



ENIGMA 2021, SECURITY AND PRIVACY IDEAS THAT MATTER
FEB 1-3, 2021, OAKLAND, CA

Does Your Threat Model Consider Country and Culture?

A Case Study of Brazilian Internet Banking
Security to Show that it Should!

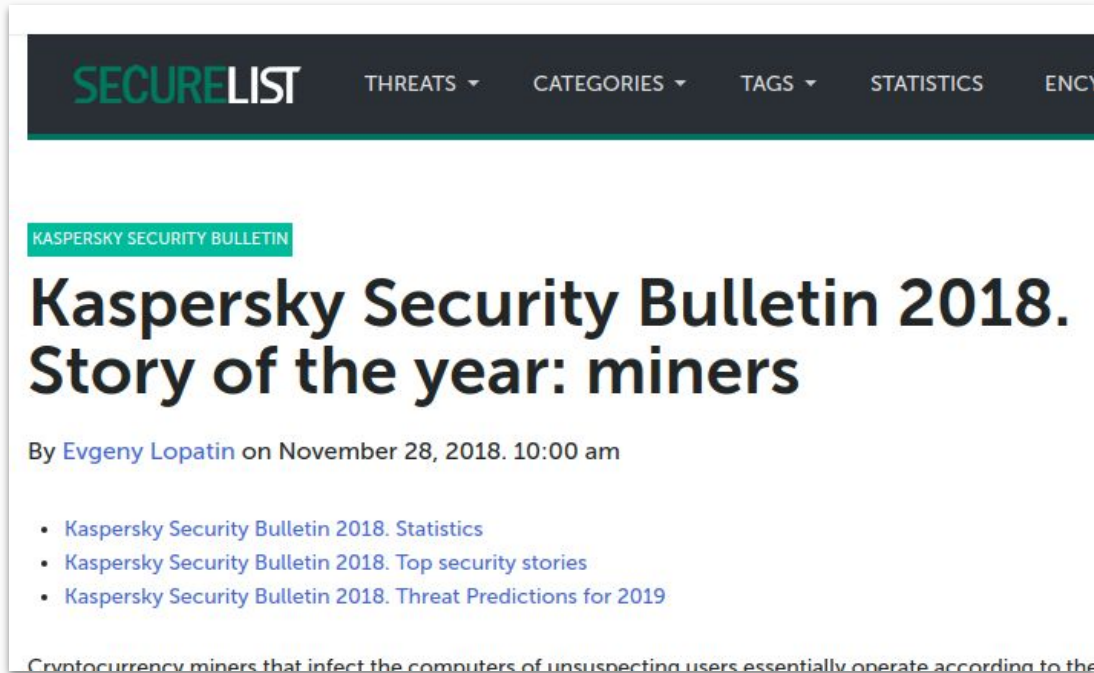


Marcus Botacin

Federal University of Paraná, Brazil

@MarcusBotacin

The Year of...



The screenshot shows the top of a web page with a dark navigation bar. The 'SECURELIST' logo is on the left, and navigation links for 'THREATS', 'CATEGORIES', 'TAGS', 'STATISTICS', and 'ENCYCLOPEDIA' are on the right. Below the navigation bar, a teal banner reads 'KASPERSKY SECURITY BULLETIN'. The main headline is 'Kaspersky Security Bulletin 2018. Story of the year: miners'. The author is 'By Evgeny Lopatin on November 28, 2018. 10:00 am'. A list of three links is provided: 'Kaspersky Security Bulletin 2018. Statistics', 'Kaspersky Security Bulletin 2018. Top security stories', and 'Kaspersky Security Bulletin 2018. Threat Predictions for 2019'. The beginning of the article text is visible at the bottom: 'Cryptocurrency miners that infect the computers of unsuspecting users essentially operate according to the'.

