I
nternational Workshop on Cyber
 Crime (IWCC 2013)
Date: 24 May, 2013
Location: San Francisco
http://stegano.net/IWCC2013/

Today’s world’s societies are becoming more and more dependent on open networks such as the Internet - where commercial activities, business transactions and government services are realized. This has led to the fast development of new cyber threats and numerous information security issues which are exploited by cyber criminals. The inability to provide trusted secure services in contemporary computer network technologies has a tremendous socio-economic impact on global enterprises as well as individuals. This poses new challenges for law enforcement policies and forces the computer societies to utilize digital forensics to combat the increasing number of cybercrimes. Forensic professionals must be fully prepared in order to be able to provide court admissible evidence. To make these goals achievable, forensic techniques should keep pace with new technologies.

McAfee warns of Project Blitzkrieg hack attack on http://www.theregister.co.uk/2012/12/15/mcafee_bank_attack_trojan/

Security firm McAfee warns that there is a credible threat of a coordinated Spring offensive against at least 30 US banks next year by Eastern European fraudsters. McAfee Labs, after studying the information posted and cross-referencing it with its own malware logs, suspects the threat may be real and more widespread than first thought, and Fidelity, E*Trade, Charles Schwab, PayPal, Citibank, Wachovia, Wells Fargo, Capital One, and others are at risk.

Aramco cyber attack targeted production http://www.it.com/www/com/1e/0/9233386-42da-11e2-aa4e- 071444203c.html#axzz2F9lt4ESi

Saudi Arabia has revealed that a cyber attack against its giant oil industry earlier this year aimed to stop crude oil and gas supplies, highlighting the devastating impact the virus could have had on global markets.

Dear Reader,

when you will receive this issue of the newsletter, 2012 will be already the past and a new year will have already started to roll down in front of you. Meanwhile in Europe is growing the consciousness of the need for new regulations for the Cloud World. Looking back we can say that in 2012 the word Security has been more than ever on the scene. Cyber hacktivist, hackers, multinational companies, governments all together on the stage of the cyber-security theatre. We have seen an increasing number of cyber attacks against civil critical infrastructures and against government infrastructures, the proliferation of malwares ad-hoc designed to spread across the mobile world and across industrial systems. On the other hand 2012 taught to everybody that cyber-threats cannot be faced alone. All around the world are ongoing multi-level discussions on the security of our infrastructures, on the need for new policies and new initiatives aiming at fostering a worldwide collaboration on the cyber-security matter. This will be the most ambitious objective for 2013: to bring effectively companies and governments together on the same table to put down the basis for a permanent collaboration among all the entities, to share information, practices and to be proactively able to protect collectively our life from the effects of cyber-threats. Here at GCSEC we strongly believe to this vision and we are working strenuously to see it realized in 2013.

Andrea Rigoni

“Android under attack” by Igor Nai Fovino - GCSEC

“Anonymous attacks Israel, hundreds of websites taken down and emails and passwords leaked” by Angelo Migliorisi - GCSEC

“The Google campaign for an open WEB” by Alessandra Lonardo - GCSEC

“The dark side of Internet” by Maria Luisa Papagni - Almaviva/GCSEC

“A look at Cyber Security in 2013” by Elena Agresti - GCSEC

“Follow footprints on virtual trails” by Marco Caselli - University of Twente, Enschede, The Netherlands
SAUDIARAMCO Starr Pocampiie and the world’s largest oil producer, initially said the attack had only affected desktop computers, but now the company has disclosed the real aim was to stop hydrocarbon production region.

Researchers at Kaspersky Lab said on Monday that the variant, called Mini-Flame, came from the same “cyber-weapon factory” responsible for other malware discovered this year, including the Flame and Gauss platforms, as well as the Stuxnet programme used against Iran’s nuclear facilities in 2010.

Smart TV hack highlights risk of ‘The Internet of Everything’

A smart TV is only as smart as the person controlling it. So if the person in control is a hacker, the owner could have a problem.

Researchers at security consultancy ReVuln say some smart TVs are vulnerable to hacking. It is another example of what experts say is the ever-expanding attack surface of devices that traditionally never faced the Internet, but are now “smart.”

