CCC News
Control Computer Crimes
Issue 0006 - 31 August 2009

BLIND TEEN SUPER PHREAKER 16
THE HABITS OF HACKERS 3
100 MOST DANGEROUS WEBSITES 6
HOW BOTNETS GENERATES REVENUE 30

## Message from the Editor

Welcome to the sixth issue of CCCNews Magazine.

It gives me great pleasure that CCCNews Magazine is becoming more popular and downloaded by many more readers. This is a good sign that people are taking Computer Security seriously.

Based on the feedback, you have more reports, research, analysis, surveys and less news and related matter. The news are covered in CCCNews Newsletter, published thrice a week.

In this edition, we are publishing a report on - How a 16 years old blind telephone hacker has created havoc in the life on many people and law enforcement in US by his extraordinary and supernatural skills of hacking telephone systems. This is an amazing story of using extraordinary skills for wrong usage, may be to have the sadistic pleasure and status in underground world.

Another interesting development has been the hacking of Bank accounts of US Fed Chairman Ben Bernanke. This triggered with the simple pick pocket of his wife's purse, which has many critical details. Most bankers think that they are fully secured given the battery of gadgets, they have implemented. But, can these gadgets change the human nature and culture? Human is still the weakest link in the security chain. This doesn’t mean that the technology is not required. But, technology itself has many holes but these holes are small compared to carelessness and casual attitude of human users. It will be interesting to see, what effect this hacking of US Fed Chairman will have on tightening of Cyber security.

An interesting story of the fortnight is the ban of social networking sites like Twitter and facebook by most of the employers. As per the survey, 76 % of companies have choosen to block social networking and it is now a more popular category to block than online shopping (52%), weapons (75%), alcohol (64%), sports (51%) and Webmail (58%). The results come from an analysis of more than a billion Web requests processed by the survey company. It seems, gradually the user companies are feeling the pinch and taking action to secure their IT assets.

**Rakesh Goyal**
**Editor**

# CONTENTS

CCC News
Issue 0006
31 August 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

| | |
|---|---|
| THE HABITS OF HACKERS | 3 |
| FACEBOOK, TWITTER BANNED BY MOST EMPLOYERS | 4 |
| WEB TRACKERS KNOW MORE ABOUT YOU THAN YOU THINK | 5 |
| 100 MOST DANGEROUS WEBSITES | 6 |
| MOST REDUNDANT EMPLOYEES STEAL ENTERPRISE DATA | 8 |
| CIVILIANS CYBERATTACKED GEORGIA IN 2008 WAR | 11 |
| HACKERS PREFER FIREFOX AND OPERA | 13 |
| ENTERPRISES NEED TO SECURE DATA DURING APPLICATION DEVELOPMENT | 14 |
| BLIND TEEN SUPER PHREAKER | 16 |
| HOW BOTNETS GENERATE MILLION-DOLLAR REVENUES FOR CYBERCRIMINALS | 30 |
| Events | 32 |
| Quiz | 35 |

## Survey

# THE HABITS OF HACKERS

### (a survey at DEFCON)

Enjoy the rest of your summer vacation, say the hacking community, as you're far less likely to be targeted now than during your Christmas and New Year vacation. That's the results of the "Hacker Habits" survey by Tufin Technologies, conducted amongst 79 hackers at Defcon 17 in Las Vegas this month.

Given the small number of respondents compared to the number of attendees, their opinions should be taken with caution, and may not necessarily represent what the majority of hackers at Defcon really think. In any case, what follows are the results.

89% of hackers admitted that IT professionals taking a summer vacation would have little impact on their hacking activities, as a whopping 81% revealed they are far more active during the winter holidays with 56% citing Christmas as the best time to engage in corporate hacking and 25% naming New Years Eve.

If you want to know when you should be most on your guard it's during weekday evenings with 52% stating that this is when they spend most of their time hacking, 32% during work hours (weekdays), and just 15% hacking on weekends.

96% of hackers in the survey said it doesn't matter how many millions a company spends on its IT security systems, it's all a waste of time and money if the IT security administrators fail to configure and watch over their firewalls. 86% of respondents' felt they could successfully hack into a network via the firewall; a quarter believed they could do so within minutes, 14% within a few hours. 16% wouldn't hack into a firewall even if they could.

Validating the frustrating gap between compliance and security, 70% don't feel that regulations by governments worldwide to implement privacy, security and process controls has made any difference to their hacking into a corporate network. Of the remaining 30%, 15% said compliance initiatives have made hacking more difficult and 15% believe they've made it easier.

70% of those sampled believe the number of malicious hackers – criminals motivated by economic gain-- is less then 25% of the of hacker community.

Credits : http://www.net-security.org

## Survey

# FACEBOOK, TWITTER BANNED BY MOST EMPLOYERS

Employers are increasingly putting the brakes on employee use of social networking sites on the job, according to a new survey. The research by ScanSafe, a provider of SaaS Web security, said its data shows more employers are blocking sites such as Facebook and Twitter.

The results come from an analysis of more than a billion Web requests processed by the company, officials said. ScanSafe saw a 20% increase in the number of customers blocking social networking sites in the last six months. According to their data, 76% of companies are choosing to block social networking and it is now a more popular category to block than online shopping (52%), weapons (75%), alcohol (64%), sports (51%) and Webmail (58 %).

"When Web filtering first became an option for companies we generally saw them block access to typical categories such as pornography, illegal activities and hate and discrimination," said Spencer Parker, director at ScanSafe. "In recent months, employers are obviously wising up to the dangers and negative impact on productivity linked to certain sites and more and more of our customers have chosen to block social networking, online banking and Webmail."

The research did not include explanations from customers for the increase in social network restrictions, but ScanSafe officials speculated it may be due not only to security concerns, but also to decreased productivity when the use of Web 2.0 sites is allowed among employees.

"In economic times like these, having a productive workforce is more important than ever and companies are now often expecting employees to work harder for less," ScanSafe officials said. "Restricting access to non-work related sites could be a way to encourage this much needed productivity."

Credits : Joan Goodchild; http://www.networkworld.com

## Research

# WEB TRACKERS KNOW MORE ABOUT YOU THAN YOU THINK

Social networking sites are routinely making specific personal information on their users available to tracking sites, as per a report.

The study cites Facebook, MySpace and Twitter as allowing this leakage, and describes just how tracking sites can use the information to link browsing habits to specific individuals.

With a unique identifier, a tracking site could gain access to a user's name, physical address, email address, gender, birth date, educational and employment information, and much more.

"When you sign up with a social networking site, you are assigned a unique identifier," says Craig Wills, professor of computer science at Worcester Polytechnic Institute (WPI). "We found that when social networking sites pass information to tracking sites about your activities, they often include this unique identifier. So now a tracking site not only has a profile of your web browsing activities, it can link that profile to the personal information you post on the social networking site. Now your browsing profile is not just of somebody, it is of you."

