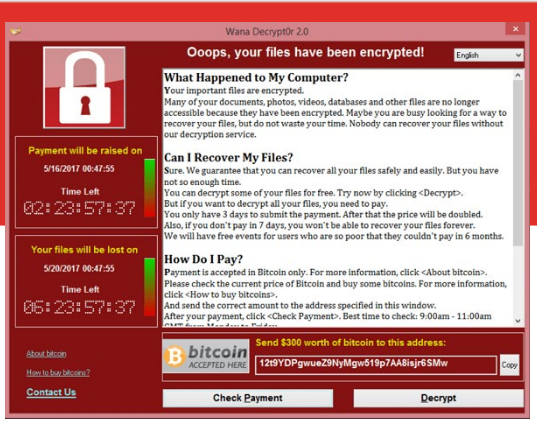
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

- Widespread in May 2017.
- Ransomware cryptoworm.
- Spread by port scanning and exploiting the flaw in SMB protocol.
- Infected > 300.000 computers worldwide.
- Demand $300-$600 in bitcoin.
- Targeted all versions of windows.
- Well known vulnerability. Not a 0-day by a long shot.

Wannacry – What was it about?



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

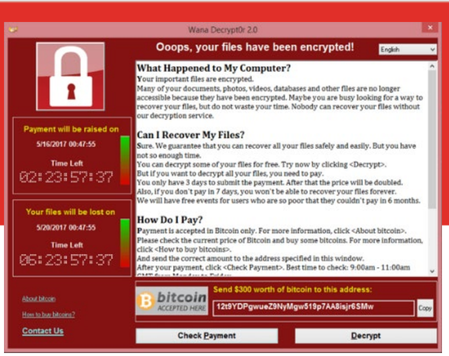
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

- Was it about money? 300K machines, \$300-\$600 ransom. Lots of bitcoin, right?
  - According to @actual_ransom (https://mobile.twitter.com/actual_ransom/), the whole campaign yielded ~**52BTC** (~\$131.000 at the time).
- There are documented cases where the group claiming responsibility ("The Shadow Brokers") let people off without paying.
- Did people think this was about money? Yes.
- Did they later think the campaign was half-baked and full of holes? Yes.
  - A quickly discovered kill switch.
  - No way to differentiate payees.
  - Decryption keys leaked.



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

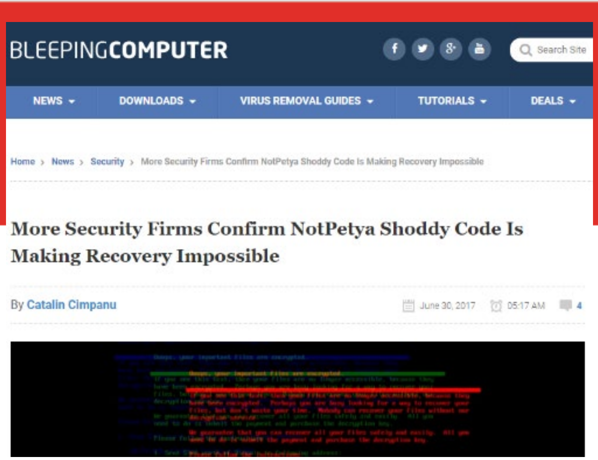
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Wannacry – Was it flawed, and about financial gain?

- Not a big financial gain.
  - And yet, the general consensus: **it was about money, but badly run**.
- No one blames the state actors.
- And then, notPetya appears.
- notPetya uses similar exploits, but the ransomware part is even more of a joke – the BTC address is wrong, notPetya actually destroys the data.
- WannaCry is a prototype for notPetya, notPetya is used to attack Ukraine's infrastructure.
- And yet the headlines in respectable press are about how incompetent hackers were, because they botched WannaCry, and shoddily executed notPetya - it always destroys your data, regardless of payment.

notPetya, an even bigger mess?