The researchers at the Malta-based company said they found a vulnerability in a number of smart TVs made by Samsung Electronics that gave them root access to the TV and any attached USB drives. Luigi Auremma of ReVuln told the IDG News Service that hackers could even use the integrated webcam and microphone to watch the victim.

"The vulnerability affects multiple models and generations of the devices produced by this vendor, so not just a specific model as tested in our lab at ReVuln," the report said.

Samsung did not respond to a request for comment, but ReVuln emailed a statement saying there is no firmware update yet, “as the details regarding this vulnerability have not been shared with the vendor.”

Security budgets again expected to rise next year

Despite a shaky economy, nearly half of surveyed IT professionals in North America saw increased security budgets this year and expect the growth to continue into the next.\n\nTheInfoPro "Information Security Study," to be released on Friday, showed that 45 percent of respondents increased their budget for security projects and personnel between 2011 and 2012.

Mobile device management is a top priority in spending next year and security projects expected to command a top investment of HK$9m in cyber security projects and personnel between 2011 and 2012.

A smart TV is only as smart as the person controlling it. So if the person in control is a hacker, the owner could have a problem.

Hong Kong Police invests HK$9M in cyber security center

The Hong Kong Police recently launched the Cyber Security Center to provide round-the-clock services, with an investment of HK$9 million in hardware and software for the new facility.

27 police officers will work in the center, which is expected to strengthen the coordination between Police, government departments, as well as both local and overseas stakeholders when major information systems come under attack.

According to Police numbers, there were 761

Since mid ‘90, analysts started to predict the rising of a new generation of malwares conceived to target mobile phones. Luckily, until 3-4 years ago those predictions seemed to be completely wrong. With the exception of the old SymbOS, cabir and SymbOS.comwarrior few other malicious codes for mobile applications gained the first pages of the newspapers.

The reason is that for long time hackers were not really interested in developing mobile-phone malwares for mainly three reasons:

1. Use of closed operating systems, making difficult to obtain the information needed to forge a working malware for a certain platform
2. Huge variety of proprietary OS, which would require to a malware, to be successful, to be multi-platform
3. Too little economic advantages, which at the end limits the amount of efforts an hacker would be interested in investing to create a malware for mobile phones

In the last years however, these barriers between our phones and the bad guys slowly disappeared. The entrance on the scene of Android, a truly open platform OS for mobile phones, gave to hackers a free aquarium to start breeding new, advanced malwares.

The planetary success of Android as the most used OS for mobile phones, gave to the same hackers the access to an entire sea to release the content of their aquariaums.

Last, but not least, the connection of smartphones with the Net, and the possibility to use them as payment terminals, social network interfaces etc. provided the economic motivation for criminals to invest in the development of these new malwares.

But which kinds of attacks are typically performed through the use of smartphone malwares?

Spyware is the most obvious answer. This class of malware is today able to record sms, calls, passwords, web sites visited and even your geographical position (through the gps chip integrated into the smartphone). Android, tapsnake is an example of this type of applications.

Pay per click, pay per download or pay per Install malwares are other aspects of the potential “market” open to smartphone hackers. In the case of pay-per-download for example, the potential damage to the end user can be huge,
especially when exists an agreement between the phone carrier and a content provider (for example an Internet TV). In that case the end user without knowing will find on its monthly bill charges for contents not really downloaded. An example of this kind of malwares is Android.Bgserv.

Ntan (transaction authentication number) Stealing is instead a class of attacks/malware related to the use of smartphones as verification device in back transactions and payments. Android.Smssniffer is a clear example of malware designed also to perform this type of attack.

After this last, and obviously not exhaustive classification of mobile malware threats, it is evident to the reader that Android is far from being considered secure.

According to the 2013 Mobile Threat Predictions report of Lookout, between the beginning of 2012 and the end of 2013, 18.4 million Android users will be infected with malware.

The prediction does not take into consideration the foreseen increasing rate of Android activations, i.e. the study is, most-probably, under-estimating the total amount of infected Android users by the end of 2013. Nevertheless the figure is scary if you consider that this number represents the 1% of the total number of Android based devices.

