Cyber Security
Threats & Vulnerabilities

S.S.Sarma, CISSP, CEH
Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

Outline

- About CERT-In
- Information Security – CIA
- Threats
  - Types of threats
- Vulnerabilities
- Cyber Security incidents
- Cyber Security measures
  - Organisational
  - User
- Resources

CERT-In

- Established in January 2004 by Department of IT
- Section 70B, Information Technology Act 2000 (Amended in 2008): Designates CERT-In as the national agency to perform the following functions in the area of cyber security:

  - Collection, analysis and dissemination of information on cyber incidents
  - Forecast and alerts of cyber security incidents
  - Emergency measures for handling cyber security incidents
  - Coordination of cyber incident response activities
  - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
  - Such other functions relating to cyber security as may be prescribed

Role of CERT-In

- Incident Response (Reactive Service)
  - Operating Incident Response Helpdesk on 24X7 basis
- Incident Prevention and Security Awareness (Proactive Service)
  - Tracking of Security Threats and Cyber attacks
  - Issuance of Security Alerts and Advisories
  - Tailored alerts to CISOs/POCs
  - Conducting Security Workshops and Security Awareness Programs
- Security Quality Management Services
  - Promotion of Security Best Practices and Security Standards
  - Empanelment of Security Auditors
  - Conducting Security Mock Drills
  - Implementation of Cyber Crisis Management Plan (CCMP)

Information Security – CIA

- Confidentiality
  - ensuring that information is accessible only to those authorized to have access
- Integrity
  - assurance of accuracy and reliability of information
  - unauthorized modification of data is prevented
- Availability
  - Information is being accessible and usable upon demand by an authorized entity

Threats to Information Security

- Confidentiality
  - Unauthorised Disclosure
- Integrity
  - Unauthorised Alteration
- Availability
  - Disruption

Information Assets

Asset: Anything that has value to the organization

- Financial data
- Business Plans
- Customer information
- Product design
- Legal documents
- Software - systems and applications

Threats

An event, the occurrence of which could have an undesirable impact on the well-being of an asset.

[International Information Systems Security Certification Consortium ISC2]

Any circumstances or event that has the potential to cause harm to a system or network .That means, that even the existence of a(n unknown) vulnerability implies a threat by definition.

[CERT]

Vulnerability

- A feature or bug in a system or program which enables an attacker to bypass security measures.
- An aspect of a system or network that leaves it open to attack.
- Absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact or both.

Categories of Threats

- Natural
  - Cyclone, Fire, Flood, Earthquake
- Unintentional
  - Accidental Power loss, Forgetting Password, Unattended Terminal Display
- Man-Made
  - Intentional Viruses, Espionage

Info Security Threats

- Transmission Threats
  - Eavesdropping/Sniffers
  - DoS/DDoS
  - Covert channel
  - Spoofing
  - Tunneling
  - Masquerading/man-in-the middle attacks

- Malicious Code Threats
  - Virus
  - Worms
  - Trojans
  - Spyware/adware
  - Logic Bombs
  - Backdoors
  - Bots

- Password Threats
  - Password crackers

Info Security Threats

- Social engineering
  - Impersonation
  - Dumpster diving
  - Shoulder surfing
- Physical Threats
  - Physical access
  - Spying
- Application Threats
  - Buffer overflows
  - SQL Injection
  - Cross-site Scripting
- Improper usage/Un-authorized access
  - Hackers
    - Whitehats, Black hats
  - Internal intruders
  - Defacement
  - Spam
  - Phishing

Cyber Security incident

“Cyber security incident” means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization”

- Information Technology Act, 2000

Cyber threats & incidents

National level

- Cyber Terrorism
- Attacks on Critical Infrastructure
- Supply chain compromise
- Ransomware
- Cyber espionage
- Mis/Dis information

Organisational level

- Scanning and probing
- Vulnerable services
- Website intrusion/ defacement
- Domain stalking
- Malicious Code
- Ransomware
- Denial of Service & Distributed Denial of Service
- Phishing
- Targeted attacks
- Data theft
- Insider threats
- Financial frauds

Individual level

- Social Engineering
- Email hacking & misuse
- Identity theft & phishing
- Financial scams
- Abuse through emails
- Abuse through Social Networking sites
- Mobile device threats
- Laptop/device theft

Cyber Security threat landscape

- Attack Targets
  - Critical infrastructure
  - Business intelligence
  - Personally identifiable information
- Attack Motives
  - Disruption of Services
  - Cyber espionage
  - Financial frauds
- Attack elements
  - Cyber criminals
  - Hacker groups
  - Malicious Insiders
- Attack vectors and medium
  - Botnets
  - Vulnerabilities and Exploit tool kits
  - Social engineering
  - Ignorant users

