ISO 9001 : 2008

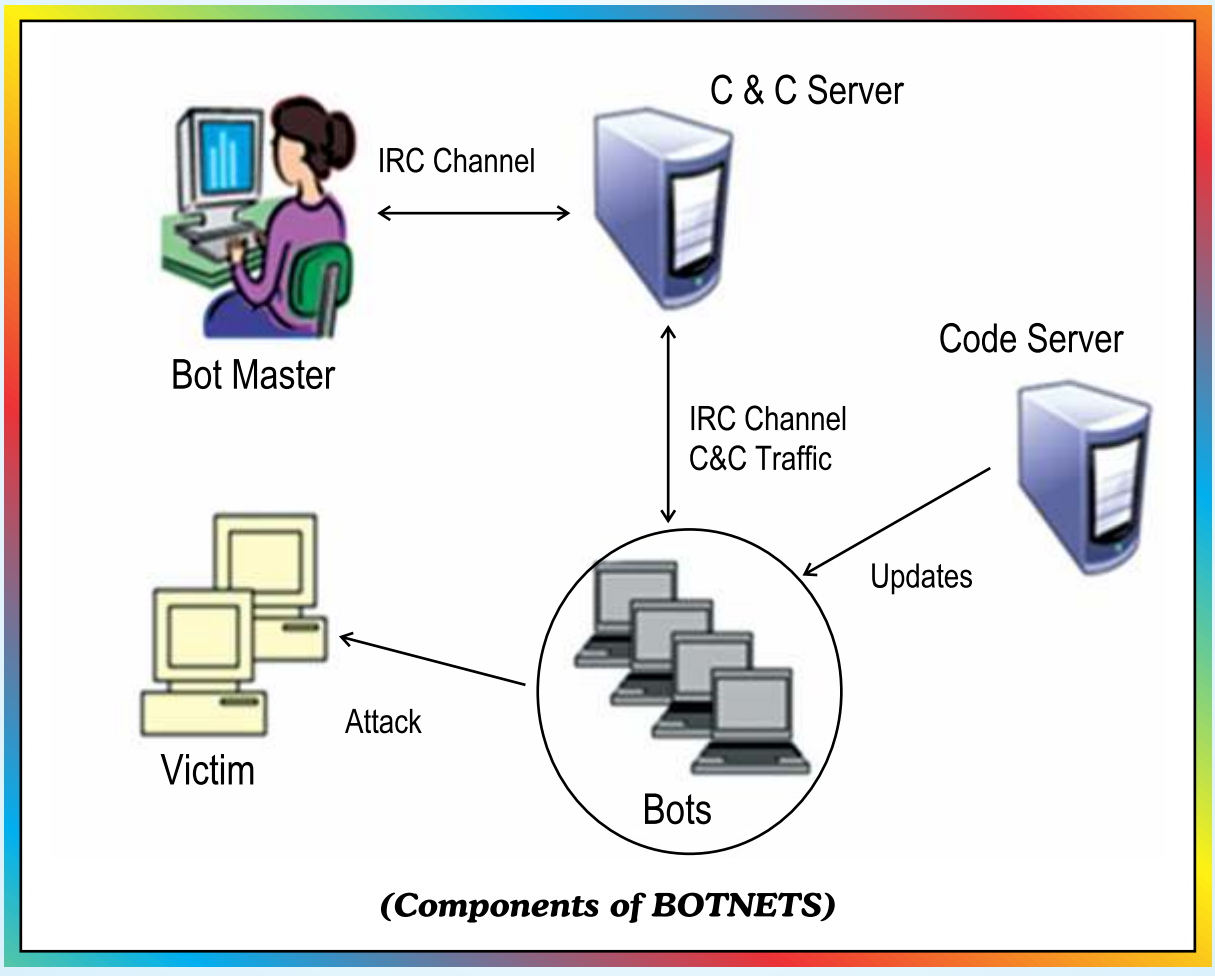
TEC

टी ई सी संचारिका

NEWSLETTER

VOL. 18 MAY 2014 ISSUE 2

CYBER SECURITY : MOVING TOWARDS A SAFE WORLD



(Components of BOTNETS)

ISO 9001:2008
TELECOMMUNICATION ENGINEERING CENTRE

IN THIS ISSUE

1.0 Introduction:

In last couple of decades, India has emerged as the largest hub of IT related activities. More and more services are being brought online, thereby improving the quality of our life but at the same time increasing our dependence on internet.