Wills says the researchers do not know what, if anything, tracking sites do with the unique identifiers once they've got them. He says they've asked, but haven't heard back officially from any.

"We are not saying that they are necessarily trying to leak private information," he says. "But once someone is in possession of your unique identifier, there is so much they can learn about you. And even if tracking sites do not use the information themselves, can they guarantee that it will never find its way into other hands?"

Credits : Emma Woollacott; http://www.tgdaily.com

**Report**

# 100 MOST DANGEROUS WEBSITES

Computer security software provider Norton Symantec has released a list of the 100 most dangerous websites on the internet, and has warned businesses to ensure they have property security to avoid being affected by malware.

The list of the top 100 dirtiest websites contain large amounts malware - malicious software designed to attack a person's computer to either obtain private information, or control it for another purpose.

While some of the sites have benign names - one is called kingfamilyphotoalbum.com - simply visiting one of the websites on the list would most likely result in a computer being infected with malware or other viruses. Hackers could use these viruses to obtain information from the computer by installing "keyloggers" - software which monitors and records each keystroke made.

Hackers who commit credit card fraud usually admit to using some type of malware, including keylogging software, to steal personal and financial details.

Norton says the top 100 sites have, on average, about 18,000 threats with about 40 containing more than 20,000 threats.

About 75 websites were found to be installing malware on other machines for more than six months, with over 50 of the websites containing hard-core pornography.

But other websites do not appear to contain adult material, with some appearing to offer advice on every-day hobbies such as ice-skating, deer-hunting and even catering services.

Norton Symantec spokesperson Natalie Connor says businesses should take notice of the list and ensure their computer systems at work are safe.

Connor says businesses should also be aware of emerging trends in regards to computer viruses and malware, as Norton says the number of threats is growing.

"There is an increase in the number of threats we are seeing, and the amount of effort we are putting in to stopping these threats is also growing. The trend is genuinely on the rise."

"But all want to do is make sure people are aware about these things. We're going to recommend they have some sort of security in place, but also make sure they are educating themselves on the actual trend. They should be reading and watching things about cybercrime, practicing not sharing your password or details about your web account. If you have a network, lock it down. Simple things like that can protect you."

*Norton has provided the following sample of sites on the list. Be warned, many of these sites contain malware.*

- *17ebook.co*
- *aladel.net*
- *bpwhamburgorchardpark.org*
- *clicnews.com*
- *dfwdiesel.net*
- *divineenterprises.net*
- *fantasticfilms.ru*
- *gardensrestaurantandcatering.com*
- *ginedis.com*
- *gncr.org*
- *hdvideoforums.org*
- *hihanin.com*
- *kingfamilyphotoalbum.com*
- *likaraoke.com*
- *mactep.org*
- *magic4you.nu*
- *marbling.pe.kr*
- *nacjalneg.info*
- *pronline.ru*
- *purplehoodie.com*
- *qsng.cn*
- *seksburada.net*
- *sportsmansclub.net*
- *stock888.cn*
- *tathli.com*
- *teamclouds.com*
- *texaswhitetailfever.com*
- *wadefamilytree.org*
- *xnescat.info*
- *yt118.com*

Credits : Patrick Stafford : http://www.smartcompany.com.au

## Research

# MOST REDUNDANT EMPLOYEES STEAL ENTERPRISE DATA

Multinational enterprises lack automated systems to cut access to exiting employees.

One of the benefits of attending as many enterprise IT events as I do, is the regular opportunity to learn about major vulnerabilities that businesses are facing, but perhaps not really properly dealing with.

One of these came to mind last week at an MIS Asia magazine hosted event, sponsored by Novell, in Kuala Lumpur. The title of the event was 'A New FSI Compliance and IT Security Era is Near: Are You Ready?'.

There were some very interesting presentations from Quint Wellington Redwood Asia's managing director, Malaysia, Michiel de Boer, and Novell's director, identity and security solutions Asia Pacific, Anthony Turco.

Michiel, who is also a representative (VP) for the itSMF chapter for Malaysia, told the delegates there was 'a growing gap between the rate of technology adoption and the rate of technology control'. He said it takes 'double or triple the energy to catch up if you are not proactive about IT compliance'.

Michiel recommended that enterprises adopt a continual improvement approach and review their compliance and compliance strategies at least once a year. One point he made that caught my ear was that you can never avoid risk, you can only effectively manage it.

### Terminated employees take data

One fact that jumped out at me was research quoted by Anthony which stated that about 70 per cent of terminated employees routinely departed with data from their former firm. Anthony said research showed that these employees thought that such action was entirely normal and justifiable.

It emerged from Anthony's presentation that, despite the accelerated numbers of redundancies and terminations stemming from the global economic downturn, the majority of enterprises do not have an automated system to either provision, or, perhaps more importantly, de-provision employees, when they join, or are asked to leave, the company.

Anthony showed one slide that demonstrated how any one employee's access to different parts of an organisation – to increasingly sensitive and valuable information – quickly snowballs, the longer they hold their job. I am sure he scared the delegates with his summary of recent major data breaches in the US, including Societe General, the recent Heartland Payment Systems data breach, and the Fannie May problems with sub-prime mortgages, when he said most of the victim enterprises did not have automated systems to quickly cut exiting employees from access to company data – called 'de-provisioning'. This was despite such systems now being routinely available.

## Mega breaches

Informed readers will recall that, in the Societe Generale case, a low-level options trader executed fraudulent transactions, using his knowledge of internal policies and process controls allowed him to hide the fraud, which cost his firm about US6.1 billion (with a 'b').

Anthony further scared delegates with information that a Fannie Mae contract worker planted a rogue script designed to destroy the company's 4,000 servers nationwide. The employee was terminated, but he retained rights to the UNIX system where he planted the script. Cleaning up the mess cost the company more than US$20 million.

In the Heartland case, hackers gained access to the network and stole credit and debit card numbers as they were being processed. Administrators did not catch the activity in the log reports generated by their payment systems.

More than 100 million transactions, containing credit card numbers and IDs were accessed by the hackers and, if you think you are safe because you are not in the US, think again. Anyone in the world who used their credit card to make a purchase, say form a 7 Eleven outlet, could potentially have had their card details exposed.

## Promptly cut access

Anthony's key point was that, terminated employees, sometimes with a chip on their shoulder, are mostly being allowed to walk out the door with thumb drives, CDs and even laptops full of sensitive data. And, they leave with their access codes working too, so they can happily pillage their former companies' crown jewels at their leisure.

It doesn't take a genius to realise that once an employee is terminated, so should any access privileges they have. In fact, perhaps the access privileges should be cut just before they are asked to leave. Anthony told the seminar that at Novell, any terminated employees access is dead within two minutes of them departing – perhaps a good model.

An here's the kicker to all this: another slide from Anthony showed a quote from a Verizon 2008 Data Breaches report which said: "Evidence of events leading up to 82 per cent of data breaches was available to the organisation prior to actual compromise. Regardless of the particular type of event monitoring in use, the result was the same: information regarding the attack was neither noticed nor acted upon."

