

EDITORIAL NOTE

From the Editor

Well folks, after this issue and the obvious intensity of the insecurity of the net, I have a few thoughts on the unfettered access to knowledge.

It is more than apparent we all live in a time where the extensive dissemination of opinions, thoughts and ideas and information are done through a modern method of transmission. The simplicity and effectiveness by which computers and networks are used to assemble, store, search, associate, recover, and share information make computer technology especially risky to anyone who wishes to keep personal or protect information from the public sphere or out of the clutches of anyone who is perceived as a probable threat. As this issues explores, the evolving and more advanced capabilities of computer viruses, phishing, fraud schemes, spyware, and hacking activity springing up from every corner of the globe and the diversity of privacy-related issues engendered by computer technology has led to a reassessment of the concept of privacy and of computer ethics.

Originally, a hacker was identified simply as any individual who wanted to understand every thing humanely possible about computers. But it wasn't long before hacking came to be linked with phreaking, (The skill or science of breaking the phone network. Example; to make illegal, free long-distance calls). It wasn't long before a plan for "hacking ethics" originated from the activities of the so-called "original hackers" in the 1950s and 1960s at MIT and Stanford University. Technology writer Stephen Levy has summarized those "hacker ethic" in this way.

- 1. Access to computers should be unlimited and total.
- 2. All information should be free.
- 3. Authority should be mistrusted and decentralization promoted.
- 4. Hackers should be judged solely by their skills at hacking, rather than by race, class, age, gender, or position.
- 5. Computers can be used to create art and beauty.
- Computers can change your life for the better.

The understanding of "Hacker Ethics" has three main functions:

- 1. It promotes the belief of individual activity over any form of corporate authority or system of ideals.
- 2. It supports a completely free-market approach to the exchange of and access to information.
- 3. It promotes the belief that computers can have a beneficial and life-changing effect.

Without a doubt, unreserved access to the resources and information on the Internet is clearly an essential mechanism for business and business opportunities, medical services, educational opportunities, and employment and many other requirements of modern life around the world.

But more important than material or monetary requirements is the uninterrupted access to uncensored life giving, freedom sustaining knowledge of events and discourse. It is more than wresting a few dollars worth of free phone calls from the phone company. The stakes are far higher. "There's a time when the operation of the machine becomes so odious, makes you so sick at heart that you can't take part! You can't even passively take part! And you've got to put your bodies upon the gears and upon the wheels, upon the levers, upon all the apparatus -- and you've got to make it stop! And you've got to indicate to the people who run it, to the people who own it -- that unless you're free the machine will be prevented from working at all!!" Though perhaps cloaked, hacking is a universal form of civil disobedience. It is a form of laying bare the truths our betters deign to trust with the rabble of civilization. Why else are the national security apparatus' of nations across the globe sentenced to fitful restless nights? Transparency /Sunlight are the best disinfec tant. When the last forest and indigenous peoples of the earth are ground into dust beneath the heel of militarism and materialism it will be too late. Hacking, exposing the minions of mammon is a key component of sustaining the planet and the mind of man.

Unfettered access to knowledge, oh yeah!

Mohit KumarFounder and Chief Editor

The Hacker News Security Services

The Hacker News Team

Kislay Bhardwaj

Patti Galle

Priyanshu Sahay

Nitin Bhardwaj

No One is Secure

In this era of internet, security is just an illusion. It is like a blind man checking that the doors of his house are secure but forgetting to check whether there are walls around it or not. Today a mere search of someone shows hundreds of records on them. There are social security numbers, Facebook profiles, blogs, websites, phone numbers, addresses, interests, likes, dislikes, hobbies, friends information and more that results in their online biography. Today even a child in 3rd grade is on Facebook. If you are an older person who can't walk or a student who met with an accident there are some who will post photos of their accident or disabilities. Hackers hacked Sony, the FBI hacked xss in Microsoft, and the news we read of it shows where we stand in sense of security.



For instance, you might not know that right now spyware is sitting in your pc and transmitting your information. This gives the ability of someone on the other side of world the ability to log into your account.

It doesn't stop there. There is much more which I haven't covered and which is still to be uncovered. Every day a new "0" day comes and many websites are compromised leaking your personal information, your account and contacts. Google uses your information, searches your mails, your friends, your likes and dislikes for customizing your search results. Facebook is recording your chats, and identifying you by your tagged photos and might be transferring it to some federal agencies. You don't know when someone is intercepting your calls and messages or who is using your stored information.

Then contact details are backed up on the server of some telecom server. If it wasn't bad enough, your contact details are backed up on some telecom server. If you have an online identity then it's sure that someone has an eye on you and about 10 to 15 pages of information about you stored somewhere. You are not secure even if you feel so. I want to share an incidence about when I went to a concert and after few days one of my friends asked me about it. I was totally amazed that he knew I was there as I hadn't told any one about going. I understand that some chap was clicking their girlfriend's photo and I was there in background and my friend saw these photos somewhere on the internet.

Every day you leak a lot of information about yourself or someone else when you upload a photo, comment, and login to some site, ask something, post an answer or post your views. Because of this, every day you are reducing the blurriness of your identity, every day you uncover yourself a bit more with your activity online. You count on the numerous sites which you login into to maintain your security but you don't know whether they will. Mostly, even if you are unable to trust them it is almost impossible to stop using those services because you are trapped in to the self created web of illusion and urge of that service. Many among you use weak passwords or the same password on multiple sites. Many don't check whether the site they just logged into is really the site you were thinking of or just a replica of it revealing your credentials to someone sitting anywhere in the world or next door.