SECURELIST THREATS ▾ CATEGORIES ▾ TAGS ▾ STATISTICS ENCYCLOPEDIA

KASPERSKY SECURITY BULLETIN

Kaspersky Security Bulletin 2018. Story of the year: miners

By [Evgeny Lopatin](#) on November 28, 2018. 10:00 am

- [Kaspersky Security Bulletin 2018. Statistics](#)
- [Kaspersky Security Bulletin 2018. Top security stories](#)
- [Kaspersky Security Bulletin 2018. Threat Predictions for 2019](#)

Cryptocurrency miners that infect the computers of unsuspecting users essentially operate according to the



The screenshot shows the top of a web page with a dark blue navigation bar. The 'HORNETSECURITY' logo is on the left, and navigation links for 'Company' and 'Services' are on the right. The main headline is '2019: The Year of Ransomware' by 'Jeffery Locke | Dec 12, 2019 | Security Information'. Below the headline is a large yellow box with a black border containing the text 'THE RISE OF RANSOMWARE IN 2019'. The bottom of the page has a dark blue footer with the text 'The Ever-Growing Threat'.

HORNETSECURITY Company ▾ Services ▾

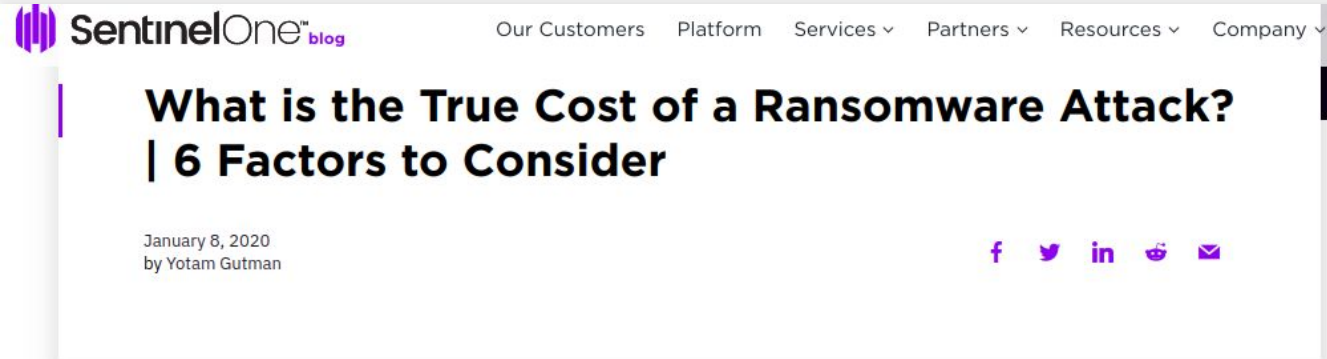
2019: The Year of Ransomware

by [Jeffery Locke](#) | Dec 12, 2019 | [Security Information](#)

THE RISE OF RANSOMWARE IN 2019

The Ever-Growing Threat

Companies will invest billions in...



SentinelOne blog

Our Customers Platform Services ▾ Partners ▾ Resources ▾ Company ▾

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

January 8, 2020
by Yotam Gutman

[f](#) [t](#) [in](#) [r](#) [e](#)



ABOUT RESEARCH LI

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

[f](#) [t](#) [in](#) [e](#)

Cybersecurity Ventures' 2019 Cybersecurity Market Report sponsored by [Secure Anchor](#)

[Home](#) | [Categories](#)

[Home](#) » [Malware](#) » Multiplatform Boleto Fraud Hits Users in Brazil

Multiplatform Boleto Fraud Hits Users in Brazil

Posted on: [March 5, 2015](#) at 8:08 pm Posted in: [Malware](#) Author: [Trend Micro](#)

 **TREND**
MICRO

[Entreprises >](#) [Pour particuliers >](#)

[Produits et solutions](#) [Renseignements](#) [Assistance](#) [Partenaires](#) [À pro](#)

[SecurityNews >](#) [Cybercrime & Digital Threats >](#) [CPL Malware Booms in Brazil](#)

CPL Malware Booms in Brazil

Years Later...



