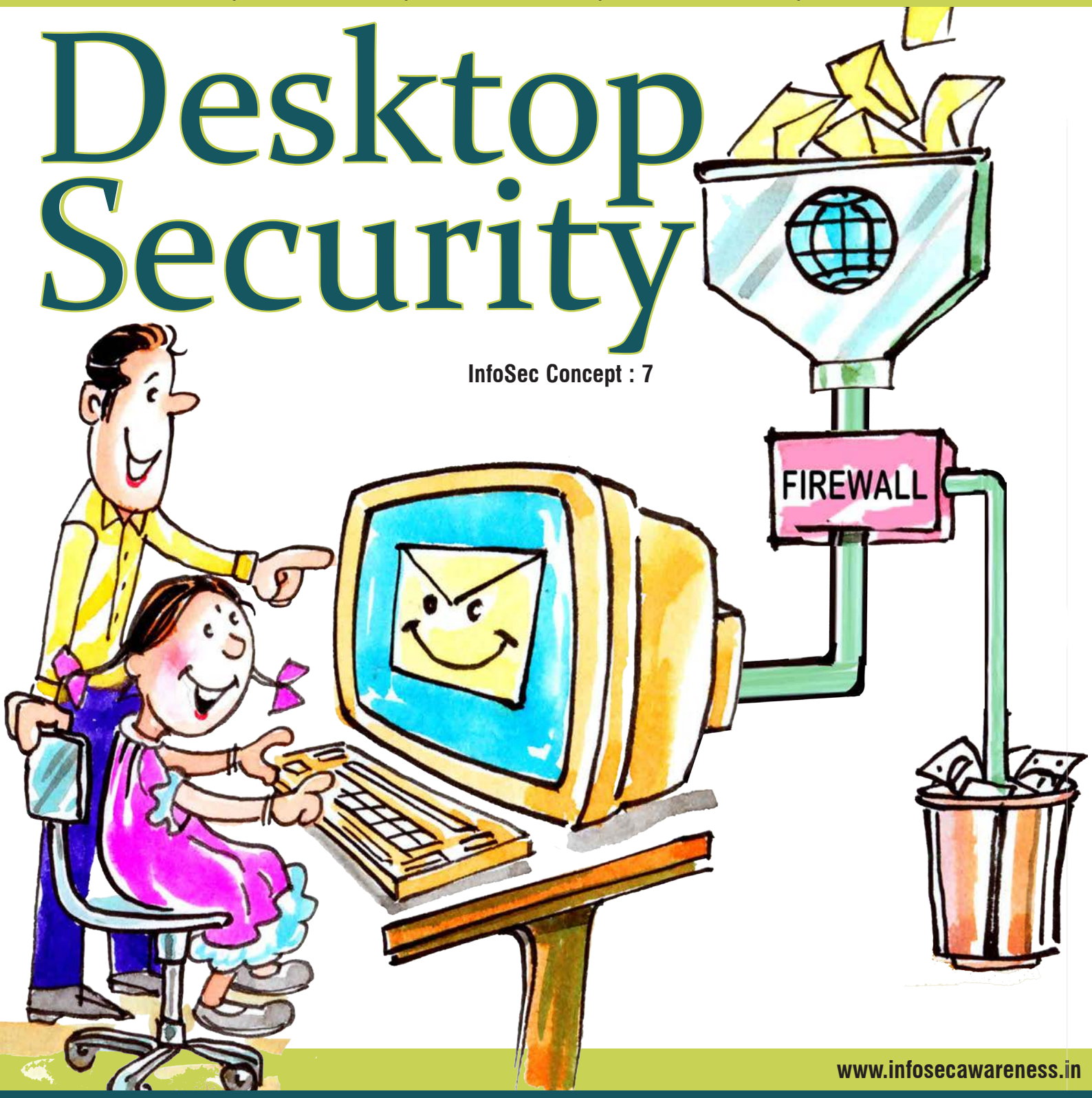
Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.

Desktop Security

InfoSec Concept : 7



www.infosecawareness.in

Supported by
For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

Executed by
सी डैक CDAC
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.

