Jan -Feb 2012

www.infosecawareness.in

Information Security Awareness

Program by
Information Security Education and Awareness (ISEA)
Department of Information Technology
Ministry of Communications and Information Technology
Government of India

Tips to Secure your PC from Malicious Software

- Always update your anti-virus software with the latest patches from the recommended vendor services.
- Scan the system with anti-virus software regularly to avoid virus, worms, and Trojan attacks.
- Take a backup of your important data or information periodically. If your system gets infected with virus, it can lead to deletion or modification of your files.
- Also use anti-spyware, anti-malware, and anti-adware tools to scan or filter your system for malwares/spywares/adware attacks.

InfoSec Tip

Take immediate action if you feel that your computer is infected with virus to avoid automatic generation. To start with,

- *Remove the network connection*
- *Install anti-virus software in your sytem and scan it.*
- *Restart the the system with network connections and update the antivirus. Thereafter once again scan the system.*

InfoSec Quote

Securing a computer system has traditionally been a battle of wits: the penetrator tries to find the holes, and the designer tries to close them. —

Gosser

InfoSec Cartoon

Never share personal details like phone number, address or photographs, etc. with a stranger met through Internet

For Virus Alerts,Incident and Vulnerability Reporting
certin
Handling Computer Security Incidents

Executed by :
Centre for Development of Advanced Computing
Hyderabad

InfoSec Quiz

1) Creating a situation where in a third party gains confidential information from you and that is called

a) Social Engineering b) Phishing c) Social Networkng d) None

2) _____is an attempt to make a computer unavailable to its intended users

a) Denial of Service b) Skimming c) Clickjacking d) Vishing

3) _____ are a small windowpane that opens automatically on your browser.

a) Cookies b) website c) Pop-ups d) None

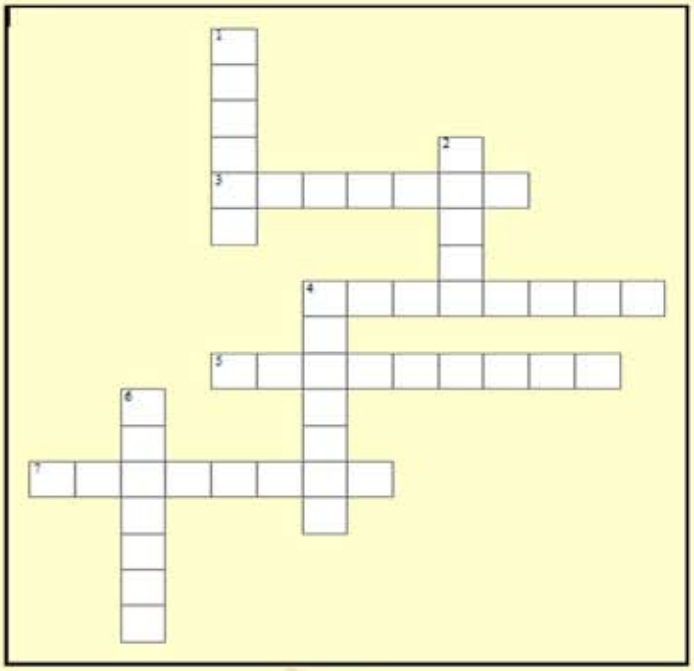
4) _____is a non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.

a) Virus b) Spyware c) Trojan d) None

5) When someone, without your knowledge, acquires a piece of your personal information and uses it to commit fraud. It is called

a) Identity theft b) Bluejacking c) Tabnapping d) All the above

InfoSec Crossword



ACROSS

3. _____an action or event that might compromise security

4. A criminal activity used to collect the information by sending the messages to mobile phone is known as

5. ____ is a program that runs in the background and allows to record every keystroke

7. It acts as a barrier between user and application or system

DOWN

1. Hoaxes are false alarms claiming reports about non-existing virus which may contain virus attachments

2. A virus is a self replicating program that produces its own code by attaching copies of itself into other executable codes

4.The software used to send the user activities and personal information to its creator

6. A criminal practise or act done through telephone

logon to www.infosecawareness.in to participate in the Infosec contest

InfoSec Tools

ROOTKIT BUSTER

Malicious software called rootkits can manipulate the components of the Microsoft Windows operating system to conceal how they harm you.Rootkits can hide drivers, processes, and registry entries from tools that use common system application programming interfaces (APIs).

Trend Micro RootkitBuster scans hidden files, registry entries, processes, drivers, services, ports, and the master boot record (MBR) to identify and remove rootkits.

