Dear Reader,
On October 5th I joined COMDEF 2012 in Washington DC, where I had the honor to speak together with representatives of US and Canada DoD and discuss about the role of Defense in security National Cyber space, including private sector.

We agreed that in Cyber Space we need something similar to the wall hydrants you see outside buildings: that is a privately owned infrastructure, built following national standards to allow a public body, as the Fire Department, to intervene to extinguish a fire in the building.

We do not have the same in Cyber Space. Real life demonstrates that in case of an attack, providing support to an organization without any preparation is useless.

The market already developed models similar to the wall hydrants: Managed Security Service provider in order to deliver their services set up an infrastructure to share data in real time and processes and procedures to notify attacks and suspicious activities as to support incident response. Such models could be standardized and used when Government strategy is to support Private Sector in case of cyber attacks.

Could this be the role of a National CERT? Majority of National CERTs are more oriented to provide early warning and security bulletins. There is the need for a new generation National CERT!

Andrea Rigoni

---

**Cyber Security is our mission**

---

### editorial

Dear Reader,
On October 5th I joined COMDEF 2012 in Washington DC, where I had the honor to speak together with representatives of US and Canada DoD and discuss about the role of Defense in security National Cyber space, including private sector.

We agreed that in Cyber Space we need something similar to the wall hydrants you see outside buildings: that is a privately owned infrastructure, built following national standards to allow a public body, as the Fire Department, to intervene to extinguish a fire in the building.

We do not have the same in Cyber Space. Real life demonstrates that in case of an attack, providing support to an organization without any preparation is useless.

The market already developed models similar to the wall hydrants: Managed Security Service provider in order to deliver their services set up an infrastructure to share data in real time and processes and procedures to notify attacks and suspicious activities as to support incident response. Such models could be standardized and used when Government strategy is to support Private Sector in case of cyber attacks.

Could this be the role of a National CERT? Majority of National CERTs are more oriented to provide early warning and security bulletins. There is the need for a new generation National CERT!

Andrea Rigoni

---

### in this number

**"Why is so hard to protect industrial plants from malwares?"**
*by Igor Nai Fovino – GCSEC*

**"Shamoon, another son of Stuxnet?"**
*by Maria Luisa Papagni – Almaviva/GCSEC*

**"Report from World Smart Week in Nice"**
*by Massimo Cappelli – GCSEC*

**"The Cloud bumps into critical infrastructures"**
*by Emiliano Casalicchio, University of Tor Vergata/GCSEC*

**"Flame: report of a malware"**
*by Marco Caselli - University of Twente, Enschede, The Netherland*

---

### events

**The Grand Conference**
*Date: 16 October, 2012*
*Location: Amsterdam, The Netherlands*
*https://www.thegrandconference.org/*

The Grand Conference is an outreach of the EU-US Joint Working Group on Cyber Security and Cyber Crime organized by CPNI.NL and supported by the European Commission, European Network of Information Security Agency (ENISA), US Department of Homeland Security (DHS), World Economic Forum (WEF), Alliander, TNO, European Network voor Cyber Security (ENCS), Global Cyber Security Center (GCSEC) and Deloitte.

The Grand Conference will contribute to the next World Economic Forum Summit, by providing insights and inspiration on the specific challenges and opportunities of cyber resilience of Industrial Control Systems and Smart Grids in a hyperconnected world.

Leading CEO’s will sign a manifest to shape that guidance. And last but not least Neelie Kroes, Vice President of the European Commission, will present her view on cyber security in Europe.

**Cyber Defence Forum**
*Date: 23 - 25 October, 2012*
*Location: Prague*
*http://www.cyberdefenceforum.com/Event.asp?id=770998*

As part of Defence IQ’s Cyber Defence conference series, the new Cyber Defence Forum is being launched to provide an enhanced opportunity for interactive debate and discussion on key cyber issues. This event will run as a series of panel discussions and round tables, to share knowledge is increased further still. The Cyber Defence Forum will focus specifically on the challenges, operations and solutions facing armed forces and governments as they formulate national strategies in-line with the international community.

**Cyber Security Summit 2012**
*Date: 6 November, 2012*
*Location: London*
*http://cybersecuritysummit.co.uk/*

The Cyber Security Summit 2012 is this year’s leading forum for policy makers, practitioners and industry stakeholders to debate the future for cyber security. Event will explain the implementation and development of the Cyber Security Strategy.
Once upon a time... It was the 1949 when Von Neumann defined the Theory of Self-Reproducing Automata, where he presented for the first time the possibility of developing small replicating programs able to control other programs with a similar structure.