According to Kaspersky Labs, the volume of new malware targeting Android devices tripled in the second quarter of 2012. Half of the malicious files classified in the last three months were Trojans programmed to steal data from smartphones; 1/4 of the malwares were SMS Trojans and the 18% were able to give the full control of the device to the attacker.

What is incredible in that apparently the history is repeating itself: the same problems we encountered in the PC Era are now affecting us in the smartphone Era, but with even heavier damages if you consider that smartphone (or their evolution) will become a sort of extension of our bodies, allowing us to be always connected to the Internet and to perform a huge variety of unbelievable (at list until 4-5 years ago) operations.

The decision of Google to include in Android 4.2 a malware scanner is a good starting point that however is not sufficient, by itself, to guarantee full protection of the end users.

As the history should have tough us, technology is efficient in protecting ourselves, only if we are the first shield against the cyber-threats, and then when using your smartphone:

- Keep network connectivity such as NFC / WiFi, or Bluetooth active only if needed (you’ll also safe some battery life :-) )
- Always Update your phone and apps
- Be careful about app permissions
- Always check the real urls you’re surfing on with your mobile
- Check regularly your phone bill
- Install a security app (and regularly update it)

Ah, one last thing: in this article Android was the star under judgment, however either you are using Apple iOS or Win8, you should be equally cautious.
Anonymous attacks Israel: websites taken down, passwords leaked.

by Angelo Migliorisi - GCSEC

Anonymous followed up with its threat of attacking Israel for taking military action in the Gaza strip. They’ve knocked down hundreds of websites including sites devoted to trade, immigration, and the office of the president, they have deleted databases and have leaked e-mail addresses and passwords.

The targets taken down include the Israel Ministry of Foreign Affairs database and Bank of Jerusalem database, which have both been deleted. On top of that, Anonymous also took down with DDoS attacks over 600 governmental, retail, and businesses sites -- some belonging to the automotive and fashion industries and pasted over 2000 email addresses and passwords.

The bank of Jerusalem, one of Israel’s largest financial institutions, has received particular attention from the hacktivists -- as the cyberattackers crowded over their achievement in deleting the organisation’s online database through social network Twitter. Trying to access the bank’s website resulted in nothing more than a database error. Now The Jerusalem bank’s database has been restored. Website of Israel’s Ministry of Foreign Affairs also appears to have been attacked and its database either deleted or tampered with. According to the latest list, 663 sites have been affected.

Beyond “denial of service” tactics that blocked sites with floods of junk data, the hackers also ramped up their attacks to penetrations of any vulnerable target available to them, resulting in tens of thousands of Israeli citizens’ and supporters’ private data dumped onto the Web. Some of the file dumps contain the full names, email addresses and passwords of website users, stolen from breached databases.

The group claimed was the personal data of 5,000 Israeli government officials. In fact, the hacked data was actually a much larger collection of 35,000 names, phone numbers, addresses and emails of Israeli citizens, taken from an unknown origin and posted to a collection of compromised domains by a hacker using the pseudonym “Gaza Hacher.”

Another 3,000 email addresses, phone numbers and addresses of those Anonymous described as “Israeli supporters” - donors for the Unity Coalition for Israel, which claims to represent “the largest network of pro-Israel groups in the world.” The document appears to be quite old: one of the military e-mail addresses belonged to U.S. undersecretary for defense under Bush, who left that job in 2005.

And several thousand more users’ email addresses and other personal data were taken from seemingly random Israeli targets like the real estate website Dirot Modii, Connections Magazine and the mailing list of what another Anonymous release described as the “Israel Coalition”.

A second document, allegedly also extracted from the coalition, appears to be an e-mail announcement list. It includes e-mail addresses from officials in the White House, Senate, and the State Department's Bureau of Diplomatic Security, as well as many news organizations.
A press release from Anonymous says that when the government of Israel publicly threatened to sever all Internet and other telecommunications into and out of Gaza, "they crossed a line in the sand." The statement continues: "As the former dictator of Egypt Mubarak learned the hard way — we are ANONYMOUS and NO ONE shuts down the Internet on our watch." Anonymous finished with a stark warning to government if it persists in trying to cut telecom and web links. In addition, the collective said that unless attacks cease, the Israeli government "will know the full and unbridled wrath of Anonymous. And like all the other evil governments that have faced our rage, you will NOT survive it unscathed."

