



The Hacker News

Who we are ?

Who we are @ The Hacker News?



Barbara Tutino from William Cullen Bryant High School, USA wrote to us and expressed their interest in our online publication of “**The Hacker News**” and the type of information we are promoting. She asked few questions and my answers are my own humble opinion. I would never, never presume to speak for any group or movement and my publication acts only as a simple disseminator of information. I would like to share this small FAQ related to ‘**The Hacker News**’ with our readers. I hope this helps you understand **WHO WE ARE AT THE HACKER NEWS!!**

The way I view the world is through the lens of a young Indian male but I do strongly believe in the statement of the United Nations ~ “***Human rights are rights inherent to all human beings, whatever our nationality, place of residence, sex, national or ethnic origin, color, religion, language, or any other status. We are all equally entitled to our human rights without discrimination. These rights are all interrelated, interdependent and indivisible***

Q. What exactly is Your Mission?

The mission of The Hacker News was first and foremost to achieve our ultimate goal of launching an on line magazine addressing the tricky and complicated world of hackers and hacking. In our first year in business we concentrated on issues that do not receive much mainstream media attention, such as the dissemination of assorted information and current events about topics that mattered to hackers and hacktivists worldwide. Our team at The Hacker News understands the importance of reporting on hacking groups that focus on the ethically wrongs in society such as unregulated corporate power, secretive government, and invasion of privacy.

Q. How Do You Define True Social Justice?

When a person is ask to define social justice many different definitions will emerge. It must be understood that individual definitions will be based on a large variety of reason like political orientation, ethnicity, religious background, and political and social philosophy. My own personal definition of true social justice is based on the simple definition stated by Dr. Martin Luther King' "The complete liberation of mankind and the elimination of injustices". I can only hope and wish that all social justice movements world-wide regardless of their methods are pushing forward and moving towards societies based on the concepts of basic human rights and equality for all of its citizens.

Q. How Are You Using the Internet for Responsible and Meaningful Social Change?

Our on line publication The Hacker News acts in the capacity of a disseminator of information, and as an advocate that helps initiate and support new ideas and attitudes that we believe can help produce positive social change. The Hacker News hopes to be a publication to help people accomplish goals and social changes that are beyond the capacity of the single individual. We understand how the Internet can and is being used in a strategic and deliberate manner by social change activists to help direct and inform a generation to understand their rights and duties, so that they can and will always stand up and fight for their rights. We hope The Hacker News, our on line publication, can be a catalyst for meaningful social change worldwide.

Q. Do you really adopt the true essence of "civil disobedience"?

I can only speak from my own personal view point and that is I endorse the teachings of Mahatma Gandhi, and utilized by Dr King in his civil rights movement. Gandhi employed non-cooperation, non-violence and peaceful resistance as his armaments in the struggle for independence from the British Empire. I believe civil rights of each individual are universal; each man woman and child on this planet has the right to seek redress against injustice. The effective means by which their redress will manifest can and will vary accordingly by culture, political tradition and concentration of power.

Q. Can You Explain the Use of Hacking as a Device for Democratic Change?

As worldwide discontentment expands exponentially the fight against corrupt political and financial establishments by the people of the world is reaching a tipping point. The people are beginning to fight back by organizing and using all means necessary to expose the corruption of governments, corrupt politicians and their corporate masters. It is evident that hacktivists worldwide are playing a large part in this important fight. Recently, Lulz Security (Lulzsec) and the Anonymous hackers have declared open cyber warfare against corrupted governments, tainted banks, and dishonest major corporations, and are calling on all hackers across the globe to join with them in their fight. Is it possible that cracking open this sinister crypt of dark secrets and bringing all the deception and greed to light can significantly help further the goal of implementing real democratic change worldwide? I believe so, and unless we try we will never know if exposing hidden information can help in the fight to bring about economic justice and true freedom. I believe it is conceivable that the hacktivists movement could really help change the world for the better. Perhaps this is just the beginning of a quiet and very angry revolution that will make the world a better place.

Q. Do you feel that invading people's privacy in the name of so-called justice is a "means to an end"?

The situation you are inquiring about is neither merely a black or white issue. Today, many young people do not think about ownership and privacy the same way their parents did. The digital revolution and the

mainstreaming of hacker culture have resulted in a world where boundaries of ownership and privacy are rapidly changing. A new way of viewing intellectual property can be closely tied to “The Hacker Ethic”. Such as, stealing from a large institution like a corrupted corporation or corrupted government is okay. Stealing from an individual or small nonprofit is not okay. “The Hacker Ethic” does not embrace theft; instead it simply defines certain things, such as information as not being personal property, or certain actions such as using phone service as ‘borrowing’ rather than theft. The hacker community tends to view hacking as a creative effort to overcome problems. There are always ethical considerations as the belief that “even the most evil has a right to their private lives”. But then there is the ethical consideration of reporting and exposing the truth. Therefore you have the dilemma of personal privacy versus corporate/governmental duplicity and public/humanitarian interest. With that said, exposing emails and private information from normal people or tacking anyone that’s neutral in the battle to obtain worldwide social justice will not help towards a righteous cause for increased social change and justice.

