European Electronic Crime Task Force (EECTF)

EECTF is an information sharing initiative started in 2009 by an agreement between United Secret Service, Italian Ministry of Internal Affairs and Poste Italiane. EECTF mission is to support analysis and development of best practices against cybercrime in European country, with a creation of a strategic alliance between public and private sectors, Financial, Law Enforcement, academia, International Institutions and ICT security vendors.

With this spirit EECTF held a conference the 22th of November in Poste Italiane where the focus was Advanced Persistent Threats (APT).

APT is a network attack or breach in which someone without the privileges enters the network and operates within the network undetected for a long period of time. The fact that they are designed to run undetected, means that are very difficult to detect and remove. The main goal behind an APT attack is to steal as much data as possible instead of causing damage or blocking the victim infrastructure. In the latest years these attacks are targeted organizations with confidential information such as the financial companies and government institutions.

In the future APT will continue to increase and will more adaptive changing pattern attacks and behavior. As discussed in the technical workshop only an early detection and a strong response capability may help organization to face this threat. Identification of Threat Indicators and Techniques, Tactics and Procedure (TTP) of attacks, as well information sharing and collaboration, can enhance prevention and detection capabilities in the organizations.

GCSEC was part of this initiative and proudly collaborate to a study done with all the EECTF partners, this study will provide an overview of APT attacks patterns, threats indicators and also recommendations. Moreover, there will be a classification model to facilitate information sharing and enhance defense capabilities.

We know that the efforts that should be placed is still a lot, the cyberspace is the battle domain in which the private public partnership should be stronger; a big effort on information sharing and knowledge is also required and we are working on maintaining high the attention on this matter.

This study will available on the EECTF web site soon, from December this nice initiative will have also a digital space that will provide news and information in order to contribute for a safer cyber space. So I’ll invite you to add a new bookmark for www.eectf.com and www.eectf.eu web sites.

Nicola Sotira  
General Manager GCSEC

Cloud Access Security Broker Event

Date: 15 December, 2016  
Location: Rome, Italy  
http://www.gcsec.org/news-events/cloudaccess-security-broker-event

The Global Cyber Security Center of Poste Italiane in collaboration with Symantec + Blue Coat, organizing the event "Cloud Access Security Broker Event" dedicated to the CASB "ELASTICA" technologies. The event will be held December 15, 2016 at the Hotel Bernini, Piazza Barberini 23, Rome. Objectives of the event is to address and discuss how can manage direct access, applications and services in cloud trough the Cloud Access Security Broker technologies for security and data compliance.

The adoption of the cloud is growing and it’s the first needs in the IT player strategies. Companies are trying to figure out how to direct the impact resulting from new applications and how addressing a clear "strategic vision", posing attention to advanced levels of cloud such as cyber security.

WEBINAR: CERT for Cybersecurity from A to Z

Date: 15 December, 2016  
Location: Milan, Italy  
http://www.theinnovationgroup.it/events/webinar-il-cert-per-la-cybersecurity-dalla-a-alla-z/?lang=it

Businesses must also commit to the front of cybersecurity incident response, a problem that occurs on a daily basis now. They can do this with an internal CERT, which achieves a greater collection capacity of reporting of cyber incidents, as well as visibility into inevitable vulnerability of ICT systems, involving the entire user community. These are the same standards, such as NIS Directive and the Regulation on the EU Privacy, to require, among other things, the notification quickly to the parties concerned in the event of breach date, then pushing companies to be more proactive in managing critical aspects for their very survival.
Artificial Intelligence (AI) and Cyber Threat Intelligence (CTI) are two important fields of scientific research that can be related for many reasons. Obviously the first can help the second to automate many processes like data search or by avoiding the false detection of attacks, for instance.

Let's start from the beginning: the term Artificial Intelligence was coined in 1956 by John McCarthy during a seminar that introduced the first theories about automata and neural networks. Since then AI became an independent science, also if it was closely linked to other sciences like mathematic, statistic, computer science, philosophy, and neurobiology. The AI algorithms have two basic purposes: to create machines that think and act or machines that simulate human behaviour (rational behaviour). The difference between...

Criminal gangs like the Cobalt gang are now focusing their efforts on the banks to steal cash directly from the ATMs with jackpotting attacks.

