CURRICULUM VITAE

Ferran Pichel Llaquet
+34 XXX XX XX XX
XXXXX (Barcelona – SPAIN)
ferran.pichel@foosec.com
http://foosec.com

Work Experience

Cyber-Threat Researcher at **Intel471** - September 2017 – Present

http://www.intel471.com

Member of TechIntel team. Intel 471 provides an actor-centric intelligence collection capability for the world's leading cyber threat intelligence teams. Our intelligence collection focuses on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber attacks.

Tasks:

- I+D+i in Cyber Threats Intelligence
- Internal DevOps within the team
- Malware analysis and code review

Cyber Threat Analyst at **Blueliv** - March 2014 – August 2017

http://www.blueliv.com

Blueliv is the Cloud-based Cyber Threat Intelligence technology that protects organizations from a range of threats including, credit card fraud, data and credentials theft, phishing, botnets, malicious mobile application, APTs and the latest malware trends.

Tasks:

- I+D+i in Cyber Threats Intelligence
- Source-Code security review
- Malware analysis

Co-Founder at **Iniciativa Biotec, S.L** - December 2015 – December 2018

http://www.iniciativabiotec.com

Iniciativa Biotec is a company located in Spain. Its mission is to improve public and private health-care services by approaching them all the new technologies and applications of the DNA studies.

IT Security Engineer at **Applus+LGAI** – January 2012 – March 2014

http://www.appluslaboratories.com

Main duties are to analyze and test IT devices/software in order to certificate in Common-Criteria. All phases of the development are analyzed. Projects are about 6 months, so you can analyze all the internal documentation, functionalities and architecture. Finally you test the device functionalities and do some Vulnerability Analysis in order to break the device/software.

Tasks:

- Common-Criteria management
- Logical Infrastructure Manager, according to Common-Criteria security requirements
- Protection Manager
- Common-Criteria evaluation and review
- Research on IT Security

Co-Founder at **Section9 Security, AG** – January 2011 – January 2012

http://section9security.com

Swiss company dedicated to e-crime and IT-security services.

IT Security Analyst at **Internet Security Auditors, S.L.** - July 2006 – January 2012

http://www.isecauditors.com
Internet Security Auditors is founded in mid 2001 with the aim to be the supplier of independent security who would needs any company offering its services globally from its offices in Barcelona and Madrid.

Tasks:

- Penetration Testing
- Web Applications Hacking
- R+D
- Scripts Development
- Task automation
- Security Analysis

@RROBA Magazine at **Megamultimedia, S.L.** – October 2004 – May 2007

http://www.megamultimedia.es
Technical and scientific publications among others.

Published Articles:

Year 2007	**Cross-Site Scripting**: Description and examples of Cross-Site scripting attacks.
Year 2006	**Basic Game Hack**: Memory alteration using 'ptrace' C function. **OS infection using java Applets**: Commands execution in user's OS using java Applets. **Bypassing a Captcha**: Captcha bypass using Bresenham's line algorithm. **Port Knocking**: Technical description and examples of PortKnocking technics. **VNC authentication bypass**: Technical description of VNC NULL authentication vulnerability. **Bug in Internet Explorer**: Technical description of 'window' bug in Internet Explorer.
Year 2005	**3com 812 Office router. Weakness of many innocents**: Exploiting tftp for fun and profit. **phpBB & Chown exploitation:** Description of phpBB_highlight and chown_gid vulnerabilities. **Rootkits**: Some examples of how to guarantee and hide the access to a server. **Practical Hacking**: 'hackerslab.org' wargame instructions, not the solutions. **Basis of Buffer Overflow Exploiting (part I)**: How to exploit some BoF example codes. **Basis of Buffer Overflow Exploiting (part II)**: How to exploit some BoF example codes. **Getting root access**: Description of some tricks to get root access. **Custom IP header steganography**: Description and example of IP Header steganography.
Year 2004	**John the Ripper**: Description of every option of the program John The Ripper. **Linux Backdoors**: Examples and analysis of different backdoors for Linux.

Education

Graduated in IT Engineering, (5 years degree) – 2004 - 2010
At Universitat Autònoma de Barcelona

Final Project (with honors): "Automated Anti-Malware Platform"

Description
This paper describes the analysis, design and implementation of the new automatic platform service offered by Internet Security Auditors, SL. It is designed to analyze Internet domains in order to detect possible infections that could affect the user's system while browsing the web. The current system has some shortcomings and this paper presents a new version, which provides significant improvements such as optimal management, with a renewed design in the management of the information and processes. It also gives the system a centralized error handling, with a real-time alarm delivery, and results in grouping and pooling.

Link to the document: http://hdl.handle.net/2072/43463

Certified Ethical Hacker (CEH), I.T. Security - 2008

At Internet Security Auditors Training

Certified Ethical Hacker (CIEH) is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council).

First Certificate in English (FCE) - 2003

At Barcelona

First Certificate in English (FCE) is one of the exams available from University of Cambridge ESOL examination. Its possession proves one's adequacy in the English language, and its successful completion means that one is able to interact socially efficiently.

Additional Information

Published Advisory **Yet another security issue with WhatsApp** – 2013

WhatsApp advisory published in 14-Nov-2013 about an internal side effect - as they said - that may provoke, among others, a DoS against the application and information disclosure as well, everything without any kind of human interaction with the device. Already solved in version 2.11.134

Source: http://foosec.com/docs/whatsapp.html

Published Advisory **Multiple Vulnerabilities in Zyncro** – 2011

Some XSS, SQL Injection and design fails.

Source: http://seclists.org/fulldisclosure/2011/Sep/230

Finalist with Int3pids team to **Defcon Contest in Las Vegas**. – 2011

Defcon in Las Vegas is one of the most important security events in the worldwide. I went with Int3pids to collaborate with them.

Collaboration with Sexy Pandas team in **Defcon pre-quals**. – 2008, 2009

In order to go to Las Vegas you must be classified into the top ten in pre-quals.

Attendance at **Chaos Computer Congress** (CCC) in Berlin – 2006

CCC is one of the most famous security events in Europe.

English skills:

- Understanding
  - Listening: Independent User (B2)
  - Reading: Independent User (B2)
- Speaking
  - Spoken Interaction: Independent User (B2)
  - Spoken Production: Independent User (B2)
- Writing: Independent User (B2)

Other languages:

- Mother tongue
  - Catalan
  - Spanish