Sept -Oct 2012

www.infosecawareness.in

Information Secuity Awareness

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

Infosec Tip

Watch out for fake email,it might be a "Phishing email" !!!!

Phishing is a technique to collect the personal information of a user through a trustworthy channel.

This technique is generally carried out by sending fake emails & redirecting to spoofed websites which look and feel similar to original sites, but in-fact they are not and prompt the users to enter personal information.This is also an example of social engineering techniques used to mislead users.

The following may be strictly adhered to ensure safety:

- Don't enter your information in the websites that start with numbers.
- Always key in the URL in the address bar yourself and don't click on the link given in the email or paste, the address
- Check for misspelled webiste address before you click on any link.

Some more TIPS

- ***Be cautious about opening any attachments or downloading files you receives regardless of who sent them.***
- ***Look for the senders email ID before you enter/give away any personal information.***
- ***Always update your web browser and enable phishing filter***
- ***If you receive any mail do call a company that you received a suspicious email from to see if it is legitimate or not.***
- ***Do use a separate email account for things like shopping online, personal, etc***
- ***Don't respond if you receive any message(sms) asking you to confirm account information that has been "stolen" or "lost" or encouraging you to reveal personal information in order to receive a prize, it's most likely a form of phishing.***

Infosec Quote

*The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it's easy to remember, it's something non random like 'Pappu.' And if it's random, like 'r7U2*Qnp,' then it's not easy to remember.*

— Bruce Schneier

Infosec Cartoon

Avoid filling forms that come through emails and ask for personal information

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

सी डैक
CDAC

Executed by :
Centre for Development of Advanced Computing
Hyderabad

Infosec Quiz

1. This is a method used to influence someone to give you confidential information either by convincing them you are someone who can be trusted or by just asking for it.
a.Social network b. password cracking c. persuasion d. none of the above

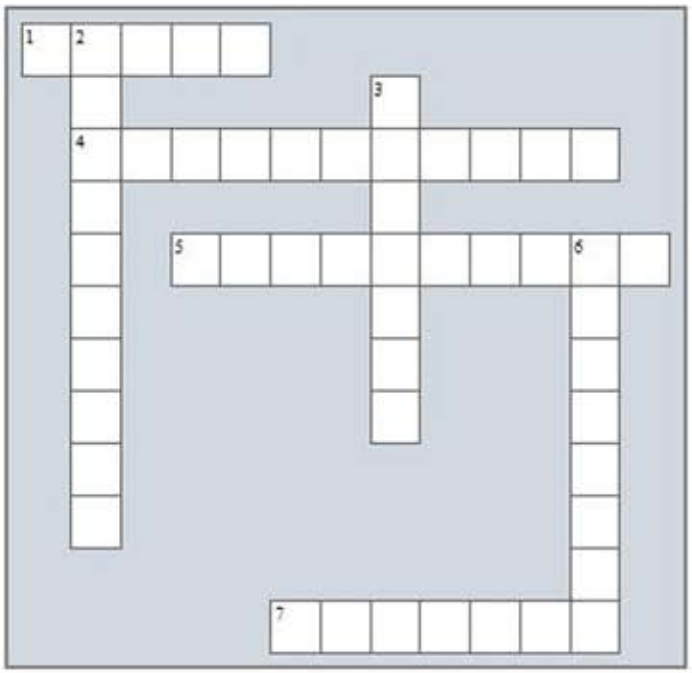
2. Spim is a
a. Spam through chat b. Spam through email
c. Spam through Mobile d. Spam through browser

3. Shoulder surfing is one of the method used to collect personal information
a. True
b. False

4. _____ is an attack involved in installing malicious code on your computer which may come through emails or email attachments.
a. Baiting b. Dumpster diving c. pharming d. none of the above

5. _____is a type of attack which causes your computer to crash or busy processing data, that you would not be able to use it.
a. Phishing b. Denial of Service c. Distributed Denial of Service d. Computer virus

Infosec Crossword



Across

1.____ is must for online banking and shopping
4.____ is a method used to send unwanted messages to the users with bluetooth-enabled mobiles devices
5.____ is a imitation of other thoughts and representing them as one's own work
7._____is the one of the method of social engineering