Even if this feature has been adopted in the last sixty years to perform a huge amount of different applications, it comes immediately in mind the most malicious of its deployments: Malwares.

In 1959 Robert Morris, Douglas McIlroy and Victor Vysotsky created a computer game, called CodeWar, based on the theory of Von Neumann and in which computer programs fought between the others, trying to "conquer" as much computer resources as possible... and it is not a case that the son of Robert Morris, create in 1972 what is considered the first computer virus, Creeper, able to infect IBM 360 on the ARPANET. To eradicate it, a virus called Reaper was created to seek and destroy Creeper. This is the true origin of today's antivirus programs.

From that point on, the cyber world has seen a never-ending evolution of malwares and antiviruses. Brain, Jerusalem, MichaelAngelo, Melissa, Code-Red, Slammer, are only few of the millions of malwares developed and spread around the cyber-world every year.

In parallel with the evolution of malwares also anti-viruses evolved, passing from traditional signature based analyzers to heuristic systems, to anti-viruses embedding emulation software allowing to predict the behavior of a suspicious code before its running into a real system.

While it is not possible to claim that modern anti-viruses are able to detect every kind of malware (especially zero-day viruses), it is also true that the correct use of these "security shields" can guarantee a high level of protection to general purpose ICT systems.

However, in the last two years (since the appearance of Stuxnet), there has been a big discussion about the cyber-security of critical industrial systems, about their vulnerability and the risks to which these installations are exposed.

Industrial companies started to invest huge amount of money in cyber-security, but, apparently, the results in term of increased level of protection does not follows the investment figure.

The question is "Why it is so hard to protect Industrial Plants from Malwares?".

The answer is quite complex and is orthogonal to almost all the organizational levels of a company owning an industrial plant.

One of the first reasons is Obsolescence: traditionally industrial systems are designed to operate for decades. It is not rare to find very old operating systems and control software on place. It is, of course, a situation mainly due to the need of maintaining the compatibility with the protocols and the devices used in the plant. In several situations, the substitution of an obsolete system would imply a huge investment in order to modernize not only that system but also all the devices controlled by it. Direct implications of that situation is the fact that those systems might be prone to vulnerabilities that in the traditional ICT world have been eradicated years ago.

Problematic Patching is another of the reasons for which it's hard to protect industrial systems. When a new vulnerability is discovered, software companies release patches to fix the problem. Unfortunately, with few exceptions, the patching operation is quite invasive. In the best situation, a system reboot might be required, while in the worst case the installed patch can interfere with the pre-existing software controlling the industrial installation. For that reason the patching speed in the industrial context is extremely slow, enlarging, in this way, the exposure window of a plant.

and the further measures being undertaken internationally to protect cyber space and promote economic prosperity.

Internet Governance Forum Meeting 2012
Date: 6-9 November, 2012
Location: Baku, Azerbaijan
http://www.intgovforum.org
The Seventh Annual IGF Meeting will be held in Baku, Azerbaijan from 6-9 November 2012. The proposed main theme for the meeting is: ‘Internet Governance for Sustainable Human, Economic and Social Development’.

The Internet Governance Forum (IGF), run by the IGF Secretariat, has the purpose is to support the United Nations Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) with regard to convening a new forum for multi-stakeholder policy dialogue.

news

Iran blamed for cyberattacks on U.S. banks and companies
http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-8730c76312_story.html

Iran recently has mounted a series of disruptive computer attacks against major U.S. banks and other companies in apparent retaliation for Western economic sanctions aimed at halting its nuclear program, according to U.S. intelligence and other officials.

In particular, assaults this week on the Web sites of JP Morgan Chase and Bank of America probably were carried out by Iran, Sen. Joseph I. Lieberman (I-Conn.), chairman of the Homeland Security and Governmental Affairs Committee, said Friday.

All you need to know about nano SIMs - before they are EXTERMINATED
http://www.reghardware.com/2012/09/18/nano_sim/

Apple’s iPhone 5 uses a nano SIM, the smallest SIM ever designed and, quite possibly, the last SIM we’ll see in any mobile telephone. The nano SIM used in the new smartphone is tiny and its pattern of electrical contacts are about two thirds the size of the original SIM. It’s almost too small to hold and certainly small enough to lose in a pocket, but despite the diminutive size its basic functionality remains unchanged: hosting encryption, electronics and serial communications at 9,600 bau.