Q. Is it true that "anarchy" is part of the philosophy or is simply promoting the freedom of information act to the maximum?

For many, the recently formed political hacking movements bring to mind one thing: Anarchy. But for most people who know nothing about a political tradition called anarchism, they tend to use the term anarchy in the convoluted frame of; “anything goes, total chaos, and the absence of rules”. This erroneous definition could not be further from the truth. With regard to hacktivists and hacker groups like anonymous it is worth pointing out that their loosely connected members come from diverse political backgrounds and traditions. An example: When individuals participate in any clearly anarchist organizations, they tend do so as an anarchist. On the contrary: When individuals participate in a hacker group, like Anonymous, they tend not to do so overtly as an anarchist, social democrat, or libertarian but as Anonymous. Nevertheless, in the hacktivists most recent manifestation they have embraced a more left leaning consciousness, and an anti-neoliberal or anti-corporate worldview. They favor democratic socialism, peaceful anarchy, alternative visions of green capitalism, and modern approaches to direct democratic action, and a firm commitment to consensus and have a strong belief that information is the life blood of any society and the desire to expose those who wish to stifle the free exchange of information. Mainstream media’s discomfort with the nebulous, unformatted, far ranging, and human centric ethos does not diminish its truth. **“The times today are a changing!”**



From the In-Security Land to Security in the Cloud



This article aims to share with you some thoughts and concepts associated with Cloud Computing and the risks involved for those who want to venture into the benefits it offers.

"From the In-Security Land to Security in the Cloud" we will reflect on how true it is that the cloud is dangerous or more dangerous than "land" and in turn how much of what is required of the cloud is rarely seen implemented on the ground.

When companies begin their assessment to go to the cloud, the first comments are generally related to the "dangers" associated with privacy and confidentiality of information, the availability of services and other issues that represent the cloud as an undesirable place to visit. This turns out to be real, but as real as could be the situation of exposure of the information in an organization that does not have security program information or at least care with basic information and associated assets.

Now, what is minimally expected from someone who cares about the privacy or confidentiality of information in the cloud is at least that the situation of your organization is better and there have been implemented controls to ensure these principles. Similarly, those aspects associated with the availability of services and issues related to continuity of operations and / or the receipt of information.

What really stands out is that the situation is closer to what they expect from the cloud, and which according to its critical position towards the latter should have on earth. Thus, there are no basic measures such as: an inventory of critical assets of the Organization, the classification of information, risk analysis, continuity of operations plans, product safety checks and risk analysis and surprisingly, the receipt of information. That is, being critical of the cloud does not have a basic security strategy for your organization, but what they expect from the cloud.

However, as has happened with other issues, you can see a global trend migrating to solutions in the cloud, some start with those applications or systems that have little relevance to the operations of the Organization, but hopefully that will quickly migrate to more relevant services to reach the critical systems and applications.

What we should keep in mind is that, both on the ground and in the cloud, security must be managed, with a clear objective of accompanying the business through the changes that occur in the operation. There is no model that does not require management, risk assessment, implementation of controls, monitoring and accountability on the part of those involved. Having said this, you might think that the real danger is people, in short it is the lack of diligence regarding risk to which information is displayed, no matter where they are. Do you still think that the management of safety and risk is a purely technological issue? Do we think that in any case the security problems of an organization are the responsibility of the IT area? Cases like Sony, Amazon, Google, DigiNotar, BlackBerry and other serious incidents make clear that security is a fundamental part of any service delivery today. However it doesn't seem that corporations will be willing to assume the cost that this will generate. Diginatar has been in bankruptcy due to this.

Finally, for those interested in evaluating a solution in the cloud there are many resources available that can make the task much less complex and also with international endorsement, that may require areas to be making decisions. In this sense, you can find material in ENISA, INTECO, NIST, CSA, etc.

The Cloud Security Alliance (CSA) has developed a number of additional documents to the traditional guides that can greatly facilitate the evaluation and subsequent analysis of a solution provider, among which we could find:

- Cloud Control Matrix (CCM).
- Cloud Assessment Initiative (CAI).
- Cloud Security Guidance (CSG).
- Security As a Service (SecaaS).
-

About the Author :

Mariano del Río | Information Security Consultant

Twitter: @mmdelrio



THE OGRE MOUNTAIN VIEW

By Laurent Chapier

Known for its search engine, Google, founded September 4, 1998 in Silicon Valley, California, by Larry Page and Sergey Brin, is a company whose evolution is constant. "The Ogre of Mountain View" made its name primarily from the monopoly of its search engine but also from some of its software such as Google Earth (allowing visualization of the Earth), its email service Gmail or more Recently the application of social networking Google +. Discover, now, behind the scenes of Google, whose mission is simply "to organize information around the world and make it universally accessible and useful."