Down

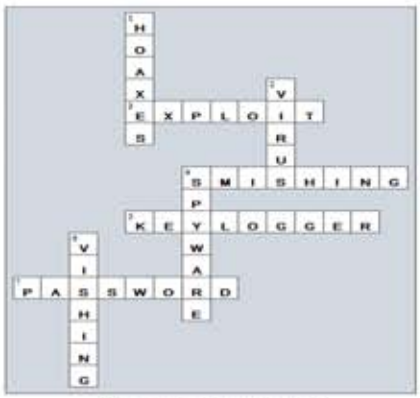
2.____ is a new type of phishing attack
3.____ gives extra functionalities to traditional web browsing but may also introduce more severe vulnerabilities if not properly implemented
6.____ is the theft of credtcard information

Last edition Contest Winners

Infosec Quiz Winners

Madhukar Saxena
Swaheeb Saikh
R Mukesh
K Ramakrishna

Last edition Contest Answers



Crossword Answers

1) a
2) a
3) c
4) c
5) a

Quiz Answers

Infosec Tools

Belarc Advisor

It builds a detailed profile of your installed software and hardware, network inventory, missing Microsoft hotfixes, anti-virus status and security benchmarks; and displays the results in your Web browser. Your PC profile information is kept private on your PC and is not sent to any web server.

- Operating Systems: Runs on Windows 7, 2008 R2, Vista, 2008, 2003, XP, 2000, NT 4, Me, 98, and 95. Both 32-bit and 64-bit Windows are supported.
- Browsers: Runs on Internet Explorer, Firefox, Safari, Opera, and many others.
- File size: 3123 KB.
- License: The license associated with this product allows for free personal use only. Use on multiple PCs in a corporate, educational, military or government installation is prohibited. See the license agreement for details.

Belarc's commercial products are used for software license management, hardware upgrade planning, cyber security status, information assurance audits, IT asset management, configuration management, and more.

For more details : http://www.belarc.com/free_download.html

Microsoft Baseline Security Analyzer 2.2

The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations.

Microsoft offers the free Microsoft Baseline Security Analyzer (MBSA) scan tool to easily assess the security state of Windows machines. . MBSA includes a graphical and command line interface that can perform local or remote scans of Microsoft Windows systems.

MBSA 2.2 builds on the previous MBSA 2.1.1 version that supports Windows 7 and Windows Server 2008 R2 and corrects minor issues reported by customers. As with the previous MBSA versions, MBSA 2.2 includes 64-bit installation, security update and vulnerability assessment (VA) checks and support for the latest Windows Update Agent (WUA) and Microsoft Update technologies. More information on the capabilities of MBSA is available on the MBSA Web site.

MBSA 2.2 runs on Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP and Windows 2000 systems and will scan for missing security updates, rollups and service packs using Microsoft Update technologies. MBSA will also scan for common security misconfigurations (also called Vulnerability Assessment checks) using a known list of less secure settings and configurations for all versions of Windows, Internet Information Server (IIS) 5.0, 6.0 and 6.1, SQL Server 2000 and 2005, Internet Explorer (IE) 5.01 and later, and Office 2000, 2002 and 2003 only.

MBSA will only scan for missing security updates, update rollups and service packs available from Microsoft Update To assess missing security updates. MBSA will not scan or report missing non-security updates, tools or drivers.

Choose the appropriate download below for English (EN), German (DE), French (FR) and Japanese (JA) for x86 (32-bit) or x64 (64-bit) platforms.

For more details :
http://www.microsoft.com/en-us/download/details.aspx?id=7558#additional-information

Infosec Concept

Broadband Internet Security

Internet is the channel to access vast pool of information & services available globally

Many home users use broadband Internet for accessing e-mail, online shopping, online banking, taking online courses, and many more. When the Internet connection is on, it is possible for other people to access our personal data by manipulating open ports on our computer.

