

CENSORSHIP!



NO QUESTION-NO FREEDOM-NO LIBERTY!

Index

1.) Internet Censorship, A Global Concern	Page 1
2.) DDOS Attacks Is Digital Protest Legal Or Illegal?	Page 3
3.) Monitoring or censorship? The big fear	Page 7
4.) Ways and Tools that Destroy Censorship	Page 13
5.) Unfortunately, No Real Surprise	Page 18
6.) Interview on Censorship	Page 21
7.) Secrets at Risk in Cyber Space	Page 25
8.) Why are information security incidents in the news?	Page 28
9.) Hacking News Updates of Month	Page 31

Internet Censorship

A Global Concern

By : Mohit Kumar

Back in the early 1960's, Canadian educator, philosopher, professor and scholar Marshall McLuhan (July 21, 1911 - December 31, 1980) apply predicted that the whole of mankind would one day be connected through "electronic interdependence". McLuhan predicted how there would be a dramatic shift from individualism to a collective identity throughout the world and McLuhan's coining of the idiom "Global Village" couldn't be more accurate than today, with thanks to the World Wide Web. The internet has made tremendous inroads since the Internet was commercialized in 1995. In December of 1995, a total 16 million people around the world were using the Internet, but by June 2010 a staggering 1.97 billion people were internet users worldwide. With so much unprecedented access to information, like no other time in world history, we are beginning to see more and more attempts by governments and businesses to control the Internet for their advantage and personal gain and oppression of the masses.

Internet censorship has rapidly become a global concern. Many countries are following the United States lead their misguided attempt to censor the World Wide Web. Therefore, it is not much of a surprise to be witnessing how censorship of the internet has become one of the main instruments of oppression and the smothering of dissent by oppressive governments and corrupt corporations around the world. Around our globe we see how tyrannical and dictatorial leaders are threatened by the power of the internet. These corrupted governments and corporations that are continually attempting to censor the internet, are also trying in numerous other ways to censor their citizens very thoughts. But there is hope, because these oppressors are vastly out numbered and the majority of people around the world firmly believe the internet should be a place for and of freedom of speech; without any considerations of religious, social, or political orientation. Within the soul of man lies the fundamental understanding that the right to express ones own opinions is one of mans most basic rights.

Tweeting, blogging, and social sites like Facebook have anointed the internet as the nucleus for rebellion and dissent into today's world.

Today, activists are effectively using the internet to resist authoritarian oppression around the globe. Not surprisingly, online activists are now an extremely important and essential part of the world-wide struggle for human rights. We are witness to a social internet rebellion, unique in human history, where hacktivists, bloggers, tweeters, Facebook and other social participants have become some of the most ardent guardians of liberty, freedom and social justice. Everyday brave on line dissidents amplify, through their untold numbers, the unassailable power of freedom and the basic right of freedom of ideas and thoughts via the tenuous fragile freedom of the internet.

As crushing inequality and extreme poverty continues to fuel unrest throughout the world; oppression by corporations, corrupt and authoritarian governments and the elite, which owns them, will be ratcheted up and we will witness a fight to the death to maintain their wealth and power and the status quo. The fact that 1 % of the world population owns 40 % of the global assets or the richest 2 % of the world population own more than 51 % of the global assets, or that the richest 10 % own 85 % of the global assets is fueling unprecedented unrest around the globe. The distinctiveness and growing power of the internet is creating a unique opportunity for online activists to promote freedom and equality and have an unprecedented impact on global human rights. Without a doubt, because of the internet, activism has been forever changed. But we must all stay vigilant because there is no conclusive proof or guarantees that those that hold the bulk of the world wealth and power are not working diligently to find a way to turn the Internet into a powerful tool of oppression.

"Censorship is never over for those who have experienced it. It is a brand on the imagination that affects the individual who has suffered it, forever"

-- Noam Chomsky

DDOS Attacks

Is Digital Protest Legal Or Illegal?

By : Lee Ives



When Mohit (THN Editor) asked if I could write this article I sat down and thought about this question for all of about 0.1 seconds.

The answer is, of course, quite obvious: NO.

DDOS attacks are illegal , I would imagine, in most countries of the world. And, if they aren't, then they certainly should be.

A Distributed Denial of Service attack involves flooding a web site with requests for data with the intention of making that site inaccessible to other, genuine, visitors. At best, a DDOS attack will leave visitors to the site frustrated. At worst, it could cause a business to potentially lose millions of dollars in lost revenue, both now and in the future. To my mind that is good enough reason for them to be illegal.

So, perhaps the question here should not be whether using DDOS attacks as part of a protest are legal, but whether they are an ethical or an otherwise valid means of getting your point across?

DDOS Attacks – Is Digital Protest Ethical?

My answer here is again NO.

I personally cannot see any set of circumstances under which a DDOS attack could be considered ethical in any way, shape or form.

Sure, protest itself should be legal, as it is in many ‘civilised’ countries of the world. It is an essential right in a democracy and one that many brave men and women have died to protect throughout history. We should have a right to free speech and we should be able to gather together to demonstrate against the powers that be when we feel that they have let us down.

But there are ways and means of doing so.

A DDOS attack isn’t so much a protest as a suppression of free speech in my opinion. If you take a web site down because they have a different viewpoint to you then how are you better than them? You’ve just censored the web based upon your own values. And that is ironic when you consider that many of the people behind such attacks are so against the likes of SOPA, PIPA and ACTA which are, arguably, so universally hated because of the way they could potentially suppress content on the web.

DDOS Attacks – Is Digital Protest Worthwhile?

There is another point here as well and that is one of perception. I don’t know about you but if I try to visit a web site and cannot gain access because it is timing out then I choose to either find what I was looking for

elsewhere or return later. I don't really stop to consider whether a site is down due to a DDOS attack or not and, unless I have read about it elsewhere, I will never know that is the reason anyway, let alone care. That may not be the right attitude to have perhaps but it is the truth and I can well imagine that many other people feel the same way.

Besides, there are far more effective means of protest anyway aren't there?