BLEEPINGCOMPUTER
Search Site
NEWS
DOWNLOADS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
Home › News › Security › More Security Firms Confirm NotPetya Shoddy Code Is Making Recovery Impossible

More Security Firms Confirm NotPetya Shoddy Code Is Making Recovery Impossible

By Catalin Cimpanu June 30, 2017 05:17 AM 4

Ooops, your important files are encrypted.

- notPetya uses similar exploits to WannaCry, but the ransomware part is even more of a joke – the BTC address is wrong.
- notPetya actually destroys the data (throws away the decryption key).
- WannaCry is a prototype for notPetya, notPetya is used to attack Ukraine's infrastructure.
- And yet the headlines in respectable press are about how incompetent hackers were, because they botched WannaCry, and shoddily executed notPetya.

WannaCry and notPetya

- Is there a connection between notPetya and WannaCry?

They use the same exploit. Only now, the world is protected against it. Well, most of the world. Except Ukraine, for example, where they frequently [illegible] was never [illegible] software [illegible]

- But, *notPetya* has no kill switch as WannaCry did! They are different!

Yes, because when you want to test malware, you want to be able to stop it infecting your machines. Once Microsoft has issued a patch, then only pirated software is vulnerable. And Microsoft has protected you.

- But both WannaCry and notPetya were horrible at extracting money. WannaCry had no way of detecting who paid for which machine. And notPetya was even worse – they did not keep the decryption keys, and the bitcoin address was wrong. Clearly incompetence. Right?

There is no proof of this, but if I was the attacker, I would make sure to gain funds in the first place, only to destroy the data and hobble infrastructure. In that case WannaCry was a proof of concept and notPetya the real thing.

- But how did the hackers then get any money out of this?

The Russians paid them.

- OK, so your conspiracy theory is that Russia is behind this? This is clearly false, they got attacked too!

They reported attacks, yes, to some oil companies. It is unclear what was actually attacked in Russia. Ukraine was however brought to its knees. [illegible] That I could claim I was a victim, and complain about the over-reach of the NSA at the same time. If I was government, I would attack my people who are getting too big for their shoes (like oil/gas tycoons) and then blame the NSA.

WannaCry / notPetya and Ethics

- In Russia, the people who launched WC and !P got medals. Therefore, to Russians, this was a moral and proper thing to do.
- Morality is context / culture dependent.

OK, but is all morality dependent on the culture?

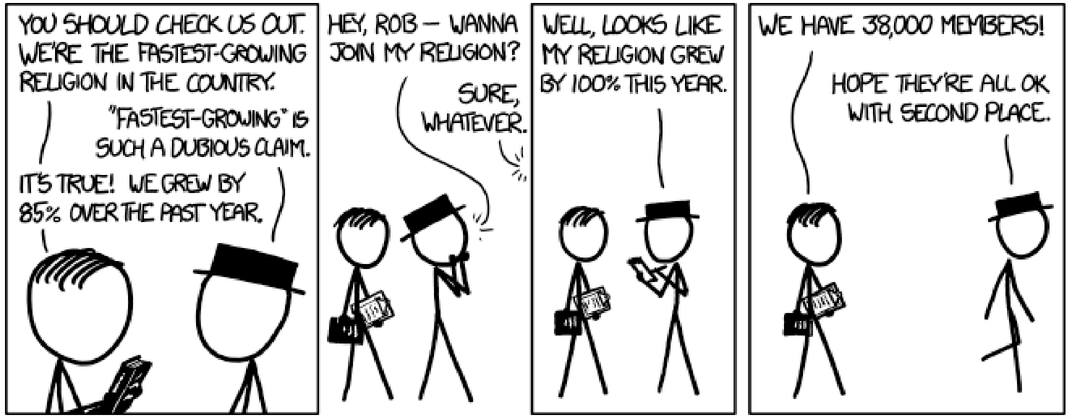
- There are still universal morality guidelines, are there not? For example:
  - War crimes (hmm… is Baghuz a warcrime?). Also, Palestine. Warcrime?
  - Murder
  - Slavery
  - Selling people for spare parts
  - Taboo transactions (Fiske & Tetlock, 1997)

Many morality theories exist…

- One theory on morality would be Kohlberg's (1958).
- Simply put, these are the stages:
  - Initial morality derived from parents' moral system.
  - In primary school teachers and peers add to moral reasoning.
  - Global morals (rules that are universally acceptable).
  - Post-conventional morals (I know what morality is based on previous stages, and construct my own moral principles on that).

