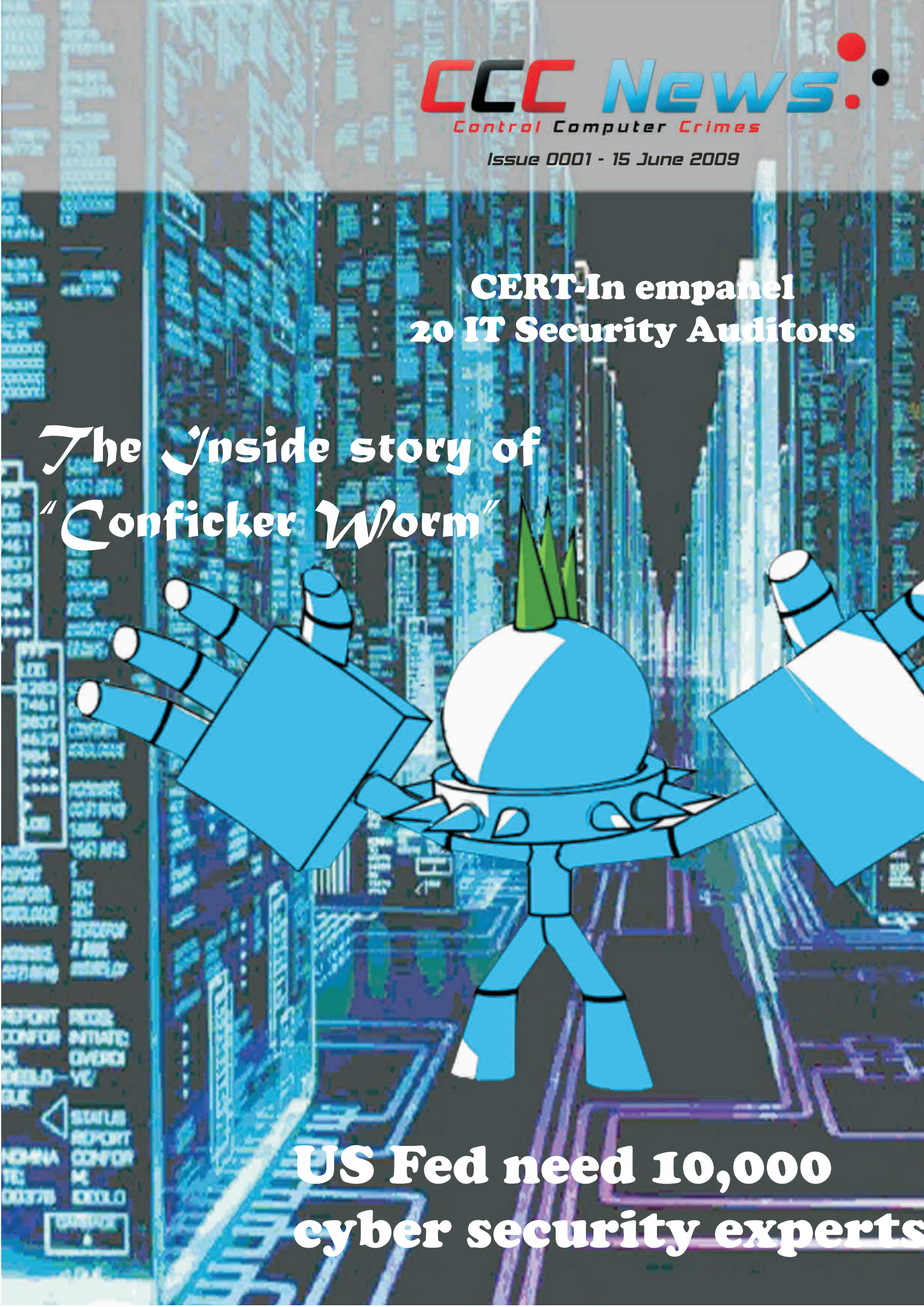
CCC News
Control Computer Crimes
Issue 0001 - 15 June 2009



CERT-In empanel 20 IT Security Auditors

The Inside story of "Conficker Worm"

US Fed need 10,000 cyber security experts

EDITOR's MESSAGE

This gives me great pleasure to introduce the CCCNews Magazine to the world.

Today, we have completed 4 years of publication of Control-Computer-Crimes Newsletter, which since June 2005, has crossed the publication of over 700 issues, every Monday, Wednesday and Friday. This is published under the auspices of CRPCC.

Today, we have over 85,000 direct subscribers and constituents, who receive the Control-Computer-Crimes Newsletter, 3 times a week. Many of the recipients circulate the newsletter further in their groups and organizations, so that more people can get benefit. We estimate the final readers tally may cross 150,000.

The ***CCCNews Magazine*** is the outcome of our 4 years efforts, learning, education and experience of publishing Control-Computer-Crimes Newsletter. The launch of CCCNews Magazine is the outcome of success of Control-Computer-Crimes Newsletter and persistent encouragement from readers. The 'CCC' in the CCCNews is derived from Control-Computer-Crimes.

The mission of the CCCNews Magazine is to create awareness about computer security, for which one must know the phenomenon of computer crimes (also known as cyber crimes, though cyber crime is a sub-set of broader term computer crimes) and how to protect oneself from the unrelenting attacks from computer criminals and perpetrators of computer crimes.

The incidents of Hacking; Phishing; 419/Advance-fee Frauds; Attack of Virus, Worm, Spyware, Malware; Botnet; ID theft; cyber wars; etc. are growing exponentially and have reached a juncture that these have surpassed the classical crimes in the physical world. Further, Computer Crimes are getting converge with organized crimes and a new Frankenstein is already created. Conficker is one such example.

Last year, we have witnessed the cyber attack and crippling of Estonia. Today, cyber attacks are order of the day. In the last one week, cyber attacks in the form of DDOS attacks were launched against Iran, South Korea, Belarus and Israel. Wireless are being hacked; banks are defrauded / looted; credit card, bank account, IDs are stolen on daily basis.

The risk has already reached dangerous threshold and is increasing day-by-day.

Thus, every user need to protect oneself from various computer crimes (includes cyber attacks) on continuous basis as one need to protect their own assets by not only properly locking the house but with other modes of surveillance; or protect oneself from rains, using umbrella or rain-coat or other-devices; or be extra cautious while crossing the busy road.

With this background, we at CRPCC and CCC Media, present you the first issue of CCCNews Magazine, with a request to update you constantly for your own protection against Computer crimes before it is too late.

This issue is just a start. We will be constantly upgrading and adding new features in future issues for your more protection.

Wish you a Safe and Secure Journey on Cyber Highway,

Rakesh Goyal
Editor

CCC News.

Issue 0001
15th June 2009

Rakesh Goyal
Editor
editor@cccnews.in

Moiz Mamoowala
Marketing & Sales
moiz@cccnews.in
+919769887077
+919967247000

Published by
CCC Media,
Mumbai, India

Index

US Fed Need 10,000 Cyber Security Experts

The head of the DoD-sponsored Digital Forensics Challenge said that contests like this will help the U.S. government find the talent it needs.

Secretary of Defense Robert Gates said earlier this year that the Department of Defense (DoD) must be able to train 200 cyber security experts, up from 80 now. How about the whole U.S. government?

There's a clear need in agencies as diverse as energy, aviation, and, of course, defense.

"We are conducting a national competition and talent search to find 10,000 security experts for the entire government," James Christy, director of future exploration (FX) at the Defense Cyber Crime Center (DC3) and a former security officer in the Air Force told InternetNews.com.

He added that the original plans, which called for a national cyber Olympics, have been scaled back but that existing contents, such as the DC3's Digital Forensics Challenge, which he runs, are expanding.

"Anybody can apply but only U.S. citizens in the continental U.S. can win," he said. He explained the rule was originally instated four years ago when the program had little money and could not afford plane fare for people from Alaska or Hawaii.