Until very recently I doubt very many people knew much at all about SOPA and PIPA. But then some major websites, such as WikiPedia, posted messages about it in order to raise awareness. Almost immediately we saw the U.S. government rethink their position.

More recently we have seen real world protests with large numbers of people taking to the streets to protest against ACTA. Again, real results have been seen here as in many countries, such as, Germany which are now rethinking their position on that piece of legislation too.

In both of these instances the protesting has been done in what I would describe as the right way, the legal way, and the results have been positive.

If a hacking group such as Anonymous had DDOS'd government web sites into oblivion do you think that we, the people, would have achieved a better result here? I don't think so.

DDOS Attacks – The Alternative View

Of course not everyone feels the same way about this topic. I've spoken to several people recently who feel as if governments and big businesses are not listening to what we want. Sometimes I think they may well have a point too.

These people feel that sometimes you have to hit these entities where it hurts by either cutting off their voices or by hitting them where it hurts, i.e. by taking money away from them. They feel that Distributed Denial of Service attacks, whilst perhaps not ethical, and certainly not legal, are in fact completely justifiable in some circumstances.

It is their opinion that taking down websites in the 21st century is not much different to barricading a physical location in the 20th century. They say it brings publicity to their cause and, in some respects, they are right.

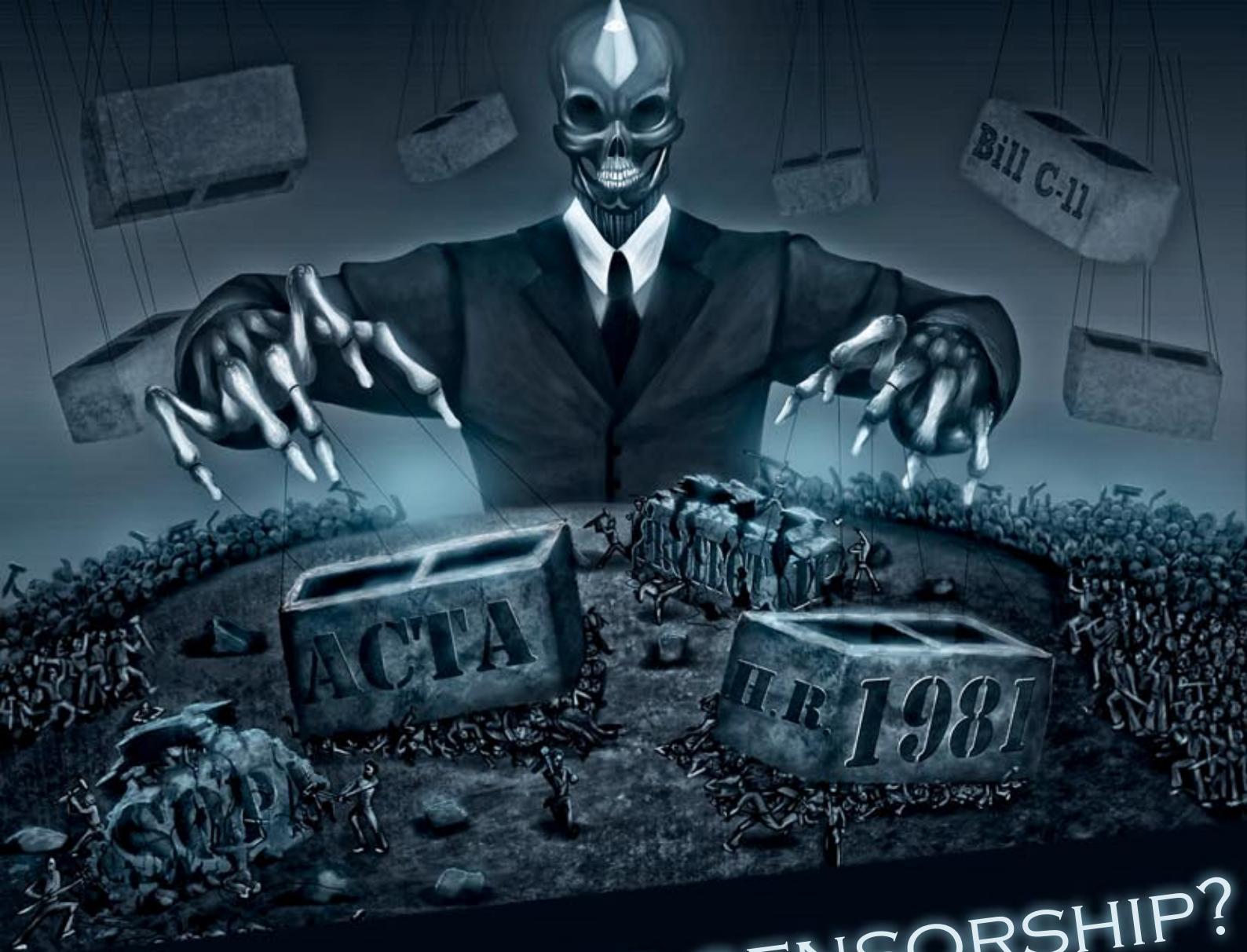
But that still doesn't excuse the fact that DDOS attacks are illegal. And as I mentioned before, there are still far more effective means of making your point. So, for now at least, in my mind DDOS attacks as a protest tool are out.

Instead, go grab your like minded friends and colleagues and make a legal protest on the web or write out your banners and march in the streets – if your cause is valid and your views are shared by the masses then your voice will still be heard.

About the Author: Lee Ives is an internet security blogger from London, England. <http://www.security-faqs.com>

Disclaimer: This Opinion piece presents the opinions of the author. It does not necessarily reflect the views of The Hacker News Magazine, its editor or Staff.





MONITORING OR CENSORSHIP? THE BIG FEAR

By : Pierluigi Paganini

During the last years we have seen the tendency to use social media as a major vector for the exchange of information. The communication concept has been totally revolutionized as billions of people could be in contact with a few clicks thanks to the social network platforms. Imperative is to be social, no matter if you need to share photos with friends, to express an opinion on a topic of public interest or manifest dissent regarding a government. Over the past year a large number of protests have been conducted through the major social networking platforms from Twitter to Facebook, because they have an extraordinary media that is able to reach an audience of planetary size with a simple click.

