STATISTICS
Connected Life

- 7,27 bn current world population
- 90 bn Google searches so far this year

- 3,01 bn Internet users worldwide

- 7 bn mobile devices worldwide

- 70% Internet penetration in Europe

- 51% of employees connect to unsecured wireless networks with their smartphones

- 2 mln blog posts written today

- 423 mln Tweets sent today

- 1,4 bn monthly active users

- 24 bn total connected devices by 2020
- 12 bn mobile connected devices

- 115 bn Emails sent today
19% Android users encountered a mobile threat

38% of user computers subjected to at least one web attack

15,577,912 malicious mobile apps worldwide

12,100 mobile banking Trojans

123,054,503 unique malicious objects detected

1,432,660,467 attacks launched from online resources

Cybercrime costs annually $445 billion or ~1% of global income

over 307 new cyber threats every minute, more than 5 every second
Some scary statistics: SPAM

• 7 Billion mobile devices
Some scary statistics: SPAM

• 7 Billion mobile devices
• 3 Billion internet users
Some scary statistics: SPAM

- 7 Billion mobile devices
- 3 Billion internet users
- 115 Billion emails per day
Some scary statistics: SPAM

- 7 Billion mobile devices
- 3 Billion internet users
- 115 Billion emails per day
- 90%+ of those are spam
Some scary statistics: SPAM

- 7 Billion mobile devices
- 3 Billion internet users
- 115 Billion emails per day
- 90%+ of those are spam

103,500,000,000
Email spam per day
More Scary Statistics

• 15,000,000 malicious mobile apps
• 123,000,000 malicious objects detected annually
• 307 new cyber threats happen every minute
Just a few more …

Q3 2014

186,094 URLs analyzed
38,562 malicious (20%)
Just a few more …

Q3 2014
186,094 URLs analyzed
38,562 malicious (20%)

Q4 2014
804,264 URLs analyzed
703,542 malicious (88%)
## Spamhaus Blacklistings May 31, 2015

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Number of Current Live Spam Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>2519</td>
</tr>
<tr>
<td>2</td>
<td>China</td>
<td>1154</td>
</tr>
<tr>
<td>3</td>
<td>Russian Federation</td>
<td>871</td>
</tr>
<tr>
<td>4</td>
<td>Japan</td>
<td>569</td>
</tr>
<tr>
<td>5</td>
<td>Ukraine</td>
<td>530</td>
</tr>
<tr>
<td>6</td>
<td>United Kingdom</td>
<td>362</td>
</tr>
<tr>
<td>7</td>
<td>Brazil</td>
<td>344</td>
</tr>
<tr>
<td>8</td>
<td>India</td>
<td>339</td>
</tr>
<tr>
<td>9</td>
<td>Germany</td>
<td>338</td>
</tr>
<tr>
<td>10</td>
<td>Turkey</td>
<td>289</td>
</tr>
</tbody>
</table>
Spamhaus CBL Blacklist - May 2015

1. China
2. India
3. Vietnam … #14 Egypt
Per-Capita Infections

<table>
<thead>
<tr>
<th>#</th>
<th>Country</th>
<th>% Rate per capita</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dominica</td>
<td>8.36%</td>
</tr>
<tr>
<td>2</td>
<td>Côte d'Ivoire</td>
<td>2.18%</td>
</tr>
<tr>
<td>3</td>
<td>Algeria</td>
<td>1.70%</td>
</tr>
<tr>
<td>5</td>
<td>Macedonia</td>
<td>1.54%</td>
</tr>
<tr>
<td>6</td>
<td>Armenia</td>
<td>1.52%</td>
</tr>
<tr>
<td>9</td>
<td>Timor-Leste</td>
<td>1.18%</td>
</tr>
<tr>
<td>10</td>
<td>Belarus</td>
<td>1.17%</td>
</tr>
<tr>
<td>11</td>
<td>Mauritius</td>
<td>0.98%</td>
</tr>
<tr>
<td>12</td>
<td>Pakistan</td>
<td>0.91%</td>
</tr>
<tr>
<td>16</td>
<td>Libya</td>
<td>0.85%</td>
</tr>
<tr>
<td>18</td>
<td>Taiwan</td>
<td>0.80%</td>
</tr>
<tr>
<td>19</td>
<td>Tunisia</td>
<td>0.80%</td>
</tr>
<tr>
<td>20</td>
<td>Kazakhstan</td>
<td>0.77%</td>
</tr>
</tbody>
</table>

Picture is much worse when we look at the data – for individuals, government and companies in developing nations, botnet infections by malware are disproportionately severe issues.
Spam per Capita