Without our knowledge, computer can be compromised and it can be used as launching pad for carrying out disrupting activities on other computers. Traditional Internet services are accessed in "dial-on-demand" mode, whereas broadband Internet is an "always-on" connection, therefore risk is very high. Since broadband Internet has penetrated every walk of life, widely penetrated, it is very important for every citizen to securely configure it for safe usage.The broadband threats, types of broadband etc, are given below:

Broadband security threats

As broadband Internet connection is "Always On" , it leads to intentional misuse through

- Trojans and backdoors
- Denial of Service
- Intermediary for another attack
- Hidden file e xtensions
- Chat clients
- Packet sniffing
- Default configurations are extremely vulnerable

In addition, Anti-socialism groups use unsecured Wi-Fi networks to send terror e-mails.Prevent your wireless network to become such a hot spot by securing it.

Types of Broadband modem

- Wireless Fidelity (Wi-Fi)
- Digital Subscriber Line (DSL)
- Asynchronous Digital Subscriber Line (ADSL)
- Very high speed Digital Subscriber Line (VDSL)
- Cable Modem
- Satellite
- Broadband over Powerlines (BPL)
- Terminal Adapter Modem
- Universal Serial Bus (USB)

Broadband Modem Setup

Please do the following to carryout Broadband modem setup

- Always read the manufacturer's manual carefully and follow the guidelines, while setting up broadband modem.
- Insert the power source into the modem and then plug the other end of it into the wall socket
- Before connecting the modem to the computer, check for propper functioning of the computer
- While setting up the modem, follow instructions specific to the modem type
- In case of signal via cable, connect the modem with the provided cable wire
- In case of ethernet, connect the modem to the computer with ethernet port
- In case of USB, connect the modem after the computer is properly initialised
- Wait until the indicators on the modem are lit
- Install the modem driver and associated software provided along with the modem
- To initialize the connectivity we need to submit the user credentials and wait for the response

Points to remember for Broadband Security

- Use effective end point security solution (with anti virus, anti spyware, desktop firewall etc) to protect computer/ laptop from broadband Internet security threats
- Enable Firewall on Modem Router as well as Computer
- Broadband modem routers contain built-in firewall feature, but this option has to be enabled. Computer connected to the broadband modem also needs to be protected with desktop firewall
- Turn off Network during extended periods of Non-Use
- In case of USB broadband modem, disconnect and remove the device after usage
- Install broadband Internet bandwidth usage monitoring tool
- Enable SSH (secure channel) for remote administration

Guidelines for Securing Broadband Internet Access

Do's

- ✔ Always download broadband drivers from th legitimate websites recommended by the manufacturer.
- ✔ Regularly download the firmware (driver code) updates
- ✔ Always use the power adapter supplied by the manufacturer along with the modem
- ✔ In case of terminal adapter modem make sure that filter is enabled for broadband lines. This helps to filter unnecessary noise added during the transmission

- ✔ ***Change Default Administrator (Passwords and User names)***
  Change the default administrator or admin password of broadband router modem, as these details are given by the manufacturer which can be misused by anyone.
- ✔ ***Assign Static IP Addresses to Devices***
  Most of the home users are assigned dynamic IP addresses, as DHCP technology is easy to setup. This convenience even helps the attackers also who can easily obtain valid address from DHCP pool. Therefore turn off DHCP option in the router or access point and use fixed IP address range.
- ✔ ***Enable MAC Address Filtering***
  Every device is provided with an unique MAC address. Broadband access points and routers provides an option for the user to add the MAC addresses of the home equipment. This helps to allow connections only from those devices.
- ✔ ***Enable Wireless Security***
  Modem routers support wireless security.User can select any one of the protocols and a protection key. The same wireless security protocol and protection key has to be enabled in computer.
- ✔ ***Turn on (Compatible) WPA / WEP Encryption***
  All Wi-Fi equipment supports some form of encryption technology, which has to be enabled.
- ✔ ***Change the Default SSID (Service Set Identifier)***
  All the access points and routers use a network name called SSID. Manufacturer normally ships their products with the same SSID set. As it can be misused by the attacker to break into the network / computer, it is necessary to change the default SSID while configuring wireless security