This dependency on internet has seen spurt of cyber attacks on individuals and institutions. Today Cyber space is witnessing groups of organized cyber criminals who are ready to pounce upon the innocent victims in cyber space. There is at least one instance of cyber war against a nation creating havoc on its economic activities.

As the technology evolves, the computing devices change in dimension, portability, mobility and complexity and so does the malware (Malicious + Software). The malware also adapts to new technologies and find many more effective ways of penetrating devices.

With time malware has increased its attributes by:

1. Infection methods
2. Persistency
3. Protective mechanism
4. Continuous Interaction with the attacker
5. Modular Up gradation of malicious software instruction

Table A gives the details about the growth of virus and malwares over the years and clearly shows that Botnets/APT(Advance Persistent Threats) have emerged as the most serious threats in the present scenario and awareness about Botnets is a step towards fighting it in the cyber space. Similarly Mobile Apps are also posing threats in our daily use of mobile phones. In this issue of TEC Newsletter, Botnets and threats posed by Mobile Apps has been discussed in detail.

2.0 BotNet

Botnets are the compromised computers whose security defences have been breached and control conceded to a third party. Each such compromised device, known as a "bot", is created when a computer is penetrated by software from a malware distribution entity. The controller of a botnet is able to direct the activities of these compromised computers through IRC(Internet Relay Chat) channels using a Command & Control Server.

IRC provides a way of communicating in real time with people from all over the world. It consists of various separate networks (or "nets") of IRC servers, machines that allow users to connect to IRC. IRC is very similar to text messaging, but designed around communicating with large groups of users instead of one on one.

Table A

Evolution of Botnet			
Malware	**Persistence since**	**Common remedial Action**	**Remarks**
Virus	**1995**	**Antivirus**	**Virus is malicious computer instruction, which needs intervention to prevent reduplicating to other computer**
Network Worm	**1998**	**Antivirus**	**Worm is virus with reduplicating power over network**
Spyware & Rootkits	**2000**	**IDS/IPS**	**Network based threat defence System**
Botnets /APT	**2005 onward**	**Research is on**	**Advanced persistence threats**

2.1 How Bots Work

Bots sneak onto a person's computer in many ways. Bots often spread themselves across the Internet by searching for vulnerable, unprotected computers to infect. When they find an exposed computer, they quickly infect it and then report back to their master. Their goal is then to stay hidden until they are instructed to carry out a task. A typical schematic of the working of Botnet is at cover page which may be referred.

After a computer becomes part of Botnet, it can be used to carry out a variety of automated tasks, some of which are given in Table B.

2.2 Command and Control Server

"Command and Control" (C&C) servers are centralized machines that are able to send commands and receive outputs of machines part of a botnet. Attackers can send special commands to their botnet's C&C servers with instructions to perform an activity on a particular target, and any infected machines communicating with the contacted C&C server will comply with.

Table B

Sending	Stealing	DoS (Denial of Service)	Click fraud
They send • spam • viruses • spyware	They steal personal and private information and communicate it back to the malicious user: • credit card numbers • bank credentials • other sensitive personal information	Launching denial of service (DoS) attacks against a specified target. Cybercriminals extort money from Web site owners, in exchange for regaining control of the compromised sites. The systems of everyday users are the targets of these attacks	Fraudsters use bots to boost Web advertising billings by automatically clicking on Internet ads.

Botnet C&C servers often exist in one of four structures:

(i) **Star** topology botnets rely on one central C&C server, which sends commands to every bot in the botnet.