Last year, the challenge had 199 participants, 19 of which submitted solutions. This year, 389 teams have already registered and the deadline for submitting solutions is November 2, 2009, so additional teams can register.

"The winning team, up to four members, gets a trip to our conference in St. Louis and we give them a plaque and then they have the opportunity to present their solutions to the group."

A separate award for teams from high schools is sponsored by the SANS Institute (SysAdmin, Audit, Network, Security), he added.

A third award is sponsored by members of CyberWATCH, a group of schools located in Maryland and Virginia that will hold their first digital forensics training session on June 15 at the University of Maryland, College Park.

That CyberWATCH training session illustrates why the government is sponsoring the contest. "The whole idea is to develop new tools and technology and to get people more excited about the field and sharing information about it," said Christy.

He acknowledged that some in the intelligence community would prefer that information not be shared. "I see it as a question of defense versus offense. And as a cop, I think defense comes first," he said.

He added that a few years ago someone in the intelligence community told him that they were upset that a specific CD cracking technique was made public during the challenge because the intelligence community had known about it for years and had been using it.

"I said, 'you didn't tell us that.' When we don't know things, we have to re-create the wheel. We don't do that. We share information with law enforcement and with the digital forensics community," he said.

Because technology changes so fast, keeping secrets serves no purpose. "The shelf life of these techniques is so short that they're obsolete in a year or two," Christy said. Sharing information helps victims, which is "defense." Not sharing information helps the intelligence community compromise enemy systems, which is "offense."

Christy encouraged anyone who is interested to apply. He said the team can evaluate 100 solutions but does not expect to receive that many. "We tell them to submit them early but they generally submit them they day before they're due because they cannot solve them all," he said. "Some are pretty hard."

Challenges are ranked in four levels: 100 for novice, 200 for skilled, 300 for expert and 400 for genius. Some challenges are things that the government would like to be able to do better or faster and others feature riddles the government has been unable to crack. Others are challenges that the government understands well but believes should be a part of any Digital Forensics curriculum.

At press time, participating teams included 10 high school student teams, 61 undergraduate student teams, 28 graduate student teams, 194 individuals, 28 corporate teams, 20 government teams and 17 military teams. Participants were from every state except four: New Mexico, South Dakota, Wyoming and Montana. International teams came from places as diverse as India, Svalbard, Argentina, New Zealand and Chad.

Source : June 7, 2009 By Alex Goldman, www.internetnews.com

CERT-In empanel 20 IT Security Auditors to secure critical IT infrastructure

CERT-In has empanelled 20 IT Security Auditing firms for carrying out IT Security audits including Vulnerability Assessment and Penetration Testing (VAPT) of networked IT infrastructure of various organizations of the Government, critical infrastructure organizations and those in other sectors of the Indian economy.

This empanelled has been done after an on-line hacking test, which was the last stage of three stage selection process. This empanelment is valid for three years till April 2012 with a provision for annual reviews.

The first stage was based on the credentials and client recommendations. Those selected in first stage was provided with an off-line test for which minimum qualifying criteria was 90% score. About 30 firms passed the second stage. The third stage was a online VAPT test with minimum pass criteria as discovery of 75% of vulnerabilities.

"Testing of competency of Auditing Organisation will go a long way to ensure National Security", says Ashish Saxena of AKS Information Technology Services Private Limited, a Delhi based empanelled firm.

By this process CERT-In has ensured that only those firms, which are competent and ethical are empanelled to address the IT security requirements of critical government and public It infrastructure.

Shashin Lotlikar of ISAAC Private Limited, a Mumbai based empanelled firm is pleased with the selection process and says "Cert-in has separated wheat from chaff with this rigorous process. We enjoyed the tests and learn a lot".

"To protect the National Information Assets of the Country, Qualified and Capable Information Security Auditors are required. CERT-In is Judging and forming a pool of such Information Security Auditors", says Anjay Agarwal, CMD of AAA Technologies Private Limited, another empanelled audit firm from Mumbai.

Sysman Computers Private Limited is another Mumbai based empanelled IT Security Consulting firm.

The process was conceived by Dr. Gulshan Rai, Director-General of CERT-In and was managed by team led by Mr. Omveer Singh, Jt. Director under the direct supervision of Mr. B J Srinath, Sr. Director – CERT-In.

Source : 15 June 2009, CCC News

China to use software on all PCs to block sites

The Chinese government has required that personal computer makers bundle software that filters Internet content from July 1, raising concerns over cyber-security as well as Internet freedoms.

The free "Green Dam-Youth Escort" software, developed by Jinhui Computer System Engineering Co, can effectively filter "unhealthy words and images", according to a Ministry of Industry and Information Technology document seen by Reuters.

Foreign computer makers are now caught between maintaining access to their fastest-growing major market, and concerns the mandatory software will make their products vulnerable to security breaches as well as potential malfunctions.

The requirement to pre-install the software is "in order to consolidate the achievements of the online campaign against pornography, combine punishment and prevention, protect the healthy growth of young people, and promote the Internet's healthy and orderly development," the ministry said.

Many aspects of the software are still unknown, but computer industry sources worry it could open a channel for industrial espionage as well as blocking content Beijing dislikes.

China already has a system to block websites deemed objectionable. Internet police monitor sites, blogs and other online venues for pornographic or politically sensitive content.

"Summer vacation is coming up, and many Chinese parents worry about what their children will see on the Internet. That's the purpose of the software," Jinhui founder Bryan Zhang said.

"Even if you wanted to use it for, say, political content, you couldn't, because it's image distinction software that tracks

PC makers must report to the ministry the number of computer units sold and software packages installed on a monthly basis in 2009, and yearly starting in February 2010, the circular says.

"Using the software is not compulsory. You can shut it down or take it out if you want to. With a password, you can turn it off at any time," Zhang said.

"It's an optional tool to prevent access to pornography, just like anti-pornography software in the United States."

An industry official, who did not want to be identified for fear of retaliation against his company, said foreign technicians testing the software had been unable to uninstall it.

The Wall Street Journal first reported the news on Monday.

China is one of the world's fastest-growing PC markets, with research firm Gartner forecasting total PC shipments will climb by about 3 percent this year to more than 42 million units.

The Chinese market is dominated by homegrown brands such as Lenovo and Founder, although global brands such as HP, Dell and Acer also have a significant market share.

Acer said it was not aware of the new requirement, while rival Taiwanese maker Asustek said it was but had not yet been officially informed by the Chinese government.

"Along with the rest of the industry ... we are studying it and working with relevant government and other parties to seek clarifications," said Dell spokeswoman Faith Brewitt.

Jinhui last year won a tender to supply filtering software to the ministry, according

to government procurement information.

Since then, the ministry has subsidised the company to make the software available for free downloads, said Zhang. It previously sold for 368 yuan (US$54) a package.

The software will remain free for a year, and after that consumers will have to pay to continue using it, Zhang said.

It has already been bundled in over 50 million locally made PCs offered rural dwellers as part of China's economic stimulus package, according to a promotional website (www.lssw365.net).

It said the software is being used by 2,279 schools across China and had been downloaded 3.27 million times by end-March.

The U.S. embassy in Beijing said it was concerned.

"We would view any attempt to restrict the free flow of information with great concern and as incompatible with China's aspirations to build a modern, information-based economy and society," an embassy spokesman said.

Compliance could leave computer manufacturers open to charges they abetted censorship and violation of privacy.

The software has a "black list" of sites with pornographic or violent content it blocks, said a customer service representative affiliated with a website offering the software for downloading.

The software also has a "white list" of permitted websites. Users can add or delete websites from the white list. While the white list is publicised, the black list is not.

Savvy Internet users in China currently stay one step ahead of censors by using virtual private networks or proxy servers to access sites outside China, and spread information domestically by quickly reposting expunged content or using oblique language.

Pornography is easily accessed on the Chinese Internet.

