International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Survey Report on the Cyber Crime Growing Vigorously in Jamtara, Jharkhand (India)

Sweta Kumari Barnwal
Assistant Professor, Dept of Electronics and Communication Engg., Arka Jain University, Jamshedpur, India

***Abstract*: This Modern Technology is almost inspirable from our daily life. Since its beginning in the 1990s, the internet has a vast electronic network. This network consists of millions of devices which is hyper-connected to each other. With the rapid technological developments, our life is becoming more digitalized. Be it business, education, shopping or banking transactions everything is on the cyber space. There are some threats posed by this incredible rise in digitization which is creating a new set of global concern called as cyber crime. It is easy to fall prey to such unethical way of hacking and penetrating into personal life which is feasible at a click of a button. Cyber crimes thereby take place in many forms like illegal access and theft of data, intrusion into devices and fraud which is a big concern amongst all the users. In a major revelation, Jamtara in Jharkhand has been identified as a new cyber hub for crime. More than fifty per cent of cyber crimes in India are traced back to this sleepy town of Jharkhand. The revelation was made by Union Home Secretary Rajiv Gauba who himself is a 1982 batch IAS officer from Jharkhand. When we hear about "Cyber crime" Our focus is gone on "cyber Security". This paper, gives detailed information regarding cybercrime and how it's affecting the life of we all. With increasing use of information technology (IT) enabled services such as e-governance, online business and electronic transactions protection of personal and sensitive data have assumed paramount importance. The economic growth of any nation and its internal security depends on how well is its cyberspace secured and protected.**

***Keywords*: Cyber Crime, Information Security, Cyber threats, Hacking, Phishing, Cyber Safety, Digital Data, Technology.**

1. Introduction

Social Media can be defined an individual or agency to communicate interactively and exchange of user generated content and it is explained by a number of tools, which includes blogs, wikis, discussion forums, micro-blogs, twitter and social networking sites. So many advantages of social media but there are threat to internal security in different forms like Cyber crime, Cyber Terrorism, Fraud, spreading violence, etc. National Security's Importance (NSI) for any nation maintained peace and harmony. Internal security challenges and Social Media act as the platform for nations face numerous. Social media is not security threat in itself but the users of these services can pose the threats by their anti-social Endeavour's.

"Jamtara is a sleepy town in the tribal region of Santhal Pargana. It still continues to be an obscure town. But has gained notoriety as cybercrime hub," Gauba said while addressing a conference on internal security. More than half of India's crimes committed by fraudsters posing as bank managers were traced back to this town. Expressing concern over the new age crime, the government is still not ready to tackle the increasing rate of cyber crimes.

2. Discussions

In these parts – Karmatand and elsewhere in the villages of Jamtara, Madhupur, and Dumka of eastern Jharkhand – the frequently-used "cyber" in Hindi and Bengali refers to cybercrime and those dabbling in cybercrime, both petty and serious. There are thousands of "cyber" in this area, about 250 km northeast of Kolkata.

When we met there a localized, he told "they guys do their cybercrime there, pointing to this area".

Fig. 1. Cyber criminals do their crimes from barren fields & nearby forests

Among the millions-strong generation of boys and young men in their teens and early 20s in Jharkhand, a state that is rich in mineral wealth (it accounts for some 40% of the country's natural resources) but counts 39 of its 100 people living in poverty. Amidst the malnutrition and poverty, smart phones make the world a less unequal place for the Jamtara's youth involved in cybercrime. With more than half of India's cyber crimes, mostly committed by fraudsters posing as bank managers and traced back to Jharkhand, this belt is clearly digital India's underbelly. This estimate comes from police officials in Jharkhand and Karnataka. To be sure, Jharkhand ranks 13th in terms of cyber crime rates in 2016, the latest year for which data is available the National Crime Records Bureau (NCRB), and 14th in terms of incidents and the percentage share of overall reported cyber crimes for the same year. But, that's primarily because most of the victims targeted by the cyber fraudsters from Jharkhand are elsewhere in the country and the crimes get reported in other states. A cyber crime police station set up in Jamtara early last year is at the forefront of the battle with cyber criminals and Jharkhand's efforts to shed its image of being home to India's cybercrime capital. Early results look encouraging with the local police claiming crimes are down by half but can they curb the menace completely? FactorDaily interviewed nearly two dozen local residents in Jamtara and surrounding areas, local police officials, cyber crime police specialists in Bengaluru, NCRB officials and others to get an inside view of the crusade against cyber crime in Jharkhand. An insidious web of mobile phone SIM cards, digital wallets, and bank accounts opened on the back of fake KYC documents power hundreds of small gangs in the state — and point to trends in the future of crime in the country. "Although the total number of cyber crimes are less than 0.1% of the total IPC and SLL crimes in a year (in India), in 30-35% of all crimes, criminals are using mobile phones for communication," says Ish Kumar, director of the NCRB. "There is an overwhelming need to train all investigating officers in cyber and digital forensics, and open cyber police stations in all district headquarters." IPC is short for Indian Penal Code and SLL for special and local laws enacted by a state. Over the past decade, especially since the mobile boom, Jamtara's unemployed youth found working the phones was an easy way to make a quick buck. "If you ask around the elders, you will learn that these areas have always been notorious for thugs. Now, the next generation has evolved," says Sumit Kumar, deputy superintendent of police (DSP) who has been with the Jamtara cybercrime police station since September last year. The station was set up in January 2017 after the state government realised it needed a dedicated force to deal with cybercrime in these parts. Kumar adds that earlier the thievery included drugging train passengers and looting them. The local gangs would even steal coal and other valuable minerals – a story told in the 2012 film Gangs of Wasseypur – with Dhanbad, India's coal capital, just about 50 km away. Dhanbad falls on the Howrah-Delhi rail route.

