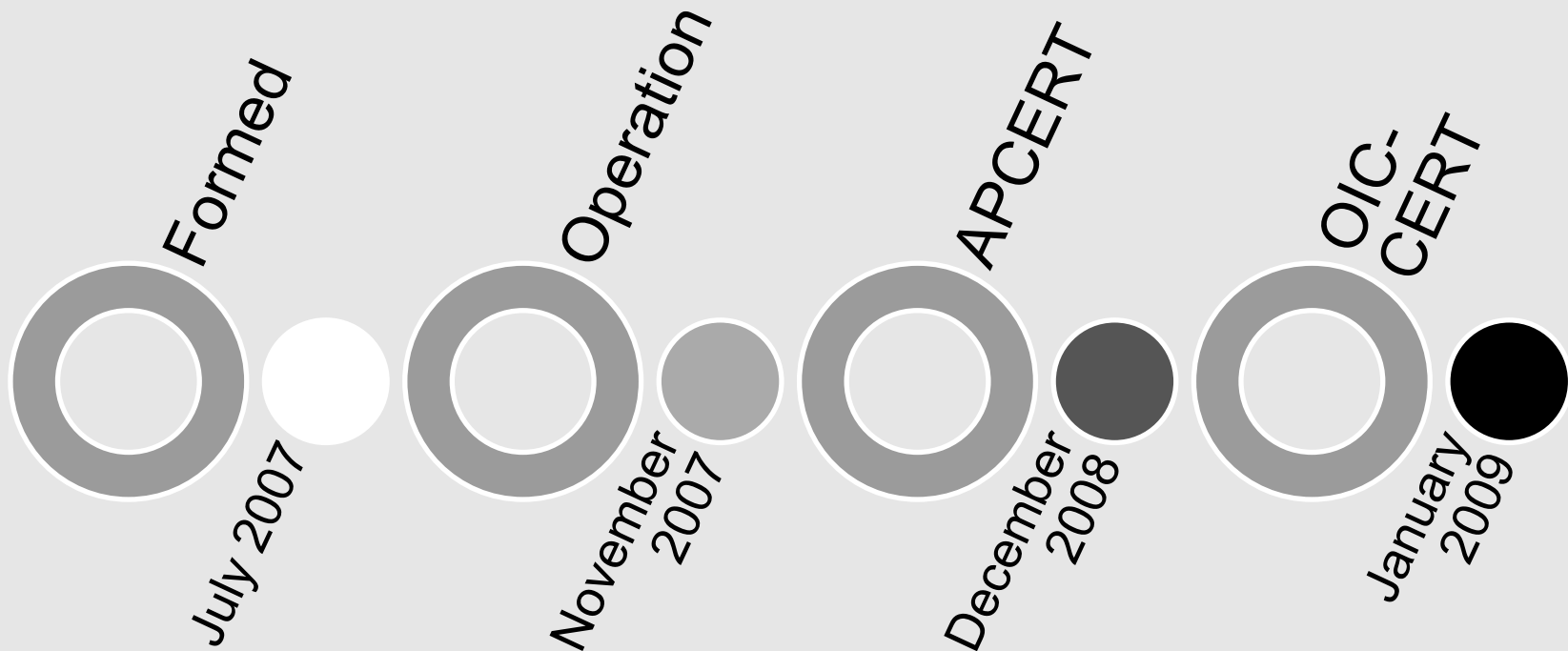


Bangladesh Cyber Incident Trends 2012 & bdCERT Update

Mohammad Fakrul Alam
Manager, Computer Forensic
bdCERT
fakrul [at] bdcert [dot] org
<http://www.bdcert.org>

bdCERT: An Overview

bdCERT



Started by few self motivated individuals on a voluntary basis.

bdCERT : Mission Statement

- Always **Trusted Contact, Increase Computer and Network Security** for Bangladesh Internet and Intranet Users, **Knowledge Sharing** with other CERTs & Related Organization.

bdCERT : Functions

- **Point of contact** for reporting local problems.
- Share **information** and **lessons** learned from other CERTs, response teams, organizations and sites.
- Incident **tracing & response**.
- Organize **training, research** and **development**.

bdCERT : Activities

■ Incident Handling

- Email
- SMS
- FAX
- Web Form

- “Internet **Traffic Monitoring** Data Visualization **Project**” with JPCERT/CC (Japan Computer Emergency Response Team / Coordination Center) named “**TSUBAME**”.
- Collaboration with **Team Cymru**.
- Participate in APCERT, OIC-CERT **Cyber Security Drill**.

bdCERT : Program

- 26 May 2012 to 27 June 2012: Training Program on Cyber Crime and Computer Forensic

2 Days long training program on Cyber Crime & Computer Forensic. Participants were from Law enforce agencies, and Government Officials.