Source : 9 June 2009, By Lucy Hornby, www.itnews.com.au

Hacker breaks into Ex-Minister's mail

NEW DELHI: Last week it was fashion designer Rina Dhaka, on Wednesday, hackers targeted former Union minister **Mani Shankar Aiya**r's email account.

All those on the address book of Aiyer's Hotmail account received a mail, supposedly from the politician, asking for monetary help as he had "misplaced his wallet".

"The modus operandi is the one that has been in use for the last two years. A JNU professor travelling abroad was the first to be targeted. The victim's travel details are usually provided by a known person to the accused,'' said a senior economic offences wing official. He said he was yet to receive a complaint from the former minister.

According to sources, e-mails started originating from the leader's Hotmail account on Wednesday to all in his address book stating that he had misplaced his wallet in England and was in urgent need of $ 3,500 to clear his hotel bills and get himself back home.

"I am sorry that I didn't inform you about my traveling to England for a seminar. I need a favour from you as soon as you receive this email because I misplaced my wallet on my way to the hotel. I will like you to assist me with a loan urgently," the mail signed off by Mani, as his friends call him, said.

It added, "I will be needing the sum of $3,500 to sort out my hotel bills and get myself back home. I will appreciate whatever you can afford to help me with, I will pay you back as soon as I return."

When contacted, Aiyar who is in New York confirmed that his e-mail account had been hacked and asked people to `avoid' it. "Unfortunately the hacker changed my password so I cannot access my account. I am in New York attending a seminar at Columbia University. I request all recipients to ignore this mischievous message," Aiyar told agencies.

Meanwhile, alarmed with the rising number of white collar crimes in which hackers have targeted well placed individuals, the Delhi Police has issued an advisory to netizens urging them to protect themselves from organised cyber criminals. In addition, the crime branch has also issued a separate advisory to check credit card frauds.

Crime branch officials said among the guidelines issued for net users, the most important one was to ask users to create a strong password. "The password ideally should be of 10 characters consisting of alphabets, digits and signs. The usual dates of birth, vehicle numbers and names of immediate relatives can be avoided,'' said Satyendra Garg, joint CP (operations).

The police have also asked citizens to avoid responding to spam mails. "Checking the authencity of any offer through search on the internet and by personally asking the company concerned is also a must,'' said Rajan Bhat, PRO, Delhi Police.

Senior officials said the process of setting up a white collar crime cell in each district to investigate such cases

would take time as there were not enough trained officials. The EOW, which deals with cyber crimes, had received 3,241 complaints last year among which 781 cases were investigated.

Source: 11 Jun 2009, by Dwaipayan Ghosh, www.timesofindia.indiatimes.com

List of Sites Banned in India

List of sites that the Government of India's Department of Telecom banned with its 13th July 2006 circular:

1. Http://www.soniamaino.com (since Aug 25, 2006)
2. http://www.hinduunity.org
3. http://mypetjawa.mu.nu
4. http://pajamaeditors.blogspot.com
5. http://exposingtheleft.blogspot.com
6. http://thepiratescove.us
7. http://commonfolkcommonsense.blogspot.com
8. http://bamapachyderm.com
9. http://princesskimberley.blogspot.com
10. http://merrimusings.typepad.com
11. http://mackers-world.com
12. http://www.dalitstan.org
13. http://hinduhumanrights.org/hindufocus.html
14. http://nndh.com (fax scan unclear, could be wrong)
15. http://bloodroyaltriped.com
16. http://imagessearchyahoo.com (http://image.search.yahoo.com)
17. http://imamali8.com
18. http://rahulyadav.com

From Censorship Wikia, the free censorship database Http://censorship.wikia.com/wiki/List_of_Sites_Banned_in_India

Katrina Kaif, Most Dangerous Search Term

According to a new study entitled "The Web's Most Dangerous Search Terms" by Security Company McAfee, 'Katrina Kaif,' the Bollywood actress is the search keyword for the most poisonous and dangerous results that could effectively upload malicious software onto users' computers.

Reveals McAfee that search requests pertaining to Katrina's name could generate results that associate with various Internet scams and malware.

As a matter of fact, the keyword 'Katrina Kaif' is associated with the highest risk rate of 28.6% meaning that the highest rate of dangerous websites that appear among the first ten search results for 'Katrina Kaif' is 28.6%. This rate is only slightly lower than 'Wapstick,' a widely-used site that offers non-chargeable downloads of ring tones, music, logos for cell-phones, animations and wall paper.

Moreover, keywords associated with the star might also be employed to take down 'ransomware' or 'scareware' that ultimately prompts the victim for a software purchase that supposedly unlocks his computer or cleans it off malware.

Research Analyst Shane Keats at McAfee and Software Development Engineer Eipe Koshy also at McAfee say that hackers or other cyber-criminals are getting more and more sophisticated about using SEO (search engine optimization) to entice unwitting users into taking down dangerous software online. Ibtimes.co.in published this on June 1, 2009.

The two experts note that hackers' greatest success is in pulling a huge crowd of victims. A particular tactic to target numerous people on the Internet is to chase current events such as natural disasters, economic meltdown, celebrities, popular music and holidays, while a chief tool that cyber-criminals employ to trap victims pertains to making the latter download a software or computer file that is laced with malware.

Meanwhile, other frequently used keywords with a high percentage of risk in India are Yahoomail, Orkut, Rediffmail, Shimla, Shahid Kapur, Namitha, Beijing 2008 Olympic Games and 'How to earn money.' In truth, different countries have different vicious, poisonous and dangerous keywords, notes McAfee.

Finally, McAfee warns that Katrina Kaif screensaver could introduce computer viruses in users' systems. Hence users must exercise caution while downloading freely obtainable screensavers that relate to Katrina or other celebrities.

Source: 05 June-2009 www.spamfighter.com

Man made $112,000 in bank account hacking scheme

He pleaded guilty to laundering money siphoned from Schwab accounts

A Hampton, New Hampshire, man has pleaded guilty to fraud charges for his role in a scheme to empty brokerage accounts by installing malicious Trojan horse software on victims' computers.

According to court documents, Alexey Mineev set up several "drop accounts" that were then wired funds stolen from banking and brokerage accounts between July and December 2007. He pleaded guilty to one count of money laundering on Wednesday, according to Mike Ruocco, deputy to Judge Paul Gardephe of the U.S. District Court for the Southern District of New York, who is presiding in the case.

The criminals would infect PCs with malicious Trojan software that would steal account numbers and passwords whenever victims logged into their accounts online. Authorities say that another conspirator, Alexander Bobnev, would e-mail Mineev screenshots of the hacked accounts showing how much money was being transferred into Mineev's drop account, along with instructions such as "Withdraw the money ... tomorrow."

Mineev would then move the cash, sometimes as much as US$10,000, to Russia, using services such as Western Union.

Trojans are malicious programs that users install on their computers, believing them to be benign. Hackers disguise them as things such as video codecs, screensavers, and even security patches.

Account theft is a growing problem for banks and brokerage firms. They want to keep offering customers low-cost online banking services but are also sustaining losses from international criminals. Once the money has been moved offshore, it is virtually impossible to recover, security experts say.

Fraudsters often try to recruit so-called money mules to move funds from hacked accounts overseas. Often these mules are unwitting participants in the scheme, believing that they are simply doing freelance payroll work for international companies.

When charges were filed against Mineev and Bobnev last November, the U.S. Department of Justice charged a third man, Aleksey Volynskiy of New York, of also setting up drop accounts and laundering stolen money. Bobnev, of Volgograd, Russia, reportedly is out of the reach of U.S. law enforcement in his home country.

Mineev faces as much as two years in prison and a fine as high as $40,000 on the charge. In his plea agreement, he said he would return the $112,000 he made from the scheme.

Source: 06 June 2009 By Robert McMillan , IDG News Service ,

Free Microsoft antivirus 'coming soon'
Beta version of 'Morro' expected shortly

A beta version of Microsoft's free antivirus software - codenamed Morro - will soon be available from the company's website, according to a report.