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.



Internet Banking Desktop Clients


Santander
Internet Banking Empresarial

 sexta-feira, 9 de dezembro de 2011

Seja bem-vindo ao Internet Banking Empresarial!


Agência: **0000** Conta: **1111111111**

Usuário:

Senha:

" ,	! @	# \$	% ^	& *	()	- =	
q w	e r	t y	u i	o p	[\	↵	
a s	d f	g h	j k	l ;	' `] "	↵
~ _	z x	c v	b n	m <	> .	: ;	? /
Caps Lock		↑ Shift		Espaço			

confirmar


Internet Banking Empresarial

Banco Santander (Brasil) S.A.
 CNPJ: 90.400.888/0001-42
 Instituição Financeira autorizada a funcionar pelo Banco Central do Brasil



Atualização: 2.2.7- Compilação: 23 - Itaú BankLine

**Itaú Bankline**

AGÊNCIA CONTA

[? Ajuda](#) | [Segurança](#)

Novo Acesso Bankline

▶ Para sua segurança o itaú está disponibilizando um sistema de acesso ao internet banking que proporciona mais segurança nos dados fornecidos. O novo acesso é mais rápido, seguro e muito mais eficiente.

Lembrando que para realizar os processos você precisa estar conectado

A Predictable Future

Today, 15:15

SUPORTE BB: Seu BB
PROTECAO Nao Foi
Ativado, Siga Orientacao no
[REDACTED] [awDG](#) evite o
Cancelamento de seus acessos





Boa tarde

Por favor, aguarde...

Estamos verificando os dados informados.



The Boleto's case

		237-2		23791.11103 60000.000103 01000.222206 1 48622000000000	
Local de pagamento PAGÁVEL PREFERENCIALMENTE NAS AGÊNCIAS DO BRADESCO				Vencimento 29/01/2011	
Cedente NF-e Associacao NF-e				Agência / Código cedente 1111-8/0002222-5	
Data do documento 25/01/2011	Nº documento NF 1 1/1	Espécie doc.	Acelite N	Data processamento 25/01/2011	Carteira / Nosso número 06/00000001001-6
Uso do banco	Carteira 06	Espécie R\$	Quantidade	(X) Valor	(-) Valor documento R\$ 20,000,000.00
Instruções (Texto de responsabilidade do cedente) Não receber após o vencimento. Boleto 1 de 1 referente a NF 1 de 06/05/2008 com chave 3508-0599-9990-9091-0270-5500-1000-0000-0151-8005-1273				(-) Desconto / Abatimentos	
				(-) Outras deduções	
				(-) Mora / Multa	
				(+/-) Outros acréscimos	
				(-) Valor cobrado	
Sacado DISTRIBUIDORA DE AGUAS MINERAIS CNPJ: 00.000.000/0001-91 AV DAS FONTES 1777 10 ANDAR PARQUE FONTES - Sao Paulo/SP - CEP: 13950-000				Cód. baixa	
Sacador / Avalista				Autenticação mecânica - Ficha de Compensação	
					