Governments and agencies all over the world are aware of this social phenomena, and an extraordinary quantity of information passes through these new social medias and the approach pursued by governments is to carry on monitoring actions in order to guarantee national security. (or so they say)

The approach in terms of national security is correct and shared, however, raises serious questions in terms of privacy. This control often causes despicable acts of censorship and repression. At stake is the freedom of thought and protection of human rights, concepts humiliated every day in the world and the cost paid by the world community is a large number of human lives. Monitoring can lead to fierce repression, can lead to torture, can lead to death.

Every day there is an unimaginable number of intercepted information, whether phone, email, SMS and data. In the name of security control, the imperative is to spy on everybody! No one is safe from the eye of the modern Orwellian Big Brother mandated by governments everywhere. An affair of many billions of dollars a year with the involvement of government agencies and private companies that make their services available to democracies and dictatorships in an unregulated market.

If you search evidences of these activities it is sufficient to Assange's "Spy Files" or Cryptome web sites, both provide useful info regarding electronic surveillance services provided by government and private companies in all countries. Amazingly, everything can be controlled and commoditized.

But what are the real causes of government interference?

There are two main reasons,

1. National security
2. The spying with the intent to acquire information that directly or indirectly can bring profit to a small group of people.

This second intent is the most dangerous, and even those two reasons are overlapped. Too often the supposed need for national security is abused to exercise control, unfortunately for private purposes. It happened to us in Italy, it is common practice in many industrialized countries.

We make a serious error if we considered the problem related only to isolated and far realities such as China, Egypt or Iran. In various ways and in varying measure all States are equipped to carry out a more or less close control of the media and of Internet in general. Western governments use a different way for this powerful platform to prevent terrorism, frauds, pornography but also to monitor the sentiment of entire populations and maybe to influence it. To understand this we can simply give a look to the "the transparency report" produced by Google that regularly receives requests from government agencies and courts around the world to remove content from their services and hand over user data. Government Requests tool discloses the number of requests we receive from each government in six-month reporting periods with certain limitations ... you will notice that behind China there are countries like Germany and France. Surprised? Do you believe that all the requests are related to piracy or similar issues?

Currently, it is really hard, we are facing the worst economic crisis, with social dissatisfaction and an overwhelming sense of profound vulnerability that the 9-11 has left. The mixture is explosive. On one hand, Governments that have to be able to control, hopefully for noble purposes, to ensure the safety of the people, on the other hand movements of thought that can not tolerate the interference of these preventive measures. Are you able to imagine a world in which everybody is free to communicate without being intercepted, spied on or tracked? Is it an unrealizable dream due the enormous interest involved?

China has been a major proponent of government spying with the "Golden Shield Project".

"If you open the window for fresh air, you have to expect some flies to blow in"

This Is The Deng Xiaoping's phrase, which effectively summarizes the essence of the project, also known as the "Great Firewall of China ". The project is related to the development of the system of censorship and most efficient surveillance in the world made by the People's Republic of China.

The monitoring model is a reference for all the authoritarian regimes for governments worldwide. Most of them have developed a specific cyber strategy that addresses surveillance procedures to ensure government security, it's happening today in USA with SOPA where they desire to legislate cyber space and impose their control to prevent any form of terrorism and dissents. We are observing a growing trend toward Internet censorship in a range of countries that are investing in the necessary technology to implement the control. The technologies are exactly the same used to secure network infrastructure from attack. Censorship seems to be intended as a new business opportunity, control and censorship through complex content filtering platforms for sale to governments and the seller avoiding every control and international law. It has happened, for example, in a sale of a similar systems to the Iranian government by an Israeli company through a Danish seller.

A few months ago I read the news regarding a tender held by the Soviet government on the implementation of an internet monitoring system. Russia's intent is to release a massive monitoring system that will be used to control internet usage made by a nation that in September became the European country with the largest number of Internet users, according to the Comscore ratings agency.

