Targeted attacks, malware, Vulnerability - Trends

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

Outline

- About CERT-In
- Incident trends
- Targeted attack trends
- Mitigation actions

CERT-In

Section 70B, Information Technology Act 2000: Designates CERT-In as the National nodal agency 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

Cyber threats

National level

- Cyber Terrorism
- Attacks on Critical Infrastructure
- Web defacement
- Website intrusion and malware propagation
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- Cyber espionage

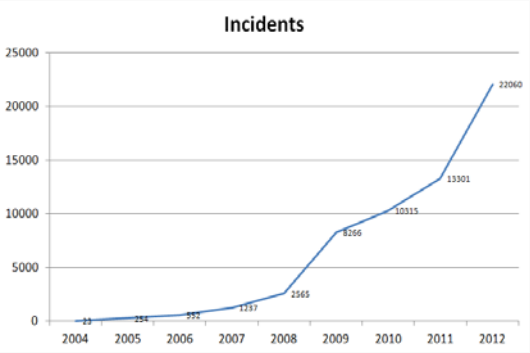
Organisational level

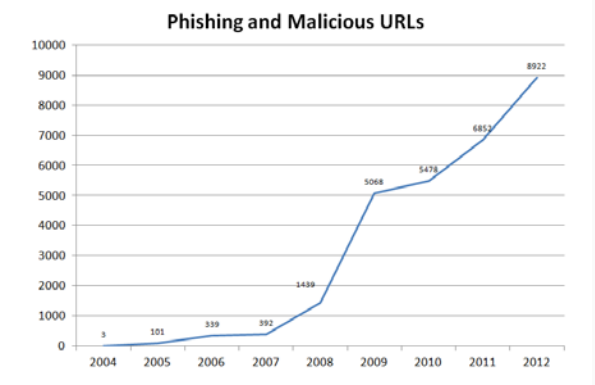
- Website intrusion/ defacement
- Domain stalking
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- Targeted attacks
- Phishing
- Data theft
- Insider threats
- Financial frauds

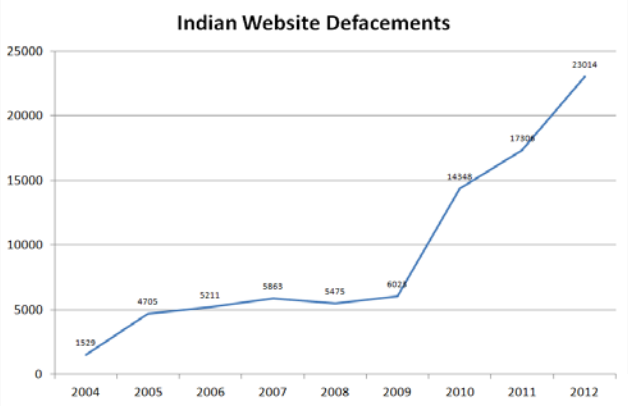
Individual level

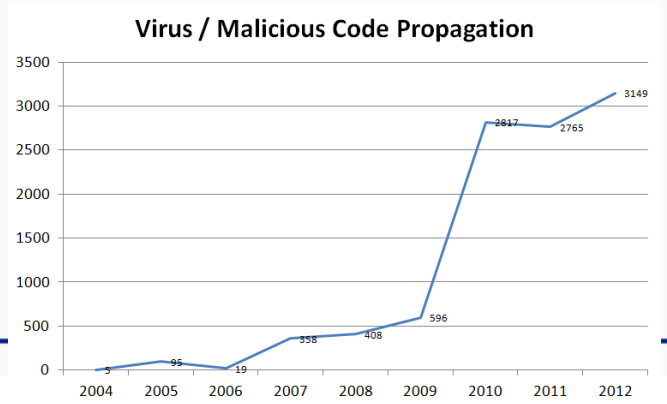
- Social Engineering
- Email hacking & misuse
- Identity theft & phishing
- Financial scams
- Abuse through emails
- Abuse through Social Networking sites
- Laptop theft