InfoSec Magazine 2013-Edition-IV

Credits

Editorial committee:

Shri.Sanjay Kumar Vyas
Joint Director, DeitY

V.Muralidharan Director
Mr.Ch.A S Murty &
Mrs.Indraveni K
Shri G.V.Raghunathan,
Consultant
C-DAC Hyderabad

Design Team
K.IndraKeerthi
S.Om Aarathi

Action Group Members

Dr.Kamlesh Bajaj
Data Security Council of India
Dr.Dhiren R Patel
Professor of Computer Engineering, NIT Surat
Shri.Sitaram Chamarthy
Principal Consultant, TCS
Dr.N. Sarat Chandra Babu
Executive Director,C-DAC Bangalore
&
HOD, HRD Division
DeitY, Government of India

Acknowledgement

HRD Division
Department of Electronics & Information Technology
Ministry of Communications and Information Technology

Comments & Feedback
mail us to
isea@cdac.in

InfoSec Quiz

1. Which one of the following characteristic is NOT associated with a computer virus?
   (a)Malicious code that infects files and can infect the bootsector
   (b)A program that replicates itself without the approval of the user
   (c)Malicious code that attaches to a host program and propagates when the infected program is executed
   (d)Malicious code that is hidden in a program that has a useful function or apparently useful function

2. A malicious computer program that is activated when a particular state of the computer occurs, such as a particular date and time, is called a
   (a)Polymorphic virus (b)Logic bomb (c)Retro virus (d)Keyed virus

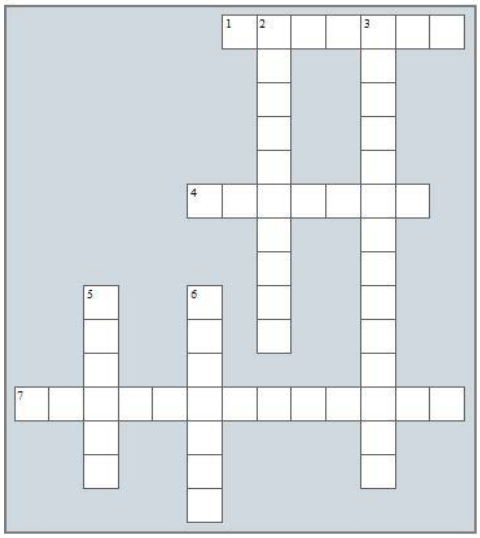
3. An individual who create or use programs to break into telephone systems & to access other computers is called a
   (a)Hacker (b)Phreaker (c)Cracker (d)Social Engineer

4. Snort is
   (a)An open-sourced audit system
   (b)An open-sourced keystroke monitoring system
   (c)A proprietary intrusion detection system
   (d)An open-sourced intrusion detection system

5. A criminal activity used to collect the information by sending the messages to mobile phone is known as
   (a)Smashing (b)Vishing (c)Smishing (d)All the above

logon to
www.infosecawareness.in/contest
to participate in Infosec Contest and WIN PRIZES

InfoSec Crossword



Down:

2. Influence someone to give you confidential information either by convincing them you are someone who can be trusted or by just asking for it.
3. A user providing a password to a system is involved with
5. A computer is called as _____ computer, which is connected to internet and controlled by hacker by inserting the malicious software and used to perform attacks
6. It is also one of the method of social engineering

Across:

1. The software used to send the user activities and personal information to its creator
4. is an attack which targets the specific high profile executives in the businesses or targeting upper management in the corporate.
7. is the use of the Internet or other electronic means to stalk someone

InfoSec Guess Tip

Guess the Tip which best suits the cartoon by logging in to http://www.infosecawareness.in

InfoSec Tip

Always beware of Spam Instant Messages in chat room

Risks through Instant Messengers

SPIM

Spim is a short form of spam over Instant Messaging(IM), it uses IM platforms to send spam messages over IM. Like e-mail spam messages, a spim message also contains advertisements. It generally contains web links, by clicking on those links malicious code enters into your PC. Generally, it happens in real time and we need to stop the work and deal with spim as the IM window pop-ups, in the e-mail we have time to delete and we can delete all spam at a time, or we can scan before opening any attachments. This cannot be done in IM. So avoid opening attachments and links in IM.

More risks through Instant Messengers :

- The most evident is that your friends can see when you are online and jump into chat, it can be frustrating if you are busy in studies or learning something over Internet.
- The voice can be trapped while talking to your friends.
- Avoid opening attachments and links in IM
- You may receive unwanted texts or spam text messages which could contain inappropriate material.
- Text messages containing private, personal information could be sent to the wrong address.
- Video chats can be used to photograph or videotape without your knowledge.
- Photos and videos can reveal a user's appearance and place.
- Criminals are able to hide their identity in Instant messages through a false name, age and some grown up can pretend to be child.
- Some times strangers may offer free gifts through instant message with false information.

For more details visit
www.infosecawareness.in

Malware Bytes

Crushes malware
Restores confidence
Because your antivirus alone is not enough

Malwarebytes is certified by Westcoast Labs for antivirus, anti-spyware, anti-trojan.

Malwarebytes Anti-Malware Free

Malwarebytes Anti-Malware Free utilizes Malwarebytes powerful technology to detect and remove all traces of malware including worms, trojans, rootkits, rogues, dialers, spyware and more.