Boleto's Malware

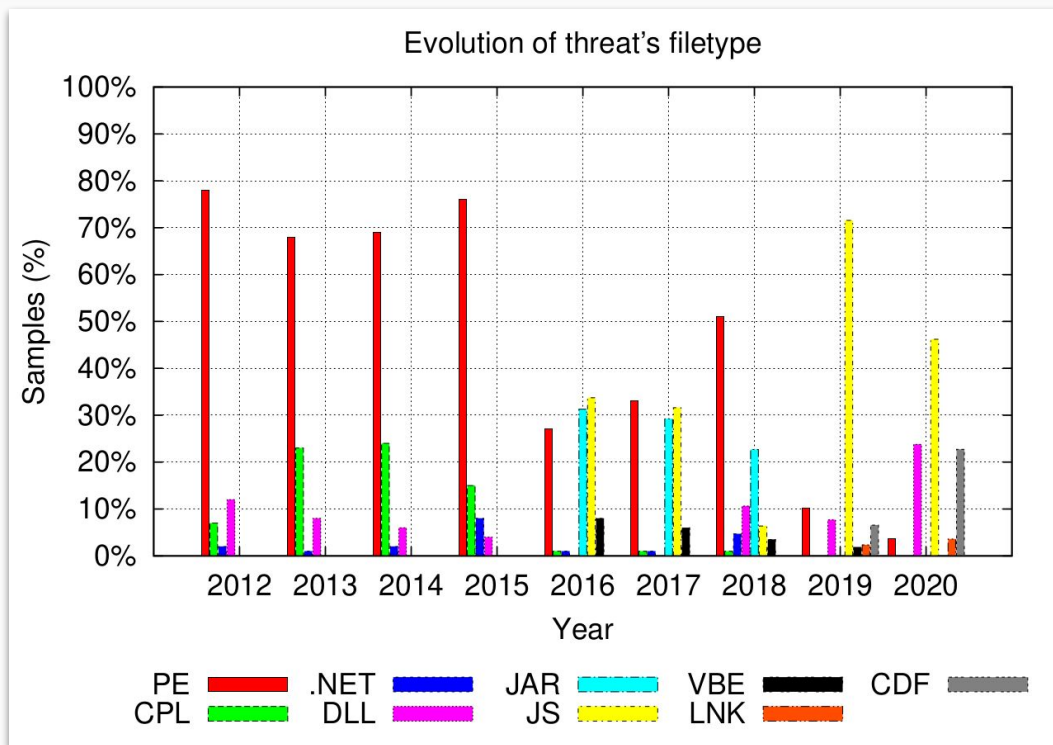
- **Local Background:** Banks were computerized, but the population was not.
- **Technical Solution:** A new payment method accessible both via digital and physical means.
- **Attacker's Decision:** Attackers created malware samples that modify the boleto's bar code before they are printed.



Let's Move Banking
to the Web!



A Profusion of File Formats



Source: 40K payloads collected from Brazilian bank user's by a bank's CSIRT.