Features

- Easier interface
- Checks the integrity of the device driver stack
- Can remove rootkits using the "Cleanboot" feature
- Capable of downloading Cleanboot components and pattern files
- Detects and removes more rootkits

source:
http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=result_page&clkval=drop_list&catid=6&prodid=155

BROWSER GUARD

Browser Guard is an easy to use browser plug-in, which prevents known and unknown web threats. Zero-day attacks such as Aurora and Hydraq can be proactively blocked by Browser Guard, which detects and prevents behavior associated with these types of threats.

Cybercriminals often use malicious JavaScript inserted into web pages, where attacks can take place silently, without any visible effect. Browser Guard also protects you from such attacks by analyzing and subsequently blocking malicious JavaScript. For the most advanced and efficient detection, Browser Guard communicates with the Trend Micro Smart Protection Network, bringing you the latest protection when you surf the web.

Key benefits

- Protects against zero day exploits
- Detects buffer-overflow and heap-spray attacks
- Protects against execution of shell code
- Analyzes and protects against malicious JavaScript
- Connects with Trend Micro Smart Protection Network to maximize detections

Source:
http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=355&regs=NABU&lang_loc=1#undefined

InfoSec Concept

SOCIAL NETWORKING RISKS AND CHALLENGES

Social networking has become common in today's Internet world. Billions of people across the world are using it to meet old friends, new Internet users, making new friends, to gather and share information and many other commercial uses . Though there are several advantages of social networking but at the same time there are several disadvantages like based on these communication tools, sites can be trapped by scammers or any hackers leading to loss of privacy and identity theft.

These social networking sites are very popular with all age groups especially the growing kids. They expose these kids to various risks like online bullying, disclosure of private information, cyber-stalking, access to age-inappropriate content , online grooming and child abuse, etc.

SOCIAL NETWORKING RISKS

Spam

Spam is one of the most classic attacks of all time with social networks continuing to add millions of users to their overall user base, crafty spammers are taking advantage of the popularity of these networks to design new spamming techniques week after week. Since nearly all of those services allow users to send messages to each other for free, it provides an easy entry point for spammers.

Scams

Some websites offer free services where you have to hand over your account name and password and they will in turn ensure that you acquire many new followers per day. Obviously it is a bad idea to share your password with strangers, since you cannot control what will be done with your account. In most cases it is also against the terms and conditions of the social networking sites. Most of these services will simply take the account and start using it to send unrelated spam messages to all the connected friends, which is surely not what the user wanted.

Phishing

Just like with phishing attacks on banks, social networking phishing comes in many different flavours. We have seen the traditional spoofed emails claiming to be from the social network service offering some update or contest. In order to see the update the user needs to follow a link and log in, thus handing over his credentials to the attacker. The linked page is a fake copy of the original login page, focused on stealing user account credentials.

Clickjacking

Clickjacking and click fraud is not a new phenomena, but get a new twist when applied to social networks. The principle behind these attacks is that users can be tricked into clicking on things that they do not see or are aware off.

For more details visit http://infosecawareness.in/clickjacking

Malicious applications

Clicking on the Social networking application(e.g. Facebook) starts the application installation process. In order to fulfil its shady business the application requests some elevated privileges from the user.

InfoSec Concept

Some more Malicious Applications

- Facebook worm spread via photo album .
- Stegobot steals passwords from your Facebook photos.
- Facebook tracks what you do online even when you're logged out.
- Bom Sabado is an orkut virus affecting profiles of many. Those who are affected by this virus are advised to change password and security question. Log out immediately and also clear the cookies and history.

Tips to avoid risks by social networking

- *Be careful about the information you put online, like if you put your photo or video or your account details will stay for a long time and who ever connected will see it. Hackers will use these sites to collect the personal information and may misuse them so be careful.*
- *Remember don't put personal information like your family details, addresses, personal photographs, video, etc. Most of the sites and services provide options for privacy settings to prevent attackers to view your information. You can make use of these options to choose/deny whom you want to allow to see your information.*
- *Be careful if you want to meet social networking friends in person, as some times it may not be their true identity which is posted. Always think before you meet such strangers. If you decide to meet then do it in a public place during the day. Kids should never be allowed to meet such strangers alone.*
- *Don't ever click suspicious link while logged into social networking accounts. If you are curious you can manually enter/key-in the URL in to the browser to view it and after that always clean it's browser's cookie and cache.*
- *Install a good and latest version of Anti virus and Anti Key logger to keep your system free from Key loggers and backdoor trojans.*
- *Don't ever run any javascripts while logged into your social networking accounts.*
- *Don't ever share your password with anyone else and keep changing your password regularly. Always use proper password (min 8 digit with a mix of alpha numeric & special characters).*
- *Don't ever login to any site other than the legitimate sites and always check the URL before you proceed further.*
- *Use Virtual Keyboard, wherever possible. to enter your password for better security as these cannot be captured by key-loggers*

InfoSec News

Techie arrested in railway e-ticket fraud


Techie arrested in railway e-ticket fraud

MUMBAI: A software consultant from Varanasi who developed pirated software and sold it to railway touts who in turn hacked into the Indian Railway Catering and Tourism Corporation's (IRCTC) website and booked e-tickets before the online windows opened and sold them in black market was arrested by the Mumbai cyber cell police on Tuesday.