In other words, if they had proper systems in place, most victim organisations could have discovered the breaches before they happened.

I trust you benefit from this valuable insight and take Anthony's closing advice, which was to adopt a 'culture of compliance', identify critical systems and automate for 'event-based action'.

Credits : Ross Storey; http://mis-asia.com/opinion_and_blogs/

## Research

# CIVILIANS CYBERATTACKED GEORGIA IN 2008 WAR

Attacks on Georgian government websites during the 2008 war with Russia were carried out by civilians - with little or no direct involvement on the part of the Russian government or military -- according to a new report.

The report from the U.S. Cyber Consequences Unit (US-CCU), an independent nonprofit research institute, says that whilst most of those carrying out the cyberattacks were Russians, sympathisers outside Russia joined in as the conflict continued. The organisers of the cyberattacks, however, had advance notice of Russian military intentions, the report said.

Moreover, according to the report, the forums used to recruit and arm the cyberattackers were primarily social networking sites, based in the Russian language.

Some of the web servers and addresses used to control and coordinate the attacks had previously been used by Russian criminal organisations. Also, the botnets used in the first wave of attacks were closely associated with Russian organised crime.

The tools for the attacks appear to have been written or customised specifically for the campaign against Georgia. For example, one tool repeatedly requested non-existent web pages, which overwhelmed servers as they looked for pages that were not there. It specifically targeted 17 different Georgian websites, according to the report.

“The most important lesson here is that Georgia was not prepared for anything of this sort,” Ariel Silverstone, an independent security consultant in Atlanta, told SCMagazineUS.com.

Georgia could have done several things to defend against the attacks, he said.

“They could have had better firewalls. Apparently, they didn't because some of the attacks that succeeded against them were very simple,” Silverstone said.

“Also, some of their sites were not patched,” he added. “And they could have simply shut off the connection to a specific group of subnets -- if an attack coming though the pipe is too strong, shut off the pipe, or divert it.”

“The real story here isn't about Georgia, of course,” John Bumgarner, chief technical officer at the US-CCU and primary author of the report, told SCMagazineUS.com in an email. “It's about the sort of cyber campaign that we can now expect to accompany most future international conflicts if they become intense enough.”

Other observers tend to agree.

“Worldwide, governments need to be more involved and coordinate better on cyber warfare issues,” Sam Masiello, VP of information security at MX Logic, told SCMagazineUS.com in an email. “Cyberwarfare moves at a speed much faster, and has the potential to cause more damage to critical infrastructures quicker, than any military offensive.”

Credits : Chuck Miller; http://www.securecomputing.net.au

## Research

# HACKERS PREFER FIREFOX AND OPERA

New research shows hackers favour running browsers with smaller installed base

Firefox and Opera appear to be the browsers of choice for hackers running web sites that launch drive-by malware attacks, according to new research.

Paul Royal, a security researcher with web security service provider Purewire, is reported to have obtained the data after infiltrating the toolkits used by hackers to carry out these attacks, such as LuckySploit and UniquePack.

The research found that 46 per cent of the hackers use Firefox, while surprisingly Opera is second with 26 per cent, despite having just a two per cent market share.

Ironically, the hackers are using browsers with a smaller market share in order to avoid being hacked themselves, according to Rik Ferguson, senior security advisor at Trend Micro.

"They don't want to get compromised themselves," he said. "They stand to lose a lot - the profits of their criminal operations, control of botnets and so on - so they're looking after themselves."

However, Ferguson warned that Firefox and Opera are not intrinsically more secure than Microsoft's Internet Explorer, or other browsers, just that they have a smaller footprint and do not attract as much attention from malware writers.

As an example, Opera version 9.x currently has 22 security advisories against it and 50 vulnerabilities, 68 per cent of them highly critical, according to the latest intelligence from vulnerability scanning firm Secunia.

Credits : Phil Muncaster; http://www.V3.co.uk

## Survey

# ENTERPRISES NEED TO SECURE DATA DURING APPLICATION DEVELOPMENT

A survey by the Ponemon Institute underscores that many application testers and developers are using real production data without proper safeguards. Experts say it's time for a change.

Sometimes it doesn’t take an external hacker to reveal customer data. Often, it happens during the application development process itself.

That is because, according to a recent survey from the Ponemon Institute, many organizations use production data during their development and testing process without having proper safeguards in place. Some of this, experts say, is due to enterprises underestimating the possibility of an insider threat; other times, it’s simply companies going with what’s easiest.

“Organizations use real customer data because it is easy for developers to just make a copy of a production database that they can use for testing. It takes a lot more effort to encrypt private data or create a phony test database,” said Forrester Research analyst Mike Gualtieri.

His point was underscored by the Ponemon survey, which focused on application developers and testers in the United States and the U.K. In the survey, 71% of the 701 U.S. respondents said that when it comes to the development and testing process, they either don't have adequate policies for protecting data or are unsure – a serious problem, since 80% are using real data.

Often times, enterprises simply do not consider insider breaches as likely as they do external hacks, and therefore there is less concern, noted Gartner analyst Joseph Feiman.

“If an insider, an employee, attacks the enterprise, this is most well-kept secret,” he said. “Enterprises don’t want to lose their reputation. So there is a lack of awareness of insider attacks.”

Developers do have some valid reasons for using real data during the jobs. After all, it does save time and complexity, analysts said.

"As system complexity and interdependencies increase it becomes harder and harder for development teams to create realistic and representative test data," explained David West, an analyst with Forrester. "This difficulty is only increased by the need to deliver more functionality faster and with less people. The third dimension is the lack of knowledge people have of legacy systems and their data. Over time data structures have evolved to such an extent that original labels and definitions are wrong, or at least wrong some of the time."

"The result is development teams look to the only source of true data, that of production," he said.

Still, through technologies such as data masking, enterprises could reduce the threat. Though data masking adoption has grown over the last five years however, the technology remains largely unused by the majority of organizations, analysts said, due to problems deciding what to mask as well as the volume of data. More than two-thirds of the U.S. respondents told the Ponemon Institute they do not mask data before it is used in testing.

Still, Gualtieri contends there is no excuse for organizations to not encrypt or mask data during the development process.

"I recently saw an online travel booking company had unencrypted credit numbers for hundreds of hotel customers," he said. "I told the CEO that he had to address this right away. The biggest difficulty that app dev shops face in encrypting data is to provide a consistent way to encrypt/decrypt the data and manage keys. The best way to do this is to not have developers do it all. It should be automated either in the database or in the data access layer. For example, if they code it Java you can use the Spring framework to inject encryption for named fields automatically. That way developers don't have to remember."

Cerdits : Brian Prince; http://www.eweek.com

## Analysis

# BLIND TEEN SUPER PHREAKERS

### 14-year-old blind kid, angry and alone, discovered that he possessed a superpower — one that put him in the cross hairs of the FBI

It began, as it always did, with a phone call to 911. "Now listen here," the caller demanded, his voice frantic. "I've got two people here held hostage, all right? Now, you know what happens to people that are held hostage? It's not like on the movies or nothing, you understand that?"