In 1996, two students at Stanford University created a search engine BackRub, to assess the importance of each web page with an assessment of the links. Two years later, Google was born, and the PageRank (trademark) or PR (analysis algorithm links competing in ranking system of web pages in the search engine), invented by Larry Page. Therefore, the company has continued to grow to better adapt to market requirements and its users. Then in its infancy, it offered results in one language, today, dozens of products and services, including a range of advertising solutions and a variety of Web applications, are available in a multitude of languages. The company, which began with two students in computer science with their room in one office university now has several thousand employees and offices (the Googleplex) around the world and can also boast of being the second international company in terms of valuation with 111.5 billion dollars (ranked BrandZ 2011). As a success story, Google has become the brand in a decade: a way of living, thinking and working.

Google's attitude is born!

Today, the Ogre, with a flawless appetite moves on its path and crushes many of its competitors. With a simple search through the sale of advertising space, the company founded by Brin & Page is always at the forefront of R & D (Research and Development). And when an entity is applied and involved, the results are waiting for you. With its "Green Initiatives" Google is thus based on its environmental impact in order to combine future economy and ecology. No doubt this kind of initiative aims to create substantial savings.

With its "server farms" whose energy consumption is equivalent to several nuclear power plants, it is clear and crucial for society to know that this issue is a priority and has quasi-financial ambitions. In a world where ecology is a predominant concept, Google invested in 2009 a Data-Center located in Hamina in Finland to reduce its environmental footprint.

But all facets of the company are unlikely to smile.

The latest example: the payment of a fine of \$ 500 million to U.S. authorities for the promotion of illegal drugs 24 August 2011.

Even at Google, sin remains!

The Undead Corporations

By Patti Galle (Editor, THN)



Corporations are soulless entities possessing privileges and the rights of citizenship that actual people have; all the while not having to shoulder any of the natural responsibilities. Undead Corporations have concentrated the essence of avarice, rage and fury to form their corporate structure. And as these covetous Corporations have accumulated immeasurable wealth they have methodically utilized this wealth and power to procure, infiltrate, and seize control of the influential and powerful American government and many governments across the world vigorously fusing them into a globe-encompassing non-living aberration, now rightfully called or labeled as Corporatocracy.

At present, on an ever escalating level, world governments are virtually serving only the interest of the wealthy and corporate profits at the cost of workers, communities, consumers, and the environment. Worldwide inequality continues to rapidly increase between the rich and the poor. At this juncture in time the extremely wealthy elite, intermingled with giant corporations are making obscene profits, purchasing the majority of politicians and directing our leaders and elections. The market, technology, and increased militarism have reduced human beings to mere mechanical commodities whose only usefulness and value lies in selling labor and consuming products. Our natural resources, institutions, and the general population must be used up and then discarded when they are no longer useful because profits must always be maximized.

Corporations must always be on the outlook for more markets to lay claim to, and the military Corporations like Lockheed Martin and Boeing must always find more countries to invade. The wars in Iraq and Afghanistan are the insidious handiwork of these Undead Corporations that have seized control of America and its institutions. America was once a Democratic Republic, but many Americans are waking from their slumber to find that America is no longer a Democratic Republic but has become a "Corporatocracy," one in which they are now governed and ruled by an alliance of gigantic Corporations, the extremely wealthy elite and Corporate-assisted (bought and paid for) government officials. And these Corporations march unabated like the Undead across the globe devouring anything and everything in their sight.

Nonetheless, the truth of such terrifying oppression and tyranny is not enough to force the majority of us from our comfortable couches to take action. Some contend that this political passivity is caused by ignorance due to corporate media propaganda from powerful media networks like Fox News, and extremist right-wing talking heads like Glen Beck and Rush Limbaugh who consistently brainwash the lower classes into fighting against their own interests while others believe the passivity to organize is directly connected to a lack of money. But perhaps the frightening truth is actually because too many of us have become politically pacified by Corporatocracy-created institutions and culture exactly like the soulless Undead Corporations planned and wanted.

The time has come for us to ask the question of how we regain our backbone, our courage and solidarity and shake off the shackles of the Corporatocracy. We can no longer sit by and idly watch as greedy Corporations continue to consolidate around the globe getting their rapacious undead tentacles into the people and the natural resources of every place in the world they lay claim. The world has been desperately in need of a movement, a global game-changer that involves a very broad mass of the marginalized, poor, and unemployed and especially the world's youth that are so dramatically affected by rapacious Corporate economic injustice. A movement has been desperately needed that consists of people who resent the corruption and the social status quo and understand that there is a link between Corporatocracy, militarism and corruption.