Anonymous hits UK government websites over Julian Assange row
http://www.guardian.co.uk/technology/2012/aug/21/anonymous-hits-government-websites-julian-assange

The hacking group Anonymous claims to have brought down British government websites in protest at the handling of Julian Assange’s bid to avoid extradition to Sweden. Hackers said they had also brought down websites belonging to the justice department and Department for Work and Pensions in the attack. Anonymous vowed to continue targeting government websites as the diplomatic temperature around the WikiLeaks founder continued to rise.

The President’s cybersecurity executive order is almost complete
Real-time requirements and low computational power are two other reasons for which the presence of anti-viruses, especially in the lowest layers of an industrial plant, is jeopardized. General-purpose antiviruses are conceived having in mind the typical “office environment”, and their impact on the performances of control systems might be not negligible.

What just mentioned gives an explanation about the difficult protection of industrial systems from common ICT threats. However these problems can be easily solved adopting proper strategies and reviewing the cyber security governance of the industrial plant. In this context GCSEC has been very active in the last year and in the coming months will publish a set of best practices and guidelines for securing industrial systems.

But what about Stuxnet style malwares? What seems instead hardly solvable today is the problem related to the Zero-Day malwares ad-hoc conceived to break into the industrial systems taking advantage of the peculiarities of their low-level protocols and devices.

Back in 2006 I’ve been one of the first proving that it was relatively easy to create a malware able to take the control of an industrial plant by directly sending commands to the PLCs controlling the plant devices. At that time the research article describing this possibility was seen as a controversial academic exercise with very few possibilities of being realized in the real life. Everybody knows how things went: when Stuxnet appeared that possibility does not seem anymore unfeasible.

Unfortunately the detection of malwares as Stuxnet by antivirus is not trivial. The reason is that antivirus techniques generally try to identify malicious behaviors (using signatures or heuristic models), i.e. antivirus are provided with models of attacker actions and search for occurrences of these models on the systems they monitor.

In a customized environment as a typical industrial system, a similar approach will easily fail. Every plant is slightly different from the others, every system implements slightly different processes (due to the use of different actuators, different sensors etc. etc.). As a result, there are uncountable different approaches an ad-hoc tailored malware can adopt to damage a plant. The idea of using signatures or heuristics to detect suspicious behaviors is, under this point of view, unfeasible, just because these techniques are used to model the behavior of what we do not know (the attacker). Back to the sixties engineers experienced the same type of frustration when trying to guarantee the safety of critical systems: how it would be possible to model all the possible incidents might occur to a plant in order to verify their robustness and safeness? To answer to this question Fault Analysis techniques were developed, aiming at studying the effect of the failure of a component starting from the analysis of the system to be protected. This is, I believe, the key for protecting modern industrial plants from advanced cyber-threats: the true knowledge about how the system works, the industrial processes that run in the plant, the identification of the unwanted critical states (i.e. which states of the system can drive it into an unstable state). Until cyber-security solutions will not be able to take into consideration all this knowledge, until they will not be deeply integrated into the industrial processes run by the plant, with solutions able to understand and to monitor the behavior of the plant, it will be hard to guarantee the complete protection of industrial systems.

Security software able to understand industrial processes, able to predict the behavior of the system they are protecting and on the basis of this knowledge identify if the system is going toward a critical state, this is the challenge of the next generation of antivirus and more in general of “security-shields” in the industrial context.
A new episode might added to the endless stream of cyber-attacks to critical infrastructures in Middle Eastern states. The subject of this episode is a new kind of malware and its name is Shamoon (or "W32.Disttrack" and "W32.EraseMBR").

Shamoon brings to mind the dramatic events that have affected critical infrastructures in recent years. The first was Stuxnet that, two years ago, demonstrated that SCADA systems could be attacked. Its complexity was unusual for a virus because it required a deep knowledge of industrial processes. After Stuxnet there was Duqu that tried to collect information useful to attack Industrial Control Systems. Its purpose was to "spy" rather than take control of a system or damage it. This year it has been the turn of Flame and Gauss, that shared some of the code used in similar settings and the structure of the malware. All these attacks had a common denominator: they were so complex that they can only be created by a group of experts with extensive resources. The Middle East was always the epicenter of the infection!

