On line privacy in US

EU is paying its attention to privacy and many Cloud providers are deploying datacenter in Europe following our rules. In this region all the companies are working on providing the compliance with the new General Data Protection Regulation (GDPR), but what is happening in US in these days? Federal Communications Commission (FCC), last year, setups new privacy rules that are requiring, to the Internet providers the obligation to obtain subscribers’ consent before sharing data on such activity as browsing history and app usage. Yesterday in all the newspaper we received information that House of Representatives voted to reverse Obama-era regulations preventing Internet service providers from selling your web browsing history on the open market.

This means that the Internet provider will be free to sell your data without your opt-in permission. In this scenario for the US citizens the only possibility is take their online privacy into their own hands. Many analysts and activists wrote that the abolition of these rules it would be only the first step towards the progressive deregulation of the Internet. Even the organizations Electronic Frontier Foundation (EFF), speaks about the danger of being controlled in every aspect of our digital lives. Internet providers will be able to sell all these data to financial agencies, marketing companies and in general to companies engaged to analyze and use this information for commercial purposes: activities out of the user control and that the user does not know. Moreover, it seems, that the measures approved by Congress with a mechanisms under the Congressional Review Act push FCC in a corner, preventing it from returning to establish rules on the same subject. In this scenario Virtual Private Network (VPN) tools start to be present in many blog and web pages promising you the net anonymity. This solution won’t fix completely the privacy issue, but is decent start. VPN may be a good privacy tool even if it has limitations. For example, using a VPN, you might find that you can’t connect to all the sites and services you normally use. Moreover you have to trust your VPN provider that doesn’t track you and sell your data itself. To have an idea and start, you may have a look to the EFF web site https://www.eff.org/deeplinks/2016/09/liv-e-eff-tools-help-you-protect-yourself-online.

Of course, the impression is that placing the burden of privacy entirely on consumers, US Congress is effectively conceding it has no good solution for protecting US citizen privacy, the public need to keep fighting for maintaining privacy and freedom on the net. We need also to understand what will happen over this year and consequences toward EU and this kind of approach. Another point that GCSEC adds on its activity is monitoring the privacy item.

Nicola Sotira
General Manager GCSEC
The Internet Revolution has radically changed the way of diffusing and exchanging information. While on the one hand the so-called Big Data and the huge amount of news available on the web have given the majority of people the possibility to access to many sensitive data, on the other hand have complicated the validation process of any knowledge that can be obtained from the web.

The constant research for information capable to give the decision-maker a grounded point of view on a specific situation, fundamental to help him taking the right decision, has been the principal activity of the intelligence (as in the film "The three days of the Condor", where is described the role of an information analyst). Nowadays the analyst role has become essential for private companies, which need information on competitors and business, and for reporters, that must take advantage of every possible knowledge to conduct significant and important inquiries.

In the digital era collecting and analyzing information constitutes the main task of the cyber intelligence, which can be divided in different categories depending on the object of analysis: HUMINT (Human Intelligence), SIGINT (Signals Intelligence), IMINT (Imaginary Intelligence), OSINT (Open Source Intelligence) and MASINT (Measurement and Signature Intelligence).
Since more than the 80% of the information are freely accessible on the web, the OSINT activities, thanks to operators able to identify, treat and extract information from high amount of data, become essential both for public and private organizations. Many kind of sources can be analyzed, as an example we may cite the mass media (newspapers, magazines, radio and television) and the public data (government's reports, financial plans, demographics data and press conferences), moreover direct examination (photographs, satellite observations) and data supplied by some expert (conferences, lectures, scientific publications) can be sources susceptible to be examined. The analysis of these sources is crucial to strengthen specific knowledge in support of a major decision.

One of the first official OSINT definition comes from 1994 CIA's Director of Central Intelligence Directive, through which it has been created the Community Open Source Program Office (COSPO): "Open Source information for purposes of this directive in the publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access.

Open source information also includes any information that may be used in an unclassified context without compromising national security or intelligence source and methods. If the information is not publicly available, certain legal requirements relating to collection, retention, and dissemination may apply ".

The more recent definition given by the Journal of US Intelligence Studies states: "The term OSINT is defined as the collection, processing, analysis, production, classification, and dissemination of information derived from source and by means openly available to and legally accessible and employable by the public in response to official national security requirements".

As asserted on the NATO Open Source Intelligence Handbook, concerning the open sources it’s necessary to make a distinction between the available types and the processes, Open Source Data (OSD): internal documents, audio-video recordings, images, debriefing and other primary sources; Open Source Information (OSI): secondary raw data or already structured ones, results of the analysis process of the OSD, usually available in the form of specialized reports, newspapers, books, blogs and news sites; Open Source Intelligence (OSINT): information obtained after searching, selecting and distributing to a select audience; and finally Validate Open Source Intelligence (OSINT-V): information that has been given a high degree of certainty, the final product object of comparisons with classified and proprietary information to which can be attributed the higher level of adherence to reality.