Now the big question is what can you do to be secure, how can you protect your identity? The answer is "you can't", but you can make it harder and more complicated for any one to track you. You can do this by either misleading them with some big and wrong information or by creating multiple identities online according to your needs. Things like a separate identity for your friends and another identity for your official life and one for the rest of the world. Granted this is not the best way to be secure in this world but you could lock yourself in a dark room and disconnect yourself from the rest of the world and internet. In other words.......the reality is "no one is secure".

Submitted By:

Anand K. Pandey
Anandkpandey@in.com





#Fail 2011

Year of the Hack

According to IT security experts Year 2011 have labeled as the "Year of the Hack" or "#Fail 2011". Hacking has become much easier over the years allowing hackers to hack into systems easier then ever before, which is why 2011 had a lot of hackings happen so far. Hackers are coming up with tools as well as finding new methods of hacking faster than companies can increase their security.

Every year is the year of the hacking as long as there are hackers out there ready to execute their malicious programs and attain their goals like gathering important information from the victim's computer, stealing important identities, credit card information, etc. 2011 could produce another generation of hacking. Every year there are always forward advancements of the tools and programs that could use by the hackers.

Have a look to some Major Hacking Cases of 2011



RSA Hack (3/17/2011)

Motive - Unknown attacker, although China believed to be suspect. Motive is probably espionage

Method - Advanced Persistent Threat (APT) targeted at individuals within an organization using social engineering. Malware hidden in an Excel spreadsheet exploited a zero-day (unpatched) Flash hole.

Harm - SecurID token deployments at financial, government and other sites were at risk.

Comodo Hack and several of its digital certificate resellers (3/23/2011)

Motive - 21-year-old Iranian patriot took credit saying he was protesting US policy and retaliating against the US for its alleged involvement with last year's Stuxnet, which experts say was designed to target Iran's nuclear program.

Method - Compromise of digital certificate registry authorities led to the theft of digital certificates that are used by sites to prove they are who they are legitimate.

Harm - If they had not been revoked the faked certificates could have been used to spoof sites like Google, Yahoo, Microsoft and Skype.

Sony (Indonesia, Japan, Thailand, Greece, Canada, Netherlands, Europe, Russia, Portugal) & Sony PlayStation Network Hacked (4/6/2011-6/8/2011)

Motive - Lulzsec ,Anonymous, Lebanese hacker Idahc and various other hackers organized the attack in retaliation for Sony attempting to identify visitors to PlayStation 3 hacker George Hotz' blog site, as well as seeking data from his Twitter and YouTube accounts as part of a lawsuit. The case was later settled out of court.

Method - Distributed Denial-of-Service (DDoS), Sql injection

Harm - Defacement of various domains of Sony and Personal information of 77 million people, including customer names, addresses, e-mail addresses, birthdays, PlayStation Network and Qriocity passwords, user names, online handles and possibly credit cards were exposed.

PlayStation Hacked

Fox Network's X Factor (5/7/2011)

Attacker - Lulzsec | Harm - X factor contestants personal information exposed and internal Fox data exposed.

PBS.org - Public Broadcasting Service Hacked (5/30/2011)

Attacker - LulzSec in retaliation over Frontline Wikileaks program they considered biased

Method - zero-day exploit in Movable Type 4

Harm - Passwords were leaked and a fake news article was published on the page.

100's of Gmail users (6/1/2011)

Motive - Google says attack originated in China and appeared designed to monitor communications of journalists, political activists and military personnel.

Method - After stealing passwords with a phishing attack, perpetrators apparently used the passwords to change Gmail users' forwarding and delegation settings.

Harm - Attack was "disrupted" but it's unknown if any snooping was accomplished.

Acer Europe Hacked (6/3/2011)

Attacker - Pakistan Cyber Army | Method - Stupidity of Server admin Harm - Source code and user data of 40,000 people reportedly compromised.

FBI partner Infragard Atlanta Hacked (6/3/2011)

Motive - LulzSec, in an attempt to embarrass the FBI and security firm government contractors

Harm - Site was hacked, defaced and 180 Infragard usernames and passwords were leaked.

Citigroup Hacked (6/8/2011):

Motive and Attacker - unknown

Harm - Names, account numbers, and contact information, including e-mail addresses, were accessed during the breach, which affected about 360,000 customers.

Turkish government (6/9/2011)

THE HACKER NEWS Motive - Anonymous, in opposition to Internet filtering plan

Harm - site inaccessible temporarily

U.S. Senate hacked (6/13/2011)

Motive - LulzSec, saying it doesn't like the U.S. government

Harm - published on the Web server's directory and file structure of the Senate site

Spanish National Police (6/13/2011)

Motive - Anonymous, in retaliation for the arrest of three people in Spain Harm - site was inaccessible temporarily

CIA Hacked (6/15/2011)

Attacker - Lulzsec

Harm - site temporarily down

Electronic Arts hack (6/16/2011)

Harm - System hosting BioWare Neverwinter Nights forum is breached and user names, encrypted passwords, e-mail addresses, mailing addresses, names, phone numbers, CD keys and birth dates may have been compromised. Some unencrypted passwords believed stolen.

Sega Hack (6/18/2011)

Harm - some Sega Pass member e-mail addresses, dates of birth, and encrypted passwords compromised.

NATO Hack (6/23/2011)

Motive - After NATO released a report singling out Anonymous' hacktivism as a cyber threat, the group warned NATO not to challenge it.

Harm - subscribers to NATO's e-Bookshop service were urged to change their passwords after a possible compromise of usernames, passwords, addresses and e-mail addresses.

Arizona Department of Public Safety (6/23/2011)

Motive - LulzSec said it is leaking the data to protest "racial profiling anti-immigrant" policies of Arizona law enforcement, specifically SB1070, which makes it a crime to be in Arizona without documentation proving United States residency. Releases another batch of data on June 29.