That's the reason why, when it became known that Saudi Arabia's national oil company, Saudi Aramco, was recently hit by a virus, the first thought goes to its possible predecessors. The hypothesis stems also from several lines of code found in the folders where the malware lurks, which contain the words "Shamoon" (Hence the name of the virus) and "ArabianGulf."

But, unlike Flame, Stuxnet and Duqu, which stalked the same ground, Shamoon did not try to hide its presence as long as possible. After completing its tasks, to ensure that its tracks don't remain, overwrites and erases the files and the Master-Boot Record (MBR), that is the sector of the hard disk which contains the sequence of commands and instructions required to boot the operating system, therefore deleting the partition table of the hard disk installed on infected machines.

It is unusual to find this type of malware in targeted attacks, because after this attack, the machine is almost unusable. The researchers of Seculert have discovered that Shamoon is actually based on two phases of attack:

I. The attacker takes control of an internal device that is directly connected to Internet. From this machine the infection extends to other internal computers, which were probably not connected directly to the Internet.

II. After the machines have been infected, cybercriminals steal all the information they need and then start the "cleaning process" erasing all evidence of other malicious software and data stolen from those machines. Once this is done, the Trojan sends to its control server through the machine that initially infected a report with the stolen data.

In any case, the infected machines will not be able to restore all the data: Shamoon is programmed to ensure that destroyed data cannot be recovered.

1 http://blog.seculert.com/2012/08/shamoon-two-stage-targeted-attack.html
directly from the erased hard disk. In fact, the malware overwrites the data with a small portion of a JPEG image taken from Internet and uses a system driver for low-level access to hard disk to clean up the boot of Windows systems.

It is interesting, according to Kaspersky Lab, the fact that the driver in question was digitally signed with a private encryption key belonging to a company called EldoS Corporation, a company that has a mission to “Help people feel confident about integrity and security of valuable information,” according to their website. Kaspersky said in its blog posting that EldoS’s digital certificate was either stolen or forged to create Shamoon, which would imply a certain level of skill of its authors.

The reaction of Eugene Mayevski, Chief Technology Officer of EldoS was immediate and in his blog has lashed out against the claims of Kaspersky: “Some not identified script kiddies have crafted a malware which wipes victim's disks. To do actual wiping they have used our driver, probably stolen from some of our clients software […] The malware was discovered by several security companies. Only two of them, McAfee and Symantec, properly identified the driver as being stolen from legitimate software.

Kaspersky Labs and several other wanna-be-specialists from other companies have made conclusion that those script kiddies managed to create the driver and sign it using "stolen private cryptographic key of EldoS Corporation", that misleads people and takes advantage in wrong direction of searching for kernel-mode developers".

In fact, even Symantec and McAfee researchers have tried to analyze the malware. Symantec's analysis of Shamoon describes its several components:

1. Dropper - the main component and source of the original infection. It drops a number of other modules, including the wiper and the reporter components. It creates a task to execute itself and a service, named "TrkSvr", to start itself whenever Windows starts.

2. Wiper - this module is responsible for the destructive functionality of the threat. In fact it replaces an existing driver with another one. The device driver is a clean disk driver that enables to read and write disk sectors and it is used to overwrite the MBR of the computer. The file is digitally signed. Furthermore, this module executes a series of commands to collect file names that will be overwritten. Finally this component will overwrite the MBR of the computer, that can no longer start. To overwrite the master boot record of hard drives it is used a JPEG picture of a burning U.S. flag (picture hosted by Wikipedia under the name "US_flag_burning.jpg")

3. Reporter - this module is responsible for reporting infection information back to the attacker. Information is structured as a HTTP GET request and contains specific data including the IP address of the compromised computer and a number that specifies how many files were overwritten.

This study noted that the boot-record wiper, the clean disk driver that enables user-mode applications to read and write to disk sectors, is used to overwrite the computer’s MBR but can be used also for legitimate purposes!

However, the researchers of Symantec explain that was a long time that a malware did not adopt as attack technique the deletion of personal files. “Ten years ago we used to see purely malicious threats like this,” says Liam O’Murchu, Symantec researcher, “It can be difficult getting anything working again […] It would probably require the help of IT professionals with experience in recovery services to get things going again, perhaps by replacing the master boot record, or connecting the hard drive to another computer to use it to access the damaged one”.