Dont's

- ✘ Don't enable the option for remote administration (via Internet), as it is not required for a home user
- ✘ Don't enable the option "Restore Factory Default Setting" in broadband modem
- ✘ Don't use connection without a filter for each broadband Internet line
- ✘ Don't tap the line before the splitter (a small dvice that separates phone line from data / PC port)
- ✘ Don't use USB broadband modem with insecure computer / laptop
- ✘ Do not leave broadband connectivity open when it is not utilized
- ✘ Never connect to unkown or untrusted network in case of Wi-Fi

- ✘ ***Do not enable SSID Broadcast***
  In Wi-Fi networking, wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals.This feature was designed for businesses as well as to access public hotspots. For a home user this feature is unnecessary and can be an entry point to break into the network
- ✘ ***Do not enable Auto-Connect to Open Wi-Fi Networks***
  In case if Auto-Connect setting is enabled, computer can connect automatically without notifying to the user.This may expose our computer to security risks.This setting should not be enabled except in specific cases

For more details logon to :
http://infosecawareness.in/sysadmin/broadband-security

Infosec News

Hackers targeting Indian banks with advanced SpyEye, Zeus malware variants

After targeting financial institutions in Europe, hackers are now increasingly targeting Indian financial institutions with the latest variants of malware like SpyEye and Zeus to siphon larger amounts of money from bank accounts, Japanese security company Trend Micro has cautioned.After targeting countries like Germany, Italy and United Kingdom, cyber criminals are now targeting Indian cities, with the highest number of phishing strikes being reported in cities like Hyderabad, Nashik, New Delhi and Bangalore and even Thanjavur, said Trend Micro, which has many banks as customers.

With a whopping 187 per cent rise in phishing attacks being reported on various Indian brands in May this year over the previous month, the Japanese global cloud security company pointed out that significantly, all phishing attacks on Indian brands in May targeted the banking sector, with one in every four using an '.in' domain and the top cyber threats created specifically to target bank balances.

"The new software allows the criminal to siphon money out while he sleeps. It could significantly increase the number of hacked accounts and the speed with which they are drained," said Trend Micro's country manager (India and SAARC) Amit Nath.

"The new code has the potential to dramatically escalate the amount being stolen from accounts and a years-old arms race between the banks and criminal groups. This has tremendous implications especially as masses are moving towards banking by phone. This attack toolkit ushers in a new era of bank heists," he added.

According to a Trend Micro report on 'Automating online banking fraud-- automatic transfer system: the latest cybercrime toolkit feature', two of the most pervasive and dangerous types of software for stealing money from bank accounts - SpyEye and Zeus - have been improved and enabled to transfer money out automatically, without a hacker's supervision and have already stolen hefty amount at a time from a single account and are in the early stages of deployment.

The programs have already used a technique called "web injection" to generate new entry fields when victims log on to any number of banks or other sensitive websites, said Trend Micro, pointing out how instead of seeing a bank ask for an account number and password for instance, a victimized user sees requests for both of those and an ATM card number. Everything typed in then gets whisked off to the hacker, who later signs in and transfers money to an accomplice's account.

For the past year or more, some variants have also captured one-time passwords sent from the banks by text messages to client cell phones as an added security measure. But in those cases, a hacker had to be online within 30 or 60 seconds in order to use the one-time password, the report pointed out.

Source:http://articles.timesofindia.indiatimes.com/20120626/hyderabad/32424458_1_phishing-attacks-bank-accounts-indian-banks

Google: We Find 9,500 New Malicious Sites Every Day

It's no secret that the Web is full of malicious content, but Google published some statistics that reveal just how breathtaking the scale of that danger really is.In fact, Google uncovers some 9,500 new malicious websites every day through its Safe Browsing initiative, according to a blog post from Google Security Team blogger Niels Provos.

"These are either innocent websites that have been compromised by malware authors, or others that are built specifically for malware distribution or phishing," Provos explained. "While we flag many sites daily, we strive for high quality and have had only a handful of false positives."

