

FEEDBACK

Write to the editor

@newagebd.com

Main Page «

Front Page «

Metro «

Business «

International «

Sports «

National «

Editorial «

Op-Ed «

Home «

Timeout «

Letters «

Others

Archive «

Launch Supplement «

# NEWAGE Xtra

March 14-20, 2008

## A click away from crime

With an inactive cyber law and a severe lack of the expertise necessary to detect cyber crime, Bangladesh is a safe haven for anyone committing a computer crime, **Saad Hammadi** discovers

At 7:30am, an overseas call abruptly awoke Sumon Ahmed Sabir, managing director of one of Bangladesh's largest internet service providers, Bdcom Online. At the other end, calling from the United States was an official from the online payment service company Paypal. 'One of your subscribers' computers is hosting a

phishing site and has to be blocked immediately,' a disgruntled Sabir was told early that morning last June. In other words, that Bdcom user's computer has been fraudulently acquiring personal identification numbers through a sham website and this sensitive information was being used to hack credit cards. It was the first time a cyber crime needed Sabir's intervention.

With an inactive cyber law and a severe lack of the expertise necessary to detect cyber crime, Bangladesh is a safe haven for anyone committing a computer crime. From viruses (which infect computers to malfunction), trojans (deceptive software or malware that appears to perform an action but instead performs another) and spam to online threats, piracy, hacking (accounts), theft (of data or pin numbers) and pornography, all these facets of computer crime have advanced significantly beyond existing modes of detection.

Bangladesh has been identified as one of the top ten hosts for



Shibu Kumar Shill

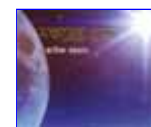
## Also



The lazy bon  
viveur



Three poems  
by Munzur-i-  
Mowla



Diverse  
thoughts in  
poetry



A synopsis of  
Muslim  
empire



Jago Manush  
Nari Odhikar  
Jago



Tribute to the  
folk legend

phishing sites — hosting fake websites or sending fake emails to obtain confidential information — according to Netcraft, a UK company that is doing research and analysis on internet applications.

The incident, although not rare, as Sabir explains is one of the critical online crimes that requires international cooperation to identify and prosecute the criminal. According to Netcraft, Bangladesh has a ratio of one phishing incident reported for every seven websites visited. A lack of international regulations against similar crimes allows its prevalence internationally, he says.

#### The first drops of a coming storm

Although experts foresee a greater volume of cyber crime in the future, Bangladesh has already experienced heinous acts of cyber crimes. In September 2007, most internet service providers (ISPs) in Bangladesh were affected by the Denial of Service (DoS) attack. A large volume of data packets was transmitted from an American data centre and caused server failure, slowing the performance of almost all ISPs. The attack was initially attempted on one ISP, Global Access Limited (GAL).

'These things usually happen because of poor technical expertise for debugging problems. But it is also a stunt for some people to trouble networks,' says Sabir.

Vast quantities of data packets, far beyond the capacity of the national gateway of Bangladesh Telegraph and Telephone Board (BTTB) were being forced through. This caused an overload that bogged down the BTTB router performance. GAL had a 10-megabyte capacity and was virtually staggered by a torrent of 100-megabyte packets. GAL's router became clogged and eventually had to shut down. Later, the port through which the packets were flooding in was identified and blocked. The entire country's ISP performance dwindled and came to a near standstill for over 24 hours. This is just one instance. Graver offences indefinitely continue, unreported and unchecked.

'The impact of cyber crime is not as alarming in Bangladesh because financial transactions have not yet been fully facilitated online,' says Freddy Tan, chief security advisor of Microsoft Southeast Asia. He warns that as soon as financial transactions are allowed online computer crimes will increase at an unprecedented rate, unless the government acquires the tools and infrastructure to prevent, detect and prosecute them. 'Online financial scams are a major threat for banks, credit card holders and alike.'

'Internet services provided through the local area network are vulnerable to similar attacks and intrusions by hackers more often when

the security level is inadequate,' says Sakib Ahmed, chief executive officer of Unilink, another ISP firm. He views genuine firewall software and firewall devices as basic modes of defence from internet threats.

#### Legal chinks and stumbling blocks

'Although the 2006 Information and Communications Technology (ICT) Act covers many of the legal aspects to prosecute cyber crime, it has not been effectively implemented since its ratification,' Mostafa Jabbar, president of Bangladesh Computer Samity (BCS) regrets. One reason for the law's ineffectiveness, he believes, is the lack of legal support and social and public awareness about computer crimes.

'In pursuance of the act, we have requested the law ministry to create special tribunal,' says SM Wahiduzzaman, the secretary of the Ministry of Science and ICT.

The government statistics for cyber crime are not remarkable, but district judges have been empowered to try cases in reference to the penal code and code of criminal procedure. The limited number of cyber crimes apprehended is confined to email threats. According to a government study conducted by the Bangladesh Computer Council, only 0.3 per cent of the total population own computers and 0.7 per cent have access to the internet.

Cyber crime analysts point out that although pornography is not considered illegal across the world, in Bangladesh it is one of the predominant computer crimes. There is already evidence of the existence of illegally hosted pornographic websites with local content. According to section 57 of the ICT Act 2006, a person convicted for uploading vulgar and obscene contents on website is punishable to a 10-year imprisonment and a fine of Tk one crore.

