Vulnerability disclosure and computer crimes

Ben Creet

For CYBR171 May 2023

#whoami

Ben Creet (aka Creeture)

- I'm a cyber security & policy professional
- Vice chair & treasurer of the New Zealand Internet Task Force
- information security awards of NZ (iSANZ) board member
- I led NZITF's work in 2013 on vulnerability disclosure

- $dayjob: National Cyber Security Centre: principal adviser, support our strategy & standards work (e.g. NZISM)

Today we're talking about...

Computer Crimes

What hacking and computer "stuff" is a crime in the Crimes Act?

Vulnerability disclosure

A practice that has built up over 20 years about what to do when you find a vulnerability in someone's public systems.

Why are we talking about this?

Actions have consequences

- You are in your first year of cybersecurity study
- You've learnt a bit about a lot
- But a little knowledge is a dangerous thing

Arm you with tools

if you ever do find vulnerabilities

1

Computer Crimes

What's what, what's not

DISCLAIMER

- I am not a lawyer
- views are my own

Computer Crimes

- The Crimes Act 1961 lists most crimes in Aotearoa New Zealand

  In 2003 it was amended to introduce specific computer crimes

  - s248 - s252
  - Penalties go up to maximum imprisonment of 10 years

248 Interpretation

For the purposes of this section and sections 249 to 252,—

access, in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system

authorisation includes an authorisation conferred on a person by or under an enactment or a rule of law, or by an order of a court or judicial process

computer system—

(a) means—

(i) a computer; or

(ii) 2 or more interconnected computers; or

(iii) any communication links between computers or to remote terminals or another device; or

(iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and

(b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.

S248: what does it mean

An interpretation section. It provides definitions and a scope for the following crimes.

tl;dr: Any use of a computer is within scope of these crimes

249 Accessing computer system for dishonest purpose

(1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—

(a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

(b) causes loss to any other person.

(2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,—

(a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

(b) to cause loss to any other person.

(3) In this section, **deception** has the same meaning as in section 240(2).

Section 249: replaced, on 1 October 2003, by section 15 of the Crimes Amendment Act 2003 (2003 No 39).

S249: what does it mean?

- Stealing something from someone else's computer with intent = <7 years
- Access a computer with intent to steal = <5 years
  (note, doesn't require successful theft)

What is copying data from a computer without permission?

250 Damaging or interfering with computer system

(1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.

(2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or

(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or

(c) causes any computer system to—

(i) fail; or

(ii) deny service to any authorised users.

Section 250: replaced, on 1 October 2003, by section 15 of the Crimes Amendment Act 2003 (2003 No 39).

s250

DDoS is a crime

If you damage or DDoS a system and someone dies (e.g. power grid, brick a range of medical devices) then you can go to jail for 10 years

Recklessness counts

251 Making, selling, or distributing or possessing software for committing crime

(1) Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has in his or her possession for the purpose of sale or supply to any other person, any software or other information that would enable another person to access a computer system without authorisation—

(a) the sole or principal use of which he or she knows to be the commission of an offence; or

(b) that he or she promotes as being useful for the commission of an offence (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of an offence.

(2) Every one is liable to imprisonment for a term not exceeding 2 years who—

(a) has in his or her possession any software or other information that would enable him or her to access a computer system without authorisation; and

(b) intends to use that software or other information to commit an offence.

Compare: 1961 No 43 ss 216D(1), 229, 244

s251

This is the “cyber” version of s227 (car conversion) & s233 (possessing burglary tools).

Designed for catching criminal in planning. Needs intent to commit crimes.

Just having / owning Metasploit or running LinuxKali isn’t illegal.

252 Accessing computer system without authorisation

(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.

(3) *[Repealed]*

Section 252: replaced, on 1 October 2003, by section 15 of the Crimes Amendment Act 2003 (2003 No 39).

Section 252(3): repealed, on 13 July 2011, by section 5 of the Crimes Amendment Act 2011 (2011 No 29).

s252

It is illegal to access computer systems or Internet-connected information unless you have authorisation.

BUT

If you can access something from somewhere you already have authority then not a crime [untested]

What does THAT mean?

Cross-site scripting	*probably* legal
Direct object reference	*probably* legal
SQLi (unauthorised)	**not** legal (probably)

Reviewing computer crimes...

Apply to any use of a computer

s248 provides a VERY broad scope

Dishonest access is bad

Dishonest access to benefit or cause loss can lead to <7 years in jail

Damaging systems is worse

DDoS endangers life = <10 years

Reckless damage can still attract <7 years

Selling 0-day is bad

s251 is based on crimes for being caught with burglary equipment.

Probably could be applied to selling exploits / 0-days

Unauthorised access crime is broad

s252 applies to a lot and whether a crime has been committed will often turn on how 252(2) is interpreted

Computer crimes are complicated

Best not to become a “test case” for some lawyer

What is the Law?

How does that apply to me if I'm not trying to do crimes?

The law is three things:

1. *What statute says*
2. *What people **think** it says*
3. *What someone will **do** about it*

2

Vulnerability disclosure

Security industry practice when finding vulnerabilities

Vulnerabilities happen

That's why:

- people get employed to test and find vulnerabilities
- we make scanning and fuzzing tools
- we have patch cycles
- scanning happens (everywhere).