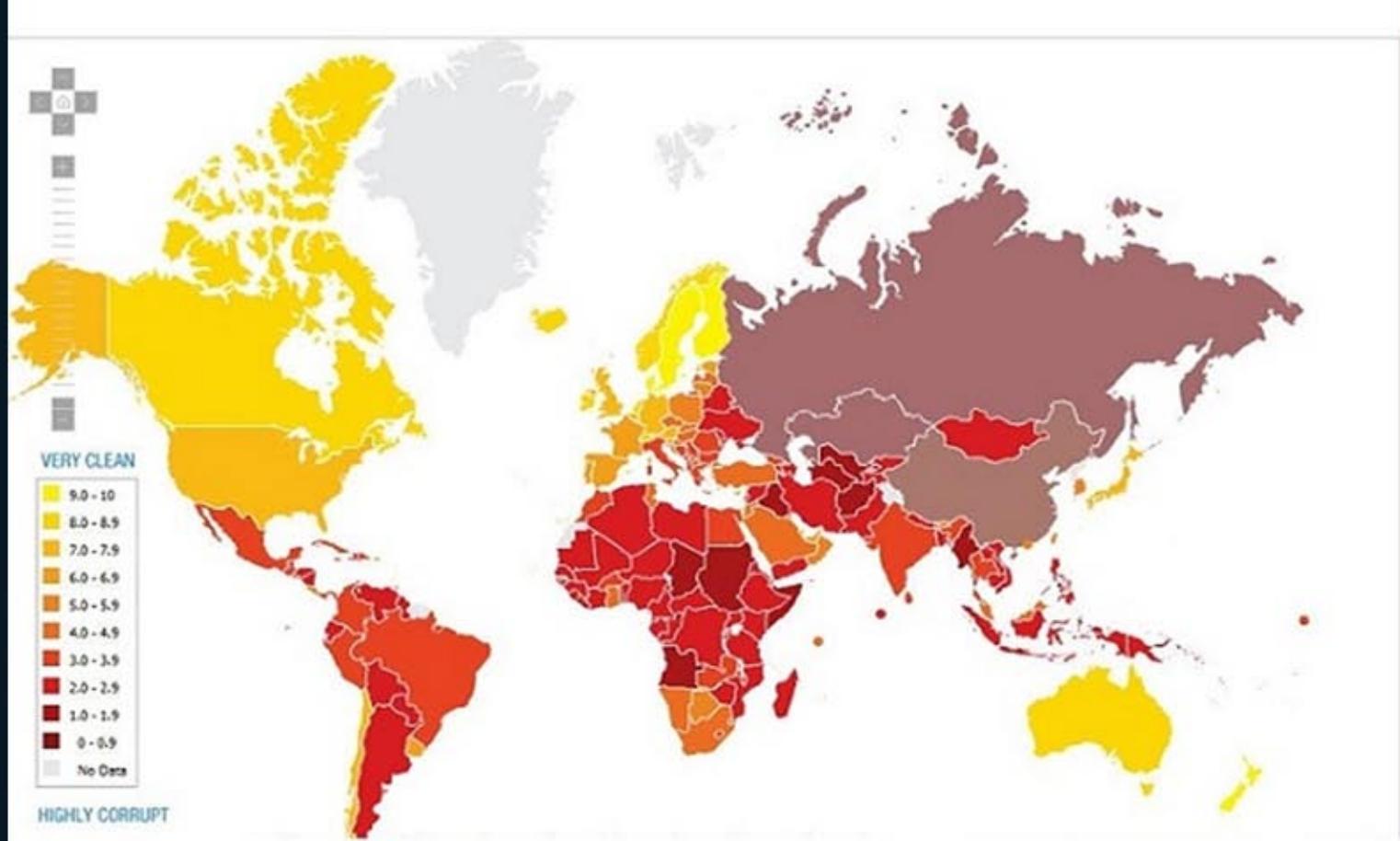
Do you not find the news disturbing? Do you remember what happened during the last election in Russia? Remember how Putin's followers have acted against the opposition in cyberspace? Are we sure that the Russian government has acted in the name of national security and not for private purposes?

The crucial point is the legality of these actions conducted by Intelligence Agencies in the name of National Security abusing the rights of citizens. To this we must consider another significant issue , the corruption. Corruption has no Country and is a cross problem widely

diffused. The dilemma is always the same ... "who controls the controller?" It is obvious that those who manage massive e-surveillance systems have a vantage point to gather confidential information and therefore make for powerful private interests.

Let's give a look to a corruption perception report and related map.
http://www.transparency.org/policy_research/surveys_indices/cpi/2010/results

CORRUPTION PERCEPTIONS INDEX 2010 RESULTS



It's clear that all those States that are investing in e-Surveillance systems are the same governments that suffer major corruption problems. I believe that the combination of these two factors is dangerous and you should want to fight the cyber threat. Here are some sample of monitoring systems deployed in Country with high level of corruption.

Recently, the United Nations declared "Right to Access" to the Internet as a Human Right. This would have a positive impact upon many Human Rights in Cyberspace. For instance, Right to Speech and Expression, Right to Privacy, Right to Know, etc cannot be violated by any CMS

Project. United Nations must expand Human Rights Protection to many more issues considered part of this violation.

It makes no sense to promote human freedom closing the eyes on corruption events, because of the direct correlation that there is between corruption and policy to implement detailed traffic filtering.

Let me conclude with the hope that all the Governments that have introduced monitoring systems are confident about their actual usage and that they will fight corruption in the same way they have declared war to any cyber threat.

About the Author : Pierluigi Paganini, Security Specialist
CEH - Certified Ethical Hacker, EC Council
Security Affairs (<http://securityaffairs.co/wordpress>)
Email : pierluigi.paganini@securityaffairs.co

Ways and Tools that Destroy Censorship

By : Mourad Ben Lakhoud

Browsing the web anonymously interests not only hackers but also people that are looking to protect their privacy. Some regimes in the world are following their citizen's online activity and arresting them for submitting a blog post or a comment they find undesirable. All this makes people more attracted to "anonymizing" their online activity. In this post we are going to list some tools and ways to bypass censorship and help you wear the Cap of Invisibility.

The Amnesic Incognito Live System

The first solution is Tails, a Debian based operating system ISO image that you can burn onto a CD-ROM or USB stick and take it with you anywhere. All you need to do is boot from it and all your connections to the internet will be tunneled over the Tor network.

