CSS | ISSUE BRIEF

Surge in Cybercrime in Brazil

Mehak Dhiman[*]

Edited by: Mihir Vikrant Kaulgud

INTRODUCTION

There is an urgent need for cybersecurity to cope with cyber advancements. This article throws light on cybercrime and its growing magnitude in Brazil. Brazil's process of digitization started in the 1990s with the growth in online banking technology. However, internet use began increasing in the 2000s, with 3% in 2000 to more than 66% in 2016.[1] Concurrently, cyber-attacks became a new trend in Brazil. From Anonymous Brasil's attack on Grupo Globo and National Security Agency's cyber espionage on Brazil in 2013 to hackers disrupting the World Cup in 2014; from a distributed denial of service (DDoS) attack on Brazil's state and municipal websites in 2016, to the recent attack on Brazilian Superior Court of Justice (STJ, in the Portuguese acronym) – Brazil has become the hotbed for cybercrime. Conceivably, most of the cybercrimes in Brazil are economically motivated and target government policies, banks and individuals that deal with e-commerce. This articles disucsses such cyber-crimes, along with the factors which make Brazil so prone to them. With references to categorization of cybercrimes by the International Telecommunications Unit (ITU), the article discusses unconventional and conventional cybercrimes in Brazil.

WHY IS BRAZIL PRONE?

Middle Class

Brazil is an emerging economy with the largest economy in Latin America or Central America. Brazil is also witnessing the expansion of its middle-class population. A growing

[*] ***The Author is a student at the Jindal School of International Affairs and Research Assistant at the Centre for Security Studies, JSIA.***

[1] Muggah, Robert and Nathan B. Thompson. "Brazil Struggles with Effective Cyber-Crime Response" *Instituto Igarapé*, June 15, 2018, https://igarape.org.br/brazil-struggles-with-effective-cyber-crime-response/#%3A~%3Atext%3DIn%20May%202017%2C%20the%20global%2Cand%20the%20energy%20company%20Petrobras.

middle class means a larger labour force and expanding market potential which leads to increase in consumer activities. The fast-growing base of internet users has ratcheted-up the demand for information and communication technologies (ICTs).[2]

Emerging Economy

Emerging economies are at a greater risk of being attacked cybercriminals. Brazil is characterized by a growing consumerism and weak governance/implementation of laws. Moreover, the growth of internet-related activities and the adoption of technology without proper precautions have made Brazil an attractive site for cybercriminals. WEF's Building Resilience Supply Chains Report of 2013 mentions that "[i]nformation technology has enabled supply chains to evolve into interdependent material, financial and information flows. While increasing efficiency, the very complexity and synergies of supply chains expose them to cyber risk." The report also states that "[a] successful breach of any one component could endanger the operation and security of other flows and result in system-wide failure."[3] To maintain economic development, a developing country needs to allow foreign investment, free trade practices and free flow of information. However, these conditions are harmful in the absence of a robust legal system coupled with the presence of political instability.

Surge in Online Activity

Brazil is far ahead of its Latin American and Caribbean (LAC) counterparts in terms of ICTs usage. The use of the internet is widespread in Brazil. Recently the boost in the number of internet and smartphone users has spiked. Most Brazilians store their information online, which is under constant threat of being misused. According to the Latin American Internet UsageStatistics in 2019, 70% of Brazil's population uses the internet and this alsoaccounts for 19% of internet users in Latin America (refer to figure 1).

