India's Need for Ethical Vulnerability Research

Khushi Deora

Final Year Undergraduate Student, Department of Journalism, Kalindi College, University of Delhi, Delhi, India

---***---

Abstract - *Security threats are not just about land and sea borders. The digital colonization that we all have conveniently adapted to, has made us vulnerable to digital encroachments in forms of data security threats. As the Bharat Net project is reaching its aim of broadband connectivity to the level of gram panchayats, banking and data frauds are prone to see an uptick. But India still seems to lack a concrete data protection law and users are thrown into an unregulated marketplace when it comes to informational privacy. Also, constructing regulatory policies for vulnerability researching and disclosure is vital for the digital transformation of both public and private entities.*

Key Words: Cyber-security, Data breach, Vulnerability Research, Ethical Hacking, Digital India

1.INTRODUCTION

Data breach is not a recent phenomenon though or just a product of digital revolution. Ever since individuals, companies and governments started maintaining records and storing confidential information in any form, intentional and accidental data breaches have been inevitable. The term 'data breach' encompasses everything, from viewing somebody's documents without permission to unauthorizedly hacking into a company's database. The purpose of cyber-attacks varies from accessing sensitive trade secrets, cyber espionage, stealing intellectual property to hijacking databases and any other cyber catastrophe that one can think of. The enormous compounding rate of data volume has paved way for the creation of a profession called independent security researchers or as they are commonly called, the ethical hackers.

1.1 Current Landscape

Sanjay Dhotre, Minister of State for Electronics and IT, said in an official statement to Rajya Sabha that a total number of 110, 54 and 59 websites of Central Ministries, Departments and State Governments were hacked during the year 2018, 2019 and 2020, respectively. According to the information tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 17,560, 24,768 and 26,121 Indian websites were hacked during the year 2018, 2019 and 2020, respectively [1].

The recent biggest data loots in the year 2021 include those of Dominos India, that leaked the financial credentials of 18crore orders; the Upstox data breach, risking the KYC data of around 25lakh customers; the Air India data leak, exposing the passport and credit card details of 45lakh customers and many more. The list of cyber-attacks can be inexhaustible. The personal, biometric and financial data of users is being stacked for sale on the cyber-crime market like a casual commodity [2]. Due to narrow definitions of personal data and weak redressal mechanisms, neither the 'Right to Privacy', nor the 'Information Technology Act, 2000, are able to strongarm the users.

In a report titled 'Threat Landscape for Pharmaceutical Companies', cyber security researcher, Cyfirma stated, "The healthcare industry, and particularly, pharmaceutical companies, has been thrust directly under global spotlight. While the world stumbles in its search for recovery, cybercriminals lurking in the dark web have seized the global event to profit from the climate of fear and uncertainty." Attackers ranging from state-backed spies to cyber criminals are constantly hunting for information. India's leading vaccine makers, Serum Institute of India and Bharat Biotech were also allegedly the targets of such attacks [3].

2. CASE STUDIES

The start-up ecosystem in India is accomplishing new milestones faster than ever. The online revolution invites new threats as most of these start-ups are related to technology, be it fintech, ed-tech or health-tech. This is bringing India to the attention of cyber criminals. Yet not enough is done to mitigate the risks of cyber-attacks. Business expansion through technological means comes with an added responsibility of ensuring a robust data security regime.

2.1 The Zomato Case

In May 2017, India's largest online restaurant guide, Zomato was brought on its knees by a security researcher and ethical hacker. The hacker had got the access of vital login credentials of the customers and threatened to sell them on the dark web cyber-crime market. Although, as conveyed by Zomato's blog posts, the hacker's primary motive was to press the company into acknowledging the vulnerabilities of its database and initiating a bug bounty program to fairly compensate white-hat hackers [4]. Since then, Zomato has paid more than $100,000 equivalent to Rs. 70 lakhs as vulnerability rewards. Before that, Zomato just used to award recognition certificates to independent security researchers.

2.2 Juspay Data Leak

Juspay is a Bangalore-based company, that processes payments from big brands like Amazon, Flipkart, MakeMyTrip, Uber, Airtel etc. It processes more than 4 crore payments worth Rs 1000 core daily across all platforms. The company acknowledged an unlawful data leak in August 2020, while a security, Rajshekhar Rajaharia claims that he noticed customer data being put up for sale on the dark web. After the initial cursory check, he notified the company through their official Twitter handle. In its blog, Juspay stated that 3.5crore user details were compromised and those too were partially masked and encrypted, whereas Rajaharia claimed that he found 10 crore credit card details on the dark cyberspace. The company stated that the exposed details could not be exploited to make transactions because of the masked numbers. Some researchers believe that the company downplayed the data breach as it could or might have affected its 10 crore customers [5].

