Part IV: Internet Governance issues – Cybercrime in India

US charges 11 in 'biggest ever' fraud case

6 August 2008

Jenny Booth
Times Online

United States prosecutors have charged 11 people with stealing tens of millions of personal credit and debit card numbers of British and American shoppers.

The alleged international conspiracy, said to have been run by a double agent of the US Secret Service, is suspected to be the largest hacking and identity theft ever prosecuted in the US. The total sum of money stolen is not known, but probably runs into hundreds of millions of dollars.

The hackers allegedly used a sophisticated technique known as "war driving" - driving around suburbs of Miami and San Diego scanning for security holes in the wireless networks at shops and banks.

They hacked into these networks and installed "sniffer programmes", which captured the card numbers, passwords and personal details. They were able to conceal the information on computer servers in the US and Eastern Europe before exploiting it themselves or selling it on to other criminals.

In an added twist, it emerged that

One's home is meant to be safest place for them. When someone is burgled or attacked within their homes, it violates every sense of their security. If we believe that, how do we deal with someone violating our private space in the online world?

If someone burgles your home, the first reaction in an urban city like Delhi, would be to call the police emergency helpline '100'. Do we have a similar reaction to someone hacking our email address? To best explore this route, we tried our hands at some investigative research to determine where the path leads us to.

First call was made to the emergency helpline. There were a few minutes of passing the buck at the call centre before anyone could determine who would be responsible for such a call. We were given the contact number of the 'Cyber Cell' which falls under the Economic Offences Wing of the Crime Branch of the Delhi Police. When we called at the 'Cyber Cell', we were told that the complaint needs to be lodged at the local police station. There is a large amount of ignorance within the police hierarchy about what cybercrime is and how to deal with cybercrime.

Tangibles and Intangibles

The police essentially respond to tangibles; physical damage or monetary loss. From the experience of the victims of cybercrime interviewed, it was felt that the loss of ideas, concepts, or information is still largely unrecognised as criminal in most cases.

One such case was of particular interest to us. It involved an eminent Professor from a leading university based in Delhi. Her experiences are a stark reminder of how helpless even an erudite, independent professional can feel in the face of cybercrime. On June 5th 2007, she received a call from a close friend and colleague who was rather concerned by her email which said that she was stranded in Lagos, Nigeria, without any recourse to funds. She had pleaded her friends and relatives to send her some money to help her get back to India. Rather surprised, she tried to log into her Yahoo email account and was unable to do so. Her email had been hacked and password changed so that she had no access to her own account anymore. Emails to Yahoo India or U.S. did not get her any replies.

She went to the local police station to lodge an FIR but they only agreed to take a complaint. The key issue

to the police was the lack of direct economic loss. The urgency to retrieve important documents or emails was not seen as a direct loss since it could not be monetised. After a couple of days of inaction, she requested a couple of her students to look into the matter. The students traced the IP address to Lagos, Nigeria and also discovered which service provider owned the IP address. When this information was presented to the police, instead of taking action which would help prosecute the miscreants, they tried to frame the students who had helped crack the case.

Officials at the Economic Offences Wing confirmed that such cases are on the rise nowadays. This is an extension of the Nigerian 419 scam. The 419 scam originated in the early 1980s as the oil-based Nigerian economy declined. Several unemployed university students first used this scam as a means of manipulating business visitors interested in shady deals in the Nigerian oil sector before targeting businessmen in the west, and later the wider population. Scammers in the early-to-mid 1990's targeted companies, sending scam messages via letter, fax, or Telex. The spread of email and easy access to email-harvesting software made the cost of sending scam letters through the Internet inexpensive. In the 2000's, the 419 scam spurred imitations from other locations in Africa, Asia and Eastern Europe.

These personalised crimes are one face of the large scale escalation in cybercrime. Spam, credit card frauds and identity thefts are on an exponential rise. The issue with cybercrime as was discovered in the above case is the difficulty in prosecution. Firstly, there is an ambiguity of who is responsible for the crimes committed. Is it the service provider, or the hosting company or the actual people committing the crime? This ambiguity is further exacerbated by the lack of comprehensive inter-country partnerships in the execution of laws. One of the largest, international cybercrime stories is in the news nowadays. An excerpt from the story is shown here. "This case highlights our increasing vulnerability to the theft of personal information," said Michael Mukasey, the US Attorney General. "Criminals can now operate from almost anywhere on the globe to steal personal information." Cases such as these are becoming increasingly common in the developed world with a large number of e-Commerce transactions as well as an exponential rise in the use of credit and debit cards for over-the-counter transactions.

The revolution in the information technologies in the field of commerce has changed society and crime fundamentally and will probably continue to do so in the foreseeable future. While many tasks have become easier, many crimes have also become easier to commit and harder to trace to the perpetrator. Vast amounts of data comprising of voice, text, music and, static and moving pictures are exchanged over the Internet which unlike traditional telephony does not require a direct connection; it suffices that data is entered into a network with a destination address or is just made available for anyone who wants to access it. This freedom of the data from direct connectivity or in fact traceability makes it susceptible to attacks from anyone, anywhere.

Write to us and contribute to the upcoming articles

- **September** – Privacy & Data Protection
- **October** – IPv4 vs IPv6

Write to us at *response@i4donline.net*

Denial of Service Attacks

Another dangerous and common attack against a larger entity like an institution or government is called Denial of Service Attacks (DoS). One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. This form of attack can be seen as cyber terrorism since it can incapacitate the economy of a country.