Digital Shoplifting: Four Hackers Arrested in South Delhi

Hackers Arrested for stealing digital vouchers

M/s Voucha Gram India Pvt.Ltd, owner of Ecommerce Portal **www.gyftr.com**, made a Complaint with Hauz Khas Police Station against some hackers from different cities accusing them for IT Act / Theft / Cheating / Misappropriation / Criminal Conspiracy / Criminal Breach of Trust / Cyber Crime of Hacking / Spooning / Tampering with Computer source documents and the Web Site and extending the threats of dire consequences to employees, as a result four hackers were arrested by South Delhi Police for Digital Shoplifting.

The Company is engaged in the business of buying & Selling of Digital Gift Codes / Digital Gift Cards / Digital Gift Vouchers for the last 4.5 years and has been dealing with esteemed customers. The Website www.gyftr.com got hacked on 19 December 2016 at 06:35 PM wherein the above said accused persons gained unlawful access to the website of the company as define under IT Act 2000, claimed discount vouchers but the same could be discovered by the Company officials only after 24 hours.

The hacking worked in this fashion - firstly the hackers started the process of purchasing the gift voucher, say Rs 10,000. Then they proceeded to make the lesser payment, say of Re 1 at the Payment Gateway www.Payu.in and when the payment confirmation was sent back from Payu.in to Gyftr.com through the browser, they change the value to Rs 10,000. This method of hacking the payment parameter and sending the actual amount of voucher selected, instead of original value of Rs 1 paid at payment gateway resulted in the loss of approx 90 lakhs to the company. The activity continued for 2 days and could be detected only on 20 December 2016 at 07:30 PM and the vouchers were blocked as far as possible. On the same day, one of the accused called Gyftr.com help desk and enquired abut the blocked vouchers and was ready to reveal the names of other accused, if he was given financial reward, which helped police get further details.

The vouchers were utilized with various merchants like MakeMyTrip.com for making Hotel Bookings and through Telecom Operators, where many mobile recharges were done at discount prices. Also the address details were revealed where many other products like cloths purchased online were delivered. And more interestingly one of the accused was updating his Facebook timeline during the time the crime was committed by posting offers as to 50% off on Hotel Bookings, Free Aircel Recharge for friends, Checkin at various Hotels and so on. And also issued a statement after he came out of eight days of Police Custody.

The hackers were booked under Section 65 and Section 66 of Information Technology Act and Section 420 of Indian Penal Code 1860. They were finally arrested in January 2017 (now out on Bail) from different places - Jind, Dehradun, Kota and Bhiwani. They seemed to have got in touch online through some Hacking Sessions, wherein some one demonstrated through Teamviewer how the website Gyftr.com had security loopholes. Later, few of them ended placing huge number of orders by taking advantage of security loopholes for over 2 days on 19th and 20th December 2016.

Further, a press release] by Delhi Police talks about further details. Extract from the same are as follows:

Preliminary interrogation:

The arrested accused persons belonging to middle class families and dreamt of living a lavish life. Over a course of their student lives, they developed interest in hacking and the leader of the gang, Sunny Nehra, quickly excelled in the field. They developed online association with various hackers operating from India as well as foreign destinations and began experimenting with hacking for gaining small amounts of money from weakly encoded/encrypted e-commerce website. With more and more determined application of the latest hacking tools and vulnerability data being made available by anonymous hackers on the internet, they soon graduated to big time cyber crime league and started exploiting the dark and the deep web which gave them access to virtual currency like bitcoins.

The digital moneys siphoned off by them was used for buying sophisticated proxy servers, virtual private networks, high end laptops and soon, they formed a formidable gang of tech savvy hackers. Most of the e-vouchers digitally shoplifted by the accused were spent in Five Star Hotel accommodations, air tickets and entertaining girl friends. From the data analysis, it has come on record that they also used to take expensive cars on rent for travelling with their girlfriends to parties and hotels.

Modus operandi:

The lead hacker, Sunny Nehra, has developed a vast network of Indian as well as foreign hackers who share their knowledge online. Most of his friends are online hackers, API hackers, coders, developers, spammers, etc. The exact term to explain his expertise is ?Data Tampering'. The various types of cyber crimes committed using this expertise are ?adding cash backs' i.e. enhancing the value of cash back offers, using the same gift card again and again without detection, placing online orders without making any actual payment or by making small payments only, etc. One of his hacker friends informed him that PayU, a leading payment gateway, was suffering from vulnerability and could be tested for data tampering. The accused was intrigued as to how such a reputed website is suffering from such vulnerability? He started testing it and soon discovered that it was allowing ?change in parameters on the processing page' i.e. data tampering. Explained simply, the process resembles this:

1. On an e-commerce website, chose a product,say priced at Rs. 5,000/- to buy,
2. Enter the product in your shopping cart so that the cart value becomes Rs. 5,000/-,
3. Reach the page which says ?select payment method',
4. Now, using data interceptors (functionalities of testing software's like ?burp suite' etc.), this webpage is ?jammed' and the parameters are edited,
5. The ability to edit the parameters is learnt by learning the ?source codes' of the concerned websites' processing page. It may be recalled that whenever customers are making online purchases, after entering debit/credit card details and clicking on the ?make payment' icon, the customer is advised that ?your payment is being processed; please do not refresh or press the back button'. The hackers, when this stage is reached,press cancel or back page icon and save the source codes which, decoded, read like xxxxx = failure, yyyyy = successful, zzzzzz = error, etc. Once proficiency in decoding these source codes is attained, the parameters are edited on a?jammed' webpage,
6. The parameter of Rs. 5,000/- as the cart value is edited and made Rs. 1/- from the ?debit value',
7. The interceptor is ?put off' and the order is placed by transferring money from an online e-wallet which has been opened by the hacker using fictitious or a proxy identity. In this manner, the hacker earns Rs. 4,999/- (either in digital money to be used elsewhere or by purchasing actual goods) against making a notional payment of Rs. 1/- only.