Security experts are assisting a change of tactics for the criminal organizations who target the ATMs and online banking credentials. Crooks are now focusing their efforts on the banks in the attempt to steal cash directly from the ATMs. In the last months, cyber criminals targeted ATM machines in Taiwan and Thailand, in both cases, crooks used a malware to infect the machine and have instructed them on spitting out cash on demand. The principal ATM manufacturers, Diebold Nixdorf and NCR Corp., confirmed to be aware of the ATM attacks and had already been working with their customers to mitigate the threat.

ATM machines are now under attack and a recent hack in systems in at least 14 countries including the UK and the Netherlands have been remotely hacked by an organized gang to spit out cash for rapid collection by the attackers. Russian cyber security firm IB Group said that perpetrator of this 'jackpotting' of cash machines was an Eastern European hacking group known as Cobalt. ATMs in Malaysia, Belarus, Armenia, Bulgaria, Estonia, Georgia, Kyrgyzstan, Moldova, Poland, Romania, Russia and Spain were also affected. The company, however, declined to name any specific banks.

A few days ago I was contacted by a young hacker that breached Indian embassies across the worlds, he goes online with the moniker Kapustkiy. Kapustkiy is a pentester that is targeting organizations and embassies across the world. Recently he breached the Paraguay Embassy of Taiwan (www.embapartwroc.com.tw), while a few days ago the hacker and his friend Kasimierz ( @Kasimierz_ ) hacked the Indian Embassies in Switzerland, Mali,
the first and the second approach is that in the first the machines are not developed following the human rationality, but they can act following an own rationality, depends on optimal choice at each stage with the hope of finding a global optimum. This kind of AI is used to provide methods for solving a lot of problems, for instance making decision based on a large amount of data, that cannot be solved without applying AI.

Considering that, let’s talk about artificial neural networks. They are self-learning systems based on biological neural network, a series of interconnected neuron whose activation defines a recognizable linear pathway. An artificial neural network is an adaptive system that changes its structure according to data flowing through the nodes on the network. It receives external signals on a set of input nodes connected to internal nodes that process the signal and transmit it to other nodes. The self-learning system in artificial neural network allows it to adapt to its contents through a set of data called training set that is known (we know both input than output). After that, network is trained by an algorithm, using data in order to modify the weights and other parameters in all nodes involved. Ultimate goal is the prediction of output value for each input value.

The implementation of AI algorithms in Cyber Threat Intelligence already occurred, specially the artificial neural nets algorithms. They help in all processes that affect decision-making, improving the speed of operations. Artificial Neural Networks algorithms are well applicable in many fields of Cyber Threat intelligence, from problem detection to assets protection, malware classification and forensic investigations. Regarding problem detection we have some examples already implemented like DoS, computer warm, spam and zombie detection. The success of this kind of algorithm is the high speed in processing and the adaptability to new agents and events.

Another field of AI is the Expert System. It is a software for finding answers to question in some application domain. Expert system tries to repeat the performances of many experts, in a limited domain with a full knowledge (for example in medical diagnosis, in finance or cyberspace). At the base of Expert System there is a knowledge base, where expert knowledge is stored. Above this knowledge there is the inference engine for deriving answers based on this database and for adding additional knowledge. Many tools of Cyber Threat Intelligence have these purposes: of detecting threat starting from a set of data and of updating the database improving quality of future services. In cyber threat intelligence the experts systems facilitate the selection of security measures with an optimal use of resources.

AI brings a lot of improvements in CTI and the best are provided by the research in Artificial Neural Networks. Despite this, there is a need for application AI in several areas where Artificial Neural Nets are not the optimum (like decision support, situation awareness and knowledge management), then we could use system like Expert System.

“Humans are superb problem solvers; superb learners; superb at coordinating functions of sensing and locomotion and problem solving into an integrated unit. However, computer programs can claim intellectual niches that evolution did not provide for us marvelous creatures” (Edward A. Feigenbaum).

Geopolitics Theories and Cyberspace
by Massimo Cappelli, GCSEC

During the centuries, the battlefield domains have been topics for geopolitics theories that have influenced politics and militaries, even following scientific progress and anticipating the current eras. Some brief examples:

The theories of Alfred T. Mahan highlighted the relevance to have a strong and well equipped fleet. In “The influence of Sea Power upon History” he explained that to dominate the world, it was fundamental to become a sea power and not a terrestrial one. His publications, such as "The Interest of America in Sea Power", influenced the governments of the
U.S., Germany, Japan and U.K. to start a campaign of Naval enhancement during the late 19th and early 20th centuries.

