Metrics & Quantification of Cybercrime

Lies, damn lies & statistics!

Jart Armin  (CyberDefcon)
WHAT’S HAPPENING RIGHT NOW?
WHAT’S THE COST?
Global Security Mapping – Today’s Attacks - Europe

- # of Networks attacked
- 56% above normal
Global Security Mapping – Today’s Attacks - US

Automated scanning trojans and worms looking to infect new computers scanning randomly generated IP addresses
Global Security Mapping – Today’s Attacks – RU & Asia
Based on Attack Traffic (DDoS, etc.)

<table>
<thead>
<tr>
<th># ATTACKS / HR</th>
<th>ATTACK ORIGINS</th>
<th># ATTACKS / HR</th>
<th>ATTACK TARGETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>4,429</td>
<td>China</td>
<td>11,032</td>
<td>United States</td>
</tr>
<tr>
<td>4,240</td>
<td>United States</td>
<td>1,454</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>1,143</td>
<td>Mil/Gov</td>
<td>842</td>
<td>Thailand</td>
</tr>
<tr>
<td>1,084</td>
<td>Hong Kong</td>
<td>542</td>
<td>Canada</td>
</tr>
<tr>
<td>930</td>
<td>Germany</td>
<td>525</td>
<td>Portugal</td>
</tr>
<tr>
<td>525</td>
<td>Canada</td>
<td>306</td>
<td>Spain</td>
</tr>
<tr>
<td>514</td>
<td>Netherlands</td>
<td>276</td>
<td>Australia</td>
</tr>
<tr>
<td>502</td>
<td>Taiwan</td>
<td>265</td>
<td>France</td>
</tr>
<tr>
<td>386</td>
<td>Thailand</td>
<td>265</td>
<td>Poland</td>
</tr>
<tr>
<td>343</td>
<td>Poland</td>
<td>235</td>
<td>Turkey</td>
</tr>
</tbody>
</table>

Network Attacks

<table>
<thead>
<tr>
<th># ATTACKS / HR</th>
<th>ATTACKED SERVICE</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,433</td>
<td>ssh</td>
<td>22</td>
</tr>
<tr>
<td>1,246</td>
<td>domain</td>
<td>53</td>
</tr>
<tr>
<td>565</td>
<td>netbios-dgm</td>
<td>138</td>
</tr>
<tr>
<td>824</td>
<td>snmp</td>
<td>161</td>
</tr>
<tr>
<td>620</td>
<td>microsoft-ds</td>
<td>445</td>
</tr>
<tr>
<td>951</td>
<td>ms-sql-s</td>
<td>1433</td>
</tr>
<tr>
<td>572</td>
<td>ms-wbt-server</td>
<td>3389</td>
</tr>
<tr>
<td>617</td>
<td>efi-lm</td>
<td>3392</td>
</tr>
</tbody>
</table>

“Attack traffic,” meaning countries and regions where port probes, worm, malware, viruses, and reflection attacks originate.
• Peak attack traffic: 2008 - just over 30 GBPs took out Georgia
• Unlawful intrusion attempts detected: - 2011 - 2.6 billion / 2008 – 0.38 billion
• Intruders & attackers? - probes, botnets, zombies, vulnerability scanners, scrapers, malware & worms…
• In 2009 - 2014 we observed a 95% correlation - extrapolated the data to make predictions up until 2016
- Renewed predictions show attacks exceeding 1 Tbps by 2017
- In 2015 / 2016 against ‘BBC’ = 600GB/sec
CYBERCRIME METRICS – What do the e-citizens think?

Top → Down
<table>
<thead>
<tr>
<th>Population</th>
<th>Worldwide</th>
<th>Poland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adults who have experienced cybercrime in their lifetime</td>
<td>61%</td>
<td>60%</td>
</tr>
<tr>
<td>Adults who experienced cybercrime in the past 12 months</td>
<td>41%</td>
<td>40%</td>
</tr>
<tr>
<td>Adults who have been victim of cybercrime and risky behaviours</td>
<td>50%</td>
<td>49%</td>
</tr>
<tr>
<td>Males who have been victim of cybercrime in their lifetime</td>
<td>64%</td>
<td>66%</td>
</tr>
<tr>
<td>People aged 18-32 who have been victim of cybercrime in their lifetime</td>
<td>66%</td>
<td>70%</td>
</tr>
<tr>
<td>Number of victims in the past 12 months (million)</td>
<td>378</td>
<td>6</td>
</tr>
</tbody>
</table>
Cybercriminal activity personally encountered

- Malware
- Phishing
- Spam
- Rogueware/Ransomware/Scareware
- Targeted Attack
- Data Breaches
- Information leakage
Who should take responsibility for Internet security?

