How to Disclose or Sell an Exploit Without Getting in Trouble

Jim Denaro

@CipherLaw

This presentation is not legal advice about your specific situation.

This presentation does not create an attorney-client relationship.

While these approaches are designed to reduce risk, they cannot eliminate it.

Overview

- Types of Risks to Researchers
- Risk Mitigation Strategies
- Disclosure Options
- Risk Mitigation for Selling Exploits

Your Goal: Be a Harder Target

Risks in Disclosing or Selling

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 crypto protecting media

You wrote a better RAT

Many of the same risks apply

What are we talking about?

“Techniques”

Information relating to both exploits and vulnerabilities that enable another party to obtain unauthorized access to a computer, deny access by others to a computer, or cause permanent or temporary damage to a computer or a network

When is There Risk?

- *Threats* of with legal action *before* conference or disclosure
  - Chris Paget (IOActive) (Black Hat) - 2007
  - Princeton Prof. Felten (USENIX) - 2001
- *Injunction* barring disclosure *before* conference or disclosure
  - Megamos (USENIX) - 2013
  - MIT - Massachusetts Bay Transportation Authority (DEFCON) - 2008

When is There Risk?

- Legal actions initiated *after* conference or disclosure
  - Cisco - Michael Lynn (ISS) (Black Hat) 2005
    - Civil lawsuit filed after talk
  - Dmitry Sklyarov (DEFCON)
    - Taken into custody in Las Vegas after DEFON presentation

Computer Fraud and Abuse Act

accesses “without authorization”

“exceeds authorized access”

by deployment or development effort

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?

Conspiracy

to violate the CFAA

risk enhanced by social media

CFAA Risk Example Cases

- 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

Risk Mitigation: CFAA

18 U.S.C. §1030

"(a) Whoever – (1) having *knowingly* accessed a computer without authorization or exceeding authorized access…"

Risk Mitigation: CFAA

18 U.S.C. §1030

"(a) Whoever – (2) *intentionally* accesses a computer without authorization or exceeds authorized access…"

Risk Mitigation: CFAA

Avoid unintentionally creating

Knowledge

Intent

Risk Mitigation: CFAA

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

Risk Mitigation: CFAA

- Be careful in providing "support".

"If I were your lawyer, I'd advise you not to answer that tweet."

Risk Mitigation: CFAA

- 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.

Risk Mitigation: TRO

- Goal: Avoid a Temporary Restraining Order (TRO)
  - Factors

    (1) Will the requestor suffer irreparable harm if the TRO does not issue?
    (2) Will there be even greater harm to the researcher if the TRO does issue?
    (3) The public interest
    (4) *Likelihood requestor will ultimately prevail*

Risk Mitigation: TRO

- Avoid use of copyrighted material.
  - Exploit including source or object code from target may infringe copyright
    - Megamos and Cisco plaintiffs cited misappropriation of intellectual property
    - "Fair use" exception
- Avoid darknet sources for proprietary or copyrighted material.

Risk Mitigation: TRO

- Be aware of any pre-existing relationships with possible targets of the technique.
  - Terms of Service (TOS), End User License Agreement (EULA), Non-Disclosure Agreement (NDA), Employment Agreements

Risk Mitigation: TRO

- Necessity of risk mitigation depends on nature of research.
- If research techniques were questionable:
  - Do not publish identity of the target system.

Disclosure Options

Option #1
Disclose to responsible party

- Relatively high risk
  - if techniques used were questionable
  - if planning to present at a conference or publish (TRO)
- Risk lowered if
  - submitted anonymously *and*
    - OPSEC is good
- Relatively low risk if to a bug bounty and no questionable techniques used

Option #2
Disclose to gov't authority

- Relatively high risk
  - if techniques used were questionable
  - anonymity is desired
- Risk lowered if
  - submitted anonymously *and*
    - OPSEC is good

Always Accept the Risk in Disclosing if You Are...

OK to Disclose

[REDACTED]

Option #3
Pilot TTP Disclosure Program

- Researcher discloses vuln to trusted third party (TTP attorney) *only*.
  - Maintains attorney-client privilege
- TTP discloses vuln to responsible party.
- TTP [does | does not] publish the vuln on behalf of researcher after *y* days.
- Researcher can remain anonymous [temporarily | permanently].
- *Researcher maintains control of disclosure process.*

Selling: The Current Situation

Booming "zero-day" trade has Washington cyber experts worried

Fri, May 10 2013

By Joseph Menn

WASHINGTON (Reuters) - The proliferation of hacking tools known as zero-day exploits is raising concerns at the highest levels in Washington, even as U.S. agencies and defence contractors have become the biggest buyers of such products.

White House cybersecurity policy coordinator Michael Daniel said the trend was "very worrisome to us."

The U.S. Senate Wants to Control Malware Like It's a Missile

Posted By John Reed ■ Thursday, June 27, 2013 - 2:35 PM ■ Share

The NDAA Senate Bill

"The President shall establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative export controls, law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate."

The NDAA Cmtee Report

"The types of dangerous software used to perpetrate these malicious incidents are actively traded on a global black market, and they are also available in the so-called gray market, through unscrupulous companies."

"This process will require developing definitions and categories for controlled cyber technologies and determining how to address dual use, lawful intercept, and penetration testing technologies."

Senate Cmtee on Armed Services, National Defense Auth Act, June 20, 2013

The European Directive

Article 7

Tools used for committing offences

Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:

(a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

The European Exception

Whereas:

(16)…Motivated by the need to avoid criminalisation where such tools are produced and put on the market for legitimate purposes, such as to test the reliability of information technology products or the security of information systems, apart from the general intent requirement, a direct intent requirement that those tools be used to commit one or more of the offences laid down in this Directive must be also fulfilled."

Selling: Risk Mitigation

- Create dual-use tools.
  - Copy II Plus
- Know your buyer.
  - Avoid embargoed countries
    - EU, US, UN
- Ask for assurances from the buyer.
- Use disclaimer language.

Selling: Risk Mitigation

- Use disclaimers in correspondence and agreements

"Compliance with Law. Customer acknowledges that the Software can be configured by the user to obtain access to information using penetration techniques that may cause disruption in systems or services and may cause data corruption. Denial of Service attacks may be run on command that will attempt to render systems and services unavailable to authorized users. Customer specifically agrees that the Software will only be used to target devices under the authorized control of the Customer and in a way in which damage to systems or loss of access or loss of data will create no liability for [discloser/seller] or any third party. Customer further agrees to strictly comply with all federal, state and local laws and regulations governing the use of network scanners, vulnerability assessment software products, hacking tools, encryption devices, and related software in all jurisdictions in which systems are scanned or scanning is controlled."

"You also agree that you will not use these products for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of nuclear, missiles, or chemical or biological weapons."

Contact Information

Jim Denaro
jim@cipherlaw.com
@CipherLaw
https://www.cipherlawgroup.com
PGP / X.509 at
https://www.cipherlawgroup.com/professionals/denaro
SilentCircle: cipherlaw