Another father of geopolitics, Sir Halford Mackinder, a British geographer, claimed the existence of a pivot area of the world (or Heartland "Heart of the World"), which he identified in the area belonging to the former Soviet Union (1904). Those who had owned this land would also have controlled the Island World that includes Europe, Asia and Africa. This area, in fact, is a natural fortress, unapproachable by sea powers.

Assumptions about the importance of the Eurasian area, however, did not take into account the technological advances that saw the introduction of military weapons such as missiles at long range capable of hitting anywhere in the world.

Even Nicholas Spykman (1893-1943), leader of the American geopolitical school, considered the importance of Heartland, but, around it, he assumed a sort of Rimland, a region intermediate between the Heartland and the surrounding seas, including Europe, the Middle East, India, the region of the Jacutia. The formula that was proposed by him was as follows: "Who controls the Rimland, controls Eurasia, who rules Eurasia controls the destinies of world ". The same policy of containment of President Truman is thought to have been influenced by the theories of Mackinder and Spykman.

The Progress in the field of aeronautics and missile, with the invention of nuclear bomb, led to re-evaluate the importance of geo-strategic position of a particular State within the world stage.

The Russian pilot Alexander P. de Seversky (1894-1947) understood the role that would take aviation in the strategic field. In the essay "Victory Through Air Power" (1942), divided the world into two large circles with hearts as a center of industrial United States and Soviet Union and operating ranges as those of strategic bombers of the time. Now, the political concept of territory has been broken again by the technological evolution.

In "The End of Territories" (1996) Bertrand Badie, professor of political science at the Institute of Political Studies of Paris, says that the importance of the territory, intended as: something that had to define the membership function of an individual to a national context, is now to waver.

Remember the statement: "WE ARE ANONYMOUS". People of several countries, several cultures, several ages supporting common ideas of hacktivism on the web against finance, oil & gas, media, governments. Remember how they also supported Arab Spring. Hactivists join common topic of protest and the numbers and typology of people change on the basis of the topics, like waves. There is no longer a place of belonging. The world becomes a "global village" where everyone is a citizen of the world and everyone could participate to a campaign.

In 1994, Lanxade Admiral, Chief of Staff of the French army, said: "the security of France will be played at distances farther and farther from its territory". The closing decades of the last century have seen the growth of a new era driven by digital information technologies, whose centerpiece is Internet.

The digital environment has been named “cyberspace”. The cyberspace represents a new field of conquest for public and private entities.

Mahan was convinced of the relevance of Sea Power, Mackinder and Spykman highlighted the importance of Lands Power, on the other hand de Seversky bet on Air Power. Everybody was convinced that the Hegemony on a field will lead to the Victory.

In the new era, there is a new battle field beyond sea, land, air and space, partially unregulated and with undefined borders: the cyberspace.

In May 2010, the U.S. Defense Secretary Robert Gates announced the appointment of four-star Gen. Keith Alexander as the country's first commander of the newly created U.S. Cyber Command. Concerns were expressed also in a report of Northrop Grumman delivered to the U.S.-China Economic and Security Review Commission. It stated that “U.S. telecommunication supply chain is particularly vulnerable to cyber- tampering.
and an attack could result in a catastrophic failure of U.S. critical infrastructure. A typical Internet router could have components made in 16 locations, many in Far East countries, which all could provide avenues for meddling.

The cyberspace domain is probably the toughest.

If we want to translate geopolitics theories of the past in the present, shall we still consider that who will dominate the cyberspace will probably “dominate” the world? Internet has no owners but it is also truth that a lot of companies struggle everyday in order to prevail on the others for what is concerning the Hegemony of IT devices and online services.

Microsoft, Apple, Symantec, Kaspersky, Samsung, Huawei, Cisco are only part of the brands that everyday deploy new software/hardware on millions of computers. Facebook, Twitter, Google+ are only part of social networks that gather information worldwide.

- 400 millions of devices with the same operating system;
- 100 millions of smartphone sold worldwide of a single brand;
- 1,65 billions of users of one single social network around the world.

Just to give you an idea of the numbers.