The accused, Sunil Sharma (34), a software consultant from Banaras in Varan was detained by the cyber cell police and will be brought to Mumbai. Police said Sharma will be booked for cheating, forgery, and breach of trust as well as under various sections of the Information Technology (IT) act.

Earlier in June, the cyber cell police had arrested Suraj Yadav and Kalpesh Shah, both 19 years of age, who are Mumbai based touts and who used.

A software consultant from Varanasi who developed pirated software and sold it to railway touts who in turn hacked into the IRCTC website and booked e-tickets before the online windows opened and sold them in black market

A software consultant from Varanasi who developed pirated software and sold it to railway touts who in turn hacked into the Indian Railway Catering and Tourism Corporation's (IRCTC) website and booked e-tickets before the online windows opened and sold them in black market was arrested by the Mumbai cyber cell police on Tuesday. The accused, Sunil Sharma (34), be booked for cheating, forgery, and breach of trust as well as under various sections of the Information Technology (IT) act. A 21 year old man received a 14 year prison sentenced on Friday for running an online business that sold counterfeit credit cards encoded with stolen account information with losses estimated at more than $3 million.

Source:
http://timesofindia.indiatimes.com/city/mumbai/Techie-arres ed-in-railway-e-ticket-fraud/articleshow/10059745.cms

Facebook scare: 2 lakh accounts hacked in Bangalore

The recent Facebook hack has reportedly claimed over 2 lakh victims in Bangalore. According to a news report , some two lakh Facebook users in Bangalore had their accounts hacked and weblinks to their morphed pornographic pictures sent as feeds to friends and family.

Quoting social networking analysts, the report says that more than 2 lakh Bangalore Facebook accounts were hacked. The cybercrime department too is reported to have received calls and complaints regarding the mass hacking.

According to the report, there are around 50 posts on Facebook stating that the users are quitting the social networking site forever after being embarrassed before friends and family. Incidentally, according to a Bloomberg report, Facebook claimed that it has identified those responsible for the deluge of hardcore porn and violent images in some users' newsfeeds, and said it is working with its legal team "to ensure appropriate consequences follow."

Facebook said that it has "drastically limited the damage caused" by a spam attack that took advantage of a browser vulnerability. "Protecting the people who use Facebook from spam and malicious content is a top priority for us," Palo Alto, California-based Facebook said in a statement.Users were tricked into pasting malware into their browsers, which in turn resulted in the sharing of offensive content.

Cybercrime now third biggest business crime issue says PwC survey

Cybercrime is now the third biggest crime problem experienced by UK businesses behind only asset theft and accounting fraud, the PricewaterhouseCoopers (PwC) Global Economic Crime Survey has found.

Nearly half of the 178 middle and senior managers in private and public sectors said that cybercrime (defined as loss of IP, malware incidents and industrial espionage) had increased in the last year, with a quarter reporting more than 10 incidents.

The main cybercrime worry in the UK was reputational damage which belies the fact that only 57 percent reported having a media or PR plan in place to respond to data loss incidents.

source:
http://articles.timesofindia.indiatimes.com/2011-11-16/social-media/30405151_1_facebook-users-offensivecontent-spam
http://www.computerworlduk.com/news/security/3321715/cybercrime-now-third-biggest-business-crime-pwc-survey-finds/

InfoSec News

Google Chrome Multiple Flaws Let Remote Users Execute Arbitrary Code

Systems Affected

Google Chrome versions prior to 15.0.874.121

Overview

A vulnerability have been reported in the Google Chrome,which could be exploited by remote attackers to cause a denail of service condition or to execute arbitrary code to take control of the affected system.

Description

This vulnerability occurs due to an out-of-bounds write error in the v8 engine in google Chrome, which could be exploited by a remote attacker, via a specially crafter HTML file.
Successful exploitation of this vulnerability could allow a remote attacker to cause Denial of Service condition or execute arbitrary code to take control of the target system.