- Search engine (Google, MSN, Yahoo… etc.)
- CERTs
- Your government
- Intergovernmental e.g. UN, ICANN, ITU… etc.
- Yourself / the end user
- Law enforcement
- IT and security departments in companies
- ISPs & hosts
Trusted sources on cybercrime

- Social media
- Cyber security bloggers
- Press - Security news articles
- Anti-virus vendors
- Blacklists / block lists
- Academic papers
- Government advisories
- Your own discoveries e.g. log files...
- Cyber security associations e.g. OWASP...
- Cert threat advisories

Legend:
- No trust at all
- Reasonable level of trust
- High level of trust
Top Cyber threats (based on ENISA's Top Emerging Threats)

- Spam
- Phishing
- Malicious code: Worms/Trojans
- Web-based attacks
- Botnet activity
- Ransomware/Rogueware/Scareware
- Web application / Injection attacks
- Identity theft/fraud
- Denial of service (DoS, DDoS)
- Exploit kits
- Data breaches
- Cyber espionage
- Information leakage
- Cyber terrorism
- Insider threat
- Physical damage/theft/loss
How much time was lost as a victim of cybercrime?

- 36.4% < 4 hours
- 27.3% 5 - 8 hours
- 13.6% 9 - 24 hours
- 22.7% 25 hours +

Should consumer rights organizations in any country or region be given enhanced powers to sanction heavier legal & financial penalties, when poor security measures result in data breaches or cybercriminal events?

- Yes: 92.90%
- No: 7.10%
Top 6 From stakeholders

1. Education in cybercrime prevention
2. Cyber security management
3. Laws and policies on cybercrime
4. Risks & effects of cybercrime
5. Economic impact of cybercrime
6. Cybercrime definitions and classifications
WE TALK ABOUT RESEARCH TOPICS, BUT WHAT SHOULD BE THE BUDGET?

What should the EU spend on cybersecurity research and why?
CURRENT ESTIMATES, HOW MUCH R&D?

- The annual cost to the global economy from cybercrime is more than **€300 billion Euros**
  
  *McAfee, Intel, & others*

- Cost of cybercrime for the **EU 0.4% of its GDP = €13 billion / annum** (2014 IMF)

- Cybercrime market globally itself of **€15 billion / annum**

- Market for security products and services **€50 billion / annum**

- Compare with EU **0.0005% of its GDP = € 150 million / annum** on Cybercrime R&D e.g H2020?

- Should be EU **0.0025% of its GDP = € 750 million / annum** on Cybercrime R&D = ?

- = **A BETTER RETURN ON INVESTMENT (ROI) FOR EU** - So end result (5 years) reduce Cost of cybercrime for the **EU to €7 billion / annum & develop a €5 billion / annum cyber security industry (10% of the world market)**

- Example ‘SISSDEN’ project aim to reduce cost of cybercrime in EU by **€ 100 million / annum & in 5 years develop an EU company earning €25 million / annum**
Cholera / Ebola (Disease)

BankTexeasy / Tilon (Banking Malware)
Epidemiology: the science that studies the patterns, causes, and effects of health and disease in defined populations.

Cholera, Bubonic Plague, Aids, Ebola!

Ransomware, Stuxnet, Zeus, Conficker, BlackEnergy…. + DDoS, Spam…

Cybercrime & Cyber Threats = the public health analogy – an epidemiological approach. – i.e. patterns & causes

Just to note: The science of: Public health & epidemiology = >150 years – Cybercrime & Threat Data research = < 10 years

Policy decisions and evidence-based practice by identifying threats and targets for prevention.
A methodological approach

- **CyberROAD Triad of evidence-based practice**
  - to validate all the choices made in cybercrime metrics and threat data

- on the basis of the **available data and interaction of the data** coming from:
  - A. scientific evidence
  - B. practitioners and expertise knowledge (e.g., industry)
  - C. stakeholders and consumers

- This is useful for:
  - D. guaranteeing that the underlying assumptions agree with the available evidence
  - E. defining precise metrics

- Long-term goal of the proposed methodology: making the fight against cybercrime and cyber threats an **empirical science**
WHAT ABOUT CYBERTERRORISM?
“We are in a ‘technology arms race’ with terrorists recruiting an army of hackers to their cause”
– The Guardian

“If our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage but of lives lost.”
– The Independent

"[The Paris attacks] have added... urgency to countering the extremism problem. Dealing with material online is the first item on the agenda."
- EU's counter-terrorism chief
Water Utilities Threats

**Status:**
Utilities (such as water, gas and electricity) are managed by automated system. Industrial control system (ICS) threat landscape has evolved significantly over the recent years.