[2] Diniz, Gustavo, Robert Muggah, and Misha Glenny. 2014 "Deconstructing cyber security in brazil." *Instituto Igarapé*. https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf

[3] World Economic Forum. 2013. "Building Resilience in Supply Chains: An Initiative of the Risk Response Network In collaboration with Accenture" https://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf

Latin American Internet Usage Statistics, 2019[4]

Country	Population Est.2019	Internet Users 30-june-19	%Population (penetration)	%users in Region
Brazil	212,392,717	149,057,635	70.2 %	19.1 %

Fig-1

To keep up with cyber developments Brazil needs to make well-informed and urgent decisions regarding investments in cybersecurity. Bruno Prado, the CEO of information security company UPX says that “investment in digital security in Brazil has not kept pace with average global spending, even considering the increasing numbers of users and utilization of cloud services in the country.” Lack of cybersecurity measures renders most users vulnerable to cyber-attacks. The expected arrival of 5G will also pose a new set of challenges. It is estimated that 5G-driven IoT connections will drive worldwide data to 1 trillion gigabytes, by 2025. This will consequentlyincrease the number of data breaches and cyber-attacks.[5]

<u>Rate of Growth in E-Commerce</u>

The increase in E-commerce automatically poses a greater threat of cybercrimes such as cyber laundering, data breach, cyber theft etc. Brazil was an early adopter of E-banking, and most Brazilians use it, along with ATM transactions and online purchasing. Brazil is second in world in online banking fraud and financial malware. Brazil has a high density of ATMs in the country, with 130 machines per 100,000 adults.[6] With COVID-19 acting as a facilitator, Brazil comes after China when it comes to use of online methods for purchasing.[7] Therefore, e-commerce is the fastestgrowing sector in Brazil and will continue to expand even after COVID.[8]

[4] “Latin American Internet and 2019 Population” *Internetworldstats*, 2019, https://www.internetworldstats.com/stats10.htm

[5] “Why is Brazil so vulnerable to cyber attacks?” *BNAmericas.* 6 January, 2020. https://www.bnamericas.com/en/features/why-is-brazil-so-vulnerable-to-cyber-attacks

[6] “Brazil’s Cybercrime Problem” *Instituto Igarapé.* 18 September, 2015. https://igarape.org.br/en/brazils-cybercrime-problem/

[7] “COVID-19 and E-Commerce: Findingds from a survey of online consumers in 9 countries” *Netcomm Suisse Observatory and United Nations Conference on Trade and Development*. October 2020. https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf

[8] Angelica Mari, “E-Commerce Sales Reach All-Time High in Brazil,” *ZDNet* June 2020, https://www.zdnet.com/article/e-commerce-sales-reach-all-time-high-in-brazil/.

Recently it was found that over 693 COVID-19-related Brazilian cybercriminal websites were created year.[9] Such sites usually target government-driven financial assistance programs which act as a relief for the people worst hit by the pandemic. An example of such a crime is when IBM X-Force used its access to spam databases to look for messages that contained the words "Brazilian government's COVID-19 assistance program" aka "*auxílio emergencial*". Spikes in these messages on May 22, May 27, June 4, and June 8-9, 2020, suggested that criminal campaigns capitalizing on Brazil's government assistance program continue to be active and had increased in number.[10]

Unemployment Rate

Most of Brazil's cyberattacks have an economic motive behind, which indicates it might be connected to the country's problem with unemployment. Brazil's unemployment rate rose from 11.2% in Jan 2020 to 14.6% in October 2020, which is the highest ever unemployment rate recorded in Brazil.[11] Due to loss of jobs and financial security, people are likely to give into "quick money" schemes which direct them to money laundering sites that misuse any data provided by the targeted individual. Unemployment also facilitates impersonation scams. Cybercriminals claim to be from organizations like World Health Organization (WHO) as well as various NGOs asking for monetary donations.

Political Instability

Apart from the economic motive several cybercrimes are motivated by political gains. Social media is vastly used to promote propaganda and manipulate people. This is both a cause and consequence of political instability within a country. In "Dimensions of Cyber Attacks", RobinGandhi et. al. divide politically driven cyberattacks into three subcategories: 1) protest against political actions, 2) protest against laws or public documents, and 3) outrage against acts related to physical violence.[12] Brazil is prone to such unscrupulous cyber activities due to its current socio-political scenario. Brazil's politics, after being run by two

[9] Macedo, Jefferson and Camille Singleton "COVID-19 Cybercrime Capitalizing on Brazil's Government Assistance Program," *Security Intelligence* July 7, 2020, https://securityintelligence.com/posts/covid-19-cybercrime-capitalizing-on-brazils-government-assistance-program/.

