Does Your Threat Model Consider Country and Culture?
A Case Study of Brazilian Internet Banking Security to Show that it Should!

Marcus Botacin
Federal University of Paraná, Brazil
@MarcusBotacin

By Evgeny Lopatin on November 28, 2018. 10:00 am


Cryptocurrency miners that infect the computers of unsuspecting users essentially operate according to the...
Companies will invest billions in...

What is the True Cost of a Ransomware Attack? | 6 Factors to Consider

January 8, 2020
by Yotam Gutman

Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021

In Brazil...

Let's Move Banking to Computers!

Let's Move Banking to the Web!

Let's Move Banking to Mobile!

Implications

Recommendations
Years Later...

Introduction

Let's Move Banking to Computers! Let's Move Banking to the Web! Let's Move Banking to Mobile!

Implications

Recommendations
The Brazilian Banking System

- Desktop-based Apps
- Web-based Apps
- Mobile-based Apps
Let’s Move Banking to Computers!
Internet Banking Desktop Clients

- **Local Background**: Daily price changes due to high inflation. Hard to manually keep up with it.
- **Technical Solution**: Banks created Internet Banking Desktop apps with security configurations under their control.
- **Attacker’s Decision**: Phishing Applications.
Introduction

Let’s Move Banking to Computers! Let’s Move Banking to the Web! Let’s Move Banking to Mobile!

Implications

Recommendations
A Predictable Future

Introduction

Let’s Move Banking to Computers!
Let’s Move Banking to the Web!
Let’s Move Banking to Mobile!

Implications

Recommendations

Today, 15:15

SUPORTE BB: Seu BB PROTECAO Nao Foi Ativado, Siga Orientacao no awDG evite o Cancelamento de seus acessos

Boa tarde
Por favor, aguarde...
Estamos verificando os dados informados.
The Boleto’s case

Introduction

Let’s Move Banking to Computers! Let’s Move Banking to the Web! Let’s Move Banking to Mobile!

Implications

Recommendations
Boleto’s Malware

- **Local Background:** Banks were computerized, but the population was not.
- **Technical Solution:** A new payment method accessible both via digital and physical means.
- **Attacker’s Decision:** Attackers created malware samples that modify the boleto’s bar code before they are printed.
Let’s Move Banking to the Web!
Source: 40K payloads collected from Brazilian bank user’s by a bank’s CSIRT.
Web-based Internet Banking

- **Local Background**: Not all bank customers have their own desktops, although some have access to the Internet via third party’s computers.
- **Technical Solution**: Internet Banking moved to the Web via Java applets.
- **Attacker’s Decision**: Attackers can now assume all computers have Java installed, so they developed Java malware.
Tracking the Attackers

Evolution of Cleosvaldo malware family

PE32/DLL
PE32/CPL (UPX)
PE32/CPL (PEC2)
PE32
CMD

Year
2012 2013 2014 2015 2016 2017 2018

Introduction
Let's Move Banking to Computers!
Let's Move Banking to the Web!
Let's Move Banking to Mobile!
Implications
Recommendations
Let’s Move Banking to Mobile!
The case of WhatsApp

- **Local Background:** Unrestricted data plans are expensive. Limited plans with unlimited WhatsApp access.

- **Technical Solution:** Let’s support bank operations via WhatsApp messages.

- **Attacker’s Decision:** Let’s attack Whatsapp directly.

Implications
## Percentage of Samples that Exhibited Specific Behaviors in [7]’s and in BR, US, and JP 2017 Datasets.

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Bayer et al.</th>
<th>BR</th>
<th>US</th>
<th>JP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts file modification</td>
<td>1.97%</td>
<td>1.09%</td>
<td>0.04%</td>
<td>0.92%</td>
</tr>
<tr>
<td>File creation</td>
<td>70%</td>
<td>24%</td>
<td>64%</td>
<td>70%</td>
</tr>
<tr>
<td>File deletion</td>
<td>42%</td>
<td>12%</td>
<td>34%</td>
<td>34%</td>
</tr>
<tr>
<td>File modification</td>
<td>79%</td>
<td>16%</td>
<td>63%</td>
<td>46%</td>
</tr>
<tr>
<td>IE BHO installation</td>
<td>1.72%</td>
<td>1.03%</td>
<td>0%</td>
<td>0.59%</td>
</tr>
<tr>
<td>Network traffic</td>
<td>55%</td>
<td>96%</td>
<td>53%</td>
<td>52%</td>
</tr>
<tr>
<td>Registry key creation</td>
<td>64%</td>
<td>29%</td>
<td>48%</td>
<td>45%</td>
</tr>
<tr>
<td>Process creation</td>
<td>52%</td>
<td>16%</td>
<td>45%</td>
<td>50%</td>
</tr>
<tr>
<td>Setting AutoRun</td>
<td>35%</td>
<td>14%</td>
<td>22%</td>
<td>21%</td>
</tr>
</tbody>
</table>
Recommendations
Recommendations

- Develop threat models that consider the regional and socio-cultural aspects of the targeted populations.
  - Representativity & Reproducibility guidelines
- Incentivize localized and focused research work with specific datasets.
  - More focused venues (e.g., ENIGMA)
- Promote security companies’ local teams.
  - Easier when we are all Working From Home (WFH).
- Share local information with the World.
  - Where is your paper about the threat scenario in your country?
Does Your Threat Model Consider Country and Culture?
A Case Study of Brazilian Internet Banking Security to Show that it Should!

Thank you!

Contact: mfbotacin@inf.ufpr.br or @MarcusBotacin
Our Website: secret.inf.ufpr.br

Marcus Botacin
Federal University of Paraná, Brazil
@MarcusBotacin