Features:

- Real-Time Active Malware Prevention Engine Blocks Known Threats.
- Heuristic Protection Prevents New Zero Day Malware Infections.
- Malicious Website Protection Blocks Access to Known and Zero Day Malicious Web Content.
- Automatic Priority Updates and Scheduled Scanning .
- Blazing Fast Flash Scans.
- Advanced Malware Detection and Removal.
- Industry Proven Clean-up Technologies Eradicate Existing Malware Infections.
- Rapid Response Malware Database and Heuristics Updates.
- Access to our Expert Community and Knowledgeable Support Team (Email/ Forums)
- Chameleon Technology Gets Malwarebytes Running on Infected Systems

Malwarebytes Anti-Malware Pro

Detect and Protect with Byte:
Malware is big and malware is bad. Your computer is constantly at risk from infection by malware including viruses, worms, trojans, rootkits, dialers and spyware. Malwarebytes specializes in fighting malware.

If viruses are mischief, malware is mayhem. Malware doesn't just want to disrupt your network, it wants your keystrokes, logins, passwords, address book, data, credit card information, favorite t-shirt and possibly your cat.

Malware is not going away any time soon. Malware is growing, developing, constantly evolving. Malware is becoming more difficult to detect, and even harder to remove.

Only the most sophisticated anti-malware techniques can detect and remove malicious programs from your computer. Malwarebytes Anti-Malware PRO combines powerful new technologies designed to seek out, destroy, and prevent malware.

Features include:

- Flash - Lightning fast scan speeds
- Thorough - Full scans for all drives
- Works Well With Others - Cooperative functionality Learn More
- Puts YOU first! - Priority database updates
- Puts Malware in the Slammer - Quarantine function holds threats and lets you restore at your convenience
- Talk to the hand - Ignore list for both the scanner and Protection Module
- For Your Pleasure - Customizable settings enhance performance
- Lock It Down - Password protect key program settings
- Chameleon - Gets Malwarebytes running when blocked
- Toolbox - Extra utilities to help remove malware manually
- Nitty Gritty - Command line support for quick scanning
- RPP, Yeah You Know Me - Realtime Proactive Protection Module
- Hablamos Everything! - Multi-lingual support (Klingon still in beta)
- Support for XP, Vista, 7, and 8 (32-bit and 64-bit)

Malware bytes is certified by Westcoast Labs for antivirus, anti-spyware, anti-trojan.

Malwarebytes Anti-Malware Mobile

Take your anti-malware protection to go:
Malwarebytes Anti-Malware Mobile guards your identity and personal data on-the-go. So you and your Android smartphone or tablet are safe from malware and unauthorized surveillance. Wherever you are. Whenever you go.

Make your smartphone smarter:
Is that app or downloaded photo safe? With Malwarebytes Anti-Malware Mobile, you never have to worry again. Powerful anti-malware and anti-spyware technology protects your Android device. Detecting Trojans, spyware, and other malware before they can steal your identity or eavesdrop.

Choose what you keep private:
Cybercriminals, and even legitimate companies, can collect private information from your Android device. Where you go. Who your contacts are. Malwarebytes Anti-Malware Mobile identifies what your applications are doing, and which private information is being accessed. So you can choose who knows what.

Close the security holes:
Malwarebytes Anti-Malware Mobile automatically recognizes security vulnerabilities in your phone's settings. Then it makes recommendations on how to close those holes.

Make your smartphone lighter:
Mobile security software is typically overloaded with location features (Remote Lock, Locate on a Map, etc.). Features that can already be found on your phone's Android Device Manager. Malwarebytes Anti-Malware Mobile preserves your phone's performance by adding only the necessary security features.

Features:
Anti-Malware/Anti-Spyware

- Proactively scans applications and files for malware and spyware
- Scans native memory and SD card
- Schedules automatic scans
- Updates the protection database automatically

Privacy Manager

- Identifies every application's access privileges in detail
- Breaks down access priveleges by category: Contacts, Identity Information, Simple Message Service (SMS), and Security Settings

Security Audit
- Identifies security vulnerabilities on your device, suggests remediation
- Links seamlessly to Android Device Manager's device location features so the device can be located, locked or reset if it is lost or stolen

Application Manager
- Identifies which applications are currently running
- Identifies installed applications
- Enables custom whitelisting of approved apps

Malwarebytes Secure Backup

Features:
- Seamless integration with Malwarebytes Anti-Malware
- Backs up to the cloud and/or local drives
- Convenient 50, 100, and 200 GB plans
- Unlimited device backup (your Malwarebytes Secure Backup software must be installed on a Windows PC before you can access your accounts from iOS and Android devices)
- Unlimited file versioning (only the largest version of the archived file counts against your storage allotment)
- Deleted files archived
- Automatic backups
- Web management portal
- Network drive and external drive support

Malwarebytes Anti-Exploit BETA

Feeling exploited? We have you covered: Malwarebytes Anti-Exploit BETA protects you from zero-day exploits targeting browser and application vulnerabilities. Its proprietary technology protects you in that critical period between the release of a new exploit and its subsequent security patch. And, unlike antivirus products, Malwarebytes Anti-Exploit BETA proactively prevents the exploit from installing its payload. Before it can do damage.