Harm - publicly released hundreds of private intelligence bulletins, training manuals, personal e-mail correspondence, names, phone numbers, addresses and passwords belonging to Arizona law enforcement.

Former British Prime Minister Tony Blair Hack (6/24/2011)

Motive - TeaMp0isoN says it targeted Blair over his support for the Iraq War Harm - contents of his electronic address book, including contact data for members of Parliament

Arizona Department of Public Safety Hack (6/29/2011)

Attacker - Antisec | Harm - hackers release second dump of data, including more personal data on specific officers

Al-Qaeda Hack (6/29/2011)

Harm - hackers shut down al-Qaeda's Internet communications, halting the flow of videos and statements online

Arizona Fraternal Order of Police, Fraternal Order of Police in Mesa, Tucson Hack (6/30/2011)

Attacker - Antisec | Harm - 8 Web sites defaced, documents released including passwords and e-mail addresses of 1,200 officers, some financial data of specific officers and personal e-mails

Apple Hack (7/4/2011)

Attacker - Antisec | Method - exploited security flaw in the software Apple used

Harm - 26 admin usernames and passwords for an Apple server exposed

Fox News Twitter account Hack (7/4/2011)

Harm - The Fox News Twitter feed was used to publish false reports that President Obama had been killed.

German Federal Police Hack (German Federal Police)

Attacker - n0-N4m3 Cr3w

Harm - The hackers compromised a server used by the country's customs service and posted location coordinates, license plate and telephone numbers, police usernames and passwords, and a GPS application in response to government communications interception.

News Corp. sites, The Sun and News International Hack (7/18/2011)

Attacker - Lulzsec

Harm - Hackers redirected The Sun home page to fake story about death of News Corp. owner Rupert Murdoch, and then later to LulzSec's Twitter feed, as well as redirected a News International's page with a statement on the hack to the LulzSec Twitter feed. They also released phone numbers of News Corp. employees and an e-mail address and password for former Sun editor Rebekah Brooks, who is embroiled in the mobile phone voice mail hacking scandal at News of the World.

Italian Police's National Center for Computer Crime and the Protection of **Critical Infrastructure (7/22/2011)**

Attacker - Antisec

Harm - Hackers claim to have stolen more than 8 GB of internal data that was allegedly seized during police investigations, including information on the Ministry of Transport in Egypt, Ministry of Defense in Australia, Russian companies and U.S. Justice Department. They threatened to publish it online.

72 public and private organizations in 14 countries Hack (8/2/2011)

Motive - McAfee report does not speculate, but there's a pattern in the targets which do not include China but do include political non-profits, a prodemocracy organization, the World Anti-doping Agency, and the International Olympic Committee and Olympic committees in three countries, which were targeted right before and after the 2008 Olympic Games in Beijing.

Method - targeted phishing attacks with e-mail exploit that installed a back door

Harm - National secrets, classified government data, source code, bug databases, email archives, details for new oil and gas field auctions, legal contracts, SCADA configurations and more.

Citigroup Japan hack (8/5/2011)

Method - A source said the scheme was perpetrated by a third-party vendor that had been given access to Citi's internal systems.

Harm - Personal information of 92,408 Citigroup credit card customers in Japan was stolen and sold to third parties, the bank said.

70 U.S. law enforcement agencies and police association in Italy Hacked (8/6/2011)

Attacker - Antisec

Harm - 10GB of personal information, private e-mails, passwords, training files, data from informants, Social Security numbers and stolen credit card information

Government of Syria (8/8/2011)

Attacker - Anonymous

Harm - Home page of the Syrian Ministry of Defense site defaced with Anonymous logo and a call for the downfall of President Bashar al-Assad.

BlackBerry maker Research In Motion (RIM) Defacement (8/9/2011)

Attacker - Team Poison

Harm - RIM's BlackBerry blog was hacked in retaliation for RIM offering to assist London police in combating rioters, many of whom are using BlackBerrys to organize.

Hong Kong stock exchange Hack (8/10/2011)

Harm - Hackers broke into news site of Hong Kong stock exchange, where corporate filings are published, forcing the suspension of trading for seven companies.

"No matter how sophisticated technology is, it always has one big hurdle that cannot outwit us. How we use somethings 'how we behave' will always condition technology, either by how it is designed or how it is used. Nothing is private online. Somethings are more difficult to access than others. Now judge: **Are you Secure**?"

Ghost in the Wires

My Adventures As The World's Most Wanted Hacker

Kevin Mitnick (BOOK REVIEW)

Some call him a saint, some a criminal, others adore him. Industry may loathe him but we here at hacker news say "Get Reading" loyal subscribers and laugh, get mad, feel revenge, and pure educational enjoyment reading Kevin Mitnick's new book "Ghost in the Wires". Yeah, we consider him pretty cool and the father of Social Engineering which is just ours and yours level of interest.

If a guy that can stay one step ahead of big business, catching them with their pants down and their hands in the Cookie jar, then this is the book for you. If you admire a person who can squeeze blood from a turnip, you have the right read waiting for you. Just when you think it can't be done, Mitnick wows you with his technical skill in squeezing past high tech security systems and into the arms of classified information of some of the biggest businesses in the world. Try Motorola, sun Microsystems and pacific bell for starters.

Mitnick is no less than a genius as he knits a story of intrigue and suspense as he navigates through the mazes of high tech companies keeping them jumping and realizing they are not invincible.....not even close.

Perhaps the greatest gift from the book is how human Kevin appears and as readers we ride the train of emotions with him being in solitary confinement to the high of breezing past the most complex of security systems. I think Mitnick even wonders how he does it!