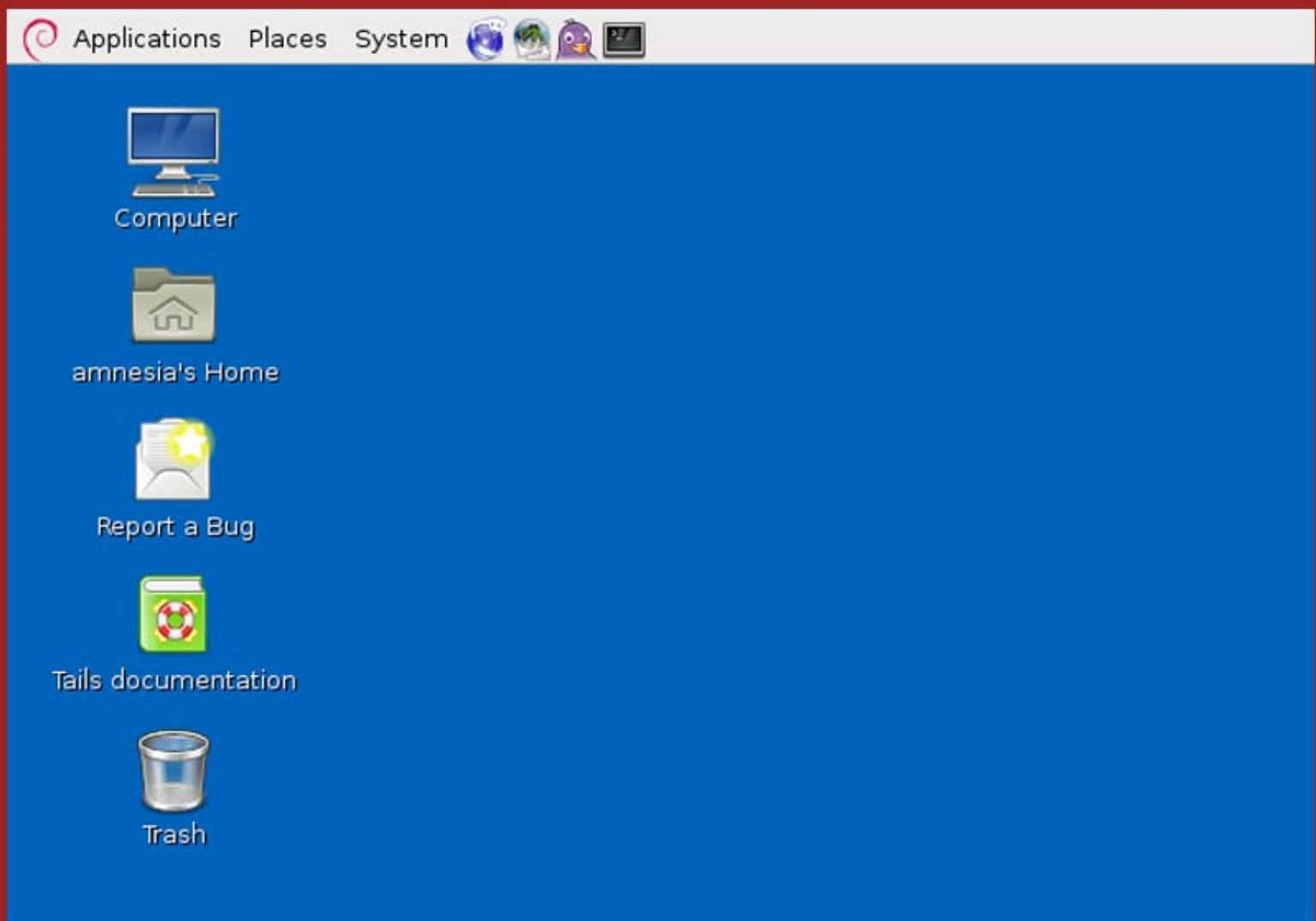
Tails will provide you with a complete desktop and all necessary applications (such as open office, Pidgin, Firefox and more). It also supports 3G connections so you don't need to install any third party applications, and it supports several languages including Arabic, Chinese and more. The image is about 2GB and when you stop the machine you leave no traces about your activities.

At the encryption level there are a bunch of important and useful tools that you have on the system including the following:



- LUKS (Linux Unified Key Setup) a Linux standard program for encrypting storage. If you are using a USB stick you can directly store on it any document or file with a solid encryption
- HTTPS encryption over the browser by using a standard Firefox plug-in HTTPS Everywhere. This can be a good way to secure your navigation at the Tor network, so if there is a person attacking on your road all your navigation is protected.
- Email signing tool with the standard openPGP. If an attacker receives your email it is almost as secure as if it was signed by your keys.
- For the Instant messaging system you can find OTR a crypto tool to authenticate and encrypt your IM communication so there is no way for a MITM Attack.

If you are using a public computer that blocks access to boot your system you can download virtualbox and run your ISO image on the virtual machine. I am a Debian user so I prefer Incognito.



Screenshot for Incognito Live System

Liberté Linux

The second tool is Liberté Linux, a hardened Gentoo based operating system that comes with increased safety for communication over the Tor network. You can use it in the same way as previous LiveCD or a flash USB boot system. Tools that are available on the system are the following:

- Midori a light web browser that provides all required functionality for navigating the internet (by the way it is preconfigured to use Tor network).
- Claws Mail fast and easy e-mail application that supports GPG encryption.
- Evince, a tool to open pdf files.
- AbiWord is a free word processing program similar to Microsoft Word.



For the Google search Midori is configured to use <http://www.scroogle.org/> but this search engine was disabled by Google, instead you can use <https://ixquick.com/>, a good online search engine that will protect your privacy.

Note that all required services are torified but you still can use the unsafer browser in some cases such as registering your computer on a wireless network. Netfilter is installed and configured to block all inbound and outbound traffic for packets including DHCP, DNS, NTP and even all downloaded signing keys, as well as the kernel patches checksums, are located in the Liberté source tree.

Privatix Live-System

The third solution is Privatix Live-System “Privatix Live-System is a live-cd for encryption and privacy issues and helps you to install Debian GNU/Linux and is very easy on an encrypted usb-key or on an encrypted external harddisk.



You can use it as:

- Installer to setup a Debian GNU/Linux system with a persistent home on an encrypted usb-key or on an encrypted external harddisk without much knowledge and work. For example, you can start the installed mobile live-system on unknown computers to encrypt your email with thunderbird, enigmail and gnupg or to work safely with your private data. All your settings and data will be safely encrypted on the usb-device.
- live-cd for rescue or administration work needing encryption-tools
- Easy to use live-cd for anonymous internet surfing with Tor, Firefox and Torbutton. You will be able to do that safely even if security holes are detected in Firefox or tor, the live-cd can clone itself including the Debiants latest security fixes”

Conclusion:

Whether we are being de-privatized by government, media outlets or any other controlling entity, free political expression is every ones right, and the internet comes as an important place for sharing and producing information without any censorship for the benefit of the entire globe. Apparently, freedom doesn't come free and we all must fight to end censorship and invasions of privacy.

Reference:

- [1] <https://tails.boum.org/>
- [2] <http://dee.su/liberte>
- [3] <http://www.mandalka.name/privatix/index.html.en>

Written By : Mourad Ben Lakhouda is an Information Security practitioner. Admin at www.sectechno.com | info@sectechno.com

UNFORTUNATELY, NO REAL SURPRISE

By : Patti Galle
Editor THN



In the last year THN has published numerous articles on internet privacy. It has been our mission to draw attention to the fact that all governments worldwide are increasing their cyber spying on their citizens. THN hopes our readers have become more mindful of the escalating and serious situation of governmental spying.