"OK," the 911 operator said.

"One of them here's name is Danielle, and her father," the caller continued. "And the reason why I'm doing this is because her father raped my sister."

The caller, who identified himself as John Defanno, said that he had the 18-year-old Danielle and her dad tied up in their home in Security, a suburb of Colorado Springs. He'd beaten the father with his gun. "He's bleeding profusely," Defanno warned. "I am armed, I do have a pistol. If any cops come in this house with any guns, I will fucking shoot them. I better get some help here, because I'm going fucking psycho right now."

The 911 operator tried to keep him on the line, but Defanno cut the call short. "I'm not talking anymore," he snapped. "You have the address. If I don't have help here now, in the next five minutes, I swear to fucking God, I will shoot these people." Then the line went dead.

Officers raced to the house, ready for an armed standoff with a homicidal suspect. But when they arrived, they found no gunman, no hostages, no blood. Danielle and her father were safe and sound at home — alone. They had never heard of John Defanno, for good reason: He didn't exist.

"John Defanno" was actually a 15-year-old boy named Matthew Weigman — a fat, lonely blind kid who lived with his mom in a working-class neighborhood of East Boston. In person, Weigman was a shy and awkward teenager with a shaved head who spent his days holed up in his room, often talking for up to 20 hours a day on free telephone chat lines. On the phone, he became "Lil' Hacker," the most skilled member of a small band of telephone pranksters known as "phreaks." To punish Danielle, who had pissed him off on a chat line, Weigman had phoned 911 and posed as a psycho, rigging his caller ID to make it look like the emergency call was coming from inside Danielle's home. It's a trick known as "swatting" — mobilizing SWAT teams to exact revenge on your enemies — and phreakers like Weigman have used it to trigger some 200 false raids in dozens of cities nationwide.

"When I was a kid, a prank was calling in a pizza to a neighbor's house," says Kevin Kolbye, an FBI assistant special agent in charge who has investigated the phreaks. "Today it's this."

Like a comic-book villain transformed by a tragic accident, Weigman discovered at an early age that his acute hearing gave him superpowers on the telephone. He could impersonate any voice, memorize phone numbers by the sound of the buttons and decipher the inner workings of a phone system by the frequencies and clicks on a call, which he refers to as "songs." The knowledge enabled him to hack into cellphones, order phone lines disconnected and even tap home phones. "Man, it felt pretty powerful for a little kid," he says. "Anyone said something bad about me, and I'd press a button, and I'd get them."

But in the end, those close to Weigman feared that his gift would prove to be his downfall. "Matt never intended on becoming the person he became," says Jeff Daniels, a former phreaker who befriended Weigman on a chat line. "When you're a blind little tubby bald kid in a broke-ass family, and you have that one ability to make yourself feel good, what do you expect to happen?"

Matthew Weigman was born blind, but that was hardly the only strike against him. His family was a mess. His father, an alcoholic who did drugs, would drag the terrified Matt across the floor by his hair and call him a "blind bastard." His dad left the family when Weigman was five, leaving Matt and his older brother and sister to scrape by on his disability pension and what their mother earned as a nurse's aide. For Weigman, every day was a struggle. "There were times I hated being blind," he recalls. At school, as he caned his way through the halls, other kids teased him about how his eyes rolled out of control. "Kids can be cruel, because they don't understand what they're doing," he says. "They can't even begin to fathom what they're causing, and that stuff eats at your mind."

At age four, Matt surprised his mother by making out flashing bulbs on the Christmas tree. After that, he could perceive faint lights — and he exploited the ability for all it was worth. He cooked for himself by feeling his way around the kitchen — eggs here, frying pan there, toaster over there — and refused to stop, even after he burned himself. He shocked his brother by climbing on a bicycle and tearing down the road, using the blurry shadows for guidance. He taught himself to skateboard, too. To build his confidence, his mom's new husband let the eight-year-old Matt drive his car around the empty parking lot at Suffolk Downs, a nearby racetrack. "It made me feel a lot better," Weigman recalls. "I thought, 'I'm doing something that people who see can do.'"

And he could do one thing even better than sighted people: hear. Weigman became obsessed with voices, music and sounds of all sorts. He could perfectly mimic characters he heard on the Cartoon Network, and he played his favorite songs on a small keyboard by ear. He would also dial random numbers on the phone, just to hear who picked up — and what kind of response he could elicit from them. He fondly recalls the first time he called 911, at age five, and duped them into sending a cop to his door.

"You need the police?" the officer asked.

"No," Weigman replied. "I'm just curious. I wanted to see what the operator would do."

The cop reprimanded the boy sharply. "I wouldn't do that no more," he said.

But Weigman was hooked. In real life, he was gaining weight and dodging bullies, struggling to find a place to fit in. By age 10, however, he had found the perfect escape: a telephone party line. The service — a precursor to Internet chat rooms — allows multiple callers to talk with each other over the phone. Despite the rise of online video streaming, there are still scores of telephone party lines scattered across the country, an odd and forgotten throwback to a pre-digital world. Compared to texting or video chat, the phone lines have a unique appeal: They offer callers a cloak of anonymity coupled with the visceral immediacy of live human voices. Some call to socialize, others for phone sex.

Hoping to give Weigman a social network beyond the confines of his tiny bedroom, a friend had slipped him the number of a free party line known as Studio 55. The second Weigman called, a new world opened up to him. He heard voices. Some were talking to each other. Others piped in only occasionally, listening in as they watched TV or played video games. Weigman found he could decipher each and every ambient sound, no matter how soft or garbled. Many of the callers were social misfits and outcasts: ex-cons and bawdy chicks and unemployed guys with nothing better to do all day than talk shit to a bunch of complete strangers. People without a life. And that's when it hit Weigman: No one here could see each other. They were all just disembodied voices. "We're all blind right now," he announced to the group.

Weigman wasn't a freak anymore. But he was about to become a phreak.

Telephone phreaking isn't new: The practice, which dates back half a century, was the forerunner of computer hacking. In 1957, a blind eight-year-old named Joe Engressia accidentally discovered that he could whistle at the precise frequency — 2,600 hertz — used to control phone networks. A pioneering phreak named John Draper later realized that the free whistles given out in Cap'n Crunch cereal boxes also replicated the exact same tone. Kids with a mischievous streak and too much free time were soon competing to see who could achieve the most elaborate phone hack. A tech-savvy student named Steve Wozniak, who would soon invent something called Apple with his friend Steve Jobs, once used a series of high-pitched whistles to make a free international call to the Vatican to prank the pope.

