

HONEYPOTS



Alberto Doblado Vera

Houston Symonel Charles Sosa

Nuestro proyecto consiste en la creación y monitorización de un honeypot, una gran herramienta para IDS (Intrusion Detection System). En este caso se ha utilizado **T-Pot**.

Y para conseguir monitorizar la mayor cantidad de ataques durante este tiempo hemos montado un T-Pot en México que ha estado funcionando durante las dos últimas semanas, y 2 T-Pots en España, uno de ellos con todos los puertos abiertos a modo de prueba durante un día y otro con 5 puertos abiertos durante una semana que ha recibido pocos ataques.

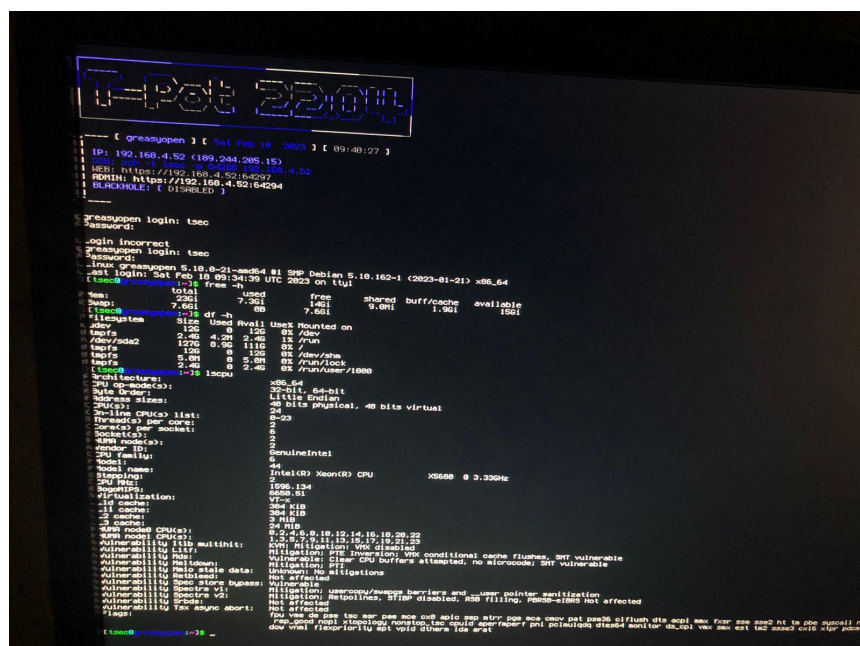
A continuación procedemos a explicar la instalación de un sistema T-Pot, en este caso el creado en **México**.

Se utilizó un servidor Dell R610 con 24 GB en ram, 128 GB HDD y procesador Intel Xeon x5680 de 3.33 Ghz con 24 núcleos.


Se instaló **tpot_amd64.iso** descargado de GitHub <https://github.com/telekom-security/tpotce> y booteado utilizando la herramienta rufus y una memoria usb.

Se establecieron 3 accesos durante la instalación:

SSH puerto 64295
Sysadmin web puerto 64294
T-POT web puerto 64297



Se procedió a establecer una IP fija para el servidor en un router con **PfSense** para poder crear las reglas de port forwarding según los puertos deseados usando una tabla de servicios y puertos del sistema T-Pot.



COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ pfSense ▾

Firewall / NAT / Port Forward

?



















































Port Forward


1:1


Outbound


NPT


Rules


<input type="checkbox"/>		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.4.52	443 (HTTPS)	tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	64297	192.168.4.52	64297	web tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	64294	192.168.4.52	64294	admin tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	64295	192.168.4.52	64295	ssh tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.4.52	80 (HTTP)	tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	110 (POP3)	192.168.4.52	110 (POP3)	tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	995 (POP3/S)	192.168.4.52	995 (POP3/S)	tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	143 (IMAP)	192.168.4.52	143 (IMAP)	tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	993 (IMAP/S)	192.168.4.52	993 (IMAP/S)	tpot	  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	21 (FTP)	192.168.4.52	21 (FTP)	tpot	  