In a move that separates this from other campaigns, the hacktivists have put together a downloadable "care package" for residents of Gaza in the scenario that the Israeli government's promises come true and Internet connections are severed. It contains useful information on evading Israeli Defense Force (IDF) surveillance as well as basic first aid data. In addition, Anonymous wants to make clear that it is not a "terrorist organization", by stating that the hacker's mission is to "protect the rights of Palestinian people who are threatened with silence. [...] We know what happens to victims of oppression when the lights go dark."

On the other side, the Israeli Defense Force (IDF) has begun a campaign of its own - a game called IDF Ranks which rewards frequent visitors and to its blog and content sharers with different badges and virtual military ranks. The website says this is to fight "misinformation" concerning the IDF and Israel.

Anonymous' attacks, of course, hardly register compared with the physical damage inflicted by both sides in the Gaza conflict. But the mass-hacking of Israeli targets has at least got the attention of the country's authorities.

Israeli Finance Minister Yuval Steinitz said that the attacks had opened a "second front" in the Gaza fighting, claiming that the government had "deflected 44 million cyber attacks on government websites." But Steinitz said that the government remained nonplussed by the horde of hackers, and claimed that only one of the targeted websites went down for "six or seven minutes."

"This is an unprecedented attack, and our success has been greater than we anticipated," Steinitz said. With many more than that one site downed or breached by Anonymous' just a day after his comments, Steinitz may now be wondering just how much more "unprecedented" the hackers' attacks will become.

So, Anonymous did what it does best: swore vengeance against a superpower. Anonymous has never been a well-run organization, that's what used to make it so dangerous: no organization but thousands and thousands working for the cause. Emerging from this was LulzSec, an elite and independent Delta Force of Anons, commanding respect among sympathizers and fear among corporations. They got big things done, like embarrassing major credit cards, dumping gigantic data leaks like clockwork, and even knocking down the CIA's website. And then they went to prison.

In the end, this attack did not have incredible results, if this were a hacker collective under any other name, we'd hardly take notice. But they did successfully in getting attention from authorities and gaining their titles on worldwide press.

“The Google campaign for an open WEB.”

by Alessandra Lonardo - GCSEC

On the occasion of the World Conference on International Telecommunications 2012 (WCIT-12), organized by the International Telecommunication Union (ITU), that took place in Dubai early December, Google has set up a “take action” campaign, with the slogan “A free and open world depends on a free and open web”.

The meeting in Dubai aims to bring together regulators from 193 countries from all over world to re-negotiate the International Telecommunication Regulations treaty, signed in Geneva in 1989.

Google states that not all governments support the free and open Internet and that 42 countries filter and censor Internet content, moreover it adds that some of these governments are trying to use a closed-door meeting to regulate the Internet, without any involvement of citizens and stakeholders.

Recently, a few countries adopted 19 new laws that, according to Google, threaten free expression online: some of the proposed amendments to the Treaty might increase censorship and threaten innovation, allowing governments to censor legitimate speech or even to cut off Internet access; other proposals could result in toll payments by services like YouTube, Facebook, Skype, to reach people across borders, thus limiting access to information, especially in emerging markets.

“Internet policy should work like the Internet — open and inclusive”, suggests Google. Besides Governments, the billions of web users and the technicians working to make the Internet accessible and operational should also be involved in the process of implementation of the policy.

The most significant positions regarding this matter, have been taken by the Russia, China and United States. Russia and China and a few Arab countries are forwarding the cause of a stricter National Government Control over the Governance of the Internet, leaving less room for maneuver to private organizations, as is the case in the United States through ICAAN (U.S. based Internet Corporation for Assigned Names and Numbers).

As of today the petition has been signed by more than three million people from all over the world.
As the name suggests, Darknet is the hidden part of the Internet, for years the haven for all those seeking refuge from the prying eyes of authorities. Yes, because the anonymity plays a key role in the Darknet and is one of the main reasons why cyber criminals get involved.