<table>
<thead>
<tr>
<th>#</th>
<th>Country</th>
<th>% Rate per capita</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dominica</td>
<td>1.28</td>
</tr>
<tr>
<td>2</td>
<td>Kyrgyzstan</td>
<td>0.949</td>
</tr>
<tr>
<td>3</td>
<td>Armenia</td>
<td>0.594</td>
</tr>
<tr>
<td>6</td>
<td>Botswana</td>
<td>0.486</td>
</tr>
<tr>
<td>7</td>
<td>Kazakhstan</td>
<td>0.443</td>
</tr>
<tr>
<td>8</td>
<td>Vanuatu</td>
<td>0.406</td>
</tr>
<tr>
<td>9</td>
<td>Macedonia</td>
<td>0.364</td>
</tr>
<tr>
<td>12</td>
<td>Israel</td>
<td>0.283</td>
</tr>
<tr>
<td>18</td>
<td>Georgia</td>
<td>0.207</td>
</tr>
<tr>
<td>19</td>
<td>Cayman Islands</td>
<td>0.202</td>
</tr>
<tr>
<td>20</td>
<td>Libya</td>
<td>0.201</td>
</tr>
</tbody>
</table>

We see poorly-administered networks in relatively industrialized nations as well, but spam (an indicator of compromised and infected machines) is mostly an effect of economics and scarcity of security resources, a cost centre.
Distributed Denial of Service Attacks (DDoS)

Q1 2013

- 2934 DDoS attacks per day
- Peak attack measured is at 253 Gbps
- Over a thousand botnets were detected.
THREAT LANDSCAPE
North African hackers infiltrate 100s of French websites

The attacks come as a group which declared sympathies for Islamic State hacked US America’s Central Command's Twitter account – Agence France-Presse
Cyber Crime in North Africa a 'New and Very Recent Trend’ - 2010

Cyber experts with United Nations have cautioned about a recent trend in online attacks originating from African countries.

- “It is important to note that the ‘minds’ behind the crime organisations have recently moved to North Africa, which is a totally new and very recent trend,” Francesca Bosco, of the United Nations Inter-regional Crime and Justice Research Institute, said in an interview with Express.

- Detailing the geographical specialties in the evolution of cyber crimes, Bosco said 419 scams started in the 1980s with faxes being sent to companies and entrepreneurs (but now involve all manner of attacks).
DETECTION
Detection Methods

Reports
- Users (FeedBack Loops (FBL))
- Trusted sources (network to network)
- Popular and technical media & press
- Spam Reporting Centres
- Intra-CERT coorperation

Spamtrap Networks
- Shadowserver
- Abusix
- Threatwave
SOLUTIONS
Best Practices to Address Online, Mobile, and Telephony Threats

Prepared by the Messaging, Malware and Mobile Anti-Abuse Working Group and the London Action Plan
Purpose of the Report

- To provide a plain language description of the threats facing businesses, network providers and consumers in the online and mobile threat environment
- To suggest best practices for industry and governments to address these threats
Background

- October 2011: members of LAP and M³AAWG presented to the OECD Committee on Consumer Policy (CCP) on addressing future online threats.
- October 2012: Best Practices to Address Online and Mobile Threats was published
- The original report was divided into four key sections:
  i. Malware and Botnets
  ii. ISP and DNS
  iii. Phishing and Social Engineering
  iv. Mobile Threats
New Report

- Operation Safety-Net: Best Practices to Address Online, Mobile and Telephony Threats

- This 2nd version includes:
  - updates to the four original sections,
  - Voice over Internet Protocol (VoIP) and Voice Telephony fraud,
  - Caller ID Spoofing,
  - abuse issues for Hosting and Cloud Services, and
  - online harassment.
The Evolution of Online Threats

- Since 2006 there been significant evolution of online threats and the emergence of novel attacks.
- The tools used to defraud and steal in the online and mobile environment today are increasingly sophisticated.
- The OECD, LAP, M3AAWG and other international organizations have been effective in developing public-private coordination and cross-organizational collaboration.
- Globally, there continues to be a need for stronger, more comprehensive legislation and regulatory regimes, cross-border cooperation, and implementation of best practices.
Bibliography

Spamhaus network statistics
- http://cbl.abuseat.org/nas.html

M3AAWG Email & Botnet Statistics
- https://www.maawg.org/email_and_bot_metrics_report

Arbor Networks Atlas Dashboard
- https://atlas.arbor.net
Bibliography

North African hackers infiltrate 100s of French websites
middleeasteye.net/news/north-africa-hackers-infiltrate-100s-french-websites-564661351

Cyber Crime in North Africa a 'New and Very Recent Trend'

Phishing Gang is Audacious Manipulator – Krebs on Security
krebsonsecurity.com/2015/05/phishing-gang-is-audacious-manipulator/

The Sakawa Boys: Inside the Bizarre Criminal World of Ghana’s Cyber-Juju Email Scam Gangs
Bibliography

North African Spammer & Hackers – Social media

https://www.facebook.com/krystal.teams?ref=br_rs
Bibliography

FBLs
- Word to the Wise ISP Feedback Loop Information
  https://wordtothewise.com/isp-information/

Spamtrap Networks
- Shadowserver https://www.shadowserver.org
- Abusix https://abusix.com
- Threatwave https://www.threatwave.com

Spam Reporting Centres
- U.S. Federal Trade Commission
  https://www.ftccomplaintassistant.gov
- Industry Canada http://fightspamgc.ca
Operation Safety-Net

M3AAWG: https://www.maawg.org/published-documents
http://londonactionplan.org
http://cauce.org


NEW M3AAWG Documents
Bibliography

• NEIL@CAUCE.ORG
• Jerry Upton
  jerry.upton@M3AAWG.org
• admin@londonactionplan.org