Threat Landscape

Threat	Current Trend	Targeted Entity	Assets	Impact
Targeted scanning, probing and attacks (hacking and intrusion)	↑	All	Network Architecture, IT systems, applications and services, websites	Focused attack leading to total/ partial disruption of services, loss of reputation, data theft and cyber crisis
Malware (Virus, Spyware, Trojans and Ransomware)	↑	All	End user systems, mobile devices, Point of sale systems, ATM	User level data theft, Financial loss and ransom
Sophisticated malware	↑	Utilities , Manufacturing	Industrial control systems	Total/ partial disruption of essential services and business
Identity theft, phishing and vishing	↑	Finance , Retail , Citizens	Payment gateways, portals , user credentials	Economic loss to financial institutions and individuals
Attack on Domain Name server and routers (Gateway and ADSL)	↑	Telecom	Domain Name server , Routers, Home user systems	Disruption of internet traffic and illegal diversion of Internet and mail traffic to other countries
Botnets and Spam	↑	Telecom	Computers, Cloud , mobile devices , IoT	Large scale disruption of service, annoyance, piracy and financial frauds
Targeted Attacks / APT	↑	BFSI/ Finance, Govt, Military , Research /Academia, Healthcare	Computer, Mobile, Applications	Espionage, Data breach, IP theft, Unauthorized Transactions/ Financial Loss
Distributed Denial of Service (DDoS)	↑	Telecom and Banks	Internet bandwidth	Disruption of Services
Hacktivist Attacks	↑	Citizens	Information in websites and social media	Public safety and create civil disobedience