Great book, lots of interesting facts, a good story and you'll walk away amazed and proud that we aren't always controlled by big government or corporations. ACCEPTED TO

Mohít Kumar Founder: THN

Hacks of the Month

- 1.) Welt.de hacked using an SQL Injection and Credit Card info of 30264 users Compromised | Read more http://tinyurl.com/4yd3fsd
- **2.)** Mibbit AJAX IRC client service being hacked. Data including the personal information of 9 Mibbit operators including their names, accounts and e-mail addresses leaked | **Read more** http://tinyurl.com/3tsx6jo
- **3.)** South Korean police claim \$6 million was stolen after 30 hackers from the North infiltrated online game servers in Seoul. **Read more** http://tinyurl.com/3s4q7mj
- **4.)** AntiSec target defense contractors Vanguard Defense Industries (VDI) again. 4,713 emails and thousands of documents taken during the breach. AntiSec targeted VDI's website due to their relationship with several law enforcement agencies from Texas and other parts of the U.S., as well as their relationship with the FBI, the DHS, and U.S. Marshals Service | **Read more** http://tinyurl.com/3fjouoa
- **5.)** A database belonging to the BART Police Officers Association appears to have been hacked by Anonymous Hackers and the names, postal and email addresses of officers posted online. Also San Francisco Bay Area Rapid Transit (BART) hackede and personal details of 102 police officers leaked | **Read more** http://tinyurl.com/3qgtuvm
- **6.)** Epson Korea Co. Ltd. said that hackers had breached the personal data of its 350,000 registered customers last week. **Read more** http://tinyurl.com/3mmp6c3
- **7.)** Anonymous Hackers upload a file on Torrent contain of the snapshot the the Danish Government database of companies. There are approximately 1,000,000 companies in the database & CVR reports of 550,000 companies | **Read more** http://tinyurl.com/3gml7k4

Hacks of the Month

- 8.) Israeli Prime Minister Netanyahu's Website Defaced by Egyptian Hacker. The hacker who managed to penetrate the webpage of Netanyahu wrote "Anti Zionism"; the site was then gradually taken offline. Read more http://tinyurl.com/43q455e
- 9.) Nokia Developer Forum hacked by pr0tect0r AKA mrNRG and Redirect a page of it to his custom page Read more http://tinyurl.com/3ljcs64
- 10.) Recently discovered attempts of an SSL man-in-the-middle attack against Google users - spotted by a number of Iranian Internet users have revealed that Dutch Certificate Authority DigiNotar has issued an SSL certificate for all *.google.com domains.

Read more http://tinyurl.com/3eg667f

11.) The WikiLeaks website, which contains thousands of U.S. embassy cables, has crashed in an apparent cyberattack.

Read more http://tinyurl.com/3mbtvc7

12.) Anonymous Hacker Hack Orange. Fr and upload the database and Site source code backup on file sharing site.

Read more http://tinyurl.com/3prqoxq

13.) Gabia a South Korean domain registrar was hacked on Saturday, affecting the online connection with 100,000 registered domains, according to a report Monday by the Korea Herald. This hack exposing over 100,000 domains and 350,000 users data. THE HACKER NEWS