[10] Ibid.

[11] "Brazil Unemployment Rate," *Trading Economics*, 2022, https://tradingeconomics.com/brazil/unemployment-rate.

[12] Gandhi, Robin et. al. 2011. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political" *Technology and Society Magazine*, IEEE. 28 - 38. https://www.researchgate.net/publication/224223630_Dimensions_of_Cyber-Attacks_Cultural_Social_Economic_and_Political

moderate parties till 2018, is now dominated Jair Bolsonaro, a niche congressman. Bolsonaro almost immediately gained popularity despite his misogynistic, homophobic, and racist mindset. He won the 2018 elections with ease, with manysaying he won due to his charisma and radical rhetoric. However, there are several indicators which suggest that his campaign was successful solely because he resorted to spreading fake news. His campaign used WhatsApp, YouTube, Twitter and Instagram for micro-targeting and spreading misinformation.[13] There is no doubt Bolsonaro will keep resorting to these means to maintain his popularity.

Weak Cyber Law Enforcement

Law enforcement and administration in Brazil is inefficient. The laws meant to regulate the cyber space are not implemented effectively. This allows people to conduct a number of malicious consequences without consequences. Brazil's digitization is occurring for its cyber regulation to keep up. Brazilian cyber security experts lag behind cyber offenders. Most hackers who target Brazilians are Brazilians themselves.[14] Usually crimes like data breach, ransomware attacks, malware attacks, spread of fake news, cyber espionage etc., are committed by foreign hackers. Unlike other countries, Brazilian hackers' resort to targeting their own country due to unhindered access to information and data accompanied with lack of consequences.

Security vs Privacy

Lack of consensus is harmful for the existing law and order as well as the process of creating new laws. This holds relevance to Brazil's cyber security since the country needs to urgently strengthen its cyber laws for better cyber space regulation. The growing polarization surrounding the debate between security versus privacy makes it difficult for law makers to make effective laws.[15] The advocates of security vouch for tighter government and military control, however, due to the misuse of power and lack of trust the advocates of privacy vouch

[13] Evangelista, Rafael, and Fernanda Bruno. 2019. "WhatsApp and political instability in Brazil: targeted messages and political radicalisation". Internet Policy Review 8 (4). https://policyreview.info/articles/analysis/whatsapp-and-political-instability-brazil-targeted-messages-and-political.

[14] Insikt Group "Pirates of Brazil: Integrating the Strengths of Russian and Chinese Hacking Communities" *Recorded Future*, April 16, 2019, https://www.recordedfuture.com/brazilian-hacking-communities.

[15] Muggah, Robert and Nathan B. Thompson. "Brazil Struggles with Effective Cyber-Crime Response - Instituto Igarapé" 2018.

for greater digital rights, universal access, and net neutrality. The debates seem to be never ending. But regardless of the unrest, the decision makers needto address the problem of laws without giving into the polarization which will result complexand inadequate laws.

Lack of Expertise in the field

In Brazil, there is a wide knowledge gap between the offenders and enforcers of cyber laws. Brazil is the biggest example of rapid digitization met with lack of understanding of the same. It has been predicted that by 2021 there will be 3.5 million unfilled security jobs.[16] Companies within Brazil also frequently talkabout the lack of skilled personnel for cyber security related posts. Policy makers also need to have a better understanding of the cyber domain to be able to come up with effective strategies to counter cyber-threats.

TYPES OF CYBERCRIMES

The International Telecommunication Union (ITU) is a specialized agency of the United Nations(UN) which is concerned with information and communication technologies (ICT). The ITU categorized cybercrimes into four categories:[17]

- Content related Offences: this includes offences such as child pornography, racism, hate speech, glorification of violence, illegal gambling and other illegal content.

