Looking into Malicious Insiders

JPCERT/CC
Koichiro Sparky Komiyama

First Conference, Vienna
Agenda

• Background
  – Previous work
  – Information leakage by malicious insider
• Our Research
• How to prevent
Insider Threat

• Definition by CERT/CC insider threat study
  • A current or former employee, contractor, or business partner who
    • Has or had authorized access to an organization’s network, system, or data and
    • Intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems
WHY INSIDER THREAT?
More insiders are arrested

• How unauthorized access happens? How do attackers obtain credentials? (N=1740)

- 1368, 79%: Insiders
- 183, 11%: Social engineering
- 163, 9%: weak, guessable passwd, miss configuration
- 26, 1%: others

NPA, FY2008, Act on the Prohibition of Unauthorized Computer Access
OUR RESEARCH
• Motivation
• Project members
  • National Police Agency (NPA, prefectural police department)
  • Department of Criminology and Behavioral Science, National Research Institute of Police Science
  • JPCERT/CC
• Survey 30 cases/criminals who
  1. Fit the malicious Insider definition by CERT/CC
  2. Were arrested and prosecuted for Cybercrime related law from 2007 to Jun, 2009
1, visit local police office
2, fill in survey form with referring police investigative report
3, Sanitize to secure anonymity
4, Correlation analysis by 24 variables
24 variables: Case

• The case is
  - By a repeat offender
  - caused financial damage
  - computer which company provided was used
  - access from outside
  - Delete/modify logs of activity
  - use his/her own account to login
24 variables: Surrounding

• Company/Organization
  □ Has insecure account management (like easily guessable user name)
  □ Does not have any physical monitoring (video monitor, guards)
24 variables: Criminals

• Criminal is
  - Is a lone criminal
  - Has no job at the time
  - Is in dire financial circumstances
  - Is under strong pressure
24 variables: Relationship

- Criminal is
  - a former employee of the company/organization
  - Has been terminated in the past
  - caused any trouble in the past
  - Is in charge of system management
  - Is a web admin
  - Is in charge of accounting or finance
24 variables: Motives

- Criminals motivation is
  - To make money
  - To get information, then to make money by selling those
  - Sabotage
  - Personal satisfaction
Correlation Map
FINDINGS
IT sabotage (10)

Fraud (9)

Theft of Information (15)
HAVE A LOOK AT 30 INSIDERS
## WHO? (Gender, work history)

<table>
<thead>
<tr>
<th>Type</th>
<th>Fraud(9)</th>
<th>IT Sabotage(10)</th>
<th>Information Theft - Money(7)</th>
<th>Information Theft - Satisfaction (8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male(6) Female(3)</td>
<td>Male(9) Female(1)</td>
<td>Male(7)</td>
<td>Male(8)</td>
</tr>
<tr>
<td>work history</td>
<td>hopping part time job</td>
<td>job change 5times</td>
<td>job change 3times(3)</td>
<td>job change 4 times</td>
</tr>
<tr>
<td></td>
<td>job change 3times(2)</td>
<td>job change 4 times</td>
<td>job change 2times</td>
<td>job change 3times(2)</td>
</tr>
<tr>
<td></td>
<td>job change 1 time(fired by ex-company)</td>
<td>job change 3 times(3)</td>
<td>job change 2 times(3)</td>
<td>job change 2times</td>
</tr>
<tr>
<td></td>
<td>job change 1 times (own his start-up and shut it down)</td>
<td>no job</td>
<td>no job</td>
<td>no job</td>
</tr>
<tr>
<td></td>
<td>no job(3)</td>
<td>unknown</td>
<td>job change 3times(2)</td>
<td>job change 2times</td>
</tr>
<tr>
<td></td>
<td>job change 4 times</td>
<td>job change 2times</td>
<td>job change 1time(3)</td>
<td>no job</td>
</tr>
<tr>
<td></td>
<td>job change 3times(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>job change 2times</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>job change 1time(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>no job</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Frequent job change can be seen all categories
## WHO? (Personality)

<table>
<thead>
<tr>
<th>Fraud(9)</th>
<th>IT Sabotage(10)</th>
<th>Information Theft - Money(7)</th>
<th>Information Theft - Satisfaction (8)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Humble, sociable</strong></td>
<td>clumsy at office, cannot communicate with others</td>
<td>good guy, a bit of a scatterbrain</td>
<td>easily offended, hold by his own idea</td>
</tr>
<tr>
<td>wear torn jeans, not like a business man</td>
<td>very active for any business and solid person</td>
<td>polite, perfect young gentleman</td>
<td>Sociable, sometimes acts paranoid for minor problem</td>
</tr>
<tr>
<td>patient and quiet.</td>
<td>quiet</td>
<td>stiff and proper, can't refuse when someone asks</td>
<td>very childish</td>
</tr>
<tr>
<td>always exhibitionistic.</td>
<td>not very good at communication</td>
<td>act in a childish manner</td>
<td>popular among project team members</td>
</tr>
<tr>
<td>unknown</td>
<td>habitually lying</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

- Less conversation, less communication
### WHO? (Criminal record, Education)

