# Masterclasses Program

Cybersecurity Summer BootCamp 2017

## Cybersecurity Summer BootCamp 2017

18-29 July - León (Spain)

www.incibe.es/en/summer-bootcamp

Organised by:

GOBIERNO DE ESPAÑA · MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA OAS

With the collaboration of:

universidad de León

AYUNTAMIENTO DE LEÓN

León Cuna del Parlamentarismo

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

Santander

IDB Inter-American Development Bank

EUROPOL EC3 European Cybercrime Centre

INTERPOL

# SPEAKERS

Luis Fernández

Francisco J. Rodríguez

Antonio Sepúlveda

## Detection of cybercriminals in the dark ... and in the light

Tuesday, July 18th 2017
12:15 – 13:10
Auditorium City of León


**Abstract**

The purpose of this paper is to explain how from INCIBE we detect cybercrime in the dark, that is, crimes committed by criminals under the protection of the anonymity provided by the networks in the DeepWeb.

To achieve the objective, three key factors are combined: the power of technology development for task automation, applied research in fields such as Artificial Intelligence and the end-user experience of the Law Enforcement Agencies.

It will be described how an artificial vision algorithm allows to label services within the most popular of these networks, TOR; How the crime categorization is performed automatically, how the relevance of these hidden services is established, or how a child is automatically detected and identified in an image hung from a forum.

Likewise, it will be exposed the fact that not all crimes occur in the darkness of anonymity. Examples of detection of nearer cybercrimes will be described, crimes that occur on the Internet and that seek clarity to increase the number of victims.

# SPEAKERS

Alejandro López Parra

Javier Berciano

## WannaCry and Petya: the most mediatic ransom-worms

Tuesday, July 18th 2017
13:10 – 14:05
Auditorium City of León


**Abstract**

Seminar on the recent global cyber attacks WannaCry and Petya that are the ones with more media impact in recent years.

Their background, technical and impact data as well as comparative data will be discussed to highlight their similarities and differences.

Special emphasis will be placed on what has happened in Spain as well as the operations deployed by INCIBE and the actions carried out by the CERT.

# SPEAKERS

Simón Roses

## Software & Hardware Made for Pentesting

Wednesday, July 19th 2017
16:00 – 17:30
Auditorium City of León


**Abstract**

This talk will cover some of the latest software & hardware devices that pentesters can use to test their clients security from physical to digital attacks.


Raúl Siles

## WhatsApp End to End Encryption Demystified

Wednesday, July 19th 2017
17:30 – 19:00
Auditorium City of León


**Abstract**

WhatsApp finally implemented end to end (E2E) encryption last year. This talk will perform an overall review and in-depth look at the technologies involved in that implementation, and more specifically, the Signal protocol. The Signal cryptographic protocol is becoming the de-facto standard and widely adopted reference for secure (instant) messaging solutions, such as WhatsApp, Signal (TextSecure), Google Allo, Facebook Messenger, etc.

The goal of the talk is to explain the history, evolution, design, security properties and features, technical aspects, numerous keys and cryptographic components of this complex modern protocol, plus other associated algorithms and protocols, trying to facilitate its understanding to non-cryptographers... ;o)

# SPEAKERS

Adolfo Rodriguez de Soto

## *Artificial Intelligence and Cybersecurity: an unavoidable alliance*

Wednesday, July 19th 2017
19:00 – 20:00
Auditorium City of León


**Abstract**

The application of Artificial Intelligence (AI) to various fields is experiencing a second youth, especially thanks to the development of deep learning techniques that have, in a short time, become the benchmark solutions to many problems in which the results obtained by the machines were not comparable to the performance achieved by the human being. This has made possible to extend its scope and it has several consequences on Cybersecurity.