THN is certain that many of you have been surprised to learn how doggedly governments are spying on its citizens, even those of you living in democratic countries. We hope we have also help inform any unaware reader how security vendors, who publicly work to protect the public from electronic eavesdropping, are complicit in such monitoring of their own citizens.

It comes as no surprise to learn from WikiLeaks founder Julian Assange that virtually all world governments spy on their own citizens and on foreigners using clandestine spyware on cell phones, GPS devices, computers, and numerous other new electronic devices. In December of 2011, WikiLeaks released a 287 file document dump WikiLeaks called The Spy Files. The released files described in great detail the relationship between national intelligence agencies and the commercial software, security and surveillance companies they hire to provide technology that allows them to secretly listen in on cell phone conversations, text messages, email and Facebook, Internet traffic and other location data. Another large conflict of interest inherent in the complex web of relationships described in The Spy Files is the intricate relationship of phone manufacturers, most of which are multinational corporations, with various governments. As an example, Cisco Systems is listed as helping with both computer and cell-phone monitoring not only helping the US government but other repressive governments such as China and the manufacturer and maker of Dragon Naturally Speaking speech recognition software, Nuance Technology was also listed as helping with cell phone and speech analysis.

Steven Murdoch a University of Cambridge researcher recently alleged that governmental intelligence agencies are spying on their own citizens not out of some illusive inkling that their citizens are up to no good, but as an across-the-board strategy to collect information on the hypothesis it may eventually be of some use. "We're seeing increasingly wholesale monitoring of entire populations with no suspicion of wrongdoing," Murdoch said during the panel session. Without controls on this industry, the threat that surveillance poses to freedom of expression and human rights in general is only going to increase." Murdoch stated.

Without a doubt, personal privacy and an individual citizens basic right to hold personal and political views include not being singled out and spied on by their own government. This is unquestionably indispensable to any society that calls itself free or is moving towards a more democratic society. It is the discrepancy between the unrestrained powers of tyrannical governments and the deteriorating freedoms of the average citizen where the critical issue of privacy resides.

In the end, without personal privacy and the basic right to hold personal and political views without being singled out and spied on by their government, a population is poorly equipped to thwart the growth of tyranny or produce anyone to defend those important and basic rights.



“Having been blacklisted from working in television during the McCarthy era, I know the harm of government using private corporations to intrude into the lives of innocent Americans. When government uses the telephone companies to create massive databases of all our phone calls it has gone too far”.

~ Studs Terkel ~

Interview on Censorship

As a treat for our readers we have a short but very informative interview with **Pierluigi Paganini**, a well known Security Specialist & CEH - Certified Ethical Hacker.

1) How possible is it for governments or other bodies to police the web successfully? What are the normal technologies they use? How do people in turn use technology to work their way around it?

All Governments are extremely interested in the control of the Web and beyond, they also closely monitor telephone calls and any social media. The detailed control is possible through essentially the same technology used for the implementation of major infrastructure networks.

The methods used for control are varied and I propose to split them into categories:

- Tools for massive wiretapping. In this category are placed both hardware devices and software platforms for content filtering, both able to analyzes the content of the traffic within a network. In recent years the attention towards the main social media has increased. Specifically, developed software allows the tracing of communication within social networks by providing systems for complex investigations. These software are capable of analyzing an impressive amount of information and are able to punctually trace the profile of each user. In recent years, in order to enhance these tools that have been used even facial recognition systems that are able to parse huge volumes of information in search of a face or a place are subject to analysis.



- Monitoring through the use of malware. These techniques involve the use of malware that infects the victim's computer allowing you to monitor all operations performed on it. An example is what happened in monitoring Skype communications in Germany. Usually this technique is used for specific monitoring and targeted investigations, however, they are known in the security sector companies who are specialized in the development of agents to control the masses through this technique. Wanting to give an example I quote the FinFisher company that produces systems that can infect computers by falsifying websites or updates of popular software and getting the user to download the ITS software. This remote monitoring software can then monitor what the user is doing on the Internet - Including emails, web surfing and even transfer of sensitive documents.
- Interception systems. In this category we find packet inspection systems which monitor the individual packets of data traveling across the Internet travelling from the main backbone to the final user. Other common techniques inside small networks make use of well known techniques called "man in the middle" in which the controller inserts himself between two devices that are communicating.
- Telephone Interception devices. Commercially available systems that can intercept and eavesdrop without problems every kind of communication from GSM phones to the latest generation. Again, with particular reference to smartphones, it is possible to make use of malware or other apps that can monitor communications from the target devices.
- Data Analysis Systems - Software platforms that are able to analyze data being collected through surveillance and other methods. The more sources of information the more complex the analysis.
- Last but not in order of importance is the chapter OSINT, or open-source intelligence, the gathering and analyzing data from publicly available sources (e.g. government records and documents, social-networking and user-generated Web content like forums and personal web pages.)

It is impossible not to be intercepted, or better, precautions should be taken but they are not justifiable from a private account.

2) China is quoted as the only country which has successfully done it? How do they manage it? What are the technologies that they employ which make it possible? Or is their success entirely dependent on their system of governance ?(Is there a case for saying that the Internet can only be policed successfully if you have the ability to police free thought itself)

The success of the Chinese project, "The Golden Shield," has been possible thanks in part to western technologies. Systems networking products from major companies such as Cisco, Siemens and others. No alchemy. Consider also that the important support of the Chinese Huawei is one of the leading global ICT solutions provider.

3) Is it possible for networking sites like Facebook and file sharing sites like Megaupload to monitor everything that is uploaded? Can there be technologies they can use to make it possible? Or is it just an impossible ask?

No doubt, yes they can! Companies have the technologies required to analyze the content passing through their platforms. With regard to social networks I have a personal belief that the companies providing these services very close to Government agencies. Social networks are the modern massive filing systems. They are a sign of the times, the individual tries to fill his empty existence with these tools.