Not only that, but between 12 and 14 million Google Search queries every day return results that include at least one hacked site, Google says. A full 300,000 downloads per day, meanwhile, get flagged with a warning through Google's download protection service for Chrome."The threat landscape changes rapidly," Provos wrote. "Our adversaries are highly motivated by making money from unsuspecting victims, and at great cost to everyone involved."

'Sophisticated' Phishing

The details behind some of these new statistics are illuminating.In the realm of phishing, for instance, many attackers continue to emphasize online commerce sites like eBay and PayPal, Provos noted. Their methods, however, are becoming more creative and sophisticated.Many phishing sites remain online for less than an hour so as to avoid detection, for example; such sites are also becoming more diverse and are increasingly used to distribute malware, he added.

Social Engineering on the Rise

Focusing on malware, Google's Safe Browsing effort identifies two kinds: legitimate sites that are hacked on a mass scale to deliver or redirect to malware--often via "drive-by downloads"--and attack sites that are specifically built to distribute malware."As companies have designed browsers and plugins to be more secure over time, malware purveyors have also employed social engineering, where the malware author tries to deceive the user into installing malicious software without the need for any software vulnerabilities," Provos explained."Fake Anti-Virus" alerts, for example, masquerade as legitimate security warnings even as they infect the user's computer with malware.

Socially engineered attacks are not yet as common as drive-by downloads, but they're "a fast-growing category likely due to improved browser security," Provos said.

For more:http://www.pcworld.in/news/google-we-find-9500-new-malicious-sites-every-day-75862012

Infosec News

DDoS attacks on Indian websites

It is observed that some hacker groups are launching Distributed Denial of Service attacks on websites of Government and private organizations in India. The attacks may be targeted to different websites of reputed organizations.
These attacks are being launched through popular DDoS tools and can consume bandwidth requiring appropriate proactive actions in coordination with Service Providers.
The network administrators may keep vigil on traffic and any abnormal raise in traffic levels may be reported to CERT-In (incident@cert-in.org.in) immediately.

Actions prior to attacks:

- Identify critical services and their priority. Develop Business Continuity Plan.
- Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks.
- Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common DDoS tools.
- Maintain list of contacts of ISPs. Vendors of network and security devices and contact them as appropriate
- Understand your current environment , and have a baseline of the daily volume. Type, and performance of network traf fic.
- Implement Egress and Ingress filtering at router lebel.
- Implement a bogon block list at the network boundary.
- Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic,network level floods (TCP, UDP, SYN, etc) and application floods (HTTP GET)
- Maintain and regularly examine logs of webservers to detect malformed requests/traffic.
- In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.

Action To be taken if attack occurs:

- Identify the type of attack such as flooding of paricular types of packets/requests (TCP SYN, ICMP, HTTP GET etc) by examining logs of network and security devices such as Router / IPS / IDS / Firewall or DDoS attack Prevention Solu tions
- Identify the attack sources.
- Block the attack sources at Router/Packet filtering device/DDoS prevention solutions.
- Disable the non essential ports/services.
- Preserve all logs indicating type of attack and attack sources.
- In case of high volume of DDos, consult your ISP to block attack sources and apply appropriate rate limiting strategies.
- Allocate traffic to unaffected available network paths, if possible, to continue the services.
- Consult your Business Continuity Plan for appropriate actions in case critical services are affected.

Source:http://www.cert-in.org.in/SecurityIncident.jsp

Is your printer spewing gibberish? Could be malware

Malware that is triggering massive print jobs is found primarily on computers in the U.S. and India, but other countries in Europe and South America as well.
Over the last few weeks, companies around the globe have been reporting that their print servers are emptying paper trays by printing endless pages of meaningless characters. Symantec now says malware may be to blame.
Dubbed Trojan.Milicenso, the malware targets Windows-based computers and can spread through malicious e-mail attachments or visiting Web sites hosting malicious scripts, including fake codecs, Symantec said in a blog post yesterday. It has infected computers primarily in the U.S. and India, but also in Brazil, the U.K. and other countries in Europe and South America.
"Our telemetry data has shown the worst hit regions were the US and India followed by regions in Europe and South America," Symantec said. "We originally encountered Trojan.Milicenso in 2010 and our initial investigation had shown that this was basically a malware delivery vehicle for hire. The payload that is most commonly associated with this latest version is Adware.Eorezo; an adware targeting French speaking users."
Although the malware appears to have been designed to direct computers to pages that have advertisements, a side effect in some networks is that it triggers massive print jobs. "Based on what we have discovered so far, the garbled printouts appear to be a side effect of the infection vector rather an intentional goal of the author," according to Symantec.