The relationship between Artificial Intelligence and Cybersecurity can be said to be of mutual need. On the one hand, the expansion of AI-based solutions will lead to the use of many more automatic systems in previously unfeasible places, with more systems likely to be attacked with serious consequences. The development of the autonomous car is a good example. But in general the Internet of Things (IoT) will cause the creation and constant use of automatic controls that can be hacked and many of them will be complex systems whose functionality will be achieved thanks to AI techniques. Thus, cybersecurity must be concerned with the special nature of these systems, some of which have mechanisms of operation quite difficult to explain. Moreover in some cases the implications that can be derived from an unwanted modification are not as simple to analyze and explain as traditional software systems can be.

On the other hand, cybersecurity should take advantage of AI methods to achieve more useful tools in solving their classic problems. AI can help, and is already a reality in some cases, to detect attacks, or to detect intruders, or at least to filter scenarios. The ability of new attacks to adapt to established security measures may be limited if those security measures are sufficiently skilled to be transformed or masked in turn.

This double relationship and expectation of mutual help is what will be exposed in this conference, showing cases of application and future lines of work..

# SPEAKERS

David Barroso

## False flag operations: looks can be deceiving

Thursday, July 20th 2017
16:00 - 17:30
León Oeste Auditorium


**Abstract**

Attribution is hard. And it's hard not only because there are usually very few clues about the origin of an attack, but many attackers are using false or fake pieces of information in order to try to blame other attacker. In the military world, it is common to find these false flags operations and nowadays we are seeing how they are used in the digital realm. In this presentation we'll describe specific examples of how some nation states and criminal groups are using these false flag operations in their daily operations.


European Cybercrime Centre
EC3 - EUROPOL

## Uncovering connections: Malware and virtual currencies

Thursday, July 20th 2017
17:30 – 18:30
León Oeste Auditorium


**Abstract**

The fight against malware attacks and the abuse of virtual currencies are two top priorities for law enforcement agencies worldwide. This masterclass will provide an overview of the services and analytical products that Europol/EC3 can deliver to the Member States in the fields of malware analysis and virtual currency investigations. It will also demonstrate how these products are nowadays used as an instrument to investigate crimes and prosecute the perpetrators. Best practices and law enforcement challenges, opportunities and techniques will also be shared through concrete case examples.

# SPEAKERS

Horacio J. Azzolin

## Follow the white rabbit. Lessons Learned from Cybercrime Research

Thursday, July 20th 2017
18:30 – 19:30
León Oeste Auditorium

**Abstract**

Cybercrime investigators face some challenges, related to the digital environment in which it produce.
How do you research in the internet? How can we found evidence in a scenario that favors anonymity?
How do you obtain evidence when you need to apply to agencies located in other countries? What are the problems we face today and those that will touch us in a more or less near future?
How is a case constructed under these conditions, respecting due process?
This and other issues will be dealt with from the work experience of the UFECI, the cybercrime unit of the Attorney General of the Argentine Republic.

Colin Weherill

## Protecting the World's Nervous System - Global Cyber Intelligence-Sharing and Collaboration)

Thursday, July 20th 2017
19:30 – 20:00
León Oeste Auditorium

**Abstract**

Abstract to be defined.

# SPEAKERS

Belisario Contreras

## Cyber-security, terrorism and crime. Are we prepared in Latin America?

Friday, July 21st 2017
16:00 – 17:00
León Oeste Auditorium

**Abstract**

The talk will introduce generalities on the concept of cybersecurity, as well as the use of the internet for terrorist and criminal purposes. During the presentation there will be an analysis of how prepared the region is to deal with these threats.

Carlos Álvarez

## The DNS as an attack vector

Friday, July 21st 2017
17:00 – 18:00
León Oeste Auditorium

**Abstract**

The Domain Name System (DNS) was intended to make it easier for humans to use online resources without the need to memorize complex numerical or alphanumerical addresses. From an operational perspective, the DNS is a distributed infrastructure operated by thousands of entities, most of which are not related to one-another. From a purely technical perspective, the DNS is a protocol that is part of the TCP/IP suite of protocols.

And, although the resources that are part of this immense infrastructure are mostly operated by persons or entities for legitimate and legal purposes, and although the protocol was designed for benign purposes (to make life easier for users), criminals have –for years– given creative uses to existing vulnerabilities in both the protocol as well as to resources that are part of the DNS as a global system.

