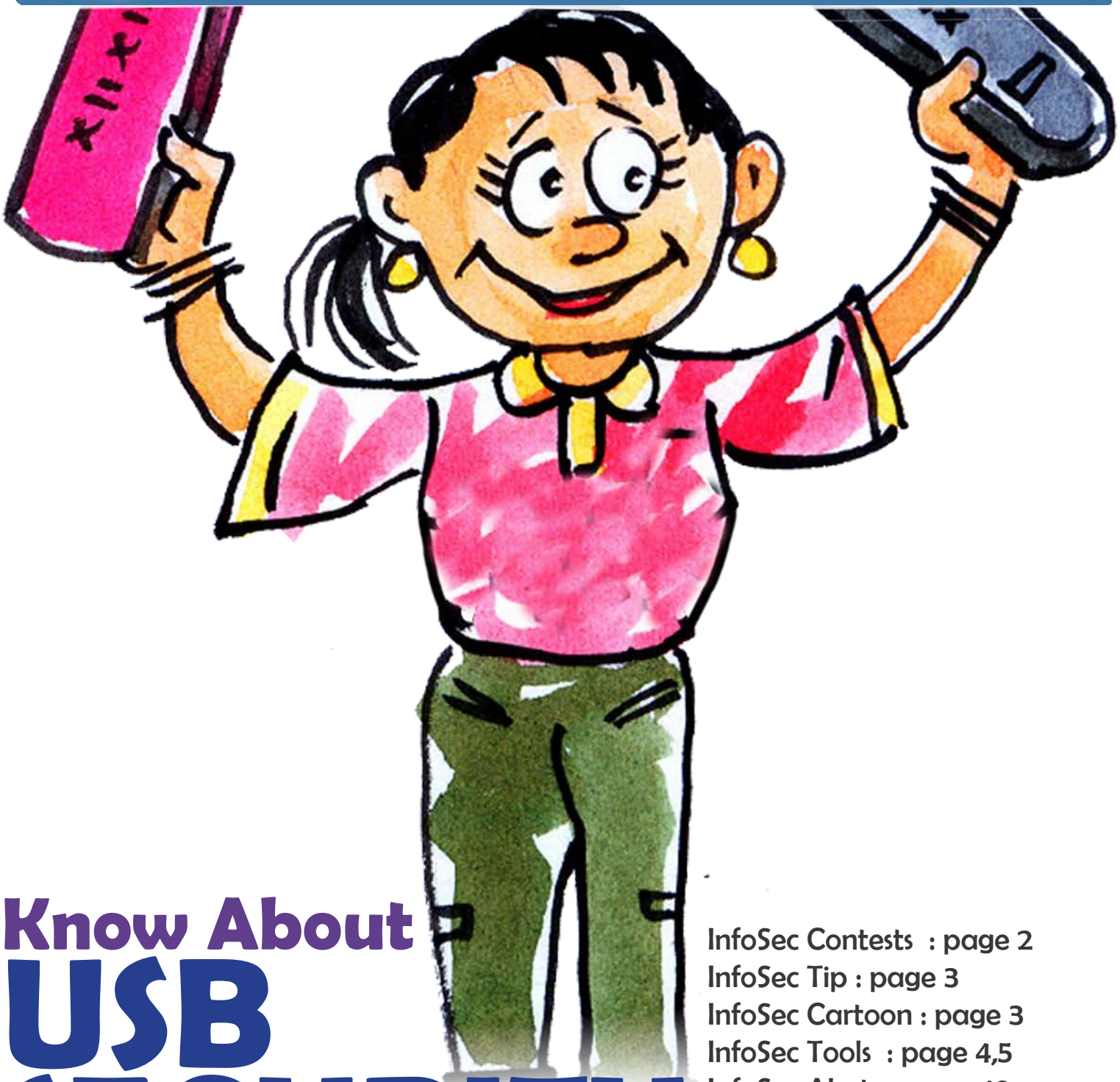
Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.