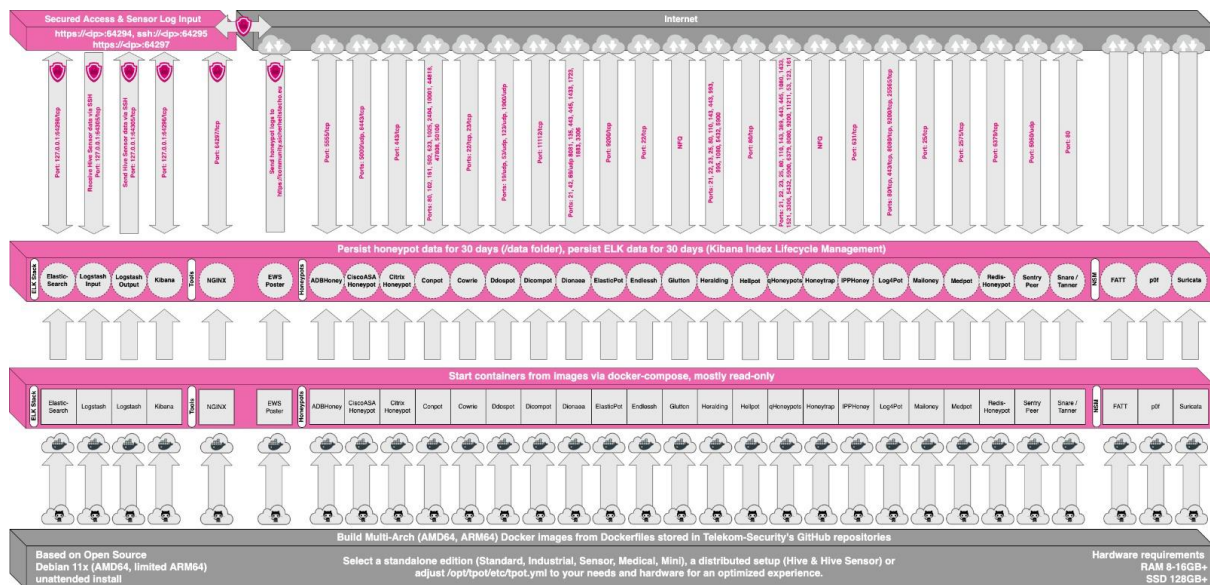
 Add

 Add

 Delete

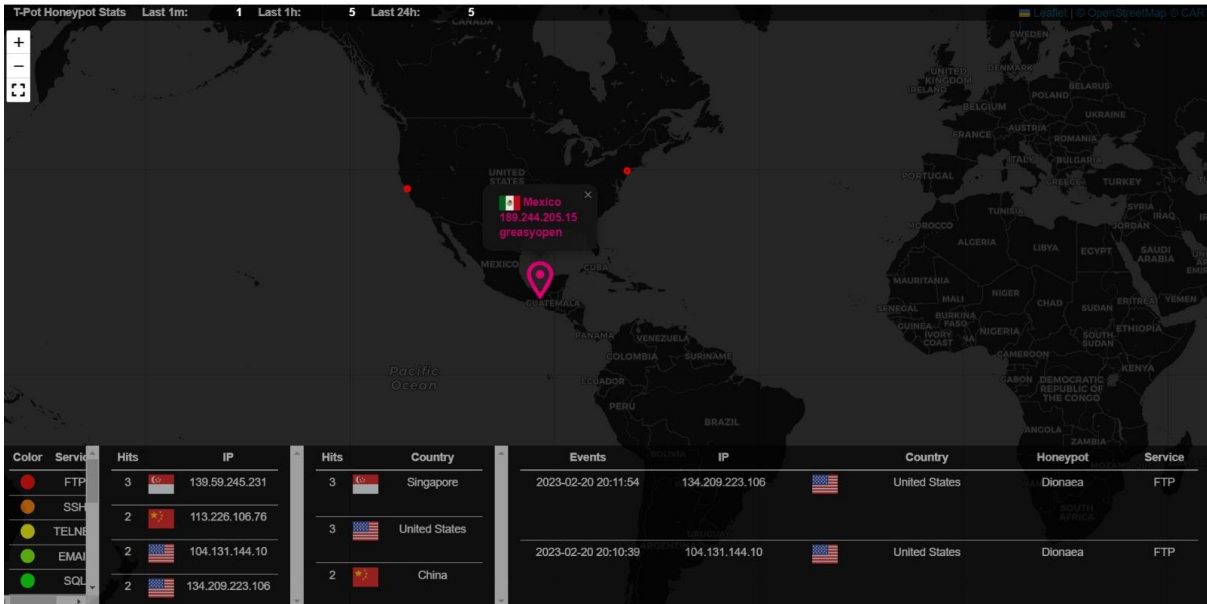
 Save

 Separator



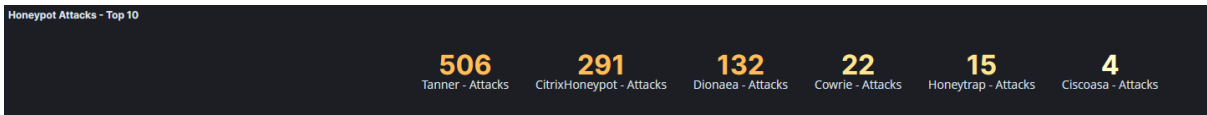
Una vez configurado el firewall comprobamos el funcionamiento del sistema

En la imagen se puede ver que el servidor ha quedado correctamente configurado desde el dashboard de mapa de ataques en tiempo real.



Recopilación de datos de los T-Pots utilizados:

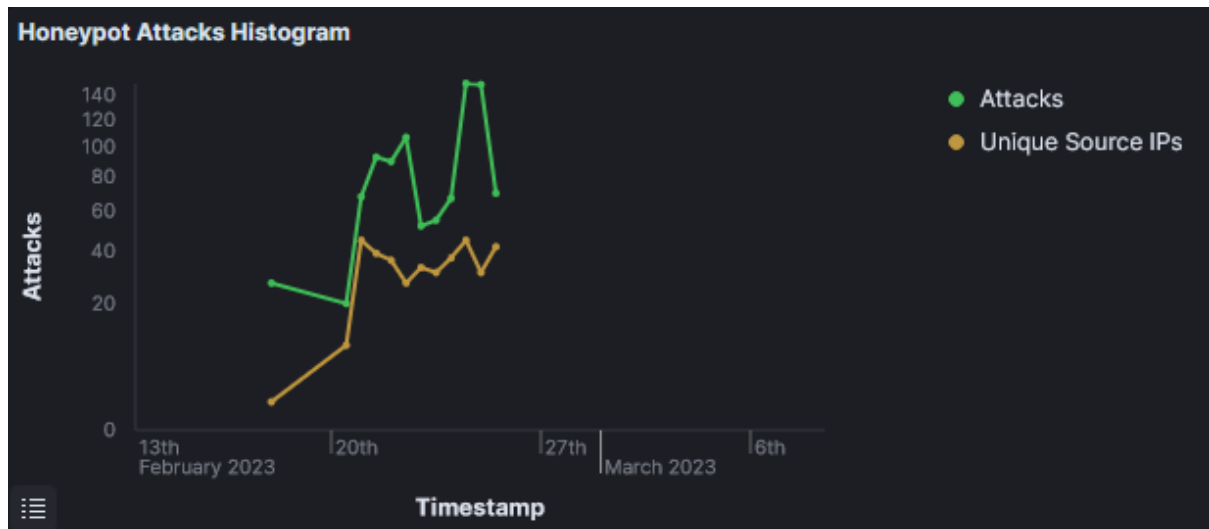
En el T-Pot montado en **México** hemos recopilado los siguiente datos.