<table>
<thead>
<tr>
<th>Type</th>
<th>Fraud(9)</th>
<th>IT Sabotage(10)</th>
<th>Information Theft - Money(7)</th>
<th>Information Theft - Satisfaction (8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal record</td>
<td>• No(5)</td>
<td>• No(6)</td>
<td>• No(6)</td>
<td>• No(6)</td>
</tr>
<tr>
<td></td>
<td>• professional embezzlement and stealing</td>
<td>• twice for theft of lost or mislaid</td>
<td>• assault</td>
<td>• twice for theft of lost or mislaid property</td>
</tr>
<tr>
<td></td>
<td>• stealing</td>
<td>property</td>
<td></td>
<td>• assault</td>
</tr>
<tr>
<td></td>
<td>• assault</td>
<td>once for theft of lost or mislaid</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• trademark law violation</td>
<td>property</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>shoplifting, stealing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>False entry in resume</td>
<td>• False entry (2)</td>
<td>• False entry (3)</td>
<td></td>
<td>• False entry (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Over 80 percent are first-time criminals
- Some lie on a resume, especially their educational background
When? and Where?

• When
  – Fraud: during business hours
  – IT sabotage: one to six month after resignation/termination, most of those failed to get a new job. Night Time
  – Insiders start with trivial activities, then escalate

• Where
  – Fraud, Information Theft: in office
  – IT sabotage: from home
<table>
<thead>
<tr>
<th>WHY? (direct motivation)</th>
<th>Fraud(9)</th>
<th>IT Sabotage(10)</th>
<th>Information Theft - Money(7)</th>
<th>Information Theft - Satisfaction (8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• get money to pay off debts (3)</td>
<td>• betrayed the expectations of being a full time worker</td>
<td>• can not find new job and want to make money, even if only a little</td>
<td>• sudden random thought while drinking</td>
<td></td>
</tr>
<tr>
<td>• frustration at long hours, aim to get back at management</td>
<td>• want to harass(5)</td>
<td>• want to make money by selling personal information (2)</td>
<td>• want to understand the situation he used to work in</td>
<td></td>
</tr>
<tr>
<td>• feel less secure since spouse doesn’t work</td>
<td>• get fired despite of his outstanding performance</td>
<td>• get info in order to please his boss</td>
<td>• he has pending lawsuit with the company. And he checks if there are any other trouble</td>
<td></td>
</tr>
<tr>
<td>• get money to pay off debts</td>
<td>• company contact him as a last resort.</td>
<td>• feels it’s such a waste letting points to expire</td>
<td>• Money, ★恨み, 人間関係、ストレス</td>
<td></td>
</tr>
</tbody>
</table>

• More likely to occur when they failed to get new job.
## How they get into the system?

<table>
<thead>
<tr>
<th>Fraud(9)</th>
<th>IT Sabotage(10)</th>
<th>Information Theft - Money(7)</th>
<th>Information Theft - Satisfaction (8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• during his/her regular duty (4)</td>
<td>• login to Web server with ex-coworker’s account (2)</td>
<td>• Modify mail server settings to forward all e-mail to his private account. Even after his termination.</td>
<td></td>
</tr>
<tr>
<td>• studying similar abstraction cases reported in a newspaper.</td>
<td>• login to other server with one’s own superuser account (2)</td>
<td>• He/She is the admin for a server that contain sensitive personal information(2)</td>
<td></td>
</tr>
<tr>
<td>• start it as a trial with curiosity</td>
<td>• login PC with one’s own account</td>
<td>• there’s politics among staff. Then he installs key logger to PC’s of his opposition.</td>
<td></td>
</tr>
<tr>
<td>• stole password using key logger. Someone taught him how to use it</td>
<td>• login to server with co-worker’s account (using guessing)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• make secret back door on a server that enables him to connect from home.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modify mail server settings to forward all e-mail to his home.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• login to mail server with his boss’s ID. Successfully guess password.</td>
<td></td>
</tr>
</tbody>
</table>

More than half of 30 cases are preventable by disabling user account(s) right after termination.
Victims

• We could not find elements that victims have in common
• IT Sabotage: Small company, one single system administrator, selfish owner
• Pay less or no attention to security
Login to mail server

Login and read other’s email

Modify config to forward all email outside

Modify a few records and logs

“DROP DATABASE”

Login to database and patch

Escalation curve
HOW TO PREVENT
Considerations

• Pre-employment period
  – Check resume for certain points (job hopper? degree certificate)
  – Sign NDA

• During employment
  – Closer communication (company news letter, baseball tournament, other social events)
  – Check for visible sign (how they dress, work attitude)
  • Periodical audits, transfer as necessary
  • Try not to create too much dependency on one individual
    • Pair programming

• Upon termination
  • Suspend account immediately
  • Change passwords as necessary
Challenges for the future

• Technical details were not be clear from police investigative reports

• Need more case studies
  – No politically motivated cases

• Signs of insider threat, preventive measure could be different by country, culture and IT skill.
  – Global companies need measures for each area
Special Thanks To:

• SYAKAI ANZEN KENKYU ZAIDAN
  –http://www.syaankanen.or.jp/02_goannai/08_cyber/cyber_f.htm (JAPANESE)

• National Police Agency
Thank you.