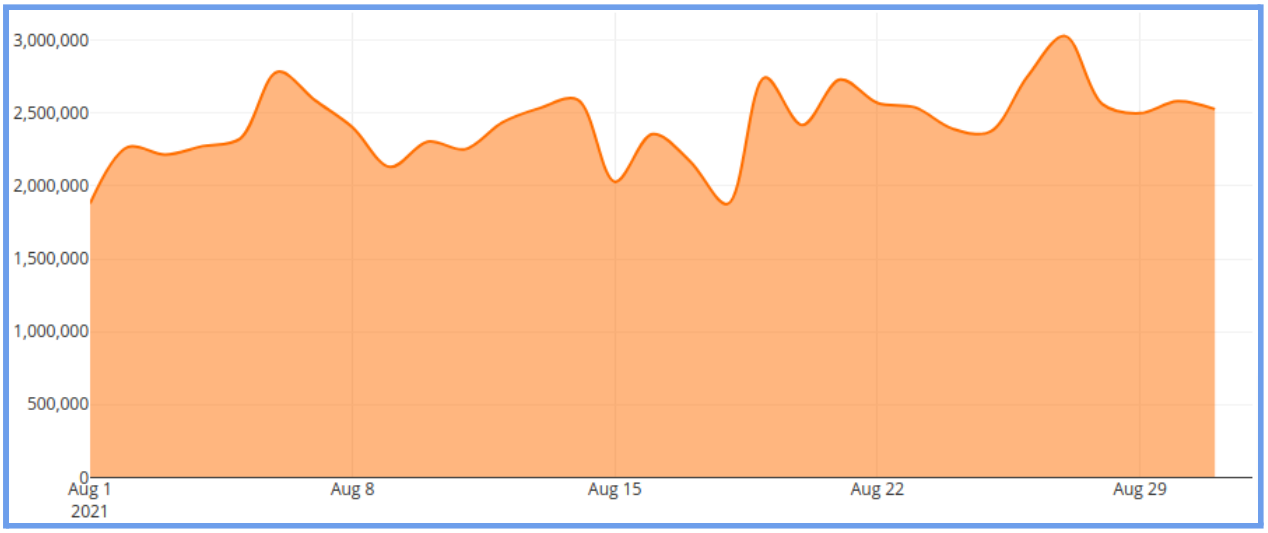
Reporte de actividad del proyecto

Despliegue de un IoT honeypot en América Latina y el Caribe

Agosto 2021

Gracias a la capacidad de extracción de datos para la generación de reportes, se pueden reportar para este mes los siguientes resultados.

Actividad de registro de datos en el sistema



El día hubo un un pico de actividad que llegó a superar ligeramente los 3 millones de mensajes procesados, manteniéndose normalmente en un promedio de aproximadamente 2.5 millones. Los días 1 y 18 fueron los de más baja actividad, con poco más de 18 millones de mensajes. Todo responde a un comportamiento normal.

Totales de mensajes y direcciones IP origen

Mensajes procesados:	Direcciones IP de origen:
75,141,605	643,278

Durante el mes se procesaron poco más de 75 millones de mensajes provenientes del proyecto de sensores, algo más de 5 millones menos que el mes anterior. Originados de casi 650 mil direcciones IP de origen distintas, alrededor del mundo, unas 250 mil menos en relación al mes anterior. Más abajo se desglosan estos orígenes por países.

Productos: Fabricantes y tipos más accedidos

Fabricante	Producto	Tipo	Eventos
Huawei	Huawei Home Gateway HG532	router	33621

Microsoft	Exchange	email	27848
MVPower	MVPower DVR	video-system	26220
Fortinet	FortiOS	firewall	25585
Realtek	Realtek SDK	embedded-system	13403
Dasan	Dasan GPON Home Router	router	12498
	Dasan GPON ONT WiFi Router H640X	router	1
Oracle	WebLogic Server	app-server	4403
	Oracle Weblogic Server	app-server	2782
MobileIron	MobileIron Mobile Device Management (MDM)	device-management-platform	4864
Zyxel	Eir D1000	router	4309
Netgear	Netgear DGN1000	router	3558
	NETGEAR R/D Series Routers	router	460

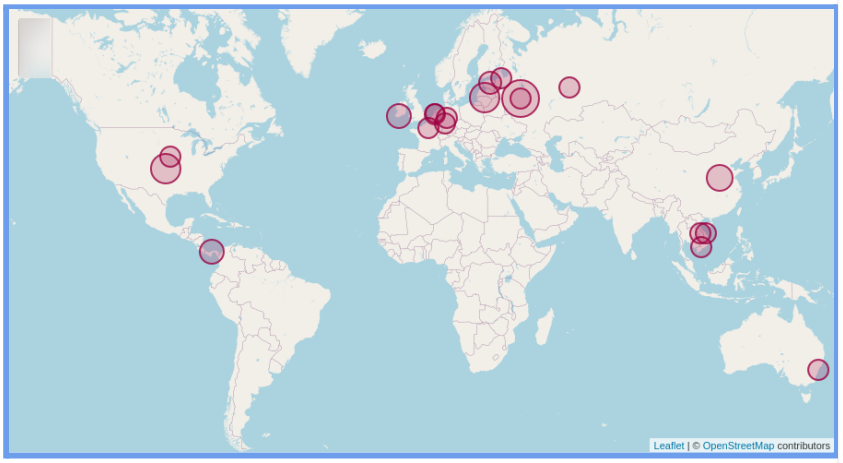
En el período, el sistema más asediado fue el gateway de hogar huawei HG532. Le sigue el servidor de correo Exchange de Microsoft y en tercer lugar, el sistema de DVR de marca MVPower, aunque muy cerca está el sistema de Fortinet.