Know About USB SECURITY

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

Executed by
सी-डैक 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-III

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
Government of India

Comments & Feedback
mail us to
isea@cdac.in

InfoSec Quiz

1. Which of the following is an entity that issues Digital Certificates in a Public Key Infrastructure.
   (a)National Informatics Centre (b)VeriSign
   (c)komodo (d)Certifying Authority

2. Wardriving is an act of searching
   (a)Mails (b)Wired networks (c)Wireless Networks
   (d)none of the above

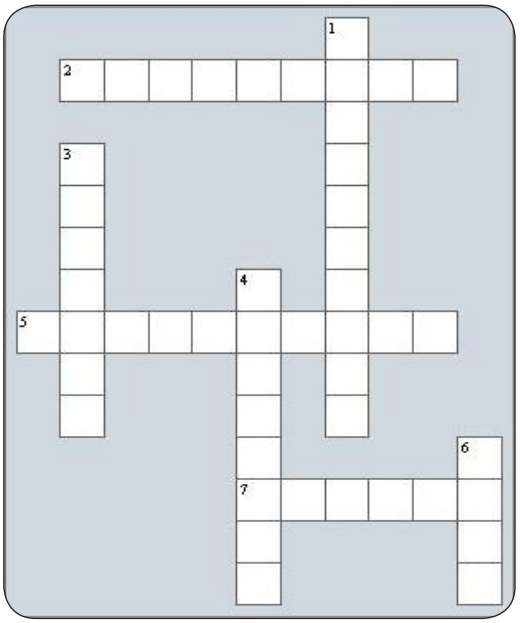
3. BOSS is a free open source operating system
   (a)True (b)False

4. Which of the following is a worm ?
   (a)hikit (b)Win32.worm.stuxnet.A (c)duqu (d)All of the above

5. Which of the following is not a free/open source operating system
   (a)fedora (b)ubuntu (c)Windows 7 (d)BOSS

logon to
www.infosecawareness.in
to participate in Infosec Contest and win prizes

InfoSec Crossword



Across:

2. What's another name for crackers -- malicious hackers who infiltrate secure systems in order to steal information or cause damage?
5. is the use of computers and computer networks as a means of protest to promote political ends
7. is a popular webserver used on internet

Down:

1. Going behind somebody through the access doors without using own access card
3. Computer worms, viruses and trojans are grouped in to one category called
4. is used to block unwanted traffic from Internet
5. is a famous Trojan Horse that steals banking information.

Guess the Tip

Guess the Tip which best suits the cartoon by logging on to www.infosecawareness.in

InfoSec Cartoon

Never keep any of your sensitive documents on your desk-top.

InfoSec Tip

Do not download Software from untrusted sources

Computer users often download software from Internet and install them. These software may contain virus, worms, Trojan Horses, etc. Installing unnecessary applications and software may compromise the security of the system. Even if the software or applications are found to be legitimate, it is suggested that these may be installed only if it is essential.

Tips for safe downloads

- Scan the software before installing with up-to-date Antivirus.
- Do not install unnecessary software, which are not required.
- Always update the applications and sofware installed on the PC.
- Always follow the standard advisory from original developers of software.
- Set secure browser settings before you download anything.
- Read carefully before you click on install or run application. That means read terms and conditions.
- Set firewalls, set antivirus to actively scan all the files you download.
- Close all the important applications before downloading in order to be safe if something goes wrong while downloading.

For more guidelines on safe downloads visit :
www.infosecawareness.in

WehnTrust

When you need to Trust Windows

Though Windows XP is more than a decade old Operating System it has still ~30% share in enterprise PCs. Ofcourse, if in these ten years hackers have reached new heights, security researchers also have chasen them to full. Most noticeable security feature is Address Space Layout Randomization (ASLR). This kind of exploit protection is not available on Windows XP.

Overview :

WehnTrust is a Host-based Intrusion Prevention System (HIPS) for Windows 2000, XP, and Server 2003. It includes support for exploit mitigations that are designed to make exploitation more difficult by preventing the use of specific exploitation techniques and by making exploitation unreliable.

Features

The tool has following three main features:

1. IT provides ASLR which makes exploitation very difficult.
2. SEH Overwrite Prevention
3. Format String Vulnerability Prevention

User need not do any configuration after installing this software. If any attempt to exploit is prevented by Wehn- Trust then it logs it which can be viewed in event viewer.

