Crime DOES Pay
(Unless you get caught)

Renana Friedlich, IR & Forensic Team Leader
Hacktics Advanced Security Center,
Ernst & Young
February 2013
Traditional Forensics
Digital Forensics

He’s tough, but we’ll make him talk.
Example – Bredolab

Diagram showing connections between Russia, Netherlands, and France.
Agenda

► Computer Crime Definition

► Crime Detection

► Dealing with an Incident
  ► Jurisdiction
  ► Punishment

► Case Studies

► Summary and Recommendations
Computer Crime Definition

► What name would best describe this type of offense?

► Is it a new form of crime?

Computer as a target

Computer as a weapon
Rising Above the Noise Level

Vectors that may lead to detection:

- Security systems
- Subject of attack
- Proportions
Relevant Parties for Detection

- Governmental Agencies
- Auditing Processes
- Security Vendors
- Local Police
- HoneyNets
- SOCs
- ISPs
- And more …
- End Users
## Top 10 Detected Incidents

### Verizon 2012 Data Breach Investigations Report

<table>
<thead>
<tr>
<th>Rank @ Large Org.</th>
<th>Overall Rank</th>
<th>Attack</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>Use of stolen login credentials</td>
<td>Hacking</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>Backdoor</td>
<td>Malware</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>Exploitation of backdoor C&amp;C channel</td>
<td>Hacking</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>Tampering</td>
<td>Physical</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Keylogger/Form-grabber/Spyware</td>
<td>Malware</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
<td>Pretexting (classic social engineering)</td>
<td>Social</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>Brute force and dictionary attacks</td>
<td>Hacking</td>
</tr>
<tr>
<td>8</td>
<td>15</td>
<td>SQL injection</td>
<td>Hacking</td>
</tr>
<tr>
<td>9</td>
<td>20</td>
<td>Phishing (or any type of *ishing)</td>
<td>Social</td>
</tr>
<tr>
<td>10</td>
<td>22</td>
<td>C&amp;C (listens for and executes commands)</td>
<td>Malware</td>
</tr>
</tbody>
</table>
Early detection heavily depends on the organization’s security maturity level.

Duration Until the Incident is Discovered

- Self Detection: 28 days
- Law Enforcement: 51.5 days
- Public Detection: 87.5 days
- Regulatory Detection: 156.5 days

Average time until detection (Days)
Dealing with an Incident

Common ways of dealing with an incident:

- Internal Care
- Law Enforcement Entity
  - Regulations
  - Incident Severity
Jurisdiction

- Local crime
- International crime
  - Law enforcement authorities ask for extradition
    - Accepted
    - Denied
Punishment

The penalty usually depends on the following factors:

- **Financial damage**
- **Current & potential damage**
- **Offender intentions & personal gain**
Case Study 1

► Attacker: Pablo Escobar (James Jeffery)

► Victim: Abortions website

Every year at bpas we help thousands of women who are considering abortion.

PabloEscobar
@PabloEscobarSec

bpas.org hacked:
postimage.org/image/l1wzwuo2... Database
dump will be released tomorrow...
#anonymous #antiabortion #humanrights

An unborn child does not have an opinion, a choice or any rights. Who gave you
the right to murder an unborn child and profit from that murder?

"The product, abortion, is skillfully marketed and sold to the woman at the crisis time in her life.
She buys the product, finds it defective and wants to return it for a refund. But, it's too late."
Case Study 2

► Attacker: Gary McKinnon

► Victim: USA military computers ("The biggest military computer hack of all time")

► The US authorities tried to get an extradition

► Requested penalty: Up to 60 years in prison
Case Study 3
Case Study 3

Take 1
► Age – 19
► Arrested for hacking to computers at NASA, the Pentagon, and more.
► Didn’t try to get a hold of secrets, rather to prove that the systems were flawed.

1.5 years in prison

Take 2
► Age – 28
► Accused with charges of conspiracy and fraud.
► Increased or deleted cards limit, then sold the stolen credit card numbers in the black market.

3 years probation + $503,000 fine
Summary

► The chances of getting caught are slim.

► Even if an offender does get caught, there is a long way to go before he may stand trial.

► Since so “MANY” stand trial, penalty is disproportionate.
And the Conclusion Is …

Crime Does Pay …
Recommendations

- **Poor**: Save logs
- **Moderate**: Continuous log monitoring
- **Good**: Build incident response capabilities
How good is your detection mechanism...?
Thank you.

Renana Friedlich,
Incident response & forensic team leader
Renana.Friedlich@il.ey.com, 054-2661260