Get back to INFOSEC!

- *Wait, what? Universal morals get broken all the time!*
- …and people who do this might not consider it immoral, even if it is against the law.
- **Also, what connection is there between this and hacking?**
- *Bear with me.*


YOU SHOULD CHECK US OUT. WE'RE THE FASTEST-GROWING RELIGION IN THE COUNTRY.
"FASTEST-GROWING" IS SUCH A DUBIOUS CLAIM.
IT'S TRUE! WE GREW BY 85% OVER THE PAST YEAR.
HEY, ROB – WANNA JOIN MY RELIGION?
SURE, WHATEVER.
WELL, LOOKS LIKE MY RELIGION GREW BY 100% THIS YEAR.
WE HAVE 38,000 MEMBERS!
HOPE THEY'RE ALL OK WITH SECOND PLACE.

Norms

- There seems to be a discrepancy between laws, and morals/ethics.
- They are not always aligned.
- Let's introduce the concept of norms.

Norms

- Norms are: a set of rules that govern a particular society.
- They are:
  - Formal – Laws and ordnances
  - Informal – social guidelines of what is considered acceptable.
- Sometimes, they do not align.
- When they don’t, people from a given culture generally support the informal norms and complain about how formal norms are stifling and un-lifelike.
- Examples on next slide.

Norms clash

- Examples:
  - Martin Krpan
  - Sir Arthur Harris
  - Smoking ban in EU.
  - Eating or drinking while driving (UK)

Norms and sanctions

- All norms include sanctions for non-compliance.
- If there is no penalty for not observing norms, then they are *suggestions*, and not norms.
- Formal norms are sanctioned through the legal system. Breaking the formal norms (laws) is an offence and legal sanctions follow.
- Breaking informal norms is punished too.
- The sanctions include ostracism and expulsion from the social networks, guilds, etc.

Formal norms pertaining to cyber-crime in Slovenia

- Misrepresenting yourself as an uniformed individual carries up to 1 year prison sentence each time (penal law KZ-1, article 305).
- Identity theft is treated as abuse of personal data – up to 3 years prison sentence.
- Stealing corporate IP carries 3-5 years prison sentence for the thief and 1-3 years for the person who enabled it (1 year if malfeasance, 3 years if malicious).

So, where are we?

- Norms (formal and informal) guide the perception of what is *moral*.
- *Moral acts* are perceived as *Ethical*.
- Therefore ethical behaviour means acting according to written and unwritten rules of a society.
- How is that applicable to security?

Anecdotal Attitudes (ethical hacking)

- A colleague of mine, a brilliant pen tester and an ethical hacker of some renown (winner of several MIT hacking challenges, etc). Said this in conversation: ”*I do not believe in the concept of ethical hacking at all. We are all just using tools. It is like saying that guns kill people. … After all, there is no ethical accountancy or ethical psychology courses taught. It is just accountancy and psychology, right?*”

- Let’s pick this apart, a bit.

Anecdotal Attitudes (~~ethical~~ hacking)

- *" … After all, there is no ethical accountancy or ethical psychology courses taught. It is just accountancy and psychology, right?"*
- There are courses available both in ethical accountancy, and ethical psychology.
- The first book on accounting was published in 1494 and it includes ethical guidelines for accountants.