Read more http://tinyurl.com/3ggja9q

More Hacks and Updates at 'The Hacker News' http://www.thehackernews.com/

TOOLS UPDATE

1) INSECT Pro 2.7 - Penetration testing tool download

http://tinyurl.com/3zgorfs

2) Killapache: DDOS tool http://tinyurl.com/3bfsp7a



3) THC-ipv6 Toolkit – Attacking the IPV6 Protocol

http://tinyurl.com/3lcl8ee

4) BackTrack 5 R1 Released - Penetration Testing Distribution

http://tinyurl.com/3jkh84m

5) SSDownloader: 50 Free Essential Security Tools

http://tinyurl.com/3cmhf26

6) Matriux Krypton security distribution Released

http://tinyurl.com/3tqpqlb

7) The Social-Engineer Toolkit v2.0 Released

http://tinyurl.com/4x7ldjl

8) OllyDbg 2.01 alpha 4 released

http://tinyurl.com/3nfgvgd

9) Window AutoPwn (WINAUTOPWN) - Auto Hacking/shell Gaining Tool

http://tinyurl.com/3jwoe27

10) Metasploit Pro 4.0 released - Enterprise Integration, Cloud Deployment

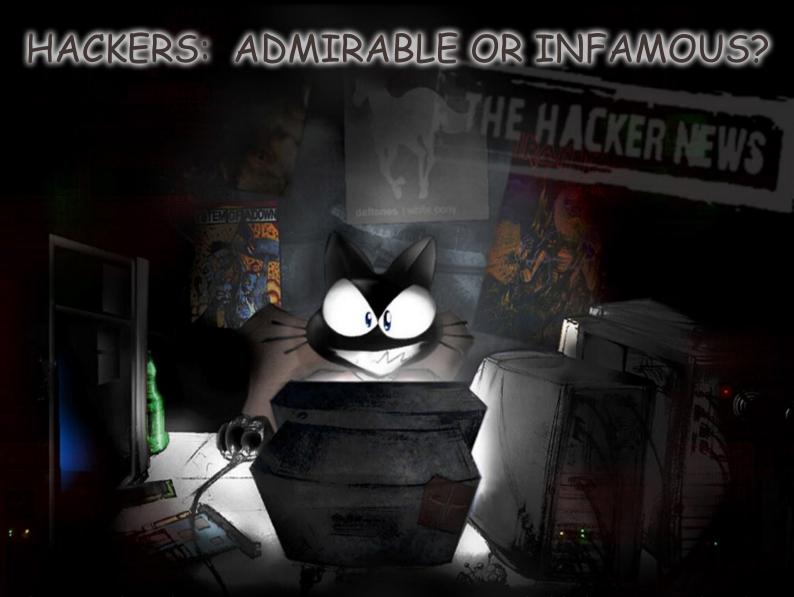
http://tinyurl.com/4xf5nwm

11) Wireshark 1.6.1 and 1.4.8 Released

http://tinyurl.com/3ghejso

12) PuTTY v.0.61 New Version released After 4 years

http://tinyurl.com/3okutzn



If you work in the computer security arena you probably have a good understanding of the different types of hacking that occurs and how you feel about. If not, your views on hacking may be slightly warped by the media who over journalizes the term "Hacking or Hacker" purely to describe the 'bad guys' who steal data and bring computer systems to their knees. After all, if you read it in a newspaper it must be true. The truth is that such a blanket label is wholly unfair to the hundreds of security professionals who 'hack' for altogether different reasons than stealing, breaking into personal information, or trying to gain political persuasion. Not to mention, sell newspapers.

In reality you cannot simply classify hackers as bad guys or good guys. There is a whole lot of grey sitting between those two extremes. Dictionaries all over the world are getting bigger as "Hackers" adopt names, such as, black hats, white hats, script kiddies, crackers, packet monkeys, s'kiddiots, phreaks, hack-tivists and ethical hackers. For most, breaking into a company website in order to see how insecure it is may be the only common thread they share. Once they're in, their actions can often be quite different.



Black hat hackers

A black hat hacker will likely be looking to cause damage to a company's network and/or steal from them. This is the most dangerous type of hacker. They display accomplished technical skill and understand the importance of anonymity. They mostly slip in and out of computer networks unnoticed until such time their work is done.

Admirable or Infamous?

From my perspective there is some admiration and some distain. I think you would be hard pressed to find a black hat hacker that is anywhere close to being on the right side of the law. Still, the best certainly do have an advanced set of skills that one cannot help but admire. In fact, the best of the best are so skilled at what they do you will probably never know their names or where they live. What they do isn't right but they are the elite, no question about it.

Ethical hackers

On the other end of the spectrum you have the ethical hacker. A more apt description would probably be a "computer expert" but it is a name that has stuck nonetheless. An ethical hacker could be considered a good guy because they are not looking to make money or otherwise profit from their work. At least not in the sense you may imagine - they do get paid, it's their job!

An ethical hacker is someone who is employed, typically on a contract basis, to break into a company's computer systems in order to compile a report of where any vulnerabilities may be. Suggestions will then be made as to how the company can overcome these vulnerabilities, thereby making their networks much more secure.

Admirable or Infamous?

Definitely admirable in my opinion but only in the area of doing good work to secure data. Let's face it, when you are hired to secure an unethical corporationand there are many, it is harder to admire the worker. Still, an ethical hacker often has advanced skills that they have picked up through many years of hard work in the educational system. They put these skills to good use in order to protect organizations from those other hackers who don't share the same ethics. Well paid, no doubt, but they work on the right side of the law and make far less money than many of the guys they are defending the computer systems against.





Hacktivists

Another type of hacker which has come to prominence lately is the hacktivist. If you've kept up with recent news then I'm sure you have heard of LulzSec and Anonymous, two groups of like-minded hackers who could be described as 'hackers with a cause'.

Typically, a hacktivist is said to have a political cause though sometimes it can be hard to find what the political point of some of these attacks really is. For example, LulzSec are in it for 'the Lulz', i.e. to have a laugh. Anonymous touts the motto of hacking for exposing criminal and politically black companies and governments.

When a hacktivist breaks into a company's network they are not looking to make money from the breach. And chances are they are not looking to cause direct damage to any of the data they find. Instead, a hacktivist is likely to engage in activities.

by changing a site's home page to something of their choosing, along with a suitable message. Or, perhaps, theft will be the motivation - lately many of the web sites breached by Anonymous and LulzSec have allegedly had emails and other important data stolen in order for the hacktivists to make sensitive or potentially embarrassing information public.

Another favourite of the hacktivists is to make a web site they don't like 'disappear', at least for a while. This is accomplished through the use of a Distributed Denial Of Service (DDOS) attack which floods a site with so much 'traffic' that it falls over under the strain.

Admirable or Infamous?

Hard to say. It's true that computer hacking protest is sometimes necessary as we all know that our leaders don't listen to what we want and press on with their plans for (their own) Utopia regardless! I believe that if hacktivists were to channel their energies into other avenues and pull together in a more cohesive manner, then they may yield far more positive publicity and generate far better results. By attacking high profile sites they gain notoriety and some sympathy for their causes from the impressionable but I doubt they make many friends amongst those who really could benefit their aims

Your views

Each of the 3 types of hacker's I mentioned is involved in exposing the weaknesses in security management across the web, be it a small web site or the web presence of a large multinational company. They work in different ways and have different aims but all expose flaws that need fixing.

Is that something we should appreciate and find admirable? Should we hold each of their different methods and missions on the same level of esteem or split them into the "good guys vs bad guys" categories? The Hacker News wants to know. Bend our ear and send us your thoughts.

About The Author:

Lee Ives is an internet security blogger from London, England. He started his web site a couple of years ago as a means of communicating security topics to the average internet user in a way that they would understand. Contrary to some people's expectations he works in retail and not the security industry which goes to show how just about anyone can accumulate a great deal of knowledge about how to protect themselves online if they are prepared to look for the answers.



