

Ismael Briones Vilar
Shepherds Bush Road
London, W67LU, London, UK
Mobile: +44 757 679 6559
+34 654 751 182
Email: ismael.briones@gmail.com

Education

- **University of Valencia (Spain)**
 - BS Technical Engineer of Telecommunications (Electronic Systems)

Professional Experience

Senior Incident Respond Manager

European Commission – Cyber Attack Response Team, CSIRT

Government Agency; 10,001+ employees; International Affairs industry
February 2011 till date

CART, Cyber Attack Response Team, is the CSIRT for the European Commission and it's an important player of the Commission's Security Directorate. It provides Cyber Security Incident Response Services to the Commission, being the single point of contact among affected internal organizations. CART was created in 2010, but due to the significant increase of cyber attacks on the European Commission, it was necessary to restructure and expand the CSIRT.

Working as CART Incident Respond Manager, I'm responsible for enhancing and expanding the current CSIRT team. This includes development, refinement and implementation of policies, processes and procedures for responding to cyber security incidents. European Commission is a large institution: ~50k users, so we usually have to work closely with other internal European Commission institutions and external entities such law enforcements, NSA and other CSIRTs.

Some of my I.R. Manager responsibilities are:

- Provides the single point of contact among affected internal organizations and between them and any affected or concerned external entities such law enforcements, NSA and other CSIRTs.
- Develops, validates, and improves incident response plans and procedures.
- Manage all aspects of notification, handling, resolution and reporting of cyber security incidents.
- Support the technical response to security incidents, performing evidential level acquisition and forensic analysis, ensuring that we apply the basic EU principles and standards to protect EU Classified Information.
- Write incident reports.

Other technical responsibilities:

- Enhance the forensic laboratory in term of software and hardware: XRY mobile forensic, Forensic Box with Write blockers(Tableau T3458is Forensic bridge), FTK3, HBGary Responder Pro
- Conduct digital forensic analysis involving APT (Advanced Persistent Threat) intrusions and cybercrime incidents.

- Performed advanced static (reverse engineering) and dynamic malware analysis, related to APT investigations, to extract forensic artifacts.
- Advanced application and use of Forensic toolsets (FTK3, Sleuth Kit (TSK) & Autopsy, XRY mobile forensic, foremost/scalpel, Write Blocker Tableau T3458is Forensic bridge), logs analyzer: Splunk
- Conducted memory analysis using Volatility Framework, HBGary Responder Pro/Digital DNA
- Advanced application an use of Reverse Engineering toolsets (Ollydbg, WinDBG, IDAPro, HBGary Responder Pro)

Senior Malware Researcher

Panda Security

Privately Held; 1001-5000 employees; Computer Security industry
November 2003 – February 2011 (2 years 2 months)

Company Profile: Panda Security is a global leading provider of IT security solutions, with millions of clients in more than 200 countries and products available in 23 languages. Panda Security mission is to develop and supply global security solutions to keep their clients' IT resources safe from the damage inflicted by viruses, intruders and other Internet threats.

- **Job Responsibilities:**
 - Analyze (reverse engineer) malware: virus, trojans, rootkits and vulnerabilities.
 - Design and develop, in Python, a system to classify malware, based in their internal structure. (Presented at Virus Bulletin Conference, Ottawa 2008)
 - Design and develop tools to analyze malware, using different programming/scripting languages: Python, Perl, C/C++/C#.
 - Penetration testing, including web application penetration testing.
 - Vulnerability assessment and exploit development of 0-Day vulnerabilities.
 - Set up and run computer malware forensics: FTK.
 - Reverse Engineering with IDA Pro and debuggers: WinDBG and OllyDBG.
 - Network protocols analysis: TCP/IP Networking (Wireshark).
 - Design and develop Snort Preprocessor to detect and block high obfuscated protocols like Skype.
 - Develop new Honeypots systems and distribute them in several countries.

Senior Malware Researcher

Virustotal

Privately Held; 10-50 employees; Computer Security industry
June 2009 – December 2010 (1 year 6 months)

Company Profile: Hispasec Sistemas is a technical lab specializing in information security and technologies. Since 1998, our team has focused on researching data protection problems and offering corrective and/or preventive solutions. VirusTotal is a service developed by Hispasec Sistemas that analyzes suspicious files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and web analysis toolbars.

- **Job Responsibilities:**
 - Senior contract for design and develop, in Python and Perl, a multi-threading and distributed system to analyze URLs with several web analysis toolbars, using MySQL as the backend database.