Reuters says Microsoft employees are already testing the software ahead of a broader rollout in the near future. The company declined to provide a specific date for Morro's release, but said the trial version would be available "soon".

Microsoft announced its plan to replace its Windows Live OneCare security software with a free antivirus product last November.

The company said at the time that Morro would help encourage more people to take antivirus seriously, claiming nearly 50 percent of Windows users don't have an antivirus tool installed on their PC.

"Our goal with OneCare was to get more customers more protected, and I don't think we were able to do that to the extent that we would have liked," said Amy Barzdukas, a senior director of product management with Microsoft. "As we look around the world now, the countries where PC growth is most rapid, in emerging markets such as Brazil and India and China, the malware threat is even greater."

However, Morro, which is expected to run Windows OneCare's antimalware engine but will use fewer system resources, won't be bundled into the operating system, Barzdukas said at the time. That decision could help placate concerns from security software vendors, whose ability to sell antivirus products to consumers would be hampered if Microsoft bundled a free tool with its operating systems.

Source 11 June 2009, By Oliver Garnham , www.networkworld.com

The Internet is incomplete, says its co-designer, Vinton Cerf

Cerf cites security and mobile as pressing needs

WASHINGTON - The co-designer of the Internet's basic architecture, Vinton Cerf, said the Internet "still lacks many of the features that it needs," particularly in security, during a blunt talk to a tech industry crowd here.

Cerf, who is a vice president and chief Internet evangelist at Google Inc., co-designed with Robert Kahn the TCP/IP protocols that underpin the Internet. That was in 1973. And despite its having become operational in 1983, and commercially available in 1989, the Internet remains incomplete, he said.

Cerf is influential because of his accomplishments, but he may be even more so today because of his affiliation with Google. President Obama's administration has appointed a number of Google employees, including CEO Eric Schmidt, to important positions.

One of the most critical needs is authentication, Cerf said, and he told the crowd at a TechAmerica gathering Wednesday that anyone who performs transactions over the Internet -- which is everyone -- should "should be deeply concerned about that technology."

The lack of authentication is pervasive and is even a problem in simple cases, such as authenticating entries in the domain name system, he said.

"Authentication isn't available on an end-to-end basis at all layers of the architecture," Cerf said. While users are good "at building concrete tunnels" using simple SSL (Secure Sockets Layer) techniques, they don't identify the endpoints and just secure the channel, he said. You can have an e-mail with an attached virus, thoroughly encrypted, and send it through an encrypted tunnel, and once it gets to the other end, "it gets decrypted and then, of course, does its damage," he said.

Mobile is another problem. "We do a terrible job serving up mobile," Cerf said, referring to the ever broadening use of the Internet via mobile devices. He said protocol work is needed to address it.

Asked later what the White House should be doing in regard to this issue, Cerf cited the work that has been assigned to the National Institute of Standards and Technology in coordinating standards on the smart grid and health IT. However, he said he would anticipate that Obama's new CTO and CIO will "have some things to say about what the U.S. government hopes will emerge in the infrastructure of our digital communications system."

The Obama administration recently released a report on cyberspace security and has promised to make the issue a priority. The actions have been met with cautious optimism by the security industry.

Source: 11 June 2009, by Patrick Thibodeau, www.computerworld.com

European Commission plans tougher sentences for cybercrime

New laws could see jail terms for cybercrimes increased to more than five years, according to the Financial Times.

EC cybercrime officials say the current jail terms of one to three years are not severe enough to dissuade criminals responsible for increasing numbers of large-scale cyber attacks.

International cybercriminals are moving at lightning speed to defeat corporate security, attendees heard at the eCrime Congress 2009 in London in March.

Cybercriminals targeted an estimated 4.7 million computers in Europe, the Middle East, and Africa in 2008, according to the latest internet threat report from security firm Symantec.

The EC wants to bring all 27 EU member states in line with countries like the UK, France and Germany, which have longer sentences for cybercrime.

The EC also plans to set up a regional reporting system to enable EU member states to notify each other quickly of cyber attacks and related prosecutions to help improve security.

The new rules will be introduced when the EC updates the Council Framework Decision on Attacks Against Information Systems. The update is expected to be published at the end of this year.

The EC has a budget of £47m from the Safer Internet fund, which it plans to use to fund projects aimed at fighting cybercrime over the next four years.

Source: 15 Jun 2009 by Warwick Ashford

The inside story of the Conficker worm

A HOTEL bar in Arlington, Virginia, 23 October 2008. A group of computer security experts has spent the day holed up with law enforcement agencies. It is an annual event that attracts the best in the business, but one the participants like to keep low-key - and under the radar of the cybercriminals they are discussing.

That evening, conversation over drinks turned to a security update Microsoft had just released. Its timing was suspicious: updates usually came once a month, and the next was not due for two weeks. "I remember thinking I should take a look at this," recalls Paul Ferguson, a researcher at Trend Micro, a web security company in Cupertino, California.

He did. So did the rest of the computer security industry. In fact, they talked, puzzled and worried about little else for months after. The update heralded the birth of the Conficker worm - one of the most sophisticated pieces of malignant software ever seen.

Despite an unprecedented collaboration against them, Conficker's accomplished creators have been able to bluff and dodge to gain control of machines inside homes, universities, government offices and the armed forces of at least three nations, establishing a powerful and lucrative network of "zombie" computers. New Scientist has pieced together the sobering details of that cat-and-mouse fight.

The dry, technical language of Microsoft's October update did not indicate anything particularly untoward. A security flaw in a port that Windows-based PCs use to send and receive network signals, it said, might be used to create a "wormable exploit". Worms are pieces of software that spread unseen between machines, mainly - but not exclusively - via the internet (see "Cell spam"). Once they have installed themselves, they do the bidding of whoever created them.

If every Windows user had downloaded the security patch Microsoft supplied, all would have been well. Not all home users regularly do so, however, and large companies often take weeks to install a patch. That provides windows of opportunity for criminals.

No one knows the identity of Conficker's "patient zero" computer, or precisely when it was infected. It was probably a machine that the hackers already controlled. Once installed, the software set to work, surreptitiously scanning the internet for other vulnerable machines to send itself to.

The new worm soon ran into a listening device, a "network telescope", housed by the San Diego Supercomputing Center at the University of California. The telescope is a collection of millions of dummy internet addresses, all of which route to a single computer. It is a useful monitor of the online underground: because there is no reason for legitimate users to reach out to these addresses, mostly only suspicious software is likely to get in touch.

The telescope's logs show the worm spreading in a flash flood. For most of 20 November, about 3000 infected computers attempted to infiltrate the

telescope's vulnerable ports every hour - only slightly above the background noise generated by older malicious code still at large. At 6 pm, the number began to rise. By 9 am the following day, it was 115,000 an hour. Conficker was already out of control.

That same day, the worm also appeared in "honeypots" - collections of computers connected to the internet and deliberately unprotected to attract criminal software for analysis. It was soon clear that this was an extremely sophisticated worm. After installing itself, for example, it placed its own patch over the vulnerable port so that other malicious code could not use it to sneak in. As Brandon Enright, a network security analyst at the University of California, San Diego, puts it, smart burglars close the window they enter by.

Conficker also had an ingenious way of communicating with its creators. Every day, the worm came up with 250 meaningless strings of letters and attached a top-level domain name - a .com, .net, .org, .info or .biz - to the end of each to create a series of internet addresses, or URLs. Then the worm contacted these URLs. The worm's creators knew what each day's URLs would be, so they could register any one of them as a website at any time and leave new instructions for the worm there.

It was a smart trick. The worm hunters would only ever spot the illicit address when the infected computers were making contact and the update was being downloaded - too late to do anything. For the next day's set of instructions, the creators would have a different list of 250 to work with. The security community had no way of keeping up.