As he listened in on the party lines, Weigman began pressing random numbers on his phone, just to see what would happen. Once he held down the star button and was surprised to hear a computerized voice say, "Moderator on." He had no idea what it meant. But when he hit the pound key, the voice suddenly began ticking off the private phone number of every person in the chat room. Weigman had discovered a secret tool through which a party-line administrator could monitor the system. Now, whenever someone on the line trash-talked him, he could quietly access their number and harass them by calling them at home.

By 14, Weigman was conning his way through AT&T and Verizon, tricking them into divulging insider information — like supervisor identification numbers and passwords — that gave him full run of the system. If he heard a supervisor’s voice once, he could imitate it with eerie precision when calling one of the man’s underlings. If he heard someone dialing a number, he could memorize the digits purely by tone. A favorite ploy was to get the name of a telephone technician visiting his house, then impersonate the man on the phone to extract codes and other data from unsuspecting co-workers. Once he called a phone company posing as a girl, saying he needed to verify the identity of a technician who was at “her” door. Convinced, the operator coughed up the technician’s company ID number, direct phone line and supervisor — key information that Weigman could later put to nefarious use, like cutting off a rival’s phone line.

There seemed to be no limit to what he could do: shut off your phone service, dig up your unlisted cellphone number, even listen in on your home phone — something only a handful of veteran phreaks can pull off. Celebrities were a favorite target. Weigman claims to have hacked and called the cellphones of Lindsay Lohan (”She was drunk, and my friend tried to have phone sex with her”) and Eminem (”He told me to fuck off”). Last year, during the presidential campaign, Weigman heard a YouTube video of Mitt Romney’s son Matt dialing his dad. Weigman listened closely to the touch tones, deciphered the candidate’s cellphone number — and then made a call of his own. “Mitt Romney!” he said. “What’s going on, dude? Running for president?” Weigman says Romney told him to shove the phone up his ass, and hung up.

In addition to relying on his heightened sense of hearing, Weigman picked up valuable tips on phone hacking from other phreaks on the party lines. One of the most valuable tricks he learned was “spoofing” — using home-brewed or commercial services, such as SpoofCard, to display any number he chose on the caller- ID screen of the person he phoned. Intended for commercial use — allowing, say, a doctor to mask his home phone number while calling a patient — SpoofCard is perfectly legal and available online for as little as $10. Some services let callers alter their voices — male to female — as well as their numbers.

Weigman performed his first “swat” at age 14, when he faked an emergency call from a convenience store down the street from his home. “Listen,” he told the 911 operator, “there’s a robbery here! I need you to show up right now!” Then he hung up and called his brother, who was standing watch outside the store. “Oh, God, dude!” his brother told him. “There’s police everywhere!”

“Really?” Weigman replied in awe. Over the phone, he heard sirens wail in the darkness.

Weigman began spending several hours a day talking shit on assorted party lines. When someone on the line would challenge him or piss him off, he would respond by faking a 911 call and sending an armed SWAT team to their door. “I probably did it 50 or 60 times,” he says.

He spent most of his time on party lines like Jackie Donut and Boston Loach, which teemed with lowlifes, phreakers and raunchy girls whom Weigman calls “hacker groupies.” Men on the party lines competed to see who could score the most. “A lot of guys on there were looking for free phone sex,” says Angela Roberson, a tongue-pierced blonde from Chicago who got to know Weigman on Boston Loach. The 34-year-old Roberson, who stumbled on the line one night when she was bored and drunk, found its rough-and-tumble community oddly appealing. “You can sit and talk smack to whoever you want to,” she says. “You get to live in a whole different world.” Weigman might be overweight and blind and stuck in his room, but the party line provided him with plenty of opportunities the real world didn’t offer. When asked how much phone sex he had, he says, “Oh, Jesus, man — too much.”

Weigman soon realized that one caller on the party line got his way with the hacker groupies more than anyone else. Stuart Rosoff, a middle-aged party-liner from Cleveland, had started out as a teenager making obscene phone calls and ended up serving three years in prison. Overweight and unemployed, with a hairy chest and thick mustache, Rosoff cruised the party lines for girls, introducing himself as Michael Knight, after David Hasselhoff’s character on Knight Rider. He was also a member of a gang of phreaks nicknamed the Wrecking Crew.

When Rosoff didn’t get what he wanted on the party line, he turned ugly. “Stuart was a malicious phreaker,” says Jeff Daniels, the former phreak who hung out on the party line. “He was limited in knowledge, but good at things he knew how to do.” One time, showing off to Weigman, Rosoff singled out a woman who had refused him phone sex and called the police in her hometown, scrambling the caller ID to conceal his identity. The woman, he told the cops, was abusing her kids — causing the 911 operator to dispatch police officers to her door. Having proven his power, Rosoff called the woman back and demanded phone sex again. If she didn't want to do it, he added generously, he would gladly accept it from her daughter.

"Stuart was like a mentor to Matt," says Roberson. "They would joke around and threaten to shut each other's phones off just because they were bored." It wasn't long, however, before Weigman surpassed Rosoff as a phreaker. He began to harass the older man, disconnecting his phone and digging up his personal data to use for leverage and revenge. Phreakers call this "the information game," and Weigman was the undisputed master. Rosoff was soon reduced to groveling on the chat lines, begging Weigman to leave him alone.

Roberson felt threatened by Weigman and by Rosoff, who kept pestering her for phone sex. Once, after a confrontation with Weigman, she picked up her phone only to hear the high-pitched squeal of a fax machine in place of the dial tone. It had been rigged to last all night. Despite Weigman's denials, Roberson claims he also hacked into her voicemail. To protect herself from attacks, she became close to another member of Rosoff's gang, eventually moving in with him and taking part in one of the Wrecking Crew's pranks.

Roberson was surprised when she learned that Weigman was just a teenager. "I would have never thought that he was a 16-year-old," Roberson says. "He was smart, and he was feared." When Weigman called up a party line, he would brashly announce his presence in the chat room with a little smack talk: "How you doing, you motherfuckers?" He might be an overweight blind kid, but on the party lines, he could be whoever he wanted. "That's why he did what he did," says Roberson. "He was insecure, but he could be powerful here."

As Weigman's reputation as a phreaker surpassed even Rosoff's, his hobby became an obsession. In a single month, he would place as many as 40,000 calls — ranging from a few seconds in length to several hours. He dropped out of 10th grade, spending all day on the phone. His mother was proud that he had found something he was good at and glad he had finally made some friends, if only on the phone. "She left it alone because it was my social outlet," Weigman says. Matt was also using his newfound skills to bill purchases to bogus credit cards, snagging everything from free phone service to Dunkin' Donuts gift cards. ("I love Dunkin' Donuts!" he says.)

Weigman became a master of what phreakers call "social engineering" — learning phone-industry jargon and using it to manipulate telecommunications workers. One day, Weigman picked up the phone and dialed AT&T. Two rings, then a voice: "Thanks for calling, this is Byron. How can I help you?"

"How you doing, Byron?" Weigman asked, adopting the tone of an older man, one at ease with his own authority.

"Good," Byron said. "And you?"