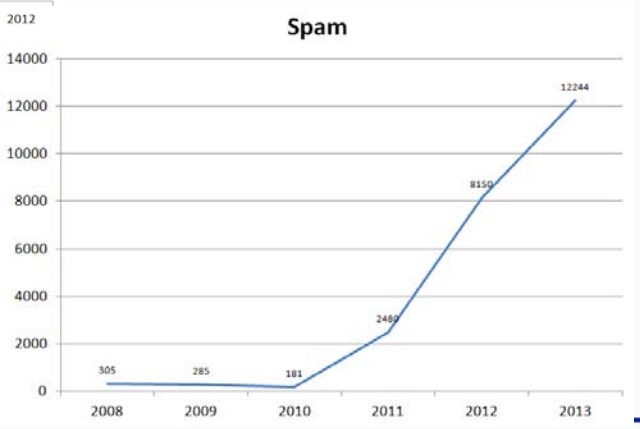
Threat Trends











Malware threats

- Stuxnet, Duqu, Flame, Gauss, MiniDuke ….
- Rimecud (Mariposa)
- Conficker
- Zbot (ZeuS)
- ZITMO
- Geinimi
- Pushdo
- Cutwail
- Bohu
- Zero-Access
- Koobface…

Advance Persistent Threat

- Usually refers to a group, with both the capability and the intent to persistently and effectively target a specific entity
- Advanced – Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques. Combine multiple attack methodologies and tools in order to reach and compromise their target
- Persistent – Operators give priority to a specific task, rather than opportunistically seeking immediate financial gain
- Threat - there is a level of coordinated human involvement in the attack

Targeted attacks - vectors

- Spear phishing – emails
- Malicious office/pdf documents
- Pre-malware loaded USB (pen) drives
- Malicious websites hosted by exploit kits
- Watering hole
- Social networking