No way, that is, until Phil Porras got involved. He and his computer security team at SRI International in Menlo Park, California, began to tease apart the Conficker code. It was slow going: the worm was hidden within two shells of encryption that defeated the tools that Porras usually applied. By about a week before Christmas, however, his team and others - including the Russian security firm Kaspersky Labs, based in Moscow - had exposed the worm's inner workings, and had found a list of all the URLs it would contact.

Those addresses had to be blocked right away. "The thing could use domains like oxygen," says Rick Wesson of Support Intelligence, a network security company in San Francisco. "If you take them over, the fire should go out." Wesson has years of experience with the organisations that handle domain registration, and within days of getting Porras's list he had set up a system to remove the tainted URLs, using his own money to buy them up.

It seemed like a major win, but the hackers were quick to bounce back: on 29 December, they started again from scratch by releasing an upgraded version of the worm that exploited the same security loophole.

This new worm had an impressive array of new tricks. Some were simple. As well as propagating via the internet, the worm hopped on to USB drives plugged into an infected computer. When those drives were later connected to a different machine, it hopped off again. The worm

also blocked access to some security websites: when an infected user tried to go online and download the Microsoft patch against it, they got a "site not found" message.

Other innovations revealed the sophistication of Conficker's creators. If the encryption used for the previous strain was tough, that of the new version seemed virtually bullet-proof. It was based on code little known outside academia that had been released just three months earlier by researchers at the Massachusetts Institute of Technology.

The new worm strain spread rapidly. Its reach is impossible to measure precisely, but more than 3 million vulnerable machines may ultimately have been infected. These reportedly included computers in branches of the British, French and German militaries, in the British parliament and in hospitals and universities in the US. On 12 February, Microsoft offered a $250,000 award to anyone who could identify Conficker's authors.

Why the bother, though? For all its ingenious features, the worm had yet to do anything damaging. The answer was - and still is - that there is plenty it could do. The worm's owners might use its army of zombie PCs to attack the routers that govern internet traffic flow or cripple organisations within which they had managed to infect a large number of machines. "That much resource could be used to do devastating things," says Ferguson. "It could take down the infrastructure of half the planet."

Indeed, worse was to come. On 15 March, Conficker presented the security experts with a new problem. It reached out to a URL called rmpezrx.org. It was on the list that Porras had produced, but - those involved decline to say why - it had not been blocked. One site was all that the hackers needed. A new version was waiting there to be downloaded by all the already infected computers, complete with another new box of tricks.

Now the cat-and-mouse game became clear. Conficker's authors had discerned Porras and Wesson's strategy and so from 1 April, the code of the new worm soon revealed, it would be able to start scanning for updates on 500 URLs selected at random from a list of 50,000 that were encoded in it. The range of suffixes would increase to 116 and include many country codes, such as .kz for Kazakhstan and .ie for Ireland. Each country-level suffix belongs to a different national authority, each of which sets its own registration procedures. Blocking the previous set of domains had been exhausting. It would soon become nigh-on impossible - even if the new version of the worm could be fully decrypted.

Luckily, Porras quickly repeated his feat and extracted the crucial list of URLs. Immediately, Wesson and others contacted the Internet Corporation for Assigned Names and Numbers (ICANN), an umbrella body that coordinates country suffixes. Wesson did not sleep much. Given the differences in national practices, there was little chance of defusing every time-bomb URL in time for the 1 April deadline, but at least he could ensure that all the country-level operators had been warned.

In the meantime, frenzied headlines were proclaiming the impending meltdown of

the internet. But 1 April passed without event. This was not a total surprise. After all, it was just the first date on which the worm's URL strategy could change - it was still up to its creators to flick the virtual switch. To the outside, it looked like a gigantic April Fool.

And indeed it may have been. In fact, the whole URL business was probably a red herring: using a centralised URL to release a worm upgrade - even one as painstakingly concealed as Conficker's - is not a particularly sensible approach. It gives the authorities a specific target to counter-attack. From the second version onwards, Conficker had come with a much more efficient option: peer-to-peer (P2P) communication. This technology, widely used to trade pirated copies of software and films, allows software to reach out and exchange signals with copies of itself.

Peer pressure

Six days after the 1 April deadline, Conficker's authors let loose a new version of the worm via P2P. With no central release point to target, security experts had no means of stopping it spreading through the worm's network. The URL scam seems to have been little more than a wonderful way to waste the anti-hackers' time and resources. "They said: you'll have to look at 50,000 domains. But they never intended to use them," says Joe Stewart of SecureWorks in Atlanta, Georgia. "They used peer-to-peer instead. They misdirected us."

The latest worm release had a few tweaks, such as blocking the action of software designed to scan for its presence. But piggybacking on it was something more significant: the worm's first moneymaking schemes. These were a spam program called Waledac and a fake antivirus package named Spyware Protect 2009. This software was probably not the work of Conficker's creators. Confident of the strength of the network of machines they had built up, they were now renting out access to other criminals.

Such schemes can be hugely profitable. Just a tiny fraction of people targeted need to click on spam for the advertised business to make money. Storm, a previously widespread spam sender, generated millions of dollars a year in revenue. The same goes for fake software: when the accounts of a Russian company behind an antivirus scam became public last year, it appeared that one criminal had earned more than $145,000 from it in just 10 days.

Since that flurry of activity in early April, all has been uneasily quiet on the Conficker front. In some senses, that marks a victory for the criminals. The zombie network is now established and being used for its intended purpose: to make money. Through its peer-to-peer capabilities, the worm can be updated on the infected network at any time.

It is not an unprecedented situation. There are several other large networks of machines infected with malicious software. Conficker has simply joined the list. The security community will continue to fight them, but as long as the worm remains embedded in any computer there can be no quick fixes.

It's a depressing message, yet all the experts who spoke to New Scientist said that good things have come out of

Conficker and the publicity surrounding it. As the scare grew, academics, industry experts and domain registries came together in an unprecedented collaboration to fight the worm. By sharing information, they were able to warn users and produce scanners to check for it - at least until the next version appeared - and so curb its spread. After this experience, all agree, such collaboration will be much easier. The US Department of Homeland Security is funding a report on what can be learned from it.

That makes the effort worthwhile, says Wesson - despite the financial costs. He put up $30,000 of his own money to secure the URLs that Porras identified, and is still not sure whether he'll see any return on his investment. He would do it again, though. "We learned an enormous amount," he says. "Would I pay $30,000 to have the world change the way it looks at malware? Sure."

Source: 12 June 2009 by Jim Giles, www.newscientist.com

35% of IT staff snoop on privileged data

A recent survey of IT security staff has found that 35 percent admit to having snooped on sensitive insider information such as HR records, customer databases and merger and acquisition plans, according to security vendor Cyber-Ark.

The survey of 400 IT administrators and staff in the U.S. and UK also found 74 percent who said they could get around security controls to prevent access to internal information and data theft. Asked what they would take if they were fired by their company, 47 percent said they would take M&A plans, as opposed to 7 percent who said so in the 2008 survey.

One in five companies in the survey admitted to cases of insider sabotage or IT security fraud, 36 percent of which said they suspect their competitors received sensitive information or intellectual property as a result.

According to a report from the Carnegie Mellon Computer Emergency Readiness Team (CERT), insider threats extend beyond the organization itself - half of insiders who stole or modified information for financial gain were recruited by outsiders, including by business partners or organizations looking to acquire the insider's company.

The 2007 E-Crime Watch Survey conducted by the U.S. Secret Service and the CERT Coordination Center found that, in cases where respondents could identify the perpetrator of an electronic crime, 31 percent were committed by insiders.

Source: June 11, 2009, www.mxlogic.com

Most Employees Disobey Security Policies

New Ponemon Institute report finds end users are evading security controls at an increasing rate

Turns out end users are getting even worse about following security policies: A new study to be released tomorrow by the Ponemon Institute found that the majority of employees routinely violate their organizations' security policies.