- Copyright and Trademark related Offences: this includes counterfeiting brand names, images, logos and other trademarked/copyrighted content. To protect companies from this, copyrightand trademark laws are enforced.

- Computer related Offences: according to the ITU, "this category covers a number of offences that need a computer system to be committed."[18] This category includes computer-related fraud, computer-related forgery, identity theft, and misuse of devices.

[16] "3.5 Million Unfilled Cybersecurity Jobs by 2021: Report," *Economic* Times. June 28, 2018, https://cio.economictimes.indiatimes.com/news/digital-security/3-5-million-unfilled-cybersecurity-jobs-by-2021-report/64776284.

[17] "UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES" *International Telecommunications Union.* April 2009. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

[18] Ibid.

- Combination Offences: This category focuses on cybercrimes which are multidimensional, such as cyber terroris, cyber laundering, and "phishing" to obtain personal data.

These four categories are common, well-known cybercrimes. There are also emerging cyberthreats emerging which also need to be addressed. The following section discusses conventional, complex, and emerging cybercrimes which are more of a threat for Brazil.

CYBER CRIMES RISKING BRAZIL'S CYBER SECURITY

Phishing

Phishing is a type of online scam where criminals impersonate legitimate organizations to steal sensitive information. Such crimes often lead to trademark violations and identity theft. Venezuela comes first in the list of countries affected by phishing which is followed by Brazil with 14.95% of users (figure 2) who were targeted by phishing in the first quarter of 2020. Offenders in Brazil have developed advanced techniques to prevent users from realising that a certain site as illegitimate. The victim clicks on the false link which prompts them to divulge a variety of sensitive information. The number of successful phishing attacks in Brazil are increasing. Brute force cyberattacks are a form of phishing which aims to collect information through trial and error. The criminals list out the number of possible password combinations which are then entered one after the other till they hack into the account. Brazil has seen a spike in brute force cyberattacks especially since people shifted to mode of remote working.[19]

[19] Angelica Mari, "Brute-force cyberattacks on the rise in Brazil," *ZDNet* August 2020. https://www.zdnet.com/article/brute-force-cyberattacks-on-the-rise-in-brazil/

Countries most targeted by phishing attacks worldwide during the first quarter 2020[20]

Serial no.	Countries most targeted by phishing attacks worldwide during first quarter 2020	Percentage of users attacked
1.	Venezuela	20.53%
2.	Brazil	14.95%
3.	Australia	13.71%
4.	Portugal	12.98%
5.	Algeria	12.12%
6.	France	11.71%
7.	Honduras	11.62%
8.	Greece	11.58%
9.	Myanmar	11.54%
10.	Tunisia	11.53%

Fig – 2

Ransomware

Ransomware is a type of malware that locks out the system and does not allow the users toaccess files in the drive until they pay a certain amount. Ransomware can easily shut down large scale organizations, cities, local governments and healthcare organization.[21] Brazil was the worst hit, after India, when it came to ransomware attacks (figure 3). Just like in phishing, 73% of ransomware attacks carried out by cybercriminals turned out to be successful, hence, we shouldn't expect the offenders to stop anytime soon.[22]

[20] "Phishing: Distribution of Attacks by Country 2020" Statista. 2020. https://www.statista.com/statistics/266362/phishing-attacks-country/.

[21] "Cybersecurity Report" *Check Point Software Technologies Ltd.* 2020. https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

[22] "The State of Ransomware 2020" *Sophos*. 2020. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Percentage of organizations hit by ransomware attacks in 2020

Serial no.	First five countries worst hit	Percentage
1.	INDIA	82%
2.	BRAZIL	65%
3.	TURKEY	63%
4.	BELGIUM	60%
5.	SWEDEN	60%