Source:http://news.cnet.com/8301-1009_3-57459098-83/is-your-printer-spewing-gibberish-could-be-malware/

Infosec Virus Alerts

sKyWIper/Worm.Win32.Flame

It has been reported that a new attack toolkit is propagating in some Middle East countries. This attack toolkit is named as "Flame" by Kaspersky Labs, "sKyWIper" by Laboratory of Cryptography and System Security (CrySyS Lab) & McAfee, "Flamer" by Symantec & ESET.

sKyWIper/Flame is designed with advanced functionality for information stealing and propagation. It is reported that the malware contains multiple exploits and propagation methods which could be configured by its master/attacker. It could be propagated via removable media and local area network shares. As per analysis by CrySyS Lab sKyWIper also uses print spooler exploit (MS10-061) (CIVN-2010-0199) and lnk exploit (MS10-046) (CIVN-2010-0169) for spreading over network. It is also suspected that it may contain exploit for vulnerabilities in Media Decompression (MS10-033) (CIVN-2010-0148).

sKyWIper/Flame is capable of performing several complex operations including network traffic sniffing, Scanning network resources, collecting lists of vulnerable passwords, capturing screen, capturing video, recording audio, capturing keystrokes, scanning disk for specific file extension & content, and information stealing. If Bluetooth is available, it could collect information about discoverable devices in range of infected system. Information captured is available to the sKyWIper master through the link to sKyWIper's (C&C) servers. It is reported that the malware uses more than 50 domains as C&C servers. It communicates with C&C server over SSH and HTTPS protocols.

The malware can detect the presence of over 100 security products (Antivirus, Antispyware, Firewall etc). sKyWIper employing complex internal functionality using Windows APC calls and threads start manipulation, and code injections into Internet Explorer, services and other key processes. It is Loading as part of Winlogon.exe. It creates ~ named temp files, It uses SQLite database to store collected information and a custom database for attack modules. sKyWIper uses compression and encryption techniques to encode its files.

Primarily the malware is infecting Windows XP, Vista and Windows 7 operating systems. sKyWIper does not modify too many registry keys as most information, data, configuration are stored in files. The affected registry entries are the following:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Autenthication Packages will contain in new line mssecmgr.ocx:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]"Authentication Packages"=hex(7):6d,00,73,00,76,00,31,00,5f,00,30,00,00,00,6d,\
00,73,00,73,00,65,00,63,00,6d,00,67,00,72,00,2e,00,6f,00,63,00,78,00,00,00,\00,00

Some of the Malware binaries observed are:

windows\system32\mssecmgr.ocx
Windows\System32\ccalc32.sys
Windows\System32\msglu32.ocx
Windows\System32\boot32drv.sys
Windows\System32\nteps32.ocx
Windows\System32\advnetcfg.ocx
Windows\System32\soapr32.ocx

Recommendations/Countermeasures:

- Maintain updated Antivirus on desktop and gateway level
- Monitor encrypted/SSL traffic to untrusted websites and block the same
- Isolate suspected systems from network and report the same to CERT-In
- Exercise caution while opening e-mail attachments received from unknown sources.
- 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
- Maintain all applications such as MS office, Adobe reader/Flash, Browsers, media players etc updated with latest patches

Source:cert-in.org.in

Infosec Virus Alerts

Virus ACAD/Medre.A

It has been reported that an industrial espionage tool dubbed as ACAD/Medre.A, targeting AutoCAD files is propagating. The malign application is written in AutoLisp and VBS, and arrives generally as hidden acad.lsp alongside AutoCAD drawing files(*.dwg), that automatically loads when a drawing is opened.
Once successfully installed the malware steals AutoCAD files and drawings among others such as email client files OUT-LOOK .PST files, Foxmail, and exfiltrate to email addresses (hardcoded).