4) Would you remember any specific Indian anecdote relating to hacking or security systems which shows how difficult it is to police the Net?

Honor to history! The milworm group, precursor of moder "hacktivists". It was responsible for penetrating the computers of the Bhabha Atomic Research Centre in Mumbai, the primary nuclear research facility of India, on June 3, 1998.

Returning to the present, every day dozens of cyber attacks are directed against Indian institutions and the suspect is on Pakistani and Chinese hackers. Another notable case was the virus Stuxnet. India was one of the main victims of the Stuxnet virus widely considered the first real cyber weapon.

5) What is the answer to regulating the internet given that questions of piracy and crimes like child pornography are very valid concerns?

There is no deterministic and sudden response. Network control is unquestionably necessary for reasons of national security. The real issue is who controls the controller? I remind the close relationship between the level of corruption and the adoption of monitoring systems. The censorship spectrum is just around the corner.

Coming back to be present day, and I think that the questions is about this, I am profoundly opposed to the SOPA. The bill is a threat to free online speech and carries a load of unacceptable exceptions to the rule of law.

Secrets at Risk in Cyber Space

By : Nidhi Rastogi

Cyber espionage is being used at a threatening speed to gain a competitive edge among Nations and States. Going by the reports from major market data analysis firms like Bloomberg and Gartner, opponents will continue to use this medium aggressively to attempt steal information related to defense, technology, and trade.

Why is it easier?

Industrial and economic espionage is not a new concept and has been in practice since ancient Greek and Indian civilizations. Technological advancements in the field of internet and information technology have made the world more connected than ever before. Most data today is stored in electronic form on computers, server, thumb drives and disks. Data, including the critical ones, now pass over networks which offer more opportunities for malicious actors to compromise the integrity and security of data. Earlier, a physical meeting was required for a foreign collector, increasing the chances of being caught. Add to this the logistics of transporting this information to the desired destination. In comparison to this, cyberspace makes it possible for foreign collectors to gather enormous quantities of information quickly and with rather less risk of detection by using Advanced Persistent Threat, or an insider downloading of proprietary information onto a pen drive at an opponent's behest.



What we saw in 2011

The year 2011 was a busier year for IT Security professionals' vis-à-vis the previous ones with respect to espionage. It was marked with a regular influx of attack vectors on firms, big and small. One of the biggest victims of large-scale cyberattack was Sony's PlayStation network comprising approximately 130 servers and 50 software programs. Hackers breached its network and gained access to the personal data, including credit card numbers, of millions of its customers in the month of April. In September, Duqu, arguably a Stuxnet variant, was discovered by a Hungarian research firm. In Symantec's words, it gathers intelligence data and assets from entities, such as industrial control system manufacturers, in order to more easily conduct a future attack against another third party.

In December 2011, a US Drone aircraft was forced landed by Iran Engineers. Iranian Security experts used the weakest point in the aircraft, the GPS navigation. They jammed the communications and forced the aircraft into autopilot. It is believed that Iran can reverse engineer the aircraft and mass produce similar drones.

Rik Ferguson, director of security research and communication at the security firm Trend Micro says, "I absolutely expect this trend to continue through 2012 and beyond". Adds Gerry Egan, director of security at Symantec, "It is quite possible that we will see another of these threats in the near future".

It gets worse as no measurable means exists to estimate a loss of this kind. Sometimes companies realize the existence of such threats only after the fact. It forces them into being reluctant to report the loss, fearing potential damage to their reputation with investors, customers, and employees.

Why is it hard to catch the thief?

Although there is a continued need of vigilance in protecting critical infrastructure, the picture isn't that bad. Countries like the U.S., U.K., Germany, China and India have established specialized teams and centers to defend government assets against cyber-attacks. However, determining who is behind Internet-based hostile operations with certainty is impossible most of the time.

Despite reports indicating intrusions originating from IP addresses in China, in several cases, it is difficult to put blame for these operations. Stealth is followed by using hackers as proxies, and routing operations through third world countries making it difficult to attribute responsibility for computer network intrusions. Several other countries are using US data stolen data from cyber-espionage operations to benefit domestic companies and gain competitive advantage, says a report by the US-China Economic and Security Review Commission.

How to protect?

Effective defense is possible by first identifying critical information and its value to the company and to the competitors. The storage for this data and the IP range of the location must have controlled access and security vulnerabilities must be identified on a regular basis. Special attention should be given to zero-day security holes. A security awareness program for company employees can help create a strong defense against several attack vectors. Honeypots, if used correctly, can also help counteract attempts at unauthorized access of the system.

In the wake of monetary losses and that of sensitive information, governments have finally begun to seek the capability to address cyber espionage. A National Cyber Counterintelligence Working Group led by FBI was established by the US government in 2011 with the objective of creating a coordinated response to the threat in cyber space.

Despite taking all the necessary steps and following best practices for protecting the network, it may still get compromised. This does not mean that one cannot put measures in place that make the company less likely to be a victim. Having a well-planned incident response plan can considerably reduce the extent of damage and timely equip the response team. There can never be a full-proof defense program but making a response plan is as important as cyber security.

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.

Why are information security incidents in the news?

By : Mariano M. del Río

Shortly into 2012 security incidents appeared on the cover of many newspapers and in specialized media. Also, the closure of Megaupload and discussions around copyright, privacy and freedom. All of this happened in less than 2 months. The source code theft of Symantec 6 years ago, hacks to Verisign in 2010 and in the last week the call between the FBI and Scotland Yard intercepted by Anonymous.... All make it sound like a science fiction movie, but it's reality and thus begins the new year.

This article is not intended to delve into each of the above cases, since there is so much information, but to open the discussion regarding why security incidents are in the news?

As you read about each case and get to know the information, usually they do not meet the "unprecedented attack" on the Sony Play Station Network last year.