Países de origen de conexiones

Tabla de conexiones por país:

País	Conexiones
RU	10796508
CN	7463152
LT	7091825
VN	6639398
DE	2893493
NL	2822593
KR	2271015
IN	1692935
GB	1469901
AU	1399475

Representación Geográfica de orígenes:



Cerca del 21% de las conexiones provinieron de Rusia, casi duplicando las conexiones desde China, siendo estos dos los que en total abarcan el 35.4% de las conexiones tabuladas. Lituania está cerca de China con casi el 14% y le sigue Vietnam con casi el 13%.

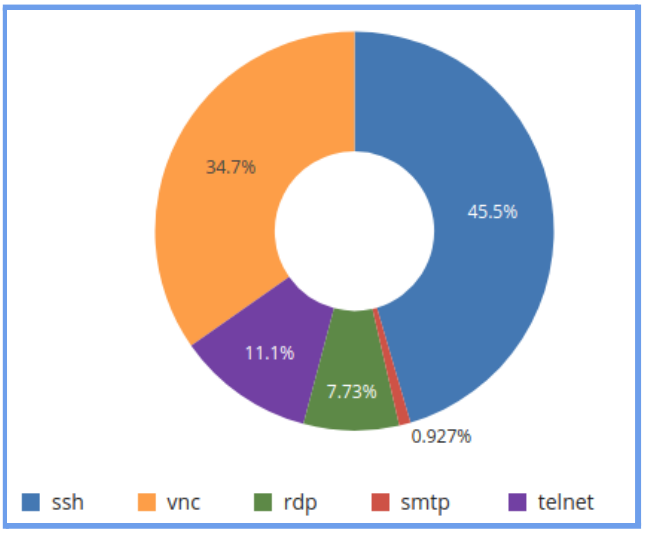
PA	1119310
BR	954049
MD	915665
HK	741764
SG	730692
FR	709004
PL	690207
BD	601690
ID	589750

En LAC, Panamá destaca con cerca del 2.87%, siguiéndole Brasil con el 1.85%.

💡 Es de notar que en el mapa no se representan todos los países de la lista tabulada, pues algunos países, como Estados Unidos, tienen geográficamente más de una ubicación (Ciudad) de origen, por lo que en el mapa se grafican sólo las 20 principales ubicaciones, no necesariamente consolidadas por país, que es lo que justamente se tabula a la izquierda.

Protocolos más accedidos

De las conexiones registradas, los protocolos que más se usan para acceder a los sistemas, son los representados en la siguiente imagen.



Cabe indicar que sólo se grafican los 5 primeros, pues a partir del 6to en adelante los valores realmente son muy pequeños, considerando que el propio protocolo SMTP en la gráfica (5to en presencia) sólo tiene un 0,93% de ocurrencia.

Usuarios y contraseñas más usados

Finalmente se presenta el top 20 de usuarios y contraseñas más comúnmente usados para acceder a los sistemas emulados por los distintos sistemas de honeypot en los diferentes sensores de la red:

Usuario	Ocurrencias	Porcentaje	Contraseña	Ocurrencias	Porcentaje
`admin`	251259	31.74 %	`password`	80355	12.81 %
`user`	66390	8.39 %	`1234`	66694	10.63 %

default	44995	5.68 %	**admin**	59137	9.42 %
test	44464	5.62 %	**123**	58366	9.30 %
support	35846	4.53 %	**12345**	56281	8.97 %
guest	32080	4.05 %	**1**	41894	6.68 %
administrator	30633	3.87 %	**12345678**	32067	5.11 %
ubuntu	29251	3.70 %	**test**	30312	4.83 %
user1	27184	3.43 %	**123456789**	24743	3.94 %
postgres	26178	3.31 %	**qwerty**	21948	3.50 %
web	25982	3.28 %	**passw0rd**	21368	3.41 %
ubnt	25714	3.25 %	**1234567**	20729	3.30 %
admin1	25693	3.25 %	**admin123**	20478	3.26 %
demo	23306	2.94 %	**root**	16547	2.64 %
tech	21869	2.76 %	**pass**	15644	2.49 %
oracle	21222	2.68 %	**88888888**	15585	2.48 %
MikroTik	20690	2.61 %	**11**	15328	2.44 %
profile1	20184	2.55 %	**admin1**	15195	2.42 %
telecomadmin	18559	2.34 %	**user**	14847	2.37 %