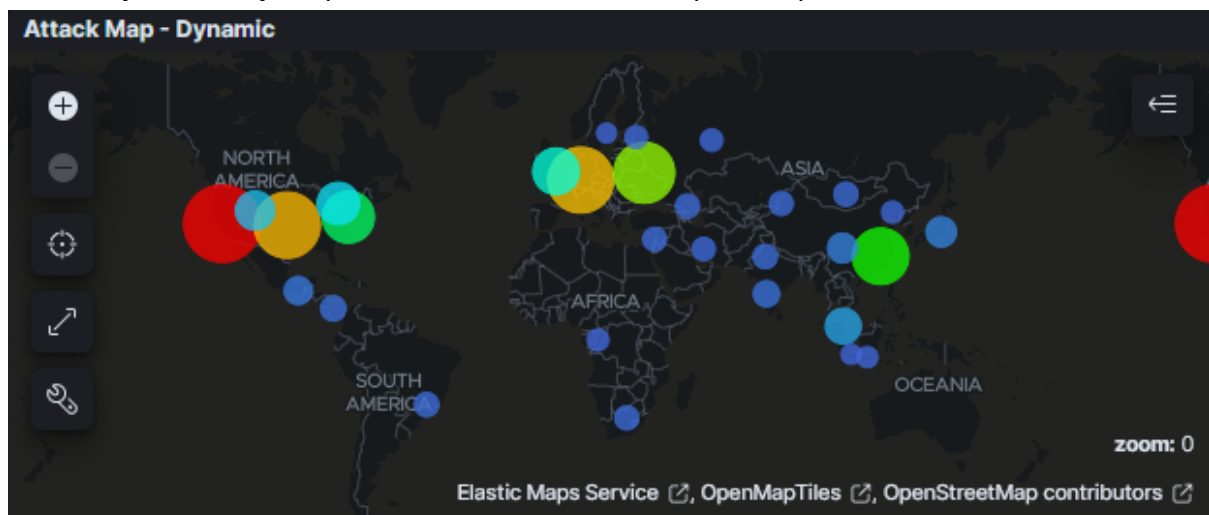
En el Top 10 de los Honeypots atacados nos encontramos con un total de **970 ataques** repartidos entre ellos, siendo **Tanner** el que más ha recibido y **Ciscoasa** el menos atacado.



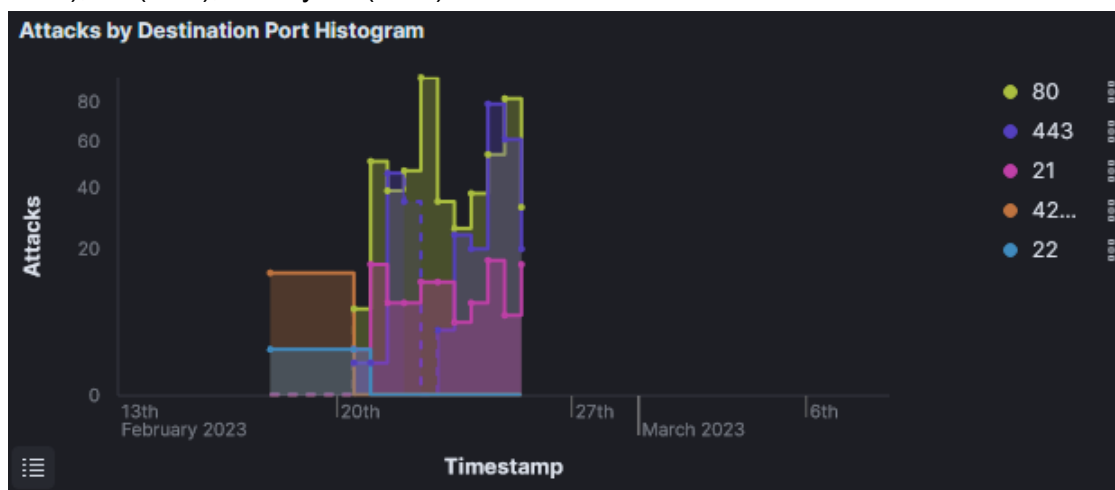
En cuanto al **mayor pico de ataques** recibidos fue el día 24 de febrero a las 12:00 con un total de **150 ataques** desde **45 IPs**



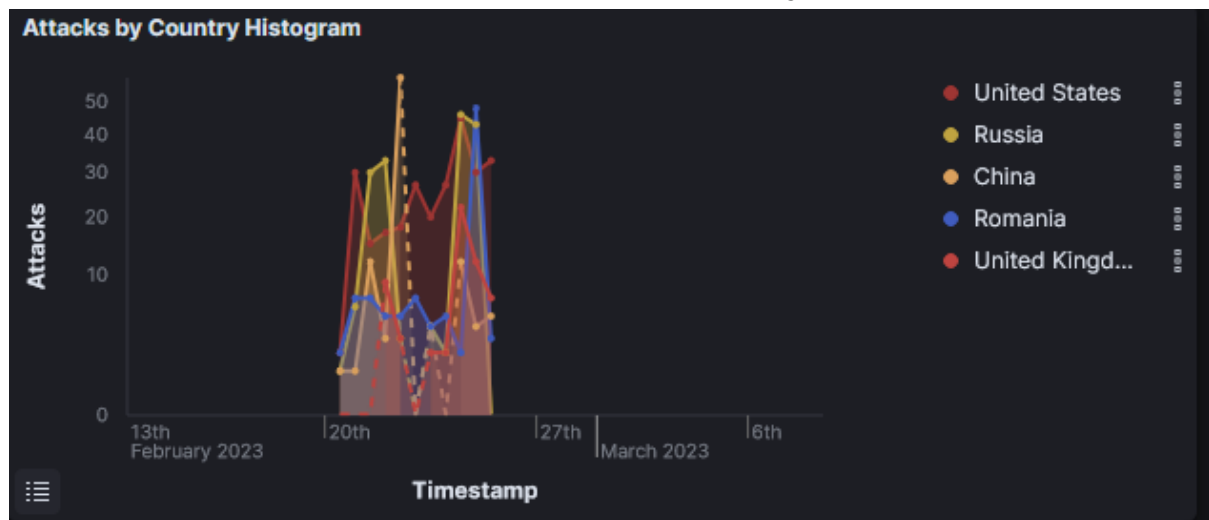
En el **mapa de ataques** podemos ver la cantidad de países que nos han atacado.