Anyway, fresh analysis of the malware showed that the authors seem to be only "talented amateurs". The Kaspersky lab’s researcher Dmitry Tarakanov has carefully analyzed the code of Shamoon and the analysis shows a big number of "silly" errors, as where the author intended to create a full path using “sprintf” function and instead of use the correct format string "%%s%%d.%%", the malware writer used “%S%S%d.%s” with an uppercase “S”. This causes a "sprintf" function failure and no full path string is created. Lack of full path means that no file is dropped. No file, no execution. So, the Shamoon malware does not have a functionality to execute other programs.

Furthermore, “the fact that they used a picture of a fragment of a burning US flag possibly shows that the motive of Shamoon’s authors is to create and use malware in a politically driven way. Moreover, they wished that their protest which was embedded into the malware would not go unnoticed". The researcher concluded: "We’ve got other clues that people behind creating the Shamoon malware are not high-profile programmers and the nature of their mistakes suggests that they are amateurs albeit skillful amateurs as they did create a quite practicable piece of self-replicating destructive malware”.

So, Shamoon seems to be less sophisticated than Flame, Stuxnet, or Duqu. The method of dissemination and the presence of glaring errors in the source code suggests that it is a job of amateur organizations, non governmental organizations and with limited means, probably isolated groups activists with the purpose of vandalism and retaliation. Besides being one of the most complex and incisive Trojan horses studied right now, is very difficult to detect even with up-to-date antivirus software due to its stealthy features.

But the rudimentary nature of this malware has not hampered its effectiveness, since it is still able to evade

---

3 [http://mayevski.blogspot.it/](http://mayevski.blogspot.it/)
Despite this, Member States (art. 13 COM(2012)238), including under a notified scheme at European level. and accepting lack of common legal basis. This clause allows COM(2012)238) that removes legal barriers caused by the

Other boost to adapt their law less margins of interpretation. National authori give more “regulation” form itself, instead of the directive one, aims to
draft also other aspects of electronic identification: documents and web aut

decommerce activities.

The main issues emerged from a EU official Impact Assessment of the Directive are inter-operability problems in cross-border interactions and lack of trust and confidence of citizens, businesses and administrations that don’t feel secure in using electronic signature.

The goals of the new regulation is to fix the above issues and also to boost the single digital market, including in this draft also other aspects of electronic identification: electronic seal, electronic time stamp, electronic documents and web authentication. The proposed “regulation” form itself, instead of the directive one, aims to give more harmonization inside Member States, leaving less margins of interpretation. National authorities have not to adapt their laws to meet EU goals.

Other boosting factors of this proposal are:
• mutual recognition and acceptance rule (art. 5 COM(2012)238) that removes legal barriers caused by the lack of common legal basis. This clause allows recognizing and accepting notified electronic identifications, falling under a notified scheme at European level.
• the definition of the supervision tasks in charge of Member States (art. 13 COM(2012)238), including monitoring and reporting activities to the Commission and to other Member States.

Despite this, Member States are free to have inside their digital identities. The soft digital identity is that kind of identity that doesn’t require a strong registration and authentication process (i.e. social network account, ecommerce account…).

Moreover, the current draft doesn’t consider a large part of digital identities that populate digital market: the so called soft
domestic anti-virus systems and cause extensive damage and leakage of data for the unfortunate victims.

Saudi Aramco, the first suspected victim of Shamoon, announced that are about 30 thousand the restored infected systems on 25 August, machines belonging to the internal network but detached from the systems responsible for the extraction and refining of crude oil. At least three different hacker groups have claimed responsibility for the Saudi Aramco attack, including a previously unknown group called the “Cutting Sword of Justice.

The post on an online bulletin board where the group has claimed its responsibility said that Saudi Aramco

The Directive 93/1999 has led to large margins for different interpretations at national level during the last 10 years. The national interpretations of the Directive have manifested through additional national requirements, allowed by the public sector clause of the Directive (art. 3.7), and also through national implementations, often using different technological solutions.

On 19th September 2012, GCSEC participated with a speech at the World Smart Week in Nice. The topic of the panel was: “The new European ID and eSignature Regulation: What implications for Citizens, Industry & Public Services?”.


The Directive 93/1999 led to large margins for different interpretations at national level during the last 10 years. The national interpretations of the Directive have manifested through additional national requirements, allowed by the public sector clause of the Directive (art. 3.7), and also through national implementations, often using different technological solutions.

The main issues emerged from a EU official Impact Assessment of the Directive are inter-operability problems in cross-border interactions and lack of trust and confidence of citizens, businesses and administrations that don’t feel secure in using electronic signature.

