



Máquinas trampa: Conoce a tu enemigo

Urko Zurutuza

Mondragon Unibertsitatea

Miramón Enpresa Digitala, Donostia, 18/03/2010



ÍNDICE

INTRODUCCIÓN

DETECCIÓN Y RESPUESTA ANTE INCIDENTES
¿QUÉ ES UN SISTEMA TRAMPA?


TIPOS DE SISTEMAS TRAMPA

THE HONEYNET PROJECT RESEARCH ALLIANCE

ORGANIZACIÓN
PROYECTOS RELEVANTES

EUSKALERT: RED VASCA DE HONEYPOTS

ARQUITECTURA
RESULTADOS

A close-up photograph of a hand holding a small, rectangular piece of light-colored paper. The paper is held between the thumb and index finger, with the middle and ring fingers visible behind it. The word "INTRODUCCIÓN" is written on the paper in a bold, black, hand-drawn font. The background is a soft, out-of-focus green and yellow, suggesting an outdoor setting. The lighting is bright and even, highlighting the texture of the paper and the skin of the hand.

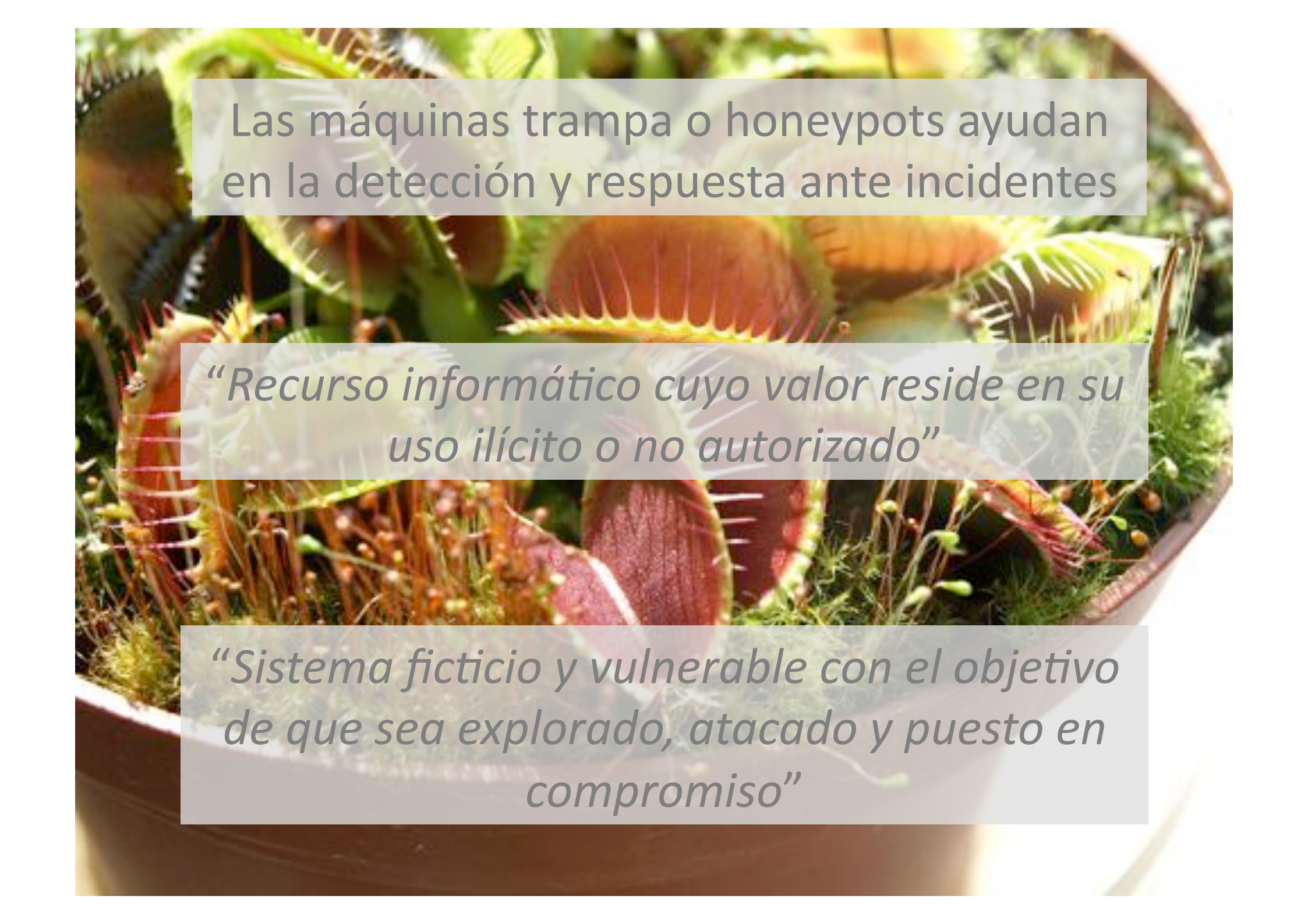
INTRODUCCIÓN



Dificultad para analizar los métodos
y técnicas de atacantes

Detección y respuesta ante Incidentes: Logs y más logs





Las máquinas trampa o honeypots ayudan en la detección y respuesta ante incidentes

“Recurso informático cuyo valor reside en su uso ilícito o no autorizado”


“Sistema ficticio y vulnerable con el objetivo de que sea explorado, atacado y puesto en compromiso”



No tiene ningún valor productivo en la organización

No debería recibir ningún tipo de tráfico

Cualquier interacción es al menos sospechosa

A close-up photograph of a hand holding a small, rectangular piece of off-white paper. The paper is held between the thumb and index finger of the right hand, with the middle and ring fingers also visible. The word "TIPOS" is written on the paper in a bold, black, hand-drawn font. The background is a soft, out-of-focus green and yellow, suggesting an outdoor setting. The lighting is bright and even, highlighting the texture of the paper and the skin of the hand.