Security research is a whole thing

Full Disclosure vs Coordinated Disclosure

Coordinated disclosure

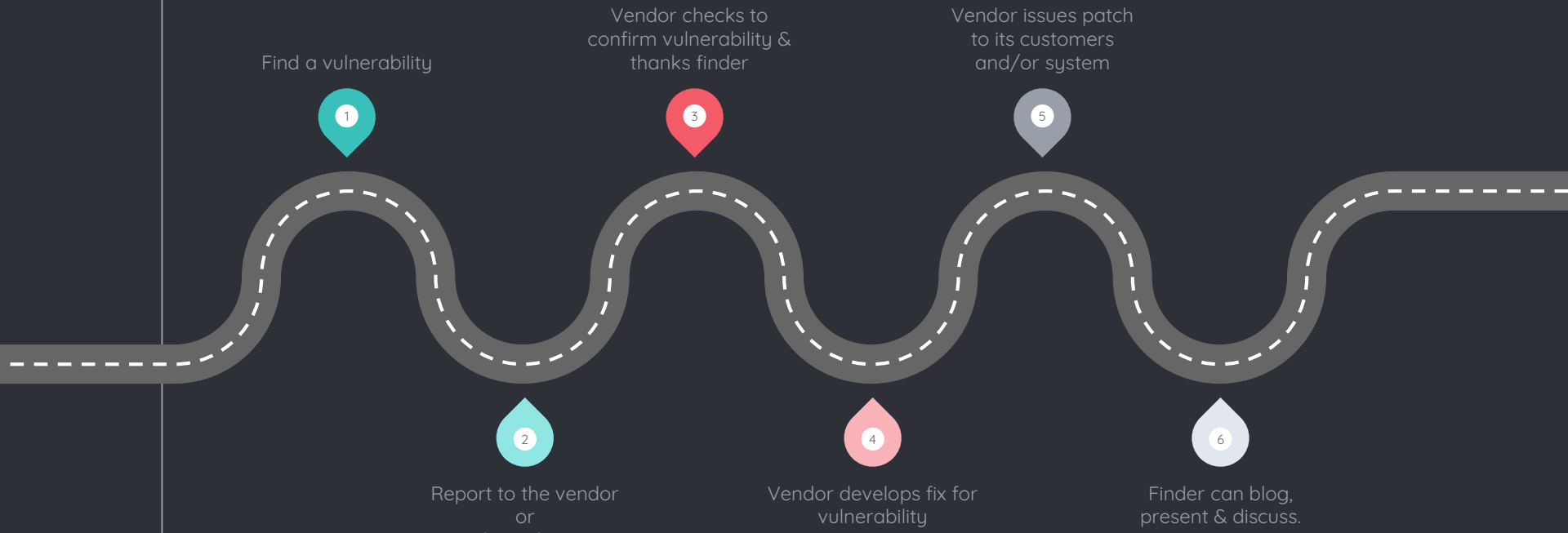
(aka responsible disclosure)
is researchers talking to companies AND companies fixing bugs

Full Disclosure

Tell the world (on twitter?)

Often end up talking to law enforcement

Coordinated disclosure roadmap



If you find a vulnerability

Keep it secret (keep it & yourself safe)

Document vulnerability

Report it to the vendor or system owner

- Do they have a policy? (security.txt)
- Is your vuln within scope?
- How do they want to receive vulnerabilities?

If you find a vulnerability

If they don’t have a disclosure policy?

= report to CERT NZ. Don’t try a cold approach

Answer questions and provide additional information if you can

Wait for the vendor or organisation to fix (or accept) the vulnerability (90 day window is industry standard)

You’re doing it wrong if…

- You are ‘disclosing’ the bug over twitter
- You tell other people before the vendor issues a patch
- You try and sell the vulnerability

Final tip: NEVER use the words “**or else**” (that’s blackmail)

If you find something REALLY bad?

- Contact CERT NZ:
  https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/

- If CERT NZ can't help:
  disclosures@nzitf.org.nz

Want to try new skills?

Home labs

Bug Bounties

BugCrowd

https://www.bugcrowd.com/

HackerOne

https://www.hackerone.com/

BigTech

Large tech companies run their own bug bounties

A final review

Security needs you

And will pay you well to do good, fulfilling work

Computer crime is complicated

The Computer Crimes in the Crimes Act can be unclear, and hard to understand

There is very little case law

Best not to become a “test case” for some lawyer

Vulnerability disclosure

Is the best way to deal with any vulnerabilities that you might find

A plug: NCSC is a great place to work

Women in STEM Scholarship

- The GCSB awards up to three scholarships a year.
- Find out more and apply here: https://beyondordinary.nzic.govt.nz/students/women-in-stem-scholarship/

GCSB Graduate programme

- Once you are finishing your studies you will want a job. GCSB has a great grad programme:
- https://beyondordinary.nzic.govt.nz/students/graduate-programme/

Thanks!

ANY QUESTIONS?

References

- Crimes Act 1961
- CERT NZ disclosure policy
- security.txt
- NZITF coordinated disclosure guidance
- New Zealand Information Security Manual | section 5.9
- ISO 29147 Vulnerability disclosure ($)
- ISO 30111 Vulnerability handling processes ($)