"I'm doing all right. My name is William Jones. I'm calling you with AT&T asset protection. I'm actually working on a customer-fraud issue. We need to write out a D order." In a few short sentences, Weigman had appropriated the name, voice and lingo of a real AT&T agent, ordering a rival's phone to be disconnected.

"What's the telephone number?" Byron asked. Weigman rattled off the name and number on his rival's account. Then, to authorize access, he gave Byron the AT&T security-ID code belonging to Jones.

For a moment, the phone filled with the sound of rattling computer keys being struck by expert fingers.

"Looks like it's paid in full," Byron said, puzzled.

"Yeah," Weigman said, "we're looking at a fraud account, sir. We're just going to have to take that out of there."

As Byron filed a disconnection order, Weigman made idle chitchat in his "Jones" persona, speculating on the twisted minds of phone phreaks. "Deep down, I know that they know someday they're going to get caught up, you know?" he told Byron. "They just really don't think about it. It's crazy."

The words applied to Weigman himself. By now, he had "stoolies" on the party lines eager to do his bidding. As his power on the phones grew, he began to change. Unable to take the teasing and the pity he got for being blind, he grew sneering and mean, lowering his voice, adopting a manly bluster. Using the phone to lash out at others, he directed all the rage he felt at the world against his fellow phreaks. To prove his prowess, he targeted Daniels, a 37-year-old from Alabama who had been arrested for phone hacking as a teenager. "He was calling my landlord and telling him I was a child molester and that I killed people," Daniels claims.

Still, there was something sympathetic about the kid. “To me, he was still a boy,” Daniels says. Having been to jail himself, he didn’t want Weigman to make the same mistakes he had. So he got Weigman’s attention the only way he could: by beating him at his own game. When Weigman refused to stop the phone attacks, Daniels tracked down the teenager’s detailed personal information, including his Social Security number. That earned him Weigman’s respect, and the two became friends. They would talk for hours on the phone at night, Weigman’s put-on baritone suddenly replaced by a more childish tone. “He was not the big shot he made himself out to be,” Daniels realized.

Weigman opened up about his miserable and impoverished life, crying as he told Daniels how much he longed to see the world with his own eyes. His weight fluctuated from boyishly pudgy to extremely obese, and he was spending more and more time locked in his room upstairs, listening to Nirvana and Muddy Waters. One time, a teacher took his class to a blues club in Boston, and the music seemed to capture what he was feeling: the poverty, the despair, the sense of being trapped. “He lived in a jail at home,” says Daniels. “He lived in a box.”

Daniels urged him to drop the macho bullshit on the party lines and stop drawing attention to himself. Weigman agreed to keep his mouth shut and even christened his new self-image with a more stoic nickname. From now, on he would no longer be Lil’ Hacker. He called himself “Silence.”

On a June night in 2006, James Proulx was watching television at 1 a.m. when a SWAT team suddenly surrounded his home in Alvarado, Texas. A stocky, gray-haired trucker who had recently undergone open-heart surgery, Proulx went to the door, where he was confronted by two armed policemen — their guns pointed directly at him. The officers threw Proulx to the ground, snapped handcuffs on him and put him in the back of a squad car.

They had reason to be suspicious. A call to 911 had come in from Proulx’s house; a man identifying himself as Proulx said he was tripping on drugs and holding hostages. He demanded $50,000 so he could flee to Mexico. He also claimed to have killed his wife. If any cops got in his way, he warned, he’d kill them, too.

As the police soon discovered, however, Proulx was just another swatting victim. It turned out that Proulx’s 28-year-old daughter, Stephanie, spent time on Jackie Donut. When she clashed with Weigman and others, they decided to strike back. “If a female wouldn’t give Matt phone sex,” she recalls, “he would call them a fucking bitch and send a SWAT team to their house." Weigman considered Proulx a "crazy chick who would threaten hackers," and he was very direct with her. "You're annoying," he told her. "I might come after you." Four months after Stephanie's father was swatted, police showed up at her home in Fort Worth, Texas, drawn by a fake call to 911.

One afternoon, not long after Proulx was swatted, Weigman came home to find his mother talking to what sounded like a middle-aged male. The man introduced himself as Special Agent Allyn Lynd of the FBI's cyber squad in Dallas, which investigates hacking and other computer crimes. A West Point grad, Lynd had spent 10 years combating phreaks and hackers. Now, with Proulx's cooperation, he was aiming to take down Stuart Rosoff and the Wrecking Crew — and he wanted Weigman's help.

Lynd explained that Rosoff, Roberson and other party-liners were being investigated in a swatting conspiracy. Because Weigman was a minor, however, he would not be charged — as long as he cooperated with the authorities. Realizing that this was a chance to turn his life around, Weigman confessed his role in the phone assaults.

Weigman's auditory skills had always been central to his exploits, the means by which he manipulated the phone system. Now he gave Lynd a first-hand display of his powers. At one point during the visit, Lynd's cellphone rang. "I can't talk to you right now," the agent told the caller. "I'm out doing something." When he hung up, Weigman turned to him from across the room. "Oh," the kid asked, "is that Billy Smith from Verizon?"

Lynd was stunned. William Smith was a fraud investigator with Verizon who had been working with him on the swatting case. Weigman not only knew all about the man and his role in the investigation, but he had identified Smith simply by hearing his Southern-accented voice on the cellphone — a sound which would have been inaudible to anyone else in the room. Weigman then shocked Lynd again, rattling off the names of a host of investigators working for other phone companies. Matt, it turned out, had spent weeks identifying phone-company employees, gaining their trust and obtaining confidential information about the FBI investigation against him. Even the phone account in his house, he revealed to Lynd, had been opened under the name of a telephone-company investigator. Lynd had rarely seen anything like it — even from cyber gangs who tried to hack into systems at the White House and the FBI. "Weigman flabbergasted me," he later testified.

But Weigman's decision to straighten out didn't last long. "Within days of agreeing to cooperate, he was back on the party line, committing his crimes again," Lynd said. Weigman didn't like being cut off from the only community he had. "I was a hardheaded little kid, and I wanted to do what I wanted to do," he recalls. "I didn't think this could be serious." He was also obsessed. "He's not a criminal — he's an addict," says his friend Daniels. "He's addicted to Silence, to Lil' Hacker, to being the person who is big and bad and bold. He's addicted to being the person who can get every girl to do what he asks over the phone."

Daniels, who owns a party line called the Legend System After Dark, tried to channel Weigman's energy in a more positive direction by giving him a position as a moderator, making him responsible for managing the phone chats and reining in jerks like Rosoff. As Weigman ran the calls, he began softening up. He even had a girlfriend in her 30s, Chastity, whom he had met on a party line. He seemed calmer since he met her, more the kid he really was. When they had relationship troubles, he confided in Daniels rather than swatting her.