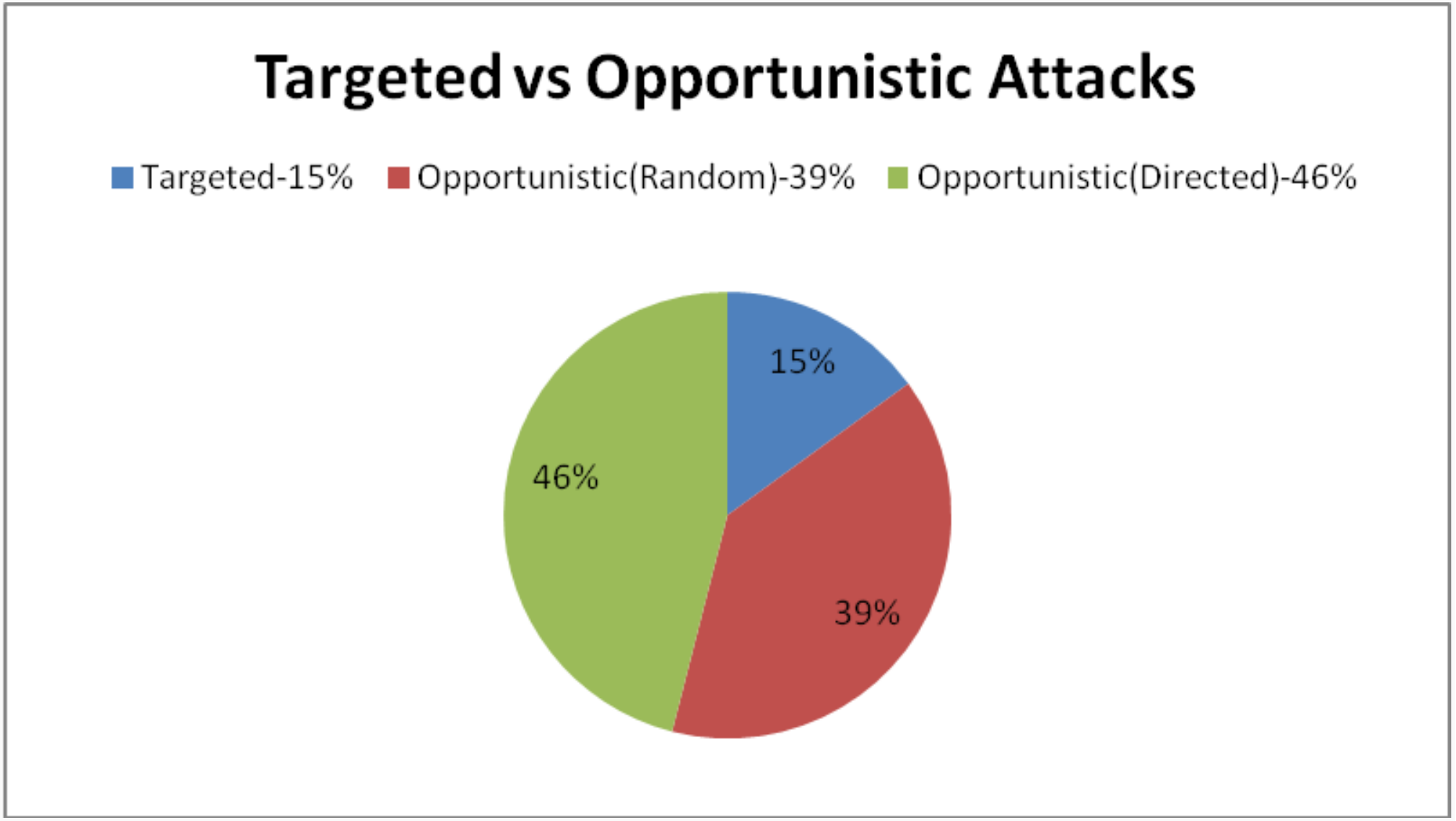
Web attacks

- Web defacement
  - Exploitation of web server vulnerabilities (IIS, Apache)
  - Exploitation of Application vulnerabilities (Joomla, PHP, ASP etc)
  - SQL Injection
  - RFI/LFI
  - Hacking of credentials (admin)
  - Web shells
- Website intrusion and malware propagation
  - SQL injection (automated) – Asprox botnet
  - Gumblar (stolen FTP credentials)
  - Toolkits –Neosploit, Phoenix, RIG etc

Blended threats

- Rise in sophisticated ransomware attacks
- Targeted scanning/probing and intrusion in network
- Lateral movement to compromise key accounts and reach critical systems
- Exfiltration of data prior to encryption
- Threat of data leakage – partial and full data leakage in specific time period

Cyber Attack - Trends



Source: Data Breach Investigation Report Verizon, 2010

Attack life cycle

Physical access: USB

Spear phishing

SMS/MMS

Drive by Download /Watering Hole

- Reconnaissance
- Company Info
- Email id
- Organisation Structure
- Tele No./ Mobile
- Social Networking

Attack

System Compromise

Gathering target profile
System Information
Connections
User Profile
User activities

Call Back

Locking of Target
- Backdoor
- RAT

Data Exfiltration

Determination of Targets

Attacker

Command & Control

Staging Server

Threat landscape and Challenges faced during Pandemic (1)

- **Business Continuity Plans (BCP)** and incident response plans are inadequate or even non-existent for dealing with pandemics
  - never anticipated or tested such plans for a situation like this.
- **Covid-19-themed attacks** in the form of malicious websites, phishing emails with malicious attachments that drop malware to steal data and credentials
- **Increased attack surface**
  - VPN, Remote Office Infra, Web meetings, Insecure personal digital devices accessing enterprise applications
- **Poor operational and monitoring controls**
  - Traditional security measures prior to COVID-19 not suitable in current scenario
  - Delays in cyber-attack detection and response due to lack of human analysts in Security Operations
- Need for keeping employees synchronized (especially those working in agile teams), such software increases the risk of hacking sensitive data
- **Increased Potential Insider Threats**
  - IT Sabotage, Intellectual Property Theft, IT Fraud, Espionage, Unintentional Insider Threat
- **Physical Security**
  - Home is new office, how to protect business data at home

Threat landscape and Challenges faced during Pandemic (2)

- Pandemic has forced everyone to conduct business in a nonstandard manner
  - Unfamiliar environment - more chance of errors – more advantage to adversaries
- Hybrid model (Office:WFH) in effect
  - 80% of IT/ITES workforce has switched to Remote/WFH
  - Most sectors have adopted to WFH, willingly or unwillingly, to varying degree
- Rapid digitization across all sectors
  - especially Health, Telemedicine, Education etc. without secure architecture
- Increased reliance on Digital Payments, Entertainment, e-Commerce activities – enhancing risk of cyber frauds
- Heightened Risk to Healthcare data / availability of IT systems
- Need for continuous availability of E-Governance and online services
- Exploitation of human weakness - Opportunistic attacks and frauds -Craving for information on pandemic conducive for Social engineering attacks
    - Coronavirus themed phishing and malware campaigns
- Misinformation campaigns

Defences & mitigation measures

- Security policies and procedures
- CSIRT/CISO/Administrator/Users
- Building Human defense
- Multi-layered defense mechanism
  - Network behavior analysis
  - Proxy logs
  - Perimeter Defense
  - Database Activity Monitoring
  - SIEM, EDR/XDR, Adv. Malware Protection, Threat Intel
- Updated/Patched applications
- Content inspection systems/DPI at perimeter, DLP
- Pre defined procedures for information sharing
- Authentication of emails/accounts (Digital signatures, MFA)
- User awareness