3. How they work

The mobile phone worked as cyber a cyber café for them. A few years ago gangs such as his used to operate from one of the dozens of cyber cafes in and around Jamtara. The cops have made that difficult with cyber cafe owners being co-opted into police informer networks. Every morning they gather in the barren fields close to the dry jungles bordering the village. One of them brings updates from an underground network of phone number database sellers, new phone connection resellers and general buzz about who could be on the radar of Jamtara's cyber police.

The localized of there, they don't allow to take the pictures. They normally chase away people with cameras trying to enter the village. They even pelt stones on police teams who come into our villages sniffing around," the friend says boastfully, picking up a small stone as he talks. After shortlist the phone numbers of people from different parts of India to call posing as bank managers, the action begins. The most common tactic is impersonation. They make calls posing as bank managers, getting their victims to share bank account and card details, and then use the information to move the money to their accounts. Typically, targets are told that their ATM card has been blocked and that if it's not renewed soon, it will remain inactive. India has over 1.6 billion savings and current banking accounts and some 29 million credit cards and 820 million debit cards approx. - and the chances of someone believing the call to be a genuine one are high. They provide so many offers, such as heavy loan with low interest, credit card with higher limit, or they scared the victims that your account or ATM would be closed. Then they asked for the 16-digit card number and its details. While on the call, self or one of them feed that information in an e-wallet, including the CVV number, and expiry date of the card. Then, they ask the victim to share an OTP message they would be receiving from the bank, which is essential for the criminals to transfer money from the victim's account to an e-wallet such as Paytm or Oxigen. This e-wallet is already linked with a bank account opened only for this purpose. Mostly a fake bank account opened with fraud KYC documents.

Image credit: indiarailinfo.com

Fig. 2. More than half of India's cyber crimes mostly committed by fraudsters posing as bank managers have been tracked back to this place & its neighbouring places make for the hotspot.

Very Soon, the money is withdrawn and distributed among everyone involved in the crime. Not all involved in the crime have e-wallets; the ones that do become the centrepiece of this entire chain. They told sometimes it's difficult to transact through e-wallets, especially the more established ones such as Paytm because accounts require KYC documentation. But Jharkhand's digital-savvy criminals won't give up so easy. They have discovered a bunch of e-wallets including Tapzo, TMW, Kitecase and so on. They always try to find new e-wallet, for this they take account on lease from the respective users & for that they pay some amount to that user. Police team have been tightening the noose around the networks of SIM card sellers, e-wallet companies and bank accounts involved in this chain and have aggressively moved on the local cybercrime networks. "We act on the leads and information mostly suo moto. Based on local inputs, we conduct regular raids. This year we have done so far 60 arrests.

Fig. 3. Jamtara & nearby places have very strong telecom network

4. Inside Jamtara: A battle against cybercrime

The quiet railway station in the heart of Karmatar draws its name from one of the country's greatest social reformers, but today hardly anyone seems to be aware of the connection of this place to Ishwar Chandra Vidyasagar. Only a few hundred metres from the Vidyasagar railway station is the place where he lived for 18 years, taught girls in a thatched school, and distributed medicines from a home clinic. Some of the articles used by him are still lying here but the place, which should have been a tourist destination, does not get any visitors these days. Instead, this nondescript little town in Jharkhand's Jamtara district is often frequented by police from different States: it has emerged as one of the biggest hubs of cybercrime in the country. Records at the Karmatar police station reveal that between April 2015 and March 2017, police teams from 12 different States have visited the station 23 times and arrested around 38 accused. Over 80 cases have been registered suo motu by the Jamtara district police between July 2014 and July 2017 against 330 residents of the area. At Karmatar police station alone, the number of arrests in 2017 has crossed 100. Jamtara's cyber criminals and their flashy lifestyles are topics that start discussions of fervour. Until a couple of years ago, Jamtara's cyber crime masterminds operated without much hassle because police teams from Ranchi and Dhanbad took time to reach remote areas of their operations – and, if they did, the operatives were alerted. Secondly, Jamtara's residents, too, used to turn a blind eye. Local merchants like wine shop owners and meat sellers did brisk business as Jamtara's cyber criminals spent freely on the good life.