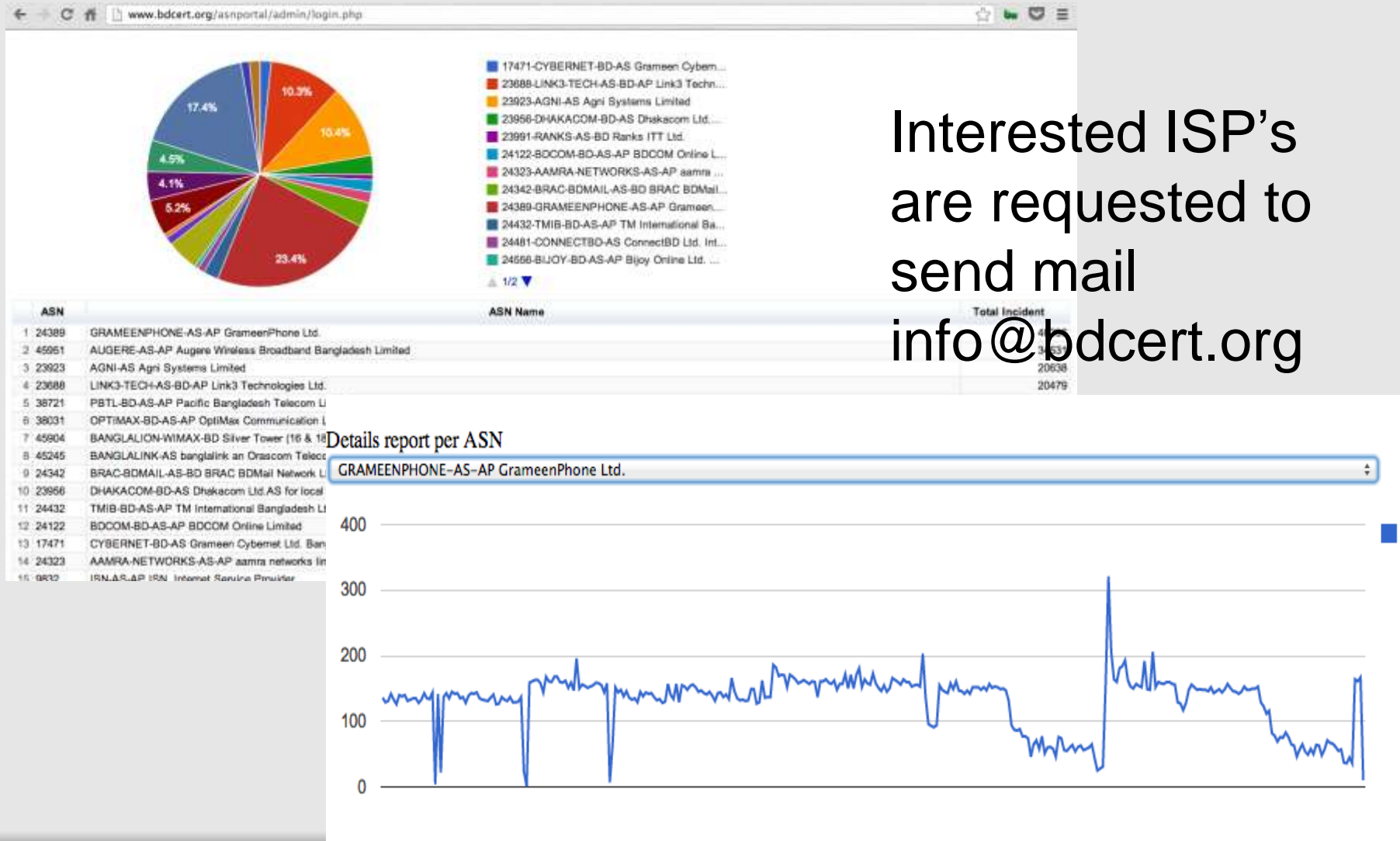
bdCERT : Program

- 11 June 2012 to 13 June 2012: Training program on Cyber Attack & Network Forensic

3 days long training program on Cyber Attack & Network Forensic organized by ISPAB in collaboration with bdCERT. This training program is supported by ICT Business Promotion Council. Participants come from all area which includes Financial Institute, Law enforce agencies, Government Officials, ISP, Telecommunication Industry.



bdCERT : ASN Portal Service



bdCERT : Future Plan

- Introduce **New services**.
- Consulting & **Awareness Programs**.
- New **collaborations**.
- Cyber Security **Workshop** for **Government** and **Academics**.