2.3 Digital India and the Pandemic

The costs of data breaches are unimaginably higher than investing in bug bounty programs. It has been observed through these numerous cases of cyber-attacks that companies are more focused on front-end technology advancement and not giving equal importance to security functions. Choosing to disclose the vulnerabilities and draw a company’s attention towards them, instead of exploiting them, separates white hat hackers from black hat ones. Hacking as a service might have taken a front seat in the recent times, especially in the light of COVID-19 pandemic, but it has existed on the dark web for a very long time. The hiring processes and operations are as good as corporate employment contracts, with varying budgets and employable skills.

The Digital India campaign that was launched in 2015, picked up its true pace only in 2020, with pandemic forcing businesses to go digital and consumers getting used to the new digital normalization. Mr. Dipesh Kaura, General Manager, Kaspersky, South Asia explains, “As we look forward to building a digital nation, it becomes equally necessary for us to be prepared to fight against the perils of the world wide web. Cybercriminal groups have been more active than ever in 2020 and will continue to try and exploit our vulnerabilities for their financial gains. The best way to avoid being a target is to understand the evolving threat landscape, and develop a robust security system for our devices that will help us in keeping our data safe.” [6]

3. VOLUNTARY BUG DISCLOSURE BY THIRD PARTIES

Presence of vulnerabilities is technically inevitable, especially while carrying out the daunting tasks of creating software and handling big data. Bug Bounty programs work like a ‘prevention is better than cure model’ and ensure continuous mitigation of security flaws. Independent ethical hackers look for vulnerabilities in the security configurations of companies' websites and databases and report them back.

Bug bounty programs incentivize ethical hackers to check the cyber proofing of systems and give recommendations on fixing security flaws. Only when security researchers feel fairly compensated and rewarded, will they contribute in making the digital infrastructure stronger. The argument that open bug bounty programs will attract black hat hackers does not hold reason as brittle security systems can be targeted any time and any day and agencies will then find themselves in threatened position. Whereas having bug bounty programs will ensure that systems pass through various levels of security screening as independent researchers will explore various angles of exposure any system has, giving the agency an opportunity to plug the loophole.

The complexity or in most cases in India, the absence of reporting mechanism poses a big challenge to security researchers. Government entities that include the Indian Computer Emergency Response Team (CERT-IN), the National Informatics Centre Computer Emergency Response Team (NIC-CERT) and the National Critical Information Infrastructure Protection Centre (NCIIPC) are supposedly the points of contact, but there is no standardized framework when it comes to submitting the details [7]. The efficiency of telephone-based and email-based helplines is also not very impressive. Though governments get their cyber systems periodically checked, the relations between hackers and governments have always remained strained. In corporate entities, the procedural hassles might be comparatively less, yet Indian corporates are not proactive in security advancements. Lack of trust in independent security researches and unwillingness to invest in digital security, endanger India’s public and private technological infrastructure.

4. LEGITIMATE VULNERABILITY RESEARCH

4.1 Legal Notice to Air India

In July 2021, almost a month after the data leak was confirmed by Air India, a Delhi based journalist, Ritika Handoo sent a legal notice to the airline, seeking damages of Rs. 30 lakhs, on grounds of leaking sensitive personal information, citing the Company's Customer Care Data Privacy Policy. Rule 3 of the Information Technology Rules, 2011 states that information relating to passwords, credit/ debit card information, biometric information, physical, physiological and mental health condition or any detail relating to the above clauses as provided to body corporate for providing service, stored or processed under lawful contract or otherwise is to be treated as 'sensitive personal information.' In the current legal regime, any proof of wrongful loss or wrongful gain caused by the negligence might offer limited protection to the complainant, but the mechanism for compensation still stands vague. The Consumer Protection Act that came into effect in July 2020, also does not deal with protection of data [8].

4.2 Legal Scenario

Section 43 of the Information Technology Act, 2000, imposes penalties on several cyber practices in cases where a person without the permission of owner or any other person-in-charge damages the Computer System, or Computer Network. The lines between authorized and unauthorized access were yet not clearly defined. The vague regulatory provisions of this act are often used to harass and legally threaten the researchers. Revised regulatory policies need to clearly distinguish between vulnerability search and malicious cyber-attack [9].

The National Cyber Security Policy of 2013 tried identifying the threats and challenges in the cyber space but is considered just an aspirational document that lacks any legal binding. But the fact that our policy makers were able to prepare such a draft encompassing issues of risk assessment and all forms of potential cyber threats, along with their economic implications, is a testimony to the fact that it was a good starting point in securing the cyber space [10]. Furthermore, a common loophole in any existing or proposed cyber law is that no law is applicable to governmental authorities that fail to take into consideration the privacy needs of the citizens if any matter arises.

5. DISCUSSION

Bug bounty programs are also subject to dual views. On one hand, the cyber community believes that it acts as a defensive pessimistic approach that ensures multiple layers of vulnerability checks and each check reduces the probability of any organization falling prey to the devious attacks of cyber criminals. They also argue that fair compensations can also make some black hat hackers to take the ethical hacking route. They are also of the opinion that vulnerability reporting should not have any criminal liability attached to it, unless it is exploited beyond the point of research or revealed prematurely.