A darknet is a virtual private network where users connect only with people they trust. In its more general meaning, a darknet can be any kind of closed group of persons who communicate, but the name is most often used specifically for networks of file sharing. The term was originally coined in the seventies to designate networks that were isolated from ARPANET (the old Internet) for security reasons. In general, darknets have some key features:

- They are distributed through peer-to-peer;
- They use the Internet infrastructure for their traffic;
- They use non-standard protocols and ports.

Of course, not all systems that satisfy these conditions can be defined Darknet. Skype, for example, is a closed network, with its ports and its protocols, each client only communicates with other Skype clients, it has peer-to-peer file sharing capabilities, but it cannot be classified as a darknet!

To catch what characterizes a darknet, and the security aspects related to it, is essential understanding its infrastructure and operation.

One of the most famous darknet is Tor (The Onion Router). It was born for military purposes, but now is used by activists, terrorists, anarchists, revolutionaries, journalists, police, government organizations and much more. The Tor network is based on a set of nodes, called "reley", consisting of intermediate servers through which pass data before arriving at destination. These nodes can be made from our own computer connected to the Tor network and functioning as a server. Our data, before getting to the required website server, randomly pass on these nodes and always use a different path. The network is structured in such a way as to automatically modify the path of our data every ten minutes. After that, our data are run through a different circuit. The complexity of these paths is the reason because the data transfer is slower than the regular Internet.

The following picture shows Tor network functioning:

The red links indicates that data are encrypted, the terminals with a red cross are the nodes of the Tor network. Tor only works for TCP streams and applications that support the SOCKS protocol. It follows that the websites do not understand where to receive the request. For increased security, all data exchanged between the server are encrypted in a way that cannot be read. Unencrypted data (the green link on the figure) are exchanged only from the last node to the destination server to ask for the file.

This is only an oversimplified description of a darknet infrastructure. In fact, Tor is just one of the many darknets that can be found on Internet, brought to light one year ago when Anonymous took down child porn site on its network.

There are many other famous hidden network, as Freenet (which lets you anonymously share files, browse and publish "freesites", web sites accessible only through Freenet, and chat on forums, without fear of censorship) or I2P (anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate).

Obviously you cannot find these networks only typing "darknet" on Google. Conventional search engines are not useful for this purpose. There are, however, of the large link lists, accessible on specific sites, on which there are thousands of links, each of which returns to contents present on a computer of the Darknet. Here you may find everything from music, movies and software, all illegal material. According to experts, the amount of data available on Darknet is huge: an estimated amount of 500 times higher than the one on the "normal" Internet.

But not only the infrastructure distinguishes darknets from standard canons of Internet, also the ways of access to them is different. Getting started is easy: all you need is special software to be installed on the operating system and integrates with the browser and does not require too elaborate settings. The program is essential to encrypt the data stream. Each darknet can use its own client software and encryption algorithms. In many cases, cybercriminals use SSH tunnels to maintain encrypted traffic and will hack the servers of other clients to use their storage capacity. Some groups of criminals also use tool as PGP and even if the encryption systems used are usually not as strong, they're good enough and have the benefit of fast key generation. Furthermore, the complex routing system makes it difficult to trace communications.
As said by the computer security expert Anshul Abhang:\(^2\): “Many government policies and laws, including information technology (guidelines) Intermediaries Rules, 2011, speak of the central and state monitoring of the communication that takes place on the Internet. Normal telephone and data communication in an open network (WhiteNet) can be monitored as such a network involves no encoding. Instead, darknet are networks that are encrypted by anonymous users whose identity is not known. Thus, the difficulty in deciphering data passing through these networks. If whitenets, some companies, such as banks, will bring encryption to protect sensitive information. Encryption This, however, can be stopped as a result of the law-enforcing agencies after having procured the appropriate permissions.

On the other hand, criminals and underground communities have their own networks that are encrypted to obscure them. Such networks cannot be intercepted by any agency, governmental or private, as there are several controllers anonymous involved in cryptography”

“Through participation in the global criminal forums,” says Eli Jellenç, who manages the international cyber-intelligence team at iDefense. “These forums attract a lot of beginners and the lower echelons of the cybercrime world, he says.