Features:
Defeats dangerous exploits, shields software vulnerabilities
- Lightweight
- Runs silently in the background
- Install and forget—no management necessary
- Compatibility with anti-malware and antivirus products
- No signature database—no need for daily updates

Browser protection
- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Opera
- Java, Flash, Shockwave, Acrobat, and any other browser plugin

Application protection
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Adobe Acrobat Reader
- Adobe Acrobat PRO
- Foxit Reader

Media players protection:
- Windows Media Player (wmplayer)
- Windows Media Player (wmplayer2)
- VLC Player
- Apple QuickTime
- Winamp

For more details visit
http://www.malwarebytes.org/

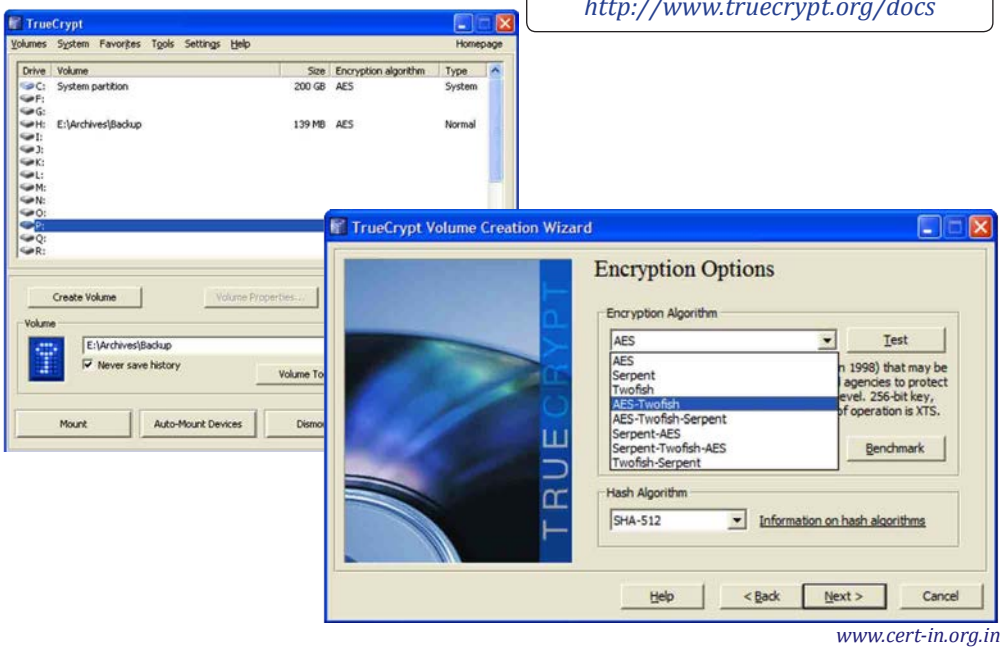
True Crypt

Free Open Source on-the-Fly Encryption

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

TrueCrypt is software for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted right before it is saved and decrypted right after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).

Files can be copied to and from a mounted TrueCrypt volume just like they are copied to/from any normal disk (for example, by simple drag-and-drop operations). Files are automatically being decrypted on the fly (in memory/RAM) while they are being read or copied from an encrypted TrueCrypt volume. Similarly, files that are being written or copied to the TrueCrypt volume are automatically being encrypted on the fly (right before they are written to the disk) in RAM. Note that this does not mean that the whole file that is to be encrypted/decrypted must be stored in RAM before it can be encrypted/decrypted. There are no extra memory (RAM) requirements for TrueCrypt. For an illustration of how this is accomplished, see the following paragraph.



The following features are planned to be implemented in future versions:
- Full support for Windows 8
- Ability to encrypt Windows system partitions/drives on UEFI-based computers (GPT)
- Command line options for volume creation (already implemented in Linux and Mac OS X versions)
- 'Raw' CD/DVD volumes and more

For more details visit
http://www.truecrypt.org/docs

Microsoft Silverlight

Information Disclosure Vulnerability

Description: This vulnerability exists in Microsoft Silverlight due to improper handling of certain objects in the memory. A remote attacker could exploit this vulnerability by enticing a user to visit website containing a specially crafted Silverlight application.

Successful exploitation of this vulnerability could result in exposure of sensitive information on the targeted system resulting in complete system compromise.