My question is: could the application/tools/update be transformed as potential instruments in a cyber war? Probably, most of experts in Economics will answer that none of the above companies will never allow to a Government to use their products as “weapons” because they will loose market share and customers’ trust. I totally agree with them. However, the issue will rise up in case of conflicts that threat state sovereignty, unification, territorial integrity or security.

National mobilization laws could oblige private industries to be under control of National government. It happened in Japan (1938) with the nationalization of strategic industries but also in U.K in 1939, in U.S. in 1917.

It happened in February 2010, China’s top legislature passed the National Defense Mobilization Law, in which substantially the National People’s Congress Standing Committee approved that in order to successfully enforce wartime mobilization, special measures could be taken to supervise and control key industries and areas, according to the Law.

Substantially, we can affirm that cyberspace has no owners in peacetime but we could not be sure on that during wartime. Devices, applications and in general any kind of IT assets could become part of an attack, as showed at the end of October current year in USA.

In the meeting of Warsaw of July, NATO Member States have recognized cyberspace as a domain of operations (article 71).

“Each Ally will honour its responsibility to improve its resilience and ability to respond quickly and effectively to cyber attacks, including in hybrid contexts”.

The cyberspace is the domain in which the private operators have a relevant defense role. I suggest you to read the book “Blackout” of Marc Elsberg in order to have a picture of a European Crisis Scenario after a persistent cyber attack, impacting all the EU Member States and citizens.

Private sector is the first line of defense and also the first line of attack in the cyber domain. If I have to attack a Nation, the first thing I would do it’s to paralyze the infrastructure of a country: telecommunication, transport and energy at first. Using cyber attack allows maintaining intact the infrastructures. No cost of re-construction.

The private companies own these infrastructures so they are the first line of defense. But they are the first line of attack too. The same infrastructures could become vectors of attack (think about the concept of botnets or Internet of Things). The private sector has to strengthen its defense capabilities and can learn a lot by defense sector.

European Union and NATO are building a series of public private partnership to improve the resilience of our network. Personally, I have learnt a lot participating to the NATO Industrial Advisory Groups and to the EU Funding Programme such as Horizon 2020. I would like to promote in private sector what I have learnt from the colleagues known there. For example: the countermeasures put in place in private sector are similar to that one of military sector. The approach of CERT and SOC are evolving to a concept of Cyber Defense Situational Awareness too.

Together NATO and EU include 34 countries, 22 of them are in both the organizations. In terms of research and development, in terms of know-how, in terms of capability there is a huge capital to exploit.

What is missing? It is not sufficient the number of Nations. It’s not sufficient to express the will to collaborate. It’s time to act more concretely all together.
A EU-NATO common strategy should be put in place with clear operational objectives to reach together. Will it be sufficient? No, because it is still missing the main PILLAR of all the initiatives we can think and develop together. A pillar that is not related to technology or to capabilities. It's a pillar that you could have or not. It's like a binary code 0 or 1. That pillar is TRUST. Trust each other, trust concretely to our relationships, trust on what we want build together. We should just be more effective and our society will become more resilience and our citizens more protected.

How much will the cyber crime countermeasures cost you? E-CRIME Project
by Alessandra Zaccaria, GCSEC

The scope of the E-Crime project is to evaluate the impact of cyber crime on non-ICT sector, such as finance, health, transport, energy and retail and to define the adequate countermeasures to contrast this phenomenon. We describe 15 scenarios of attack and step by step we suggest the security solutions, according to the classification of the Cyber Security National Framework of NIST. For each countermeasure, we propose a calculation methodology of the costs on corporate budget that will be validated or updated by stakeholders through a survey.

Here, we present an abstract of the attack journey against the SCADA System through the Business Architecture Network. The ICS Systems are designed to be hosted on isolated network, while often they are integrated into business architecture to reduce time and cost of production, not minding the cyber exposure risk. The SCADA system is not always compatible with antivirus software: slowdown, performance loss, reboot of the system hinder the delivery of a service, which should be always-on and on the same intensity for safety reasons. Therefore it is plausible that an attack can follow this pattern to gain the access into the network of a power plant. Then the attacker will take control of system consoles and move into the internal network in stealth mode. In our attack journey, how it actually happens, we expected a SCADA System not patched, no sort of end-points defences installed and an user authorization enforcement not implemented. The attacker will detect this vulnerability, exploit it and in the end alter the energy stock data to determine financial losses.