Anecdotal Attitudes (~~ethical~~ hacking)

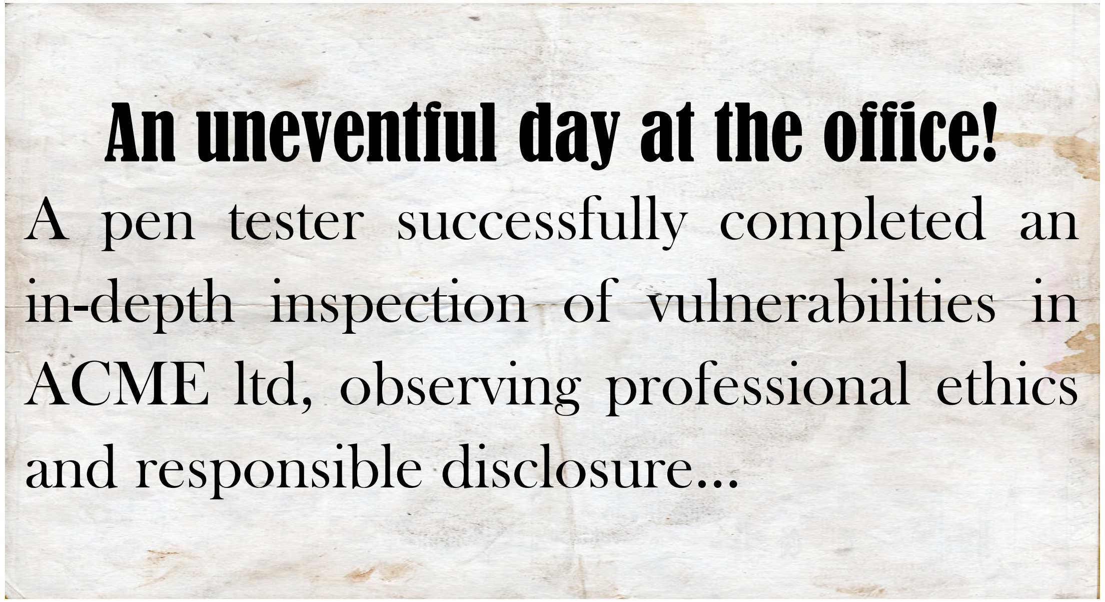
- In psychology observing professional ethics serves several purposes:
  - Not spoiling it for the next guy (If we abuse people in experiments, then, eventually, we will run out of participants).
  - Unethical behaviour devalues research findings through introduction on added uncontrolled variables (mistrust, anger towards the experimenter, skewed responses…).
  - Avoiding potential legal action.
  - Continued membership in the guild of psychologists.

Anecdotal Attitudes (~~ethical~~ hacking)

- Saying that merely using tools absolves you from moral responsibility shows a fundamental misunderstanding of how norms work.
- It is safe to assume that the general population isn't overly informed about the taxonomy of hackers.
- Do you want to know *why I* think that?

Public perception

- Here is an example of two (semi-fictional) headlines. Which one do you think is more likely to be published?



An uneventful day at the office!

A pen tester successfully completed an in-depth inspection of vulnerabilities in ACME ltd, observing professional ethics and responsible disclosure...

Digital Hell!

Hackers are stealing your privacy! You are all exposed and your porn viewing habits will be shown to your wife and neighbours!

Public perception

- Let's look at a brief clip form the movie "*The fate of the furious (2017)*".

Public perception

- Let's look at a brief clip form the movie "*The fate of the furious (2017)*".
  - *"Even anonymous won't touch her?"*
  - *"I want every 0-day exploit chip"? "Hack them all"?*
- This is hilarious. But people watch this. And nod, sagely.
- Do not assume that there are many examples in the media where hackers are portrayed as anything else but a "*digital act of God*".
- I can only think of one recent show, which was technically sound – *mr. Robot.*
- And still, the hackers in *mr. Robot destroy the world.*

Are hackers evil?