Mobile Security and Lack thereof



Mobile technology, particularly smartphones, has come of age and is increasingly replacing PCs for internet surfing, emails, gaming and social networking. As per a recent survey by Neilson Media Research, smartphones now comprise over 38% of the U.S. Cellphone Market and will become the majority by end of the year. To meet this growing demand, cellphone companies are fast churning out new models with killer features, latest and greatest in technology.

With this growth it has also come to attention that security of these devices cannot be left behind. Every day a new data breach is making headlines suggesting hackers have gone into overdrive. However, what is of particular interest is that a bulk of them is being attributed to cellphones. Hacking alone accounted for \$3.2 billion in losses for the telecom industry, says CFCA.

The culprits are many. Several companies like Apple and Google own online application store that allow 3rd party developers to upload programs that can be made available for download by the users. Many users are deceived into downloading applications that appear to be legitimate. The terms are conditions are loosely defined which makes them easy to accept. Once on the device, the "app" can do a variety of damage, and at times without alarming the user. The App Genome Project by the company Lookout showed that in a study of 100,000 apps for iPhones and Android devices, a substantial proportion contained code which could pose a security risk.

In another recent finding, security researchers at Trend Micro discovered a malware on Android devices that disguised itself as a Google+ app. The app was capable of performing malicious activities like recording phone calls and gathering GPS location, and more. This user data was then uploaded on a remote server. The application called itself Google++, which apparently was overlooked by several customers. It's worth mentioning here that a big factor in the working of a malware is the casual behavior of the user, who fails to pay enough attention when installing a program on their device.

In another report, SMS Android Trojan was hidden inside a movie player app and, once installed, would send out premium text messages. Many such malwares and viruses combined have affected up to 250,000 android devices to date.

The rationale behind making smartphone the target by hackers is very simple. A smart phone today not only stores contacts but also other sensitive information like emails, pictures, and more. And in the case of some devices, a history of user visited locations with timelines. The faster and improved cellular networks and Wi-Fi capability have made handheld computing very convenient, making it a widely accepted product. Hence, it has attracted the attention of hackers with malicious intent. This increased visibility has, however, put pressure on software companies as well as hardware manufacturers to provide security features and configuration options. Facebook now offers its users secure logging via SSL on their wireless devices by activating an account setting. Twitter followed suit by enabling "always-on SSL" and thereby keeping user data secure even when connected through a public Wi-Fi.

The users too need to be vigilant of their devices. In case of a lost device, remote erasure of data or locking of the device is recommended. An alternative is to trigger the remote kill switch which will render the phone dead. If the device contains sensitive information, it is recommended to store digital assets in encrypted folders. Other simple tricks include keeping the Bluetooth off and in non-promiscuous mode at all times, unless when in-use. Contacts, photos and videos should be periodically backed-up in a safe location, preferably encrypted. Several anti-virus software compatible with various OS platforms are available for download from online application markets to help make sure that mobile devices are as secure as possible.

About Author

Nidhi Rastogi is a Security Consultant with Logic Technology Inc., a New York based company since April, 2010 providing consulting service to GE Global Research Center and Energy. She has earlier worked in a similar role at Verizon Wireless and has a Master Degree in Computer Science from University of Cincinnati with focus on Wireless Security. She can be contacted through email at nidhi.gupta@gmail.com.

VULNERABILITY

-- Just Ahead --

- 1) 10 year old Girl hacker "pseudonym CyFi" revealed her zero-day exploit in games on iOS and Android devices that independent researchers have confirmed as a new class of vulnerability at at DefCon 19.She is cofounder of DEFCON Kids. Read More http://tinyurl.com/3csmlxv
- 2) A security penetration tester at Italian security firm AIR Sicurezza Informatica has claimed that flaws exist in Google's servers that will allow would-be hackers to exploit the search giant's bandwidth and launch a distributed denial-of-service (DDoS) attack on a server of their choosing.

Read more http://tinyurl.com/3nmof57

- 3) \$30 Child Toy is enough to hack FBI Radios. The portable radios used by many federal law enforcement agents have major security flaws that allowed researchers to intercept hundreds of hours of sensitive traffic sent without encryption over the past two years. Read more http://tinyurl.com/3nggby7
- 4) There are remotely and easily exploitable vulnerabilities in the BlackBerry Enterprise Server that could allow an attacker to gain access to the server by simply sending a malicious image file to a user's BlackBerry device.

Read More http://tinyurl.com/42xrog4

5) A new Android Trojan is capable of recording phone conversations, according to a CA security researcher. The trojan is triggered when the Android device places or receives a phone call. It saves the audio file and related information to the phone's microSD card, and includes a configuration file with information on a remote server and settings used by the trojan. THE HACKER NEWS

Read more http://tinyurl.com/3j44hx6

6) Hackers are exploiting a zero-day vulnerability affecting TimThumb, a free image resizing utility widely used on the blogging platform WordPress.

Read more http://tinyurl.com/3kmxbaj

DIGITAL AGE BRINGS SECURITY RISKS

Gone are the days when you had your personal files stored in a physical library and your only risk was that someone might steal them. Life now a days is all about digital. Your "life" is on the web and at any moment your digital life could be stolen. There are many risks that we the users need to be aware of and prepared for. Today, digital information is very much a security risk for the common person not just big corporations.

Not only do you have your files stored in the cloud, but also your reputation. With services like Twitter and Facebook you are dependent on these websites to keep your information safe and free from undesired access. Most don't realize that it isn't just the web owner's job to keep you secure but you must take precautions also.

First is personal security. Software updates and antivirus programs are the most common thing that users never apply and for that reason we are often attacked and have our security breached because we failed to apply a patch

that could have solved the problem or prevented a computer virus. PC users need to be more responsible about this because our hardware is our responsibility and the damage that has been made from this type of breach has been a big one. With bot networks that count millions of infected computers, we are responsible for a lot of security issues in the last few years.

