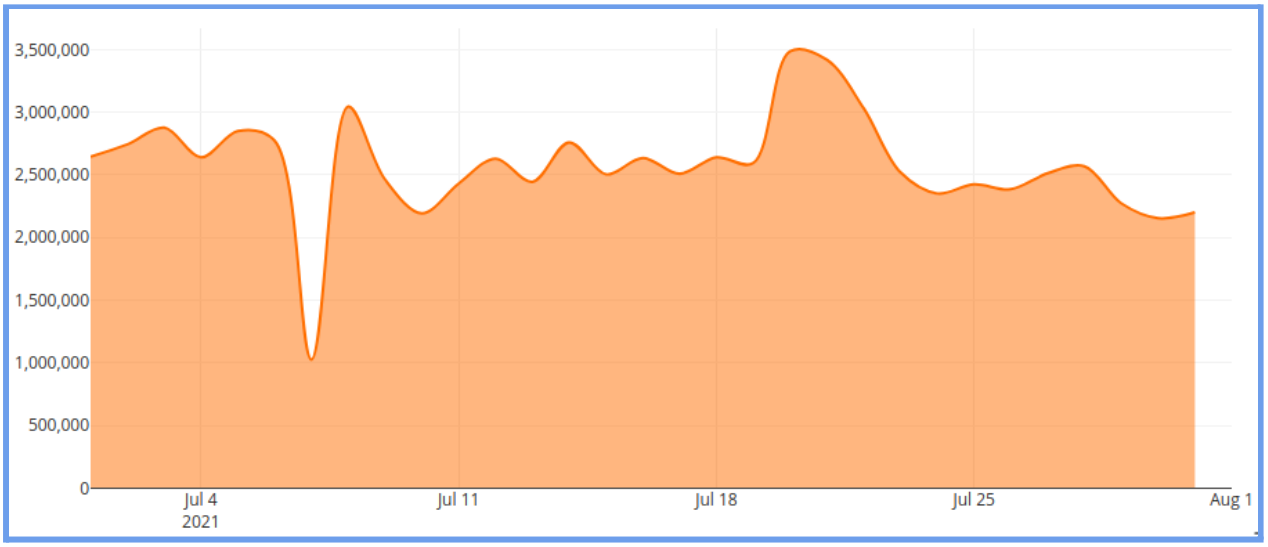
Reporte de actividad del proyecto

Despliegue de un IoT honeypot en América Latina y el Caribe

Julio 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 20 de julio hubo un un pico de actividad que llegó a los 3.5 millones de mensajes procesados, manteniéndose normalmente en un promedio de aproximadamente 2.6 millones. El día 7 se procesaron sólo poco más de 1 millón de mensajes. Todo responde a un comportamiento normal.

Totales de mensajes y direcciones IP origen

Mensajes procesados:	Direcciones IP de origen:
79,749,574	893,005

Durante el mes se procesaron cerca de 80 millones de mensajes provenientes del proyecto de sensores, casi 20 millones más que el mes anterior. Originados de casi 900 mil direcciones IP de origen distintas, alrededor del mundo, más que duplicando este valor 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	36342

Microsoft	Exchange	email	29639
Realtek	Realtek SDK	embedded-system	21606
Dasan	Dasan GPON Home Router	router	15413
	Dasan GPON ONT WiFi Router H640X	router	9
Fortinet	FortiOS	firewall	9445
MVPower	MVPower DVR	video-system	8592
Oracle	WebLogic Server	app-server	4725
	Oracle Weblogic Server	app-server	2637
MobileIron	MobileIron Mobile Device Management (MDM)	device-management-platform	4912
Zyxel	Eir D1000	router	4189
Netgear	Netgear DGN1000	router	3200
	NETGEAR R/D Series Routers	router	703