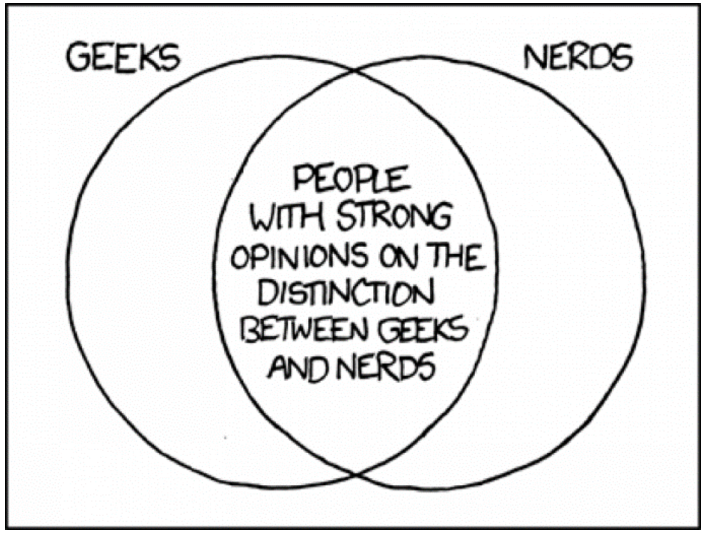
- Because there are only scary stories that are reported or portrayed, the informal norm is that all hackers are *evil*.
- Saying that all hackers are the same does not mean that the general public will now think everyone is a *White hat*.
- Therefore this attitude means a *Black hat* runs afoul of both formal and informal norms and a *White hat* is condemned through informal norms.

Dichotomy

- We have a nice dichotomy here:
  - The formal norms distinguish between *(a) unauthorized*, and *(b) authorized* access of a computer system.
  - The informal norms of the general population do not. "*All hackers are evil!*"
  - The informal norms of the hacking community are apparently flexible on this topic - *"Hacking is a skill, regardless of how it is used."*

Norms and hacking community

- The hacking community has two options (in order to not feel bad):
  - Hackers thrive in marginalized groups where skill = reputation
  - Hackers invent ways of rationalizing their actions in order to avoid thinking they are doing something bad (in the eyes of the public).
- But do hackers actually rationalize?