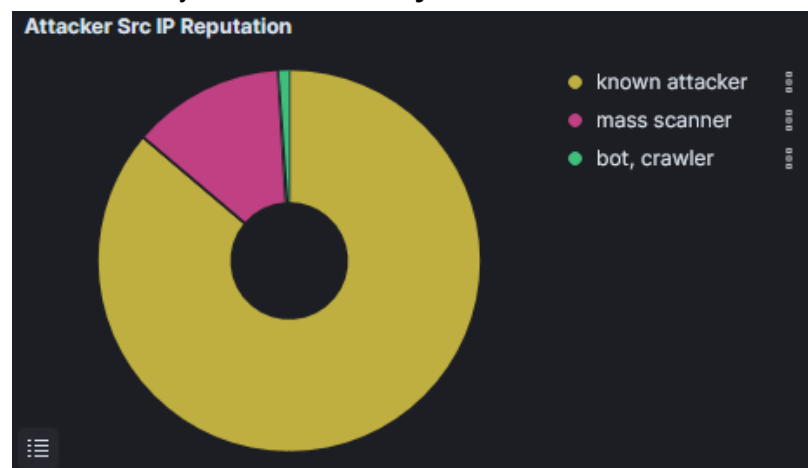
En cuanto a los **puertos que más ataques han recibido** se encuentran el **80** (HTTP). **443** (HTTPS), **21** (FTP), **4297** y **22** (SSH).



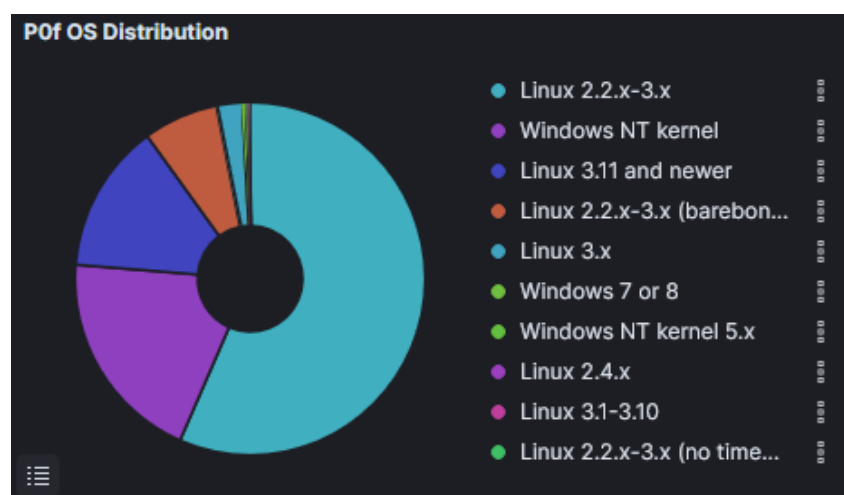
Los **países que más nos han atacado** ordenados de mayor número de ataques recibido a menor han sido: **Estados Unidos, Rusia, China, Rumanía y Reino Unido.**



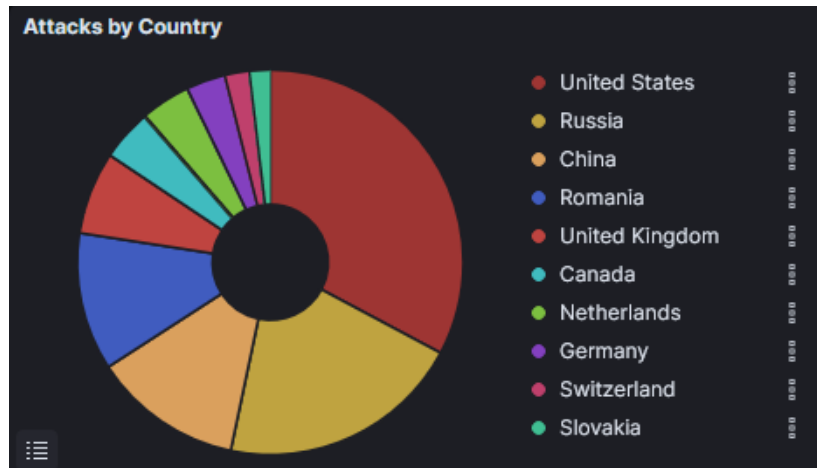
En cuanto a la **reputación de origen de los atacantes** nos encontramos con el siguiente gráfico en el que la mayor parte se compone de **atacantes conocidos**, seguido de un **escaneo masivo de redes** y finalmente **bots y rastreadores**.