The reliability and validity of the obtained information depends on data comparison or on the instruments used for research. According to a British Armed Forces technique, adopted also by other NATO’s countries, each intelligence assessment receives an alphanumeric evaluation that reflects the source reliability and the credibility of the information. In addition to the Surface Web (Google, Bing, Yahoo) that represent only 4% of the virtual world, it is interesting to look at the so-called Deep web or the Dark web, which contains an entire anonymous world, accessible through free software (Tor, I2P and Freenet).

To help the work of the analysts, specific tools used to perform online targeting investigation have been created. To better clarify, we present a brief list of those instruments: Search Engine and Metasearch are privacy, security and causing economic and reputation damage. To prevent and deal with such threats, experts will come together to exchange views on some dimensions of the highest relevance: Cyber Security, Cyber Defense, Cyber Espionage and more. An important Round Table will involve the highest institutional offices to profile scenarios and provide solutions in order to unify the global response to the Cyber Crime through collaboration between states. The new DPCM on cyber security defines and attributes to the Director General of the DIS the lines of action that will ensure the necessary levels of security systems and of strategic networks, both public and private, checking and eliminating vulnerabilities.
Given a set of observations, it should formulate a hypothesis, consult information that can help validate or refute the hypothesis and derive a conclusion based on evidence.

**Cyber-Attack on ABTA Website Puts Thousands at Risk**

goo.gl/viJFHw

News has surfaced today that a cyber-attack on the website of the Association of British Travel Agents (ABTA) could potentially have impacted as many as 43,000 people. As explained in a statement on the company’s website, it is believed that those behind the attack (which occurred on 27 February) gained access to about 1000 files which may include personal identity information on customers of ABTA Members, the majority of which are email addresses and encrypted passwords, relating to complaints made about ABTA staff. ABTA CEO, Mark Tanzer, said: “We recently became aware of unauthorized access to the web server supporting abta.com by an external infiltrator exploiting a vulnerability. The web server is managed for ABTA through a third party web developer and hosting company. The infiltrator exploited that vulnerability to access data provided by some customers of ABTA Members and by ABTA Members themselves via the website. “We immediately notified the third-party suppliers of the abta.com website who immediately fixed the vulnerability. ABTA immediately engaged security risk consultants to assess the potential extent of the incident. Specialist technical consultants subsequently confirmed that the web server had been accessed.”

**Ransomware Cost Businesses $1bn in 2016**


Ransomware continues its dominance as the most lucrative criminal business model in the history of malware, costing businesses upwards of $1 billion in 2016. According to KnowBe4’s 2017 Endpoint Protection Ransomware Effectiveness Report, antivirus solutions have a marked inability to protect against ransomware. About 33% of respondents have experienced a ransomware attack in the past 12 months; out of those, 53% had deployed multiple solutions against ransomware but still became victim to it. And about half (48%) of the total number of respondents (72%) who had downloaded KnowBe4’s ransomware simulator, RanSim, were not able to detect the simulator’s behavior, despite their antivirus deployments. “Ransomware is primarily delivered via a phishing email, which means your users have to be trained to identify it in order to prevent it, making antivirus ineffective at stopping ransomware,” said Stu Sjouwerman, CEO of KnowBe4. “It’s a simple concept—if users can learn not to click the link or open the attachment they won’t infect their workstation with ransomware!"
From field to "cyberlaundering" - The "Agromafie" Threaten Network Security
An interview with Gian Carlo Caselli President of the Centre's Scientific Committee on crime in the food industry
by Massimiliano Cannata - Technology innovation, training and security culture Reporter

The turnover "agromafioso", has grown from 16 billion to 21.8 billion (official 2016 data) with an increasing of 30%; this gives us an idea of the severity of the phenomenon. The crime abandoned the "military clothes" to dress "white collars", to take advantage of globalization and the Finance 3.0. This sector is very attractive, because in addition to the inadequacy of the laws there is the ubiquity of its different articulations.

Gian Carlo Caselli, Public Prosecutor and President of the Centre's Scientific Committee on crime in the food industry can boast decades of experience in the fields of fight against organized crime and terrorism. In this interview addresses the hot topics of Agromafie Report, in its fifth edition, founded on the initiative of the Eurispes President Gian Maria Fara and realized in collaboration with Coldiretti.

Mr. Caselli, the agribusiness is a growing business for the crime. What should scare us more?

First, we should consider capacity of mafia to change skin; treating the phenomenon, according to the patterns we have followed in recent decades, could be a mistake. Nobody wants to deny the historical origins of a peculiar phenomenon of our southern territories, which over the years proved capable of expand in the Center and in the North of Italy. But today, what's really scary is the "silent mafia": it proliferates by adopting operating ways totally different from the past. In order to understand the ongoing transformation process, just think of the Cyberlaundering phenomenon, the recycling of dirty money on line.

What does it exactly mean?