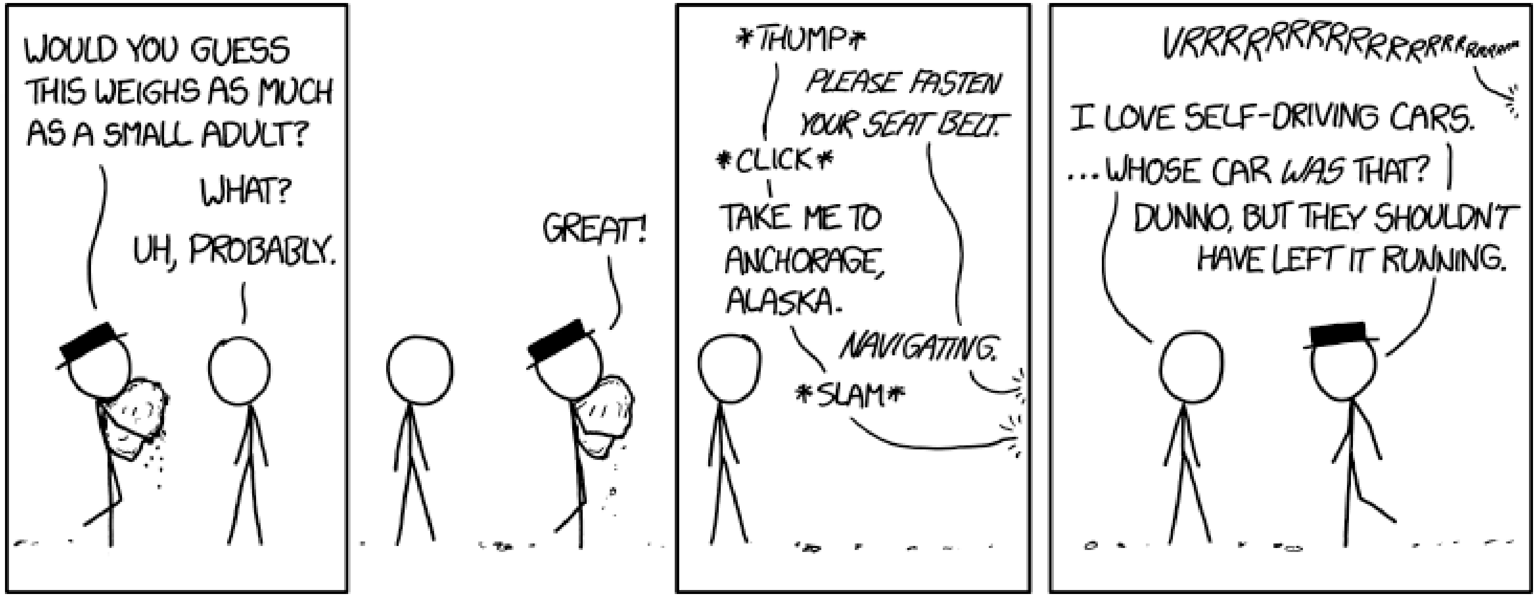

GEEKS
NERDS
PEOPLE WITH STRONG OPINIONS ON THE DISTINCTION BETWEEN GEEKS AND NERDS

What is a “rationalization”?

- *Rationalization* is a defense mechanism designed to appear to logically justify behaviours that are controversial (Freud, 1991).
- Rationalizing is common in Internet Fraud:
  - *Techniques of neutralisation* (Sykes and Matza 1957) scammers reduce their own inhibitions and make their actions morally justified (in their minds), using vocabularies of adjustment (Cressey 1953).
- The vocabulary of adjustment might also work among hackers.

Justifying (un)authorized access

- There is not much research available.
- Luckily we've done some at Cambridge.


WOULD YOU GUESS THIS WEIGHS AS MUCH AS A SMALL ADULT?
WHAT?
UH, PROBABLY.
GREAT!
THUMP
PLEASE FASTEN YOUR SEAT BELT.
CLICK
TAKE ME TO ANCHORAGE, ALASKA.
NAVIGATING.
SLAM
VRRRRRRRRRRRRRRRrrrrrrrr
I LOVE SELF-DRIVING CARS.
...WHOSE CAR WAS THAT?
DUNNO, BUT THEY SHOULDN'T HAVE LEFT IT RUNNING.

Experimental outline

- **N = 4136** (two waves, raw N1 = 6025, raw N2 = 3346)
- Removal of (a) empty responses, (b) those who answered < 50% Offending and (c) <50% psychometrics -> results in removal of 5235 responses.
- Looking at people who reported to be offenders in cybercrime.

Brief analysis I.

- Descriptives of the new DV's show that there are still very low numbers active offenders.
- We'll take the results with a grain of sand, but they might indicate trends, still.
- Initial multiple regression (Offender Progress x Individual * corporate) shows:
  - Low explained variance, but regression is significant.
  - Both factors influence offending by a significant amount (p < .001).

- INTERPRETATION -> Black hat offenders are more likely to rationalize their actions, to make what they are doing OK.

Thus, Black hats do actually rationalize their actions.

Brief analysis II.