They're also the hangout of many criminal groups in Eastern Europe and Asia because the forums provide easy business opportunities and they have reason to believe there's very little chance of them getting caught. Law enforcement can get a foothold in these forums. Once they've built trust, they can get access to the shade, more sophisticated groups”.

It seems clear that most people use Darknet because is interested to anonymity. So come immediately to mind those who want to exchange information regarding stolen credit card details, drugs, pornography, piracy and much more.

However, you cannot think that Darknet has only a negative meaning. In times of oppressive regimes of the government, are a channel for the freedom of speech. Think, for example, at when the Mubarak regime decided to block access to Internet in Egypt. The dissidents have used Tor darknet to maintain communications with the rest of the world. So Darknet is just a technology, use an encrypted network or a proxy is not illegal… the use you do of it makes the difference!

“Through participation in the global criminal forums,” says Eli Jellenç, who manages the international cyber-intelligence team at iDefense. “These forums attract a lot of beginners and the lower echelons of the cybercrime world, he says.

They're also the hangout of many criminal groups in Eastern Europe and Asia because the forums provide easy business opportunities and they have reason to believe there's very little chance of them getting caught. Law enforcement can get a foothold in these forums. Once they've built trust, they can get access to the shade, more sophisticated groups”.

It seems clear that most people use Darknet because is interested to anonymity. So come immediately to mind those who want to exchange information regarding stolen credit card details, drugs, pornography, piracy and much more.

As said by the computer security expert Anshul Abhang\(^2\): “Many government policies and laws, including information technology (guidelines) Intermediaries Rules, 2011, speak of the central and state monitoring of the communication that takes place on the Internet. Normal telephone and data communication in an open network (WhiteNet) can be monitored as such a network involves no encoding. Instead, darknet are networks that are encrypted by anonymous users whose identity is not known. Thus, the difficulty in deciphering data passing through these networks. If whitenets, some companies, such as banks, will bring encryption to protect sensitive information. Encryption This, however, can be stopped as a result of the law-enforcing agencies after having procured the appropriate permissions.

On the other hand, criminals and underground communities have their own networks that are encrypted to obscure them. Such networks cannot be intercepted by any agency, governmental or private, as there are several controllers anonymous involved in cryptography”

“Through participation in the global criminal forums,” says Eli Jellenç, who manages the international cyber-intelligence team at iDefense. “These forums attract a lot of beginners and the lower echelons of the cybercrime world, he says.

They're also the hangout of many criminal groups in Eastern Europe and Asia because the forums provide easy business opportunities and they have reason to believe there's very little chance of them getting caught. Law enforcement can get a foothold in these forums. Once they've built trust, they can get access to the shade, more sophisticated groups”.

It seems clear that most people use Darknet because is interested to anonymity. So come immediately to mind those who want to exchange information regarding stolen credit card details, drugs, pornography, piracy and much more.

However, you cannot think that Darknet has only a negative meaning. In times of oppressive regimes of the government, are a channel for the freedom of speech. Think, for example, at when the Mubarak regime decided to block access to Internet in Egypt. The dissidents have used Tor darknet to maintain communications with the rest of the world. So Darknet is just a technology, use an encrypted network or a proxy is not illegal… the use you do of it makes the difference!

"A look at Cyber Security in 2013.”

by Elena Agresti - GCSEC

We are in the first days of the 2013, year 2012 is the past, so it is the time to look back.. What cyber security challenges have been addressed in 2012? What can we learn and what can we improve?

The 2012 year has been characterized by sophisticated attacks against specific targets, in most cases critical infrastructures or government installations; protest attacks of Anonymous, password and username leaks, hacktivist actions have been under the lights of the scene. As consequence, we have seen major government efforts and interest in cyber security, new national ad international legislation development and activities on cyber security.

In this year, critical infrastructures have been subjected to new attacks such as Gauss, Flame, Mahdi and Shamoon. These new attacks were complex and required highly skilled people and extensive resources. They targeted specific objectives and Middle East has been almost always the epicentre of the infection.