(ii) **Multi-server** topology botnets are very similar to star topology botnets, except that the central "server" consists of a series of interconnected servers that allow for redundancy (preventing the single point of failure problem of star topology botnets).

(iii) **Hierarchical** topology botnets (involving a series of C&C servers in a hierarchy) allow for botnet owners to more easily divide their botnet up into "separate" chunks for re-sale or renting, as well as prevent researchers from enumerating the location of all other C&C servers and bots within a network with only a few captured C&C servers due to the restricted visibility of the entire botnet from lower hierarchy certain servers.

iv) **Random** topology botnets do not rely on any C&C servers, rather all botnet commands are sent directly from one bot to another if they are deemed to be "signed" by some special means indicating that they have originated from the botnet owner or another authorized user.

2.3 Botnet Detection Techniques

These can be classified as below

- Honeypot
- Passive anomaly analysis
- Based on traffic application.

2.3.1 A **honeypot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

2.3.2 The passive anomaly based detection is done by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that falls out of normal system operation. This is as opposed to signature based detection which can

only detect attacks for which a signature has previously been created. In order to determine what traffic attack is, the system must be taught to recognize normal system activity.

2.3.3 Botnet detection techniques **based on traffic application** classification are usually guided by botnet C&C control protocol e.g. if one is only interested in IRC-based botnets then traffic will be classified into IRC and non-IRC groups.

2.3.4 Protection against Bots

To safeguard against bots, the following suggestions will help the users:

1. Install best in class security software.
2. Configure software's settings to update automatically.
3. Increase the security settings on the browser.
4. Limit user rights when online.
5. Never click on attachments unless the source is verified.
6. Ensure that OS is patched with the most OS Update.

3.0 Mobile APPs : Reality and Threat

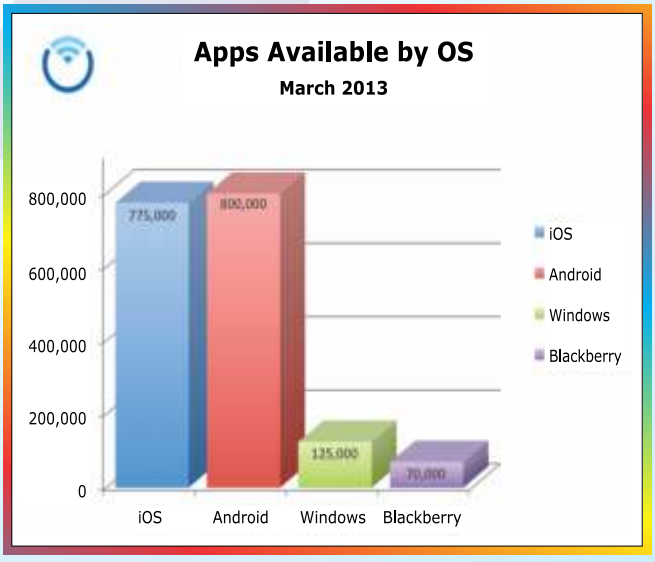
In 2013 handset makers sold over 40 million units of smart phones. Use of mobile applications is one of the main feature of the smart phones. These application are usually available through application distribution platforms, which began appearing in 2008 and are typically operated by the owner of the mobile operating system(OS), such as the Apple App Store, Google Play, Windows Phone Store, and BlackBerry App World.

A typical Android Ecosystem is shown in the diagram below:.

Android Ecosystem

There are millions of Apps developers across the globe having tie ups with smart phone manufacturers and service providers on commercial basis.

3.1 Mobile Apps figures for various mobile OS are indicated below:



(source:http://www.pureoxygenmobile.com/how-many-apps-in-each-app-store/)

3.2 App user trend worldwide

Table C

Users of mobile apps worldwide by 2012-2017 according to Portio Research			
Region	**2012**	**2013**	**2017 (projected)**
App users worldwide	1.2 billion	N/A	4.4 billion
Asia Pacific	30%	32%	47%
Europe	29%	28%	21%
North America	18%	17%	10%
Middle East & Africa	14%	13%	12%
Latin America	9%	10%	10%
Source: © Portio Research (March 2013)		**via: © mobiThinking**	

(source : http://mobithinking.com/mobile marketing-tools/latest-mobile-stats/e)

Before an App is downloaded by user on to his or her Smartphone , the App ask access for user smartphone key data stored in smartphone compromising security and confidentiality of user. Though the apps have made life easier for net users but seeking access to their personal and confidential information raises serious concerns about security.