Aliases:

ALisp/Blemfox.A (Microsoft), Trojan.Acad.Bursted.W (BitDefender), Virus.ALS.Bursted (Kaspersky), ALS/Bursted (McAfee), ALS.Bursted.B (Symantec), ACAD/Bursted (Avira), AL/Bursted-A (Sophos)

Activites:

Creates the following files:
%windir%\System32\Acad.fas
%windir%\ Acad.fas
%current_working_directory_of_DWG%\cad.fas
%current_ working_directory_of_DWG%\acad.fas
%ACAD_support_directory%\cad.fas
%ACAD_support_directory%\acad.fas
Steal AutoCAD drawings , email client files and snoops to pre-configured email address over to smtp.163 .com and smtp .qq.com (TCP/25)
Creates a password protected (password=1)RAR-file containing the drawing and the requisite "acad.fas" file and a ".dxf" file and send it separately by e-mail.

Recommendations:

- Care must be taken while opening archive files from unknown users.
- Never run an unknown AutoLISP file or VBA macro without inspecting it first
- Enable the macro virus protection in AutoCAD
- Search for acad.fas or cad.fas files that may indicate the presence infection
- Search for the acad.fas from the AutoCAD command line by typing (findfile "acad.fas"), including parenthesis.
- Monitor unnecessary SMTP ports.

For more details:
http://usa.autodesk.com/adsk/servlet/ps/dl/item?siteID=123112&id=13717811&linkID=9240617

Phishing attacks on Indian businesses grow by 187%

The number of phishing attacks on Indian companies and brands have seen a sharp increase recently. According to Symantec, in May 2012, it was observed that a whopping 187% rise over the previous month in phishing attacks on Indian brands, all of which were in the banking sector. While these attacks originated around the world, Hyderabad hosted the second highest number of phishing attacks on Indian brands.

Hyderabad also topped the list of cities for May that hosted phishing sites in India of non-Indian brands followed by Nashik, New Delhi and Bangalore in the 3rd and 4th place respectively. Hyderabad was at 7th place in April and Thanjavur has been featured in this list for the first time.

India is not only positioned higher than the global average as a target for spammers but is also the top source of spam globally.
The Symantec report also observed that globally the Defense industry has been the targeted industry of choice in the first half of the year, with an average of 7.3 attacks per day.

According to Computer Emergency Response Team India (CERT-In), some hacker groups launched Distributed Denial of Service attacks on websites of Government and private organizations in India. The attacks are being launched through popular DDoS tools.

http://timesofindia.indiatimes.com/business/india-business/Phishing-attacks-on-Indian-businesses-grow-by-187/articleshow/14852173.cms

Infosec Workshops


@Hyderabad


@Bangalore


@Jammu


@Sikkim

@Pune

Infosec Workshops

TEACHERS & PARENTS

@Gorakpur @Megalaya

STUDENTS

@Chandigarh @Assam

OFFICERS

@Lehragaga, Punjab @Kolkata

Users Views on the Cartoon – Guess Tip Contest

Please do not open files with file extensions (.exe, .vbs, .shs, .pif).

Please delete them immediately

-VSMurthy

Do not trust the downloaded script files, which may harm your system. Trash the files immediately.

-Rema Narayan

Wake up Users! Delete the unknown attachments while down-loading and beware of the above extensions.

-Ritu Anand

Delete online documents with unknown extensions without opening as they may contain hidden viruses

-Tripteela

User feedback on web portal

Content Provided	Look & Feel	Navigation	Usefulness	Flow of the content
Excellent	Good	Good	Excellent	Good

Great to go through such a good site. Thank you
By Anoop

Excellent	Excellent	Excellent	Excellent	Excellent

Nice work keep it up
By Ashwini Shirke

Average	Good	Good	Good	Good

More IT security related posters to be provided
By Ashish Gupta
Indian Navy

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

Comments & Feedback
mail us at isea@cdac.in

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

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

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 and 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