From outside, the yellow building looks more like a marriage hall. Jamtara's cybercrime police station set up in September last year makes a loud statement with its brightly coloured walls amid the grey blocks of the town's local court premises. The compound is teeming with lawyers, clients, and even some handcuffed under trials.

CYBER CRIME POLICE STATION
साइबर अपराध पुलिस स्टेशन
E-mail:-sp-jamtara@jhpolice.gov.in
Tele. No.-06433-222244

Fig. 4. Jamtara's cybercrime police station was set up on 1917

In January 2018, for instance, DSP Kumar, together with sub-inspectors Rohit Kumar and Prabhat Kumar and their team nabbed around half a dozen cyber criminals after raiding them in the villages of Karmatand and Narayanapura. One of them, Yugal Mandal, was a top mastermind in the area. He had built a house that was estimated to cost nearly Rs 2 crore close to Jamtara's Edward School, among the most sought-after English medium schools in the locality. In 2017, Jamtara's cyber crime cops arrested 185 criminals and registered 89 cases against them. During raids, they also collected 700 mobile phones, 900 SIM cards, 160 ATM cards, 10 four-wheelers, and 90 two-wheelers. And, Rs 17 lakh in cash was seized. In 2018 police team have already arrested 51 cyber criminals, registered 23 cases, confiscated 105 mobile phones, 135 SIM cards, 13 ATM cards, a car and 14 two-wheelers. The cash seized so far this year is around Rs 1.25 lakh. In Madhupur that is another cyber crime hub some 60 kilometres away from Jamtara. While Karmatand and Jamtara have been hogging most of the limelight when it comes to cyber crime in Jharkhand, Madhupur has had its own kingpins. Rs. 15 lakh in cash from a house had recovered along with a pricey television, music system and fridge. Cybercriminals have been moved from cyber cafes & now operated on smart phones.

5. Cases and Seizures

The area of Jamtara & nearby places is still very backward. There are hardly any signs of development on the 17-km road leading from district headquarters Jamtara to Karmatar. The road itself, which runs parallel to the railway line, is pockmarked with large potholes. The only thing that catches the eye in this semi-urban setting with a population of about 2,00,000 are the dozen mobile phone towers erected in the fields on either side of the road. And it is these towers that hold the key to Jamtara's infamy. 70 LED television monitors, three washing machines, 40 ATM cards, about 80 bank passbooks, 200 mobile phones and 9.28 lakh in cash and two soft black sofas — one of them right next to the lock-up cell — gathering dust, the newly constructed Karmatar police station appears unlike others. Within the station compound are parked brand-new vehicles — all SUVs — and over two dozen motorbikes, all seized vehicles. In one of the dimly lit rooms inside, an officer is going through a handwritten note, oblivious to an informer's repeated attempts to draw his attention to a tip-off about illegal liquor being sold somewhere. It's a petition by a man arrested in a cybercrime case alleging human rights violations. These all details had been given by the in-charge of police station.

About 12 km from Karmatar police station is the Narayanpur police station, another area where multiple cases of cyber fraud have been recorded in the recent past. Boxes of liquor seized in a raid the previous night are piled up outside the entrance of the main police station building. The registers of the police station present a maze of unknown numbers, SIM cards referring to frauds done using e-wallets. Most of the complaints of cyber fraud, like the ones at Karmatar, have been registered by the police station in charge. The charges are mostly the same: Section 419, 420 of the IPC (cheating by impersonation and cheating), 468 and 471 (forgery for cheating and using forged document as genuine), 120B (criminal conspiracy) and Section 66B, 66C and 66D of the Information Technology Act.

Some police officers call the practice "phising" (phishing) it is actually "vishing", gaining access to private financial information of a person by claiming to be calling on behalf of a bank or financial institution. She says the tricks which the local youth, mostly school and college dropouts, employ to dupe people are not very complicated. "They call up people posing as bank officials on any pretext, say, linking the Aadhaar number (UID) to the bank account, and ask for card details. Sometimes, they even warn not to give the ATM PIN and say 'we are sending you an OTP from the bank and you have to confirm the OTP number'. Unfortunately, even educated people get convinced and get duped."