How it works ?

WehnTrust randomizes the base addresses of memory allocations to make it more difficult to exploit software vulnerabilities such as buffer overflows. This technique is commonly known as Address Space Layout Randomization (ASLR) and was originally conceived by the PaX team. Microsoft has recently incorporated support for ASLR into Windows Vista and Windows Server 2008. In addition to ASLR, WehnTrust generically mitigates SEH overwrites by dynamically validating a thread's exception handler chain prior to allowing exceptions to be dispatched.

Using WehnTrust in combination with hardware-enforced DEP (non-executable pages) as included with Windows XP SP2 and Windows Server 2003 provides the greatest level of security. Non-executable pages help to counter some of the inherent weaknesses of ASLR. WehnTrust provides protection to Windows XP and Server 2003 PCs from being exploited.

InfoSec Quote

"I don't hate technology, I don't hate hackers, because that's just what comes with it, without those hackers we wouldn't solve the problems we need to solve, especially security."

- Fred Durst

The tool can be downloaded free of cost from
http://wehntrust.codeplex.com/
The commercial version of the tool is available only at
http://www.wehnus.com/products.pl

PhotoRec

PhotoRec is file data recovery software designed to recover lost files including video, documents and archives from hard disks, CD-ROMs, and lost pictures (thus the Photo Recovery name) from digital camera memory. PhotoRec ignores the file system and goes after the underlying data, so it will still work even if your media's file system has been severely damaged or reformatted.

PhotoRec is free - this open source multi-platform application is distributed under GNU General Public License (GPLV v2+). PhotoRec is a companion program to TestDisk, an application for recovering lost partitions on a wide variety of file systems and making non-bootable disks bootable again.

For more safety, PhotoRec uses read-only access to handle the drive or memory card you are about to recover lost data from.

As soon as a pic or file is accidentally deleted, or you discover any missing, do NOT save any more pics or files to that memory device or hard disk drive; otherwise you may overwrite your lost data. This means that while using PhotoRec, you must not choose to write the recovered files to the same partition they were stored on.

How it works ?

FAT, NTFS, ext2/ext3/ext4 filesystems store files in data blocks (also called data clusters under Windows). The cluster or block size remains at a constant number of sectors after being initialized during the formatting of the filesystem. In general, most operating systems try to store the data in a contiguous way so as to minimize data fragmentation. The seek time of mechanical drives is significant for writing and reading data to/from a hard disk, so that's why it's important to keep the fragmentation to a minimum level.

When a file is deleted, the meta-information about this file (filename, date/time, size, location of the first data block/cluster, etc.) is lost; e.g., in an ext3/ext4 filesystem, the names of deleted files are still present, but the location of the first data block is removed. This means the data is still present on the filesystem, but only until some or all of it is overwritten by new file data.

To recover these 'lost' files, PhotoRec first tries to find the data block (or cluster) size. If the filesystem is not corrupted, this value can be read from the superblock (ext2/ext3/ext4) or volume boot record (FAT, NTFS). Otherwise, PhotoRec reads the media, sector by sector, searching for the first ten files, from which it calculates the block/cluster size from their locations. Once this block size is known, PhotoRec reads the media block by block (or cluster by cluster). Each block is checked against a signature database; which comes with the program and has been growing in the type of files it can recover ever since PhotoRec's first version came out. It's a common data recovery method called File carving.

- *PhotoRec ignores the file system; this way it works even if the file system is severely damaged*
- *PhotoRec works with hard disks, CD-ROMs, memory cards, USB memory drives, DD raw image, EnCase E01 image etc.*

Reference:
http://www.cgsecurity.org/wiki/PhotoRec
Download:
http://www.cgsecurity.org/wiki/TestDisk_Download

USB Storage Device Security

USB flash drive is a data storage device used for storage, back-up and transfer of computer files. USB mass storage devices like pendrives, micro SD cards, external storage devices are used to store images, audio, video etc. These devices are relatively small, durable and reliable compared to floppy disks and CD-ROMs. They have replaced Floppy disks which were used earlier. USB devices are superior in terms of speed and storage capacity.