Before long, though, Weigman returned to his old ways. Daniels began hearing from party-liners who said they were being harassed by the kid. "Knowledge is power," Daniels told Weigman, "but you're using it for the wrong reasons. They're going to put you in jail, and you being blind isn't going to save you." But Weigman wouldn't listen. "He saw himself as this underage blind kid in a poor family," Daniels recalls. "So how were they going to put him in prison with big guys who might want to whup his ass?" Unable to reform his friend, Daniels had to let Weigman go.

When the FBI finally busted the Wrecking Crew, Weigman's reputation grew. Recordings and details of his fake 911 calls, including the swatting in Colorado, leaked and spread online. The attention only made Weigman grow more paranoid and vengeful. He stepped up his campaign of intimidation, warning his victims that any cooperation with investigators would warrant new attacks. He told one woman he'd make her life a "living hell" and put her husband out of business. He threatened a woman in Virginia with a swatting attack — and ended up calling in a bomb threat to a nursing home where her mother worked in retaliation for her talking to the FBI. He phoned a mother in Florida and said that if she gave his name to investigators, he'd kill her baby by flushing it down the toilet.

In 2007, Rosoff and other party-liners pleaded guilty to swatting. “I’m kind of like a nobody in real life,” he told the judge. “I was actually somebody on the phone, somebody important.” In a plea agreement that limited his prison sentence to five years, Rosoff ratted out his rival, saying that Weigman had participated in “targeting, executing and obtaining information to facilitate swatting calls.”

But Weigman was still a minor, and the FBI didn’t want to go after him. In a sense, he was being offered a break. As long as he cleaned up his act, he wouldn’t be prosecuted. All he had to do was walk away before April 20th, 2008 — the day he would turn 18. After that, any crime he committed would get him tried as an adult.

Late one night that April, the telephone rang at the New Hampshire home of William Smith, the Verizon fraud investigator who was working with the FBI. When Smith picked up, however, there was no one on the other end of the line. In the nights that followed, it happened again and again. At first, Smith didn’t make much of it. Then one night, his wife looked at the caller ID and noticed something strange: It was Smith’s work number, even though he was there at home. “Something’s not right,” she told him.

Smith changed his home number, but it made no difference. The phone would ring again at all hours — this time with Smith’s own cellphone as the point of origin. Weigman, he soon learned, was using his skills and his network of stoolies to ferret out Smith’s private phone numbers and harass him. And he knew Weigman’s history well enough to know exactly where the calls were leading: a swatting attack. “He was fully aware that he might be subject to violence by proxy if Weigman chose to make a false emergency call,” Lynd testified.

In the midst of the harassment, Smith called a travel agent and booked a flight for his wife to visit their son in Georgia. Then he called his son to inform him of the travel plans. Minutes later, the phone rang. This time, the caller ID showed his son’s phone. But when Smith picked up, it wasn’t his son after all. It was Weigman. Matt was using his phone-company connections to track every call that Smith made and received — and the veteran fraud investigator for Verizon could do nothing to stop him.

Then, one Sunday in May of last year — on a weekend after his wife had flown to Georgia — Smith was working in his yard when a car pulled up. Out stepped three young men, including one with strange, broken eyes. “I’m Matt,” the boy told Smith.

Weigman had driven up from Boston with his brother and a fellow party-liner. Standing in the yard, he could make out Smith’s dark, shadowy figure against a blotch of white light, and he heard the investigator’s familiar Southern accent — the one he had so easily identified on agent Lynd’s cellphone. Weigman told Smith he wasn’t there to threaten or hurt him — he just wanted to persuade him to call off the investigation. After years of intimidating others, Weigman was now the one who felt intimidated. He wanted it all to stop.

But Smith wasn’t having any of it. He went inside and called the police, who quickly showed up. Weigman didn’t run. He told the cops he had done things that were “not so nice.” When the officers asked what he meant, he said, “swatting.” But after a lifetime of being teased and abused, Weigman was unable to see himself as anything but a victim. He was just a young blind kid, and here he was getting bullied again. Smith, he told the officers, had a “vendetta” against him.

Less than two weeks after he showed up at Smith’s house, the police knocked on Weigman’s door outside Boston and arrested him. Weigman soon found himself being interrogated by an FBI agent. He listened in darkness as the agent dialed a number on his phone. Thirty minutes later, he spouted back the number by heart — and even knew what it was. “That’s the main number of the FBI office here in Boston,” Weigman told the astonished agent.

But now that Weigman was 18, his powers couldn’t save him anymore. Last January, he pleaded guilty to two felony counts of conspiracy to commit fraud and intimidate a federal witness. In June, he was sentenced to 11 years in prison.

These days, sitting in a small holding cell in a Dallas prison, Weigman bears no resemblance to the hulking psycho he portrayed on the party lines. Dressed in an orange jumpsuit, he’s slim and soft-spoken, his head shifting as he talks. “I’m not a monster or a terrorist,” he says. “I’m just a guy who likes computers and telephones. I used my ability to do certain things in the wrong way. That’s it.” As Weigman recounts his story, he slips effortlessly into the voices of the people he met along the way. Every ambient noise — a guard’s chatter, a bag unzipping, a computer disc whirring — draws a tic of his attention.

"Let me tell you something, man," he says, his voice a bit like that of a young Elvis. "If I would have been just a little more mature, if I could just rationalize better, I think I would have been all set. If, when I was young, I had a full-time male father figure in my life…." He stammers a bit, then recovers. "Not having my dad didn't really bother me," he says, "but inside, it kind of messed me up a bit."

Above all, though, Weigman is still a teenager. While he expresses remorse over his swatting attacks, he takes giddy pleasure in recounting his other exploits — whether punking celebrities or playing the phone companies like an Xbox. "The phone system and infrastructure is just weak," he says. "I had access to the entire AT&T and Verizon networks at times. I could have shut down an entire area." Then he segues into an earnest pitch for a future job. "I'd love to work for a phone company, just doing what I do legally," he says. "It's not about power. I know the phone and telecommunication systems and can be a crucial part of any company."

In the meantime, he's free to brush up on his skills. Though he's restricted from calling party lines, he has phone access in prison. For a self-described telephone addict, it seems almost cruel, like imprisoning a crackhead with a pipe and a rock. Could he use the prison phone the same way he used his home phone? Could he hack his way, from his prison cell, beyond the guard towers and the razor wire, into the world outside?

Weigman bobs his head and kneads his hands. "I'm sure I could," he says.

Credits : http://www.thepeoplesvoice.org

## Education

# HOW BOTNETS GENERATE MILLION-DOLLAR REVENUES FOR CYBERCRIMINALS

A botnet is a network that consists of computers infected by malicious software, which allows Cybercriminals to control the infected machines remotely without the users' knowledge.

Botnet owners' sources of income include DDoS attacks, theft of confidential information, spam, phishing, search engine spam, click fraud and distribution of malware and adware.

A botnet is an ideal tool for carrying out a DDoS attack. Such attacks can be used as an instrument of unfair competition or be manifestations of cyberterrorism. Confidential information kept on users' computers can also be targeted by botnet owners. The most valuable data includes credit card numbers, financial information and passwords to various services.