Half of the around 1,000 corporate end-user respondents in the study, which was commissioned by IronKey, say their corporate data security policies are mostly ignored by both employees and management, and that those policies are difficult to understand, anyway.

"We found the rates are very high [of their] doing things that are violations of corporate security policy," says Larry Ponemon, chairman and founder of the Ponemon Institute. "I believe organizations across the board are trying to deal with [this]," he says.

Among the policy violations: misuse of USB sticks, personal email use, downloads of free apps for either personal or work use, loss of mobile devices, turning off firewall and other security settings on their machines, and social networking, Ponemon says.

Around 66 percent say they copy confidential data onto USB sticks -- up from 51 percent in 2007 -- while 87 percent say they "believe" such behavior is prohibited by their company's security policy. More than 50 percent say they use Web-based email accounts from their work machine, up from 45 percent in 2007. But 74 percent say they believe there is no corporate policy against doing so.

Around 43 percent have lost or misplaced a device that holds company data, an increase from 39 percent in 2007, and 75 percent did not immediately report the lost or missing device. Around 53 percent download personal applications onto their corporate machine, up from 45 percent in 2007, while 38 percent say their corporate policy does not allow that.

More than 70 percent of end users don't think their organizations have apolicy forbidding their turning off security settings (including a host firewall) on their work computers. And 21 percent say they disable those security settings, up from 17 percent two years ago.

Although more than 70 percent say their company forbids password-sharing with their colleagues, 47 percent still do so (compared to 46 percent in 2007). With more tools available online, as well as portable USB technologies, Ponemon says it makes sense that noncompliance could increase as end users start deploying these tools in the workplace. "Technology is a friend, but can also be an enemy from a security and privacy perspective," he says. "And the lack of enforcement [of security policies surrounding these tools] may be a function of the dismal financial conditions we're facing."

Still, with more organizations setting security policies and improved security technologies available, compliance should be better, he says. "That mean policies are not good enough," he says, or enforcement isn't occurring.

Source: Jun 09, 2009 By Kelly Jackson Higgins, www.darkreading.com

Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites

Approximately 24 hours ago, the Iranian oposition coordinated an ongoing cyber attack that has successfully managed to disrupt access to major pro-Ahmadinejad Iranian web sites, including the President's homepage which continues returning a "The maximum number of user reached, Server is too busy, please try again later..." message.

Through a combination of DIY (do it yourself) denial of service attack tools (DDoS), multiple iFrame loading scripts, public web page "refresher" tool, and a much more effective PHP script, the participants have already prompted some of the major Iranian outlets to switch to "lite" versions of their sites in an attempt to mitigate the attack.

Let's assess this very latest example of people's information warfare concept, find out which sites remain affected, and discuss the attack tools used:

The campaign appears to have been organized through Twitter, which despite public reports that the site has been banned in Iran, appears to be still accessible through a a persistent supply of proxy servers on behalf of the opposition.

Moreover, the ongoing distributed denial of service attacks, are using techniques which greatly resemble those used in last year's Russia vs Georgia cyber attack, and the ones Chinese hacktivists used back in 2008 in order to temporarily shut down CNN, with a single exception - there's no indication of a botnet involvement in the present attack.

Instead, the attack relies on the so called people's information warfare concept, which is the self-mobilization of individuals, or their recruitment based on political/nationalistic sentiments by a third-party, for conducting various hacktivism activities such as web site defacements, or launching distributed denial of service attacks.

The following are some of the sites that are currently under attack, remain totally unresponsive, or return "server is too busy" error messages:

- Ahmadinejad.ir - Mahmoud Ahmadinejad's Official Blog - under attack
- Leader.ir - Office of the Supreme Leader, Sayyid Ali Khamenei - under attack
- President.ir - Presidency of The Islamic Republic - under attack
- Farsnnews.com - Fars News Agency - under attack
- Irib.ir - Islamic Republic of Iran Broadcasting - under attack
- Kayhannews.ir - News Portal - "Service Unavailable"
- Irna.ir - Islamic Republic News Agency "service unavailable"
- Mfa.gov.ir - Ministry of foreign affairs , Islamic Republic of Iran - under attack
- Moi.ir - Ministry of Interior - under attack
- Police.ir - National Police - under attack
- Justice.ir - Ministry of Justice - under attack
- Presstv.ir - Iranian Press TV - "server is too busy"

Chatter from the hacktivists' trenches send over Twitter, or web forums during the past 24 hours:

- "Overload Iran's propaganda websites–we can do it together!"
- "we can suspend IRIB propaganda! just click & keep it refreshing!"

- "Take part in disabling the iranian propeganda leave on as long as possible"
- "Our efforts are working!!! RT @NewIRAN: Leader.ir; President.ir; FarsNews.com all now appear to be down"
- "Iran needs your help. Help us flood Iran Govt sites khamenei.ir is one of our targets. Go to PageReboot.com and set @ 2 secs"
- "we are currently flooding Iran Government websites - we have successfully taken down numerous sites already"
- "Great news! PressTV.ir has been shut down thanks to our efforts!"
- "IRIB, RESALAT, Kayhan, FarsNews, President.ir, and Leader.ir all brought down. Please help keep them down."
- "president.ir is down!!!"
- "SPREAD: tool for denial of service web attack. run on president.ir and irib.ir"
- "I'm reaping at 200kb/sec baby."
- "sweeeeeet, Farsnews is finally down! keep it up guys. I have 5 browsers open using Page Reboot."
- "Let's continue the attack. They have a very efficient server compared to other sites, but we successfully killed it many times already. Try to reload your application."
- "It's down again. I can't view it from NZ. Keep at it people."
- "I'm going to set up a massive solo attack on Resalat using 8 virtual machines on 8 CPUs while I go to bed. I understand it'll be hard to make it go down but I'm going to try."
- "done. I am also using couple of virtual M. Lets see if we can bring it down."
- "HAHAHAHAHAHAHAHAHA!!!! RESALAT DOWN!!!!!!!!!! THAT WAS F*CKING BRUTAL!!!"

Among the first web-based denial of service attack used, is a tool called "Page Rebooter" which is basically allowing everyone to set an interval for refreshing a particular page, in this case it's 1 second. Pre-defined links to the targeted sites were then distributed across Twitter and the Web, through messages link the following :

"Please spread word about a cyber effort to exert pressure on the paramilitary in Iran. They have launched denial of service attacks on US websites that are run by live bloggers feeding us up to the minute information about what is going on in Iran on the ground. To fight back, open these two URLs in as many tabs/windows as possible and simply leave your computer running overnight! We must show solidarity with them in their quest for freedom! The 2nd link targets PressTV, the mouthpiece of Ahmadinejad and Khamenei."

The second stage of the campaign consisted in the distribution of a multiple iFrame loading script which was automatically refreshing farsnews.com; irna.ir and rajanews.com, the results of which you can see in the attached screenshot. The script has since changed its location and is advertised under a new domain.

The third stage included a combined attack, this time including DIY (do-it-yourself) denial of service tools (DDoS), which despite their primitive nature are indeed causing server overload for their targets. Each of the tools is distributed with a simple manual, including links to large images at the targeted web sites, one which the software using proxies will attempt to obtain automatically.

* Go through related hacktivism posts: Chinese hackers deface the Russian Consulate in Shanghai; Georgia President's web site under DDoS attack from Russian hackers; Thousands of Israeli web sites under attack; Pro-Serbian hacktivists attacking Albanian web sites; Hundreds of Dutch web sites hacked by Islamic hackers; 300 Lithuanian sites hacked by Russian hackers; Chinese hackers deface the Russian Consulate in Shanghai; China detains web site defacer spreading earthquake rumors

The tools themselves, BWRaeper.exe (detected as Worm.AutoIt.AA); PingFlooder.exe (flagged as banker malware); Server_Attack_By-_C-4.exe (Riskware.ServerAttack.F) and SupportIran.php, have already been picked up by antivirus vendors.