The goals of the new regulation is to fix the above issues and also to boost the single digital market, including in this draft also other aspects of electronic identification: electronic seal, electronic time stamp, electronic documents and web authentication. The proposed “regulation” form itself, instead of the directive one, aims to give more harmonization inside Member States, leaving less margins of interpretation. National authorities have not to adapt their laws to meet EU goals.

Other boosting factors of this proposal are:
• mutual recognition and acceptance rule (art. 5 COM(2012)238) that removes legal barriers caused by the lack of common legal basis. This clause allows recognizing and accepting notified electronic identifications, falling under a notified scheme at European level.
• the definition of the supervision tasks in charge of Member States (art. 13 COM(2012)238), including monitoring and reporting activities to the Commission and to other Member States.

Despite this, Member States are free to have inside their country as many electronic identification tools as they want. All these tools shall only be notified to European Authority in order to be recognized in other Member States. The internal strategy of each Member State will be fundamental in this case. If, the Member State will not govern the proliferation of electronic identification means inside its country, the result could be internal fragmentations, multiplicative effect of costs and disincentives for people to use them. A national strategy will create the right environment for the development of digital market.

On 19th September 2012, GCSEC participated with a speech at the World Smart Week in Nice. The topic of the panel was: “The new European ID and eSignature Regulation: What implications for Citizens, Industry & Public Services?”.


The Directive 93/1999 has led to large margins for different interpretations at national level during the last 10 years. The national interpretations of the Directive have manifested through additional national requirements, allowed by the public sector clause of the Directive (art. 3.7), and also through national implementations, often using different technological solutions.

The main issues emerged from a EU official Impact Assessment of the Directive are inter-operability problems in cross-border interactions and lack of trust and confidence of citizens, businesses and administrations that don’t feel secure in using electronic signature.

The goals of the new regulation is to fix the above issues and also to boost the single digital market, including in this draft also other aspects of electronic identification: electronic seal, electronic time stamp, electronic documents and web authentication. The proposed “regulation” form itself, instead of the directive one, aims to give more harmonization inside Member States, leaving less margins of interpretation. National authorities have not to adapt their laws to meet EU goals.

Other boosting factors of this proposal are:
• mutual recognition and acceptance rule (art. 5 COM(2012)238) that removes legal barriers caused by the lack of common legal basis. This clause allows recognizing and accepting notified electronic identifications, falling under a notified scheme at European level.
• the definition of the supervision tasks in charge of Member States (art. 13 COM(2012)238), including monitoring and reporting activities to the Commission and to other Member States.

Despite this, Member States are free to have inside their

country as many electronic identification tools as they want. All these tools shall only be notified to European Authority in order to be recognized in other Member States. The internal strategy of each Member State will be fundamental in this case. If, the Member State will not govern the proliferation of electronic identification means inside its country, the result could be internal fragmentations, multiplicative effect of costs and disincentives for people to use them. A national strategy will create the right environment for the development of digital market.

Moreover, the current draft doesn’t consider a large part of digital identities that populate digital market: the so called soft
digital identities. The soft digital identity is that kind of identity that doesn’t require a strong registration and authentication process (i.e. social network account, ecommerce account…).

The development of a national program for a single digital market could not exclude to regulate also that kind of identities, vital for e-commerce activities. Other additional European and national key actions shall be also considered to create ideal conditions for electronic identification:
• Bureaucratic simplification and harmonization: barriers are created also by the complexity of bureaucratic systems to inter act with Public Administrations. An administrative harmonization through Member States will encourage cross-border inter-actions information sharing on cyber crime related to electronic identities.
• Reduction of cultural device: creation of educational program in informatics and cyber security since the primary school; increasing the use of English language in school program and mandatory translation of public digital services in English language.
• Creation of cyber security profiles and capabilities:
definition of an European set of competencies for cyber security experts and creation of effective tools for information sharing on cyber crime related to electronic identities.

The new proposal of regulation is currently under the review of Member States. Member States could present recommendations or suggestions to modify the text.

The regulation is only the first step for a common legal framework on electronic identities. The point is that Member States have already invested in national technological solutions for electronic identification that could differ between them. This regulation could be considered a good compromise for the short term.