On the other hand, organizations also seem to be justified in their risk averse approach as they believe that inviting independent and anonymous researchers to scan through their software systems might damage their systems or lead to major data theft. In their perspective, any such program will invite several black-hats as well as there is no framework that rates the ethicality of any security researcher. Even in case of ethical vulnerability reporting, researchers often submit duplicate, invalid or low value reports and companies are left with the daunting task of inspecting and identifying valid reports, that are usually very less in number as compared to the junk received. The widely increasing use of cryptocurrency adds to the risk as cybercriminals ask for extortion money in form of cryptocurrency due to the anonymity of transaction.

As per the reports by BugCrowd and Facebook, India leads the charts for most bug hunters worldwide and the money rewarded to them. But as a result of absence of legal clarity and lack of opportunities, Indian cybersecurity talents are left with no choice but to serve foreign clients. Like many other employment sectors, Indian security researchers experience a large pay benefit due to the dollar-rupee gap, as foreign clients pay them in dollars. Even after negotiating it becomes a win-win situation for both the parties.

Cyber security is emerging as a whole new sector and demands for better public-private partnership. In 2018, the Government Technology Agency of Singapore and the Cyber Security Agency of Singapore partnered with HackerOne, a platform that maintains bug-bounty programs for organizations and companies, to secure critical infrastructure and develop symbiotic trust between the government and the community of security researchers [11].

6. CONCLUSION

White-hat and black-hat hackers use the same hacking tools, difference is just in the intent. The objective of governments and institutions should be to make ethical hacking a regulated and licensed profession. This will ensure collectively agreed upon codes of conduct and practitioners would then be willing to accept liability as well. Making it a credible pursuit will increase participation in the profession and for the clientele it will eliminate the fear of risk factor brought by the security testers. In today's digitally hostile scenario, India must provocatively move towards comprehensive security.

REFERENCES

[1] Economic Times. (2021, March 18). "Over 26,100 Indian websites hacked in 2020 as per CERT-In data: Sanjay Dhotre." Retrieved July 2021, from https://economictimes.indiatimes.com/news/defence/over-26100-indian-websites-hacked-in-2020-as-per-cert-in-data-sanjay-dhotre/articleshow/81569782.cms?from=mdr

[2] Ravi, R. (2021, May). "Five Biggest Data Breaches That Hit India in 2021." Retrieved from Jumpstart https://www.jumpstartmag.com/five-biggest-data-breaches-that-hit-india-in-2021/

[3] Ahaskar, A. (2021, March). "Indian pharma companies and hospitals targeted by Chinese, Russian and Korean hackers groups." Retrieved from Mint: https://www.livemint.com/technology/tech-news/indian-pharma-companies-and-hospitals-targeted-by-chinese-russian-and-korean-hackers-groups-11614618146968.html

[4] Dey, A. (2017, May). “Ethical hacking: The Zomato case highlights how the government should use bug bounty programmes.” Retrieved July 2021, from Scroll: https://scroll.in/article/838633/the-zomato-case-highlights-how-the-government-should-use-the-skills-of-ethical-hackers

[5] Variyar, M. (2021, January). “Juspay data breach could get worse, cyber experts call company 'highly irresponsible'.” Retrieved from CNBC TV 18: https://www.cnbctv18.com/technology/juspay-data-breach-could-get-worse-cyber-experts-call-company-highly-irresponsible-7906901.htm

[6] Kaspersky. (2021, March). “The growing cyber threats for Digital India: Kaspersky report reveals that 35% of Indian Online users were attacked by web-borne threats in 2020”. Retrieved from https://www.kaspersky.co.in/about/press-releases/2021_the-growing-cyber-threats-for-digital-india-kaspersky-report-reveals-that-35-of-indian-online-users-were-attacked-by-web-borne-threats-in-2020

[7] Saini, K., Prakash, P., & Hickok, E. (2019, January). “Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India.” Available at SSRN 3459416.

[8] Business Standard. (2021, July). “Passenger sues Air India for personal data breach: What happens now.” Retrieved from: https://www.business-standard.com/article/companies/passenger-sues-air-india-for-personal-data-breach-what-happens-now-121070601451_1.html

[9] Indian Freedom Foundation. (2020, January). “Security researchers need legislative protection for responsible disclosure.” Retrieved from https://internetfreedom.in/security-researchers-need-legislative-protection-from-vexatious-lawsuits/

[10] Diamond, J. (2013, July). “India's National Cyber Security Policy in Review. Retrieved from The Centre for Internet and Society.” https://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review

[11] Business Wire. (2018, December). “Singapore Government to Launch Second Bug Bounty Initiative with HackerOne to Boost Cyber Defences.” Retrieved from: https://www.businesswire.com/news/home/20181220006005/en/Singapore-Government-Launch-Bug-Bounty-Initia