One of the most popular apps, Whatsapp works even where mobile SIM does not work ; all it needs is a WI-FI connection.

3.3 Potential threats arising from an infected mobile apps.

Table - D

Types of Threats	Technique	User Implication
Data Stealer	Steals information stored in the mobile device and sends it to a remote user	Stolen information maybe used for malicious purposes
Premium Service Abuser	Subscribes the infected phone to premium services without user consent	Unnecessary charges for services not authorized by user
Click Fraudster	Mobile devices are abused via clicking online ads without users' knowledge (pay-per-click)	Cybercriminals gain profit from these clicks
Malicious Downloader	Downloads other malicious files and apps	Mobile device is vulnerable to more infection
Spying Tools	Tracks user's location via monitoring GPS data and sends this to third party	Cyber criminals track down location of users
Rooter	Gains complete control of the phone, including their functions	Users' mobile devices are exposed to more threats

3.4 Possible Solutions: Controlling of the fallouts of threats from the mobile apps in a country appears to be a tall order till the world community is able to find any mechanism to regulate the apps from the points of view of privacy and security. Presently, the only solution appears to be community awareness.

4.0 Cyber Security event in DOT HQ

NTIPRIT organized one day seminar on ***"Cyber Security: Moving towards a safe world"*** in DOT HQ. The aim was to create awareness among DOT officers about the cyber security. The seminar was inaugurated by Shri M F Farooqui Secretary (T). Total 72 participants attended the seminar.

Speakers from IIT Delhi, CERT- in, Security Cell of DoT, NTIPRIT, and TEC made the audience aware of various perspective of the cyber security. The seminar was appreciated by all the participants.

Inaugration of seminar: L to R, Ms. Annie Moraes, Member (F), Shri S.C. Misra, Member (S), Shri M. F. Farooqui, Secretary (T) & Shri Anil Kasuhal, Member (T)

4.1 Cyber Security Practices around the world

Entire world community has given enormous thrust on the cyber security and many efforts have been done so far making internet a safe place to work. In this regard many countries like the USA, UK, Russia, Japan prepared their cyber security policies to take utmost care for the safety of their citizens. Emphasis on generating awareness among common user is being given by every country.

In the last week of Feb 2014 a delegation from DOT attended a ten days training on " Cyber Security and technologies for Broadband" at Tokyo in Japan. This gave an opportunity to see how Japan is putting effort. The training was organized by the APT(Asia Pacific Telecommunity).

It was informed during the training that Japan has Online Monitoring System **NICTER** (Network Incident analysis Center for Tactical Emergency Response) and a project named **PRACTICE** (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) funded by MIC(Ministry of Internal affairs and Communications) to implement the measures for combating against spam.

Apart from making all these efforts, Japan prepared a comprehensive plan to generate awareness among common users of Internet. It is important to mention here that Japan observe one full month as " Information Security Awareness Month".

Activities at NTIPRIT

1. In-service Courses for DOT Officers

i. One day Workshop on RTI Act held at TEC
ii. One day Seminar on Cyber Security held at Sanchar Bhawan
iii. One day course on "Understanding IPv6" conducted for DeITy
iv. Advanced GSM course held at NTIPRIT
v. Advances in Transmission Technologies course held at NTIPRIT