Overview: An information disclosure vulnerability has been reported in Microsoft Silverlight, which could allow a remote attacker to access sensitive information on a targeted system.

Workaround: Temporarily prevent Microsoft Silverlight from running in Internet Explorer. Mozilla Firefox and Google Chrome.

Solution: Apply appropriate updates as mentioned in the Microsoft Security Bulletin MS13-087

Systems Affected:

- Microsoft Silverlight 5
- Microsoft Silverlight 5 Developer Runtime

Microsoft Security Bulletin MS13-087

Vulnerability in Silverlight Could Allow Information Disclosure (2890788)

Executive Summary: This security update is rated Important for Microsoft Silverlight 5 and Microsoft Silverlight 5 Developer Runtime when installed on Mac and all supported releases of Microsoft Windows. For more information, see the subsection, Affected and Non-Affected Software, in this section.

Microsoft Silverlight Memory Object Processing Information Disclosure Vulnerability

Description:A vulnerability in Microsoft Silverlight could allow an unauthenticated, remote attacker to access sensitive information.The vulnerability is due to improper memory operations performed by the affected software when handling certain objects. An attacker could exploit the vulnerability by convincing a user to follow a malicious link. A successful exploit could allow the attacker to access sensitive on a targeted system.

Functional code that demonstrates an exploit of this vulnerability is publicly available.

Microsoft has confirmed the vulnerability in a security bulletin and released software updates.

For more details visit :

Vendor Information Microsoft
http://technet.microsoft.com/en-us/security/bulletin/ms13-087
CISCO
http://tools.cisco.com/security/center/viewAlert.x?alertId=31063
Secunia
http://secunia.com/advisories/55149
CVE-Name
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3896

Worm:Win32/ Yeltminky.A!inf

It has been observed that new variant Win32/Yeltminky.A!inf is spreading . this worm creates a autorun file on the victim's local drives, network drives or external devices to spread ad infect other computers. Upon installation ir creates autorun. inf file and copies itself to the safedrv.exe file in the root directory of all the devices and drives detected. The file autorun.inf is to ensure that safedrv.exe runs every time the drive is opened or USB/removable inserted into same or other computers.
To detect and remove this threat and other malicious software that may be installed on your computer, run a full-system scan with an appropriate, up-to-date, security solution.

Countermeasures

- Enable firewall at desktop and gateway level
- Disable the Autorun functionality in Windows

http://support.microsoft.com/kb/967715

- Keep up-to-date patches and fixes on the operating system and application software
- Keep up-to-date Antivirus and Antispyware signatures at desktop and gateway level
- Consider tools for USB vaccination avoid further spread of worm
- Protect yourself against social engineering attacks
- Use strong passwords and also enable password policies
- Limit user privileges on the computer
- Avoid downloading pirated software

References

http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Yeltminky.A!inf
http://www.securelist.com/en/descriptions/7714002/Trojan.Win32.Buzus.dzwk

For more details visit

New viruses creep upon a daily basis. It is important that we do back up our valuable data files regularly.

Desktop/Laptop/Tablet Security

Why do you need to secure your Desktop?

A personal computer used without proper security measure could lead to exploiting the system for illegal activities using the resources of such insecured computers. These exploiters could be Virus, Trojans, Keyloggers and sometimes real hackers. This may result in data theft, data loss, personal information disclosure, stealing of credentials like passwords etc. So, protect and secure your Personal Computer before it is compromised.

Guidelines

Things to remember while using your personal computer :

- Always install Licensed Software so that you have regular updates of your Operating system and Applications. In case of open source software, make sure to update frequently.
- Read the "Terms and Conditions" / "License Agreement" provided by vendor/ software before installation.
- Properly shutdown and switch off your personal computer after the use along with your external devices like Monitor, Modem, Speakers etc.

Software Installation :

1. Installation of Operating System:Get proper Licensed Operating System and read license agreement carefully before in stalling the OS.
   - Switch on your personal computer and go to BIOS Settings and change your first boot drive to CD Drive.
   - Insert your CD/DVD into the CD drive and restart your system using Ctrl+Alt+Delete.
   - After restart, the system boots from the CD/DVD.
   - Follow the installation steps as specified by the vendor document.
2. Use the CD provided by the Vendor to install your
   - Motherboard drivers
   - Monitor drivers
   - Audio & Video drivers
   - Network drivers

" To setup your computer safely Read the Vendor document carefully and follow the guidelines"

Physical Security: The first step in security is considering the physical security of the PC. Maintenance of physical security depends on the location and the budget.

The second step is the factors related to physical stability that include the power supply, physical location of the computer, room temperature, etc. Failure of anyone of the above said factors leads the computer into risks.

There is a good chance that your home PC is one of the most expensive things in your home, or if you have got a laptop, it is likely to be the most expensive thing you carry in a bag.