- Actually the system is analyzing 9500 urls/hour with 6 URL engines: Google Safebrowsing, Firefox, GData, Pareto Logic, Opera and Phishtank.
- URL: <http://www.virustotal.com>

Senior System Administrator

El Mundo / www.elmundo.es

Privately Held; 201-500 employees; Newspapers industry
September 2000 – November 2003 (3 year 3 months)

Company Profile: El Mundo is a young newspaper (1989) but has a lot of popularity in Spain. Investigative Journalism made that paper famous in the 90's. Now it is well positioned in the market with a strong view on design, graphics, type and illustration. All Department areas are integrated with Internet from 2008.

- **Job Responsibilities:**

- Installation, configuration & administration of Clustered Linux Server (with OS/Application level clustering & Load balancing) including management of web site. Installation and troubleshooting Linux Operating Systems and Server.
- Management of various services like DNS, MySQL and PostgreSQL databases. Design, implementing and Managing LAN & WAN.
- Installation, configuration and troubleshoot of MySQL server which includes creation, maintenance and administration of users and databases in MySQL server and back up and restoration of databases. Migration development and replication server data as needed.
- Installation, configuration & administration of Linux Servers. Maintain & Manage various services running in Linux system which include apache web server, proxy server, mail server, network file server, routers and firewall.
- Managing NAS Servers (NetApp F710 y F810)
- OpenSwan VPN, PPTP, L2TP and PPP configuration.

Systems and Security Administrator

Amutis Telecomunicaciones S.A.

Privately Held; 10-50 employees; Computer Security industry
January 2000 – September 2000 (9 months)

- **Job Responsibilities:**

- Installation, configuration and administration of Linux Servers.
- Management of various services like DNS, MySQL, PostgreSQL, Apache, Qmail and Samba.
- Security Consultancy: ISO 17799 Security Standard

Specialties

Cyber-security Incident Response, Digital Forensics, Malware Analysis, Reverse Engineering.

Skills

- Computer Forensics
 - AccessData FTK3
 - HBGary Responder Pro/Digital DNA
 - Volatility Framework
 - Sleuth Kit (TSK) & Autopsy
 - XRY mobile forensic
 - File carving foremost/scalpel
 - Write Blocker Tableau T3458is Forensic bridge
- Reverse Engineering
 - ASM x86
 - IDA Pro
 - WinDBG
 - OllyDBG
 - Hiew
- Vulnerability Scanners
 - Nessus
 - Nmap
 - Retina
- Programming:
 - Perl
 - Python
 - PHP
 - C/C++/C#
 - SQL
 - Bash Shell
- Linux, Windows Administration
- Apache
- Databases:
 - MySQL
 - PostgreSQL
- Qmail
- Intrusion Detection System:
 - Snort IDS
- Firewalls and Policy Routing
 - Iptables
- TCP/IP Networking, QoS, VPN, PPTP, L2TP, IPv6, DNS, DHCP, SNMP, SNTP

Publications and Meetings

Virus Bulletin

September 2008

Speaker at Virus Bulletin Ottawa

Title: Graph, Entropy and Grid Computing: Automatic Comparison of Malware

- <http://pandalabs.pandasecurity.com/archive/Back-from-VB2008.aspx>
- <http://www.virusbtn.com/conference/vb2008/abstracts/Vilar.xml>

Certifications

- **SANS Institute**
 - GIAC Reverse Engineering Malware (GREM)
 - Stay Sharp Master Packet Analysis (SSP-MPA)

Researches

I've discovered the following vulnerabilities:

- Skype (3.6.0.248 and older) Security Bypass Vulnerability
 - <http://www.securityfocus.com/archive/1/493081>
 - <http://www.skype.com/security/skype-sb-2008-003.html>
- Trend Micro SSAPI Long Path Buffer Overflow Vulnerability
 - <http://www.securityfocus.com/archive/1/469300>
 - <http://www.inkatel.com/index.php/2007/09/16/trend-micro-ssapi-long-path-buffer-overflow-vulnerability/>
- NOD32 Antivirus Long Path Name Stack Overflow Vulnerability
 - <http://www.securityfocus.com/archive/1/469300>
 - <http://www.inkatel.com/index.php/2007/05/20/nod32-antivirus-long-path-name-stack-overflow-vulnerability/>
- Oracle 8.1.5 CHOWN Path Environment Variable Vulnerability
 - <http://www.securityfocus.com/bid/3129>
 - http://otn.oracle.com/deploy/security/pdf/dbsmp_alert.pdf
- Vulnerability in 3Com OfficeConnect Remote 812 ADSL Router
 - <http://www.securityfocus.com/bid/4841>