But, there is something that is becoming a habit in organizations that are "victims" of the attacks and it has to do with the lack of communication about the impact of the incident, especially if they are involved with customer data. It is interesting that in most cases these companies have not taken advantage of the basic controls related to information security: weaknesses associated with patch management, lack of proper separation of environments, lack of implementation of principle of least privileges, network segmentation, no hardening in the devices, insecure coding applications, lack of security controls related to human resources, lack of protection against malicious code (lack of antivirus), no audit logs, use of generic accounts and more. With this picture, who needs to perform the "unprecedented attack?" Most companies make it easy for any kind of attack.

If anything could make the situation worse it is becoming a bad habit to hide the incident, but not only to customers (some already serious), but is becoming known in some cases that the incident is hidden inside the doors of the organization. Not even their governing boards know of the situations.

Can you imagine the executives of an organization outside of this situation? If this is information is hidden from the Board, how can the end user hope to be notified?

It is what is happening. Neglect to inform is happening everyday and now they not only hide the incidents to customers, but also to the Managers.

We have a chance to speak to those who should listen. Undoubtedly, it is the executives of the organizations as they are the most responsible, and although they hide the information, they are still responsible for what happens. They are responsible for hiring competent and responsible people, to keep them trained and give them the resources required to perform their work. If this does not happen it is likely that we will continue to hear daily about various information leaks, attacks and other variants.

On the other hand, users should begin to require security at the highest level. It is regrettable to see how personal data is supplied, your personal tastes and habits in a few GB of disk in the cloud or a premium account with a service of 2.0. Maybe just once users will choose a secure service over an insecure one. Executives will begin to give importance to security and everything will begin to spin, but until it happens, we can only hear as news security incidents.

About the Author :

Mariano M. del Río

Information Security Consultant

ISSA, OWASP, CSA Member

[Linkedin.com/mmdelrio](https://www.linkedin.com/in/mmdelrio)

@mmdelrio

Hacking News

Forget terrorists attacks here are 2012's Most Vulnerable Cities At Risk for Cyber Crime (Idiots) : <http://goo.gl/4VYGf>

Slum Dog India demands Real time monitoring on Indian Gmail & Yahoo Emails. Do they really have nothing better to do?
<http://goo.gl/iYO5H>

Iran will probably drop nuclear development cause they think they need to Develop their own security Software, No more foreign Solution, they might suggest banning the Burka too! : <http://goo.gl/QVheH>

Three Greek Anonymous hackers arrested for defacing Government Sites. They couldn't make the street protest! : <http://goo.gl/EyMux>

Facebook Hacking - Student jailed for eight months. They ought to jail Facebook for having such a stupid site : <http://goo.gl/PwkHt>

FAQ : DNSChanger Trojan, Impact and Solutions :
<http://goo.gl/IE2Qh>

How Hackers can Track your Mobile phone with a cheap setup ?
<http://goo.gl/YxyKK>

Anonymous does the work of angels and defaces National Consumer and Federal Trade Commission sites against #ACTA :
<http://goo.gl/H4Bc8>

Tor Bridge Relay to Bypass Internet Censorship : <http://goo.gl/PqVG8>

Dangerous IE browser vulnerabilities, Allows remote code execution !
<http://goo.gl/31n5N>

Anonymous Hackers take stock and target Nasdaq website
<http://goo.gl/XeNUz>

Hacking News

Anonymous shows a cyber army is better than any other and leaks 400 Mb Documents from US Army Intelligence Knowledge Network
<http://goo.gl/KL2L3>

Microsoft Store India got hacked in India ! : <http://goo.gl/87HUp>

"NASA Own3d Again" - NASA Database Leaked by rootworm
<http://goo.gl/skmUQ>

Cia.gov Tango Down - #FuckFBIFriday by Anonymous. Anonymous reports it was one of the best fucks they ever had! :
<http://goo.gl/dF7av>

Because Iran is sooooo very democratic they Shutdown Google ,Yahoo & other Major sites using Https Protocol : <http://goo.gl/H1Ntv>

Apple Supplier Foxconn's Servers Hacked, Exposing Vendor Usernames and Passwords : <http://goo.gl/fbkba>

Arab Countries websites urged to Increase Security Against Israeli Hackers and stop importing Challah bread : <http://goo.gl/ZozkE>

Cryptographers : Satellite phones vulnerable to eavesdropping
<http://goo.gl/2aB0S>

Anonymous Hack Syrian President's Emails with Password "12345" they knew that cause he can't count higher than that : <http://goo.gl/WBNFV>

YamaTough Hacker Demanded \$50,000 for not releasing Stolen Symantec Source Code. Other Anons likely to hack him if he doesn't share
<http://goo.gl/9XqD1>

Citigroup sites hit by Brazilian Anonymous hacker #OpWeeksPayment
<http://goo.gl/1NO32>

Hacking News

- # Anonymous Hacks FBI and Records Conference Call. Confirms FBI stands for Fools Bastards & Idiots : <http://goo.gl/ZGw4A>
- # NASA and Pentagon Hacker - TinKode Arrested in Romania
<http://goo.gl/KwoOL>
- # FBI will Monitor Social Media using Crawl Application. Since they can't crawl out of a paper bag we won't get too worried : <http://goo.gl/hiff8>
- # CBS Broadcasting Hacked by Anonymous Hackers for #OpMegaUpload
<http://goo.gl/wyb6m>
- # Brazil Under Anonymous Attack - Tangara da Serra city site defaced ! I guess they are mad we named a body waxing after them
<http://goo.gl/QNoGj>
- # Woohooo! After #SopaBlackout, Congress Postpones Action on #SOPA, #PIPA : <http://goo.gl/Oz4nR>
- # Tit for Tat - Anonymous Hackers Brings Down FBI website for #OpMegaupload. Apparently Anonymous loves a good you know what :
<http://goo.gl/nbhpT>
- # SOPA in US and Censorship in India: A cocktail to destroy Internet Freedom ! Idiots! : <http://goo.gl/OQQiC>
- # Cyber War : Another 7000 Israel credit cards Exposed on Internet. Apparently the hackers wanted to see where the good Hanukkah shopping was : <http://goo.gl/xHuX5>
- # Saudi hackers target Israeli stock exchange and National air carrier, mad because they didn't get a Hanukkah present : <http://goo.gl/6Ayz7>