The session will cover issues related to the DNS as a vector to attack third parties (malware distribution, botnet command and control, phishing, pharming, exfiltration or planting of information), as well as attacks against the DNS itself.

# SPEAKERS

Javier Candau

## Cyber-threat and the challenge of sharing

Monday, July 24th 2017
16:00 – 17:00
INCIBE building


**Abstract**

Cyber threats in 2017 are evolving rapidly, highlighting the transfer and publication of information / exploits unknown by manufacturers and with a spectacular ability to control infected computers and colonization of target networks, which were initially in the domain of the states (considered cyber-weapons) and that now by negligence or with deliberate intention is available to any attacker. This scenario, as shown by WANNACRY and PETYA, has modified the rules of the game. Security managers face the challenge of sharing to quickly address these new attacks.

Threats, whether arising from cybercrime, cyberspaming or cyber-sabotage, are increasingly taking advantage of the slowness of exchanging between the different players on the defensive side. However this scenario is changing; The exchange standards are consolidating, more and more trust groups are being created for an agile exchange of information, although we still have challenges to overcome such as the treatment of classified information, the exchange of information between governments and the private sector (especially security companies that provide services and convert that information into money), gain the confidence of private security professionals in different sectors and define automated channels based on trust and willingness to share.

# SPEAKERS

Omar Cruz

## *Leveraging Cyber Threat Intelligence for CSIRTs*

Tuesday, July 25th 2017
16:30 – 17:30
INCIBE building

**Abstract**

During the course of responding to cyber security incidents, Cyber Threat Intelligence (CTI) has enabled CSIRT Analysts to gain a better understanding of the cyber threat actor's Tactics, Techniques and Procedures (TTPs) as well as the level of risk that such incidents represent to their organization. This presentation will cover how CSIRT Analysts can leverage CTI during major cyber security incidents, as well as lessons learned and best practices for leveraging CTI..

José Antonio Vázquez Tain

## *Cybercrime and Justice: Are We Ready?*

Wednesday, July 26th 2017
16:00 – 17:00
INCIBE Building

**Abstract**

The varied and changing criminal phenomenology that is included in the so-called cybercrime, offers a very specific problem, not only technological, but also a legal approach, both substantive and procedural. While the various crimes that are discussed in, or through cyberspace, increase and proliferate, the justice response is usually not even up to the meritorious work of the police forces. The paper tries to detect the shortcomings of our judicial system to give an adequate response to these new modalities of attacking the rights of citizens.

# SPEAKERS

Prof Michael Goldsmith

## *Assessing National Cybersecurity Capacity Maturity*

Thursday, July 27th 2017
16:00 – 17:00
INCIBE building

**Abstract**

As a leading international centre for research on efficient and effective cybersecurity capacity building the Global Cyber Security Capacity Centre (GCSCC) has created the Cybersecurity Capacity Maturity Model for Nations (CMM), the first-of-its-kind model to review a country's cybersecurity capacity maturity across five dimensions: cybersecurity policy and strategies, cybersecurity culture, knowledge development, legal and regulatory frameworks, and risk controls. Together with key strategic international partners, such as the World Bank, the Organization of American States (OAS), the Commonwealth Telecommunications Organisation (CTO), and the International Telecommunication Union (ITU), the Capacity Centre has since 2015 successfully deployed the CMM in 18 countries around the world, and significantly underpinned a regional study in Latin America and the Caribbean through collaboration with the OAS.

In this session, Prof Goldsmith will outline the comprehensive approach that the CMM is taking, its structure (including dimensions, factors and their respective indicators), and how it is applied by the Capacity Centre and its partners. He will also provide observations from its global deployment and how those insights may inform national cybersecurity-capacity development.

Manuel Guerra

## *Forensics in the 21st Century*

Friday, July 28th 2017
16:00 – 17:00
Auditorium City of León

**Abstract**

The seminar will present the new techniques in the field of computer forensics and will deepen the workflows in the treatment of digital evidences, so that this treatment is carried out in the most appropriate way possible.