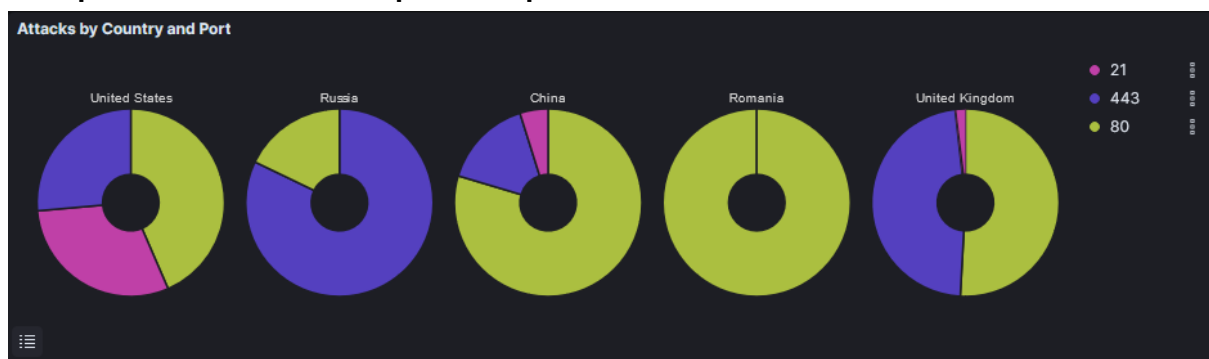
La **distribución de SO más utilizada** por los atacantes ha sido **Linux 2.2.x-3.x** seguida por Windows NT Kernel.



En el **top 10 de países** que nos han atacado se encuentran los siguientes:



Y los **puertos más atacados por cada país** han sido estos:



Los **usuarios** y **contraseñas** que más han probado han sido los siguientes:



Finalmente tenemos una recopilación en formato top 10 de las organizaciones que nos han atacado, IPs, vulnerabilidades de seguridad conocidas y las alertas de firma de Suricata.

Attacker AS/N - Top 10			Attacker Source IP - Top 10			Suricata CVE - Top 10			Suricata Alert Signature - Top 10		
AS	ASN	Count	Source IP	Count		CVE ID	Count		ID	Description	Count
43865	Intek-M LLC	149	183.136.225.32	77		CVE-2020-11899	1,963		2200007	SURICATA IPv4 padding required	6,832
14061	DigitalOcean, LLC	116	109.237.98.226	71		CVE-2019-11500 CVE...	19		2200094	SURICATA zero length padN option	2,790
58461	No.288,Fu-chun Road	84	109.237.97.180	70		CVE-2008-3802 CVE...	3		2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read	1,963
204229	Sevastre Cosmin Mihai Persoana FL...	45	152.89.196.211	45		CVE-2019-9621 CVE...	2		2002752	ET POLICY Reserved Internal IP Traffic	1,406
209003	Next Vision Ltd	45	178.212.63.89	45		CVE-2019-9670 CVE...	2		2027397	ET POLICY Spotify P2P Client	374
35478	Bunea TELECOM SRL	44	193.32.162.159	44		CVE-2021-41773 CVE...	2		2009582	ET SCAN NMAP -sS window 1024	320
51852	Private Layer INC	23	192.168.4.3	36		CVE-2018-10582 CVE...	1		2230003	SURICATA TLS invalid handshake message	201
6939	Hurricane Electric LLC	21	134.209.223.106	26					2230010	SURICATA TLS invalid record/traffic	201
15169	Google LLC	19	139.144.150.205	18					2210051	SURICATA STREAM Packet with broken ack	142
63949	Linode, LLC	18	143.244.50.172	16					2402000	ET DROP Dshield Block Listed Source group 1	129

La organización que más atacó a este T-Pot es **Intek-M LLC**, procedente de Rusia.
<https://ipinfo.io/AS43865>

En cuanto a las IPs la primera **183.136.225.32** procede de **China** y si la introducimos en **Talos** o **VirusTotal** podemos ver que tiene mala reputación y con todos los ataques que se encuentra relacionada esta IP.

https://www.talosintelligence.com/reputation_center/lookup?search=183.136.225.32
<https://www.virustotal.com/gui/ip-address/183.136.225.32/detection>

Las IPs **109.237.98.226**, **109.237.97.180** y **152.89.196.211** pertenecen a **Rusia**.
https://www.talosintelligence.com/reputation_center/lookup?search=109.237.98.226
<https://www.virustotal.com/gui/ip-address/109.237.98.226/detection>

Mientras que **178.212.63.89** pertenece a **Italia**, y tanto en VirusTotal como en Talos tiene una reputación neutral.
https://www.talosintelligence.com/reputation_center/lookup?search=178.212.63.89
<https://www.virustotal.com/gui/ip-address/178.212.63.89/detection>

193.32.162.159 es de **Rumanía** y tiene mala reputación en ambas.
https://www.talosintelligence.com/reputation_center/lookup?search=193.32.162.159
<https://www.virustotal.com/gui/ip-address/193.32.162.159>

134.209.223.106 es de **EEUU** y está relacionada con malware.
https://www.talosintelligence.com/reputation_center/lookup?search=134.209.223.106
<https://www.virustotal.com/gui/ip-address/134.209.223.106>

139.144.150.205 se ubica en **Londres** y también es maliciosa.
https://www.talosintelligence.com/reputation_center/lookup?search=139.144.150.205
<https://www.virustotal.com/gui/ip-address/139.144.150.205>

143.244.50.172 se encuentra en **Los Angeles (EEUU)** y tiene mala reputación.
https://www.talosintelligence.com/reputation_center/lookup?search=143.244.50.172
<https://www.virustotal.com/gui/ip-address/143.244.50.172>

En cuanto a las vulnerabilidades más destacadas nos encontramos en primer lugar con **CVE-2020-11899** tiene una puntuación de **4.8** y es una vulnerabilidad de **ejecución remota de código (RCE)** que afecta a las versiones de Windows 10 y Windows Server 2019. Esta vulnerabilidad reside en la biblioteca de gráficos de Windows (Win32k) y puede permitir que un atacante remoto ejecute código arbitrario en un sistema afectado si logra persuadir a un usuario para que abra un archivo especialmente diseñado o visite un sitio web malicioso.