Vulnerabilities exploited

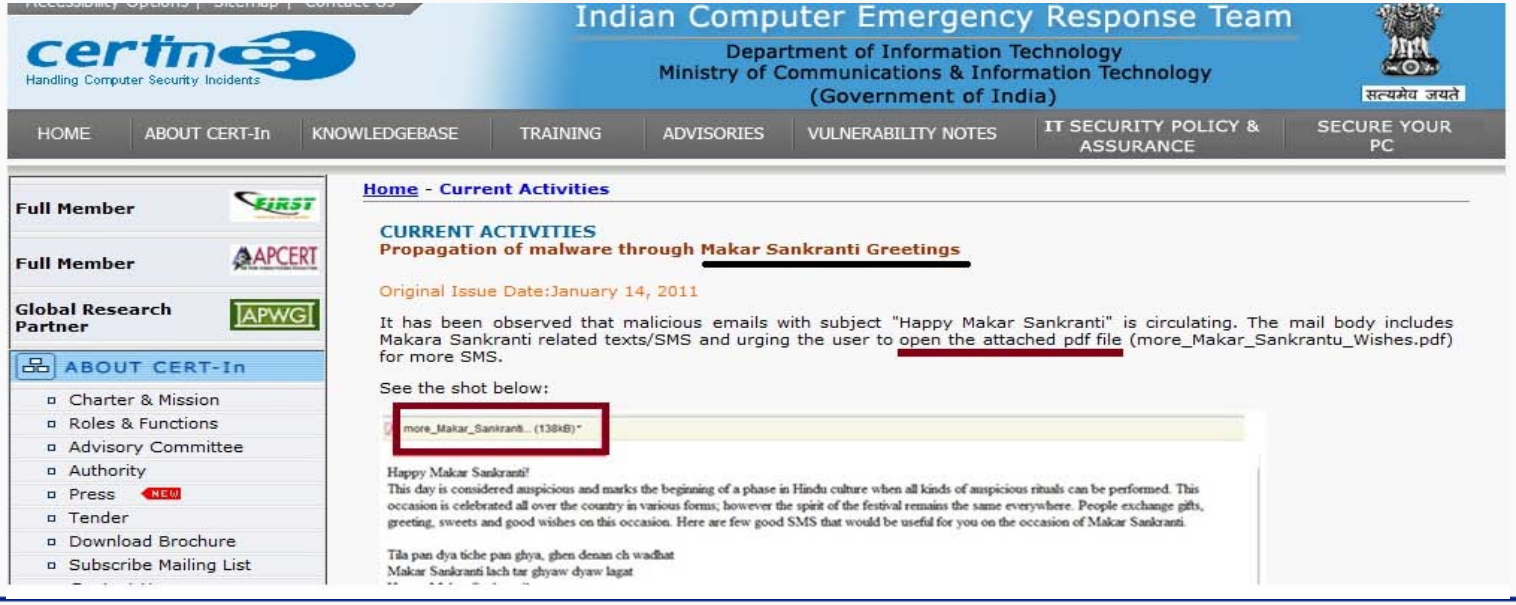
- CVE-2014-1776- Remote Code Execution Vulnerability in Internet Explorer 9 to 11-
- CVE-2013-3906- A graphics vulnerability exploited through Word documents
- CVE-2014-1761- Remote code Execution- Microsoft word RTF vulnerability
- CVE-2013-3918- (Internet Explorer 7 and 8)Remote code execution vulnerability of a legacy ActiveX component used by Internet Explorer
- CVE-2014-0322- Microsoft Internet Explorer 10
- CVE-2013-0640, CVE-2013-0641: PDF vulnerabilities
- CVE-2009-4324 -Doc.media.newPlayer()in Multimedia.api
- CVE-2010-3333- Microsoft Office RTF File Stack Buffer Overflow Vulnerability
- CVE-2012-0158 -Microsoft Windows MSCOMCTL.OCX ActiveX control
- CVE-2011-0611- Adobe flash player code execution vul
- CVE-2010-0188 -Adobe Acrobat and Reader PDF LibTiff Integer Overflow Vulnerability
- CVE-2010-2883-Adobe Reader SING Table Parsing Vulnerability

Malware via pdf.. Latest context

Subject: **Japan nuclear progress as toll up**
To:
Date: 03/22/11 07:48 AM
From:

Fukushima_updats_and... (283kB)

The United Nations nuclear agency (IAEA) says there have been positive developments in Japan's efforts to tackle a nuclear emergency after the 11 March quake.
But it said the overall situation remained very serious.
The overall death toll has now risen to 8,450, with 12,931 people missing.
Electricity has been restored to three reactors at the crippled Fukushima nuclear power plant - this should allow the use of on-site water pumps soon.
Engineers have been spraying fuel rods with salt water to try to cool them enough to avert radiation leakage.
"We consider that now we have come to a situation where we are very close to getting the situation under control," Deputy Cabinet Secretary Tetsuro Fukuyama said.
What situation Japan has come to? What infulence the contamination will make to Japan and futhermore the whole world? Here we also provide an attached file to elaborate to specifics.Please kindly check it on behalf of you and your br-loved ones.Thanks.



Exploit set – phoenix kit

- Flash exploits
  - Adobe Flash Integer Overflow in AVM2 - CVE-2009-1869
  - Adobe Flash Integer Overflow in Flash Player CVE-2007-0071
- PDF exploits
  - Adobe Reader CollectEmailInfo Vulnerability CVE-2007-5659
  - Adobe Reader Collab GetIcon Vulnerability CVE-2009-0927
  - Adobe Reader LibTiff Vulnerability CVE-2010-0188
  - Adobe Reader newPlayer Vulnerability CVE-2009-4324
  - Adobe Reader util.printf Vulnerability CVE-2008-2992
- Internet Explorer Exploits
  - IE MDAC Vulnerability CVE-2006-0003
  - IE SnapShot Viewer ActiveX Vulnerability CVE-2008-2463
  - IE iepeers Vulnerability CVE-2010-0806
- Java Exploits
  - JAVA HsbParser.getSoundBank Vulnerability CVE-2009-3867
  - Java Development Kit Vulnerability CVE-2008-5353