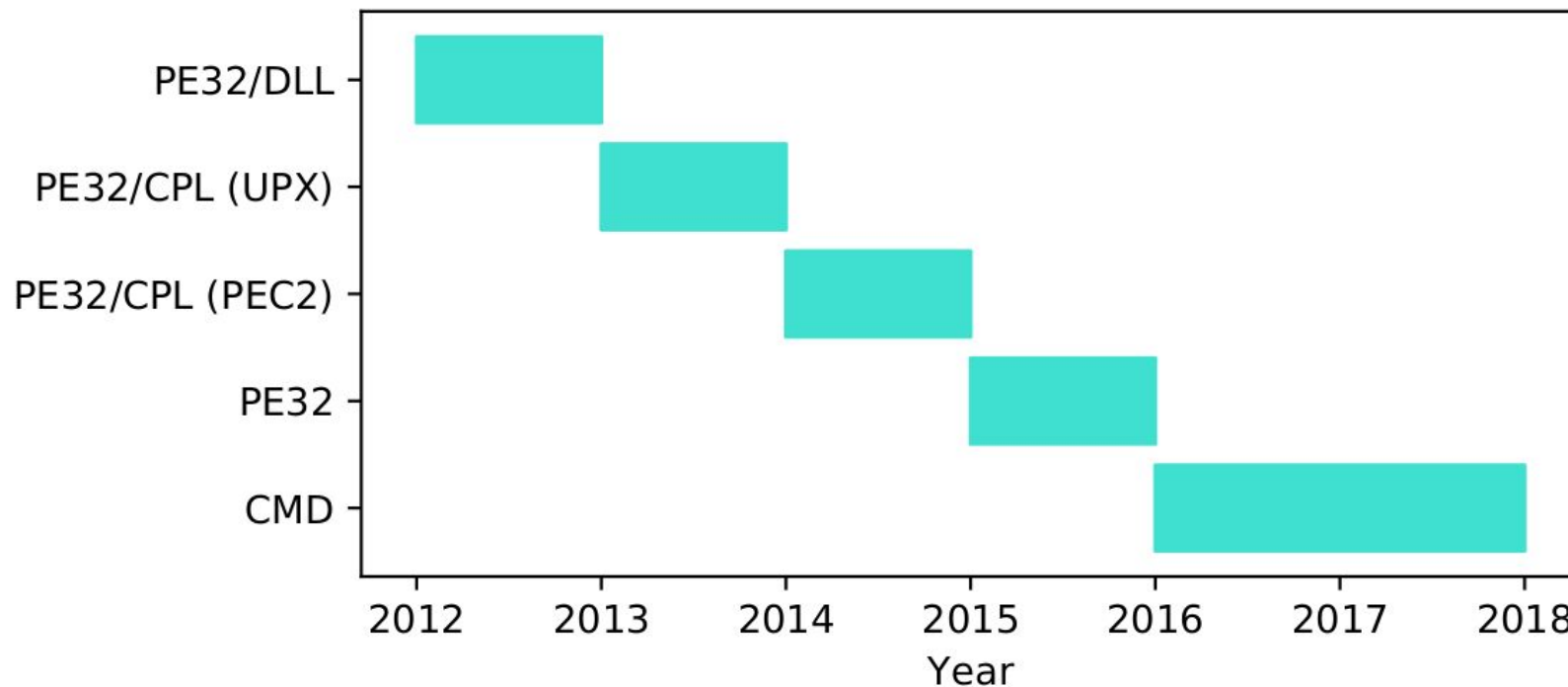
Paper: "One Size Does Not Fit All: A Longitudinal Analysis of Brazilian Financial Malware" ACM TOPS. 2020.

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.



Evolution of Cleosvaldo malware family

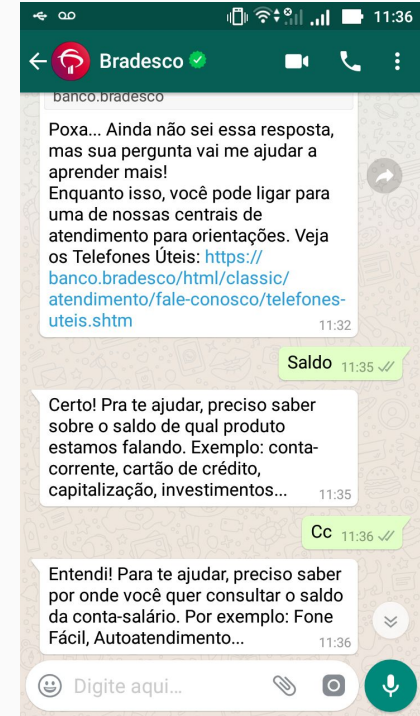
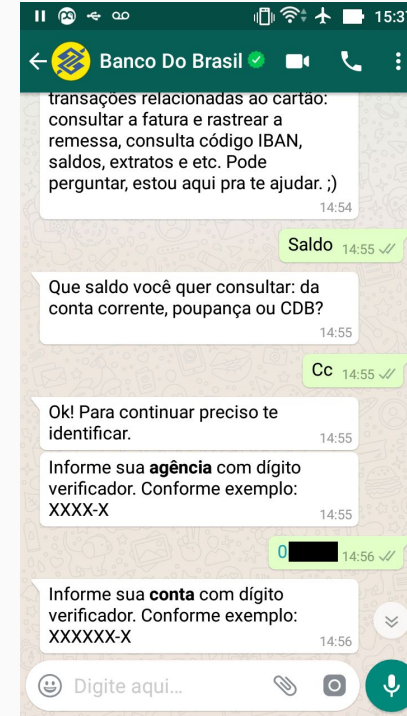


Let's Move Banking to Mobile!