2. Induction courses for Officer Trainees

i. ITS-2011 and ITS-2012 & BWS-Civil Engineering 2011 Batch are undergoing their induction programme.
ii. Highlights of Orientation Programme of ITS 2012 batch: Shri M. F. Farooqui, Secretary (T) & Chairman Telecom Commission, Shri Anil Kasuhal, Member (Technology), Shri S.C. Misra, Member (Services), Ms. Annie Moraes, Member (Finance), Ms. Nirmala Pillai Advisor(F), Shri Ram yagya Advisor(O), Shri A K Purwar Advisor (T), CMD, BSNL, MTNL, TCIL interacted with the officer trainees and shared their experiences giving them important tips to become a good government officer

3. In-service courses scheduled during quarter (up to June 2014)

i. Cyber Security (05-05-2014 to 07-05-2014)
ii. GSM, CDMA and UMTS Technologies (19-05-2014 to 23-05-2014)
iii. Role of Telecom in Disaster Management (26-05-2014 to 27-05-2014)
iv. Greening the Telecom for sustainable Development (03-06-2014 to 04-06-2014)
v. Billing and IN (09-06-2014 to 10-06-2014)
vi. Understanding Network Security (23-06-2014 to 25-06-2014)

हिंदी कार्यशाला

दूरसंचार अभियांत्रिकी केंद्र द्वारा दिनांक 24.03.2014 को एक हिन्दी कार्यशाला का आयोजन किया गया। श्री केवल कृष्ण (वरिष्ठ तकनीकी निदेशक), राजभाषा विभाग द्वारा राजभाषा हिन्दी के लिए आईटी का उपयोग तथा ई-महाशब्दकोश, लीला सॉफ्टवेयर से हिन्दी सीखना, गूगल में अकाउंट बनाकर अनुवाद करने, विंडोज एक्स पी एवं विंडोज विस्टा में यूनिकोड सक्रिय करने के बारे में बारीकी से बताया गया।

कार्यशाला में भाग लेते हुए अधिकारी एवं कर्मचारीगण

Approvals from JAN 14 to MAR 14

S.No	Company/Product & Modal No
1	M/s Tata Power Company Limited,
1.1	IP PABX FOR PRIVATE USE, IPVCS 2121
2	M/s ZTE Telecom India Private Ltd.
2.1	Switching node with network-network interface at 2048 Kbits (Soft switch controlled by Media gateway),ZXC10- 3GCN(MSCe/MGW/SGW),
3	M/s Huawei Telecommunications India Co. Pvt. Ltd
3.1	Switching Node with Network-Network Interface with STM-1,UGC 3200and UMG 8900
3.2	Switching Node with Network-Network Interface ,MSOFTX 3000 with UMG 8900
4	M/s MATRIX COMSEC PVT. LTD.
4.1	ISDN PABX ,ETERNITY ME
5	M/s CLIXXO Broadband Pvt. Limited
5.1	IP PABX FOR PRIVATE USE, CLIXXO IPX-22K
6	M/s Coral Telecom Limited
6.1	IP PABX FOR PRIVATE USE, CLIXXO IPX-22K
6.2	ISDN/DID EPABX ,DX2000
7	M/s Aspect Contact Centre Software India Pvt Ltd.
7.1	System Employing Computer Telephony Integration,TMS-00
7.2	System Employing Computer Telephony Integration,UMS-00
8	M/s Smartlink Network System Ltd.
8.1	High Speed Line Drivers, DG-LM
9	M/s D-link (India) Ltd.
9.1	High Speed Line Drivers,DLM-E2000V
9.2	High Speed Line Drivers,DLM-E2000G
9.3	High Speed Line Drivers,DSL-1504G
9.4	High Speed Line Drivers,DLM-E2000G
9.5	High Speed Line Drivers,DLM-E2000V
10	M/s Siemens Enterprise Communications
10.1	ISDN PABX FOR PRIVATE USE, Open Space Branch 500i DP8 with Open Scape Voice
11	M/s NEC India Pvt. Ltd.
11.1	Indoor Unit (IDU) for Point to Point Digital Microwave Relay System,MDP-400MB-1BB
12	M/s ECI Telecom India Pvt. Ltd.
12.1	Digital Multiplexer(SDH)STM-4,BG20B
12.2	Digital Multiplexer(SDH)STM-16,XDM 900
12.3	Digital Multiplexer(SDH)STM-4,XDM100
12.4	Digital Multiplexer(SDH)STM-16,XDM 300
12.5	Digital Multiplexer(SDH)STM-1,μSDM
12.6	Digital Multiplexer(SDH)STM-4,BG30
12.7	Digital Multiplexer(SDH)STM-16,BG30
12.8	Digital Multiplexer(SDH)STM-4,BG64
12.9	Digital Multiplexer(SDH)STM-16,XDM 100
12.10	Digital Multiplexer(SDH)STM-16,XDM 100
13	M/s Sunren Technical Solutions Pvt. Ltd.
13.1	Terminal for Connecting to PSTN,PC1616
13.2	Terminal for Connecting to PSTN,PC1832
13.3	Terminal for Connecting to PSTN,PC1864
13.4	Terminal for Connecting to PSTN,PC4020
13.5	Terminal for Connecting to PSTN,PC9155-433
13.6	Point of Sales Terminal,VX 520
14	M/s Beetel Teletech Limited
14.1	Electronic Telephone Instrument,SECURE-I
15	M/s Team Engineers Advance Technologies
15.1	High Speed Line Driver,Teamlink 3002 SHDSL E1
15.2	High Speed Line Driver,Teamlink 3002 SHDSL V.35
16	M/s TEJAS NETWORKS LTD.
16.1	STM -1 TM/ADM,TJ 1400
16.2	STM -4 TM/ADM,TJ 1400
16.3	STM -4 TM/ADM,TJ 1400
17	M/s Alcatel- Lucent
17.1	IP based Integrated Media Gateway (MGW-7520)