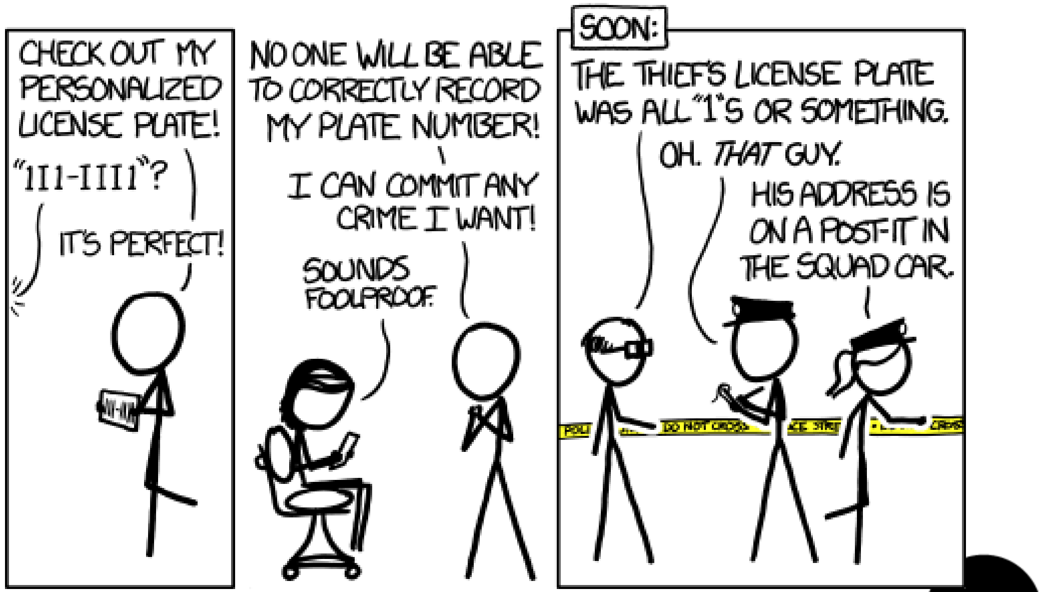
- We have done another MR (**Offender Progress x Motivational items**).
- Stepwise regression converged in seven steps. Significant (p = .01). **15%** of variance explained.
- Seven regressors remained. All significant (p range **.014** to **< .001**).
- **Interpretation -> Those who are better at finding a justification for their action(s) are more likely to engage in black hat activities.**
- Summary: **The ability to rationalize ones actions as excusable or moral is one of the driving forces in unauthorized access to computer systems!**

So where are we now?

- Norms (formal and informal) guide the perception of what is moral.
- Moral acts are perceived as ethical.
- Therefore ethical behaviour means acting according to written and unwritten rules of a society.
- Is that applicable to security and hacking?
- YES, clearly from the experiment. But do these rationalisations work?

The myth of the perfect crime

- In psychotherapy, there is the concept of the *Myth of a perfect crime*.
- Most of us get disabused of this by the age of five or so.
- But, do hackers?


CHECK OUT MY PERSONALIZED LICENSE PLATE!
"1I1-I1I1"?
IT'S PERFECT!
NO ONE WILL BE ABLE TO CORRECTLY RECORD MY PLATE NUMBER!
I CAN COMMIT ANY CRIME I WANT!
SOUNDS FOOLPROOF.
SOON:
THE THIEF'S LICENSE PLATE WAS ALL "1"S OR SOMETHING.
OH. THAT GUY.
HIS ADDRESS IS ON A POST-IT IN THE SQUAD CAR.
DO NOT CROSS

Let’s get back to the conversation with my hacker friend

- D(avid): …. There is a myth of a perfect crime. But it is a myth.
- H(hacker): Is it?
- D: Yes. It is unlikely one will get away with it, long term.
- H: Only stupid people get caught.
- D: Operational security is hard.
- H: Still, some people never get caught.
- D: Perhaps the problem is in the definition. A perfect crime is a crime with no consequences to you.
- H: YES, agreed.

(continued on the next slide)

The conversation with my hacker friend (cont.)

- D: Well, even if you are not caught, but you need to be constantly on the lookout, and you need to move to an island in the Carribean, and you cannot have a relationship, and have to have a go-bag constantly packed… Surely you cannot claim that these are not consequences of your action impacting you?
- H: I wouldn't mind any of that.
- D: That is not the point. You are mixing consequences of breaking formal norms with consequences of breaking informal norms. It does not matter whether you mind this or not.
- H (*is quiet for a bit*): Look, I have work to do. Is there anything else you wanted to discuss?

D leaves. This conversation happened. Honest to God.

Summary

- Pretending that ethics are not applicable to hacking is *pointless.*
- Ignoring this has consequences.
- (potentially) being caught is a corollary of breaking formal norms (laws).
- Substantially changing your lifestyle is a corollary of avoiding the consequences of breaking informal norms.