In the table below, our experts divided the attack in 5 steps. For each step of attack, we identify one or more countermeasures that could be effective. For each countermeasure, we define a cost evaluation method and we classify it inside the Category and Function of the National Cyber Security Framework of NIST.
<table>
<thead>
<tr>
<th>Step</th>
<th>Attack Journey</th>
<th>Countermeasure</th>
<th>Cost evaluation method</th>
<th>Category Unique Identifier</th>
<th>Category</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The SCADA system is located within a network that is not connected to the Internet. In order to make the real time power production data available for the energy stock trade the SCADA system has been connected to Business Architecture Systems</td>
<td>Security Policy</td>
<td>(Employees time dedicated to policy [definition, divulgation, review] x salary average) + amortisation of document management system</td>
<td>ID.GV.</td>
<td>Governance</td>
<td>Identify</td>
</tr>
<tr>
<td>2</td>
<td>The software used to monitor the energy production, and related reporting application, were developed by an external supplier. The software were designed with poor security requirements due the short time available and the necessity of “going live” as soon as possible. The supplier agreed with the plant management to fix any security vulnerabilities in the application at a later time: the primary goal of the management is to be ready by the launch day of the energy stock</td>
<td>Secure Design</td>
<td>(Employees time dedicated to Application Design x salary average) + (Cost Secure Code Training x number employees involved in Application design)</td>
<td>PR.DS.</td>
<td>Data Security</td>
<td>Protect</td>
</tr>
<tr>
<td></td>
<td>Risk Analysis</td>
<td>(Employees time dedicated to RA x salary average + amortisation of document management system)</td>
<td>ID.RA.</td>
<td>Risk Assessment</td>
<td>Identify</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>The attacker team performs a reconnaissance activity on the web application; The attacker avoided detection by covering their activity with anonymizing systems (i.e. Using Tor Networks, abusing third-party machine and using them with VPN connections);</td>
<td>NIDS</td>
<td>(Employees time dedicated to NIDS x salary average) Amortisation of NIDS</td>
<td>PR.PT.</td>
<td>Protective Technology</td>
<td>Protect</td>
</tr>
<tr>
<td></td>
<td>Web Application Firewall</td>
<td>(Employees time dedicated to WAF x salary average) + amortisation of WAF</td>
<td>PR.PT.</td>
<td>Protective Technology</td>
<td>Protect</td>
<td></td>
</tr>
</tbody>
</table>
The NIST Framework Core consists of five Functions, Identify, Protect, Detect, Respond, Recover, associated to underlying key Categories and Subcategories. As a whole, the Core represents the lifecycle of an organization’s management of cyber security risk, from the executive level to the operation one. We suggest the following countermeasures for each step of the scenario and we define some examples of cost evaluation method:

- **IDENTIFY**: For the effective use of the Framework it is essential understanding the business context, the value of assets and the cyber risk exposure in order to create a strategy of risk management aligned with the needs of corporations. We suggest these countermeasures:

- **STEP 1**  
  **GOVERNANCE: SECURITY POLICY**
  Governance consists in processing and sharing the requirements, procedures and policies, that assign roles and responsibilities within the company. In our scenario, the security policy have to provide a safe and secure integration between the SCADA System and the Business Architecture to make real time power production data available for the energy stock trade.

  Cost evaluation method annex: the cost related to the security policy include the cost of defining it, the time spent by employees to divulgate and review it and the amortisation of document management system on corporate budget. We have not considered the cost of utilities (i.e. energy) that could be expressed as percentage or not at the discretion of industry.

- **STEP 2**  
  **RISK ASSESSMENT: RISK ANALYSIS**
  The necessity of “going live” as soon as possible must be replaced by a secure going live! The SCADA System and the related reporting application, originally designed with poor security requirements, must be subjected to the Risk Analysis to identify and management threats and vulnerabilities, evaluate the existing countermeasures, end estimate the potential impact of a cyber attack. Be ready but not safe and secure at launch day of the energy stock can turn into a misstep.

  Cost evaluation method annex: the cost related to the Risk Analysis should include the cost of defining it, the time spent by employees to learn and perform it and the amortisation of document management system on corporate budget. It will be at the discretion of the industry whether to include or not the cost of utilities (i.e. energy).