<https://www.cvedetails.com/cve/CVE-2020-11899>

En segundo lugar tenemos **CVE-2019-11500** con una puntuación de **7.5** es una vulnerabilidad de seguridad que afecta a la implementación del protocolo VPN. Esta vulnerabilidad podría permitir a un atacante remoto sin autenticación acceder a la red interna de una organización que utiliza un dispositivo VPN de Pulse Secure afectado.

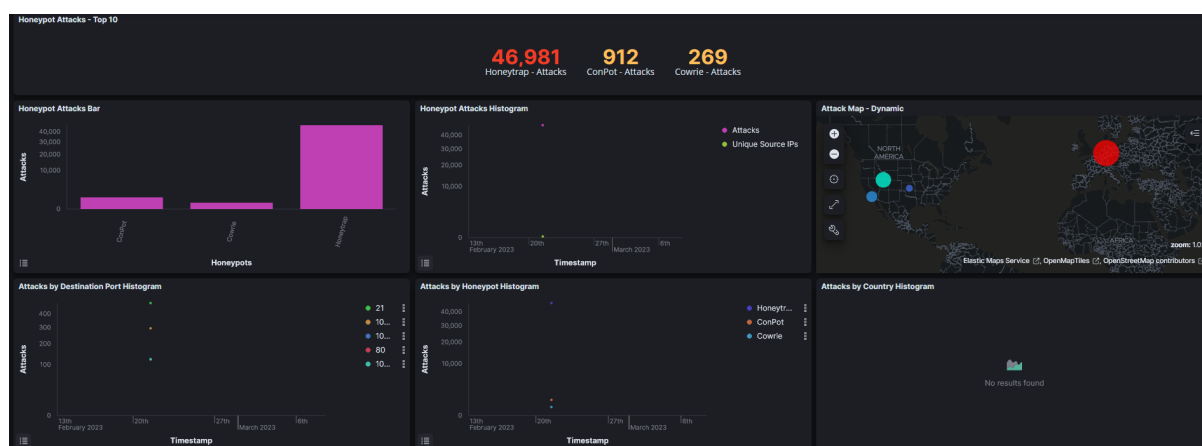
https://www.cvedetails.com/cve-details.php?cve_id=CVE-2019-11500

En el tercer puesto encontramos **CVE-2006-3602** con una puntuación de **5.0** es una vulnerabilidad de seguridad que afecta a múltiples versiones del software de navegación web Mozilla Firefox, así como a otros navegadores web basados en Mozilla, como Netscape y SeaMonkey. La vulnerabilidad se debe a un error en la forma en que el navegador maneja ciertos tipos de contenido web, lo que puede permitir a un atacante ejecutar código malicioso en el sistema de la víctima si ésta visita una página web especialmente diseñada.

https://www.cvedetails.com/cve-details.php?cve_id=CVE-2006-3602

T-Pot de España

Respecto a los T-Pot montados en España vamos a empezar mostrando la información recolectada del que tuvimos funcionando durante unas horas con todos los puertos abiertos.

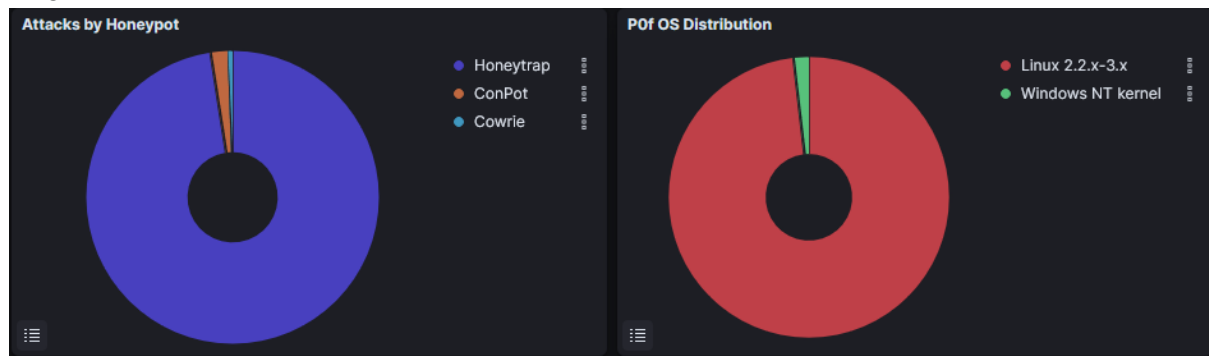


En el poco tiempo que se mantuvo online recibió un total de **48.162** ataques, repartidos entre 3 Honeytraps de los cuales **Honeytrap** recibió **46.981**, **ConPot** **912** y **Cowrie** **269**.

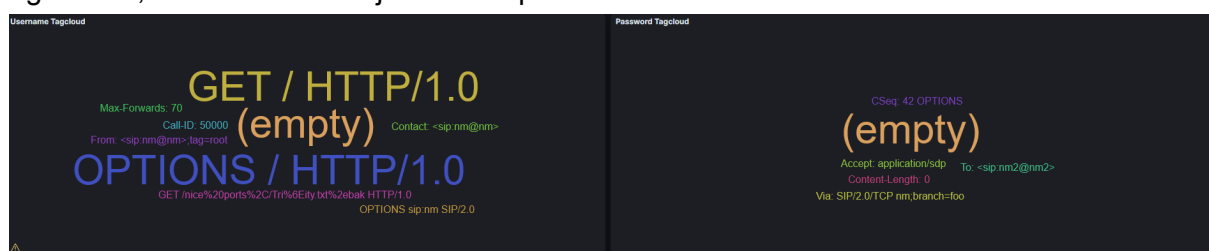
En cuanto a los **países** atacantes contamos con **Estados Unidos** y **Alemania**.