The great American political activist Howard Zinn said "If there is going to be change, real change," "it will have to work its way from the bottom up, from the people themselves. That's how change happens." Professor Zinn explicitly understood how imperative it is for students and peoples throughout the world have a detailed understanding of history. Zinn stated "To me, understanding history is a matter of life and death," "If you don't understand history, you're a victim." What Zinn meant was that if citizens didn't understand their own history of exploitation at the hands of the robber barons and industrialists, who fought for deregulation at the expense of their employees in order to accumulate larger profits, then they would be doomed to repeat those tragedies. Fortunately it would appear that enough world citizens are learning their true history

lessons from their many brothers and sisters who are now actively engaged in the social justice struggle world-wide.

I believe if the great Howard Zinn were alive today he would be tremendously pleased to be witness to the bottom up, citizen driven out-break of demonstrations and occupations in America and around the globe that's demanding political change. Tens-of-thousands of people, young and old, around the world are getting off their couches to flood out into the streets and force the world's leaders listen to their cries against poverty and injustice. These brave citizens are helping organize a movement that breaks down barriers to create a just and fair economy in all societies. We at The Hacker News stand in solidarity with those all around the world that are in the streets, in the parks, in the roads and in the cyber world that are helping place a stake in the heart of the Undead Corporations.

Dissent is the Highest Form of Patriotism
- Howard Zinn

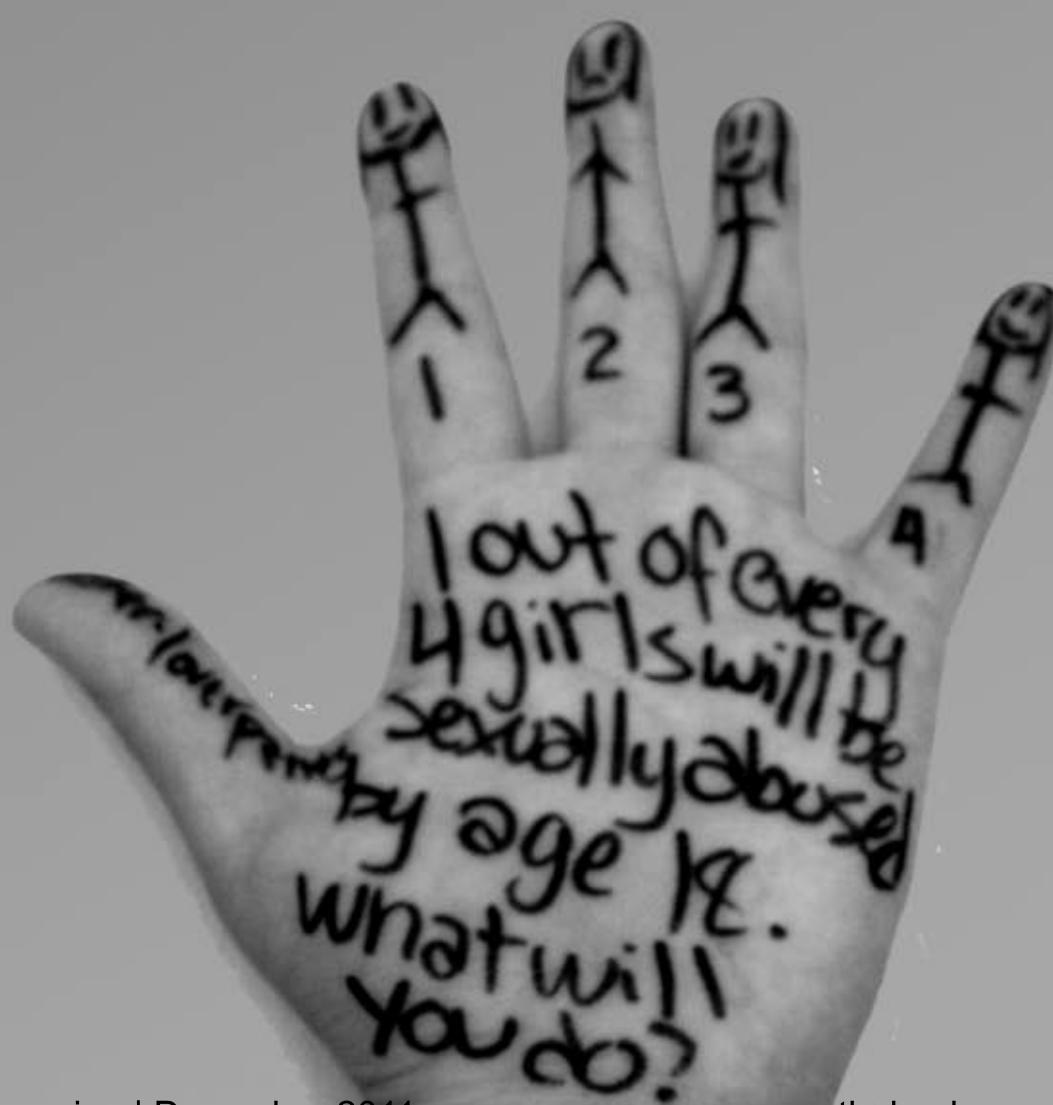
The Naked Truth of Child Pornography

Now days the internet has become the fountain of knowledge and fun for most of us, but cyber criminals are also there to remind us that this is not the safest playground, especially for children.