The following are the instructions found in the StopAhmadinejadOnline package, consisting of BWRaeper.exe and PingFlooder.exe :

"New hacking/DoS attack tool. Please learn and use: This is an online war

1. Please download
2. Extract it into a folder on your desktop and click on BWRaeper
3. Then click on Raep That's all.

FarsNews, AN's website, KHamenei's Website, IRIB and many other sites can be brought down with this technique. This is an online war. Don't let them win. They filter information, we will too. There's more of us. EDIT: Please add the following URLs to your list of URLs after you've completed the steps above. To do this, open the file "urls.txt" and paste the following line in it. Once you've added this URL, Run BWRaeper again

irna.ir/Images/uiImages.gif
resalat-news.com/Pic/6729000.jpg
resalat-news.com/image/Heder.jpg
resalat-news.com/Pic/6729.gif
resalat-news.com/Pic/6729011.jpg
resalat-news.com/Pic/6729021.jpg"

The manual within Server_Attack_By-_C-4.exe entices users to participate in the attack, in the following way:

"I also found another DOS file to attack. just another option.

1. dl this zip file from here and unzip it on ur desktop:
2. take IP address of IR sites(Farsnews.com, irna.ir, president.ir, rajanews.com) from here: http://www.selfseo.com/find_ip_address_of_a_website.php
3. insert the IP address in "Server Address" section and press Attack.
4. let it run and it'll attack all of their servers"

The last tool is a basic PHP script targeting those running a server that supports PHP in order to use it - "Want to help DDoS attack Iran gov't? Have a server that runs PHP? Use this script!".

SupportIran.php has also been released as an improved version to the multiple iFrame loader, and is currently used in the attack as well, having the following sites pre-defined to attack simultaneously - khamenei.ir; presstv.ir; irna.ir; president.ir; mfa.gov.ir; moi.ir; police.ir; justice.ir; live.irib.ir.

There have already been speculations that the magnitude of these local attacks — Iranian users targeting Iranian web sites – is contributing to the "strange changes in Iranian traffic transit" reported during the last couple of days.

The attacks are ongoing, updates will be posted as soon as they emerge.

Source: June 15th, 2009, by Dancho Danchev, blogs.zdnet.com

S. Korea military networks under growing cyber attack

South Korea's military computer networks are under ever-growing cyber attack with 95,000 cases reported daily on average, officials said Tuesday.

The Defence Security Command said in a report to a security forum that every day the military counters an average of 10,450 hacking attempts and 81,700 computer virus infections in addition to other cases.

The attacks increased 20 percent this year compared to 2008, it said.

A spokesman for the command told AFP most of the attacks are the same as ordinary people experience at home, but one-tenth are serious.

"Eleven percent of the total are sophisticated and vicious attempts to hack into military servers and to gather intelligence," the spokesman said.

The command did not elaborate where the cyber attacks originated. Defence officials in Seoul have previously pointed to North Korea and China, which they say run elite hacker units.

Yoo Ho-Jin, an official of the National Intelligence Service, said his agency recently proposed that the president name an aide to deal with cyber-security.

"Our country continues to be vulnerable. Some of our government branches failed to function when we recently simulated a cyber-attack on them," Yoo told a security forum on Tuesday, according to Yonhap news agency.

"This is a grave threat to our national security."

South Korea and the United States in April agreed to cooperate to defend their defence networks from countries including China and North Korea.

Last year South Korean Prime Minister Han Seung-Soo warned his cabinet against what he called attempts by Chinese and North Korean computer hackers to obtain state secrets.

Source: June 16th, 2009, www.physorg.com

Israel and foes in internet war

The battlefield in the Middle East may be changing. Israeli intelligence agencies have warned citizens of the risks in using social networking sites such as Facebook.

They say that the internet is a war zone between Israel and its enemies including Hamas, Hezbollah and Iranian groups.

According to the Israeli intelligence analyst, Dr Ronen Bergman, Israel's concerns are twofold: first, that Israeli internet sites might be breached and sabotaged; second, that Israeli soldiers might be enticed to give away secrets.

Israeli intelligence officials are worried that Israelis risk leaking sensitive information or may even be kidnapped if they speak too openly with Palestinians and Lebanese online.

They fear that Israelis might be encouraged to leave Israel to meet someone they meet in the virtual world of Facebook and then be kidnapped in the hope that they can be exchanged for some of the thousands of Palestinians held in Israeli jails.

Many national governments issue advice to their citizens about using the internet safely. But Israeli intelligence tips are more like strict orders.

National service is an obligation of Israeli citizens and many have knowledge of information which is secret or at least highly sensitive.

Dr Ronen Bergman says that Hamas claims that it got important information via the internet about intelligence networks and spies and also about some of the elite units in the Israeli army.

Of particular concern are social networking sites such as Facebook.

The fear is that people who use Facebook may let their guard down in a way they would never do if they were speaking face-to-face.

Virtual Training Camps

But Israel cannot just rely on giving advice.

A battle is being fought day and night by trained "soldiers" fighting an enemy they cannot see.

Private companies are involved in this war to provide protection for government and financial websites which are constantly under attack and sometimes breached.

Safenet Aladin was formed in the United States 26 years ago and now has branches in over 100 countries

It has a specially designed laboratory in Israel to conduct experiments and simulate electronic attacks.

The laboratory is a kind of virtual training camp where engineers are taught how to use the most sophisticated programs to repulse electronic invasions.

The manager of security technology at the Israeli branch of the company, Ofer Alzam, told BBC Arabic Radio about the

laboratory and how the battle is fought on the internet.

One of the tools they use in the battle is an electronic key which contains encrypted data and is provided to a number of clients to help protect vital secret information.

The key not only protects secret information but also foresees computer threats.

"First, we have to foresee the threat. If we can anticipate it we can normally deal with it. In one or two percent of cases however, we have to minimise the threat window to provide protection and security against new threats, particularly for major internet providers" says Mr Alzam.

Bullet proof

The most sensitive Israeli strategic sites are those housing electronic databases.

The companies that provide these for individuals, the government and private companies pride themselves on the level of security they provide their clients.

Saji Maysar, the marketing manager of on such internet security company, Samial, took me to a room secured by strong doors and bullet-proof glass.

Over the loud hum of the computer servers housed there he said that if there was ever a successful attack on this room it would be the equivalent of a strike on a key military base.

He said the room held sensitive information which not only had to be protected against cyber-attack but also against physical attack by those who wanted to harm Israel and its citizens.

The Israeli army itself has a division trained to fight cyber warfare to protect military secrets.

When intelligence officers resign from the army, some take their knowledge to one of the prestigious computer companies.

Many analysts now believe that the Israeli capability in this cyber war may now be as strong as more traditional Israeli defences built up over the past half-century.

It is difficult to judge who is winning this war, or sometimes to even find out where the battles are being fought.

But Israel's considerable intelligence resources need to be constantly on full alert to prevent a successful attack by nimble enemies who are becoming increasingly astute in fighting a virtual war from their laptops.

Source: 15 June 2009, By Ahmad Budeiri, BBC Arabic, Jerusalem

Belarus media sites under attack by zombies

Echoes of Russia-Georgia cyberwar reverberate in Minsk

The spectre of politically-motivated hacking attacks has once again risen in Eastern Europe.

Media websites in Belarus, in particular news site Charter97.org, are under a distributed denial of service attack. Charter97 has been unavailable for several days and under lower-level attack for much longer, security tools firm Arbor Networks reports.

Translated versions of local reports on the attack against Charter97 can be found here.

Jose Nazario, manager of security research at Arbor Networks, said the nature of the attack and the type of botnet used to run it is similar to those used to attack the Georgian presidential website in July 2008. More on the Machbot-like botnet behind the Belarus attacks can be found in a blog posting by Arbor here.