Los **puertos más atacados** por orden del que mayor número de ataques recibió al que menos son **21** (FTP), **1025** (Group Policy), **1027** (aplicaciones de servidor de correo electrónico), **80** (HTTP), **1030** (Remote Login Protocol).

Al igual que en el de México el **SO más utilizado** por los atacantes ha sido **Linux 2.2.x-3.x**



En cuanto a los usuarios y contraseñas más utilizadas por atacantes tenemos los siguientes, destacando el dejar los campos vacíos.



En este caso no se han conseguido ASNs pero se ha conseguido recolectar la información de algunas IPs y CVEs.

Attacker Source IP - Top 10		Suricata CVE - Top 10		Suricata Alert Signature - Top 10		
Source IP	Count	CVE ID	Count	ID	Description	Count
192.168.1.131	47,690	CVE-2020-11899	4,097	2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read	4,097
172.18.0.1	238	CVE-2015-0204 CVE-...	15	2200094	SURICATA zero length padN option	3,591
172.22.0.1	115	CVE-2001-0540	8	2007571	ET POLICY Remote Desktop Connection via non RDP Port	2,986
172.23.0.1	109	CVE-2002-0013 CVE-...	4	2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port	2,986
192.168.1.135	10	CVE-2008-2639	1	2013409	ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware	2,890
				2034730	ET POLICY GIOP/IIOP Request Outbound	2,871
				2200007	SURICATA IPv4 padding required	2,658
				2031489	ET POLICY SSLv3 Used in Session	1,546
				2034718	ET POLICY RMI Request Outbound	1,500
				2002752	ET POLICY Reserved Internal IP Traffic	217

Al pasar las IPs por VirusTotal todas tienen buena reputación.

En los CVEs encontrados en primer lugar contamos nuevamente con **CVE-2020-11899**.

En segundo lugar se encuentra **CVE-2015-0204** con una puntuación de **4.3**. También conocida como **FREAK (Factoring RSA Export Keys)**, es una vulnerabilidad de seguridad que afecta a ciertas versiones de sistemas operativos y navegadores web. Esta vulnerabilidad permite a los atacantes interceptar y descifrar el tráfico cifrado SSL/TLS entre un servidor web y un cliente.

https://www.cvedetails.com/cve-details.php?cve_id=CVE-2015-0204

En tercer lugar tenemos **CVE-2001-0540** tiene una puntuación de **5.0** es una vulnerabilidad de desbordamiento de búfer que afecta al software de servidor web Apache. La vulnerabilidad se debe a un error en la forma en que el servidor Apache maneja las solicitudes HTTP que contienen ciertos caracteres especiales en los nombres de archivo o directorio.

Un atacante puede aprovechar esta vulnerabilidad enviando una solicitud HTTP maliciosa al servidor Apache, que contenga una cadena especialmente diseñada con caracteres de escape que pueden desencadenar un desbordamiento de búfer en el servidor. Si el ataque es exitoso, el atacante puede ejecutar código malicioso en el servidor web y obtener acceso no autorizado a la información del sistema, archivos y otras actividades maliciosas.

https://www.cvedetails.com/cve-details.php?cve_id=CVE-2001-0540

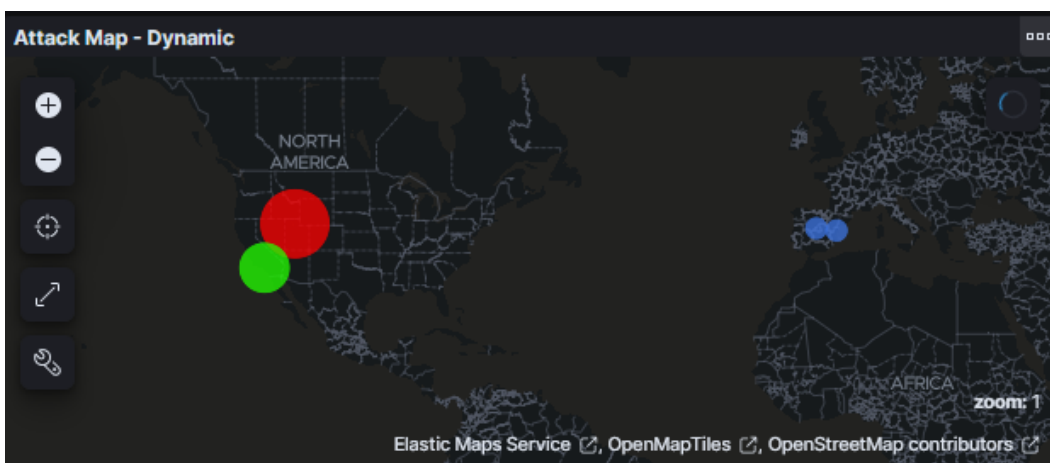
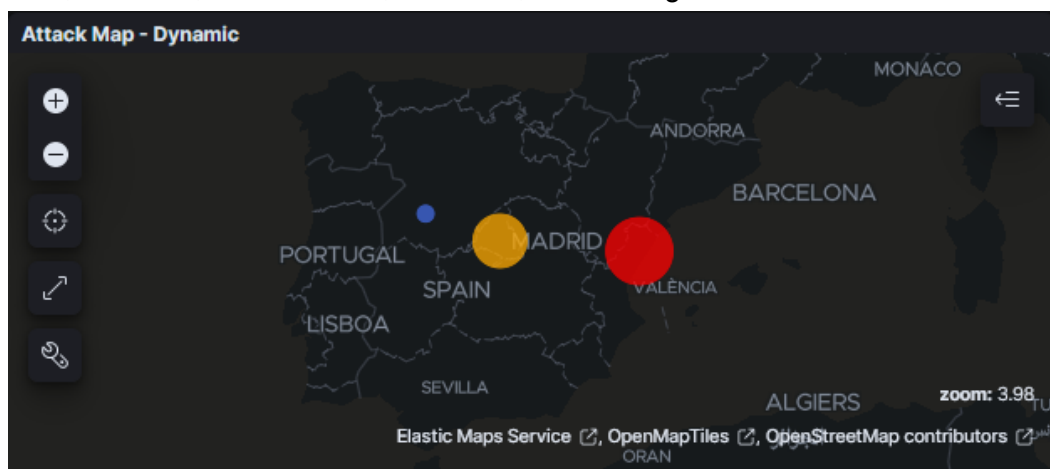
T-Pot de España con 5 puertos abiertos