Solution

upgrade to Google Chrome version 15.0.874.121

For more details :

www.cert-in.org.in

http://googlechromereleases.blogspot.com/2011/11/stable-channel-update.html

http://securitytracker.com/id/1026313

Guess the tip which suits the cartoon picture and win prizes

logon on to
www.infosecawareness.in
to send the tip

InfoSec Virus Alerts

Stegobot steals passwords from your Facebook photos

THINK twice before uploading your holiday pictures to Facebook - you could be helping someone to steal information from your computer. A botnet called Stegobot was created to show how easy it would be for a crook to hijack Facebook photos to create a secret communication channel that is very difficult to detect.

Like most botnets, Stegobot gains control of computers by tricking users into opening infected email attachments or visiting suspect websites. But rather than contacting the botmasters directly, it piggybacks on the infected user's normal social network activity. "If one of your friends is a friend of a friend of the botmaster, the information transfers hop by hop within the social network, finally reaching the botmasters,"

Stegobot takes advantage of a technique called steganography to hide information in picture files without changing their appearance. It is possible to store around 50 kilobytes of data in a 720 by 720 pixel image - enough to transmit any passwords or credit card numbers that Stegobot might find on your hard drive.

The botnet inserts this information into any photo you upload to Facebook, and then waits for one of your friends to look at your profile. They don't even have to click on the photo, as Facebook helpfully downloads files in the background. If your friend is also infected with the botnet - quite likely, since any email you send them will pass it on - any photo they upload will also pass on the stolen data.

Source:

http://infosecawareness.in/wiki/index.php/Stegobot_steals_passwords_from_your_Facebook_photos

Fake Flash Player installer for MAC OSX

A new attack against Apple Mac OS X Lion (10.7) has been detected by Intego. The threat is a trojan, dubbed Flashback, installed via a fake Adobe Flash installer downloaded from a third party site.

As with the MacDefender and Revir malware the Flashback attack uses social engineering to entice the user to download then install the malware. The malware is hosted on a site that prompts the user to install Flash in order to view content. The user must elect to install the "Flash" software, then walk through a complete standard installation process for the malware to function. The malware presents a standard and professional looking installer screen to create a backdoor via a dynamic library called Preferences.dylib. Once installed, Intego indicates that the malware uses RC4 encryption for communications to a remote server, and transmits data such as the users MAC address, OS version, UUID, and more. The malware can also potentially be used to allow the malware author to inject code into the target Mac.

Flashback can not install by itself without user intervention and as of this writing the distribution is extremely small, so the threat posed by the malware is very low.

Safety tips:

While this particular malware is not a major threat, it is a reminder that users should follow the best practices of:

1. Only downloading Adobe Flash and Acrobat software from Adobe.com
2. Disable "Open "Safe" files after downloading" from the Safari preferences
3. Run antivirus or internet security software

source: cert-in.org.in

for more details: http://blog.eset.com/2011/09/27/new-apple-os-x-malware-fake-adobe-flash-installer

InfoSec Virus Alerts

Malware Win32 "DUQU"

It has been reported that a new malware called"Duqu" which is based on Stuxnet cose is in the wild.It is used as a reconnaissance tool and as an advanced Remote Access Trojan(RAT) rather than targeting any industrial SCADA PLC'S. One of the driver file has been signed with a stolen certificate belonging to a taiwanese company called C-Media electronics Incorporation.
The threat installs a information stealer capable of sniffing various information from the victime system such as lists of running processes, account details and domain information, Drive names and other information, including those of shared drives, Security Responses, Screenshots,Network information(interfaces, routing tables, shares list etc) key presses, open window names,enumerated shares,file exploration on all drives,including removable drives.

Countermeasures

- Apply appropriate workarounds as mentioned in Microsoft Advisory and CERT-In vulnerability Note.
- Install and maintain updated anti-virus software at gateway and desktop level.
- Keep up-to-date on patches and fixes on the operating system.
- Install and maintain Desktop Firewall and block the ports which are not required.
- Exercise caution while visiting trusted /untrusted sites.
- Disable active Scripting through Browsers while visiting untrusted websites.
- Do not open the documents received as attachments through unsolicited and suspicious emails.
- Use the Microsoft office Isolated Conversion Environment (MOICE) when opening files from unknown or untrusted sources .

source : www.cert-in.org.in

Malware exploiting JBOSS application server vulnerability

A worm is making the round infecting JBoss application servers. JBoss is an open source Java based application server and it is currently maintained by RedHat.
The worm exploits older configuration problem in JBoss, which only authenticates GET and POST requests. It was possible to use other methods to execute arbitrary code without authentication. The problem has been fixed last year, but there are apparently still a number of vulnerable installs out there.