The second point of security is the access from outsiders or hackers as we call them today. People who hack have proven that they are a security risk and that their wave of attacks will increase over time.



The bigger the company, the more likely it will be a target. Anonymous and LulzSec have been wreaking havoc among different sites and agencies that prove we are not yet ready for a full attack on our personal and smaller business sites. These groups defend their hacking as a kind of "ethical" procedure and claim that they only attack sites that restrict privacy or which affects the freedom of the internet, however, there are other groups like the one that attacked the PSN network a few months ago, that have proven that they will attack and will do it just for the monetary gain and nothing else. We also have something that many have considered but none has proof, that there are government sponsored hacker teams. That they work to create anarchy in government sites, and to infiltrate and steal valuable information from these governments. I think that there is more to this theory than meets the eye, and we will see more about this type of attack in the future. A solution to this? Better preparation for the IT manager, faithfully applies software updates, and tries to be one step ahead of the hacker.

The third point of security is our privacy with "official" sites. Facebook and Google have proven that they have very clear issues regarding sharing our information with the police or the government. During the recent riots, UK RIM offered their help to localize those responsible for the organization, and this put us all at a big disadvantage. We have trusted these sites. We voluntarily gave them our information, and they will share it with anyone if "they think it is right." We have been really naïve about this and we need to address this with these types of sites because they have our lives and personal information and apparently will violate our privacy whenever they want. We must pressure them to respect us and our personal information. We as users need to know where our personal data is being stored and secured, and what can they do with it. No matter what, we need to be informed and maybe be more responsible about what we share.

As I first mentioned, our life has become a digital life, and the security of it is the most important thing nowadays. PC users need to be more responsible, listen to what IT managers have been saying all the time, "don't open unknown mails with attachments", "update your software", "don't trust anyone", "be careful with who you share private information." Unfortunately, it seems we have failed in every aspect and we need to change that. Remember, knowledge is power, and we need to know how to protect our data.



"Now is the Time to evolve or Die"

Anonymous was formed and birthed on the internet message board 4chan in 2003. The moniker Anonymous was derived as homage to 4chan. At the time, if someone posted to 4chan's forums and no name was given then the post was credited to "Anonymous". Seizing onto the premise or the idea that actions can be taken anonymously by the lesser or powerless "Anonymous" moved beyond 4Chan and morphed into sometime larger and more potent. The original premise of "Anonymous" appeared to be a limited but noble idea; attempting to keep the internet open and free because governments and corporations were earnestly trying and demanding limits and restrictions to the freedom of expression on the internet.

To date "Anonymous" has remained a banner that many channers, as well as hacktivists and IRC users, post under and are loosely grouped together. Allied under the umbrella of "Anonymous" with no real command structure in the group, "Anonymous" remains an ever fluctuating mass of unknown identities that have often fancied themselves as cyber-avengers unfocused and more often than not unable to remain of the same consciousness even on an hourly basis.

History must be remembered and never forgotten, for the factual words of Italian fascist Benito Mussolini was stated correctly; "Fascism is Corporatism".

As the gap in wages world wide become increasingly more disparaging a significantly increasing numbers of world citizens are being harmed and maltreated by the unquenchable greed and corruption of the evolving corporate state. As the wealth of the world has rapidly been consolidated into the hands of a small minority, governments are being bought and paid for and rapidly, one by one, turned over lock stock and barrel to faceless Corporations. These greed drive soulless concerns have not hesitated to use their power as an instrument of war as a means of increasing their power and profits. Sadly, as expected along with this ever grown trend it has become a fact that human rights violations are becoming even more extreme and cruel.

THE HACKER NEWS

Since it is evident that the monstrous Corporations committing these unspeakable crimes are almost never held accountable, it is time that the young and the computer literate around the world educate themselves and become consciously aware which greedy Corporations are committing the horrendous crimes that effects the very survival of this planet and every living being on it. Because information is power, inform yourselves. Now is the time to educate yourselves and make your lists of these offenders!

By becoming more educated and informed on the global threat posed by corporations, is it possible that this idea, this premise of "Anonymous" could be channeled into the kind of tool needed to awaken global consciousness to the treachery of the global power structure. Could the true center of "Anonymous" that idea that "Anonymous" wishes to represent the truth to the world morph once more beyond its present form and limitations or will the nebulous vision behind the premise of "Anonymous" remain content to use their collective abilities for either good or bad simply content on a myopic and undisciplined path, depending on the inclination of the mob?

It is time to get off that fluffy cloud of illusion, get educated and get informed beyond such a small focus. Investigate the bigger picture, know your own power; inform others of the immediate threat of corporations and the growing take over of world governments, the biggest and baddest being taken over by fascism today is the United States of America. Internet freedom is the least of your worries now. Call it what you will, this is what Benito Mussolini correctly labeled Fascism my brothers. If you don't like it, you can oppose it. But if you ignore it and deny it; then you will remain a sitting target. "Now is the time to evolve or die"

Know your enemy. Go to corporatewatch.org



SECURITY IS MORE THAN A THREAT

The events of the recent months have hopefully shown all of us one thing, and that is anyone can get popped at any time. Anonymous, LulzSec and others have brought attention to what most security guys have been saying for a very long time. Security is a myth, plain and simple.

Security vendors such as McAfee are using fear, uncertainty and Doubt (FUD) i.e.. "The Shady Rat" to market their wares. Industries are coming to grasps with the fact that all the money they had spent on security barely reduced their risk posture. The incompetence of so called security professionals is also coming to light in what I dare to call business as usual in the security community and the rest of the world.