Wojciech Koprowicz, an ICT systems and strategy specialist working on the Police Reform Programme of the United Nations Development Programme, fears that prosecuting the operator of such a site would be made more difficult if the service is located in another country where pornography is not illegal. The act, however, states that if a person from outside Bangladesh commits a crime that is punishable in Bangladesh, the offence would be tried as though it occurred in Bangladesh. At the same time if a person in Bangladesh commits a crime outside the country that is punishable in Bangladesh; the offence would also be tried as if it occurred in Bangladesh.

#### Foreign assistance to cyber crime investigation

Although developments are underway to facilitate cyber crime investigation, the government has yet to build a legal infrastructure to

prosecute cyber crime.

One of the recent developments in fighting cyber crime is national intelligence and law enforcing agencies seeking assistance from foreign agencies and software developers. Members of the National Security Intelligence, Directorate General of Intelligence Forces, Rapid Action Battalion and Special Security Force all participated in a daylong cyber crime investigation programme on February 10. Hosted by Microsoft Bangladesh, the programme covered some technical procedures to collect computer forensic evidence and applications to detect online crimes.

'Microsoft's objective behind organising the Security Cooperation Programme is to secure its products and services from illegal usage,' says Eric White, services executive of Microsoft Corporation. The software firm has signed agreements with the American International University Bangladesh and another law enforcement agency last year to execute Microsoft's Security Cooperation Programme in the country.

Last year the UNDP introduced a US \$16 million project titled the Police Reform Programme (PRP) to develop the police force and its activities. Cyber crime investigation is one of the core components of the PRP.

As part of the project, two top officials of the special branch and the criminal investigation department were sent by the UNDP last year to the Canadian Police College for a weeklong course on cyber crime management.

'Cyber and technology-related crime is on the increase and current trends indicate that it will be a significant issue in South and Southeast Asia,' says NBK Tripura, additional inspector general and national project director for PRP. 'The police are improving their capacities to combat cyber crime,' he said at a UNDP regional seminar on cyber crime last November.

In the meanwhile, the Criminal Investigation Department (CID) has opened an Economic and Cyber Crime Unit that will purely concentrate on financial scams and cyber crimes, CID additional superintendent Ejaz Ahmed informed New Age.

'The computer forensic tools to analyse digital evidence is expected to be commissioned within next six months,' Ahmed says. 'The required software and devices are in the process of being procured for the CID.'

Security versus privacy

As the country continues to advance technologically, the government's

preparedness to fight cyber crime is strongly advocated by experts in the ICT industry. However, one glitch is that preparations to fight cyber crime will empower the government to invade people's privacy on the internet without prior warning. This invasion of privacy and the misuse of it is something industry insiders fear.

'The legal infrastructure is still at a fragmented stage and the government is not in the position to critically discuss the aspects of cyber crime controlling powers,' Wahiduzzaman says.

Abdullah H Kafi, former president of the BCS, believes it is necessary for the government to understand threats from cyber crime and execute legal powers to investigate them. At the same time, a counter intelligence agency should be in place to prevent misuse of state powers.

'There has to be a legal claim or warrant prior to invading people's private network,' says Mostafa, who fears the government may not follow set parameters once authorities have the technology. For now, Wahiduzzaman says, the government is working on to develop a legal framework loosely based on the ones implemented in neighbouring countries.

A new crime every day

Another prevailing difficulty is that cyber crime keeps evolving and taking on new unprecedented forms that can quickly become widespread. One instance is a 'bot', or a hacked computer controlled from a different location to commit crimes. Bots can be located anywhere a hacker finds unprotected computers on the internet, explains IB Terry III, an investigative consultant to the Microsoft Law Enforcement Support Team. Hackers can infect the computers with programmes that later on give them control over the computer and access to confidential information such as passwords, account names and numbers and so on, he says. 'This is yet another crime that could prevail anywhere around the world so as for criminals to dodge arrest.'

In 2003, Nigerian criminals abducted the son of an influential Bangladeshi businessman through a million dollar scam. An ICT industry source reports that the businessman's son was emailed from Nigeria, apparently with an offer to invest a substantial amount of money in a bank account. After detailed email correspondence, the young man eventually went to in Nigeria to collect the money and fell prey to an abduction trap.

The abductors threatened the victim's family that they would kill him if the family did not abide by their instructions. Luckily, after his millionaire family paid a hefty ransom, he was released and allowed to

return.

Wojciech says such scams continue to victimise people across the world.

'As long as you are connected to the internet, you are equally vulnerable to any computer threat as any other country,' says Microsoft security advisor Freddy Tan.

---

**Top | Xtra**

**COPYRIGHT © NEW AGE 2005**

**Mailing address** Holiday Building, 30, Tejgaon Industrial Area, Dhaka-1208, Bangladesh.

**Phone** 880-2-8153034-39 **Fax** 880-2-8112247 **Email** [xtra@newagebd.com](mailto:xtra@newagebd.com)

**Web Designer** Zahirul Islam Mamoon