Bangladesh Cyber Incident Trends 2012

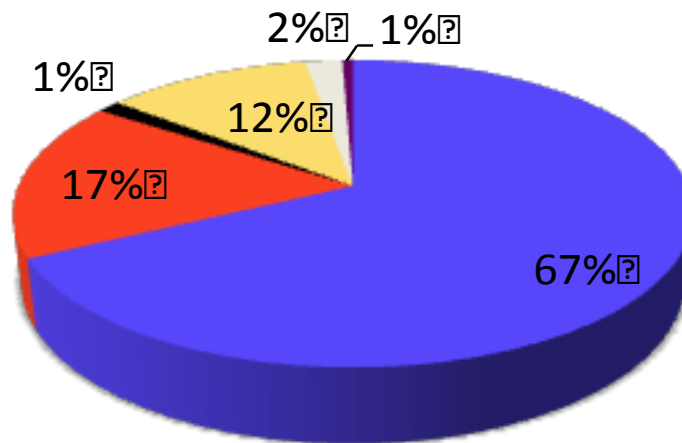
Bangladesh Cyber Security Incidents

Data received from different **sensors** across the globe.

125580 individual **incident**, **23131** Unique **IP**

Incident Distribution

Spam Bots Bruteforce Open Resolver Proxy Scanner



Data reported from 1st June, 2012 to 31st December, 2012

Hacker Groups

- Different hacker group emerge.
- Bangladesh Cyber Army & Bangladesh Black Hat Hackers are most active one.
- Claims that they have collaboration with other underground hacking group.
- Hacktivism takes center stage.

Use of Social Media

- Facebook, Twitter and other social media were used to organize the attack.



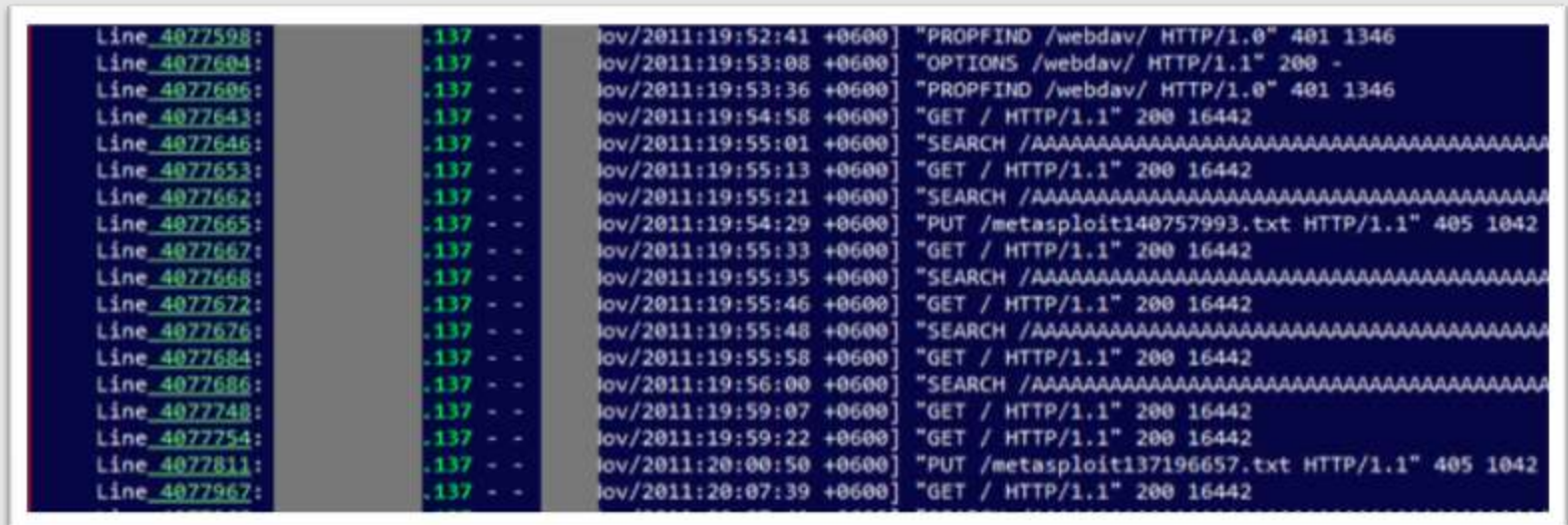
Site Defacement

- Site hacked by hacker group named Indishell.
- Government sites were targeted.