The popularity of USB storage devices has attracted attackers to use these as a medium to spread viruses, worms and trojans. USB devices are used by attackers to perform malicious activity on the targets computer.

One of the options for an attacker is to use USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware. Once malware is installed in the victim's computer, the installed malware can detect whenever a new USB drive is plugged into the computer and the malware on the infected PC infects that USB drive, which when inserted into another PC the malware tries to get installed on that PC as well. In this way the malware spreads from one system to other.

Attackers may also use their USB drives to steal information from a computer which is not even connected to internet. The most obvious security risk for USB drives is that they are easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean loss of many hours work. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

Baiting

Someone intentionally leave USB devices at your desk or place with Malware

Data thefts and Data leakage are everyday news now!

All these can be controlled or minimized with care, awareness and by using appropriate tools to secure the information. The tips and recommendations provided in this document helps you to keep your information secure while using USB storage devices.

- The Conficker worm spreads via removable devices and drives such as memory sticks, MP3 players and Digital Cameras.
- Also 30% of new worms have been specifically designed to spread through USB storage devices connected to computers.
- The Stuxnet worm was one of the year's high profile threat that spread through USB drives.

Threats

- Malware Infection
- Malware Spreads through USB storage devices. Someone may intentionally sell USB storage devices with malware to track your activities, files, systems and networks.
- Malware may spread from one device to another device through USB Storage Devices using autorun.exe, which is by default enabled.
- Someone may steal your USB Devices for Data
- Unauthorized Usage

News about USB attacks:

Stuxnet a highly sophisticated computer worm discovered in June 2010 attacked Iranian uranium enrichment infrastructure. The worm initially spread using infected removable drives such as USB flash drives. Stuxnet attacked windows systems using an unprecedented four zero-day attacks. The malware has created a huge loss to Iranian government.

Flame, also known as Flamer is a computer malware discovered in 2012 that attacks computers running Microsoft Windows operating system. Flame can spread to other systems via USB stick. It can record audio, screenshots, keyboard activity and network traffic. This data along with locally stored documents is sent on to one of several command and control servers that are owned by attackers.

The Conficker worm spreads via removable devices and drives such as memory sticks, MP3 players and Digital Cameras.

How to stop Data Leakage via USB storage ?

1. Design and adopt a good security policy to limit the usage of USB Storage devices.
2. Monitor the employees for what they are copying.
3. Implement Authentication, Authorization and Accounting to secure your information.

What to do when you loose your Device?

1. If you have stored any personal or sensitive information inside the USB drive like passwords etc, immediately change all passwords along with security questions and answers provided during any account creation [There may be chances that hacker can retrieve your online account logon information by using data from the stolen drive].
2. Also ensure that all security measures have been taken against the lost data.

How to stop Device theft?

1. Always secure the drive physically by tagging it to a key chain.
2. Never leave your drive unattended anywhere.
3. Never keep sensitive information without encryption .

Types of devices which support USB

- Card readers
- Mobile phones
- PDAs
- Digital cameras
- Digital audio players
- Portable media players
- Portable flash memory devices

Dos and Dont's for the safe use of USB storage devices:

Following these steps you can protect the data on your USB drive and on any computer that you might plug the drive into.

Do's

- Always do low format for first time usage.
- Always make sure you delete the content or important documents stored in pendrive when not in use.
- Always scan USB disk with latest Antivirus before accessing.
- Protect your USB device with a password.
- Encrypt the files / folders on the device.
- Use USB security products to access or copy data in your USB.
- Always protect your documents with strong password.

For Small Business or Enterprises

- Monitor what data is being copied.
- Block the unauthorized USB from connecting.
- Pick the device with features and correct level of encryption to meet compliance requirements and organization needs.
- Educate employees on acceptable and inacceptable use of USB flash drives.
- Document policies so that users know who is authorized and what they are authorized to do.

Dont's

- Do not accept any promotional USB device from unknown members.
- Never keep sensitive information like username/ passwords on USB disk.