- **PROTECT**: this activity defines the safeguards to limit or contain the impact of a potential cyber security event. According to our scenario, we propose this countermeasures:

- **STEP 2-4**  
  **SECURE DESIGN: DATA SECURITY**
  The secure design should ensure a basic security of a product, and in this context it should ensure the
confidentiality, integrity and availability of informations and records. In our scenario, both the SCADA System and the business reporting application are not secure by design: the former it is projected for isolated networks, the latter is designed to going live as soon as possible. The data security policy have to apply for software secure for design or at least request to make it secure to protect the confidentiality, integrity and availability of data.

Cost evaluation method annex: the cost related to Secure Design include the cost of Secure Code training and the time spent by employees to improve awareness about the Application Design. We don’t have considered the training needed to ensure data security. We focus on the countermeasures not also on the necessary capabilities to perform the activities, wich should be considered in general.

- **STEP 3-5 PROTECT: PROTECTIVE TECHNOLOGY (NIDS)**
  To ensure the security and resilience of assets are used technological solutions aligned with the corporate Security Policy. The Network-based Intrusion Detection System track intrusion through the network traffic generated by anomalies. Consequently, it is able to observe a strange traffic behaviour due to a reconnaissacncy activity on web application with the use of TOR, tird – party machine or VPN network (**STEP 3**), to a rootkit or a bakdoor (**STEP 5**).

Cost evaluation method annex: it is a monitoring activity therefore we include the cost of the amortisation of NIDS on corporate budget and the cost of time percentage of employees monitoring the tool.

- **STEP 5 PROTECT: PROTECTIVE TECHNOLOGY (NETWORK SEGREGATION)**
  Between the SCADA System and the Business Architecture Business it should not exist a direct link. An optimal solution which ensure a defense in depth is the network segregation, that is the creation of a demilitarized zone characterized by the check of access and permission of the user.

Cost evaluation method annex: it is a monitoring activity therefore we include the cost of the amortisation of the Network Segregation tool on corporate budget and the cost of time percentage of employees monitoring the effective network segregation.

Last but not least, all our suggestions will be submitted to the stakeholders trough a survey in order to check if our assumptions on methodology are optimal for all the costs attributable to the countermeasures against the cyber crime!

---

**IoT: Internet of Things or Internet of Threats?**

*by ADS Group*

Twenty billion IoT devices will be up by 2020 [1]: they will certainly be smart, but will they be “safe” enough? Who chooses to rely on a smart device, is aware of the many opportunities it offers. Likely, he doesn’t know that it had just planted a possible attack vector inside his walls... indeed, potentially, the most dangerous of the attack vectors available today. Wearable and medical devices, smart light bulbs, smart TV, smart domestic appliances... This is just a small part of “smart” devices connected to the data network, but to our lives as well, and therefore to our privacy and our confidential data. Thus, while the IoT devices are quickly and deeply adopted in the everyday life of billions people, the evolution of security related to them, both in software and hardware components, doesn’t run at the same speed, leaving the security aspect still wrongly considered as an added value. This happens mainly because of for two reasons: first, in order to contain the products price, information security principles are not always implemented “by design” in the IoT devices; second, Companies are surprisingly often not enough aware about the consequences of unsafe product which has a significant influence in the real world.

The threats ranges from business loss to life danger. In June 2016, a special kind of DDoS attack (Distributed Denial-of-Service) was carried out by a botnet composed by closed circuit television cameras (CCTV) located in many different areas of the world, and that together was capable to generate over 50.000 requests per second against a single target. By analyzing the source IP addresses, the attacks appeared to come from Taiwan (24%), USA (12%), Indonesia (9%), Mexico (8%), Malaysia (6%), Israel and Italy (5%). The devices have been likely “owned” by exploiting a vulnerability in DVR equipment for video surveillance and affecting the device firmware of million products manufactured by than 70 different Companies [2].

Speaking about DDoS, most recently (**October 21st 2016**), the malware Mirai has knocked out for few hours the websites of Companies such as Spotify, Twitter, eBay, PayPal and Yelp, in addition to the open source platform

---

1 Botnet: network of compromised computers (bots or zombies) connected via Internet and controlled by an entity called botmaster through different communication channels, including IRC (Internet Relay Chat) and P2P (peer-to-peer).
GitHub. More in detail, the cybercriminals responsible for this attack have targeted the DNS provider Dyn by the means of a Mirai (which prophetically means “future”, in Japanese) botnet composed by thousands of IoT devices sending billions of concurrent requests to the Dyn DNS servers, overwhelming the service in short time and making it inaccessible to US East Coast legitimate users.