TIPOS

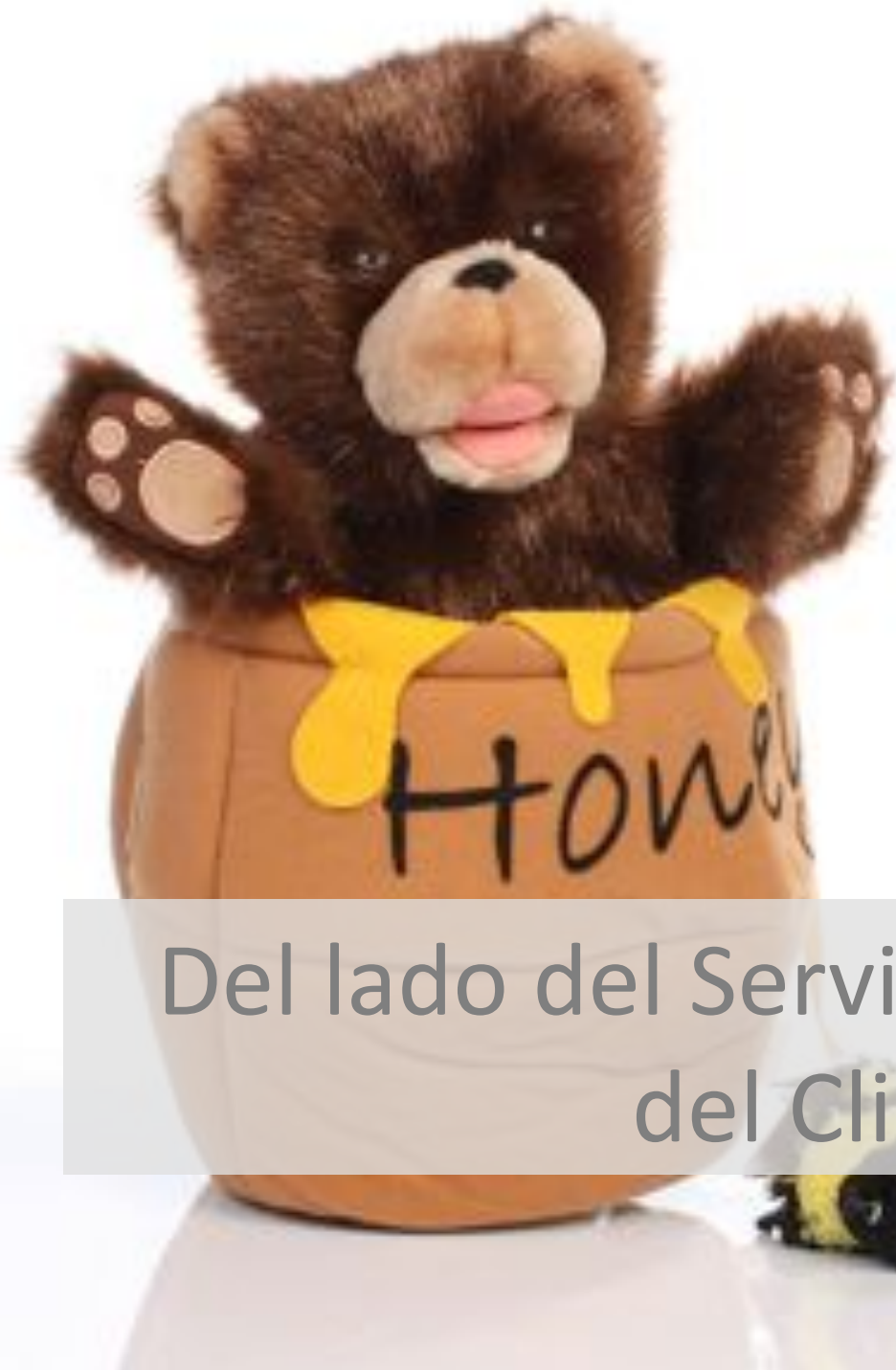
Alta Interacción Vs. Baja Interacción



- *honeyd*
- *nepenthes*
- *Amun*
- *honeytrap*
- ...



Máquinas Reales Vs. Máquinas Virtuales



- *Capture HPC*
- *HoneyC*
- *phoneyc*
- *MonkeySpider*
- ...

Del lado del Servidor Vs. del lado
del Cliente



HONEYNET
PROJECT

A photograph of three women of different ages, representing three generations. The woman in the foreground is young with long brown hair. The woman in the middle is middle-aged with long brown hair. The woman in the background is older with short white hair. They are all looking slightly to the right. The image is overlaid with semi-transparent grey boxes containing text labels for each generation.