Respecto a este T-Pot no tenemos demasiada información en los dashboards, ya que no nos muestra información en la mayoría de ellos, pero vamos a recopilar los paneles que contienen información.

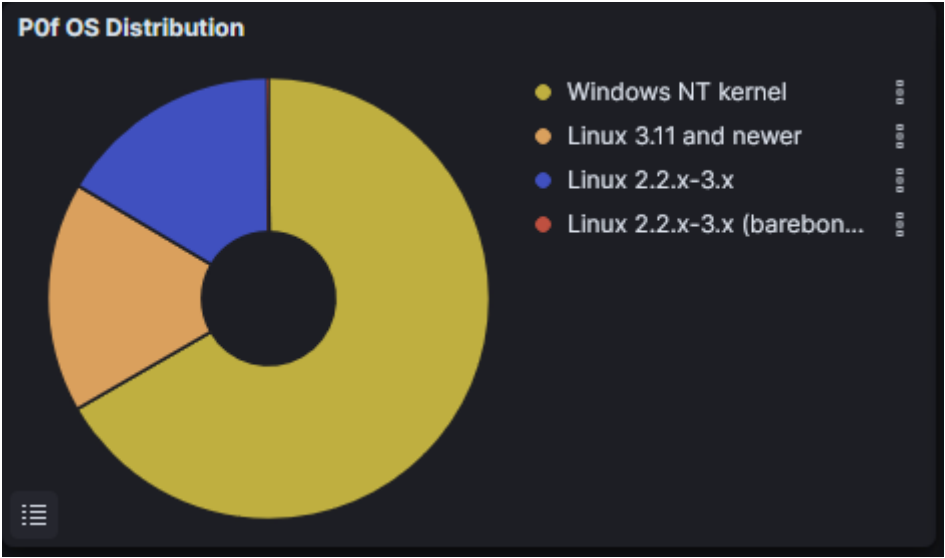
En este caso se abrieron los puertos **80** (HTTP), **21** (FTP), **22** (SSH), **25** (SMTP) y **53** (DNS).

Tenemos un total de **291 ataques**, de los cuales 8 procedían de España y el resto de EEUU.

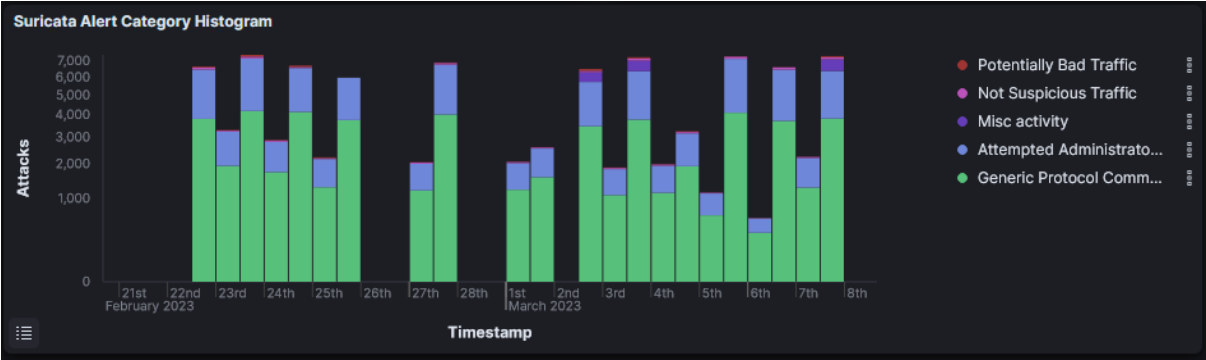
4 Valencia, 3 Madrid, 1 Salamanca, 198 Utah, 85 Los Angeles.



En este caso el **SO más utilizado** por los atacantes es **Windows NT kernel**



En las alertas de Suricata destacan la decodificación de comandos de protocolo genérico y el intento de ganar privilegios de administrador.



Y finalmente en las vulnerabilidades de seguridad conocidas solo nos encontramos de nuevo con **CVE-2020-11899**.

Suricata CVE - Top 10			Suricata Alert Signature - Top 10		
CVE ID	Count		ID	Description	Count
CVE-2020-11899	36,489		2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read	36,489
			2200094	SURICATA zero length padN option	31,442
			2200007	SURICATA IPv4 padding required	22,713
			2027397	ET POLICY Spotify P2P Client	1,517
			2100384	GPL ICMP_INFO PING	973
			2100408	GPL ICMP_INFO Echo Reply	973
			2002752	ET POLICY Reserved Internal IP Traffic	741
			2100401	GPL ICMP_INFO Destination Unreachable Network Unreachable	13
			2100254	GPL DNS SPOOF query response with TTL of 1 min. and no authority	4
			2210048	SURICATA STREAM reassembly sequence GAP -- missing packet(s)	4