Early last month, Anna-Senpai, an Hackforums user, has published the Mirai code [3]. This has produced a double effect: on one hand, now the code can be studied to fight it properly; on the other hand, however, improvised cyber-criminals may use it with no particular skills to create a new botnet, possibly more harmful.

At the moment of this writing, the Mirai botnet is composed by about 500,000 devices, mainly located in the American area (29% in US, 23% in Brazil, 8% in Colombia).

Let’s take a closer look to Mirai: it is a malware platform, which infects the IoT devices and is used to carry out DDoS attacks. In particular, Mirai is composed by C&C (Command & Control server) written in Go language, and by bot (client application) written in C.

The malware has two main goals:
1) to locate and compromise vulnerable IoT devices to expand the botnet
2) to launch DDoS attacks based on instructions fired by the C&C.

Mirai scans a wide range of IP addresses in order to identify poorly configured IoT devices that use weak or default administration credentials.

Once infected, vulnerable IoT will form a botnet capable to flood a target with a myriad of requests that it cannot handle, causing a resource jeopardization.

Avoiding generic passwords or changing the default ones, and disabling the remote administration (WAN, SSH, Telnet, http, https), are the key rules that can keep devices from joining the Mirai botnet.

Furthermore, an IoT device infected by Mirai can be “cleaned up” with few simple steps:
1) disconnect the device from the network;
2) reboot the device to eliminate malware;
3) replace the default password of the device with a strong password and, only then, reconnect the device to the network.

“Things vulnerabilities” may also be combined with traditional network vulnerabilities. The Man-in-the-middle attack becomes Man-in-the-IoT, in this context, and takes place when the “communications” between two IoT devices or between them and their control center or gateways are intercepted by an attacker in order to obtain the control of those devices and use them to perform malicious actions against the IoT ecosystem or other targets.

Someone considers the Man-in-the-IoT a kind of Man-in-the-Middle 2.0. In the past, a MitM victim should have been worried about the loss of sensitive data, at worst. Today, the scenario has substantially changed. The threat related to a Man-in-the-IoT, in fact, could affect people safety, up to irreversible consequences.

If you’re wondering how, just follow us in this hypothetical scenario.

A great metropolis: New York City. 12,260 crossroads regulated by tens of thousands of traffic lights. Statistics on traffic flows in the Big Apple, speak for themselves, after all: about 786,000 estimated vehicles on the road daily in the

---

[2] Anna-Senpai is the nickname used by the Mirai’s author, in tribute to Anna Nishikinomiya manga character that appears in Shimoseka Japanese series.

[3] Mirai is loaded and executed only in the volatile memory of the infected device.
Central Business District of NYC, and it must be considered that a New York commuter wastes 73 hours a year being stuck in the road traffic [4].
City administrators do care public safety. However they might not consider that it should pass through some hardware and software security as well.
For example, there are well known traffic regulation devices vulnerabilities. If “properly” exploited (possibly by the means of a new Mirai flavour), they could lead to traffic lights malfunctioning, or even deliberate sabotage, aimed at causing riots and incidents with obvious negative consequences and direct impact on people’s health, up to injuries or death. This scenario might sound hypothetical, but it’s pretty realistic. By looking at it through the ADS Risk Analysis Framework\(^5\), the major threat raised here is the T 0.41 “Sabotage” [5].
The assessment ranks the risk related to this threat as CRITICAL, considering a catastrophic economic and reputational impact, even if the likelihood is not very high (the threat agent must have noticeable skills).

A CRITICAL risk should be mitigated by:
- programming emergency interventions;
- immediate implementation of containment measures and implementation of strategic best practices;
- immediate activation of the monitoring channels focused on the threat.

Sources:
  https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html
[5] BSI Threats Catalogue

---

\(^4\) Data projection on road traffic in New York City during the period 1990-2011 (“2012 Sustainable Streets Index”, New York City Department of Transportation).

\(^5\) The ADS Risk Analysis Framework evaluates impact and likelihood from a quantitative perspective.