
Ismael Briones Vilar

Personal/Contact Information

- **Phone:** +0034 654 751 182
- **Email:** ismak@inkatel.com
ismak@uninet.edu
ismak@member.fsf.org
- **Birth Date:** April 12, 1977

Education

Technical Engineer of Telecommunications (Electronic Systems)
University of Valencia (Spain)

Languages

Spanish: Native

English: Medium-High level

Profesional Experience

- **Panda Security** (Bilbao-Spain) November 2003 - Present
As a Malware Researcher I'm involved in vulnerability analysis, Windows/Unix security and malware research.
Malware dissassembling is one of my daily works and I'm involved with HoneyPot research, development and research of new proactive techniques to fight and detect malware, automatization for malware analysis, research of new Rootkits techniques and anti-rootkits technologies...
I work with tools like SoftIce, OllyDBG, IdaPro and the following programming languages: C, C++, Perl, Python
Other skins and tasks are:
Intrusion Preventium/Detection System research
Proactive and reactive protection systems
Dissassembling and debugging techniques of malware (IDA, SoftIce, OllyDBG)
Honeypots/HoneyNets/SpamTraps
IDS signatures development (Snort Engine)
- **El Mundo** (Madrid-Spain) September 2000 - November 2003
I was involved in maintenance and development the systems and network infrastructure of the Internet site of this spanish journal.
The high availability was one of our first goal so we deployed a farm of about 15 linux system working together.
I was involved in the following tasks:
Perl, Python, PHP and bash scripting development.
Routers Cisco (3660, 7206 VXR)
Alteon AceDirector switches / WebOS (AD3 y AD4)
SAN Network Storage (NetApp F710 y F810)
IDS (Snort)

- **Amutis Telecomunicaciones, S.A.** (Valencia) Enero 2000 - Septiembre 2000
Network and System Administrator (Linux: Red Hat, Debian, Solaris 7 and OpenBSD)
shellscript, perl, c, php, python
Security Consultant (Telefonica Spain, Oncology Research Center of Valencia)
- **AIMPLAS (Technological Institute of Plastics (Valencia))** October 1999 - January 2000
6 months research fellowship
ISO 17799 (Security Policies)
Network and System Administrator (Linux: Red Hat, Debian, Solaris 7 e Irix)
shellscript, perl, c, php, python

Skills

• Vulnerabilities Research

- **Skype File URI Security Bypass Code Execution Vulnerability**
[Idefense Advisory](http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=711): <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=711>
[Skype advisory](http://www.skype.com/security/skype-sb-2008-003.html): <http://www.skype.com/security/skype-sb-2008-003.html>
- **Trend Micro SSAPI Long Path Buffer Overflow Vulnerability**
[Idefense Advisory](http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=586): <http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=586>
[Technical advisory](http://www.inkatel.com/index.php/2007/09/16/trend-micro-ssapi-long-path-buffer-overflow-vulnerability/): <http://www.inkatel.com/index.php/2007/09/16/trend-micro-ssapi-long-path-buffer-overflow-vulnerability/>
- **NOD32 Antivirus Long Path Name Stack Overflow Vulnerabilities**
[Bugtraq Advisory](http://www.securityfocus.com/archive/1/469300): <http://www.securityfocus.com/archive/1/469300>
[Advisory](http://www.inkatel.com/wp-content/uploads/2007/05/Advisory.txt): <http://www.inkatel.com/wp-content/uploads/2007/05/Advisory.txt>
- **Oracle 8.1.5 CHOWN Path Environment Variable Vulnerability**
[Bugtraq Advisory](http://www.securityfocus.com/bid/3129): <http://www.securityfocus.com/bid/3129>
Oracle Official Advisories
http://otn.oracle.com/deploy/security/pdf/dbsmp_alert.pdf
- **Vulnerability in 3Com® OfficeConnect® Remote 812 ADSL Router**
[Bugtraq Advisory](http://www.securityfocus.com/bid/4841): <http://www.securityfocus.com/bid/4841>
- **Intrusion test in an International Bank environment (BBVA)**
Danger SQL Injection vulnerability detected
- **Intrusion test in an International Bank environment (La Caixa)**
Danger Web access to Database Customer Information

• Technical Knowledge

- Unix (Solaris, Linux, OpenBSD)
- Windows 2003, XP, 2000, NT
- C, C++
- Perl, PHP, Python, Ruby, shellscript
- MySQL, PostgreSQL, Oracle
- DNS(Bind 8,9), Apache Web Server, Mail servers (qmail, postfix)
- Firewalls (CheckPoint FireWall-1, Iptables)
- Policy Routing
- QoS, Ipsec, IPv6

- Snort IDS (Intrusion Detection System)
- Load balance and High disponibility systems (24/7/365). Alteon AceDirector switches
- Cisco Routers (3660, 7206 VXR)
- SAN Network Storage

Publications and meetings

• Virus Bulletin

- **Speaker at Virus Bulletin Conference 2008 (Ottawa)**
Graph, entropy and grid computing: automatic comparison of malware
Abstract: <http://www.virusbtn.com/conference/vb2008/abstracts/Vilar.xml>
VB2008 Programme: <http://www.virusbtn.com/conference/vb2008/programme/index>

• UniNet

- **Member of UniNET (University network of Services IRC and Telematics)**
<http://www.uninet.edu>
- **I Unix Meeting (Umeet2000) Organizing Comittee member**
<http://umet.uninet.edu>
- **I Unix Meeting (Umeet2000) speaker**
Security Programming (Buffer Overflows)
- **II Unix Meeting (Umeet2001) Organizing Comittee member**
El Mundo, Spanish Journal
- **II Unix Meeting (Umeet2001) speaker**
Arp Spoofing: Spying in switched networks
Doc: [PDF](#), [PS](#)
- **III Unix Meeting (Umeet2002) Organizing Comittee member**
- **III Unix Meeting (Umeet2002) speaker**
An Introduction to User-Mode-Linux
Doc: [PDF](#), [PS](#)
- **I IPV6+Firewall+Encrypt+VPN Meeting (6FEVU) Organizing Comittee member**
<http://www.uninet.edu/6fevu/>
- **I Computer Security Meeting (InfoSec 2002) Organizing Comittee member**
<http://infosec.uninet.edu/>
- **II Computer Security Meeting (InfoSec 2002) Organizing Comittee member and speaker**
<http://infosec.uninet.edu/>
- **Arroba Spanish Computer Security Journal**
 - **Nº 44: Arp Spoofing**
<http://www.inkatel.com/new/textos/Arroba/arp-spoofing.pdf>
 - **Nº 66: Sniffing in Network Wireless**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=66&idnot=tema3>
 - **Nº 67: Hack Zones y Wargames**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=67&idnot=tema3>

- **Nº 70: Portscanning (July 2003)**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=70&idnot=tema3>
 - **Nº 71: DoS, DDOS, DRDOS (August 2003)**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=71&idnot=tema1>
 - **Nº 72: Linux Privilege Escalation (September 2003)**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=72&idnot=tema3>
 - **Nº 73: Network Data Interception: Sniffers (October 2003)**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=73&idnot=tema2>
- **El Mundo Spanish Journal**
 - Campus Magazine (El Mundo): **UniNet: Una 'médula espinal' para las universidades**
(UniNet: Spinal Marrow for the Universities)