Summary (cont.)

- If breaking informal norms was not a problem, *then there would be no need to find excuses for it*. Empirically, that is clearly not true. Blackhats do attempt to find an excuse for their actions.
- Therefore not observing ethics in hacking is problematic, whether we pin this on the premise of good and evil or not!

You See? I told you I would not be moralizing or sermonizing in this lecture.

Self-interest

- We can construe any black-hat activity in the context of game theory / 0 - sum game.
  - On one side is the potential profit.
  - On the other is the likelihood of getting caught, and the consequences.
- *Does the potential profit outweigh the likelihood of getting caught (fairly high as is), and the substantial change of lifestyle in order to not increase the likelihood of getting caught?*
- **Corollary: Is being an ethical hacker in your best interest or not?**
- No need to answer that out loud.

In practical terms

- <u>There is no crime without consequences to your lifestyle</u>.
- If you do not break the law, you are safe from official prosecution.
- But, unauthorized access is against informal norms, regardless of what excuse one comes up with it (see empirical proof).
- Regardless of whether you see yourself as a decent or bad human being* observing ethics is in your best interest.

So what do you do?

- Unauthorized access is unethical and against the law.
  - *Therefore, get authorized access – i.e. do penetration testing.*
- Disclosing or selling secrets without following the proper procedure is unethical and against the law.
  - *Therefore stick to the rules of engagement and the scope. Do not access OOS areas. And never save any corporate or individual IP on your machine!*

So what do you do II. ?

- In a practical sense:
  - Know the law.
  - Stick to the agreement.
  - Get authorization for pen testing.
  - Unless expressly allowed, never use active measures.

Questions?

(we are not done yet ☺)

Homework (send it to me by Wednesday **26.10.2020 @ 12:00**)

- General notes on homework.
  - No need to be wordy. Concise is fine. For homework 1, I will actually tolerate bullet points (but won't be ecstatic about it).
  - The general essay writing rules apply (each paragraph about a separate topic, flow, parsimony, double spaced, avoid fluff).
  - No need to go past 500 words.

Homework (send it to me by Wednesday **13.03.2019 12:00**)

- **Part 1. A thought exercise.**
- Think of a company / person / Institution, that you would like to attack. Tell me about it, and why they would be a good target.
- Describe in a step by step fashion, how you would go about compromising the target, and what would your final goal be. From the beginning. Briefly describe each step, i.e. *(a) I would google the company to find out their domain name. (b) I would look at budget reports to see who the board members are. (c) I would find the emails of the board members. etc.*
- **DO NOT DO ANY OF IT. Not even a little. Not even for fun.**

Homework (send it to me by Wednesday **13.03.2019 12:00**)

- **Part 2. Analysis**
- Look at your report. Look at all actions described there.
- List which laws you would be breaking at each step and what the prison sentences are for these offenses, i.e. *steps (a) … (e) not breaking any laws. (f) identity theft, up to 3yrs * 2, (g) breaking and entering, up to 2yrs….*
- Add the per partem sentences and report them.
- For bonus points, think about which informal norms you would be breaking, and list them.

Two presentations are going spare

- **Who wants to present Shodan hacking?**
- **Who wants to give an overview on Metasploit?**
- This is a safe space. No one will laugh at you. If they will laugh, they will laugh with you.
- No one is born with this knowledge. However, at this level, you are expected to be able to research stuff on your own. If you are reluctant to commit now, I can ask you again at the **next lecture 28.10.**

Next time…

- **Next lecture is 28.10.2020 at 16:30**
- We will talk about the process of pen testing and its pitfalls in the first part.
- In the second part, I will introduce you to the breach database, give you access and let you play around with it.
- See you in a week!

Univerza *v Ljubljani*
Fakulteta *za računalništvo*
in informatiko

www.fri.uni-lj.si

www.facebook.com/ulfri