**“The Cloud bumps into critical infrastructures”**

*by Emiliano Casalicchio, University of Tor Vergata/GCSEC*

Cloud is a buzzword that has monopolized the attention of all media, but, to date, especially for non-experts, it remains empty of content, or worse, has become a “polluted cloud”.

From a personal analysis, the "pollution" of Cloud concept is linked to its data center-centric vision that proposes it as a means of concentrating services with the sole aim to bring down costs. This restrictive view is likely to reduce significantly the potential of cloud and could trigger a reverse gear rather than a leap forward in the Internet of the future.

So, let's try to go back to the origins and meaning of the word cloud. Cloud computing is often used as a general term for any solution that allows the outsourcing of any kind of computational, network and storage resources.

Between 2007 and 2009 more than 20 definitions of cloud computing have been given, including the one from NIST (National Institute of Standards and Technologies - USA), considered as "the standard". Some definitions of Cloud stress the properties of scalability and resilience (so the ability to satisfy peak loads in a highly dynamic way). Others focus on the properties of process automation and management of large data-center, focusing on aspects of costs optimization and business models "pay-per-use" or "pay-as-you-go".

For example, a group of researchers of Telefonica Investigation (Spain) and SAP Research (United Kingdom) speak of "Clouds" (using plural): "The Clouds are a great set of virtualized resources (hardware, platforms and services) easily accessible and usable. These resources can be dynamically reconfigured to meet a variable load, thus allowing for optimal management of resources and fulfillment of service contracts (SLAs)."

As you can see there is no mention of the computational power of datacenter hosting virtualized resources, while the emphasis is on the fact that there should be more clouds, on their reconfigurability and on ease of use of services offered.

R. Choen, co-founder of CloudCamp and Vice President of Virtustream, emphasizes the fact that Cloud computing, as well as being an attempt to summarize in one word a series of concepts such as virtualization, load balancing, Web 2.0, provisioning and business models, describes the concept of "internet centric software", i.e. the ability to use services available through Internet and available for new services creation (which retain the same characteristic of usability and modularity).

Even Ben Kepes, commentator and business advisor, focuses on the concept of software as a service, then accessible via Internet, and the fact that applications, virtualized and offered as services, provide access to a wide range of features that once could be realized only "in house", with large investments in infrastructure and professional resources.

Finally, NIST clears up on deployment patterns, distinguishing between four types of cloud: private, community, public and hybrid.

A private cloud is created and operated for the exclusive use of a single organization. It can be owned, managed and operated by the organization itself, by a third party or by a combination of two. A special extended case of private cloud is the cloud community, to the exclusive use of a community of users that share a set of goals, including security, interoperability, policies, etc ...

The public cloud is created for access to the entire community, all potential users of the Internet. Classic examples are Google Apps, Dropbox, Flickr, Amazon Web Services, etc..

Finally, the hybrid cloud (or federated cloud) is the composition of two or more distinct cloud (public or private) that remain separate entities but share standards of portability (of data and applications), performance targets and safety (or SLA) and establish contracts to ensure SLAs offered (such as load balancing among the nodes of the federation).

From these definitions emerge clearly that Cloud is not only Datacenter and virtualized servers: restricting Cloud to a datacenter-centric model not only means making a
“Flame: report of a malware”

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

Discovered in May 2012 but already in activity from 2010 (or even 2007) Flame is claimed to be the most complex virus ever seen. This modular computer malware, also called Flamer or sKyWIper, is a sophisticated cyber espionage tool specifically designed for industrial systems and used to steal various kinds of information. Analyzed by multiple organizations like MAHER (the center of Iranian National CERT), Kaspersky Lab and CrySyS Lab, Flame has revealed several significant characteristics and uncommon properties. It can record audio/video streams (Skype calls included) and monitor keyboard activities as well as network traffic. Beyond that, Flame is extremely effective in replicating itself and reaching new victims.

Local networks and USB sticks are the most used infection mediums, but it is interesting to underline that the malware can take advantage also of Bluetooth connections stealing user data from nearby enabled devices even without being physically installed in them. Like Stuxnet and Duqu, Flame plays a significant role in the emerging landscape of cyber weapons.

Futuristic cyberwarfare scenarios show that the development of these new malwares is increasingly confined to groups of highly-skilled people with the support of significant resources in terms of money, time and infrastructures. This reasoning narrows the focus down on large terrorist organizations or, more likely, countries and government apparatus. From this, it follows that such kind of weapons are not used in an indiscriminate manner but instead they carry on the so-called Targeted Attacks.