It means that the "new" mafia doesn't extort money to the supermarket or car showroom owners rather becomes its business partner or takes over in toto the activity to "clean up" money for laundering. The new criminality uses Internet like an accelerator. Once, the mafia obtained mainly their revenue with exploitation and violence on territory requiring money to return "protection", today it become a "entrepreneur" that operates on virtual routes. The objective of laundering is to remove the money from its origins through a series of operations aimed to obstruct traceability of the origin of the proceeds. Internet amplifies the distance between the launderer and capital, making more complex investigation into suspected subjects.

What are the consequences of this radical change?

They are obvious: the concept of mafia and "mafioso" were expanded up to encompass other territories that require to update the regulatory framework in accordance with the "new" crime that is hidden behind the boards, holding companies, international funds, consulting firms, as well as not infrequently happens, behind the formal screen of politics and institutions.

From Kalashnikov to virtual networks

What is characterizing the strategy adopted by the criminal organizations in the food industry that demonstrate this extraordinary skills in handling the new technologies?

On the agribusiness side, another parallel economy is growing. In the Cyberlaundering hypothesis, the activity is reduced to a single virtual dematerialized operation, where laundering phenomenon can find the ideal conditions to develop itself. The organized crime is quickly passed to the world of technology, from Kalashnikovs to more sophisticated weapons like botnets, networks that control tens of thousands of computers and that can be used to attack companies and organizations on the network.

These are delicate operations, which imply the ability to put together different profiles and skills. We are in front of a new generation, as well as of methods and strategies, is it a "quantum leap" of the new organized crime?

Internet and the Web are allowing organized crime in each country to push the boundaries of its activities, providing opportunities and prospects until now unimaginable. It caused a transformation of the profile and identity of the "old mafia". It is important to note that the web is a "free zone" able to guarantee security and anonymity, a "gray area" where to commit criminal activities. In the new scenario, the networks security becomes an important aspect to contrast a criminal strategy without borders and that is becoming increasingly threatening.

The criminality demonstrates its ability to penetrate in the new markets. This is unprecedented fact, what do you think about that?

In fact this is what is happening. Mafia has an unexpected vocation to marketing. After leaving the organization and management of many forms of exploitation to "workers", mafia today affects the market, setting the prices of harvest
crops, controlling the transport and supply of entire supermarket chains, handling. Mafia exports our true or false Made in Italy, establishes overseas production plants of Italian sounding, and creates ex novo retail marketing networks.

Network security as a strategic contrast asset

It refers to the so-called “liquid mafia”?

This is the most appropriate definition to capture the attitude of the mafia to penetrate everywhere, just like water. The “mafiosi” adopting various stratagems, obtain conspicuous European funding. Just remember that the Italian Guardia di Finanza has confiscated 137 lands and identified 29,689 lands of persons belonging to organized crime; and they have also seized assets for 150 million euro value and 35 million euro of undue findings.

The innovations do not stop there. The High Frequency Trading is the other term, the key with which we have to contend. Can you please describe it in a nutshell?

This is another instrument available to the organized crime, which allows quickly exchanges in the Stock Market, operated in automatic way based on algorithms. These are speculative transactions based on the moving of sums of money to affect the performance of the Stock Exchange. We are facing high technological instruments that put high frequency orders in the Stock in a short time; it could overcome 5,000 orders per second. A sort of “automatic insider trading” where it is difficult to identity operators.

In fact, how do criminals operate?

Through the High Frequency Trading, banks and financial companies act simultaneously on different regulated platforms, such as Stock Exchanges, or, as happens more often, without any control, such as Over the counter (Otc), realizing profits of merely speculative nature. Taking advantage from the speed of operations execution, they can enter, edit and delete millions of orders a day, playing on the minimum price differences between selling and buying, and closing all positions by the end of the day.

Once again, are there the speed and control of the networks on the base of these illegal actions?

The focal point is precisely the speed: algorithms, ever more complex, "see" the orders of a title, made by competitors in different markets, and in that short period of time between the instant in which the order is entered and that in which it appears in the so-called order book of each market, i.e. in electronic prospectus which contains the proposals of sale and purchase, with quantity, price and operator – flood the markets of orders, researching the same title on other platforms, and closing the trading at a cheaper price. These thousands of orders therefore have the only one purpose of rising up or down the price of the stocks; these are then erased, after completion of negotiation, in as many fractions of a second. The speed is such that the control bodies of different countries estimate that only 10% of orders placed with the High frequency trading is brought to an end; the remaining 90% is erased.

Which initiatives should be taken to contrast so sophisticated and articulated phenomena?

The complexity of the network of criminal has reached very high levels. Our effort, in this phase, is concentrated in the activity of mapping the penetration of criminal activities in the food chain, in order to identify a "Permeability Index" that can help us to better understand the points of fragility of our territory to launch more effective prevention and protection activities up to date. We are now facing a transnational problem, but the Supervisory Authorities are national, so none of them can have a complete overview of the activities Hft operators. It is evident the need to orchestrate investigative strategies based on a transnational intelligence, to prevent risks and vulnerabilities, which shall include effective cyber security strategies. From the centrality of the fight against mafia, could descend a horizon of freedom for our country. We are facing a game we can’t lose.