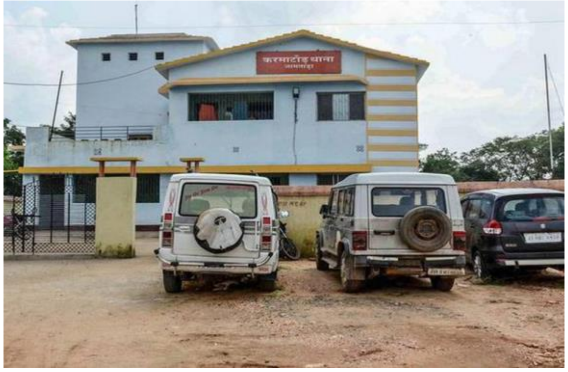

Fig. 5. The police station in front of which stand seized SUVs.

6. The curse of "Cyber"

Make no mistake; the heat is on if you are a "cyber" in Jharkhand but Jamtara's descent into cybercrime is almost as if it was foretold with the area bereft of opportunities to earn a living. "Tand means infertile land where you cannot grow anything," DSP Kumar tells me of the word that the names of most of the remote tribal villages near Jamtara end in. Not surprisingly, villages such as Jhariatand, Karmatand, and Taratand, for instance, are cyber crime hubs in the state. It is worse for those who come out of the crime. Who was part of a cyber crime gang until February last year, tells these villages and those like Narayanapura offer no opportunities. "And with a background in cyber crime, they become even more untouchable when they return to leading a normal life. The cops pick them almost every day for questioning and potential leads on their next raids." Unemployment is very high on these areas; so many youths are sited there idle. This village is the battleground for India's social reforms led by Vidya Sagar, it should be known primarily for that.

Many of Jamtara's "vishing" experts have never left town, but their reach spans the nation. In May 2018, Rashmi (name changed), who had just delivered a baby, applied for a bank account at the Central Bank of India in Darjeeling. A few days later, an 'agent' from the bank called asking for more details. The agent sounded genuinely helpful, and sympathetic, and told Rashmi that she could avoid coming all the way to the branch if she could give the name and ATM card details of a guarantor. Without giving it much thought, She called her mother, who works as a domestic help in Delhi, and passed on the latter's State Bank of India ATM number and PIN to the 'agent'. Within hours, her mother was on the line again, tearfully telling her that nearly 30,000, her savings of years, had been withdrawn from her account.

A young man in Jamtara, motorcycle-borne and wearing track pants and floaters, offers additional ground inputs. It is not that simple and cannot be done alone. They require a group. Typically the crime involves two people. One who makes a call to an unsuspecting customer seeking details about his bank account, masquerading as a bank officer. The second person sits with a smart phone, all set to click on 'proceed to make payment' for items on an e-commerce website. That person completes the transaction with the customer's bank details within moments after his partner secures them. The SIM card is then disconnected and destroyed. In most of the cases bank accounts or e-wallets of a third party is used to make these "vishing" transactions and the police have to follow a long trail to get to the main perpetrator.

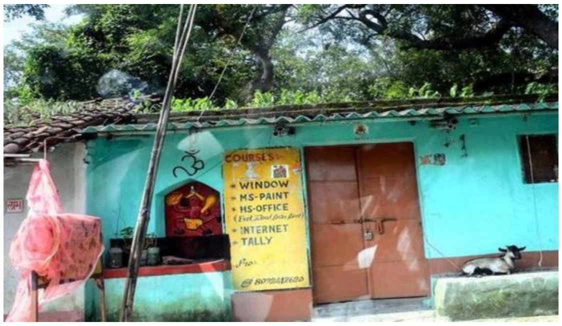

Fig. 6. A cyber café in Karmatand

"A cottage industry has developed in Jamtara," told a senior officer with Delhi Police's E-fraud Investigative Cell, detailing the modus operandi. He said scores of jobless young persons are involved in acquiring vast numbers of SIM cards on fake identities, which they used to fool unsuspecting ATM card owners. Almost all e-wallets such as Paytm, Free charge are being used. One deduction from an ATM card travels to one e-wallet and immediately into five or six other e-wallets, and then finally into a bank account, from where it is instantly withdrawn via ATMs.

7. Conclusion

According to the National Crime Records Bureau (NCRB), a total of 9,622 cybercrime cases were registered in India in 2014 while, 11,592 and 12,317 cases of cybercrime were registered in 2015 and 2016 respectively. Cyber attacks have become more organised with significant funding, passion, they are sophisticated, they often gain access and they wait for the right time, for the moment of their choice for their attacks. By increasing employment and awareness in these areas such crime can be controlled.

References

[1] www.indianrailinfo.com