Industry observers are realizing that and, on May 2012, AIIC (the Italian Association of Critical Infrastructures) and Cloud Security Alliance Italy have signed a cooperation agreement with high technical and scientific level, for the security of Cloud systems that oversee critical infrastructures.

Furthermore, risk and opportunity of cloud is to break down the boundaries of corporate ICT assets leading to a potentially dangerous traffic of data. If you think to the convergence of Cloud and Mobile, the breaking down of boundaries has a worldwide dimension. Inspired by the title of the famous book by Thomas Friedman, I like to consider Cloud as a way to a “Flat World of ICT assets.”
According to The Washington Post, Flame is in fact part of a larger classified project code-named Olympic Games which was intended to collect sensible information in preparation for a cyber-sabotage campaign aimed at slowing Iranian nuclear efforts. In confirmation of these rumors, Iran was the most affected country with hundreds of compromised computers among governmental organizations, educational institutions and private individuals. The infection has also been reported in Israel, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt.

To create Flame, developers take advantage of the Lua scripting language with compiled C++ code linked in. Some of the exploits the malware uses to compromise systems were previously seen in both Stuxnet and Duqu but the DLL injection mechanisms were unknown. Researchers from the Polish CERT analyzed the infection process showing that the malware distributes its elements throughout different operating systems processes. It uses chains of up to three injections involving up to four processes in order to perform its trojan operations. This kind of distribution among various processes obviously makes a behavior-based detection very hard to implement. The malware uses an SQLite database to store structured information and several encryption methods but it is very interesting to note that most of them are actually very easy to crack. However this is not a weakness since sophisticated encryption causes high randomness that can be easily detected by protection systems while “looking like common data” can be a successful camouflage for the attack. Differently from other high-level malwares, Flame is not designed to deactivate automatically but it supports a “kill” function. This feature allows it to eliminate all traces of its files and operations from a system avoiding any kind of forensics and post-mortem analysis.

To infect its victims Flame succeeded in hijacking Microsoft Update connections thanks to a fraudulent certificate of the Microsoft Enforced Licensing Intermediate PCA. The malware creators identified a Microsoft Terminal Server Licensing Service certificate that was unintentionally enabled for code signing. Thanks to this configuration error they were able to produce a counterfeit copy of the certificate. After that, Flame’s authors used it to sign some components of the malware so making them appear to have originated from Microsoft. In this way the malware is actually capable of intercept requests to Microsoft Update servers and, instead to accomplish those tasks, it delivers to the compromised machine a malicious executable that is signed with a rogue, but technically valid, Microsoft certificate.

After its discover Flame's creators have been trying to batten down the hatches. Symantec claimed that the authors of the malware sent the aforementioned “kill” command already in June 2012 attempting to remove all the copies from infected computers and avoiding further analyses. Lately, the efforts of the computer security experts are focusing also in attempting to trace the source of Flame’s infection. This action concentrates on recovering information from Command & Control servers used to direct malware activities. Kaspersky’s researchers recently succeeded in cracking the password protecting a server that controlled the Flame espionage botnet giving them access to the malware control panel and allowing them to learn more about how the network functioning. Despite this, the company stated that due to the size and the complexity of the program a full analysis could require as long as ten years and a complete understanding of the malware is still far away.

As previously pointed out Flame is a highly sophisticated espionage tool but, actually, it has no modules aiming at subvert industrial control systems. This is probably the feature that most distinguishes it from Stuxnet that, besides gathering information, includes a programmable logic controller rootkit. The most appropriate comparison is the one with Duqu. Both malwares have the main purpose to collect useful information in preparation for an attack aimed at disturbing process control systems and undermine the functioning of critical infrastructures. Despite that, the behavior of Flame is much more aggressive, both in the processes of infection and of espionage, while Duqu tries to acquire information in the less intrusive way possible. From a technical point of view the two malwares have many differences and they seem not to share the same development team. However it is impossible to rule out the possibility that they were implemented by independent teams hired by the same attacker for an identical malicious purpose.

The first characteristic of Flame that struck security experts is the unusual dimension of the malware. With is twenty megabytes is much larger than Stuxnet or any other malicious programs ever studied. Despite that, it is designed in such a way that it is nearly impossible to track it down thanks to its advanced stealth capabilities. One of them allows the malware to determine what antivirus software is installed and to customize its configuration (for example by changing the filename extensions) reducing the probability of been detected.