Important Activities of TEC during JAN 14 to MAR 14

New GRs/IRs Issued :

- GR on Policy and Charging Rule Function
- GR on Server, OTN Analyser
- GR on Integrated Gateway Router(IGR)
- GR on MPLS Router Based Transport Network
- GR on 34 Mbps Bandwidth Saving Satellite System
- GR on RAN Optimization for Satellite & Terrestrial Network
- GR on Universal Mobile Charger
- IR on WiFi CPE(USB)

Revised/Amended GRs/IRs Issued :

- IR on Router, CPE for MPLS Network
- IR on Mobile Radio Trunking Communication Equipment and subscriber Unit
- GR on SBC , LMG, CDN, LAN Switch,
- GR on Set Top Box, Firewall, NMS for NGN, Router for Cordect system, NMS for IP based Transit and Local Public Switch Network
- GR on Electronic Locator System

Study Paper / White Paper issued on:

- Policy and Charging Rule Function
- Wimax Future Road Map
- IMT 4G Technologies (Progress & Deployment)
- BWA Technologies for Rural Area
- Satellite Interference and Carrier ID
- IP Network Security
- Approach Towards Standardization of Green Telecom Equipments
- FTTH Cable Network
- Quality of Service in IP Network

Other Activity

- Testing/field trial of Priority Call Project at ALT Ghaziabad
- Testing/field trial of CMS Project at CDOT Delhi
- तकनीकी विषयों की हिन्दी शब्दावली का निर्माण

ISO 9001 : 2008

Certifications issued by TEC

Type Approval (TA)

Interface Approval (IA)

Certificate of Approval (CoA)

Visit

www.tec.gov.in

Regional TEC Contacts

Eastern Region	:	033-23570010
Western Region	:	022-26610900
Northern Region	:	011-23329464
Southern Region	:	080-26642900

Approvals issued by TEC during the period from JAN 2014 to MAR 2014

Interface Approvals.....41
Type Approvals 0
Certificate of Approvals.....0

टी ई सी संचारिका : दूरसंचार इंजीनियरी केन्द्र
मई 2014 : खुर्शीद लाल भवन
भाग 18 : जनपथ
अंक 2 : नई दिल्ली-110001

Editor : Sunil Purohit, DDG (S) Phone : 23329354 Fax : 23318724 E-mail : ddgs.tec@gov.in

Sai Art Graphics : Mob. 9899027477