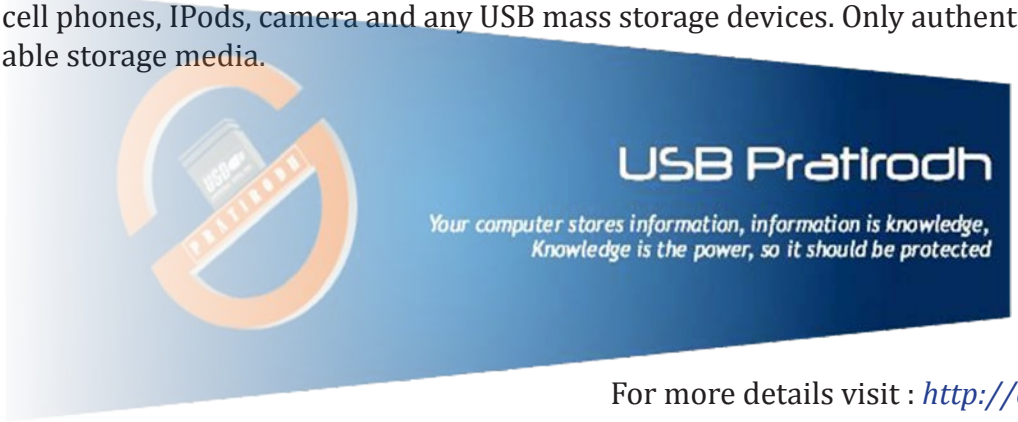
Don't use USB keys, CDs, or laptop drives for unencrypted sensitive data.

Remember to remove the USB drive from your computer before you walk away.

USB Pratirodh

Regulating removable storage device access

USB Pratirodh is a software solution which controls unauthorized usage of portable USB storage devices. The USB Pratirodh blocks and controls the usage of removable storage media like pen drive, external hard drives, cell phones, IPods, camera and any USB mass storage devices. Only authenticated users can access the removable storage media.



Features:

- User authentication
- Device Control
- Co-existence
- Support for both Windows and Linux
- Device Control

For more details visit : *http://cdachyd.in/products/usb-pratirodh*

More Tips

Use and Maintain security software and keep all software up to date

Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions up-to-date.

Use different drives for official and personal purpose.

Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.

Take advantage of security features.

Use passwords and encryption on your USB drive to protect your data and make sure that you have the information backed up in case your drive is lost.

Disable Autoplay

The Autorun feature causes removable media such as CDs, DVDs and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically and harming your personal computer.

Don't use a USB stick that you found or receive for free.

Always buy from trusted sources and never collect any pendrives which were found. Always clean the USB drive with latest Antivirus software when you bought for the first time.

Don't leave your flash drive in extreme temperatures.

Below freezing temperatures or excessive heat can damage your flash drive, leaving it unusable. Always keep it in a safe place, preferably at room temperature.

Do save your work to your flash drive frequently.

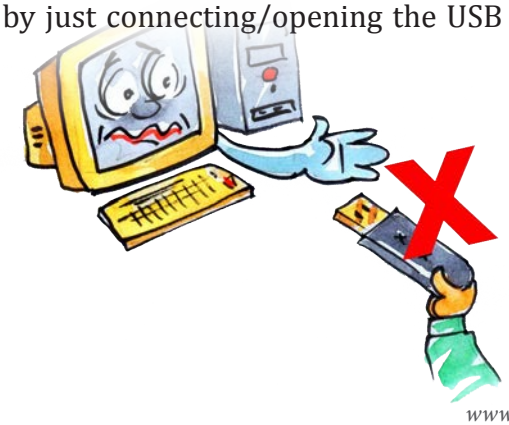
If you are writing an important paper which is directly stored in the USB drive, get in the habit of saving your work every 10 minutes. The sudden loss of power or accidentally closing out the program you're using can be extremely frustrating, but even more so if you haven't saved your progress and then have to go back and write it all over again.

Don't allow someone else to put a USB stick of unknown origin into your computer.

Sometimes the USB stick from not trusted sources may contain malware which can harm your computer. If necessary scan the USB drive with latest Antivirus software and use them.