Although your insurance policy may cover the costs of replacing hardware if it's stolen, there is nothing that money can do to retrieve precious or personal data. So physical security is as important as software security.

" Always keep the desktop firewall on."

Data Security: Data Security means ensuring that the data is free from any type of fraud and the access to this data is controlled in such a way that only authorized users can access the data. Data refers to personal information regarding the individuals, bank details, etc. Data in transfer, across and between company networks, are usually the focus of extensive security efforts.

However, organizations typically regard data residing on internal storage devices as secure enough. Hence, there is a need for everyone to secure the data so that it does not fall into the hands of unauthorized users.

Different methods of securing data:

- Shared Information
- Web browser
- Secure e-Mail programs
- Secure Shell
- Data backup
- Securing data by disposal
- Secure e-Mail programs

Internet Security:

- Follow Internet Ethics while browsing.
- Check the copyright issues before using the content of Internet.
- Always access the site which uses https (Hyper Text Transfer Protocol Secure) while performing online transactions, accessing emails etc, which is secure.
- If the site uses SSL, verify the Certificate details like who is the owner, expiry date of the certificate etc to confirm whether it is trusted or not.
  h•*You can do this by clicking the lock icon.*
- Use only original websites for downloading the files rather than third party websites.
- Scan the downloaded files with an updated Anti-Virus software before using it.
- Install and properly configure a software firewall, to protect against malicious traffic.

E-mail Security: e-Mails are just like postcards from which the information can be viewed by anyone. When a mail is

transferred from one mail server to another mail server there are various stops at which there is a possibility of unauthorized users trying to view the information or modify it.
Since a backup is maintained for an e-Mail server all the messages will be stored in the form of clear text though it has been deleted from your mailbox. Hence there is a chance of viewing the information by the people who are maintaining backups. So it is not advisable to send personal information through e-Mails.

Desktop firewall provides a helpful defense against remote installation of spyware by hackers

Wireless Security: Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfill their needs.
Anyone with Wi-Fi connectivity in his computer, laptop or mobile can connect to unsecured Access Points(wireless routers). Anyone in the range of Access point can connect to an Access Point if it is unsecured. Once the connection is established the attacker can send mails, download classified/confidential stuff, initiate attack on other computers in the network, send malicious code to others, install a Trojan or botnet on the victims computer to get long term control on it through Internet, etc.

Tips for securing Wireless Communications.

- Change default Administrator passwords.
- Turn On WPA (Wi-Fi Protected Access) / WEP Encryption.
- Change default SSID
- Enable MAC address filtering
- Turn OFF your wireless network when not in use.

"Do You Know?
81 % of Home Users experienced at least one security threat during 2013"

Instructions to be followed while connecting Wireless Modem :

- Make sure you have the necessary equipment. Your wireless modem package should include the wireless modem (or wireless adapter), an installation CD-ROM with a manual; an Ethernet cable (or a USB cable if you have a wireless USB modem); a wireless antenna (conforming to wireless standards such as 802.11a, 802.11b, or 802.11g); and a power adapter. Call the retailer or the manufacturer of your wireless modem if any of these items are missing.
- Read the manual to learn how the equipment functions. For example, use the wireless antenna to connect to the wireless network ; use the Ethernet cable (or USB cable) to connect the computer to the modem.
- Attach your wireless antenna to the modem.
- Hook up an Ethernet cable from your computer to a LAN/Ethernet port on the modem. Or, if you have a wireless USB modem, connect the USB cable to the USB port of the computer.
- Connect the power adapter to the power connector of the modem, plug it in and switch it on.

Setting Up the Wireless Modem

- Open your Web browser and enter the URL of the modem's administrative site. If you can't find it in the users' manual, call the modem manufacturer's/vendor's customer service.
- Log in to the administrative site by entering the user name and password provided in the user manual. Again, if you cannot locate these, call the modem manufacturer vendor's customer service. Usually the default username and password is "Admin."

" All Wi-Fi equipment support some form of encryption. So,

- Select the Internet connection type. There are four types of Internet connection: "Dynamic IP Address," "Static IP Address," "PPPoE/PPPoA" and "Bridge Mode." Call your Internet service provider (ISP) to ask which setting best suits their wireless service.
- Choose "Dynamic IP Address" to get an IP address automatically from the ISP's server. For every wireless Internet connection you make, you receive an IP address. In some cases the IP address is dynamic (it changes every time you connect to the Internet) and in other cases it is static (the IP address remains the same even after you disconnect and reconnect to the Internet). If the address is dynamic, you will have to choose this setting so that the modem automatically takes the IP from the ISP's server whenever a new wireless connection is established. Enter your modem's MAC Address (usually found at the back of the modem) and other details. Refer to the user manual or call the modem manufacturer / vendor customer service to get these details.
- Select "Static IP Address" if you are provided with a static IP. You will need to fill in the fields for "VPI," "VCI," "IP Address," "Subnet Mask," "ISP Gateway Ad-

Use desktop firewalls when using wireless networks.

dress," "Server Address," "Primary DNS Address," "Secondary DSN Address" and "Connection Type." These details can be otained from your ISP.