Armed conflict between Georgia and Russia over the ethnically Russian separatist region of Georgia provided a background to these cyberattacks. The motive, much less the source of cyberattacks against Belarussian websites, is unclear.

However, the attacks follow increased political tension between Belarus and Russia, culminating in Russia's recent decision to withhold the last quarter of a $2bn loan to Belarus.

Alexander Lukashenko, the president of Belarus, has accused the Russians of punishing his country for failing the recognise the independence of rebel-held regions of Georgia. Increased friendship between Belarus and the EU is also an issue.

The former Soviet republics have often found themselves on the front-link of cyberattack over recent years. The internet infrastructure of Estonia, which relies heavily on online services, was ripped apart in 1997. The central Asian republic of Kyrgyzstan was turfed offline for more than a week back in January.

The Kyrgyzstan attack, blamed as with previous assaults on Russian cybermilitia, probably had far less effect on the ground than the Estonian assaults, because it occurred in a region with low internet penetration where online access to government service and banking is not much of an issue.

Source: 12th June 2009, By John Leyden, www.theregister.co.uk

What Is Rogue Anti-virus Software?

It is almost unheard of in this day and age to be online without using anti-spyware and anti-virus software to safeguard your computer against viruses and other malicious code. It's not surprising to see the prevalence of rogue anti-virus software.

Also called scareware, or rogue security software, or smitfraud, this type of software is also most commonly defined as malware—it is designed specifically to damage or disrupt your computer system. In this case, not only is the software going to disrupt your system, it's going to try and trick you into making an unsecure credit card purchase.

Rogue anti-virus programs usually appears in the form of a fake Windows warning on your computer system that reads something like, you have a specific number of viruses on your computer (usually in the hundreds) and that this software has detected those viruses. To get rid of these viruses, you're prompted to buy the full-version of the antivirus software (which is really rogue antivirus software).

The good news is that you probably do not have a computer that is infested with hundreds of viruses as the rouge software claims. The bad news is that the rogue antivirus software itself is on your computer and you must remove it. Removal is hindered as rouge software can lock the control panel and the the Add/Remove Programs function to prevent you from removing it easily.

Other things that may be disrupted by the rogue software include being unable to visit reputable and valid anti-virus and malware Web sites, being able to install legitimate antivirus software and also being unable to access your desktop.

The rogue software wants to stop users from removing the program and proceeding with the purchase instead. It's important to remember that by purchasing the "claimed full version to remove the viruses" you will be submitting your personal information to unscrupulous persons and may also end up being a victim of credit card or identity theft.

Common names of rogue antivirus software include; AntiVirus (2007, 2008, and 2009), MS-Antispyware, XP AntiVirus (2007, 2008, and 2009), Home Antivirus 2009, SpyWareGuard, Malware Cleaner, Extra Antivirus, AV AntiSpyware, SpywareProtect2009, WinPC Defender as well as many other names.

How Does a Computer Get Infected with Rogue Antivirus Programs?

The reason these rogue anti-virus programs are successful (for the malicious coders) is because the warning screens very closely resemble legitimate Windows warning screens, plus the rouge software program names closely resemble or sound like legitimate antivirus programs.

When you load an infected Web site you might see a warning screen pop up and think that it is a legitimate Windows warning. Users unknowingly are tricked into downloading the software because they believe the warning to be a legitimate Windows messages.

You might also be on a Web site trying to view a video and a screen may pop-up telling you that you need to download a codec to view the file. The window prompting you to download the codec looks legitimate, however you are not

In April of this year, it was also reported that systems that had been previously infected with Conficker, found this worm had began installing rogue antivirus programs on infected machines. In the early cases this turned out to be a rogue application called SpywareProtect2009. Kaspersky researchers reported this was a typical rogue program that offered to clean the computer for $49.95.

Lastly, if you use file sharing networks you also risk downloading a rogue antivirus as it can be easily hidden inside a legitimate program—that you may or may not be legitimately downloading.

How to Spot Rogue Antivirus Warnings

For the most part, you need to look at the windows that are popping up and the name of the program being shown. If you know the program name of the antivirus and spyware software you use, then seeing a different name in the warning window is the first clue. Also, Windows itself doesn't warn you of a virus. Legitimate warnings on your system would come from the anti-virus program you have installed, not a random Windows operating system style pop-up window. A great resource for learning how to spot these malicious programs through fake warning messages can be found on bleepingcomputer.com. This page lists the text of some of the more common false warning screens, including the following:

Malware Cleaner: Trojan detected! A piece of malicious code was found in your system that can replicate itself if no action is taken. Click here to have your system cleaned by Malware Cleaner.

AV AntiSpyware: Spyware Alert! Your computer is infected with spyware. It could damage your critical files or expose your private data on the Internet. Click here to register your copy of AV AntiSpyware and remove spyware threats from your PC.

How Do I Get Rid of Rogue Antivirus Programs?

It can be a difficult task to get rogue anti-virus programs off your computer. To complicate the matter, there are many variations of this malicious program and not all variants can be removed in the same way. This is not something that novice computer users may be able to deal with on their own.

Also, due to the popularity of these infections and people searching for answers on how to remove the program a number of scam programs also exist that lead users to believe it will remove the infection. Yes, these programs that claim to rid your system of Antivirus 2009 (or whichever variant you have been infected with) will scan your system and then prompt you for a credit card number so you can download a full version to remove the infection. Sound familiar? It should. This is a vicious cycle that users can unwittingly become trapped in.

Still, the good news is that in many instances you can get rid of the rouge antivirus program without wiping and formatting your hard drive. If you are already infected and you cannot access legitimate security related Web sites, you will need to download the following programs from a second computer and burn them to CD to run on the infected computer.

WARNING: Before running any of the following programs, you should turn off System Restore (you won't be able to use System Restore as this deletes all restore points). If you don't turn it off, the programs may not be able to access those system files to clean them. If you are infected the System Restore is not going to return you to an earlier uninfected date anyway. You can turn it back on after you have successfully removed the rouge antivirus program.

The quickest way, and first thing to try is to download Malwarebytes Anti-Malware to get rid of the rogue antivirus. On it's own this will usually rid your computer of the problem. If Malwarebytes didn't have the desired results, or you simply want to do a total and complete system clean, you will want to use a combination of CCleaner, Malwarebytes, Asquared, and SpyBot Search and Destroy. These programs all offer freeware versions.

NOTE: In some cases, the rogue anti-virus may block one or more of these legitimate programs. If this is the case, you will need to open the folder where you installed the program on your hard drive and rename the executable file (.exe) to anything other than the program's name. (e.g. rename mbam.exe to aaa.exe).

Once you have run all the programs, be sure to go back and run CCleaner a final time to get rid of dead registry links from having the rouge antivirus removed. Continue to run the registry option of this program until no problems are found.

By Vangie Beal, www.webopedia.com

Quiz 0001

The Quiz is from the Magazine Articles ?

China will install a _____ _____ software for tracking pornographic _____

What is the high risk rate % of Katrina Kaif search term?

Where are the CYBERWATCH schools located?

What was Microsoft's reward to find Conficker author?

Terms & Conditions

- One Grand Prize winner will be awarded a cash prize of INR 1000.00.
- Three consolation prizes will be gift hamper of 3 books published by CRPCC/Sysman.
- Winners having all correct entries will be selected by lottery.
- If there is no "all corrrect" entries no prize will be awarded.
- Decision of CCCNews will be final and can not be challenged.
- Gift hampers will be collectable from CCC News office in Mumbai.
- Last date to send entries is 20 June 2009 IST 24:00 hrs.
- Winners will be declared in next issue of CCC News Magazine.
- Please send email with correct answers of all 4 questions to quiz@cccnews.in with your name, age, designation (if any), company (if any), Postal address, Phone no. & email address, please write "Quiz 0001 answers" in subject.
- Ambiguous answers may be out right rejected