Source: m86security.com

Watering hole

- Identify target
- Determine browsing habits
- Select favorite website
- Compromise and host exploits
- Drop malware
- Determine target profile
- Further compromise

Defences & mitigating factors

- Security policies and procedures
- CSIRT/CISO/Administrator/Users
- Building Human defense
- Multi-layered defense mechanism
  - Network behavior analysis
  - Proxy logs
  - Perimeter Defense
  - Security Information and Event Management
  - Database Activity Monitoring
- Updated/Patched applications
- Host based Intrusion Prevention System
- Content inspection systems/DPI at perimeter, DLP
- Pre defined procedures for information sharing
- Authentication of emails (Digital signatures)
- User awareness

Actions for users

- Awareness! Awareness! Awareness!
- Install and enable :
  - Personal firewall
  - Anti-spyware
  - Anti-phishing controls and HIPS
- 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.
- Report suspicious emails/system activities to CERT-In

www.cert-in.org.in

Accessibility Options | Sitemap | Contact Us

Indian Computer Emergency Response Team

Handling Computer Security Incidents

Department of Electronics and Information Technology
Ministry of Communications & Information Technology
Government of India

सत्यमेव जयते

HOME | ABOUT CERT-In | KNOWLEDGEBASE | TRAINING | ADVISORIES | VULNERABILITY NOTES | IT SECURITY POLICY & ASSURANCE | SECURE YOUR PC

Full Member FIRST

Full Member APCERT

Global Research Partner APWG

ABOUT CERT-In

- Charter & Mission
- Roles & Functions
- Advisory Committee
- Authority
- Press
- Tender NEW
- Download Brochure
- Subscribe Mailing List
- Contact Us

REPORTING

- Incident Reporting
- Vulnerability Reporting
- Feedback

KNOWLEDGEBASE

- Guidelines
- Presentations
- White Papers
- Monthly Security Bulletin
- Annual Report

Security Tips for Common Users NEW

ADVISORIES

VULNERABILITY NOTES

RELATED LINKS

- World CERTs
- Security Sites
- Security Tools

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 recent 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-2014-0172 NEW
(July 22, 2014)
Multiple Vulnerabilities in WordPress Plugins

CERT-In Vulnerability Note CIVN-2014-0171
(July 22, 2014)
Cisco Wireless Residential Gateway Remote Code Execution Vulnerability

CERT-In Vulnerability Note CIVN-2014-0170
(July 21, 2014)
Multiple Vulnerabilities in WordPress Plugins

CERT-In Advisory CIAD-2014-0047 NEW
(July 25, 2014)
Multiple Vulnerabilities in Mozilla products

CERT-In Advisory CIAD-2014-0046
(July 22, 2014)
Multiple Vulnerabilities in Oracle Products

CERT-In Advisory CIAD-2014-0045
(July 18, 2014)
Multiple Vulnerabilities in Red Hat JBoss Enterprise Application Platform

Current Activities

Havex Malware targeting ICS/SCADA control systems NEW
(July 02, 2014)
It has been reported that an industrial information stealing malware, dubbed Havex, is targeting ICS based systems by leveraging OPC protocol implementation. OPC is OLE for [More >>]

Gameover aka Zeus-P2P malware surge
(March 11, 2014) (Update : June 03, 2014)
It has been reported that "GameOver" malware aka Zeus-P2P is surging with new tactics techniques and procedures (TTP). GameOver malware is the incarnation of the [More >>]

Attacks through SSHD root kit targeting Linux Systems
(March 11, 2013)
It has been reported that a USER-mode root kit is in the wild targeting major Linux flavors (majorly RPM based) which logs user names and password pairs that are sent to the [More >>]

MORE

Thank you

Incident Response HelpDesk

Phone: 1800 11 4949

FAX: 1800 11 6969

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

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