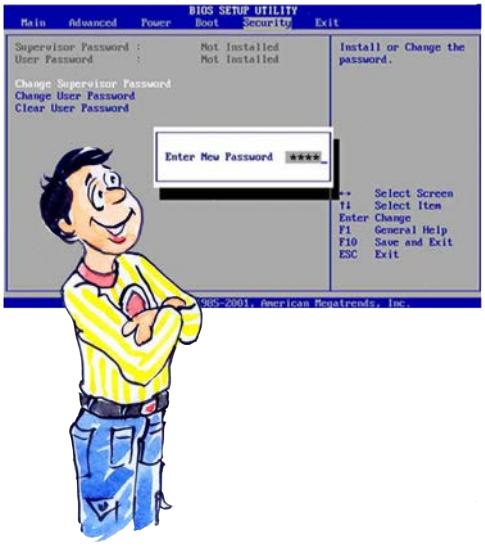
- Opt for "PPPoE/PPPoA" if your ISP uses this type of connection. DSL users may use this connection. Enter your username, password and other details. These will be provided by your ISP.
- Select the "Bridge Mode" if your ISP uses this connection type. Enter the relevant details provided by your ISP.
- Finish the process by clicking on the icon that says "Finish" or "OK" or something similar. Your modem should be set up now.
- Enter any URL address in your browser to check whether Internet is working or not.

Setups

BIOS Settings:

(Basic Input/Output System) Settings :

- Computers BIOS is the first program that runs when computer is started. You can tell the BIOS to ask for a password when it starts, thus restricting access to your computer.
- To enter the BIOS setup program, sometimes called CMOS setup:Turn on or reboot your computer. The screen will display a series of diagnostics and a memory check. A message will come "Hit the <DEL> key to enter the BIOS setup program" will appear. [It's not always the DEL key some BIOS's use F2 or F10 or any other key combination, check your motherboard manual for more details].
  Note: Some BIOS versions use a graphical type menu with icons (a GUI) or have a text inter- -face, the principle however is exactly the same.
- There are two options that relate to passwords, Supervisor Password and User Password, these relate to controlling access to the BIOS Setup Program and the Machine Boot respectively.
  Note: Not all BIOS's have this password feature, your BIOS may not have it in which case you won't be able to restrict access to your computer in this way.



- Select USER PASSWORD and you'll be prompted to enter a password.You should now enter a password of up to eight characters (most BIOS's are limited to eight characters unfortunately). We recommend to use the full eight but take care that you choose something you'll not forget. The BIOS will then prompt you to confirm the password, just type the same thing again. Now you'll want to set your system to ask for that password every time it boots, so select the BIOS FEATURES SETUP option, to see a menu. It's the Password Check option if you are interested in, so select it and change the setting to "ALWAYS". Now navigate back to the main menu and select SAVE & EXIT SETUP. Your machine will then reboot and you'll be prompted for the password. Each and everytime you boot you'll be asked for password you chose.
  Note: This method of restricting access to your computer is not completely foolproof, there are ways around it. But it will stop or at least delay the majority of casual attempts to get ac -cess.
  Note: If you forget your BIOS password, refer your motherboard manual or if you don't have one, refer the website of the BIOS manufacturer.

For more details visit
www.infosecawareness.in
www.secureelectronics.in

InfoSec Cartoon

"Delete chain e-mails and junk e-mail. Do not forward or reply to any to them."

C-DAC Courses

C-DAC Online Courses (paid)

- Core Competency in Software Process Management [CCSPM]
- Courses list C-DAC's Course on Cyber Security [CCCS]
- Courses list C-DAC Certified Course on Cyber Security Professional [CCCSP]
- Courses list C-DAC's Certified Professional in Linux Kernel Programming & Device Drivers [CCP-LKPDD]
- Courses list C-DAC's Certified Professional in Linux System Programming [CCP-LSP]

C-DAC Online Courses (free)

- Right to Information Act - Hindi Course
- Courses list Sustainable Agriculture - Telugu Course
- Courses list Computer Fundamentals - Telugu Course