Site Defacement

- Site defacement using known techniques like SQL Injection, **Metasploit** and **CMS** vulnerability.
- **64** district web-portals inaugurated on 06 January 2010 while the hackers invaded **19** of them by 21 March/2010.



```
Line_4077598: .137 - - [06/Nov/2011:19:52:41 +0600] "PROPFIND /webdav/ HTTP/1.0" 401 1346
Line_4077604: .137 - - [06/Nov/2011:19:53:08 +0600] "OPTIONS /webdav/ HTTP/1.1" 200 -
Line_4077606: .137 - - [06/Nov/2011:19:53:36 +0600] "PROPFIND /webdav/ HTTP/1.0" 401 1346
Line_4077643: .137 - - [06/Nov/2011:19:54:58 +0600] "GET / HTTP/1.1" 200 16442
Line_4077646: .137 - - [06/Nov/2011:19:55:01 +0600] "SEARCH /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Line_4077653: .137 - - [06/Nov/2011:19:55:13 +0600] "GET / HTTP/1.1" 200 16442
Line_4077662: .137 - - [06/Nov/2011:19:55:21 +0600] "SEARCH /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Line_4077665: .137 - - [06/Nov/2011:19:54:29 +0600] "PUT /metasploit140757993.txt HTTP/1.1" 405 1042
Line_4077667: .137 - - [06/Nov/2011:19:55:33 +0600] "GET / HTTP/1.1" 200 16442
Line_4077668: .137 - - [06/Nov/2011:19:55:35 +0600] "SEARCH /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Line_4077672: .137 - - [06/Nov/2011:19:55:46 +0600] "GET / HTTP/1.1" 200 16442
Line_4077676: .137 - - [06/Nov/2011:19:55:48 +0600] "SEARCH /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Line_4077684: .137 - - [06/Nov/2011:19:55:58 +0600] "GET / HTTP/1.1" 200 16442
Line_4077686: .137 - - [06/Nov/2011:19:56:00 +0600] "SEARCH /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Line_4077748: .137 - - [06/Nov/2011:19:59:07 +0600] "GET / HTTP/1.1" 200 16442
Line_4077754: .137 - - [06/Nov/2011:19:59:22 +0600] "GET / HTTP/1.1" 200 16442
Line_4077811: .137 - - [06/Nov/2011:20:00:50 +0600] "PUT /metasploit137196657.txt HTTP/1.1" 405 1042
Line_4077967: .137 - - [06/Nov/2011:20:07:39 +0600] "GET / HTTP/1.1" 200 16442
```


DDoS Attack

- DDoS attack on several financial institutions websites.
- Reported **application layer** (HTTP GET Flood) on online newspaper portal. Attack stays for **72 hours** with roughly **5 million packets** per second.

Phishing Attack

Team,

We are an Internet security company in the United States working on behalf of Live.com - Microsoft. We are contacting your organization to report phishing content targeting Live.com - Microsoft's brand and customers that was detected on 7/2/2012.

Our research shows that your organization provides services for a website that's been compromised and used in a phishing attack. Please investigate the location(s) below:

http://www.█.gov.bd/upload/img/Hotmail_Email

IP Address: 123.49.32.█

This is an illegal and unauthorized copy of Live.com website that was created in an attempt to trick customers into sending sensitive personal and financial information to criminals. We request that you deactivate this immediately.

> -----Original Message-----

> From: █
> [mailto:customers.service@█.net]
> Sent: Tuesday, June 29, 2010 1:27 AM
> To: █@█.net
> Subject: Internet Banking Upgrade

> INFORMATION - SECURITY SERVER UPGRADE

> Dear Valued █ la Bank Customer,

> █ technical department will be carrying out a systematic upgrade on
> our Network server from 3.00 pm today to 5am tomorrow morning
> to avoid hackers from accessing your account.
> To take your account through this upgrade process,

> Please click below to upgrade your account

> Click here

> *Note. █ la Bank will not be responsible for loss of funds to
> online Phishers
> as a result of failure to comply with this new directive.

Information Leakage

- Information data leakage in PASTEBIN



The screenshot shows a web browser window with the address bar containing the URL `pastie.org/pastes/[REDACTED]/text`. The page content displays several lines of text, including server names, links, IP addresses, and credentials for various services.

```
Server Name:  
Link: test.[REDACTED].gov.bd  
  
IP: 10.[REDACTED].30.173  
username: root  
password: dghs2[REDACTED]  
  
ftp  
everyhting same... Just port is 22  
  
host: localhost  
mysql username: root  
password: mist[REDACTED]db  
-----  
Server Name:  
Link: app.[REDACTED].gov.bd  
  
ftp username: 10.[REDACTED].47.38.11  
username: mls[REDACTED]min  
password: ml[REDACTED]admin@2013  
port: 22
```

Thank You