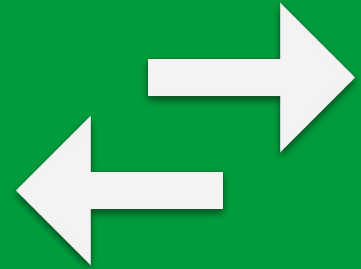
The case of WhatsApp

- **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.



Paper: "The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study". ACM ARES 2019.

Implications

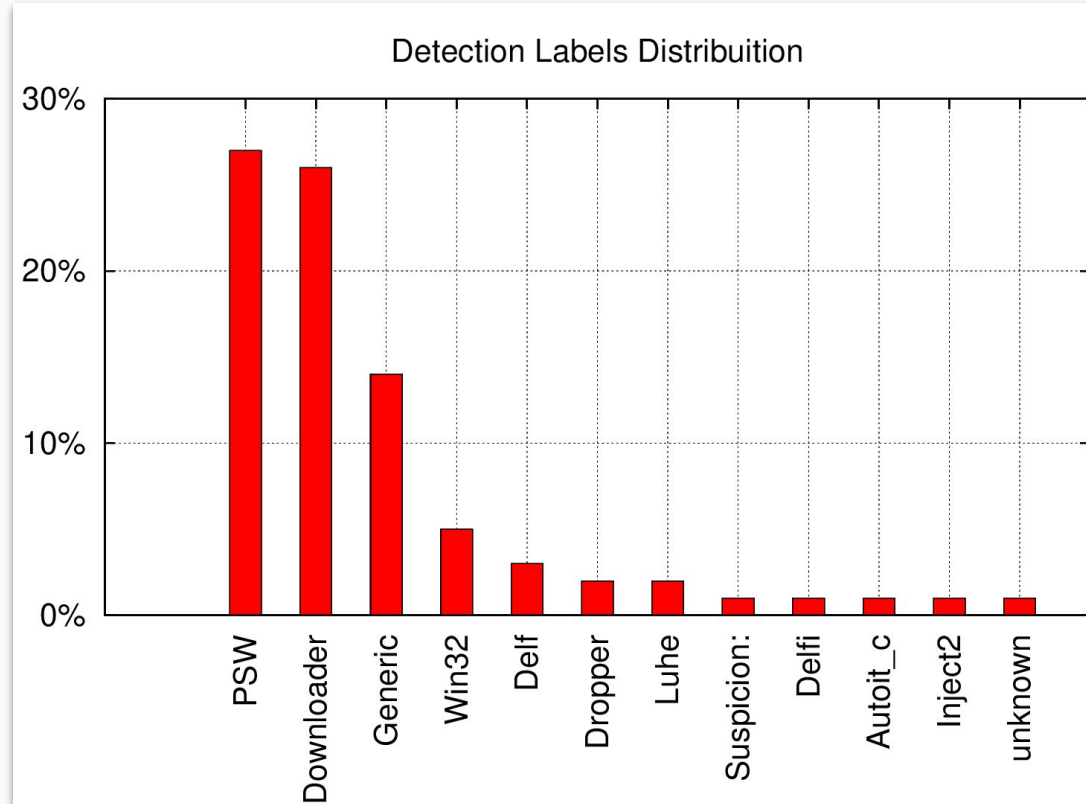


A Scenarios Comparison

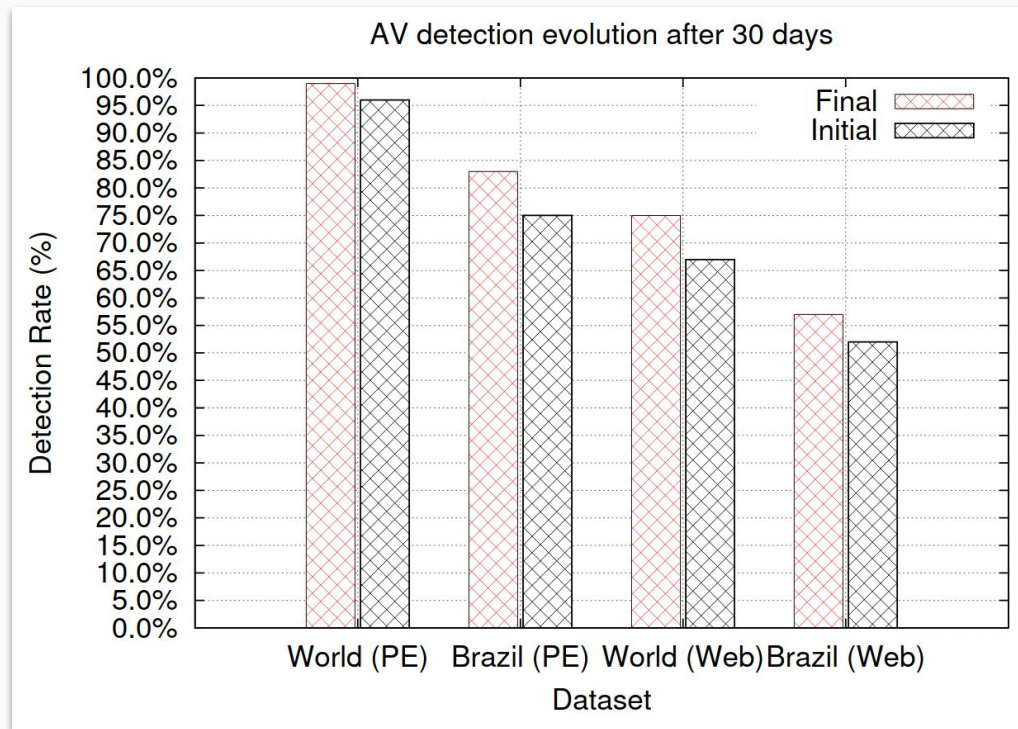
PERCENTAGE OF SAMPLES THAT EXHIBITED SPECIFIC BEHAVIORS IN [7]'S AND IN BR, US, AND JP 2017 DATASETS.