Recent research has shown that very few parents know how exactly to protect their children from sexual predators and their attempts to exploit children in any way they can.

A few of these criminals primarily collect and trade child-pornographic images, while others aim at having personal encounters with children.

Year by year, children get to know the internet in more and more younger ages, and every year statistics show that Internet-related crimes against children are on the rise. But let's not forget that there are some forces fighting sexual predators, like Anonymous who recently attacked websites with child pornography material.



In this article you will be able to see the naked truth of the latest research about online children exploitation and abuse:

- 22% of teenage girls say they have already posted naked or semi-naked photos or videos of themselves online.
- The biggest volume of porn websites are of children between the ages of 12-17.
- 86% of girls claimed to be able to conduct online chats unaware by their parents, 57% have access to their parents' e-mails, and 54% are able to conduct online relationships.
- 20% of teenage internet users have been the target of an unwanted sexual solicitation (requests for sexual activities, chat, or information).
- 20% of all internet pornography involves children, with more than 20,000 new posted in a weekly basis.
- 69% of teens regularly receive requests for chat or other types of online communication from strangers, without informing their parents.
- 725,000 children approximately, have been continuously asked for sex, defined as an offer to meet in person.
- 1 in 5 youth ages 10 to 17 received a sexual solicitation or were approached online.
- A surprising 1/4 of households only protect their children with the appropriate software.
- An estimated 116,000 child pornography requests are made every day online.

In order to properly protect children from internet sexual predators and avoid such phenomena, all parents should have their eyes wide open for any suspicious online moves.

The most important thing for the parents is to win their children's trust and make clear that internet on the first hand is a beautiful beach in which we are able to surf and have fun, but on the other hand internet is a beach full of sharks ready to rip them off.

Article Shared By : Guys at "<http://www.secnews.gr/>"

It Wasn't Me, It Was Bennett Arron

So, Identity Theft. What is it really? Well, I'm glad you asked. It's basically when your personal details are used fraudulently to open accounts or obtain documentation in your name. This could result in debts being accumulated, for which you would initially be accountable – until you prove yourself innocent.



ID theft is quite commonplace now, but when it happened to me several years ago, no one really knew much about the crime. I had to convince the Police, as well as all the companies to which I allegedly owed money, that I was me, and not the person pretending to be me.

Someone had used my name to ring up thousands of pounds worth of bad debts. This gave me a bad credit-rating which meant I couldn't get a mortgage, couldn't get a credit card and couldn't open a bank account. I couldn't even join my local gym as they wouldn't accept my direct debit – so it wasn't all bad news. As a result of this crime I eventually became homeless and penniless and had to move in with my parents.

A few years after this happened, as some kind of cathartic exercise, I wrote a comedy show about the experience. As a result of this I was asked to be the guest speaker at a number of Fraud Conventions and I was also asked to make a television documentary on the subject.

In the documentary I proved how easy a crime ID theft is to carry out by firstly going through someone's rubbish at 1 o'clock in the morning (they had thrown away bank statements and other personal information with which I opened accounts in their name) and then setting up a stall in a Shopping Centre and telling people that I could stop them from having their identity stolen if they gave me their personal details. Which they did (it's online, have a look). The other thing I did in the programme was to steal the identity of the British Home Secretary – for which I was subsequently arrested....

Still at least I proved my point, which is that ID theft is a very, very easy crime to carry out.

When I looked into my own identity theft, I discovered that the thief (I think the term Fraudster sounds too exotic) had been running up debts in my name for the previous year and a half. He hadn't accessed my accounts, nor had he cloned my cards. He had simply used my personal information to set up new accounts.

So what can we do to prevent this from happening?

At a recent corporate event I was asked what people could do to stop them from having their identities stolen. I replied "nothing." Needless to say, that didn't go down too well. Of course there are preventative measures; shredding documents, not giving out information unless you are positive of the source, keeping your PIN safe, having regular credit reports etc. And in the vast majority of cases these will suffice. Yet, as I have proven several times, if I really wanted to steal someone's identity I probably could. However, as I have already been arrested for it once, I am now looking into alternative hobbies.

