Retaliatory Hacking: Risky Business or Legitimate Corporate Security?

Presenter: Sean L. Harrington

- Cybersecurity Partnership Manager and information security risk assessor in the banking industry;
- Digital forensics examiner in private practice;
- Graduate with honors from Taft Law School, and
- holds the MCSE, CISSP, CHFI, CCFP, and CSOXP certifications;
- Has served on the board of the Minnesota Chapter of the High Technology Crime Investigation Association;
- Current member of Infragard, FS-ISAC, the Financial Services Roundtable's legislative and regulatory working groups, Chamber of Commerce Cyber Working Group, among others;
- Teaches digital forensics for Century College in Minnesota;
- An instructor for the new ISC^2 CCFP certification.

Not Legal Advice

This presentation is based upon a scholarly work, and is intended to promote discussion and innovation. This presentation is not intended to convey legal advice. Readers should not act or refrain from acting based upon the presenter's oral or written statements

Overview

1. Key terms & concepts
2. Key statutes
3. Active Defense Approaches & associated legal, regulatory, ethical, and practical considerations
4. theories rationalizing active defense
5. Promising alternatives

Active Defense

Hack Back

Offensive Counter Measures (“OCM”)

Retaliatory Hacking

Protecting and defending electronic information and assets in and beyond one’s own network.

Federal Statutory Prohibitions

- Computer Fraud and Abuse Act of 1986
  - Provides both civil and criminal penalties for violation
- Electronic Communications and Privacy Act of 1986
  - Provides both civil and criminal penalties for violation
  - Title I: Wiretap Act
  - Title II: Stored Communications Act
  - Title III: pen register and trap and trace devices
- 18 U.S.C. § 2252; 18 U.S.C. § 2252A*
- Many states have counterpart statutes, some of which contain more specific language and are less antiquated.

CFAA

- Directed at criminal computer hacking
- Prohibits computer intrusions — accessing computers "without authorization," or "exceed[ing] authorize[d]" access, which statutory phrases have been the continuing subject of appellate review.
- Private parties who can show "damage or loss" in excess of $5,000, which can include the cost of hiring a forensic examiner plus his or her assessment of the damage caused to the victim's computer or business, can sue.
- The Government can pursue felony charges if damages are in excess of $5,000
- House Judiciary Committee considering augmenting the Act — all offenses would be felonies

ECPA — Title I

- Update of the original wiretap law of 1968
- Prohibits interception, disclosure, or use of wire, oral, and electronic communications in transit
  - must be contemporaneous with transmission
  - examples: e-mail, text/video messaging, keystrokes (some courts)
- Prohibits public Internet carriers from disclosing content of in-transit e-mail

Privacy

- CA and MN
  - Data handling
  - Data Breach Notification
- PCI DSS
- Gramm-Leach-Bliley Act: requires financial institutions to protect information collected about individuals, and prohibits disclosure of their customers' account numbers

ECPA — Title II (Stored Communications Act)

- Applies to ISPs. Inapplicable to private companies' internal e-mail systems.
- Restricts Government access to customer and subscriber information and records
- Providers may disclose protected information if:
  - Consent is given by the sender, an addressee, or the recipient
  - Content was inadvertently obtained and appears to contain evidence of the commission of a crime

Ethics

- Codes of Conduct describes the expected behavior of members of an association or practitioners of a profession, and generally seek to protect the organization or profession from the consequences of bad behavior of its members.
  - ABA Model Rules 1.2, 5.3, 8.4(c)
  - $(ISC)^2$ Code of Ethics Preamble*
  - $(ISC)^2$ Code of Ethics Cannons**
  - Model Rules

Active Defense Approaches

Approaches		Risks
Beaconing		Legal
Threat Intelligence Gathering		Ethical
Sinkholing		Escalation
Honeypots		Misattribution and collateral damage
Retaliatory Hacking		Goodwill & reputation

Active Defense – Hack Back

Theories advanced for justified retaliatory hacking:

- Recapture of chattels
- private necessity
- Castle doctrine
- private security guard doctrine

Promising Alternatives to Hack Back

- Preventive: Private entities' collaboration with ISPs and industry partnerships to combat; Intelligence sharing and gathering (ISACs); perimeter hardening
- Detective: tools; know your network traffic; behavioral anomaly analysis; parse your logs
- Corrective: collaboration with government and other private corporations: (*e.g.,* takedowns of Citadel, Zeus)
- Corrective: cyber legislation
- Risk transfer ? (outsourcing, cyber insurance)

References

The following are works of the presenter, but collect citations to authoritative works of other experts, scholars, and commentators on the subject

- *The CIP Report,* George Mason University Center for Infrastructure Protection and Homeland Security, Volume 12, No. 4 (Oct., 2013) http://cip.gmu.edu/wp-content/uploads/2013/06/October-2013_Financial-Services.pdf , pp. 11-15

- *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?* 20 RICH. J.L. & TECH. 1 (2014) (draft copy available at http://works.bepress.com/sl_harrington/)