New phishing sites are now mass-produced by Cybercriminals, with botnets used to protect sites from closure. The income from phishing is comparable to that from the theft of confidential data using malicious programs and adds up to millions of dollars per year. About 80% of all spam is sent via zombie networks. In the past year, spammers made about $780 million.

Resources provided by zombie networks can also be used to distribute adware and malicious programs. Online advertising agencies that use the PPC (Pay-Per-Click) scheme pay for unique clicks on advertisements. Botnet owners can make significant amounts of money by cheating on such companies. About 17% of all advertising link clicks in 2008 were fake, of which a third was generated by botnets.

Today, the most effective method of combating botnets is to join the forces of antivirus experts, ISPs and law enforcement agencies. Such cooperation has already resulted in the closure of three companies: EstDomains, Atrivo and McColo, whose servers hosted command and control centers for major spam botnets.

According to Yury Namestnikov, antivirus analyst at Kaspersky Lab, only law enforcement agencies can stop the command and control centers and catch Cybercriminals. On the other hand, it is obvious that without help from users, combating botnets cannot be effective, since it is home computers that make up the lion's share of all bots. It is important for users to stick to simple IT security rules.

Credits : http://www.securitypark.co.uk

# EVENTS

## iT'S Bengaluru

**Location :** Hotel Chancery Pavilion, Bangalore
**email :** jairaj@totalesp.org
**Website :** http://www.totalesp.org/

| Date | Themes | Tracks |
|---|---|---|
| 22 August, 2009 | Information & Communication Technology applications | Banking, Insurance, Finance Sector(NSE, BSE, Commodity Exchanges,NSDL & SEBI) |
| 29 August,2009 | Information & Network Security | Non IT Sector (Manufacturing,Services, Academics) |
| 5 September, 2009 | Technology & Management | Telecom Sector |
| 12 September, 2009 | Information Security Strategy Management | Core IT Sector |
| 19 September, 2009 | Technology Management | Hardware Network and BPO Sector |

**Media Partners :** CCC News Control Computer Crimes

## FRHACK 01 (by hackers, for hackers)

**Date :** September 7, 2009
**Location :** Besançon - France
**Website :** http://www.frhack.org

## Cyber Conflict Legal & Policy Conference 2009

**Date :** September 9, 2009
**Location :** Tallinn, Estonia
**Website :** http://www.ccdcoe.org/legalconference/5.html

## OWASP Ireland AppSec 2009 Conference

**Date :** September 10th 2009
**Location :** Trinity college,Dublin

**Website :**
https://www.owasp.org/index.php/OWASP_Ireland_AppSec_2009_Conference

## IMF 2009

5th International Conference on IT Security Incident Management & IT Forensics

**Date :** September 15, 2009
**Location :** Stuttgart, Germany
**Website :** http://www.imf-conference.org

## HITB Security Conference 2009

**Date :** October 5, 2009
**Location :** Malaysia
**Website :** http://conference.hackinthebox.org/hitbsecconf2009kl/?page_id=292

## "Bangalore Cyber Security Summit- 2009"

a National Conference on Cyber Security

**Date :** 8-9 October, 2009
**Location :** Hotel Ashok, Bangalore, India
**email:** osd@bangaloreitbt.in, kulkarnitr@gmail.com

## Gitex Technology Week

**Date :** October 18, 2009
**Location :** Dubai International Conventional Exhibition Centre, Dubai
**Website :** http://www.gitex.com/

## fourth annual eCrime Researchers Summit (eCRS)

**Date :** October 20, 2009
**Location :** Tacoma, WA, USA
**Website :** APWG <http://www.antiphishing.org/>
http://www.ecrimeresearch.org/2009/cfp.html

## The 3rd International conference on IPRs

Personal Data Protection and National Security

**Date :** October 20-22, 2009
**Location :** Beirut, Lebanon
**Website :** http://www.cybercrime-fr.org/index.pl/cyberlaw2009

## OWASP AppSec Brasil 2009

**Date :** October 27, 2009
**Location :** Câmara dos Deputados in Brasília, DF
**Website :** https://www.owasp.org/index.php/AppSec_Brasil_2009

## T2'09

**Date :** 29 October, 2009
**Location :** Câmara dos Deputados in Brasília, DF
**Website :** http://www.t2.fi/

## New age cyber crime – by Marcusevans

Date: 29 & 30 October 2009
Location: Le Royal Meridian, Mumbai, India
Email: leec@macrusevanskl.com

**Media Partners :** CCC News Control Computer Crimes

# QUIZ 0006

1. Facebook is also called a _______ networking site.

2. Indian competitor of Google earth is called _________.

3. In reporting bugs / errors, reporting a non-existing bug / error is called false _______.

4. A program downloaded with limited features for evaluation, which can be purchased later, if liked, is called _________.

5. An IP address (in IPv4 or IP version 4) has 4 dot-______ notations.

## Terms & Conditions

1. One Grand Prize winner will be awarded a cash prize of INR 1000.00.
2. Three consolation prizes will be gift hamper of 3 books published by CRPCC/Sysman.
3. Winners having all correct entries will be selected by lottery.
4. If there is no "all corrrect" entries no prize will be awarded.
5. Decision of CCCNews will be final and can not be challenged.
6. Gift hampers will be collectable from CCCNews office in Mumbai.
7. Last date to send entries is 10 September 2009 IST 24:00 hrs.
8. Winners will be declared in next issue of CCCNews Magazine.
9. Please send email with correct answers of all 5 questions to quiz@cccnews.in with your name, age, designation (if any), company (if any), Postal address, Phone no. & email address, please write "Quiz 0006 answers" in subject.
10. Ambiguous answers may be out right rejected

# Answers to Quiz 0005

1. Penetration Testing can also be described as ***(ETHICAL)*** hacking.

2. Conficker is a type of ***(WORM)***.

3. Copy back the Backed-up data is called ***(RESTORE)***.

4. In windows, by deleting a file using "delete key", the file is not deleted but available in ***(RECYCLE BIN)*** folder.

5. The device used to filter and analyse the flow of data between your computer and internet / network is called ***(FIREWALL)***.

## Winners for Quiz no 0005

### Grand Prize

Aprenta Bhutia, Sikkim, India

### Three consolation prizes

1. Carlos Sauser, Madrid, Spain
2. Hemant Dhar, Rourkela, India
3. Martin James, Tiruchi, India

**Congratulations to all winners and others with correct answers.**

## Sysman Computers Private Limited, Mumbai

1. Pioneer in IT Security since 1991
2. Empanelled with CERT-In
3. Done over 2000 IT Security assignments
4. Provide Research Support
5. Create Public Awareness
6. Published 6 Books / 50 papers
7. An associate consultant to BSI to implement ISO 27001-ISMS

**Contact –**

**Sysman Computers Private Limited, Mumbai**

sysman@sysman.in

**+91-99672-48000**

**www.sysman.in**