FULL DISCLOSURE

David C Frier
Atos
RSS - 2017

FULL DISCLOSURE: Topics

- About your speaker
- What is -- and is NOT -- a “hacker”?
- Cybercriminals and Researchers
- What is -- and is NOT -- a “zero-day”?
- Disclosure, Responsible and Otherwise
- Bug Bounties

About Your Speaker

- David C Frier, CISSP, CISM, CRISC, CCSK
- Client Security Manager for Atos, caring for Xerox's infrastructure

  ...but I speak only for myself, not for Atos!
- I've been doing Information Security for a dozen years
- I've been doing IT of one sort or another for Jack Benny's age
- Avid player of poker and Ingress, enthusiastic rider of a Trek.
- $FIRST.$LAST@{gmail.com | atos.net}
- Not on LinkedIn ...*but feel free to check my profile at Google+ if the Ambien has stopped working.*

What's a Hacker?

- Hacker n. *(from Wikitionary)*
  1. (*computing*) One who is expert at programming and solving problems with a computer.
  2. (*computing*) One who uses a computer to gain unauthorized access to data, or to carry out malicious attacks.
  3. (*computing*) A computer security professional.

- The top discussion item on that wiki entry simply says,

  Unfortunately, the original sense of this word is no longer primary, and as much as I would like to reclaim the original sense, that battle is long since lost. If you use hacker outside the hacker community, expect to be misunderstood.

- **TL;DR - Hacker ≠ Criminal**

Cybercriminals?

- Cybercriminals may or may not be hackers.
  - They may hire technical capability, and not exercise it themselves
  - They may be only script-kiddies
  - They might not even be criminals: They may be state-sponsored, and thus their actions are legal, *under* ***their nation's*** *laws*

- Meanwhile, ***hacking*** is:
  - A set of problem-solving approaches
  - A toolbox of techniques
  - Morally neutral

- IFF the goal of the hacking is a crime, then a hacker ***also happens*** to be a cybercriminal.

Researchers - who they are

- A researcher's job is to find ways that our systems can be exploited
  - Some do malware reverse-engineering
  - Some do vulnerability discovery and analysis
- Most of our companies don't employ them: it's too specialized
  - Large providers and specialty firms (Verizon, FireEye) provide the talent
  - We consume the output - reports and alerts
- Independent researchers also work as consultants
  - With companies, e.g., after an attack
  - Providing bug reports to manufacturers
  - Red/Blue team exercises
- Depending on "hat color"... other possible revenue-generation models

- Without question, Security Researchers are ***hackers***

Zero-Day

- What it really means
  - A vulnerability exists in a product
  - A black-hat researcher discovers it...
  - ...and uses it to launch an attack
  - The vendor learns about the hole by means of attack(s) “in the wild” being analyzed.
- Called “zero-day” because the vendor had zero days’ notice before attack(s) in the wild forced them into a crash-effort to develop the patch.
- Once a patch is released, it’s no longer a zero-day
- Sadly, this does not prevent companies’ PR folks from using the term more loosely, to deflect blame they might otherwise face for not fixing or applying available fixes

Disclosure

- When and how the researcher tells someone about the defect
- A researcher has a lot of options for whom to tell
  - The manufacturer of the vulnerable product
  - That manufacturer's competitor
  - Their own government
  - Another government
  - Julian Assange (or similar)
  - WIRED Magazine (or similar)
  - Pastebin
  - Some Russian mob
  - Any of the above
  - None of the above
- So what they do… depends on motivations and incentives and risk/reward assessments

Disclosure Modes

- Non-Disclosure
  - Tell nobody
  - Exploit what you can
  - Sell what you can't exploit - or can't be bothered to
  - Model: Black Hats, Commercial Exploit Vendors
- Full Disclosure
  - Publicize immediately
  - Allows informed risk assessment
  - Pressures vendors to get fixes out quickly
  - Model: Bugtraq, US-CERT
- Responsible Disclosure *(AKA Coordinated Disclosure)*
  - Gives vendors a head start to patch - but pressure is still on
  - Disclosure will still happen
  - May give sophisticated attackers a time-window to exploit

Responsible Disclosure

- Researchers advise companies of defects found in their products
- A reasonable amount of time is allowed for fixes
  - How much depends on a good estimate of the time to create and propagate the fix
- Companies may compensate the hacker for the report
  - This offsets some of the hacker's incentive to use the knowledge for darker purposes
- The time limit is firm: the defects will be made public, fix or no
  - Companies know they don't want to get caught with pants down. Motivation!
- This is intended to balance public right-to-know vs. revealing defect to criminals who will exploit it
  - Even without a fix yet, there can be other mitigations to take

All About the Benjamins?

"Money may not buy happiness, but I'd rather cry in a Jaguar than on a bus."

--Francoise Sagan

- So how do independent hackers get paid?
- Some vendors pay for bug reports detailing important defects in their products. *Microsoft, Facebook, Google, more*.
- MS and FB also sponsor the Internet Bug Bounty program, covering a wide variety of internet infrastructure software: *Apache, Flash, OpenSSL, Python*
- Security.TXT: A proposed standard for security disclosure policy publication, trying for RFC
- Last year the US Gov't ran "Hack the Pentagon" and paid out over $70K
- Bug "markets" or "brokers" *e.g., HackerOne, BugCrowd*

Remember

- Hacker ≠ Criminal
- If your pen-tester is not a hacker…. you probably need a new one
- Disclosure will happen; wise vendors choose the terms when they can
- Check out the Electronic Frontier Foundation (EFF.org) for more issues - legal obstacles, etc.
- Have you Hugged a Hacker Today?

Questions?

Contact & Links

My Own Full Disclosure:

Work Email Personal Email Google+ Blog

Disclosure:

CERT-CC Disclosure Policy *(the FAQ that follows it is great.)*

The Open Source Responsible Disclosure Framework

Security.txt

Bug Bounties:

bugcrowd.com resources

HackerOne

Security Research as a Career

How a person becomes a security researcher

So you want to be a security researcher

Both of the above pieces are more oriented to a laundry list of technical skills than to the hacker mindset. But that's OK -- you either have the mindset or you don't.

"Hacker"

Stallman Rochester's Hackerspace