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

A Real Dataset

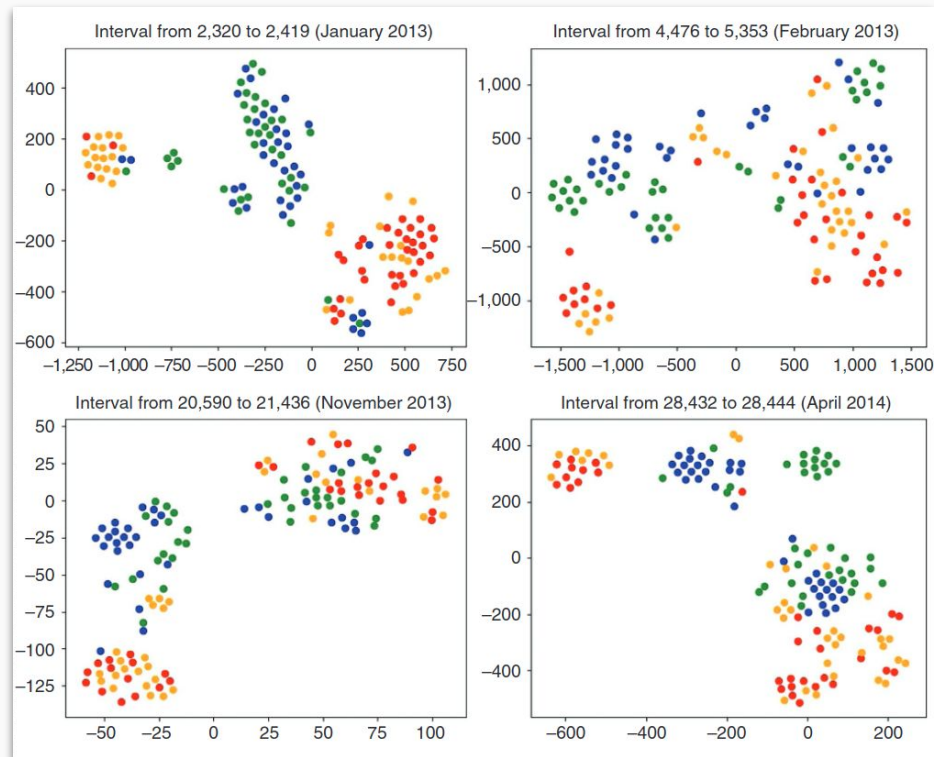
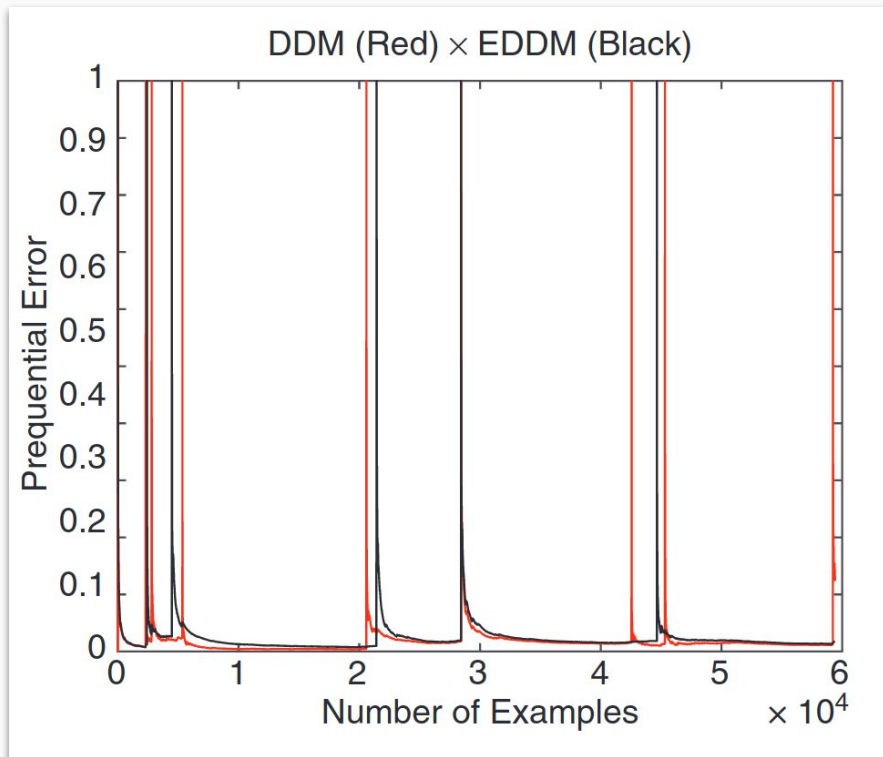


Brazilian Malware vs. Antiviruses



Paper: “We need to talk about antiviruses: challenges & pitfalls of AV evaluations” Computers & Security. 2020.

Brazilian Malware vs. Machine Learning



Paper: “ The Need for Speed: An Analysis of Brazilian Malware Classifiers” IEEE S&P Magazine 2018.

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?



ENIGMA 2021, SECURITY AND PRIVACY IDEAS THAT MATTER
FEB 1–3, 2021, OAKLAND, CA

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](https://twitter.com/MarcusBotacin)

Our Website: secret.inf.ufpr.br



Marcus Botacin

Federal University of Paraná, Brazil

[@MarcusBotacin](https://twitter.com/MarcusBotacin)