Of course, with the advent of social websites like Facebook, these crooks now have a new way of gaining personal information because as well as letting their families and friends know what they're up to or what mood they're in, people who use these sites have a tendency to add their address, date of birth and information as to when they are going away on holiday!

But it's not only down to the individual. Banks, shops, mobile phone companies etc should be more stringent in their screening processes. It's too easy just to take on new clients and deal with any consequences of fraud later.

Having your identity stolen is not a victimless crime. It's far from it. And having a bad credit rating can cause endless problems.

But don't take my word for it, ask Bennett Arron....

About The Author :

Bennett Arron is an award-winning writer and stand-up comedian as well as a speaker on the subject of Identity Theft.

For more information visit: www.bennettaron.com

Follow Bennett on Twitter: @bennettaron



SOCIAL NETWORK POISONING



"Be Social" is the imperative of the last years. We live alternative lives, weave dense networks of relationships; we feel the irrepressible urge to be part of a group, to fill the void that we carry within. But this human propensity to aggregation is now the foundation of the concept of "social network", a community of people, each of them defined "node" by researches, which are united by friendship, kinship, passions, interests, religious beliefs. The whole world is represented by a lattice structure that scientists have long taken to study, to achieve the classification of that human "node", classify its customs, and especially to predict the behavior and through it influence the response of the community a particular event. The philosophy is that of the control.

In May I defined the term "Social Network Poisoning" writing before to Wikipedia EN and also to Italian Wiki.

The term social network refers to the poisoning effect produced by the application of methods designed to make unreliable the knowledge related to a profile and its relationships. The application of this kind of attack on large-scale could lead to the collapse of Social Networking platforms affect its value for commercial purposes, as well as the utility in terms of knowledge and correlation of data provided by users, with a significant impact on its economic value.

In the same way as the "route poisoning" (affecting the telecommunications network), the "poisoning action" are conducted with the aim to pollute the contents of this social network profiles typically introducing artifacts and relationships exist between them and real ones thus making the information unreliable. The result is the consequent failure of the chain of trust which are based on all social networks, in order not to allow search engines specifically developed to retrieve information of any kind relating to a particular profile.

Starting from the assumption that Internet and in particular the social network lacks a coherent and safe management of digital identity, it is possible to introduce the main tools currently poisoning and to hypothesize a new and viable in a future scenario:

Current tools

- Replacement of identity, or the ability to impersonate another user to the wide variety of purposes intelligence social engineering.
- Simulation of identity, creating a false profile, which does not correspond to any existing person, for malicious purposes or simply to remain anonymous.
- Fuzzing profile, the voluntary introduction of elements false and / or non-matching to your profile to deceive intelligence systems, to prevent OSINT activities or other forms of personal gain.
- Fuzzing social graph, the association intended to groups and individuals that have nothing to do with their interests and relations with the intention of introducing "noise" in their social graph.

Future instruments:

Personal /social bots , creating a large number of fake profiles (e.g. millions of fake profiles) managed by machines, able to interact with real users in a way likely, thus changing the "sentiment" and "conversation" "large-scale as well as altering all the social graph and to preclude meaningful correlations on the data.

Black curation, the use of real users "holes" or fictitious to speak on topics of which you want to change the meaning, or to create new one ad-hoc, in analogy to the black SEO (search engine optimization) already use on search engines.

How easy to understand the interest in social networks are the stars. Complex systems analyze information, scan faces and places, building new relationships and providing new information. Government agencies and companies have realized the full potential of the medium, a real gold mine in which the imperative is the power, information, and control of a at the expense of a user too distracted and inattentive to the dangers ahead.

What to suggest to a friend node, be social, but sparingly. Be human first!

If you are interested to real case refer

<http://securityaffairs.wordpress.com/category/social-networks/>

Author :

Pierluigi Paganini, Program & Delivery Manager at Bit4Id s.r.l.

Monthly THN Updates

The Spy Files: Wikileaks expose Mobile Phone, Email Hacking capability (12/01/2011)

Wikileaks has released (<http://spyfiles.org/>) dozens of new documents highlighting the state of the once covert, but now lucrative private sector global surveillance industry. According to Assange, over 150 private sector organisations in 25 countries have the ability to not only track mobile devices, but also intercept messages and listen to calls also. **Read More :** <http://goo.gl/crWFL>

Your Android Phone is Spying On You, Use custom ROM To Protect your Privacy (11/30/2011)

In this digital age, privacy is more important than ever. Just because you “don’t have anything to hide,” does not mean that you shouldn’t value your privacy or fight for it when companies do things like this, especially with something as personal as your cell phone. An Android developer recently discovered a clandestine application called Carrier IQ built into most smartphones. **Read more :** <http://goo.gl/mz8dZ>

Security Research : Be friend to anyone on Facebook in 24 hours (11/29/2011)