Both the jmx-console and web-console are standard servlet 2.3 deployments that can be secured using J2EE role-based security. Both consoles ship with a skeleton configuration, allowing an administrator to easily enable security using username/password/role mappings found in the jmx-console.war and web-console.war deployments in the corresponding WEB-INF/classes, users.properties and roles.properties files.
The security setup is based on two pieces: the standard servlet URI to role specification, and the specification of the JAAS configuration which defines how authentication and role mapping is performed.
In AS 6 M3 and greater deployments, the JSR-160 JMXConnector is opened for remote access and should also be secured.

Source:
www.cert-in.org.in
http://community.jboss.org/blogs/mjc/2011/10/20/statement-regarding-security-threat-to-jboss-application-server
https://threatpost.com/en_us/blogs/jboss-worm-exploiting-old-bug-infect-unpatched-servers-102111
http://isc.sans.org/diary/JBoss+Worm/11860

InfoSec Workshops

STUDENTS

Participants Comments

Presentation was really good. It awakened us from the sleep in which we were. Such PPTs if given at early stages will definitely reduce cyber crimes

Neha
Student

@Bangalore

STUDENTS

Participants Comments

Informative presentation, updated us about internet abuse by hackers and others.Nice presentation

Jestashree
Student

@Khalsa, Amritsar

Participants Comments

The slides showed us many ways as to how to play it safe on the net, we have learnt many things and sure to implement it.

Roshel Preeti
Student

@ Agartala

www.infosecawareness.in

InfoSec Workshops

EMPLOYEES

@ Goa

@ Hyderabad

TEACHERS

@ Jaipur

Users Views on the Cartoon – Guess Tip Contest

Beware of Threats and Be Aware of Prevenive Actions

-Guruvayurappan Mani
Chennai

Use anti spam, antivirus software and firewalls and take regular backup for information security.

-Prema

Always update to the latest available security measures to avoid future trouble.

-Tripteela
Goa

Protect your system from Virus, Phising and malware by installing all Antivirus, Firewal software.

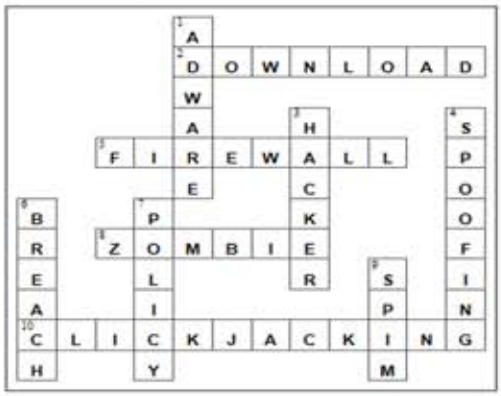
-Rema

Last edition Contest Answers and Winners

Infosec Quiz

1) a *2)* c *3)* b *4)* d *5)* c

Infosec Crossword



Infosec Quiz

1. Mukul -Gurgaon, Haryana
2. Risna Dhar - Pondicherry
3. Prashant Rao -Mumbai

Infosec Crossword

1. Eswara Rao
   -Tadipatri, Andhra Pradesh
2. Vijaya
   - Bangalore
3. Rajendra B
   -Kolkata

Interested to organize InfoSec Workshop at Your Place ?

Please visit ....

http://infosecawareness.in/isea-pi

or

mail us at isea@cdac.in

Our Sincere Thanks to Action Group Members for Guiding us

Dr. Kamlesh Bajaj, Data Security Council of India
Dr. B.K.Murthy, Director, Head of Division – HRD & NKN, DIT
Dr.Diren R Patel, Professor of Computer Science Department, IIT ,Gandhinagar
Shri Sitaram Chamarthy, Principal Consultant, TCS
Dr.N.Sarat Chandra Babu, Executive Director, CDAC Bangalore

Special Thanks:
Dr.Ponnurangam K, IIIT Delhi

Editorial Committee :
Shri.D.K .Jain,
Director
C-DAC Hyderabad
Shri G.V.Raghunathan,
Consultant, CDAC Hyderabad
Shri.S.K.Vyas,
Joint Director ,DIT
Mr.Ch.A S Murty &
Mrs.Indraveni.K ,
C-DAC Hyderabad

For Virus Alerts,Incident and Vulnerability Reporting

certin
Handling Computer Security Incidents

Comments & Feedback
mail us at isea@cdac.in

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-Learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain management and Wireless Sensor Networks.

Supported by

Department of Information Technology Government of India

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India

JNTU Campus, Kukatpally, Hyderabad - 500 085. Tel: 040-2315 0115. Fax: 040-2315 0117. Website: www.cdac.in