Santé publique pour la prévention des attaques par logiciels malveillants

Fanny Lalonde Lévesque
Étudiante au doctorat, Polytechnique Montréal
Chercheuse appliquée, Element AI

Journée de la recherche du FRQNT
16 mai 2018
## Computer threats

**What’s the problem?**

| **2.3** connected devices *per capita* in 2016 | ✈️ in 2021 ¹  |
| 4.6 trillion of Internet users in 2021 ¹ |
| **285,000** new malware samples everyday in 2017 ² |
| **136** public data breaches in 2005 | 🔒,885 in 2018 ³ |
| Ransomware alone costed **5** billion USD in 2017 ⁴ |
| Global cost of attacks estimated at **6** trillion USD in 2021 ⁴ |

---

Prevention

What are the solutions?
Public health

“Public health is defined as the science of protecting the safety and improving the health of communities through education, policy making and research for disease and injury prevention.”

Public Health Agency of Canada
Public health framework

1. Define the problem

2. Identify risk and protective factors
   - Identify the causes and correlates related to the problem

3. Develop and test strategies
   - Develop and evaluate prevention strategies

4. Ensure global adoption
   - Implement and disseminate the strategies
Application to malware prevention

1. Define the problem
   - Study the trends and patterns of malware attacks

2. Identify risk and protective factors
   - Identify the causes and correlates related to Malware attacks

3. Develop and test strategies
   - Develop and evaluate strategies aimed at preventing and/or reducing malware attacks

4. Ensure global adoption
   - Implement and promote strategies proven effective at preventing and/or reducing malware attacks
Application to malware prevention

Define the problem

Study the trends and patterns of malware attacks

Identify risk and protective factors

Identify the causes and correlates related to Malware attacks

Develop and test strategies

Develop and evaluate strategies aimed at preventing and/or reducing malware attacks

Ensure global adoption

Implement and promote strategies proven effective at preventing and/or reducing malware attacks
Identify risk and protective factors

<table>
<thead>
<tr>
<th>Environment and politics</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Economy</td>
</tr>
<tr>
<td></td>
<td>Education</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>Demographics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Characteristics</td>
</tr>
<tr>
<td></td>
<td>Behavior</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware</td>
</tr>
</tbody>
</table>
Identify risk and protective factors

| Environment and politics | • Technology  
|                        | • Economy  
|                        | • Education  
|                        | • Governance |
| User                   | • Demographics  
|                        | • Characteristics  
|                        | • Behavior |
| System                 | • Software  
|                        | • Hardware |
National-level factors

What national-level factors correlate with the rate of malware infections?

10+ M
10+ million unprotected devices running Windows
Malware infections from MSRT
June to September 2014

186 countries
15 factors
Economy
Education
Technology
Cybersecurity

National-level factors

National-level factors

### National-level factors

#### Multi-level risk analysis by HDI status

<table>
<thead>
<tr>
<th>HDI Status</th>
<th>Number of Countries</th>
<th>Average Infection Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;= 0.8</td>
<td>45</td>
<td>10%</td>
</tr>
<tr>
<td>0.8 &gt; HDI</td>
<td>74</td>
<td>26%</td>
</tr>
<tr>
<td>&gt;= 0.55</td>
<td>26</td>
<td>38%</td>
</tr>
</tbody>
</table>

Identify risk and protective factors

- Environment and politics
  - Technology
  - Economy
  - Education
  - Governance

- User
  - Demographics
  - Characteristics
  - Behavior

- System
  - Software
  - Hardware
User-level factors

Are age and gender independent risk factors of malware victimisation?

10+ M
10+ million devices running Windows 10
Malware encounters from Windows Defender
October to December 2015

Male Female
0-17, 18-24, 25-34, 35-49, 50+

### User-level factors

Risk analysis of **age** and **gender**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.32</td>
<td>Male are 1.32 more likely to encounter malware than female</td>
<td>26% male, 19% female</td>
</tr>
<tr>
<td>1.99</td>
<td>Age group 18-24 is 1.99 more likely to encounter malware than the 50+ age group</td>
<td>29% age 18-24, 30% 50+, 26% 60+, 21% 70+, 17% 80+</td>
</tr>
</tbody>
</table>

User-level factors

Risk analysis of age by malware types

F. Lalonde Lévesque et al., Age and gender as independent risk factors of malware victimisation, BHCI 2017.
User-level factors

Risk analysis of **age** by **malware types**

Risk analysis of age by malware types

F. Lalonde Lévesque et al., Age and gender as independent risk factors of malware victimisation, BHCI 2017.
User-level factors

Risk analysis of gender by malware types

User-level factors

Risk analysis of gender by malware types

Findings and implications

Identification of risk and protective factors at the national and user level

Identification of at-risk populations

Direction and magnitude of factors differ depending on the context

Support evidence-based decision making and prioritisation of effort

Design of targeted interventions

Development of ecologic strategies
Future perspectives

- Establish sound causation
- Investigate more multi-level factors
- Extend the application of the public health model to information security
About me...
Thanks!
Questions?

Fanny Lalonde Lévesque
fanny@elementai.com