People have simply ignored the threat posed by adding a profile without checking if this profile is true. New Technologies have loopholes, but it is up to the users to be aware of this type of flaw. Social networks can be fantastic, but people make mistakes. Privacy is a matter of social responsibility. **Read More :** <http://goo.gl/DjXTC>

Millions of printers open to devastating attack (11/29/2011)

Could a hacker from half-way around the planet control your printer and give it instructions so frantic that it could eventually catch fire? Or use a hijacked printer as a copy machine for criminals, making it easy to commit identity theft or even take control of entire networks that would otherwise be secure? It’s not only possible, but likely, say researchers at Columbia University. **Read More :** <http://goo.gl/H7DoR>

Monthly THN Updates

New Facebook Worm installing Zeus Bot in your Computer (11/29/2011)

Recently We Expose about 25 Facebook phishing websites and also write about biggest Facebook phishing in French which steal more then 5000 usernames and passwords. Today another new attack on Facebook users with Zeus Bot comes in action. **Read More :** <http://goo.gl/ubfw7>

More than 100 Pakistani Government Sites Under Malware attack Website Malware (11/29/2011)

A newer form of malware is what can be found attacking websites today. In the old days malware was mostly in the form of computer viruses. In today's age of globalization, malware starts to target websites and mobile devices. Almost 100's of Pakistan Government sites are under attack by Godzilla Malware, Which is Created and implemented by an Indian Hacker. **Read More :** <http://goo.gl/pVh70>

Discovered the biggest Facebook phishing in French (11/28/2011)

Two Days before we publish that Geeks at Security Web-Center Found 25 Facebook phishing sites. Security Web-Center found another biggest Facebook phishing site in French which steal more then 5000 usernames and passwords, using the fake domain www.frfacebook.fr to scam the victims. **Read More :** <http://goo.gl/DPhoI>

Manila AT&T hackers linked to 26/11 Mumbai terror attack (11/28/2011)

Police in the Philippines working with the US Federal Bureau of Investigation have arrested four people over a premium-line phone scam that targeted customers of the American telecommunications giant AT&T to funnel money to a Saudi-based militant group. These four suspected hackers accused of funnelling profits from attacking corporate telephone networks to an Islamic terrorist group blamed for the attacks on Mumbai three years ago. **Read More :** <http://goo.gl/kXdf3>

Monthly THN Updates

Largest DDOS attack hit Chinese company (11/24/2011)

A week-long DDoS attack that launched a flood of traffic at an Asian e-commerce company in early November was the biggest such incident so far this year, according to Prolexic, a company that defends websites against such attacks. The distributed denial-of-service attack consisted of four consecutive waves launched from multiple botnets between Nov. 5 and Nov. 12, 2011. **Read More :** <http://goo.gl/VYmSt>

New Approach to automatically detecting bugs and vulnerabilities in Linux (11/22/2011)

Australian researcher Silvio Cesare, PhD student at Deakin University has released a tool capable of automatically detecting bugs and vulnerabilities in embedded Linux libraries. Developers may “embed” or “clone” code from 3rd party projects. This can be either statically link against external library or maintaining an internal copy of a library’s source or fork a copy of a library’s source. **Read More :** <http://goo.gl/QV5RW>

Hackers destroyed a pump used by a US water utility (11/19/2011)

Hackers destroyed a pump used by a US water utility after gaining unauthorized access to the industrial control system it used to operate its machinery. Five computer screenshots posted early Friday purport to show the user interface used to monitor and control equipment at the Water and Sewer Department for the City of South Houston, Texas. **Read More :** <http://goo.gl/qE1vF>

Stuxnet 3.0 to be possibility released at MalCon? (11/15/2011)

Malware coders and security researchers are increasingly looking at MalCon malware convention to show-off their latest creations and research. We were pretty shocked to see in a twitter update today from MalCon, that one of the research paper submissions shortlisted is on possible features of Stuxnet 3.0. **Read More :** <http://goo.gl/IWP7Z>

Monthly THN Updates

Duqu computer virus Detected by Iran civil defense organization (11/13/2011)

The virus is called W32.Duqu, or just Duqu create fear after the opening Pandora's Box of Stuxnet. The head of Iran's civil defense organization told the official IRNA news agency that computers at all main sites at risk were being checked and that Iran had developed software to combat the virus. First, Duqu is not deigned to harm industrial automation. **Read More :** <http://goo.gl/xdYOM>

Bizztrust : The Most Secure Android Phone (11/12/2011)

With companies these days justifiably concerned about the security of the mobile devices provided to their workforce, many workers find themselves carrying around two mobile phones - one for personal use and another for business. Sure, mobile phones aren't the huge pocket-stretching devices they once were but for the sake of convenience, one is most definitely better than two. **Read More :** <http://goo.gl/YHXec>

Possible Credit Card Theft in Steam Website Hacking (11/10/2011)