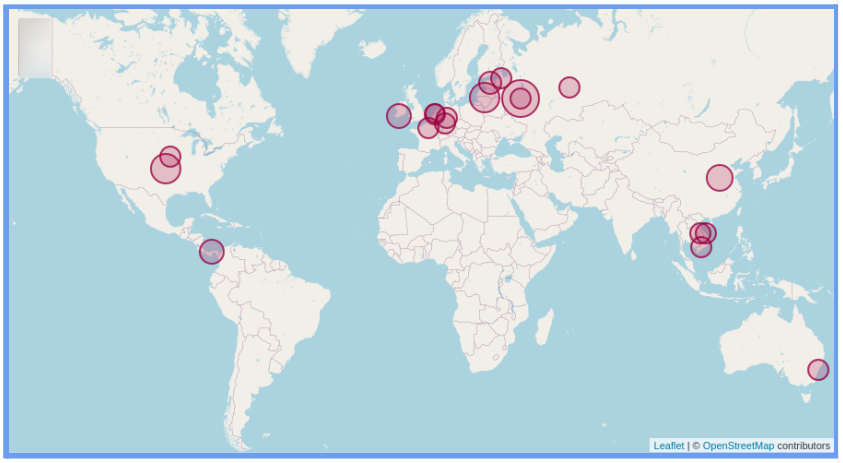
En el período, el sistema más asediado fue el gateway de hogar huawei HG532. Le sigue el servidor de correo Exchange de Microsoft y en tercer lugar, un sistema embebido de Realtek.

Países de origen de conexiones

Tabla de conexiones por país:

País	Conexiones
US	12800179
CN	7202296
LT	6793887
VN	3674971
IE	3651258
PA	3365774
NL	2467971
DE	2316023
KR	1933810
AU	1846442
EE	1782930

Representación Geográfica de orígenes:



Cerca del 23% de las conexiones provinieron de Estados Unidos, casi duplicando las conexiones desde China, siendo estos dos los que en total abarcan el 35.5% de las conexiones tabuladas. Lituania está muy cerca de China con el 12%. Le siguen Vietnam e Irlanda valores alrededor del 6.5%.

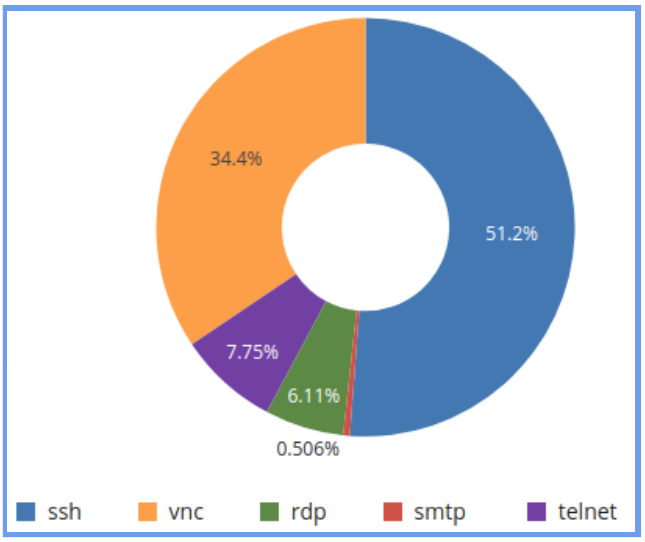
IN	1673681
FR	1423452
GB	1325675
PL	934520
HK	895448
BR	893843
SG	754048
BD	607032

En LAC, Panamá destaca con cerca del 6%, siguiéndole Brasil con el 2.35%.

💡 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 0,5% 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
`root`	1525143	73.09 %	`123456`	63510	12.20 %
`admin`	175487	8.41 %	`password`	53362	10.25 %

user	49549	2.37 %	**admin**	51802	9.95 %
default	48841	2.34 %	**1234**	45757	8.79 %
support	30338	1.45 %	**12345**	38768	7.44 %
guest	26323	1.26 %	**123**	27473	5.28 %
administrator	23516	1.13 %	**root**	26540	5.10 %
ubnt	23291	1.12 %	**1**	23841	4.58 %
admin1	20887	1.00 %	**12345678**	20702	3.98 %
user1	19678	0.94 %	**default**	18571	3.57 %
web	19452	0.93 %	**test**	18483	3.55 %
tech	18762	0.90 %	**123456789**	17118	3.29 %
MikroTik	18144	0.87 %	**1234567**	16643	3.20 %
profile1	17545	0.84 %	**qwerty**	15782	3.03 %
demo	17404	0.83 %	**admin123**	14970	2.87 %
telecomadmin	16251	0.78 %	**passw0rd**	14635	2.81 %
test	14184	0.68 %	**88888888**	13652	2.62 %
ubuntu	8357	0.40 %	**11**	13417	2.58 %
postgres	6864	0.33 %	**admin1**	13052	2.51 %
supervisor	6784	0.33 %	**1122**	12674	2.43 %