Do not plug an unknown USB drive into your computer.

If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department etc.). Do not plug it into your computer to view the contents or try to identify the owner. There is a chance that your system may get infected by just connecting/opening the USB drive you found.



Mobile as USB

The mobile phones can be used as USB memory devices when connected to computer. A USB cable is provided with the mobile phone to connect to computer.

Do's

- When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated antivirus.
- Take regular backup of your phone and external memory card because if an event like a mobile crash, lost or malware penetration occurs, at least your data would be safe
- Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.
- Remember to remove the USB connection from your computer before you walk away.

Dont's

- Never forward the virus affected data to other Mobiles.

References:
www.secureelectronics.in
http://en.wikipedia.org/wiki/Universal_Serial_Bus
http://www.infosecawareness.in
http://labs.bitdefender.com/2012/05/cyber-espionage-reaches-new-levels-with-flamer

InfoSec Security Alerts

Virus Alerts

Countermeasures

- Do not download and install applications received from untrusted sources. Download applications only from trusted sources, reputed application markets and Google Play Store.
- Run a full system scan on device with a mobile security solution or mobile antivirus solution.
- Check for the permissions required by an application before installing.
- Exercise caution while visiting trusted/untrusted sites for clicking links.

Android.Adrd

Original Issue Date:July 12, 2013

Virus Type: Trojan

Android.Adrd is a trojan horse that arrives bundled with legitimate Android applications and infects Android based smart phones. The malware seems to be created by downloading an application from a marketplace, modifying the legitimate application and then redistributing via marketplace or other separate channels. The Trojan may change mobile device settings and steal device information.

For more details :
http://cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW01

InfoSec Latest News

sakshipost

HOME NEWS BUSINESS SPORTS CINEMA LIFESTYLE VIDEOS GALLERY

Home > News > State > Lure of lottery money lands SBI manager in jail

LURE OF LOTTERY MONEY LANDS SBI MANAGER IN JAIL

THURSDAY, 06 JUNE 2013 13:22

Have you ever received a notification that you have lottery even without trying? Does the mail ask for yo

If you ever get such tempting mails, just delete them message landed in the mail box of Vizianagaram Balakrishna. The message stated that Balakrishn amount of Rs 2 crores. Instead of deleting the mes

Not surprisingly, the message Lured by the greed of money his bank.

When his fault came to light,

THE TIMES OF INDIA | Tech News

Home City India World Business Tech Sports Entertainment LIVE TV

Tech News Personal Tech Careers Enterprise IT Social Media Slideshows Reviews TechToon

Software & Services Hardware Internet Telecom Movements Outsourcing

Spam traffic grows in Q1 2013: Study

spammer | Spam mails

correspondence in percentage points) arter of 2013, Lab's spam report. emails with all, reaching 3.3%, fell 4.25 times to

dna

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.

"An attacker could exploit this vulnerability by placing other files with same name into an application package along with the legitimate files. The Android package verification occurs against the first file during installation. Thus, the crafted .APK passes the verification process and installs the second file. However, at runtime, other malicious file gets executed," the advisory said.

The cyber police have also suggested some countermeasures. "Check for the permissions required by an application before installing, exercise caution while visiting untrusted sites for clicking links, run a full system scan through a device with a mobile security solution or mobile anti-virus solution, do not download and install applications from untrusted sources and download applications only from trusted sources, reputed application markets and Google play store," the security agency said.

Source :

- *http://www.sakshipost.com/index.php/news/state/20192-lure-of-lottery-money-lands-sbi-manager-in-jail*
- *http://articles.timesofindia.indiatimes.com/2013-05-09/internet/39142376_1_spammers-kaspersky-lab-email-traffic*
- *http://www.dnaindia.com/scitech/1890792/report-email-sms-stealing-android-virus-prowling-in-indian-cyberspace*

InfoSec Workshops

@ Mohali

@ Rourkela

@ Nahan

12

@ Shimla

@ Srinagar

@ Jalandhar

National level Painting /Drawing Competition on Cyber/Information Security

For more details visit
http://www.infosecawareness.in/contest

www.infosecawareness.in

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
Department of Electronics & 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.