Valve CEO Gabe Newell has contacted all users of the Steam game distribution platform to let them know that the company has suffered a security breach. Right before going offline, users saw a new category in the forum that directed them to open a site named "Fknowned." Many users also complained that their email ids related to Steam accounts were "spammed with ads for the web site. **Read More :** <http://goo.gl/YBzgy>

Computerized Prison doors hacked with vulnerabilities used by Stuxnet worm (11/09/2011)

Security holes in the computer systems of federal prisons in the United States can effectively allow hackers to trigger a jailbreak by remote control. The discovery of the Stuxnet worm has alerted governments around the world about the possibility of industrial control systems being targeted by hackers. **Read more :** <http://goo.gl/ESXbH>

Monthly THN Updates

Anonymous Hackers hack neo-Nazis website & leak personal info of 16,000 Finns (11/08/2011)

Anonymous Hackers have successfully hacked the neo-Nazi website and published the database of its 16000 membership application database containing personal data of some applicants from all around the country.

Read More : <http://goo.gl/CS9rI>

Researcher Charlie Miller kicked out from iOS dev program for Exploiting iOS security flaw (11/08/2011)

A major security flaw in Apple's iOS operating system that could allow hackers to remotely gain unauthorized access to an iPhone, iPod touch or iPad has been uncovered by a security expert "Charlie Miller ". Charlie Miller gets a kick of out defeating Apple's security mechanisms, using his hacking skills to break into Macbooks and iPhones. **Read More : <http://goo.gl/qU7Tx>**

China is the birth place for most of malicious Android apps (11/07/2011)

Mobile malware is rising, and there have been explosions in the world of viruses and Trojans. Virus makers are now targeting mobile platforms-thanks to their growing popularity. If we take the statistics from last 6 months, the chances of Android smart phones to be infected have doubled. **Read More : <http://goo.gl/RNBGJG>**

Brazil ISP servers under Massive DNS poisoning attacks (11/07/2011)

Kaspersky Lab expert Fabio Assolini Report that A massive DNS cache poisoning attack attempting to infect users trying to access popular websites is currently under way in Brazil. Several large ISPs in the highly connected country have been affected by the attack, and police have made at least one arrest in connection with the operation.

Read More : <http://goo.gl/xHF2D>

Monthly THN Updates

Anonymous attack on Israeli government & security services websites (11/06/2011)

Several Israeli government websites crashed on Sunday in what appeared to be a cyber-attack by Anonymous hackers. The websites of the IDF, Mossad and the Shin Bet security services were among the sites that went down, as well as several government portals and ministries. The Israeli army and intelligence agencies' websites were offline. **Read More :** <http://goo.gl/h7baF>

Duqu malware was created to spy on Iran's nuclear program (11/05/2011)

A Report by Kaspersky Lab Expert, Ryan Naraine says that the DUQU malware was created to spy on Iran's nuclear program. IrCERT (Iran's Computer Emergency Response Team) Duqu is an upgraded version of "Stars". Back in April this year, The Iranian government says it is being targeted by a new piece of malware aimed at its federal computers. **Read More :** <http://goo.gl/Cy7iG>

Super Cryptography : The Next Generation Encryption (11/03/2011)

The next generation of encryption technologies meets this need by using Elliptic Curve Cryptography (ECC) to replace RSA and DH, and using Galois/Counter Mode (GCM) of the Advanced Encryption Standard (AES) block cipher for high-speed authenticated encryption. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. **Read More :** <http://goo.gl/gPqdG>

Happy Holidays !!

It is hard to re-cap the past year and all the excitement and hard work we have experienced launching an online magazine. The subject, Hacking, is even more exciting as the technology world awakens to the security issues facing all internet users from government, large corporations and personal users.

We have tried very hard to keep the readers informed and up to date regarding security threats and security breaks world wide. Our daily news aims to give business and personal PC users an understanding of what is happening in computer security developments and what criminal activity is breaching security systems.

Mostly, we understand the importance of disseminating information and keeping the internet free of restrictions. We believe that information and opinion are the foundation of a healthy society and we strive constantly to address the political and social issues facing our new world of electronic communication. You may or may not agree with all we have to say but know that we have your best interests at heart and work hard to give you all that you need to know what is happening in the world and how it affects you.

Truth is power. Our mission is to keep all of us powerful in a positive and productive manner and let those that try to suffocate our rights know that we are watching and taking appropriate action.

In the end, The Hacker News could not be successful without you, the reader. We have so much heartfelt thanks for your support and your participation in our emerging success.

We also know that we could not be who we are without the following people:

- Patti Galle
- Kislay Bhardwaj
- Priyanshu Sahay

We here at The Hacker News wish all of you a Happy Holiday and a safe, secure new year.

Mohit Kumar,
Founder & Director - The Hacker News