Fig-3

On 3 November 2020, Brazil encountered a massive ransomware attack that crippled the operations of Superior Court of justice in Brazil for an entire week. This attack impacted the court's backup files and data. The virus was found in the court's network and, as a safety measure, the Internet or disconnected, prompting the cancellation of trial sessions. Without this decision, the attack could have done more damage.[23]

Attacks on SCADA

Supervisory control and data acquisition devices, according to the hacker group GhostShell were not created while keeping security in mind. They believe that it is not too difficult to cause enormous disruptions. Most critical infrastructure, such as nuclear plants, electrical transmission systems, water treatment plans, etc., are managed by SCADA systems. Disruption of any of these critical infrastructures can lead to multiple crises. SCADA devices are found online without much effort along with this, while some devices are protected most are not due to the usual ignorance and negligence. According GhostShell threats are extremely dangerous considering the levels of negligence. They said "like the Internet, SCADA was never created with security in mind. Its servers in

[23] Angelica Mari, "Brazilian Superior Electoral Court Hit by Major Cyberattack," *ZDNet*, November 6, 2020, https://www.zdnet.com/article/brazilian-superior-electoral-court-hit-by-major-cyberattack/.

Brazil and just about everywhere else I'd exposed to the most basic attacks. Connecting to a programmable logic controller takes one simple step: used the client interface to breach the targeted protocol."[24] While the standards and guidelines for industrial control systems were designed to prevent SCADA systems from being compromised the threat still persists.

Emerging threats

There is a need to invest in research regarding the emerging cybercrimes. Drugs and arms trafficking, online extortion, spread of cultural violence, cyber money launderingand tax evasion are relatively new cybercrimes compared to the categories mentioned by the ITU. However, the types and techniques of crimes will keep proliferating. Artificial intelligence has already been incorporated in the corporate sector and is also seeping into the domain of national security. Therefore, cyber security needs to stay updated with developments in AI. There is a need to develop security strategies which combats the possible misuses of new innovations. This cannot be done unless there are sufficient skilled experts who capable of analyzing the emerging cyber trends and suggesting efficient ways to prevent the potential threats that come along with it.[25]

CONCLUSION

Brazil was introduced to digitization, E-banking, E transactions and online practices very early. While this is one of the factors why Brazil is prone to cybercrimes, it is also why Brazil has found ways to deal with some of these threats. Brazil has conducted the Rio + 20 Summit in 2012, the Confederations Cup in 2013, the World Youth Day in 2013, the football World Cup in 2014, and The Olympic and Paralympic Summer Games in 2016 successfully by avoiding any major cyberattack. Therefore, Brazil's cyber-defence is effective to some extent. However, with emerging threats, Brazil needs to update its approach to cybercrimes.

[24] "Brazil's Critical Infrastructure Faces a Growing Risk of Cyberattacks," *Council on Foreign Relations*, 2018, https://www.cfr.org/blog/brazils-critical-infrastructure-faces-growing-risk-cyberattacks.
[25] Foluwa T Rewane, "Top 6 Cybercrime Trends for 2020," *Iron Defense Security*, January 31, 2020, https://www.irondefencesecurity.ca/post/top-6-cybercrime-trends-for-2020.

Brazil needs to focus on why it is gradually becoming a hotbed for cybercrimes and why its capability to deal with them has declined. Brazil will have to keep improving its cybersecurity to combat emerging threats such as breaches in hospital medical networks, ransomware attacks on the public sector, compromised election security, cloud jacking common vehicle, and AI-powered cyberattacks.[26] In February 2020, Brazil published its first national cybersecurity strategy. While it grants more power to law enforcement agencies, tt confuses content related cyber-regulation with cybersecurity. This may cause further challenges since content regulation may clash with the constitutional rights to freedom of speech. Brazil still faces the challenge of implementing these rules and guidelines. Brazil needs implementation more than new guidelines. The country also needs do come up with a multi-stakeholder governance model which requires different agencies to work together and combat cybercrime.

[26] "115 Cybersecurity Statistics and Trends You Need to Know in 2021," *Norton*, 2021, https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html