I remember the 90s when websites getting popped on a daily basis was the norm. The morning routine for people in the security business consisted of; Coffee, Smoke and a quick perusal of attrition.org to see who got egg on their face. The industry was still fairly small at the time, and more than likely you knew who to call and mock. You would think that with several years of security under our belts that the routine would have changed. Well, you'd be wrong.

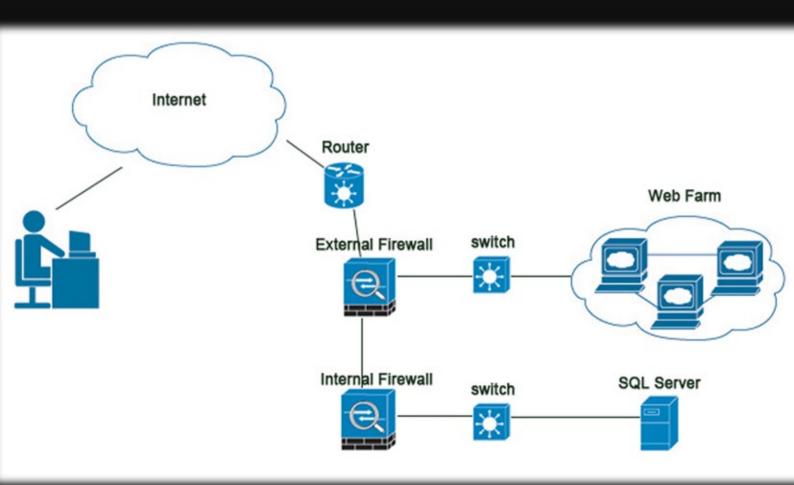
Things have changed somewhat.. These days the content filters we were tasked with implementing back then are blocking our access to Attrition. The industry has also changed and I'm sorry to say for the worse.



The security community has become convoluted with industry experts that have no industry expertise. To break in to the corporate security world, you must obtain certifications that say you're an expert. The problem is that a certificate does give you the experience or the know how to minimize the lulz. I'd like to point out that I don't think any of the recent attacks are complex in the least; but if companies such as Sony, Booze Allen and others are being popped, we have a serious problem.

Common practice in most organizations is spending a ton of money on appliances and miracle solutions without looking at any of the underlying issues. The problem is that a magic device does not exist, regardless of how many inept security professionals would like it to. So you have a firewall and you think you are protected, well let's take a look at why that isn't the case.

The Diagram below is a typical scenario. Web servers are behind an external firewall, SQL Server is on a server segment off a different set of firewalls and everything should be secure right? WRONG....



To allow access to your web servers you allow TCP/80 & TCP/443 through the firewall. Yes, most firewalls are smart these days and can do advanced layer 7 filtering, but how many of you actually implement the technology? I'm going to go out on a limb and say no one, or very few. So the firewall that you just dumped a ton of cash on is nothing more than a layer 4 router. Do you see where I am going with this? SQL works because of the way the applications are configured. Firewalls are set up to allow the web server access to them. This is the configuration, and a SQL call is a valid request. Obviously I omitted Intrusion Detection/prevention, Reverse Proxy, WaF technology and the list goes on and on... The bottom line is none of these technologies will stop a dedicated attacker. They may slow them down but they won't stop them completely. I've heard the argument from clients in the past that they don't have an internet presence and as such, are secure. The only thing that changes is the attack surface has become significantly reduced, but not eliminated. Every business essentially has the same attack vectors which include employees, clients and 3rd parties. A dedicated attacker can use any of these threat vectors to achieve their goals, up to and including walking right through the front door. Physical security in an organization that doesn't have an internet presence is usually the easiest to breach. The final tidbit I'd like to throw in to the mix is the recent explosion of bot-forhire providers. While everyone is susceptible to denial of service, these providers are bringing to light an interesting scenario. The industry has responded to denial of service, with load balancers, proxies, routing protocols and more. The answer is you can't, you have absolutely zero recourse. Denial of service is an interesting animal because the motives behind it are far and wide, ranging from competitive sabotage to activism. What can you possibly do if you have 40K+ bots attacking your DNS Servers? Your company has now disappeared off the internet. To close, nobody is ever truly secure. Our job as security professionals is two fold. The first part is minimizing the impact by implementing controls that make the attacks more difficult to achieve, and implement the capabilities to identify and respond to any ongoing attack. I am not a fan of the way the term APT is being tossed around by the media and the industry as a whole. Every organization has threats that must be considered as part of their threat model. Lulzsec, Anonymous and the likes should be considered as part of your Threat Model regardless of what industry you are in.

Submitted By: Boris Sverdlik

Senior Partner, Jaded Security Consulting

http://www.jadedsecurity.com | Email : boris.sverdlik@jadedsecurity.com

FEEDBACK

It was interesting to have a whole magazine about what we report on. Of course, I mean "hacking" and the consequences of it.

We here at **The Hacker News Security Services** hope you enjoyed this edition of our magazine and hope to have you as a regular reader of our daily web news.

Hacking is here to stay and so are we. We want the most informed readers possible that is why we care what you think.

We'd like to hear from you and let us know what you'd like to add to the magazine or what topics are of most interest to you.

In the meantime, Thank you for being a loyal reader and thank you for the opportunity to report on the hacker news of day.

We will see you daily and then in our next magazine coming in October 2011.

Most sincerely,

Mohit kumar Founder/chief editor The Hacker News Security Services

CONTACT AND JOIN US

Email: thehackernews@gmail.com

Twitter: https://twitter.com/TheHackersNews

Facebook: http://www.facebook.com/thehackernews

Website : http://www.thehackernews.com/