# SPEAKERS

César Lorenzana

## *Digital transformation in police investigation*

Friday, July 28th 2017
17:00 – 18:00
Auditorium City of León


**Abstract**

There is no doubt that the society in which we live has undergone a profound transformation and in the last few years passed from the analogical era to the digital one, and we are at the gates of a new era .... the information era. These changes, patented on the day of one day have had their reflection in the field of police investigation. So, just as companies have to manage a quantity of data to make their business profitable and optimize their processes, more and more data are being collected by police investigations that must be analyzed and treated correctly for them.
With the current capabilities, the analysis of the information is done semi-automatically, which entails a slowness and complexity that causes that the investigators do not face the presentation of the evidences in the judicial seat in the time and the form that they allow to be Used in the cause, since the time of the instruction has been reduced with the recent modification of the LeCrim. This is why it is necessary to update both tools and the work processes in which they are used.
Throughout the presentation will present the current challenges that suppress the management of information and the need to adapt the police standards to take advantage of current technologies in data processing to increase police effectiveness.


Mikel Gastesi

## Adventures and misfortunes of the threat researcher

Friday, July 28th 2017
18:00 – 19:00
Auditorium City of León


**Abstract**

In this talk we will see how one security researcher can analyse a malware analysis campaign. From an initial malware analysis to the gathering of the most interesting information, we will take a walk across several steps that will cause a big headache to the analyst..

# SPEAKERS

Jaime Kindelan

Fernando Díaz

## The 1%. Control of Tor exit nodes

Saturday, July 29th 2017
10:00 – 11:00
Auditorium City of León


**Abstract**

This paper provides a different point of view about the control of our infrastructures from the perspective of the attackers which are hidden behind the Tor network.
Over the past few years Tor was not only used to provide anonymity and freedoms to legitimate users, but has also provided protection to attackers and cybercriminals.

In this talk we try to expose the necessary resources to perform an effective monitoring of the network for statistical purposes, giving the possibility of an early attack detection that may influence our assets.

Bot attacks, Cybercriminals, Cyberwar, Intelligence, suspicious behaviours...

# SPEAKERS

Adrián Acosta

## Interpol and the transnational cybercrime challenge

Saturday, July 29th 2017
11:00 – 12:30
Auditorium City of León

**Abstract**

Abstract to be defined.

María Elvira Tejada

## *Response of the rule of law to cybercrime: The international adaptation and harmonization of the legal systems of States and the strengthening of international cooperation.*

Saturday, July 29th 2017
12:30 – 14:00
Auditorium City of León

**Abstract**

The impact that the impressive development of information and communication technologies is having on the field of crime is unquestionable. The widespread use of technological tools has determined the emergence of new behaviors - until now hardly imaginable – that, by seriously affecting the rights of people or the general interest, deserve to be subject to prosecution and criminal penalties. In addition, the possibility of acting against these behaviors developed in cyberspace also requires technological tools that make it feasible to investigate criminal acts and the persons responsible for them, without limiting or restricting the principles and values that constitute the Foundation of the rule of law.

The response to this situation requires a major effort on the part of multiple sectors of society. It is imperative to gradually adapt national legislation to the needs of action against these new challenges, following the internationally agreed parameters and seeking an adequate harmonization with the legal systems of the remaining States. As it is also essential to strengthen the tools of international cooperation, because the transnational character of these behaviors inescapably determines a coordinated action with the competent authorities of other countries. And the collaboration of private sector and citizens is also essential, given the transversal nature of these behaviors and their development and expansion through systems often available to non-public bodies and entities.

The objective of the intervention is to analyze the new challenges posed by the fight against crime that is planned and developed in cyberspace and the mechanisms that are being articulated from the rule of law, both nationally and internationally, to provide adequate responses that are effective and contribute to ensuring the rights and freedoms of citizens, the security of States and that of the International Community as a whole.