Flame was a sophisticated cyber espionage tool specifically designed for industrial systems that has infected approximately 1,000 machines; Mahdi a cyber espionage malware that infected computers in Iran, Israel, and other Middle Eastern countries. Flame infection reported in Israel, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt while Saudi Aramco and Qatar RasGas were victims of Shamoon. In the case of Shamoon, cyber security experts, however, believed that a state was behind the attack, an accusation now repeated by Saudi officials.

These weren't the only attacks that involved a government in 2012. Iranian hackers have attacked U.S. banks for all year. U.S. officials said the attacks against banks, and other attacks against Middle Eastern energy companies, were sponsored by the Iranian government and approved at high levels as part of a cyber war.

Chinese government has been suspected of espionage activities carried out through Huawei Technologies Co. Ltd. and ZTE Corporation, two Chinese companies that are two of the global providers of telecommunications equipment and mobile phones. The US House Intelligence Committee has not revealed evidences to confirm espionage activities but in its report is explicitly recommended to U.S. government to exclude Huawei or ZTE components.

Attacks that involve governments have been also performed Anonymous. Anonymous claimed responsibility for disrupting the access to UK government websites, including the Home Office, Ministry of Justice and Number 10 Downing Street sites.

In 2012 Anonymous continued its protest attacks. We can remember the attack to the website of the California Statewide Law Enforcement Association to protest police brutality, the attacks against the websites of UMG, the United States Department of Justice, the United States Copyright Office, the Federal Bureau of Investigation, the MPAA, Warner Brothers Music, the RIAA, and the HADOPI protesting against shut down of

\(^1\) http://articles.timesofindia.indiatimes.com/2011-10-20/pune/30301961_1_networks-cyber-criminals-encryption

\(^2\) http://www.webvivant.com/feature-darknets.html
the file sharing service Megaupload or against European government website protesting for ACTA agreement.

In April 2012, Anonymous hacked 485 Chinese government websites, some more than once, to protest the lack of democracy and carried out other attacks such as against Boston Office Department, Syrian Government, Interpol and Quebec government.

The 2012 will be also remembered as the year of password and username leaks. Twitter, LinkedIn, Yahoo, Gmail, Hotmail passwords were leaked. In many cases, baseline security measures, such as salting or hashing, have not been implemented. Hackers have stolen $90,000 in bitcoins to Bitcoinica. The information, stored in the database violated, were usernames, email addresses and account histories. Probably the theft was carries out using account information stolen.

With the growth of cyber attacks against governments and critical infrastructures, Governments become more aware of the risks to which they are exposed and have begun to dedicate more effort to cyber security. At national ad international level, legislations in cyber security has been developed or proposed.

The European Commission has proposed a major reform of the EU legal framework on the protection of personal data [(COM(2012) 11] and a legal framework on electronic identification and trust services for electronic transactions in the internal market [COM(2012)/238]. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market. The Commission has also launched large consultations on the matter of cyber security such as on a future EU Network and Information Security legislative initiative, on cyber security, privacy and trust related Research and Development, or on security of e-payments.

In U.S. the first months of 2012, Obama Administration cyber security coordinator Howard Schmidt set an agency-wide goal for agencies to implement priorities to help protecting federal IT systems against cyber attacks. The Obama administration has also revealed new initiatives to combat botnets, one of the greatest threats to the integrity of the Internet. In U.S. has been developed the “Cybersecurity Act of 2012”, the most significant legislative undertaking on cyber security issues in the United States to date, but it failed to pass the U.S. Senate.

The 2012 has also seen large educational and awareness campaigns on cyber security. ENISA developed a large scale pilot project of collaborative awareness raising for EU citizens & SMEs and President Obama has designated October 2012 as National Cyber Security Awareness Month (NCSAM) to engage and educate public and private sector partners about cyber security and to increase the resiliency of the nation in the event of a cyber incident.

We are facing relevant issues on cyber security. Increasingly targeted attacks on critical infrastructure, occurred in 2012 and, in general, in the last years, allow us to imagine that they will become increasingly more and more sophisticated and targeted.

The protection of critical infrastructure will be a high priority in the next years. Infrastructures, before considered secure, are now exposed to new vulnerabilities and need to be adequately protected.

