Justice, Victim Corporations, and Cybercriminals

Erez Liebermann
Assistant United States Attorney
Computer Hacking and Intellectual Property Section
District of New Jersey

Laws and Penalties

- Computer Fraud and Abuse Act
- Wire Fraud
- Intellectual Property Laws

Two Sources of Threats

- Insider Attacks
- Outsider Intrusions

Insider Attacks

- Omega Engineering
  - Timothy Lloyd, working in IT, planted the logic bomb as he was being moved around and demoted.
  - Defendant sentenced to 41 months and ordered to pay $2,000,000.
  - Employee

Insider Attacks

- Cyber City
  - Neal Cotton planted logic bomb the night after he was informed he would be fired.
  - Defendant sentenced to 12 months and ordered to pay $120,000.
  - Employee

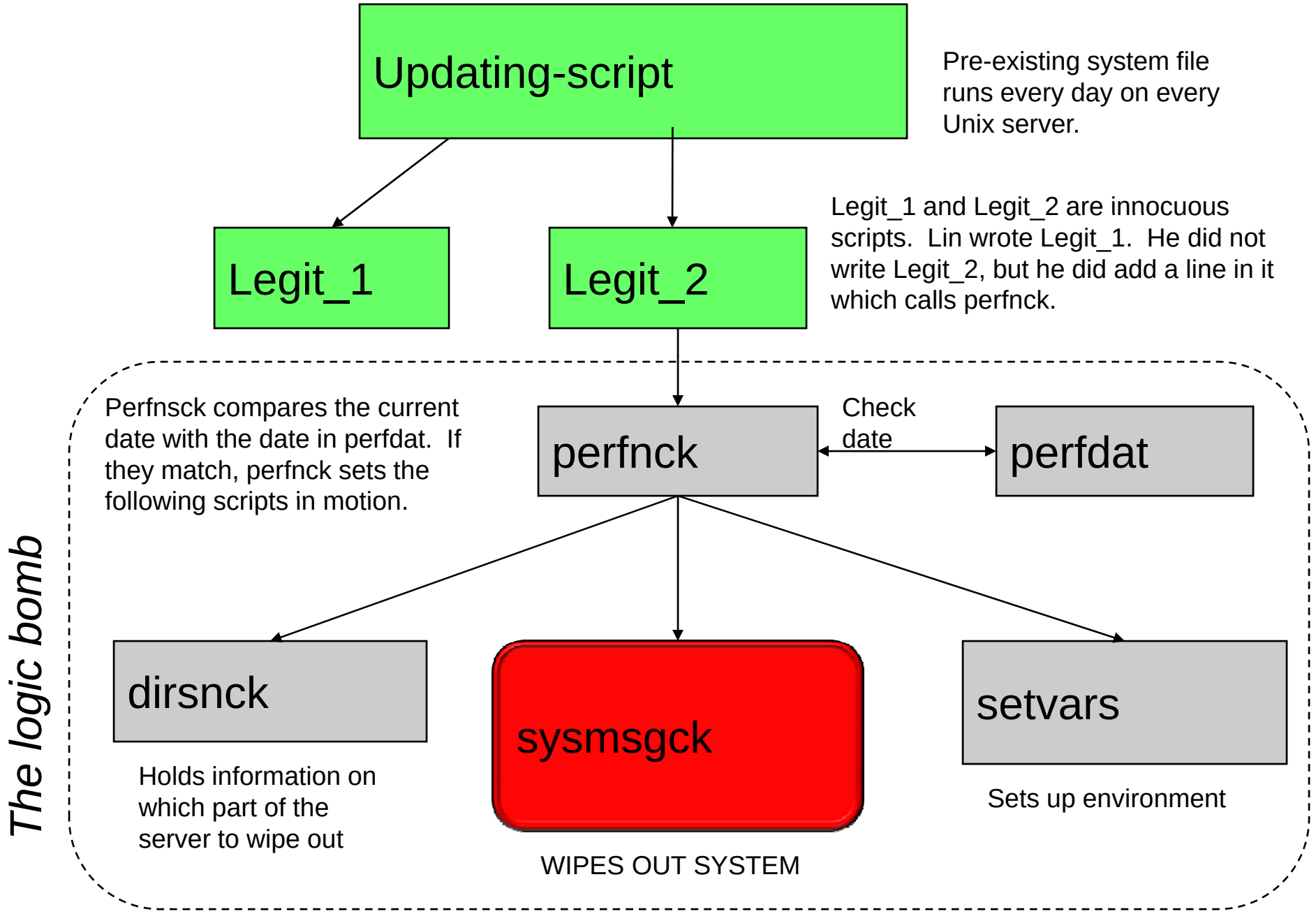
Insider Attack

- UBS
  - Roger Duronio planted a logic bomb when his bonus was not what he wanted.
    - Sentenced to 97 Months
  - Employee

Insider Attack

- Medco Health Solutions, Inc.
  - Andy Lin Feared he would be fired when rumors of layoffs spread.
  - Planted logic bomb in Medco's system.
  - Had it been triggered:
    - Financial Damage
    - Health implications

The Operation of Lin's Logic Bomb



- Medco Health Solutions, Inc. – Cont'd
  - Pleaded Guilty
  - Employee

Outsider Attack

- Voice Over Internet Protocol (VOIP)
  - Edwin Pena and co-conspirators hack into VOIP companies and unsuspecting intermediaries.
  - Brute Force Attacks.
  - Millions made.


POWER
G-WEST
MAY 20 2006

Data Breaches

- Ongoing threat
- Millions of identities and credit cards compromised
- Infiltrate the servers of merchants (e.g., the TJX companies)
- Secondary market for stolen information

Data Breach

- Lowe's
  - Wireless Intrusion into Lowe's Network in Detroit.
  - Access to all of Lowe's customer data.


CUSL2
NO


COMPAQ
W00T

Arrest and Prosecution

- Confessed and later pled guilty
- One was 20 years old, with a prior hacking conviction
- Sentence:

9 Years

Data Breaches: To Report or Not to Report?

- Data breach notification laws
- Cooperate with authorities
- Avoid aggravating factors in a lawsuit

Cyber Extortion

- Actual breach into computer systems
- Threatened breach into computer system

Military Hack

- **United States v. Gary McKinnon**
  - Weapons Station Earle
  - NASA
  - Pentagon
- Searching for info on UFO's?

"US foreign policy is akin to government sponsored terrorism these days... It was not a mistake that there was a huge security stand-down on September 11 last year... I am SOLO. I will continue to disrupt at the highest levels."


FREE
GARY
http://FreeGary.org.uk

What if it Happens?

- Call Law Enforcement.
- But...

Myth:

"If I call law enforcement, they won't care."

Myth:

"Law enforcement won't be able to catch the bad guys."

Myth:

"I can handle the situation myself."

Myth:

"If I just patch the security hole, restore my data, and fire the dirty insider, then I don't need to tell anyone."

Myth:

"If I call law enforcement, they'll come and take my servers away."

Myth:

"If I report to law enforcement, I'll lose control of my proprietary data."

Best Practices

- Protect the rights of the victim.
- Consult with senior management.
- Consult with IT staff.
- Minimize disruption to the company.
- Coordinate media releases.
- Keep the company informed.
- Build relationships before an intrusion.

Steps to Protect

- Logs, Logs and more Logs.
- Separation of Powers.
- Click-Through Banners.
- Extra vigilance.
- Immediate cut-off.

Questions?

My contact info:

erez.liebermann@usdoj.gov
973.645.2874