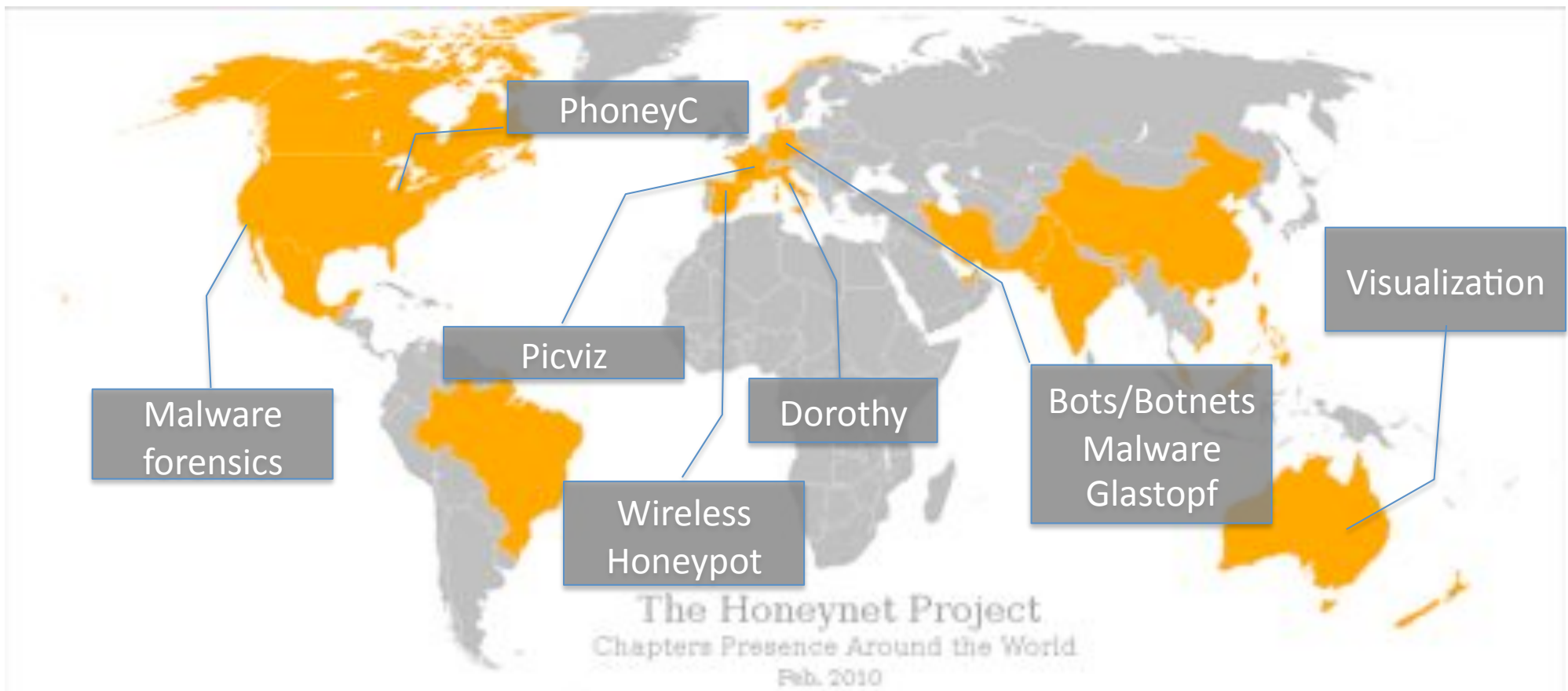
Gen I
Honeynets

Gen II
Honeynets

Gen III
Honeynets

The HoneyNet PROJECT®

Grupos distribuidos en el mundo
Cada grupo debe hacer algo diferente
Compartir las lecciones aprendidas



EUSKALERT



- Home**
- Noticias
- Estadísticas
- Resultado Encuestas
- Descargas
- FAQ

Iniciar Sesión

Nombre de usuario:

Contraseña:

Recordarme

[¿Recordar contraseña?](#)

[¿Recordar nombre de usuario?](#)

Usuarios en Línea

Tenemos 7 invitados conectado(s)

Compartelot



Euskalert - Red Vasca de Honeypots

El proyecto Euskalert se encuentra en su segunda fase. Se trata de una fase de ampliación de la red y, al mismo tiempo, de difusión de algunos de los resultados sobre la actividad en los sensores de la red en este sitio web.

Los países de origen de los ataques del último mes:



Los 5 mayores atacantes del último mes:

IP	Country	First Seen	Last Seen	Total hits
80.32.66.229	Spain	2010-03-08 11:05:00	2010-03-10 14:30:09	23
75.109.227.188	United States	2010-03-08 15:12:48	2010-03-08 15:21:34	8
193.65.205.70	Finland	2010-03-05 10:35:18	2010-03-10 13:45:58	8
82.87.64.180	Romania	2010-03-10 09:54:07	2010-03-10 09:54:09	8
115.43.208.242	Taiwan, Province of China	2010-03-08 08:28:30	2010-03-08 08:28:35	6

Los 5 ataques más habituales del último mes:

Nombre	Last Seen	Total hits

Intentos de accesos Vía FTP:

"RMD sarcaxxo"

"PASS ."

"USER administrator"