Evolution of digital world, will make digital identities increasingly subjected of attacks, and for that reason the definition of a management framework and the implementation of security measures are needed. Governments should define their cyber security strategies, define national cyber security plans, continue to engage private sector, educate and aware public and private sector on cyber security to build a stronger cyber ecosystem.

“Follow footprints on virtual trails.”

by Marco Caselli – University of Twente, Enschede, The Netherland

Let us imagine the Internet as an immense snow-clad expanse. Web users move in every direction visiting several web sites as people go house by house walking in the snow the distance that separates the buildings. In real life, we are not able to cross this stretch without leaving traces on the ground and, in the virtual world, computers leave clues of their passage as well. Each print has its own characteristics and an Internet detective will use it to his advantage, finding out "who has visited what" before the snow melts and the trail disappears.

Computer Fingerprinting, such as the process of recognition of hardware and software components by looking at specific "traces", is a well known and studied activity of the computer science. While the research community is trying to improve more and more the
accuracy of such process on the other side, hackers and crackers, always discover new ways to hide their presence.

We are not yet talking of recognizing the person behind the computer. The fingerprinting is interested in outlining operating system’s characteristics and applications. However, this is usually a first step toward any other kind of investigation or, in some cases, also toward malicious activities. For example, the fingerprinting is often used inside comprehensive testing methodologies. This is the case of network administrators that perform vulnerability assessments and penetration tests. In fact, during these activities, they often need to acquire some knowledge of the system under control and, for this reason, they exploit fingerprinting tools. In a similar way but with a different purpose, hackers and crackers attempting to access unknown networks always target their preys using fingerprinting. This is usually done in preparation to an attack against the weakest host discovered.

There are several fingerprinting methodologies. Any of them can rely on one or several sources of information. Network packets' usually contain the most valuable data. Many fingerprinting tools work by analyzing those packets in order to extract the so called "fingerprint" of the operating system running in the sending machine.

But, what are the information used to build such fingerprint? Well, most of the Web communications use today standard protocols. Two important examples are: the IP (Internet Protocol) and the TCP (Transfer Control Protocol). The first is the backbone of the Internet and allows to link heterogeneous networks together, the second is responsible for reliable communications. Protocols' specifications are not always strict and, for this reason, their implementations slightly differ from operating system to operating system. These differences are what the fingerprinting tool is looking for. In a simplistic way, suppose that a particular implementation of the Internet Protocol exploits some specific bits of the IP packet’s header. Suppose also that only Windows uses such feature. When a fingerprinting tool eavesdrops messages that use those bits it will automatically trigger an alert. The alert will notify that the machine sending those packets runs Microsoft's software since no one else uses that implementation of the Internet Protocol.

In the real world, differences are not so marked but the principle is always the same: finding unique characteristics in the inside operating systems' communication protocols. However, there are two main problems that fingerprinting have to face. First of all, the information owned by a fingerprinting tool is always limited. Each tool has a finite set of known fingerprints, called signatures, and these are the only ones it is capable to recognize. If a different combination of characteristics is recorded during the analysis, the tool will trigger an alert saying that the captured fingerprint is unknown. In these cases, some more advanced applications do statistical analysis trying to understand what kind of operating system can generate such fingerprint, but the result is usually unreliable. The second aspect that makes fingerprinting very difficult relies on the temporary validity of a signature. When an operating system installs an updated there is no certainty that its fingerprint remains the same. Because of that, fingerprinting tools’ datasets have to be always checked and updated.

These difficulties are, of course, exploited by those who do not intend to leave traces behind. There are a few tricks that hackers use to be invisible in the Internet and crackers use to access private systems without being captured. Software called “scrubbers” running on personal computers allow them to confuse the traces by modifying several characteristics of the fingerprints they leave. This makes such traces indistinguishable with each other and, therefore, useless. Moreover, the use of Proxy servers or applications like Tor allow to hide fingerprints behind new and totally fake ones.

Despite these tools, deleting all the traces of a network break-in without any possibility of being followed seems still impossible. Internet detectives have learned to patiently analyze the track and to do not neglect any detail. The investigation will continue until someone invents a method to completely melt the snow where these footprints are imprinted.