How to Disclose an Exploit Without Getting in Trouble

Jim Denaro
jim@cipherlaw.com
PGP: 0xD840D7A5

Tod Beardsley
todb@metasploit.com
PGP: 0xF577904A


DEFCON
PART II
@cipherlaw
@todb

About Us

Jim Denaro / CipherLaw

jim@cipherlaw.com
PGP: 0xD840D7A5
RedPhone/TextSecure
SilentCircle: CipherLaw
@CipherLaw

Tod Beardsley / Rapid7

todb@metasploit.com
PGP: 0xF577904A
@todb

Risks In Disclosure

Get your research buried by an angry judge
Get sued by an angry vendor
Get arrested by an angry government
Accidentally disclose 0-day!

@cipherlaw

@todb

Overview

- Types of Risks to Researchers
- Risk Mitigation Strategies
- Disclosure Options

Your Goal: Be a Harder Target

Risks in Disclosing

Research Examples:

- You found out how to see other people's utility bills by changing the http query string
- You discovered your neighbor's WiFi is using the default password
- You broke the DRM protecting media
- You wrote a better RAT

Many of the same risks apply

Specifics: CFAA

Computer Fraud and Abuse Act

access “without authorization”
or “exceeds authorized access”

Specifics: CFAA

Computer Fraud and Abuse Act

- Are you connected to the internet?
- Are you accessing a remote system?
- Do you have permission to access that system?

Specifics: Recent Case Law

Criminal prosecution

- Nestor (exploited video poker bug [CFAA charge dropped])
- Nosal (terms of use [no CFAA violation, 9th Cir.]
- Aaron Swartz (spoofed MAC address)
- Andrew Auernheimer (conspiracy to script http queries to public API)
- "conspiracy to hack a honeypot may still violate the CFAA." (DOJ CCIPS manual citing *U.S. v. Schaffer*)

Civil prosecution

- Available on the same grounds to private parties

CFAA Risk Mitigation

Do not direct technique information to someone you *suspect* or *should know* is likely to use it illegally.

CFAA Risk Mitigation

Be careful in providing “support”.

“If I were your lawyer, I’d advise you not to answer that tweet.”

@cipherlaw

@todb

CFAA Risk Mitigation

Consider not providing technique information *directly to any individuals* and limiting distribution to websites only.

Do not promote the disclosure on *forums known to support or promote illegal activity*.

If published on a website, *consider disabling comments* to avoid possibility of users discussing illegal use on your site.

Do not maintain logs.

Disclosure Options

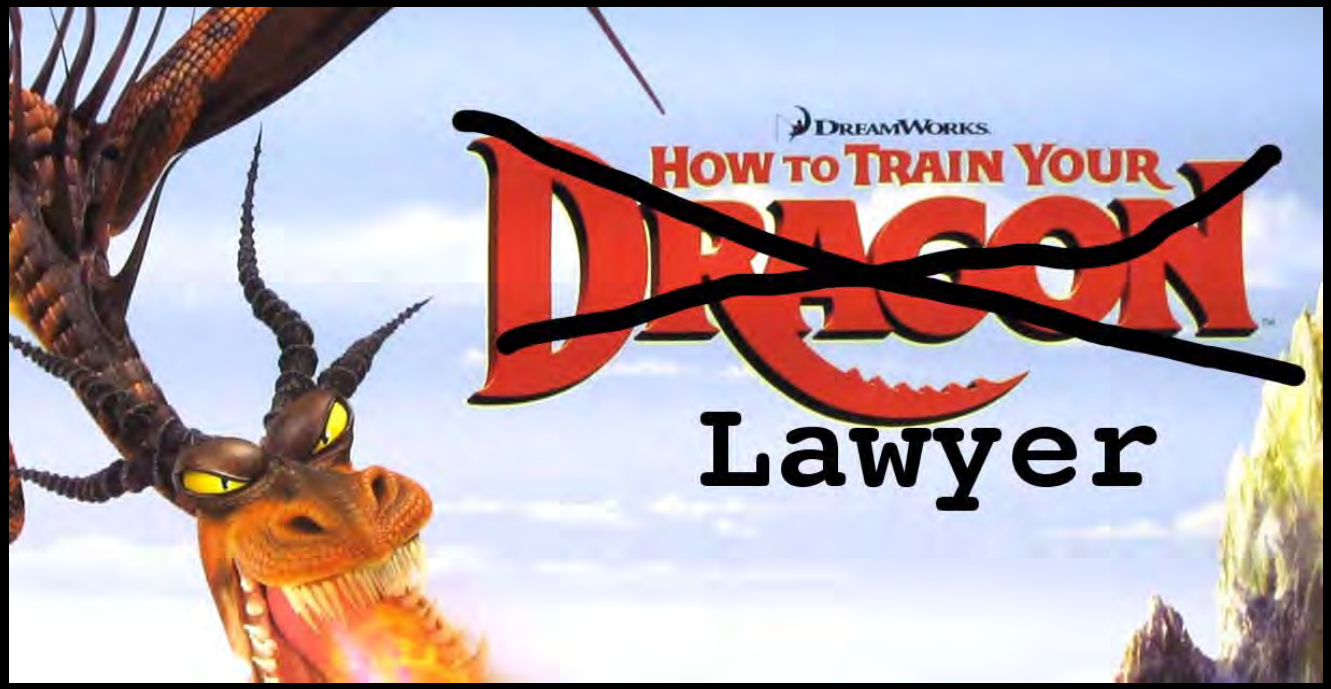
No good deed goes unpunished

Two-Stage Disclosure

Offer more details if they'll be reasonable.

@cipherlaw

@todb



@cipherlaw

@todb

Know your Adversary

A litigious multinational corporation?
An organization with disclosure experience?
A free, open source software project?
...an important one?
Do any governments have an interest?

Reasonable Precautions

@cipherlaw

@todb

Case Study: R7-2014-10

(Vulnerability details to be disclosed on site)

Vendor: TBA
Details: TBA
URL: https://rapid7.com/path/to/details

Disclosure Timeline: R7-2014-10

March, 2014: Client-Attorney Relationship Established between Cipherlaw Group and Rapid7
April 4, 2014: Vulnerability details disclosed to attorney
May 1, 2014: Details disclosed to vendor
May 23, 2014: Details disclosed to CERTs.
Today: Details published

@cipherlaw

@todb

Secure Comms Are Really Hard

@cipherlaw

@todb

Obfuscating Meta-Data

Authorship Analysis in Cybercrime Investigation http://www.personal.psu.edu/faculty/h/u/huz2/Zan/papers/authorship.isi03.pdf

@cipherlaw @todb

Questions?

Shoot!

@cipherlaw

@todb