For more details visit
http://elearn.cdachyd.in/
http://elearn.cdac.in/

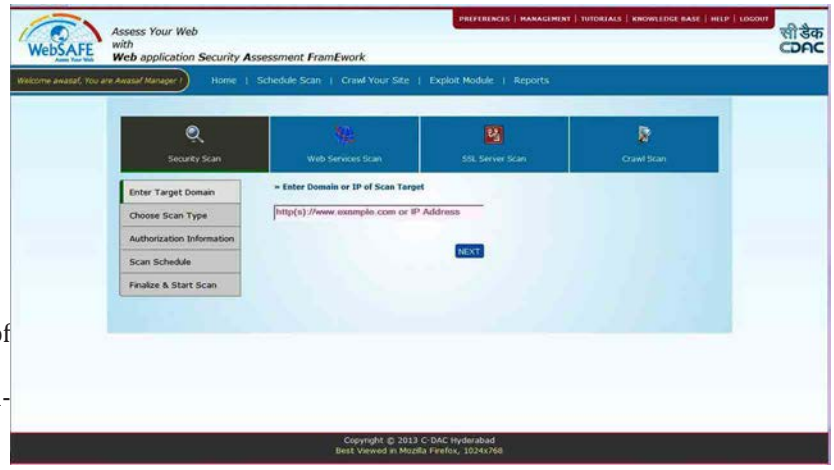
WebSAFE
Assess Your Web

Automated Web Application Security Assessment Framework

WebSAFE is a comprehensive, OWASP Complaint, extensive and powerful web based assessment framework to cater to all security assessment needs of a web application.

Features

- Simple & User-Friendly
- Multiple Scan at any instance
- Schedule Scan
- Exhaustive Information Gathering
- OWASP Compliant
- Risk Assessment
- In-Depth Crawling
- Deep analysis on SSL Configuration
- Exploitation of Discovered Vulnerabilities as Proof of Concept (PoC)
- Easy to understand - Executive Summary and Developer Reports



Security Issues Addressed

- Information Leakage
- Injection Attacks
- XSS, CSRF, Clickjacking kind of Vulnerabilities
- Authentication and Authorization failure
- Denial of Sevice

For details
http://cdachyd.in/websafe
Contact : 040 - 23150115
email: esuraksha@cdac.in

http://articles.timesofindia.indiatimes.com/2013-10-08/hyderabad/42827954_1_engineering-student-email-account-cyber-crime

THE TIMES OF INDIA

Home City India World Business Tech Sports Entertainment Life & Style Women Hot on the We

Engineering student held for hacking girl's email

TNN Oct 8, 2013, 06.53AM IST

HYDERABAD: The Cyberabad police on Monday arrested an engineering student for hacking into a girl's email account and posting her personal details on porn websites.

The accused, Goli Subash Chandra Bose, 22, is a second year BTech student in Vivekananda Global Group of Institutions located near Ramoji Film City in Hayathnagar. The victim, who is also a college student, lodged a complaint with the Cyber Crime sleuths on October 5 alleging that somebody had hacked into her email account, linked it to porn websites and also posted her personal details on those websites.

http://www.bbc.co.uk/news/technology-24348395

BBC News Sport Weather Capital Culture Autos TV Radio More... Sea

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Environment Tech Entertainment Video

Symantec disables 500,000 botnet-infected computers

By Tom Espiner
Technology reporter

Symantec has disabled part of one of the world's largest networks of infected computers.

About 500,000 hijacked computers have been taken out of the 1.9 million strong ZeroAccess botnet, the security company said.

The zombie computers were used for advertising and online currency fraud and to infect other machines.

Security experts warned that any benefits from the

http://www.dnaindia.com/scitech/1890792/report-email-sms-stealing-android-virus-prowling-in-indian-cyberspace

dna

ANALYSIS CITIES NEWS SPORTS MONEY SCI & TECH DNA P

Email, SMS stealing Android virus prowling in Indian cyberspace

Wednesday, Sep 18, 2013, 19:50 IST | Agency: PTI

A potentially damaging virus, which steals SMSes and personal details of an Android-enabled gadget-user, has been detected in Indian cyberspace and internet security sleuths have asked mobile phone and tablet users to exercise caution while operating. The malware is affecting all the versions of Android prior to version 4.2.2 (Jelly Bean).

"It has been observed that a critical vulnerability exists in Android which could allow attackers to inject malicious code into legitimate applications which makes it possible to change an application's code without affecting the cryptographic signature of the application, essentially allowing a malicious author to trick the Android device into believing that the crafted application is unchanged," the Computer Emergency Response Team-India (CeRT-In) said in its latest advisory to Android users in the country.

The malicious programme, the advisory said, is so damaging that it could be used for stealing personal information like email addresses, IMEI numbers, SMSes and installed applications. "It could also send SMS or make calls from infected devices without user consent," the sleuths of the national cyber security centre said.

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and 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

सत्यमेव जयते

Department of Electronics & Information Technology
Government of India

Executed by

सी डैक CDAC
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.