**Cyberterrorists objectives:**
- aim at disrupting the water delivery service
- prevent people from getting water
- poison the water distribution network (cause disease or death)
- targeting wastewater treatment plants to cause ecological disasters.

Wearable Devices Threats

**Status:**
Wearable devices (e.g. health implant) rely on remote database servers or computer clouds to store and retrieve information

**Cyberterrorists objectives:**
- theft of sensitive information
- physical harm to human agents (a.k.a. cyber murder), e.g. by tampering with a health sensor used for heartrate monitoring and causing an heart attack.

source: http://sourcebits.com/app-development-services/mobile-app-development/
Countermeasures & Research Gaps

Improved authentication and anonymization

Improved monitoring of critical materials we all depend on, e.g. water

Advanced malware defence and shielding.

Behavioural-based intrusion detection system.

Crypto-analytical algorithms.

Infrastructures for attack simulation.
“The cleaner a nation’s national cyberspace, less attacks on its national infrastructure & lower numbers of cybercrime victims”

Disease Control? Epidemiology…?
"Prevention of the disease is better than treatment or control"

Thanks for listening
### General Cyber Metrics

- **2.8 Billion users of the Internet (~39% world population)**
- **Over 100 billion emails processed / day**
- **959 million websites — 39 million / month added (4%).**
- **IP addresses - IPv4 = 4,294,967,296 ($2^{32}$) - IPv6 = of 2128**
- **1.4 million browser user agents - bots**

### Cybercrime – Malicious Activity

#### Measuring malicious events

<table>
<thead>
<tr>
<th>Event</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>85% of processed emails are spam</td>
<td>Barracuda</td>
</tr>
<tr>
<td>7% of all urls maliscious</td>
<td>Barracuda</td>
</tr>
<tr>
<td>Public Block List count: 1,018,203,532 IP addresses</td>
<td>Spamhaus</td>
</tr>
<tr>
<td>250 million in total identifiable malware</td>
<td>AV-Test Org</td>
</tr>
<tr>
<td>200,000 new malicious programs registered</td>
<td>AV-Test Org</td>
</tr>
<tr>
<td>1 million+ measurable cyber-attacks every day</td>
<td>Akamai</td>
</tr>
<tr>
<td>330 active Real-time Blackhole Lists (RBL &amp; DNSBL)</td>
<td>Hostexploit</td>
</tr>
<tr>
<td>€ 5.9 million is the average annualized cost of data breaches</td>
<td>Ponemon Institute</td>
</tr>
<tr>
<td>10.4% net increase cost of data breaches over the past year</td>
<td>Ponemon Institute</td>
</tr>
<tr>
<td>250,000 – 500,000 malicious binaries / day</td>
<td>Shadowserver</td>
</tr>
<tr>
<td>~280 million malicious binaries collected</td>
<td>Shadowserver</td>
</tr>
<tr>
<td>6 / 10 million unique IP’s sinkholed / day</td>
<td>Shadowserver</td>
</tr>
<tr>
<td>900,000 malicious domains / day</td>
<td>Shadowserver</td>
</tr>
<tr>
<td>500 of 52,000 ASNs worldwide (4%) account for 85% of malicious activity</td>
<td>Hostexploit</td>
</tr>
</tbody>
</table>
Considerations for Our Digital Future?

What?

- Quantification, what are the metrics? What are we dealing with?

- Cost of cybercrime for the EU **0.4% of its GDP = €13 billion / annum** (2012 IMF)

- Compare with EU **0.0005% of its GDP = €150 million / annum** on Cybercrime R&D e.g H2020

- So what proportion of EU research budget should go to reducing this cost, i.e. what should be researched?

The garbage?

- Infrastructure: Misconfigured, outdated, open resolvers - Update the systems a legal responsibility?

- Tools: Viruses, Malware, Botnets & the Zombies

**Cleaning up the garbage, who is responsible?**

**Even more specific who is going to pay for the clean up?**