Actions for users

- Awareness! Awareness! Awareness!
- Install and enable :
  - Personal firewall , End point protection
- Keep up-to-date patches and fixes on the operating system and application software
- Enable/Install anti phishing toolbars such as “Phishing Filter”, “Web Forgery” etc.
- Use latest Internet Browsers having capability to detect phishing/malicious sites.
- Exercise caution while opening unsolicited emails and do not click on a link embedded within
- Only open email attachments from trusted parties
- Practice limited account privilege.
- Exercise caution while using social media and restrict info sharing
- Report suspicious emails/system activities to CERT-In

www.cert-in.org.in

Accessibility Options | Sitemap | Contact Us

certin
Enhancing Cyber Security in India

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

HOME | ABOUT CERT-In | KNOWLEDGEBASE | TRAINING | ADVISORIES | VULNERABILITY NOTES | CYBER SECURITY ASSURANCE

Sabka Saath Sabka Vikas Sabka Vishwas Sabka Prayas

Digital India
Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Innovation Challenge on Cyber Security NEW

Full Member FIRST

Full Member APCERT

Global Research Partner APWG

ABOUT CERT-In
- Client's /Citizen's Charter
- Roles & Functions
- Advisory Committee
- Act/Rules/Regulations
- Press
- Tender NEW
- Subscribe Mailing List
- Contact Us

REPORTING
- Incident Reporting
- Vulnerability Reporting
- Feedback

KNOWLEDGEBASE
- Guidelines
- Presentations
- White Papers
- Annual Report

Security Tips for Common Users NEW

ADVISORIES

VULNERABILITY NOTES

RELATED LINKS
- World CERTs
- Antivirus Resources
- FAQ

Welcome to CERT-In

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection,analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices,procedures, prevention,response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed

Latest Security Alert

CERT-In Vulnerability Note CIVN-2021-0346 NEW
(December 10, 2021)
Directory Traversal Vulnerability in Grafana Products

CERT-In Vulnerability Note CIVN-2021-0345 NEW
(December 10, 2021)
Multiple Vulnerabilities in Google chrome

CERT-In Vulnerability Note CIVN-2021-0344 NEW
(December 09, 2021)
Multiple Vulnerabilities in Android OS

CERT-In Advisory CIAD-2021-0046 NEW
(December 10, 2021)
Remote Code Execution Vulnerability in Apache Java logging library Log4j

CERT-In Advisory CIAD-2021-0045 NEW
(December 08, 2021)
Improving Outcome of Cyber Security Audits and Reducing Threat Exposure to Cyber Infrastructure - Advisory for Auditee Organizations

CERT-In Advisory CIAD-2021-0044
(November 10, 2021)
Multiple vulnerabilities in Microsoft product

Current Activities

Drinik Android malware targeting Indian banking users, masquerades as Income Tax refund NEW
(September 21, 2021)
It has been observed that Indian banking customers are being targeted by a new type of mobile banking campaign using Drinik android malware.
[More >>]

Activities related to OnePercent Group Ransomware attacking enterprises through IceID banking Trojan
(September 01, 2021)
It has been reported that a ransomware operator dubbed as OnePercent group has been attacking enterprise networks using the Cobalt Strike post-exploit toolkit and remote
[More >>]

Phishing websites hosted on NGROK platform, targeting Indian banking customers
(August 10, 2021)
It has been observed that Indian banking customers are being targeted by a new type of phishing attack using ngrok platform. The malicious actors have abused the ngrok platform
[More >>]

MORE

CYBER SECURITY AWARENESS MONTH (Do Your Part, #BeCyberSmart)

As part of services of CERT-In, for creation of awareness in the area of cyber security as well as training / upgrading the technical knowhow of various stakeholders, CERT-In is observing Cyber Security Awareness Month during October 2021 by organising various events and activities for citizens as well as the technical cyber community in India.

UPCOMING EVENTS

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)

- Aim is to notify, enable cleaning and securing systems of end users to prevent malware infections
- Launched on 21 February 2017, is a collaborative effort between CERT-In, MeitY, academia, internet service providers and the industry
- 594 organisations including 127 ISPs participating
- Number of downloads of free bot removal tools by users 1.6 million as on October 2021
- Free tools for securing desktop and mobiles provided on website for citizens

https://www.cyberswachhtakendra.gov.in

How we can help and collaborate

- Alerts and advisories on website
- Cyber Threat Intel Exchange Platform
- Cyber Swachhta Kendra (Botnet Cleaning & Malware Analysis Centre)
- Cyber security audits (empanelled auditors)
- Exercises and Drills
- Situational Awareness project

Resources and references

https://www.cert-in.org.in

https://www.csk.gov.in

https://www.infosecawareness.in/home/index.php

https://owasp.org/

https://isc.sans.edu/

https://www.meity.gov.in/content/cyber-laws

Thank you

Incident Response Help Desk

Phone: 1800 11 4949

FAX: 1800 11 6969

e-mail: incident *at* cert-in.org.in,

https://www.cert-in.org.in