"PASS NULL"

"MKD 090713182104p"

"CWD /public/"

"PASS Pgpuser@home.com"

"USER anonymous PASS ftp@example.com PWD EPSV PASV CWD pub PASV CWD publicPASV CWD pub CWD incoming PASV CWD incoming PASV CWD _vti_pvt PASV CWDupload PASV QUIT"

Ataques / pruebas vía HTTP:

GET /twiki/bin/statistics HTTP/1.1 Accept: */* Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Toata dragostea mea pentrudiavola Host: ***.***.***.49 Connection: Close

OPTIONS / HTTP/1.1 translate: f User-Agent:Microsoft-WebDAV-MiniRedir/5.1.2600 Host: ***.***.***.61 Content-Length: 0 Connection: Keep-Alive

GET /roundcube/program/js/list.js HTTP/1.1 Accept: */* Accept-Language:en-us Accept-Encoding: gzip, deflate User-Agent: Toata dragostea mea pentrudiavola Host: ***.***.***.49 Connection: Close

GET/unauthenticated/..%01/..%01/%01/..%01/..%01/..%01/..%01/..%01/etc/passwdHTTP/1.1 Accept: */* Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Toata dragostea mea pentru diavola Host: ***.***.***.49 Connection: Close

POST /webmail/bin/html2text.php HTTP/1.0 Host: ***.***.***.69 User-Agent:Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2)Content-length: 54 Accept: ZWNobygiU3VjY2VIZGVkISA6KSIcclxuXHJcbi4iKTsK{\$ {EVAL(BASE64_DECODE(\$_SERVER[HTTP_ACCEPT]))}



Máquinas trampa: Conoce a tu enemigo

uzurutuza@eps.mondragon.edu

Mondragon Unibertsitatea

Miramón Enpresa Digitala, Donostia, 18/03/2010